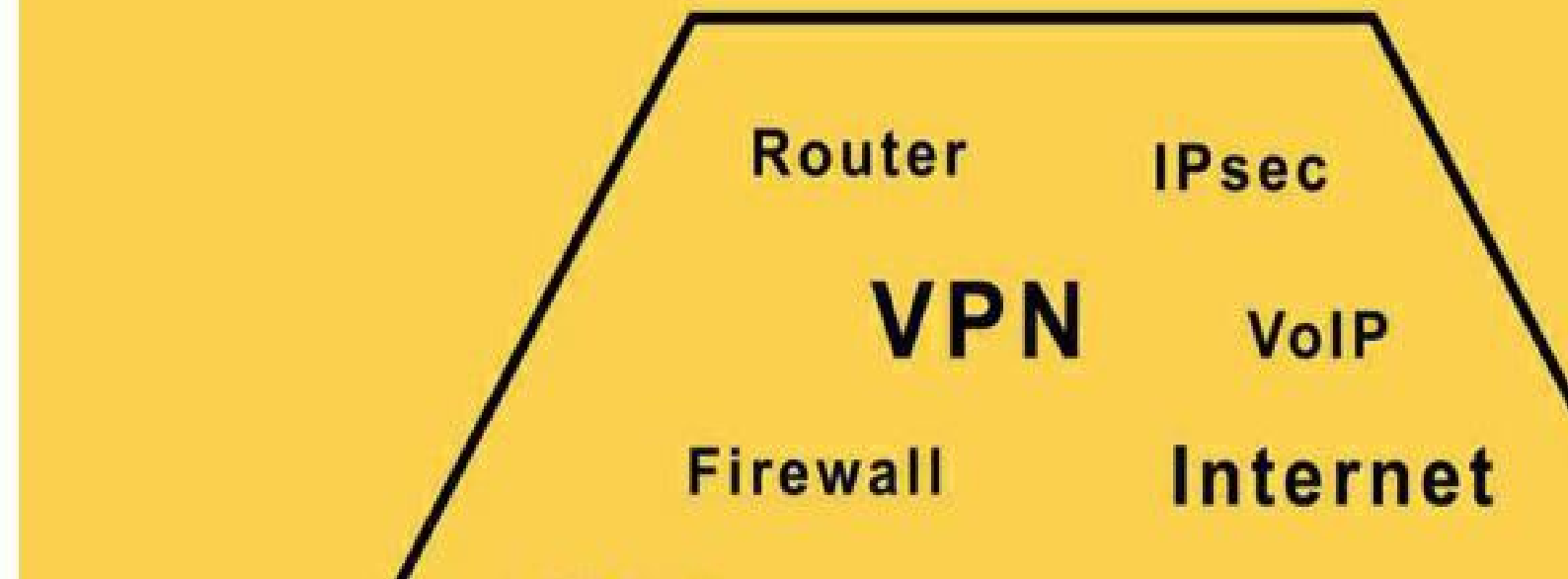
Patrick S

Netzwerktechnik-F

Gr

Übertragung

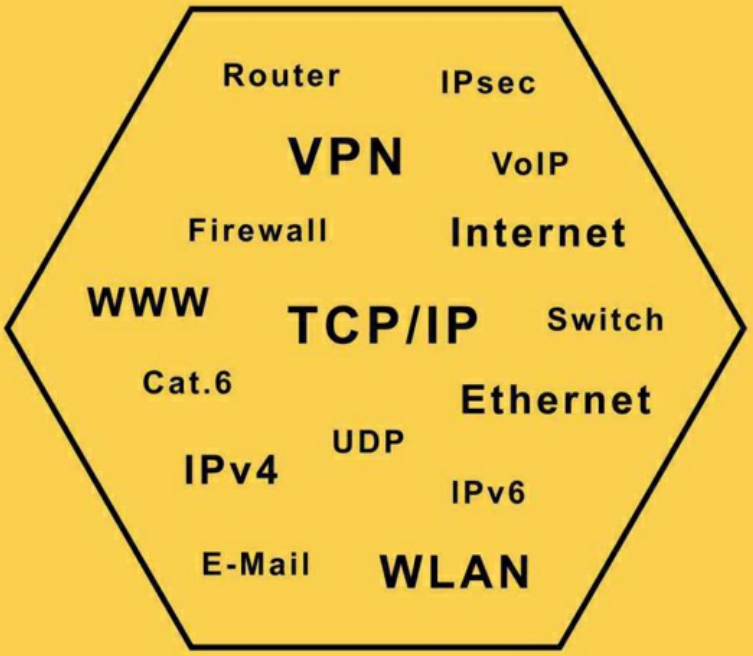
S



Patrick Schnabel

Netzwerktechnik-Fibel

Grundlagen
Übertragungstechnik
TCP/IP
Dienste
Sicherheit



http://www.netzwerktechnik-fibel.de/

http://www.elektronik-kompendium.de/

Netzwerktechnik-

Fibel

Patrick Schnabel

Dezember 2012

Grundlagen der

Netzwerktechnik

Übertragungstechnik

TCP/IP

Anwendungen und Dienste

Netzwerk-Sicherheit

http://www.netzwerktechnik-fibel.de/

http://www.elektronik-kompendium.de/

Vorwort

Im Jahr 2004 erschien die Erstausgabe der Netzwerktechnik-Fibel im Rahmen der Webseite Elektronik-Kompendium.de. Für die eBook-Ausgabe habe ich den Inhalt auf den aktuellen Stand bebracht. Insbesondere im Bereich WLAN nach IEEE 802.11. Das ist der Teilbereich der

Netzwerktechnik, in der Weiterentwicklungen recht schnell voranschreiten.

Die Absicht dieses Buches ist, dem Leser ein besseres Verständnis für Netzwerktechnik und die Zusammenhänge nahe zu bringen. Durch die Netzwerktechnik-Fibel ist es möglich, die grundlegenden Kenntnisse über Netzwerke, Protokolle und Dienste zu erwerben und die wechselseitigen Abhängigkeiten zu verstehen.

In diesem Buch werden nur die Themen beschrieben, die zum Grundverständnis wirklich notwendig sind. Dieses Buch soll Grundlagen vermitteln, Zusammenhänge erklären und das große Thema Netzwerktechnik als Ganzes erfassbar machen. Experten für Netzwerktechnik mögen mir die oft verkürzte Darstellung verzeihen. Mir kommt es vor allem auf grundlegendes

Wissen und Verständnis an. Dabei ist es notwendig die eine oder andere Komplexität zu vereinfachen.

In der Netzwerktechnik kommt es gelegentlich vor, dass die neue Technik zur alten Technik kompatibel ist.

Deshalb sind in diesem Buch auch einige "Altlasten" beschrieben, obwohl sie eigentlich in der Praxis nicht mehr zur Anwendung kommen.

In der Praxis noch wenig relevant, aber in Zukunft sehr wichtig ist das Thema IPv6. Aus diesem Grund ist IPv6 in diesem Buch an vielen Stellen berücksichtigt.

Dieses Buch ist eine Ergänzung für die schulische und betriebliche Aus- und Weiterbildung, die sich am Stoffplan orientiert. Wird dieser zu schnell durchgearbeitet, dann können Fragen oder Wissenslücken entstehen, die mit der Netzwerktechnik-Fibel schnell und präzise beantwortet bzw. aufgefüllt

werden können. Dieses Buch wendet sich also an all diejenigen, die sich mit den Grundlagen der Netzwerktechnik und darüber hinaus befassen möchten. In diesem Sinne soll die Netzwerktechnik-Fibel ein treuer Begleiter durch das Thema Netzwerktechnik sein.

Wenn Ihnen dieses Buch gefällt und nützt, dann sagen Sie es weiter. Wenn Sie Anregungen und Verbesserungsvorschläge für mich haben, dann nehme ich die gerne entgegen. Sie erreichen mich unter der E-Mail-Adresse Patrick.Schnabel@das-elko.de.

Begleitend zum Buch empfehle ich die Webseite http://www.elektronik-kompendium.de/. Dort gibt es noch viel mehr Informationen zu den Themen Netzwerktechnik, Computertechnik, Kommunikationstechnik und Elektronik.

Abonnieren Sie den Newsletter oder

RSS-Feed. So bleiben Sie regelmäßig auf dem neusten Stand.

Ich wünsche Ihnen viel Freude und neue Erkenntnisse beim Lesen.

Patrick Schnabel

Grundlagen der Netzwerktechnik

Grundlagen

Schichtenmodelle

Netzwerk-Kabel

Netzwerk-Komponenten

Grundlagen Netzwerktechnik

Als es die ersten Computer gab, waren diese sehr teuer. Vor allem 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 die 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?

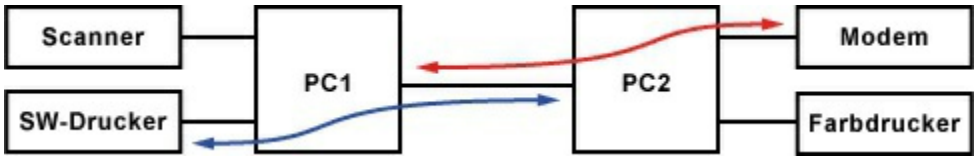
Ein Netzwerk ist die physikalische und logische Verbindung von Computersystemen. Ein einfaches Netzwerk besteht aus zwei Computersystemen. Sie sind über ein Kabel miteinander verbunden und somit in der Lage ihre Ressourcen gemeinsam zu nutzen. Wie Daten, Speicher, Drucker, Faxgeräte, Scanner, Programme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

Datenübertragung im Netzwerk

Die Datenübertragung kann grundsätzlich auf zwei Arten erfolgen. Entweder verbindungsorientiert oder verbindungslos.

Bei der verbindungsorientierten Datenübertragung wird vor dem Austausch der Daten erst eine logische

Verbindung aufgebaut. Während der Übertragung bleibt die Verbindung zwischen den Kommunikationspartnern aufrechterhalten. Die logische Verbindung bleibt solange 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 unabhängige und separate Einheiten geteilt. Die Übertragung jeder Einheit wird als abgeschlossener Vorgang behandelt. Je nach Technik wird die Einheit als Datenpaket, Frame oder Datagramm bezeichnet.

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.

Beispiel: File-Server oder Datei-Server

Ein File- oder Datei-Server ist ein Computer, dessen typische Anwendung die zentrale Datenspeicherung ist. Während man auf einem Client Dateien bearbeitet, werden sie auf dem Server gespeichert. Das ermöglicht auch eine zentrale Datensicherung und Zugriffsteuerung.

Auf dem File-Server kommt ein Betriebssystem zum Einsatz, das den gleichzeitigen Zugriff mehrerer Clients organisiert. Auf dem File-Server sind die Zugriffe der Clients auf bestimmte Ressourcen beschränkt. Zum Beispiel auf einzelne Verzeichnisse oder Dateien.

Beispiel: Datenbank-Server

Bestimmte Daten liegen nicht in Form von Dateien vor, sondern werden in strukturierter Form in Datenbanken gespeichert. Datenbanken sind im Prinzip große Dateien, in denen Daten in strukturierter Form abgelegt sind. Eine Datenbank-Software ermöglicht den Zugriff auf diese Daten. Dabei wird über eine eigene Datenbank-Sprache eine Abfrage an die Datenbank gestellt. Die Abfrage der Daten wird vom Benutzer über eine Software auf seinem Rechner durchgeführt. Die Software stellt dann eine Verbindung zur Datenbank her und

fordert die Daten an. Die Datenbank stellt die zur Abfrage passenden Daten meist tabellarisch zusammen und schickt sie zurück. Die Software auf dem Client ist dann für die Darstellung der Daten verantwortlich.

Beispiel: Groupware

Groupware ist eine spezielle Software, die die Zusammenarbeit in Arbeitsgruppen fördert, Arbeitsabläufe vereinfacht und automatisiert. Wenn in einem Netzwerk die enge Zusammenarbeit zwischen Netzwerkteilnehmern möglich sein soll, dann kommt eine Groupware-Software zum Einsatz. Sie bietet folgende Möglichkeiten:

E-Mail

private, gemeinsame und öffentliche Terminkalender

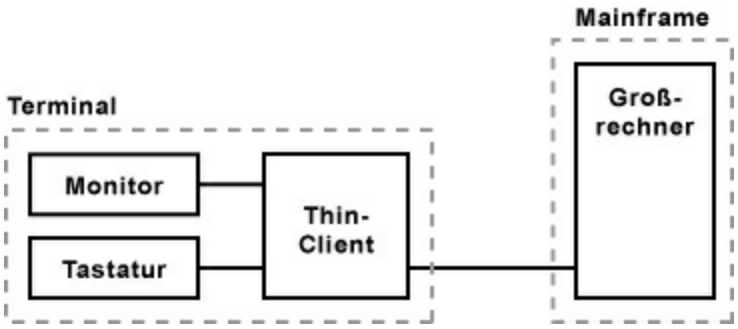
zentrales Adressbuch

Dokumentbearbeitung im Team

Zugriffsmöglichkeiten auf

Datenbanken

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 Grundbegriffe hat didaktische Gründe und ist deshalb nicht alphabetisch sortiert.

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.

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.

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.

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) 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 TCP/UDP ist eine Art Netzwerkadresse, 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.

Switching

In einem geswitchten Netzwerk bestimmt ein konstanter Pfad mit einer definierten Bandbreite, welchen Weg die Datenpakete gehen. Wenn das

Datenpaket abgeschickt wird, steht der Weg durch das Netzwerk praktisch schon fest. Switching eignet sich für Anwendungen, die eine definierte Bandbreite benötigen.

Routing

In einem gerouteten Netzwerk werden die Datenpakete nicht zwingend auf vorgegebenen Übertragungswegen vermittelt. Die Vermittlungsstationen entscheiden bei jedem Datenpaket aufs Neue, welchen Weg sie gehen. Im Prinzip suchen sich die Datenpakete ihre Weg zum Empfänger selber.
Geroutete Netzwerke sind wesentlich flexibler und effizienter bei der Netzwerkauslastung.

Tunneling

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

eingebettet ist.

Broadcast / Broadcasting

Beim Broadcasting werden die Daten an einem Punkt eingespeist und von dort an alle Teilnehmer übertragen. Dabe empfängt jeder Teilnehmer 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, Terestrisch) gemacht wird.

Unicast / Unicasting

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

Multicast / Multicasting

Beim Mulitcasting 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.
Doch viele gewöhnliche Router unterstützen kein Multicasting.

Backbone

Backbone ist eine Bezeichnung für die Hauptübertragungsstrecke in einem Netzwerk. Er besteht in der Regel aus mehreren Netzknoten, die untereinander verbunden sind. Die Netzknoten sind die Zugangspunkte zum Backbone. Man spricht auch vom Kernnetz oder Core Network.

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 und die Protokolle eines anderen Netzes konvertiert werden.

Server

Ein Server ist ein Computer in einem Netzwerk, der anderen Computern Ressourcen zur Verfügung stellt. Ressourcen können Speicherplatz, Rechenleistung oder Dienste sein.

Host

Ein Host ist ein Computer oder Rechner, der in einem Netzwerk anderen Computern Dienste bereitstellt. Einen Host bezeichnet man manchmal auch als Server.

Station

Der Begriff Station ist eine allgemeine

Bezeichnung für ein Gerät innerhalb eines Netzwerks, das aktiv innerhalb des Netzwerks agiert.

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 oder Switche die Netzknoten.

Knoten sind häufig auch die Zugangspunkte zum Netzwerk.

Leitungen und Kabel

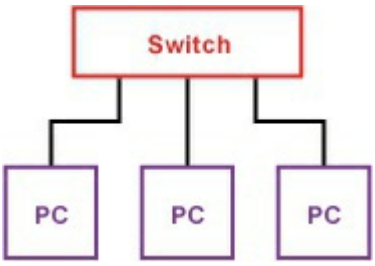
Die Begriffe Leitungen und Kabel werden häufig gleichwertig verwendet. Doch das ist nicht ganz richtig. Leitungen und Kabel kann man folgender Maßen unterscheiden. Kabel sind Leitungen, die im Boden oder auf hoher See (Meeresboden) verlegt werden. Was man sehen kann sind Leitungen, Kabel

sieht man nicht wenn sie genutzt werden.
Umgangssprachlich sagen die meisten Menschen zur Leitung Kabel, was falsch (unfachlich) ist. Es ist die häufigste Fehlbenennung in der Elektrotechnik und Informationstechnik, noch vor der Glühbirne.
Kabel ist kürzer und damit das schneller gesprochene Wort. Daher ist der falsche Begriff in vielen Bereichen üblich auch wenn es falsch ist. So befinden sich auf der Kabeltrommel kein Kabel, sondern eine Leitung. Aber den Begriff Leitungstrommel wird man im Fachhandel sicher nichts finden. Netzwerkleitung sagt auch niemand, obwohl das korrekt wäre.

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



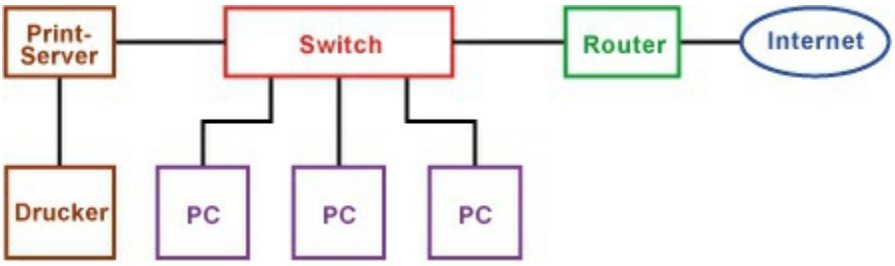
auf wenige Stationen beschränkt. Die Anzahl der Stationen kann auch mehrere hundert oder tausend betragen. Wenn es sich dabei zum Beispiel um das LAN eines großen Unternehmens handelt.

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 ein Kopplungselement notwendig. Das Kopplungselement sorgt für eine physikalische und logische Verbindung zwischen den Computersystemen

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

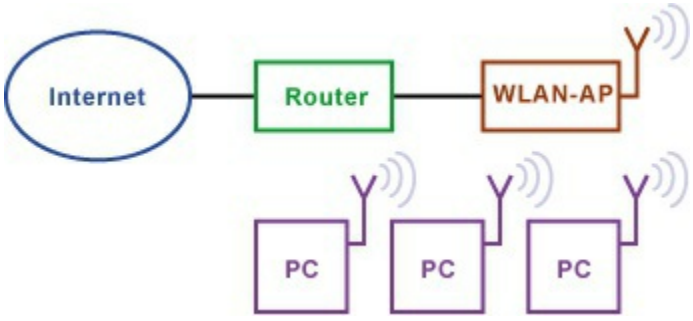


Ein lokales Netzwerk mit Internet-Zugang besteht in der Regel aus einem Switch und einem Router. Der Switch dient auch hier als Kopplungselement. Der Internet-Zugang erfolgt über einen

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.

Netzwerk-Komponenten in einem LAN

Repeater / Hub

Medienkonverter

Bridge

Switch

Router

Gateway

Server

Proxy

Printserver

Vernetzungstechnik im

Vergleich

Technik

Reichweite

Bandbreite

HomePNA max. 150 m

10 MBit/s

Home-

Plug-

Wohnung/Einfamilienhaus 200 MBit/s

Powerline

Bluetooth Zimmer/Wohnung

WLAN

typ. 20 m

54 MBit/s

IEEE

802.11g

WLAN

IEEE

typ. 20 m

300 MBit/s

802.11n

Fast-

100 m

100 MBit/s

Ethernet

Gigabit-

100 m

Ethernet

WLAN - Wireless

LAN

Wireless LAN (WLAN) ist als

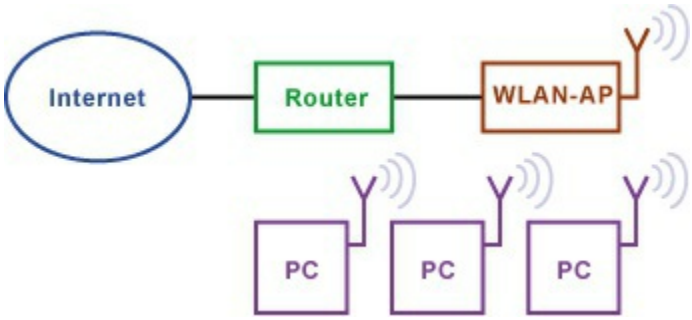
Oberbegriff für alle auf dem Markt

befindlichen drahtlosen lokalen

Datennetze zu verstehen. Darunter fallen

auch Bluetooth, HomeRF und HiperLAN. Und selbstverständlich alle anderen Techniken und Standards mit denen sich drahtlose Funknetzwerke aufbauen lassen.

Allerdings bezeichnet "WLAN" im allgemeinen Sprachgebrauch ein Funknetzwerk nach IEEE 802.11.



Die mobile Arbeitswelt verlangt häufig nach einer Datenverarbeitung und Datenübertragung, deren Bewegungsradius nicht durch Leitungen eingeschränkt ist. Die Lösung ist ein drahtloses Funknetz, auch Wireless LAN (WLAN) genannt.

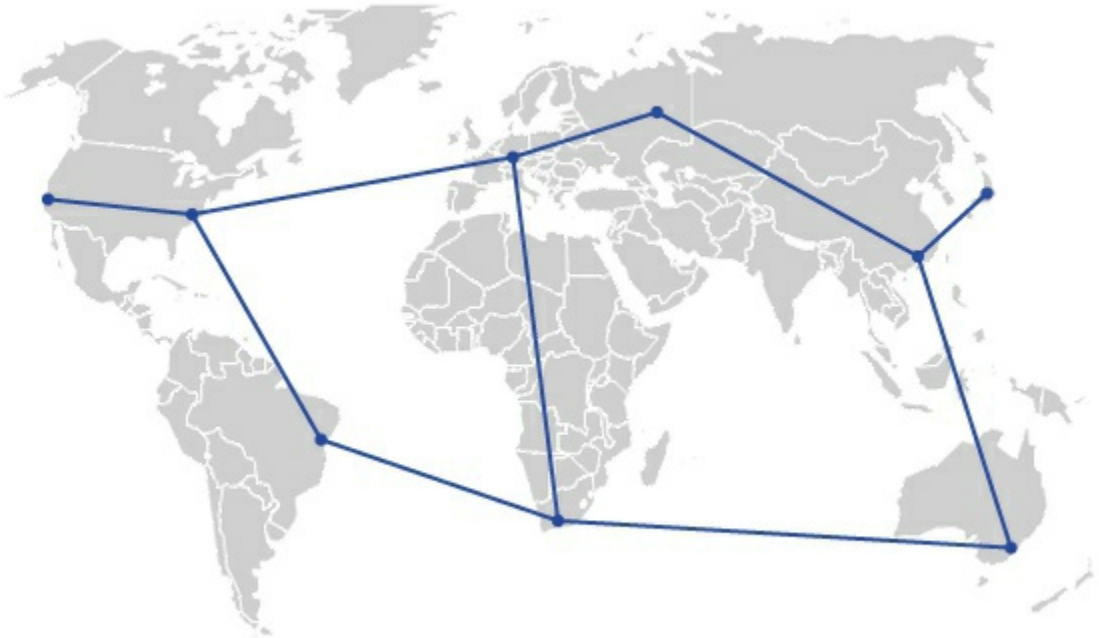
WLAN steht für ein Wireless Local Area Network, ein drahtloses bzw. schnurloses lokales Netzwerk. Anstatt

Daten über ein Kabel zu übertragen,
dient die Luft als Übertragungsmedium
und als Schnittstelle, die sich per Funk
nutzbar machen lässt. Diese
Ungebundenheit erlaubt ungeahnte
Möglichkeiten der Mobilität und des
Komforts.
Ein beliebiger Arbeitsplatz in
einem provisorischen Büro.
Zuhause auf dem Balkon oder der
Terrasse.
Überall dort, wo keine
Netzwerkverkabelung möglich oder
zu teuer ist.
WLAN-Fähigkeit sind im Regelfall in
allen wichtigen Computersystemen
integriert. Und wenn nicht, lässt sich das
meist günstig nachrüsten. In der Regel ist
der Aufwand und die Kosten für ein
WLAN niedriger als für ein
kabelgebundenes Netzwerk.

WFA - Wi-Fi Alliance

Die Wi-Fi Alliance ist ein Herstellerverband, der freiwillige Kompatibilitätsprüfungen durchführt und danach ein Siegel für die geprüften Geräte vergibt. WLAN-Geräte nach IEEE 802.11 mit einem solchen Siegel arbeiten mit hoher Wahrscheinlichkeit mit den Geräten unterschiedlicher Hersteller zusammen.

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 größtmöglich 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.

SDH/SONET

Weitverkehrsnetze werden in Europa mit der Transporttechnik SDH und in Amerika mit SONET betrieben. Beide Systeme sind nahezu identisch. Die Bandbreite wird mit einem

Zeitmultiplexverfahren aufgeteilt.
Sowohl SDH, als auch SONET bieten die gleichen Geschwindigkeitsstufen an, nur unter anderen Bezeichnungen.
SDH kommt aus der Welt der Sprachtelefonie und sollte die Netze für den hohen Bandbreitenbedarf fit machen.

ATM - Asynchronous Transfer Mode

ATM ist keine reine Übertragungstechnik, sondern eine Netztechnik, die ursprünglich als Basis für ein Breitband-ISDN (B-ISDN), mit integriertem Kabelfernsehen entwickelt wurde. Heute dient die ATM-Netztechnik in lokalen, öffentlichen und privaten Hochgeschwindigkeitsnetzwerken als Transportmedium.

FDDI - Fibre Distributed Data Interface

FDDI ist ein Standard, nach ISO 9314 1-

3 und ANSI ASC X3T9.5 für ein Glasfaser-Datennetz. Die Übertragungsgeschwindigkeit ist auf 100 MBit/s beschränkt, die Topologie ist in Form eines einfachen oder doppelten Ringes angelegt. Die maximale Ausdehnung beträgt 200 km bei 1000 Stationen. FDDI ist für den Aufbau eines Backbones und damit für die Vernetzung großer Netze untereinander geeignet.

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 soft das Protokoll dafür, dass eine Anwendung jeden beliebigen Übertragungsweg nutzen kann.

Proprietäre Systeme

Kommen Übertragungsweg, Protokoll und Anwendung von einem einzigen Hersteller, macht sich niemand Gedanken über die Technik und wie sie funktioniert. Alles ist ein abgeschlossenes System, dass selten Probleme macht, allerdings auch wenig flexibel und transparent ist. Der Anwender ist in jedem Fall an den

Hersteller gebunden.

Offene Systeme

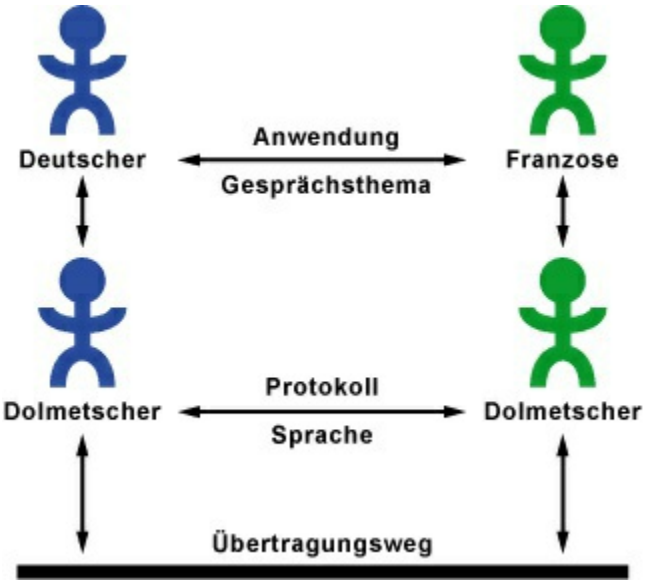
In offenen Systemen sind Übertragungsweg, Protokoll und Anwendung genormt, spezifiziert und offengelegt. D. h., jeder kann sich einen Teil heraussuchen und dazu eine Technik entwickeln, die sich dann auf dem Markt als Produkt behaupten muss und auch jederzeit austauschbar ist. Hier ist es auch möglich, dass Produkte unterschiedlicher Hersteller zusammenarbeiten und jederzeit gewechselt und erweitert 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 wird als Schicht dargestellt, die

übereinander gestapelt sind. Jede Schicht sorgt dafür, dass an den Schnittpunkten zur anderen Schicht Schnittstellen zur erfolgreichen Kommunikation enthalten sind. Im Gegensatz zu hochintegrierten Systemen, sind Schichtenmodelle nicht für hohe Geschwindigkeit oder Leistung ausgelegt. Es geht mehr um eine hohe Flexibilität der einzelnen Schichten, damit sie 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 miteinander zu kommunizieren. Beide bedienen sich eines Dolmetschers, anstatt sich direkt miteinander zu unterhalten.
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.

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.

DoD-Schichtenmodell	**OSI-Schichtenmodell**
Anwendungsschicht	Anwendungsschicht
	Darstellungsschicht
	Application Layer Kommunikationsschicht
Transportschicht	Transportschicht
	Transport Layer
Internetschicht	Vermittlungsschicht
	Internet Layer
Netzzugangsschicht	Sicherungsschicht
	Network Access
	Bitübertragungsschicht
	Layer

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 die Netzwerktopologie, das Übertragungsmedium und das Zugriffsprotokoll dar. In lokalen Netzwerken ist das Ethernet, in Telefonnetzen z. B. ISDN.

DoD vs. OSI

Wenn es um die Beschreibung von Vorgängen, Techniken und Protokollen im Internet und der Netzwerktechnik geht, dann wird wahlweise das DoD- und OSI-Schichtenmodell herangezogen. Obwohl das Internet und damit alle Netzwerke auf dem DoD-Schichtenmodell basieren, wird regelmäßig auf das OSI-Schichtenmodell

Bezug genommen.

Das OSI-Schichtenmodell wurde erst einige Jahre nach dem DoD-Schichtenmodell entwickelt. Es ist aber an dieses abwärtskompatibel angelehnt. Der direkte Vergleich zeigt eine gewisse Ähnlichkeit. Das OSI-Schichtenmodell ist allerdings wesentlich feiner gegliedert und flexibler. So lässt das OSI-Schichtenmodell die Zusammenfassung oder Entfernung einzelner Schichten zu.

Bei Ethernet und anderen Netzzugangsschichten sind für deren Beschreibung häufig zwei oder sogar mehr Schichten erforderlich. Im DoD-Schichtenmodell sind die Protokolle fest an die Schichten gebunden und lassen deshalb keine Anpassung zu. Die Netzwerk-Protokolle TCP/IP sind fest im DoD-Schichtenmodell verankert und lassen sich nicht ersetzen. In den

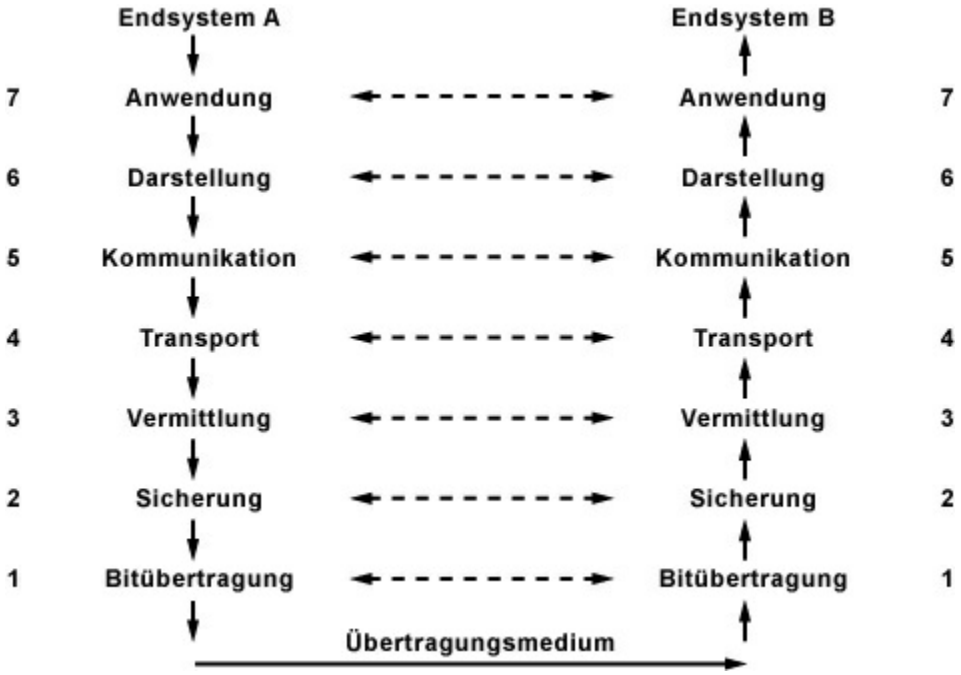
gängigen Netzwerk-Strukturen gibt es kaum Alternativen. Nur die Anwendungen und Übertragungsmedien auf den DoD-Schichten 1 und 4 lassen sich beliebig austauschen.

ISO/OSI-7-Schichtenmodell

Das OSI-7-Schichtenmodell ist ein Referenzmodell für herstellerunabhängige Kommunikationssysteme bzw. eine Design-Grundlage für Kommunikationsprotokolle und Computernetze.

OSI bedeutet Open System Interconnection (Offenes System für Kommunikationsverbindungen) und wurde von der ISO als Grundlage für die Bildung von Kommunikationsstandards entworfen und standardisiert. Das OSI-Schichtenmodell oder OSI-

Referenzmodell basiert auf dem DoD-Schichtenmodell, auf dem das Internet basiert. Im Vergleich zum DoD-Schichtenmodell ist das OSI-Schichtenmodell feiner aufgegliedert.



Das OSI-Schichtenmodell besteht aus 7 Schichten. Jede Schicht hat innerhalb der Kommunikation zwischen zwei Systemen eine bestimmte Aufgabe zu erfüllen. 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 sind eine Sammlung von Regeln zur Kommunikation auf einer bestimmten Schicht des OSI-Modells.

Die Endgeräte der Endsysteme und das Übertragungsmedium sind aus dem OSI-Modell ausgeklammert, was nicht bedeutet, dass die Endgeräte in der Anwendungsschicht und das Übertragungsmedium in der Bitübertragungsschicht nicht doch vorgegeben sind.

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. Es kann dann sogar sein, dass in manchen Verbindungen einzelne Aufgaben 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

Die Bitübertragungsschicht definiert die elektrische, mechanische und funktionale Schnittstelle zum

Schicht 1

Übertragungsmedium. Die

Physical

Protokolle dieser Schicht

unterscheiden sich nur nach
dem eingesetzten
Übertragungsmedium und -
verfahren. Das
Übertragungsmedium ist
jedoch kein Bestandteil der
Schicht 1.

Sicherungsschicht

Logische Verbindungen mit
Datenpaketen und elementare
Fehlererkennungsmechanismen
Die Sicherungsschicht sorgt
für eine zuverlässige und
funktionierende Verbindung
zwischen Endgerät und
Übertragungsmedium. Zur
Vermeidung von

Schicht 2

Übertragungsfehlern und

Data Link Datenverlust enthält diese
Schicht Funktionen zur
Fehlererkennung,

Fehlerbehebung und
Datenflusskontrolle.
Auf dieser Schicht findet auch
die physikalische
Adressierung von
Datenpaketen statt.

Vermittlungsschicht

Routing und
Datenflusskontrolle
Die Vermittlungsschicht
steuert die zeitliche und
logische getrennte
Kommunikation zwischen den

Schicht 3

Endgeräten, unabhängig vom

Network

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

Logische Ende-zu-Ende-

Verbindungen

Die Transportschicht ist das

Bindeglied zwischen den

Schicht 4

transportorientierten und

Transport anwendungsorientierten

Schichten. Hier werden die

Datenpakete einer Anwendung

zugeordnet.

Kommunikationsschicht

Prozeß-zu-Prozeß-

Verbindungen

Die Kommunikationsschicht

organisiert die Verbindungen

Schicht 5

zwischen den Endsystemen.

Session

Dazu sind Steuerungs- und

Kontrollmechanismen für die
Verbindung und dem
Datenaustausch implementiert.

Darstellungsschicht

Ausgabe von Daten in
Standardformate

Die Darstellungsschicht
wandelt die Daten in

Schicht 6

verschiedene Codecs und

Presentation Formate. Hier werden die Daten zu oder von der
Anwendungsschicht in ein
geeignetes Format
umgewandelt.

Anwendungsschicht

Dienste, Anwendungen und
Netzmanagement

Die Anwendungsschicht stellt
Funktionen für die
Anwendungen zur Verfügung.

Schicht 7

Diese Schicht stellt die

Application 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.

Das OSI-Schichtenmodell in der Praxis

Das OSI-Schichtenmodell wird sehr häufig als Referenz herangezogen. 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.

OSI-Schichtenmodell in der Netzwerktechnik

Das OSI-Schichtenmodell besteht aus 7 Schichten. Die Funktionen der einzelnen Schichten stellen der übergeordneten Schicht eine bestimmte Dienstleistung zur Verfügung. Die Aufgaben der einzelnen Schichten sind im OSI-Schichtenmodell definiert.

Das hier dargestellte und beschriebene OSI-Schichtenmodell ist stark

vereinfacht und auf die Netzwerktechnik

zugeschnitten. Dieses Schichtenmodell ist nicht vollständig oder endgültig.

Die vereinfachte Netzwerkansicht des OSI-Schichtenmodells wird aus Anwendersicht erklärt. Deshalb wird mit den obersten Schichten begonnen.

Datenverarbeitung Adressierung und Schichten

und -übertragung

Verbindungsaufbau

HTTP,

FTP,

IMAP,

SMB

URL:

SMTP (Windows) www.das-

Samba

elko.de

Anwendung

(Unix/Linux)

OSI-Schicht

5 + 6 + 7

hosts /

NetBIOS

DNS

(Windows)

Transport: TCP /

UDP (Datenpakete)

Übertragung

OSI-Schicht

Adressierung: IP /

3 + 4

ICMP (Adresse)

NDIS

Netzzugang

(physikalisch)

Treiber

OSI-Schicht

1 + 2

Netzwerkkarte

(NIC)

Beschreibung der

Datenverarbeitung

In den Anwendungsschichten 5, 6 und 7 sind alle Protokolle definiert, auf die Programme und Anwendungen direkt zugreifen. In der Windows-Netzwerkwelt stellt das SMB mit NetBIOS die Verbindung zur Übertragungsschicht her. Kommt ein Unix-Betriebssystem mit Windows in Kontakt wird der Dienst Samba genutzt, um Anwendungen die Ressourcen im Windows-Netzwerk auf dem Unix-Betriebssystem zur Verfügung zu stellen. Die Verbindung zwischen Anwendungs-

und Übertragungsschicht wird über Ports von TCP hergestellt. Anwendungen und Dienste identifizieren ihre Daten über diese Ports.

Der Datenstrom wird von dem verbindungsorientierten Transport-Protokoll TCP oder dem verbindungslosen Transport-Protokoll UDP in Pakete verpackt. Das Internet Protocol (IP) übernimmt die Adressierung der Pakete.

Der Bitstrom wird an den NDIS weitergeleitet, der mit dem Treiber der Netzwerkkarte spricht. Erst der Treiber schickt die Daten an die Netzwerkkarte (NIC). Von dort gehen die Daten im Netzwerk auf die Reise.

Bei ankommenden Daten gehen sie den umgekehrten Weg wieder zurück.

Beschreibung des Verbindungsaufbaus

Innerhalb der Anwendungsschicht dient

die URL (Universal Ressource Locator), in Windows-Netzwerken der NetBIOS-Name des Computers, zur Identifikation eines Computers und den Diensten, die darauf ausgeführt werden.
Zur Auflösung der URL zur IP-Adresse dient die Datei hosts, in der alle URLs und IP-Adressen aufgelistet sind. Da es viele URLs gibt, wurde das DNS (Domain Name System) eingeführt, das hierarchisch aufgebaut ist. Die sogenannten DNS-Server sind in der Lage unbekannte DNS-Namen beim übergeordneten DNS-Server zu erfragen.
Im Windows-Netzwerk dient die Datei lmhosts oder der WINS (Server) zur Auflösung von NetBIOS-Namen in IP-Adressen.
Ist die IP-Adresse der Übertragungsschicht aufgelöst, dann wird ARP (Address Resolution Protocol) verwendet, um die IP-Adresse

in die MAC-Adresse (Media Access Control) der Netzwerkkarte (Physikalische Schicht) aufzulösen. Die MAC-Adresse ist die einzige definitive Adresse, anhand der man einen Computer im Netzwerk sicher identifizieren kann. Die MAC-Adresse ist fest auf einer Netzwerkkarte eingestellt.

RFC - Request for Comments

Die Requests For Comments (RFC) sind eine Sammlung durchnummerierter Dokumente, die von der IETF (Internet Engineering Task Force) herausgegeben werden. RFCs behandeln Protokolle, Methoden, Programme und Konzepte, die für die Zusammenarbeit unterschiedlicher Systeme im Internet unentbehrlich sind. Dazu gehören auch Konferenzprotokolle, Meinungen und gelegentlich Beschreibungen, denen die

Ernsthaftigkeit fehlt. Zum Beispiel das Hyper Text Coffee Pot Control Protocol (HTCPCP), das zur Kontrolle und Überwachung vernetzter Kaffeemaschinen dient.

Nahezu alle Internet-Standards wurden als RFCs veröffentlicht, aber nur ein kleiner Teil der RFCs wurde als Standard von einem offiziellen Normungsgremium verabschiedet.

Die Einführung eines Systems wie RFC wurde nötig, weil sich die Internet-Protokolle schneller weiterentwickelten, als ein offizieller Standardisierungsprozess gebraucht hätte. Erst später wurden wichtige elementare und nachhaltige RFCs als offizielle Standards verabschiedet.

Tatsächlich erreichen nur wenige RFCs den Standard-Status. Die an einem RFC mitwirkenden Personen und Gruppen konzentrieren sich in der Regel auf die

Verbesserung des Protokolls, als Zeit in den Standardisierungsprozess zu investieren.

Im Zusammenhang mit Standards aus der Netzwerktechnik wird immer wieder auf RFCs verwiesen. RFCs gehören zum Standardisierungsprozess im Internet dazu.

Das RFC-System

Jeder RFC wird zuerst als Internet Draft eingereicht. Wenn die IETF und die IESG ihn angenommen haben, wird der RFC veröffentlicht.

RFC steht für Request for Comments, übersetzt: Bitte um Kommentare. Diese Bedeutung ist eigenartig, denn wenn ein Dokument als RFC veröffentlicht wurde, dann kann es von keinem Kommentar verändert werden. Kleinere Fehler und Ergänzungen erscheinen als Errata. Bei größeren Änderungen wird ein neuer RFC mit einer neuen Nummer

geschrieben und veröffentlicht. Im alten RFC wird dann die Nummer des neuen RFCs vermerkt. Deshalb gibt es zu vielen Internet-Protokollen mehrere RFCs.

RFC-Quellen

Es gibt verschiedene RFC-Quellen. Doch nicht alle sind vollständig und aktuell. Eine erste Adresse ist der RFC-Editor. Dort wird eine offizielle Dokumentation und eine Liste von RFC-Datenbanken gepflegt. Der RFC-Editor bietet die Suche in RFCs nach Nummern und Schlüsselwörtern an.

Netzwerk-

Topologie

Unter einer Netzwerk-Topologie versteht man die physikalische Anordnung von Netzwerk-Stationen, die über Kabel oder Funk miteinander verbunden sind. Die Netzwerk-Topologie bestimmt die einzusetzende

Hardware, sowie die Zugriffsmethoden.
Die im folgenden beschriebenen Topologien beziehen sich auf paketvermittelnde Netzwerke.

Bus-Topologie

Die Bus-Topologie 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-Topologie

Die Ring-Topologie ist eine geschlossene Kabelstrecke in der die Netzwerk-Stationen im Kreis angeordnet sind. Das bedeutet, dass an jeder Station ein Kabel ankommt und ein Kabel abgeht.
Im Ring befindet sich keine aktive Netzwerk-Komponente. Die Steuerung und der Zugriff auf das Übertragungsmedium regelt ein Protokoll, an das sich alle Stationen halten.

Wird die Kabelverbindung an einer Stelle unterbrochen fällt das Netzwerk aus, es sei denn die eingesetzte Übertragungstechnik kennt den Bus-Betrieb, auf den alle Stationen umschalten können.

Stern-Topologie

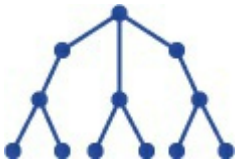
In der Stern-Topologie befindet sich eine zentrale Station, die eine Verbindung zu allen anderen Stationen unterhält. Jede Station ist über eine eigene Leitung mit der zentralen Station verbunden. Es handelt sich im Regelfall um einen Hub oder einen Switch. Der Hub oder Switch übernimmt die Verteilfunktion 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.

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.

Vermaschte Topologie

Die vermaschte Topologie ist ein dezentrales Netzwerk, das keinen verbindlichen Strukturen unterliegen muss. Allerdings sind alle Netzwerk-Stationen irgendwie miteinander verbunden. Häufig dient dieses Modell als perfektes Netzwerk in dem jede Netzwerk-Station mit allen anderen Stationen mit der vollen Bandbreite

verbunden ist. Diese Topologie wird zumindest virtuell mit jeder anderen Topologie realisierbar, wenn genug Bandbreite zur Verfügung steht und aktive Netzwerk-Komponenten das Routing der Datenpakete übernehmen. Beim Ausfall einer Verbindung gibt es im Regelfall einige alternative Strecken, um den Datenverkehr unterbrechungsfrei fortzuführen.

Die Struktur des dezentralen Netzwerkes entspricht einem Chaos an verschiedenen Systemen und Übertragungsstrecken. Das Internet stellt ein solches Netzwerk dar.

Vorteile und Nachteile der Grundtopologien

Topologie	**Vorteile**	**Nachteile**
einfach **Bus-**		

installierbar

Topologie

kurze Leitungen

verteilte

Ring-

Steuerung

Topologie

große

Netzausdehnung

einfache

Vernetzung

Stern-

einfache

Topologie

Erweiterung

hohe

Ausfallsicherheit

dezentrale

Steuerung

Vermaschte

unendliche

Topologie

Netzausdehnung

hohe

Ausfallsicherheit

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.

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

Verkabelungsnorm

EN

Informationssysteme -

Europa

50173-1 anwendungsneutrale

(2003)

Verkabelungssysteme

TIA/EIA

568 B.1 Telekommunikations-

Nordamerika

(2001) / Verkabelungsnorm für

B.2 1

Gebäudeverkabelungen

(2001)

ISO/IEC Verkabelungsnorm für

Weltweit

11801

anwendungsneutrale

(2002)

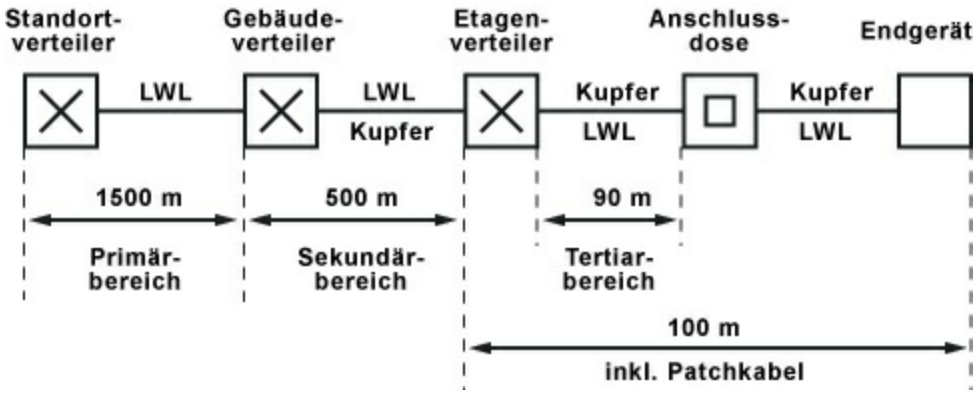
Gebäudeverkabelungen

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 Verkabelung und Komponenten 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.

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 1500 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 es, den Primärbereich großzügig zu planen. Das bedeutet, das Übertragungsmedium muss von 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 innerhalb eines Gebäudes untereinander 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 oder in einem Kabelkanal. 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 Kunststoff oder dem Grundstoff Glas.

Patchfeld und Patchkabel

Patch ist ein englisches Wort und bedeutet frei übersetzt "vorübergehend

zusammenschalten oder einstöpseln".

Patchkabel (Patchcable) sind die bevorzugten Kabel, um Patchfelder und Anschlussdosen mit den Netzwerkstationen und aktiven Netzwerk-Komponenten zu verbinden.

Patchfelder (Patchpanel) sind Vorrichtungen, an denen die Netzwerkleitungen ankommen.

LAN-Kabel

Ein LAN-Kabel ist ein unüblicher Begriff, der darauf hin deutet, dass es sich um ein Patchkabel handelt, mit dem eine Verbindung im lokalen Netzwerk (LAN) hergestellt wird.

Datenkabel

Ein Netzwerkkabel wird manchmal auch als Datenkabel bezeichnet. Allerdings ist diese Bezeichnung irreführend. Die Bezeichnung Datenkabel deutet nur darauf hin, dass über dieses Kabel Daten übertragen werden. Im Gegensatz

dazu ein Stromversorgungskabel, das der Stromversorgung dient. Die Bezeichnung Netzwerkkabel deutet darauf hin, dass dieses Kabel zur Vernetzung bzw. als Teil einer Netzwerk-Verkabelung dient. Was darüber übertragen wird ist unerheblich.

Installation von Netzwerkkabeln

Zentrale Elemente einer Verkabelung, sind geschirmte Leitungen und Buchsen, sowie Spezialwerkzeug für die Installation.

Netzwerkkabel sind grundsätzlich mit äußerster Sorgfalt zu behandeln und nur in trockenen Räumen zu lagern und zu installieren.

Quetschen, zu starker Druck und Zug sind zu vermeiden, weil es die Qualität und physikalische Eigenschaft der Netzwerkkabel

verringern kann.
Kanten auf der Verlegestrecke
müssen geglättet werden.
Biegeradius des Herstellers sind
einhalten, damit die Eigenschaften
des Netzwerkkabels nicht
beeinflusst werden.
Die Netzwerkkabel sollten direkt
von der Kabeltrommel oder
Kabelrolle abgerollen oder
gezogen und nicht abgewickelt
(Veränderung des Kabelaufbaus)
werden.
Netzwerkkabel sind getrennt von
Stromkabeln in einem Kabelkanal
zu verlegen. Zum Beispiel durch
einen Trennsteg.
Beim Auflegen sind die verdrillten
Adern von Twisted-Pair-Kabel
nicht zu weit zu öffnen und auch
nicht mehr nach zu verdrillen, sonst
bekommt die Kabelstrecke

schlechte Werte bei der NEXT-Messung.

Das geschirmte Leitungsnetz und alle metallischen Komponenten sind in den Potentialausgleich des Gebäudes einzubeziehen.

Twisted-Pair-Kabel

"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. Zum

Beispiel 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, die um die Adernpaare gewickelt sind. Das 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.

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.

Verdrillt / Verseilt / Gekreuzt

Insgesamt gibt es drei verschiedene Übersetzungen für "Twisted Pair". Man spricht von verdrillten, verseilten oder gekreuzten Adernpaaren. Falsch ist keines davon. Technisch korrekt ist es, wenn man von Verseilung oder verseilten Adernpaaren spricht. Der Grund ist das Herstellungsverfahren, dass mit dem von Seilen vergleichbar ist.

Standards bei Twisted-Pair-Kabeln

Twisted-Pair-Kabel sind genormt und um ihre Leistungsfähigkeit zu beschreiben in unterschiedliche Klassen und Kategorien eingeteilt. Jede Klasse oder Kategorie deckt verschiedene Anforderungsprofile mit bestimmten Qualitätsvorgaben ab. Die Kategorien sind nach dem US-Standard TIA/EIA 568 festgelegt und reichen von 1 bis 6. Die Kategorien 1 und 2 sind nur informell definiert und gab es praktisch nie. Für Kabel der Kategorie 3 und 4 gibt es keinen Anwendungsfall mehr. Ihre Qualität entspricht nicht mehr den Anforderungen heutiger Übertragungstechniken. Man findet sie höchstens noch in alten Netzwerk-Installationen.

Parallel zu den Kategorien der EIA/TIA 568 gibt es noch die Kategorien der

ISO/IEC 11801, in der die Kategorien 5 bis 7 festgelegt sind.

Zusätzlich gibt es eine europäische Norm EN 50172, in der Twisted-Pair-Kabel in die Klassen A bis F eingeteilt sind.

Die Standards gelten jedoch nicht nur für die Kabel, sondern auch für die Stecker und Buchsen.

Gerade aktuell sind Twisted-Pair-Kabel der Kategorie 6 oder 7 bzw. der Klasse E und F.

EIA/TIA

ISO/IEC

568

11801

EN

Kabeltyp Kategorie, Kategorie, 50173

Kat.

Kat.

Klasse

Category, Category, Class

Cat.

Cat.

UTP-1

Cat. 1

-

Class

UTP-1

-

A

Class

UTP-2

Cat. 2

B

Class

UTP-3

Cat. 3

C

UTP-4

Cat. 4

-

STP

IBM Typ 1/9

UTP,

Class

Cat. 5

Cat. 5

S/FTP

D

UTP,

Class

Cat. 5e

Cat. 5e

S/FTP

D

UTP,

Class

Cat. 6

Cat. 6

S/FTP

E

Class

S/FTP

Cat. 6A

Cat. 6A

EA

Class

S/FTP

-

Cat. 7

F

Class

S/FTP

-

Cat. 7A

FA

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.

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, auch wenn die ähnlichen Begriffe 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.

Netzwerk-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.

Netzwerk-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 fehlerfreien Kabelverbindungen.

Für Gigabit-Ethernet musste die Spezifikationen überarbeiten werden.

Die Kabel wurden mit Cat5e (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 nur noch die Bezeichnung CAT5. Die davor verlegte CAT5-Kabel unterstützen Gigabit-Ethernet nicht immer.

Netzwerk-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. CAT6A.

Netzwerk-Kabel der

Category/Kategorie CAT6A

/ CAT6A (Class EA)

Mit 10-Gigabit-Ethernet (10GBASE-T) wurden Twisted-Pair-Kabel mit dem Standard CAT6A (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.

Netzwerk-Kabel der Category 7 / Kategorie 7 (Class F)

Spätestens bei 10-Gigabit-Ethernet sind Kabel der Kategorie 7 notwendig (oder CAT6A). 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 7A 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 CAT7-Verkabelung mit RJ45-Patchkabeln und -dosen ist also keine "echte", sondern höchstens CAT6A. In der Vergangenheit haben viele Elektroinstallateure die nötige Sorgfalt beim Verlegen von CAT6- und CAT7-Kabel missen 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.

Wichtiger Hinweis: 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 nur eine CAT6A-Netzwerkinstallation.
Netzwerk-Komponenten nach CAT7 benötigen neue Steckverbindungen.
Allerdings hat sich noch keine durchgesetzt.

Steckverbinder für Twisted-Pair-Kabel

Der übliche Steckverbinder (Stecker-Buchse-Kombination) für Twisted-Pair-Kabel ist RJ45, der auch als Western-Stecker bezeichnet wird.
Mit viel Konstruktionsarbeit an der Leiterplatte kann der RJ45-Steckverbinder bis zu 500 MHz erreichen. Die 500 MHz sind die Mindestanforderungen für 10 GBit/s.
Was aber nur für eine Kabelstrecke (CAT6A) von 55 Meter ausreicht. Mehr geht mit RJ45 nicht. Deshalb wird nach einem allseits akzeptierten Nachfolger für die zukünftigen CAT7-Leitungsnetze

gesucht. Antreten werden dazu GG45, TERA und ARJ45.

GG45 von Nexans ist ein neuer Steckverbinder für Twisted-Pair-Kabel der Kategorie 7. GG45 ist abwärtskompatibel zu RJ45. Zwischen GG45 und RJ45 reicht ein einfacher Adapter.

ARJ45 ist ein von Stewart Connector entwickelter Steckverbinder, der interoperabel zu GG45 ist.

Da sämtliche Endgeräte noch über RJ45-Anschlüsse verfügen, wird der Umstieg eher langsam vonstatten gehen.

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

S = Geflechtschirm

SF = Geflecht- und Folienschirm

Y steht für die

Aderpaarschirmung

U = ohne Schirm (ungeschirmt)

F = Folienschirm

S = Geflechtschirm

ZZ steht immer für TP =

Twisted Pair

Übersicht: Bezeichnung für

Twisted-Pair-Kabel

Schirmung

U/UTP

Folie

Gesamtschirm

Drahtgeflecht

Adernpaarschirm Folie

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 nach DIN EN 50173 in Deutschland und Europa nicht zugelassen, weshalb sie hier auch nur sehr selten vorkommen. Der Grund sind die Vorgaben zur Elektromagnetischen Verträglichkeit (EMV). Dagegen sind U/UTP-Kabel weltweit die meistverwendeten Kabel für lokale Netzwerke mit Ethernet.

S/UTP -

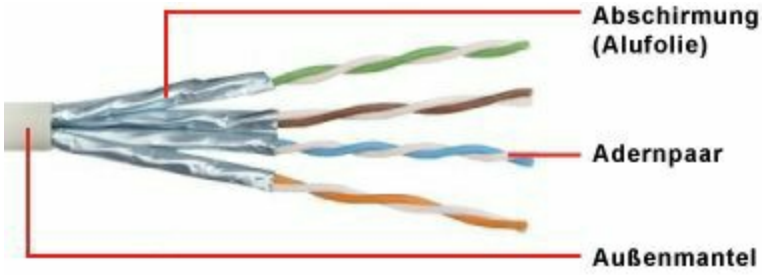
Screened/Unshielded

Twisted-Pair-Kabel

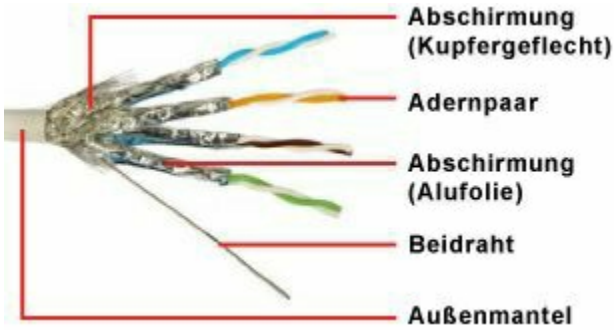
Das S/UTP-Kabel besteht aus einem Kunststoffmantel und einem Gesamtschirm, in dem sich die paarweise verseilten Adernpaare befinden. Die Schirmung darf aus Kupfergeflecht oder Aluminiumfolie (Folie, die mit Aluminium kaschiert ist) oder aus beidem bestehen. Die Qualität dieser Kabel ist wesentlich höher 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 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.

Lichtwellenleiter (LWL / Glasfaser)

Die Lichtleitertechnik überträgt Daten in Form von Licht über weite Strecken mit Hilfe von Glas-, Quarz- oder Kunststofffasern. Während die elektrischen Signale in Kupferleitungen als Elektronen von einem zum anderen Ende wandern, übernehmen in

Lichtwellenleitern (LWL) Photonen (Lichtteilchen) diese Aufgabe.
Durch Lichtwellenleiter können optische Signale ohne Verstärker große Entfernungen überbrücken. Trotz weiter Strecken ist eine hohe Bandbreite möglich. Die Bandbreite auf einer einzigen Glasfaser beträgt rund 60 THz. Das macht Lichtwellenleiter zum Übertragungsmedium der Gegenwart und Zukunft. Da kommt kein Kupferkabel oder Funksystem dagegen an.
Die Preise für die Lichtwellenleiter-Anschlusstechnik sind in den letzten Jahren stark gefallen. Glasfaser als Anschlusstechnik könnte in den nächsten Jahren preislich attraktiv werden.

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.

Prinzip eines Übertragungssystems auf Basis eines Lichtwellenleiters

Abhängig in welcher Form die Daten beim Sender vorliegen, 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 Ende der Übertragung werden die

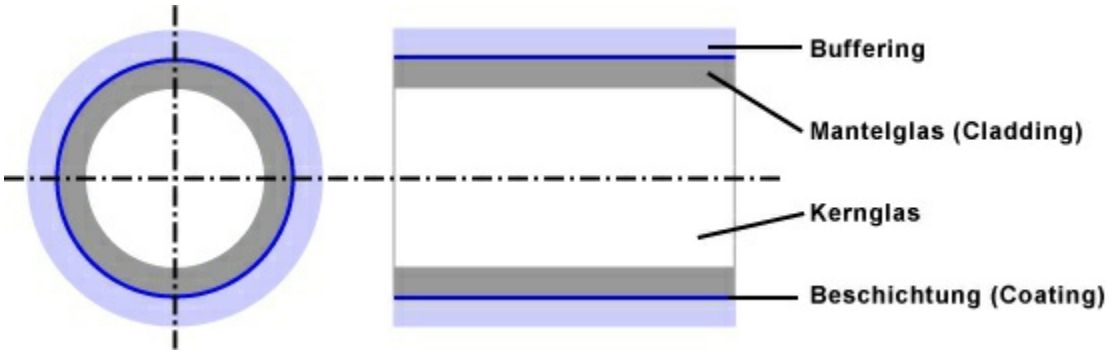
Lichtimpulse wieder in elektrische Signale umgewandelt. Ein Fotoelement, zum Beispiel ein Fototransistor, erzeugt aus dem Licht elektrische Impulse. Dann findet noch eine Digital-Analog-Wandlung statt, wenn die Daten in analoger Form und verstärkt an den Empfänger übergeben werden müssen.

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 des Lichtwellenleiters

Lichtwellenleiter (LWL) aus Kunststoff haben einen Durchmesser von etwa 0,1 mm und sind äußerst flexibel und empfindlich. Der Kern 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 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 gibt keine elektromagnetischen Störeinflüsse.

Wegen der optischen Übertragung existieren keine Störstrahlungen oder Masseprobleme.

Entfernungsbedingte Verluste des Signals wegen 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 für die Montage sind höher. Dafür haben Lichtwellenleiter eine erheblich geringere Dämpfung und eignen sich auch für weite Strecken.

Fachbegriffe

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.

Disperion

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

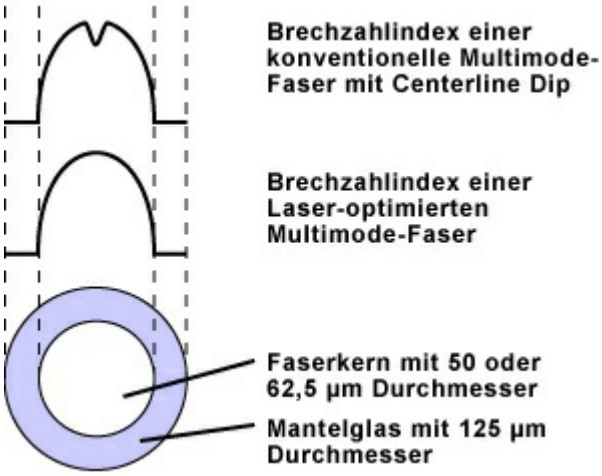
Lichtimpulserzeugung verwendet, sondern Laserdioden, die einen Impuls mit spektraler Breite von wenigen Nanometer erzeugen kann.

LED- und Laser-Lichteinkopplung

Eine Multimode-Faser hat mehrere Moden. Bei der LED-Lichteinkopplung werden alle Moden einer Faser angeregt. LEDs füllen den gesamten Faserkern aus. Man spricht von einer Vollanregung.

Die übertragbare Datenrate mit LED-Transceivern ist auf 622 MBit/s begrenzt. Wegen ihrer charakteristischen Schalthysterese ergibt sich die Trägheit für die Sende-LED. Bei Gigabit Ethernet (GbE) oder 10 Gigabit Ethernet (10 GbE) reicht ein LED-Transceiver nicht aus. Statt dessen verwendet man Laser zur Lichteinkopplung. Im Gegensatz zu LEDs regen Laser nur eine bestimmte

Anzahl von Moden an. Da Fabry-Perot- und Distributed-Feedback-Laser sehr teuer sind, werden die speziell für Lichtwellenleiter entwickelten VCSELs (Vertical Cavity Surface Emitting Lasers) von allen namhaften Hersteller verwendet. VCSELs sprechen bei der Lichteinkopplung nur wenige Moden an und haben eine Wellenlänge von 850 nm. VCSEL-Laser haben gegenüber LEDs



mehrere Vorteile:

niedrigere Dämpfung bei der Signaleinkopplung

höhere Übertragungsleistung

größere Übertragungsentfernung

längere Betriebsdauer

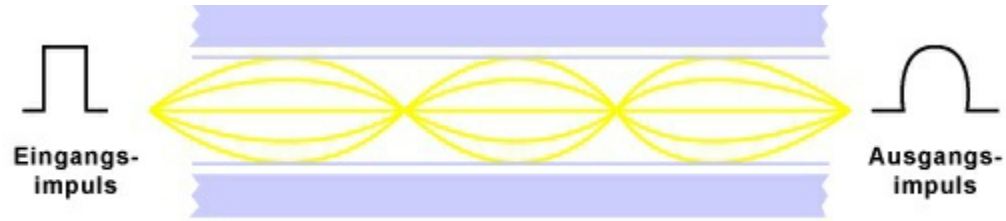
Allerdings entstehen bei der Laser-Lichteinkopplung in herkömmliche Multimodefasern häufig Störungen in Form der Centerline Dips. Der Centerline Dip ist eine Kerbe im Brechzahlprofil im Faserzentrum. Weitere Störungen können Abflachungen (Flat Tops) und Spitzen (Peaks) im Brechzahlprofil sein.
Das Lasersignal bringt einen großen Teil der Gesamtleistung auf das Faserzentrum. Dadurch entsteht eine Verformung des idealen Übertragungssignals. Die Folge ist eine höhere Bitfehlerrate und die daraus folgende schlechte Nettodatenrate und ein Ausfall der Übertragung.
Beim Einsatz von Komponenten mit

Multimodefaser mit Stufenindex-Profil

Laser-Lichteinkopplung sind zwingend Laser-optimierte Lichtleiter zu verwenden.

Multimodefaser mit Stufenindexprofil

Multimodefasern mit Stufenprofil haben einen Durchmesser von 200 µm. Durch sie werden mehrere Lichtwellen gleichzeitig geschickt. An den Wänden der Faser wird das Signal hart



Multimodefaser mit Gradientenindex-Profil

reflektiert. Die Brechzahl fällt zwischen Kern und Mantel scharf ab. Das Ausgangssignal wird dadurch schlechter. Sie werden z. B. als Verbindungskabel im Patchschrank verwendet.

Multimodefaser mit Gradientenindexprofil

Multimodefasern mit Gradientenprofil

haben einen Durchmesser von 50 µm.

Durch sie werden mehrere Lichtwellen

gleichzeitig geschickt. An den Wänden der Faser wird das Signal weich reflektiert. Die Brechzahl des Kerns nimmt meist parabelförmig zum Mantel ab. Das Ausgangssignal ist noch sehr gut. Sie werden für Verbindungen von Gebäuden oder Etagen eingesetzt.

Monomodefaser / Singlemodefaser

Singlemodefasern oder Monomodefasern haben einen Durchmesser von 10 µm. Durch sie werden die Lichtwellen gerade hindurchgeleitet. Sie werden für weite Strecken eingesetzt. Der Kerndurchmesser einer Singlemodefaser ist gegenüber der Wellenlänge des

Lichts so klein, dass sich nur ein Modus (Moden) ausbreiten kann.
Singlemodefasern erfordern den Einsatz sehr teurer Laser, was zu hohen Kosten beim Equipment führt.
Singlemode-Fasern sind für Stadt- und Zugangsnetze optimiert. Die Anforderungen an diese Lichtwellenleiter sind hoch. Neben leicht zu verarbeitende Fasern, sind Breitband-Leistungsfähigkeit für flexibles Netzwerk-Design erwünscht.
Der Lichtwellenleiter muss für kommende Technologien und Architekturen in der Netzwerkinfrastruktur gerüstet sein. Es gibt folgende Standards:
ITU-T G.652
IEC 60793-2-50 Typ B1.3
TIA/EIA 492-CAAB
Telcordia GR-20

Netzwerk-

Komponenten

In der Netzwerktechnik unterscheidet man zwischen aktiven und passiven Netzwerk-Komponenten. Während aktive Netzwerk-Komponenten eine eigene Logik haben, zählen die passiven Netzwerk-Komponenten zur fest installierten Netzwerk-Infrastruktur.
In der Regel dienen Netzwerk-Komponenten zur Kopplung der Netzwerk-Stationen. Man spricht deshalb auch von Kopplungselementen.

Passive Netzwerk-Komponenten

Kabel

Anschlussdose

Anschlussstecker

Patchfeld / Patchpanel

Netzwerk-Schrank / Patch-Schrank

Aktive Netzwerk-Komponenten

In kleinen privaten Netzwerken, haben

Netzwerk-Komponenten noch klare Bezeichnung, wie Switch oder Router. In großen Unternehmensnetzwerken ist die

Benennung der Kopplungselemente nicht immer eindeutig.

Switch

Ein Switch ist ein Kopplungselement, das mehrere Stationen in einem Netzwerk miteinander verbindet. In einem Ethernet-Netzwerk, das auf der Stern-Topologie basiert dient ein Switch als Verteiler für die Datenübertragung.

Router

Router verbinden Netzwerke mit unterschiedlichen Protokollen und Architekturen. Router finden sich häufig an den Außengrenzen eines Netzwerkes. Hier wird die Verbindung zu anderen Netzen und dem Internet geschaffen.

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 und die Protokolle eines anderen Netzes konvertiert werden.

Firewall

Sicherheit ist immer ein Gesamtkonzept, in dem festgelegt ist, was wovor geschützt sein muss, was die Angriffsflächen sind und wie man diese schließt oder minimiert. In einem lokalen Netzwerk ist die Angriffsfläche die Schnittstelle zum Internet.

Server

Was ein "richtiger Server" ist, darüber lässt sich trefflich streiten. In den meisten Fällen wird es ein Computer mit einem leistungsstarken Prozessor, viel Arbeitsspeicher, mehreren Festplatten und großzügiger Netzwerk-Anbindung sein. Auf Servern werden zentrale Aufgaben bearbeitet, verwaltet und gespeichert.

Zuordung im OSI-

Schichtenmodell (aktive

Komponenten mit

Verteilfunktion)

Schicht Repeater Hub Bridge Switch Router 7

6

5

4

3

(x)

2

x

x

1

x

x

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-Modells. 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 identifizieren.

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.

LEDs an der RJ45-Buchse

An einer Netzwerkkarte ist nicht nur die RJ45-Buchse herausgeführt, sondern meist auch zwei LEDs, die den Status der Verbindung anzeigen. Üblich sind RJ45-Buchsen, die zwei integrierte Status-LEDs in den Farben Grün und Orange haben.

Die grüne LED zeigt an, dass eine hardwareseitige Verbindung besteht. Dazu muss der Computer nicht eingeschaltet sein (bei Formfaktor

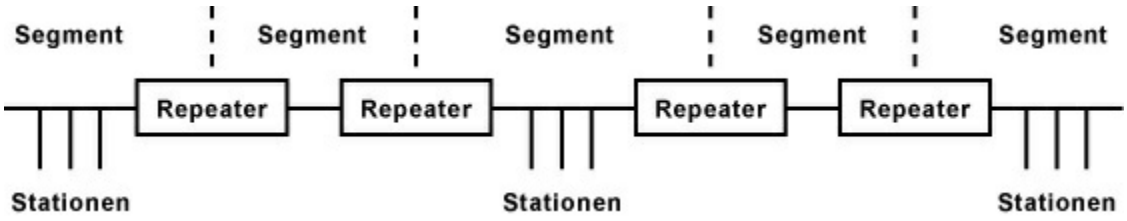
ATX). Die orangene LED zeigt den Status der Übertragung an. Wenn diese LED blinkt oder flackert, dann werden gerade Daten übertragen.
Bei manchen Netzwerkkarten sind diese Funktionen etwas anders. Wenn die grüne LED flackert, dann werden gerade Daten übertragen. Ansonsten ist sie ständig grün, wenn eine Verbindung besteht. Leuchtet die orangene (manchmal ist sie auch gelb) LED, dann besteht eine 100 MBit-Verbindung.

Repeater

Ein Repeater ist ein Kopplungselement, um die Übertragungsstrecke innerhalb von Netzwerken, zum Beispiel Ethernet, zu verlängern. Ein Repeater empfängt ein Signal und bereitet es neu auf. Danach sendet er es weiter. Auf diese Weise verlängert der Router die Übertragungsstrecke und räumliche Ausdehnung des Netzwerks.

Im einfachsten Fall hat der Router zwei Ports, die wechselweise als Ein- und Ausgang funktionieren (bidirektional).
Repeater versteht man in der Regel als Verstärker von Übertragungsstrecken.
Die weitere Beschreibung bezieht sich auf Repeater in kabelgebundenen Netzwerken, speziell in Ethernet-Netzwerken.
Ein Repeater arbeitet auf der Schicht 1, der Bitübertragungsschicht des OSI-Schichtenmodells. Damit übernimmt er keinerlei regulierende Funktion in einem Netzwerk. Er kann nur Signale empfangen und weiterleiten. Für angeschlossene Geräte ist nicht erkennbar, ob sie an einem Repeater angeschlossen sind. Er verhält sich völlig transparent.
Ein Repeater mit mehreren Ports wird auch als Hub (Multiport-Repeater) bezeichnet. Er kann mehrere Netzwerk-

Segmente miteinander verbinden.



Die Repeater-Regel (5-4-3)

Um ein großes Netzwerk mit einer möglichst großen Reichweite aufzubauen, können mehrere Repeater hintereinandergeschaltet werden. Allerdings, nicht in beliebiger Anzahl. Der Grund liegt im Laufzeitverhalten und der Phasenverschiebung zwischen den Signalen an den Enden des Netzwerks. Deshalb gilt folgende Repeater-Regel: Es dürfen nicht mehr als fünf (5) Kabelsegmente verbunden werden. Dafür werden vier (4) Repeater eingesetzt. An nur drei (3) Segmenten dürfen Endstationen angeschlossen werden.

Diese Repeater-Regel hat nur in den Ethernet-Netzwerken 10Base2 und

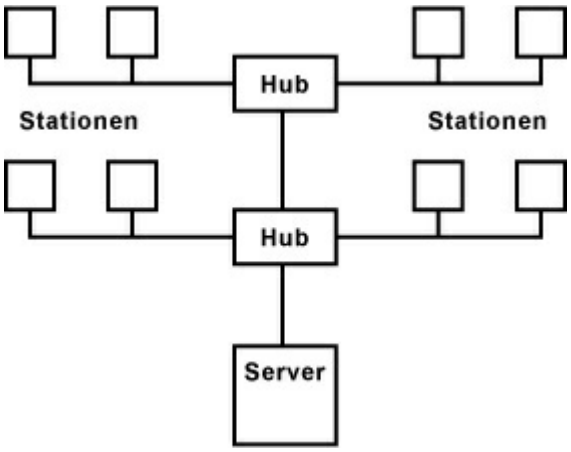
10BASE5 eine Bedeutung. In Netzwerken, die mit Switches und Router aufgebaut sind, hat diese Repeater-Regel keine Bedeutung.
Um die Nachteile von Repeatern in Ethernet-Netzwerken zu umgehen, werden generell Switches zur Kopplung der Stationen eingesetzt. In großen Netzwerken, insbesondere über unterschiedliche Übertragungssysteme hinweg, werden zusätzlich Router eingesetzt.

Hub

Ein Hub ist ein Kopplungselement, das mehrere Stationen 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 Stationen. Sie



bekommen alle Datenpakete zugeschickt, auch wenn sie nicht die Empfänger sind. Für die Stationen 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 Netzwerk-Stationen 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 Stationen erhöhen. Allerdings ist die Anzahl der anschließbaren Stationen begrenzt. Auch hier gilt die Repeater-Regel.

Alle Stationen 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 Computer zum Hub verfügt nur kurzzeitig über diese Bandbreite.

Die Versendung der Datenpakete an alle Stationen 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.

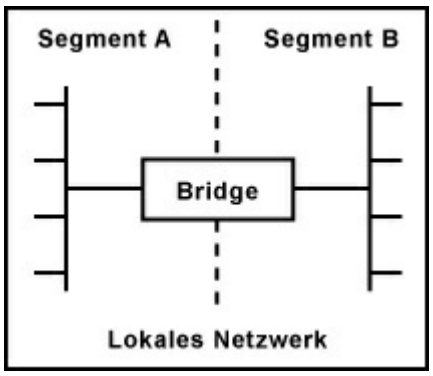
Bridge

Eine Bridge ist ein Kopplungselement, das ein lokales Netzwerk in zwei Segmente aufteilt. Dabei werden die Nachteile von Ethernet, die besonders bei großen Netzwerken auftreten ausgeglichen. Als Kopplungselement ist die Bridge eher untypisch. Man vermeidet die Einschränkungen durch Ethernet heute eher durch Switches.

Warum ist eine Bridge notwendig (gewesen)?

Das CSMA/CD-Verfahren in einem Ethernet (Netzwerk) führt zu mehreren Einschränkungen:

Alle Stationen teilen sich die verfügbare Bandbreite (z. B. 10 MBit oder 100 MBit).
Mit zunehmenden Stationen steigt der Datenverkehr und somit die Anzahl der Kollisionen. Die Effizienz des Datenverkehrs leidet darunter.
Die räumliche Ausdehnung ist auf die maximale Verzögerungszeit (Bitzeit) und die maximale Kabellänge beschränkt.
In einer Collision Domain dürfen maximal 1024 Stationen angeschlossen werden.

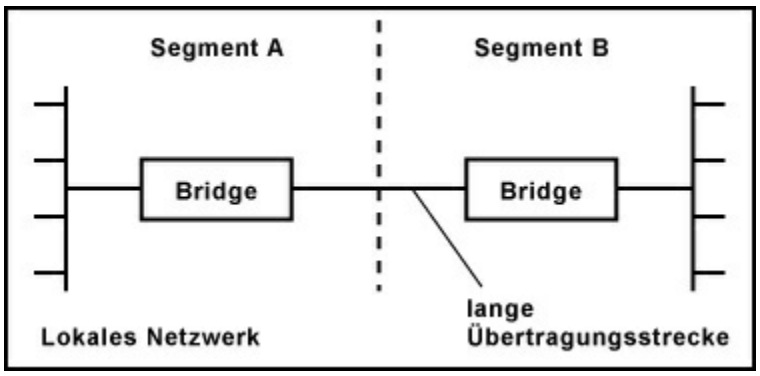


Alle diese Probleme lassen sich mit einer Bridge lösen. Eine Bridge arbeitet

auf der Sicherungsschicht (Schicht 2) des OSI-Schichtenmodells und ist protokollunabhängig. Sie überträgt alle auf dem Ethernet laufende Protokolle. Für die beteiligten Stationen arbeitet die Bridge absolut transparent.
Durch eine Bridge kann ein überlastetes Netzwerk physikalisch in Segmente aufgeteilt und logisch wieder zusammengeführt werden. Dabei bleiben alle Störungen, Kollisionen, fehlerhafte Pakete und der Datenverkehr innerhalb des Segments und belasten das andere Segment nicht. Nur der Datenverkehr, der in das andere Segment muss, wird von der Bridge über die logische Verbindung durchgelassen.
Eine Bridge legt sich eine Datenbank aller Stationsadressen (MAC-Adressen) an. Anhand dieser Daten entscheidet die Bridge, ob die empfangenen Datenpakete in ein anderes Netzwerksegment

weitergeleitet werden oder nicht. Mit der Zeit kann dann die Bridge immer besser entscheiden, in welches Segment die ankommenden Daten gehören. Eine Bridge arbeitet aber nur dann sinnvoll, wenn zwei Netzwerk-Segmente verbunden werden sollen, aber der meiste Datenverkehr innerhalb der beiden Segmente stattfindet. Multicasts und Broadcasts werden immer weitergeleitet.

Anstatt einer Bridge verwendet man heute einen Switch. Dieser ist wesentlich billiger und erfüllt die selben Funktionen.



Die Längenbeschränkungen des Ethernet-Standards werden durch mehrere

hintereinandergeschaltete Bridges aufgehoben. Nach IEEE 802.1 lassen sich 7 Bridges hintereinanderschalten. In der Regel werden nicht mehr als 4 hintereinander geschaltet.

Lokale Netzwerke, die eine längere Strecke überbrücken müssen, werden gerne mit unterschiedlichen Übertragungsmedien gekoppelt. Der Einsatz von zwei Bridges kann eine andere Übertragungsstrecke, z. B. Satellit, Funk oder Glasfaser, zwischenschalten und so als Konverter zwischen zwei Übertragungsmedien dienen.

Switch

Ein Switch ist ein Kopplungselement, das mehrere Stationen 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 Stationen, 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 welche Station erreichbar ist. Auf diese Weise erzeugt jeder Switch-Port eine eigene Collision

Domain (Kollisionsdomäne).

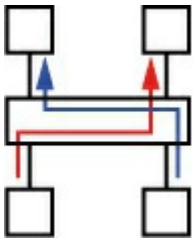
Teure Switches können zusätzlich auf der Schicht 3, der Vermittlungsschicht, des OSI-Schichtenmodells arbeiten (Layer-3-Switch oder Schicht-3-Switch). Sie sind in der Lage, die Datenpakete anhand der IP-Adresse an die Ziel-Ports weiterzuleiten. Im Gegensatz zu normalen Switches lassen sich auch ohne Router logische Abgrenzungen erreichen.

Kollisionsdomäne (Collision Domain)

Durch das CSMA/CD-Verfahren entstehen Kollisionen, wenn mehrere Stationen an einer Kollisionsdomäne angeschlossen sind. Das wiederum reduziert den Netzwerk-Verkehr, der durch wiederholte Übertragungen verursacht wird. Die Einrichtung mehrerer Kollisionsdomänen reduziert die Anzahl der Kollisionen von

Datenpaketen.

Switches bilden an jedem ihrer Ports eine Kollisionsdomäne, indem sie den Datenverkehr nur an den Port weiterleiten an dem sich die Ziel-MAC-Adresse befindet. Innerhalb einer Kollisionsdomäne (Switch-Port)



befindet sich dann in der Regel eine einzelne Station, ein weiterer Switch oder ein Router in ein anderes Netz.

MAC-Adressen-Verwaltung / MAC-Tabelle

Switches haben den Vorteil, im Gegensatz zu Hubs, dass sie Datenpakete nur an den Port weiterleiten, an dem die Station mit der Ziel-Adresse angeschlossen ist. Als Adresse 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 ab von seinem internen Speicher.

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 Switches genügend Kapazität bei der Verwaltung von MAC-Adressen haben.

Zusätzliche Leistungsmerkmale von Switches

IEEE 802.1q / VLAN

IEEE 802.1x / RADIUS

LACP

GVRP

SNMP - Simple Network Management Protocol

Bandbreite

Die Daten in einem Switch werden über die sogenannte Backplane übertragen. Über die Backplane werden alle Ports miteinander verbunden, die Daten miteinander austauschen müssen. Die

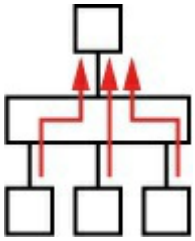
Bandbreite muss also groß genug sein,
um alle angeschlossenen Stationen mit
der Netzwerk-Geschwindigkeit bedienen
zu können.

$$Anzahl\ der\ Ports \bullet MBit/s = Bandbreite\,(MBit/s)$$

$$5\,(Port) \bullet 100\,MBit/s \bullet 2\,(Vollduplex) = 1000\,MBit/s$$

Es gilt die Faustformel: Die Bandbreite
der Backplane muss dem Doppelten der
höchstmöglichen Bandbreite aller
verfügbaren Ports entsprechen.
Vereinfacht gilt folgende Formel:
Das Ergebnis muss nochmals verdoppelt
werden (x2), wenn die Daten mit
Vollduplex übertragen werden.
Ein Switch mit 5 Fast-Ethernet-
Anschlüssen (100 MBit/s) benötigt also
eine Backplane-Bandbreite von 1 GBit/s
(1000 MBit/s).
Bei kleinen Netzwerkinstallationen
spielt die Backplane-Bandbreite in der
Regel keine Rolle. Schon billige

Switches haben eine ausreichend große



Backplane-Bandbreite. Dient der Switch aber als Verteiler zwischen Stationen mit Datenbankabfragen und File-Transfers, dann spielt die Bandbreite ein größere Rolle.

Einfachere Switches basieren in der Regel auf einer Bus-Architektur mit hoher Bandbreite, da der Schaltungsaufwand geringer ist und sich das Gerät billiger herstellen lässt.

Problemfall: Switch

Fließt der Datenverkehr in einem Netzwerk ständig nur zu einer einzigen Station, dann hat der Switch wenig Einfluss auf die Performance. Eine geringe Anzahl an Datenpaketen kann ein Switch zwischenspeichern. Irgendwann

verwirft er die eingehenden Datenpakete oder erzeugt Kollisionen.
Verworfene Datenpakete werden von höheren Protokollen, wie TCP oder IPX, erneut gesendet. Bei ungesicherten Protokollen, wie z. B. UDP oder NetBIOS kann das jedoch zu Verbindungsabbrüchen führen.
Kollisionen werden auf der Schicht 2 erkannt und erneut angefordert. In jedem Fall entstehen spürbare Verzögerungen im Netzwerkverkehr.

Bauformen

Switches gibt es in den unterschiedlichsten Bauformen und Ausbaustufen. Generell gilt, je größer und besser ein Switch ausgestattet ist, desto teurer ist er. Ein einfacher Switch hat 4 oder 5 Ports. Mit ein paar Status-LEDs sind sie in Kästchen in der Größe einer Zigarettenschachtel eingebaut.
Etwas bessere Switches haben ein

Metallgehäuse, sind stabiler und für den Dauereinsatz besser geeignet. Neben den kleinen 4- und 5-Port Switches gibt es Ausbaustufen mit 8, 16, 24 und 32 Ports. Wer mehr Ports benötigt, braucht stackable Switches, die sich über separate Kabel miteinander verbinden und übereinander stapeln lassen. Wer Switches in 19"-Schränken installieren will, der sollte auf 16-, 24- und 32-Port Switches achten. Diese verfügen über Halterungen für 19"-Einbauschienen.
Die kleinen Geräte haben manchmal Halterungen an der Unterseite und lassen sich an der Wand montieren.
Wer kleine Switches mit geringer Portanzahl kauft und nicht in einen 19"-Schrank einbaut, der sollte auf die Anordnung von RJ45-Buchsen und Status-LEDs achten. Es gibt Geräte, bei denen die LEDs auf der Vorderseite und die Anschlüsse auf der Rückseite

angeordnet sind. In billigen Geräten sind die Status-LEDs in die RJ45-Buchsen integriert. Das ist nicht immer praktisch. Z. B. wenn die Kabel nicht aus der Richtung kommen, wo man die Status-LEDs gut sichtbar haben will. In der Regel werden kleine Switches von einem Steckernetzteil mit Strom versorgt und haben keinen Aus- und Ein-Schalter. Geräte mit größerer Port-Anzahl haben das Netzteil integriert und einen Lüfter zur Kühlung. Vorsicht dann bei Gebrauch im privaten Bereich. Der Lüfterlärm ist nicht zu unterschätzen.

Switching

Switching ist ein Mechanismus, um in paketorientierten Netzwerken die Datenpakete verbindungsorientiert zwischen Eingang und Ausgang weiterzuleiten. Beim Switching wird das eingehende Ethernet-Frame analysiert. Die MAC-Adressen von Sender und

Empfänger werden in der MAC-Tabelle (FDB, Forwarding Database) gespeichert. So können die Datenpakete schneller an den Switch-Port, an dem der Empfänger hängt, weitergeleitet werden. Da eine Station an einen anderen Switch-Port umgezogen werden kann, werden alte Einträge in der MAC-Tabelle regelmäßig gelöscht (Ageing-Mechanismus).

Die Verarbeitungszeit eines Switches wird als Latenz bezeichnet. Die Dauer hängt vom verwendeten Switching-Verfahren ab.Unterschieden wird Cut-Through, Store-and-Forward, Adaptive-Cut-Through und FragmentFree-Cut-Through.

Neben der reinen Verarbeitungsgeschwindigkeit des Switching-Verfahrens ist auch die Leistungsfähigkeit der Backplane für die Latenz der Ethernet-Frames

verantwortlich. Wird ein Switch verwendet, der für alle Ports in Summe nicht genug Bandbreite zu Verfügung hat, müssen die Frames oft zwischengespeichert werden.
Die Übertragungsleistung wird in Frames pro Sekunde bzw. Packets per Second (PPS) angegeben. Kann ein Switch alle Ports ständig mit der höchsten Datenrate bedienen, wird von non-blocking oder auch von der Wire-Speed-Fähigkeit gesprochen.

Cut-Through

Der Switch analysiert bereits die Ethernet-Frames, bevor sie vollständig eingetroffen sind. Hat er die Ziel-Adresse identifiziert, wird das Frame sofort am Ziel-Port ausgegeben. Die Latenz, die Verzögerungszeit zwischen Empfangen und Weiterleiten eines Frames, ist äußerst gering.
Das Cut-Through-Verfahren verzichtet

auf die vollständige Analyse der Frames, wobei fehlerhafte oder beschädigte Frames unerkannt bleiben und ungehindert weitergeleitet werden. Obwohl dieses Verfahren sehr schnell ist, kann es auch zu einer Belastung des Netzwerks führen, weil defekte Ethernet-Frames nochmals übertragen werden müssen.

Store-and-Forward

Der Switch nimmt stets das gesamte Frame in Empfang und speichert es in einem Puffer zwischen. Erst danach wird das Frame analysiert. Dazu wird geprüft, ob das Frame die richtige Struktur (nach IEEE 802.1d) hat. Außerdem wird die Richtigkeit der CRC-Prüfsumme (nach IEEE 802.3) getestet. Erst danach wird die Ziel-MAC-Adresse ausgelesen und überprüft. Befindet sich die Ziel-Adresse in der MAC-Tabelle wird das Frame an den gespeicherten Port

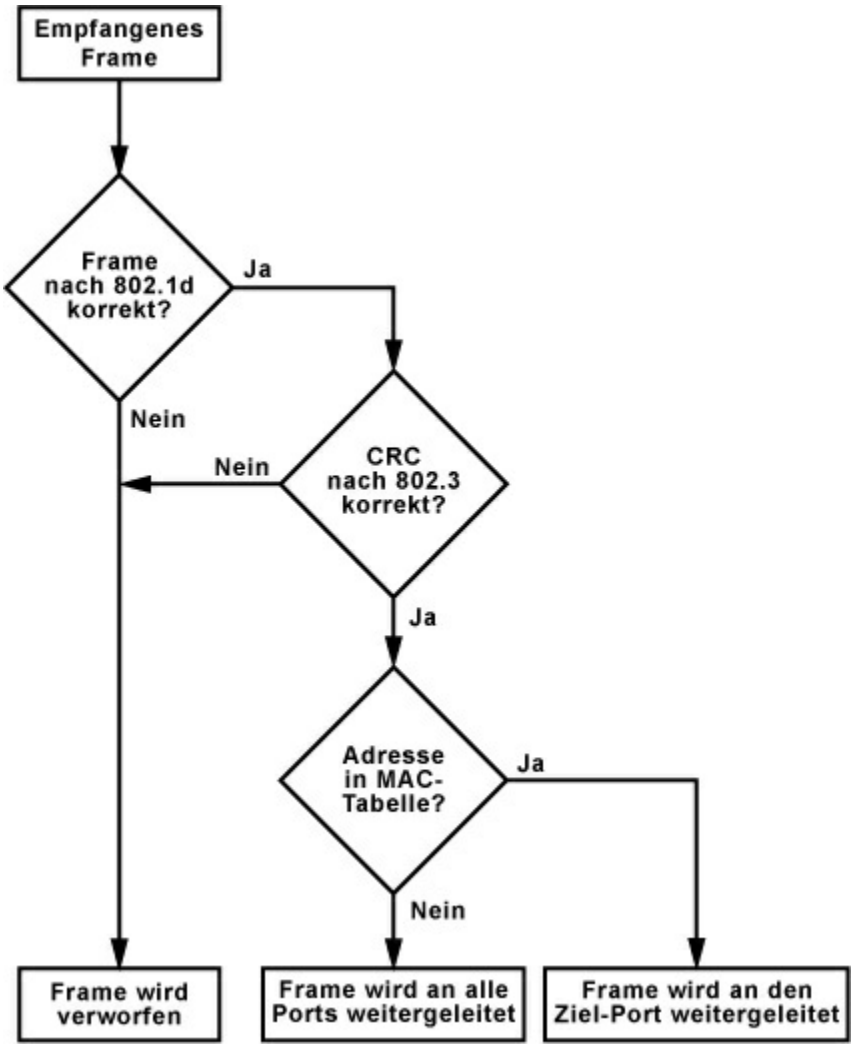
ausgegeben. Wenn die Adresse sich nicht in der MAC-Tabelle befindet wird das Frame an allen Ports weitergeleitet (Broadcast).
Wenn ein Frame der Ziel-Adresse zurück kommt, dann speichert der Switch die Ziel-Adresse und den dazugehörigen Port in seiner MAC-Tabelle. Beim nächsten Datenpaket mit dieser Ziel-Adresse schickt der Switch das Frame gleich an den zugeordneten Port.
Grundsätzlich benötigt das Store-and-Forward-Verfahren mehr Zeit bis ein Frame weitergeleitet ist. Die genaue Analyse eines Frames reduziert jedoch die Netzbelastung durch fehlerhafte Frames. Bei unterschiedlich schnellen Netzwerk-Stationen werden die Frames durch die Zwischenspeicherung vermittelt.

Folgendes Ablaufdiagramm

verdeutlicht die

Vorgehensweise des Store-

and-Forward-Verfahrens:



Adaptive-Cut-Through

Je nach Implementierung gibt es

Unterschiede bei diesem Switching-

Verfahren. In jedem Fall wird auf eine

Kombination aus Cut-Through und

Store-and-Forward gesetzt.

Im einen Fall werden die Frames mit Cut-Through weitergeleitet, aber anhand der Prüfsumme (CRC) geprüft. Wird eine bestimmte Fehlerrate überschritten wird automatisch auf Store-and-Forward umgeschaltet. Geht die Fehlerrate zurück, wird auf Cut-Through zurückgeschaltet. Mit diesem Verfahren wird in teuren Switches eine Optimierung des Datenverkehrs zwischen Schnelligkeit und Fehlerfreiheit hergestellt.
Unterschiedliche Datenraten kann dieses Switching-Verfahren nicht berücksichtigen. Die Switches unterstützen nur eine Art der Datenrate (10 MBit / 100 MBit / 1 GBit).
Eine anderen Art von Adaptive-Cut-Through entscheidet anhand der Länge des Frames, welches Verfahren angewendet wird. Ist keine Apassung der Datenrate nötig, werden Frames mit

einer Länge über 512 Byte per Cut-Through weitergeleitet. Kürzere Frames werden vor der Weiterleitung mit Store-and-Forward analysiert. Mit diesem Switching-Verfahren optimiert man die Latenz anhand der Länge von Frames.

FragmentFree-Cut-Through

Dieses Verfahren stammt von Cisco und geht von einem Erfahrungswert bei fehlerhaften Frames aus. Man hat festgestellt, dass Übertragungsfehler am häufigsten innerhalb der ersten 64 Byte eines Frames auftreten. Deshalb überprüft ein, mit FragmentFree-Cut-Through arbeitender, Switch die ersten 64 Byte auf Fehler. Ist es fehlerfrei wird das Frame per Cut-Through weiterverarbeitet. Ist ein Fehler vorhanden, dann wird das Frame verworfen.

Funktionen im Überlastungsfall

Müssen in einem geswitchten Netzwerk sehr viele Datenpakete auf einem einzigen Port weitergeleitet werden, passiert es sehr schnell, dass die Eingangspuffer der anderen Ports volllaufen und sich das Verwerfen von Frames nicht mehr vermeiden lässt. Für die Protokolle auf den höheren Schichten, wie z. B. TCP/IP ist das äußerst ungünstig, weil sich durch den Paketverlust die Übertragungsleistung des Übertragungssystems verschlechtert. TCP/IP ist dann gezwungen durch geeignete Maßnahmen, z. B. Paketverkleinerung, die Übertragungsqualität zu verbessern. Zu Lasten der Übertragungsgeschwindigkeit. Denn kleinere Pakete bedeuten einen größeren Anteil von Steuerungsdaten (Header) gegenüber dem reinen Nutzdaten.

Flow-Control

Um den Worst-Case-Fall zu vermeiden steht im Standard IEEE 802.3x das Flow-Control zur Verfügung. Dieses Verfahren funktioniert grundsätzlich nur im Vollduplexmodus von Fast-Ethernet und Gigabit-Ethernet. Flow-Control kommt zum Einsatz, wenn ein Puffer vor dem Überlaufen steht. Der Switch schickt dann dem angeschlossenen Gerät ein Pause-Frame. Dieses ist ein spezielles MAC-Control-Frame, welches als Multicast an die Adresse 01-80-C2-00-00-01 verschickt wird. Im Length/Typ-Feld des Frames steht der Wert 88-08.

Back-Pressure

Ist kein Vollduplex möglich, wird ein Verfahren namens Back-Pressure verwendet. Es simuliert Kollisionen. Dazu wird vor dem drohenden Überlauf ein JAM-Signal vom Switch gesendet. Das angeschlossene Gerät beendet

daraufhin den Sendevorgang und wartet einige Zeit, bevor es erneut Frames sendet.

Head-of-Line-Blocking

Im Regelfall unterstützen alle Gigabit-Ethernet-Komponenten das Flow-Control-Verfahren. Bei Fast-Ethernet-Komponenten ist das nicht immer der Fall. Ob diese Funktion genutzt werden kann, wird während des Link-Aufbaus (nach dem Herstellen der Steckverbindung) mit der Auto-Negotation ermittelt. Wenn nicht, bieten viele Switches die Head-of-Line-Blocking-Funktion. Sie prüft die Zieladresse und deren Port-Zuordnung. Ist der Ausgangspuffer des ermittelten Ports blockiert, wird das Frame verworfen, damit der Puffer des Eingangsports frei bleibt.

Router

Ein Router ermöglicht es mehrere

Netzwerke mit unterschiedlichen Protokollen und Architekturen zu verbinden. Router finden sich häufig an den Außengrenzen eines Netzwerkes, um es mit dem Internet oder einem anderen 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:

1. Ermittlung der verfügbaren Routen
2. Auswahl der geeignetsten Route
3. Herstellen der Verbindung

4. Anpassen der Datenpakete an die Übertragungstechnik (Fragmentierung)

Routing

Routing ist die Wegfindung zum Ziel anhand einer oder mehrere Kriterien (metric), die diesen Weg bestimmen. Je mehr Kriterien berücksichtigt werden müssen, desto genauer und gezielter ist der Weg zum Ziel, desto (zeit-)aufwendiger ist die Bestimmung oder Berechnung des Wegs.

Routing-Tabelle

Die Routing-Tabelle enthält eine umfassende und aktuelle Wegbeschreibung durch das Netz. In ihr sind alle bekannten Routen eingetragen. Die Routing-Tabelle wird entweder manuell gefüllt, also statische Routen angelegt, oder dynamisch im Austausch mit anderen nahegelegenen Routern gepflegt. Änderungen der möglichen

Routen müssen beim statischen Routing händisch vom Administrator gepflegt werden. Beim dynamischen Routing werden die Routing-Tabellen von den Routern selbständig gepflegt und an die Netzstruktur angepasst. Z. B. auch beim Ausfall von Routern oder Übertragungsstrecken.

Die Routing-Tabelle enthält folgende Angaben:

alle bekannten Netzwerkadressen

Verbindungsarten in andere Netzwerke

Weginformationen zu anderen Routern

Verbindungskosten

Routenwahlmethoden

Der Aufbau einer Routing-Tabelle entscheidet, welche Routenwahlmethode verwendet wird. Diese Methode ist ein Algorithmus, der die Einträge in der Routing-Tabelle benutzt um die Route zu

berechnen.

Die häufigsten Routenwahlmethoden sind der Distance-Vector-Algorithmus (DVA) und der Link-Status-Algorithmus (LSA).

LSA - Link-Status-Algorithmus

Der LSA bestimmt die Route anhand dem Status der Verbindungen, also deren Verfügbarkeit und Geschwindigkeit. Ein spezieller Sortieralgorithmus ermittelt dann z. B. den kürzesten Weg (Shortest Path) zum Ziel.

Beim Link-Status-Routing (LSR) werden die Änderungen in der Routing-Tabelle per Multicast zwischen den Routern ausgetauscht. In der Routing-Tabelle ist deshalb die gesamte Netzstruktur abgebildet. Der Router kennt deshalb jede erdenkliche Route.

Protokolle nach LSA werden als externe oder exterior Routing Protokolle

bezeichnet, die netzübergreifend genutzt werden.

DVA - Distance-Vector-Algorithmus

Jede Route wird anhand einiger Kriterien klassifiziert. Aus allen Routen wird dann die mit den optimalen Voraussetzungen gewählt. Besonders bei weit entfernten Zielen mit vielen Routen, lässt sich so die optimale Route ermitteln.

Beim Distance-Vector-Routing (DVR) werden die Routing-Tabellen mit dem direkten Nachbar-Router ausgetauscht. Die Routing-Tabelle wird in periodischen Abständen ausgetauscht. Das führt zu zusätzlichem Datenverkehr zwischen den Routern.

DVR-Protokolle werden als interne oder interior Routing Protokolle bezeichnet, die in lokalen Netzen genutzt werden.

Routing-Protokolle für

dynamisches Routing

BGP - Border Gateway Protocol

EGP - Exterior Gateway Protocol

IGP - Interior Gateway Protocol

OSPF - Open Shortest Path First

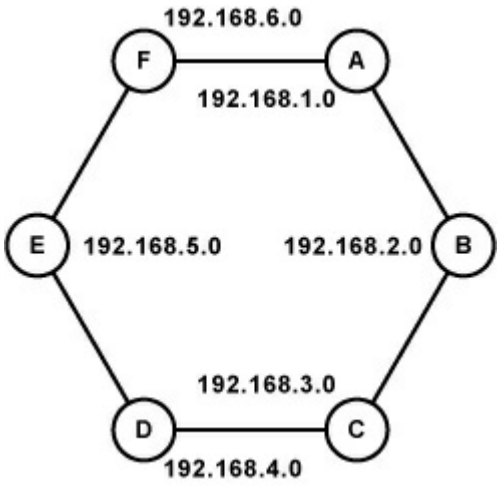
RIP - Routing Information Protocol

DRP - DECnet Routing Protocol

IGRP - Interior Gateway Routing Protocol

EIGRP - Enhanced Interior Gateway Routing Protocol

RIP - Routing Information Protocol



Netzwerk

Hop-Anzahl

Von

Nach

0

192.168.2.0 (Direktverbindung)

192.168.3.0 1

192.168.1.0 192.168.4.0 2

192.168.5.0 1

0

192.168.6.0 (Direktverbindung

Das RIP ist ein Distance-Vector-Algorithmus, also ein Distance-Vector-Routing-Protokoll. Es ist das einfachste und meist genutzte Routing-Protokoll. Die Fähigkeiten moderner Netze werden von RIP allerdings nicht berücksichtigt. Im einfachsten Fall speichert RIP in seiner Routing-Tabelle neben Netzwerkadresse und abgehende Schnittstelle nur die Anzahl der Stationen (Hops) die ein Datenpaket bis zum Zielnetz überwinden muss. Ein Hop-Eintrag von 16 gilt als unendlich und bedeutet, dass dieses Netz nicht

erreichbar ist. Deshalb ist RIP in Netzwerken mit mehr als 15 Zwischenstationen nicht geeignet. Es wird daher auch nur in lokalen Netzwerken eingesetzt, wo die Netzübergänge (Router) von gleicher Qualität sind und die Netzwerkstruktur nur selten verändert wird.
Die Routing-Tabellen werden von den Routern alle 30 Sekunden mit dem benachbarten Router ausgetauscht. Dies führt zu einem erhöhten Datenverkehr zwischen den Routern. Fällt ein Router aus, kann es mehrere Minuten dauern, bis diese Information und die entsprechend geänderte Routing-Tabelle übermittelt wurden.

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 Switches

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-Switches gegenüber reinen Routern bevorzugt. Zumindest in großen Netzen.

Layer-3-Switches lassen sich als Router, Switch oder als Mischform betreiben.

Im Vergleich zu Routern haben Layer-3-

Switches eine geringere Verzögerungszeit und einen höheren Datendurchsatz.

Funktionell ist es so, dass das erste Datenpaket einer Verbindung wie bei einem Router behandelt 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)

weniger Features

Auf IP-Ebene lassen sich durch Routing-Funktionen deutlich mehr Möglichkeiten

zur Steuerung von Netzwerkverkehr realisieren.

Gateway

Gateways behandeln die Schichten 1 bis 7 des OSI-Modells und koppeln die unterschiedlichsten Protokolle und Übertragungsverfahren miteinander. Grundsätzlich geht man von zwei verschiedene Ansätzen aus. Einmal von medienkonvertierenden Gateways, die bei gleichen Übertragungsverfahren zwischen zwei verschiedenen Protokollen der OSI-Schichten 1 und 2 verbinden. Dann gibt es noch die protokollkonvertierenden Gateways, die unterschiedliche Protokolle auf den OSI-Schichten 3 und 4 miteinander verbinden.

Gateways haben die Aufgabe eine logische Verbindung herzustellen einen Datenstrom zwischen Quelle und Ziel zu übermitteln. Beim Übergang zwischen

zwei Netzen berücksichtigt das Gateway folgendes:

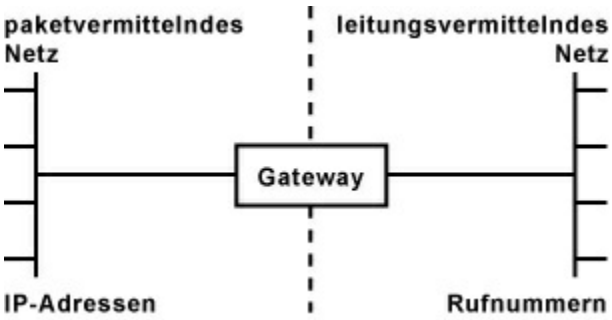
Protokolle

Adressierung

Übertragungsgeschwindigkeit

physikalische Bedingungen (Übertragungsmedium)

Beispiel für ein Gateway



Ein Gateway ist ein aktiver Netzknoten, der zwei Netze miteinander verbinden kann, die physikalisch zueinander inkompatibel sind und/oder eine unterschiedliche Adressierung verwenden. Klassisches Beispiel ist der ISDN-Router, der zwischen dem LAN und dem öffentlichen Telefonnetz (ISDN) verbinden kann. Dazu gehören auch Fax-Server und Voice-over-IP-

Gateways.

Server

Ein Server ist ein Computer, der Rechenleistung, Speicher und Daten bereitstellt und Zugriffsrechte verwaltet. In den meisten Fällen handelt es sich um einen sehr leistungsfähigen Computer, der je nach Anwendungsfall mit spezieller Hardware und Software ausgestattet ist. Auf dem Server laufen mehrere Dienste und Anwendungen, die von anderen Netzwerk-Teilnehmern über das Netzwerk anfordern werden. In einigen wenigen Fällen wird ein Server für eine einzige Anwendung oder einen Dienst eingerichtet. Um die Verfügbarkeit dieses Computers zu erhöhen, werden mehrere Server mit einem Load-Balancer verbunden, der die Anfragen auf die einzelnen Server verteilt.

Application-Server

Ein Application-Server führt für mehrere Clients ein Anwendungsprogramm aus. Je nach Struktur des Anwendungsprogramms und Anzahl der Clients ist viel Rechenleistung und viel Hauptspeicher nötig.

Compute-Server

Ein Compute-Server ist eine reine Rechenmaschine, der in der Forschung eingesetzt wird. Er sollte möglichst viel Rechenleistung zur Verfügung stellen. Und der Programmcode sollte sich effizient ausführen lassen.

Datenbank-Server

Auf einem Datenbank-Server befinden sich größere Datenbanken. Der Server hat die Aufgabe die Verwaltung, Organisation, das Suchen, Einfügen und Sortieren der Datensätze zu übernehmen. In großen Datenbank-Servern arbeiten

häufig mehrere Prozessoren oder Prozessorkerne parallel, um die Bearbeitung der vielen einzelnen Abfragen ausführen zu können. Dazu ist noch ein großer Hauptspeicher notwendig, um Teile der Datenbank im Arbeitsspeicher ablegen zu können.

File-Server

Ein File-Server stellt dem Client die Dateien und den Speicherplatz zur Verfügung, auf den auch andere Netzwerkteilnehmer zugreifen können. Der File-Server übernimmt zusätzlich die Sicherung der Dateien und Verzeichnisse.
Der Server transportiert hauptsächlich die Daten zwischen den Festplatten und Netzwerkkarten hin und her. Dafür benötigt er vor allem viel Rechenleistung, um die Koordination der Ein- und Ausgabebaugruppen durchzuführen.

In der Regel ist ein File-Server an ein Speichernetzwerk angebunden.

Internet-Server

Der Internet-Server stellt die verschiedenen Internet-Dienste zur Verfügung. Z.B. WWW, DNS, FTP und E-Mail (POP, SMTP). Die Anforderungen an die Hardware sind relativ gering, da die Last durch die Bandbreite der Internet-Anbindung begrenzt ist.

(Streaming-)Media-Server

Dieser Server stellt Audio- und Video-Daten in Echtzeit und in höchster Qualität einer großen Anzahl an Nutzern zur Verfügung. Die Hardware muss den Ansprüchen und der zu übertragenden Datenmenge entsprechen.

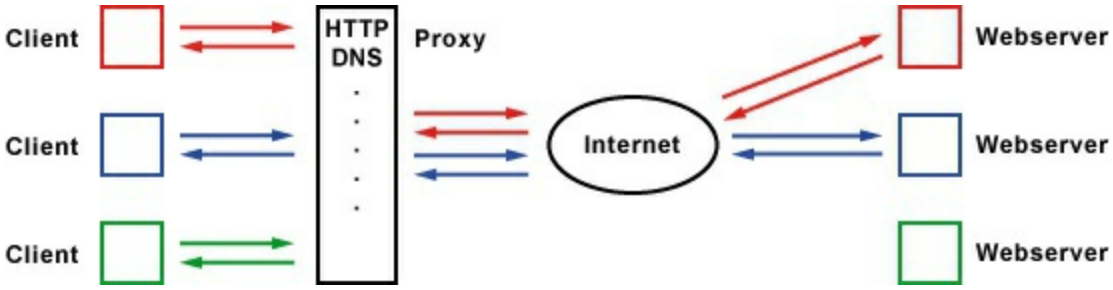
Proxy / Proxy-Server

Ein Proxy ist ein Dienst, der als Zwischenspeicher innerhalb eines

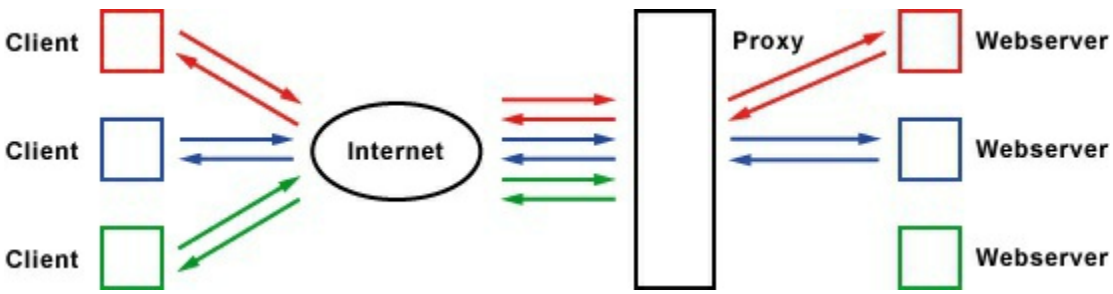
Netzwerks dient, um die Zugriffe auf immer die gleichen Daten und Dateien aus dem Speicher zu bedienen.
Der Begriff Proxy bezieht sich auf einen Server oder einen Dienst, der auf einem Server läuft. Der Proxy-Dienst ist ein Programm, dass im Hintergrund auf einem Server arbeitet. Proxy bedeutet Stellvertreter. Er ist im einfachsten Fall eine Art Cache für Webseiten. Er nimmt Anfragen von Clients entgegen und wertet sie aus. Stellvertretend leitet er die Anfrage ins Internet weiter. Die zurückgelieferten Daten werden vom Proxy vor dem Weiterleiten gespeichert. Bei einer erneuten Anfrage auf das gleiche Ziel werden die Daten nicht aus dem Internet geladen, sondern direkt aus dem Proxy-Speicher zum Empfänger geschickt. Auf diese Weise wird Datenverkehr ins Internet eingespart. Das senkt die Kosten und erhöht die

Bandbreite für andere Anwendungen.

Standard-Proxy



Die Clients schicken Ihre Zugriffe nicht direkt ins Internet, sondern zum Proxy. Dieser Server übernimmt als Mittler die Verbindung zum Webserver. Häufige Internet-Seiten oder Downloads müssen dann nicht mehr erneut über das Internet übertragen werden, sondern können vom Proxy-Server direkt an die Clients geschickt werden. Das reduziert das Datenaufkommen in das Internet und liefert den Clients die Daten schneller zurück.



Reverse-Proxy

Der Reverse-Proxy funktioniert anders herum und ist mit Load Balancing vergleichbar. Die Clients greifen zum Beispiel ohne Proxy auf das Internet zu. Ein Gruppe von Webservern ist hinter einem Proxy versteckt. Die Webserver sind also nicht direkt erreichbar.
Der Proxy leitet häufige identische Zugriffe aus dem Internet nicht an die Webserver weiter, sondern arbeitet sie selber ab, sofern er die Daten zwischengespeichert hat.
So ist eine einfache Lastverteilung möglich, ohne teures oder kompliziertes Load Balancing einrichten zu müssen.
Reverse-Proxys können auch unberechtigte Zugriffe verhindern.
In einem anderen Anwendungsfall wird die Zugriffsberechtigung für mehrere Server zentral von einem Proxy abgewickelt.

Vorteile

schnellerer Zugriff auf immer die gleichen Daten

Kosteneinsparungen beim Internet-Datenverkehr

Integration von Viren- und Spamfilter möglich

Ein Proxy bietet mehr Schutz für die Systeme, die über einen Proxy, anstatt direkt mit dem Internet kommunizieren. Unverlangte Pakete von externen Rechnern gelangen nicht mehr ins lokale Netz, weil der Proxy die Zugriffe aus dem Internet nur dann weiterleiten kann, wenn vorher eine ausgehende Verbindung bestanden hat. Zusätzlich kann ein Virenfilter auf dem Proxy installiert werden. Damit der wirkungsvoll arbeiten kann, muss jeder Internet-Zugriff über den Proxy erfolgen. Das erreicht man dadurch, dass das Standard-Gateway nicht der Router zum

Internet ist, sondern ein vorgeschalteter Proxy.

Nachteile

Cache-Kohärenz durch veraltete Inhalte im Cache

nicht jede Anwendung unterstützt Proxys

nicht für jedes Internet-Protokoll gibt es Proxys

Der Nachteil von Proxys ist, dass für jedes Internet-Protokoll ein Proxy installiert werden muss, wenn der ganze Datenverkehr über den Proxy-Server abgewickelt werden soll. Das bedeutet, das Proxy-Programm muss alle möglichen Protokolle beherrschen, die das Internet zu bieten hat. Da reicht es nicht aus, nur HTTP für den Zugriff auf Webserver zu unterstützen. Auch POP und SMTP für die E-Mail-Kommunikation müssen beherrscht werden.

In der Regel müssen die Programme auf den Clients den Datenverkehr über einen Proxy unterstützen. Bei einfachen Internet-Diensten, wie WWW und E-Mail ist das kein Problem. Doch bei Online-Spielen und P2P-Tauschbörsen wird es schwierig oder funktioniert überhaupt nicht.

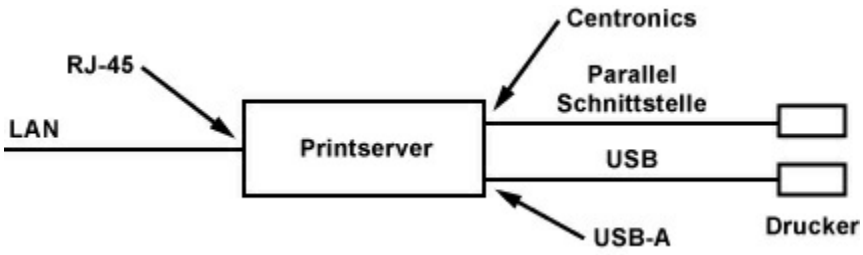
Fazit

Proxys sind in der Anfangszeit des kommerziellen Internets ein Mittel für Internet-Provider gewesen, um Datenverkehr einzusparen. Damals waren die Internet-Anbindungen noch langsamer und teurer. Außerdem waren noch viele Internet-User mit Modem oder ISDN-Karte unterwegs. Um die Daten schneller ausliefern zu können, wurden Proxys eingerichtet, um die Kunden schneller beliefern zu können und Datenverkehr einzusparen.

Inzwischen ist der Netzausbau des

Internets sehr großzügig ausgelegt, so dass ein Proxy keine Vorteile mehr bietet.

Eine Ausnahme bilden Übergänge von lokalen Netzwerken ins Internet, wo ein Proxy aus Sicherheitsgründen eingesetzt wird. Zum Einen, um die Möglichkeiten der Nutzer einzuschränken. Und zum Zweiten, um den Datenverkehr auf schädliche Inhalte, wie Viren und Würmern prüfen zu können. In der Regel geht es darum, das lokale Netzwerk zu schützen.



Printserver

Printserver sind eine Kombination aus Dienst und Schnittstellenwandler. Auf der einen Seite hängt der Printserver am Netzwerk, auf der anderen Seite ist ein

Drucker angeschlossen.

Ein Printserver ist im Prinzip ein kleiner PC mit Netzwerk- und Druckerschnittstelle, der darauf reduziert ist, die Druckaufträge aus dem Netzwerk zu verwalten und an den Drucker weiterzugeben.

Printserver-Varianten

Printserver: Die einfachste Art ist ein Drucker, der an einem Rechner lokal angeschlossen ist. Der Rechner selber ist am Netzwerk angeschlossen. Über eine Druckerfreigabe stellt der Rechner seinen Drucker anderen Netzwerkteilnehmern zur Verfügung.

Printserver-Box: Eine spezielle Printserver-Box stellt den Übergang vom Netzwerk zum Drucker-Anschluss dar. Meist verwendet man diese Printserver-Boxen, wenn man einen Drucker nachträglich ins Netzwerk bringen will. Es gibt einfache

Printserver, mit nur einer Druckerschnittstelle. Andere stellen mehrere Drucker-Schnittstelle zur Verfügung.

Eine Variante der Printserver-Box sind Router, die eine USB-Schnittstelle aufweisen. Sie haben meist einen Printserver integriert. Somit lässt sich an der USB-Schnittstelle des Routers ein USB-Drucker betreiben.

Netzwerk-Drucker: Spezielle Netzwerk-Drucker haben den Printserver bereits integriert. Sie werden direkt ans Netzwerk angeschlossen. Daher auch der Name Netzwerk-Drucker.

Drucker-Schnittstellen

Für folgende Drucker-Schnittstellen gibt es Printserver:

Parallele Schnittstelle

USB

Anwendung

Printserver machen dann Sinn, wenn

mehrere Personen mit zwei oder mehr Computer auf einem Drucker drucken können müssen. Es macht schließlich keinen Sinn, für jeden Computer einen Drucker zu kaufen. Praktischer und auch günstiger ist es, wenn alle sich einen Drucker teilen. Entweder greift man zur Druckerfreigabe, setzt eine Printserver ein oder setzt konsequent auf Netzwerkdrucker.

Voraussetzung dafür ist ein Netzwerk, in das alle Computer eingebunden sind. In der Regel besteht das bereits, wenn sich alle einen Internet-Anschluss teilen.

Übertragungstechnik

IEEE 802

Ethernet-Standards

WLAN-Grundlagen

IEEE 802

IEEE - Institute of

Electrical and Electronics

Engineers

Das IEEE (Institute of Electrical and Elektronics Engineers) 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 wurde offiziell am 1.1.1963 gegründet. Es handelte sich damals um die Fusion zweier Gremien, die sich mit ähnlichen Aufgabestellungen beschäftigen.
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. Nicht alles, was das IEEE entwickelt und standardisiert ist

marktreif geworden. Die Entwicklung neuer Standards läuft der Entwicklung im Markt meist hinterher. So kommt es, dass ein Standard verabschiedet wird, der sich wenig später als überflüssig herausstellt. Trotzdem werden in der Regel nur die Standards genormt, die technisch umsetzbar sind und auch wirtschaftliche Chancen haben.

Das IEEE kennt man vor allem durch Standardisierungen im Bereich Local Area Network (LAN). Die bekanntesten Standards sind 1394 für FireWire, 1284 für die Centronics-Druckerschnittstelle und 802 für die Netzwerkschnittstelle Ethernet, die auch heute noch weiterentwickelt wird. Eine vollständige Projektliste ist auf der Webseite des IEEE zu finden.

IEEE 802

Mit der Notwendigkeit Ende der 70er Jahre Standards im Bereich der lokalen

Netze einzuführen, wurde das Projekt 802 gegründet. Dieses Projekt umfasst Standards für Local und Metropolitan Area Networks (LAN und MAN). Die Standards der 802-Familie decken die Bitübertragungs- und Sicherungsschicht des OSI-Schichtenmodells ab. Die Sicherungsschicht 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. Neben Ethernet (802.3) und Wireless LAN (802.11) kümmert sich das IEEE auch um die Standards Bluetooth (802.15.1) und WiMAX (802.16). Durch die Zahl hinter dem Punkt wird der

Standard genauer spezifiziert. Einzelne Standards innerhalb einer Gruppe werden mit einem angehängten Buchstaben oder weiteren Ziffern und Jahreszahlen gekennzeichnet.

Das Projekt 802 hat eine hohe Bedeutung erlangt. Die Bedeutung ist so groß, dass es im Bereich der lokalen Netze ohne Ethernet und seine vielen Erweiterungen praktisch nicht mehr geht. Andere Netzwerkstandards spielen nur in Randbereichen eine Rolle.

Aufgaben des IEEE 802

Das Normungsgremium 802 entwickelt Standards für LAN und MAN, hauptsächlich aber Ethernet-Techniken. In den Standards wird besonders die physikalische Übertragungsschicht (Physical Layer) und die Verbindungsschicht (Data Link Layer) behandelt.

Vom Projekt 802 werden die Schichten

1 (Physical Layer) und 2 (Data Link

Layer) als ein Ganzes gesehen und in die

Bereiche LLC (Logical Link Control)

und MAC (Media Access Control)

geteilt.

802.2

Logical Link Control

2 802.1

802.1

Internet- Media Access Control

Working

802.4 802.5 802.11

802.3

1

Token- Token- Wireless

Ethernet Bus

Ring

LAN

Neben der Standardisierung neuer

Übertragungstechniken hat das IEEE 802

die Aufgabe bestehende Techniken

auszureizen und für neue Anwendungen

zu optimieren. Einige Standards bauen deshalb aufeinander auf oder hängen voneinander ab.

Übersicht der Projekte des IEEE 802

Die Liste folgende ist nicht vollständig. Sie bildet nur die wichtigsten Standards und Arbeitsgruppen ab. Unterstandards und nahezu unbedeutende Standards wurden hier nicht berücksichtigt.

802.1

Übersicht

802.1

Internet-Working

802.2

Logical Link Control (LLC)

Ethernet (10Base5) /

802.3

CSMA/CD-Zugriffsverfahren

802.3i

10BaseT

802.3u

100BaseT

802.3z

Gigabit Ethernet

802.3ab

1000BaseT

802.3an

10 Gigabit Ethernet

802.4

Token-Bus-Zugriffsverfahren

Token-Ring-

802.5

Zugriffsverfahren

Wireless LAN (WLAN) /

802.11

Drahtlose Netze

Breitband-Cable-TV

802.14

(CATV)

Wireless Personal Area

802.15.1 Network (WPAN) -

Bluetooth

UWB - Ultra Wideband

802.15.3a Wireless

Broadband Wireless Access

802.16

(BWA / WMAN) - WiMAX

Mobile Broadband Wirless

802.20

Access (MBWA) / Drahtlose

Breitbandnetze

IEEE 802.3 /

Ethernet

Grundlagen

Ethernet ist eine Familie von

Netzwerktechniken, die vorwiegend in

lokalen Netzwerken, aber auch zur

Verbindung großer Netzwerke zum

Einsatz kommt.

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 eine

Technik für lokale Netzwerke ist der

Name Ethernet das Synonym für alle

unter der Arbeitsgruppe 802.3

vorgeschlagenen und standardisierten

Spezifikationen.

802.2

Logical Link Control (LLC)

2 802.1 802.1

Internet- Media Access Control (MAC)

Working

802.4 802.5 802.11

802.3

1

Token- Token- Wireless

Ethernet Bus

Ring

LAN

Ethernet ist ein paketvermittelnde

Netzwerktechnik, die auf der Schicht 1

und 2 des OSI-Schichtenmodells die

Adressierung und die Zugriffskontrolle

auf das Übertragungsmedium definiert.

Die Daten kommen bereits in Paketen

von den darüberliegenden Schichten. Zum Beispiel von TCP/IP. Zusätzlich werden diese Datenpakete mit einem Header und einer Prüfsumme versehen. Danach werden sie übertragen. Bestandteil der Schicht 2 sind die LLC- und MAC-Schicht (IEEE 802.2 und 802.1). Sie sind unabhängig von Ethernet und werden auch für andere Übertragungstechniken verwendet.

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 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 bzw. die Atmosphäre. 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 80er 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.

Übertragungsmedium und Netzwerk-Topologie

Das ursprüngliche Ethernet nutzte ein Koaxialkabel als Übertragungsmedium. Dabei wurde mit einem Kabel jeweils eine Station mit mehreren anderen Stationen verbunden. Das Netzwerk wurde dann als sogenannter Bus aufgebaut. Jeweils am Kabelende wurde die Kabelstrecke mit einem Widerstand abgeschlossen.

Wegen den Nachteilen von Netzwerken mit der Bus-Topologie und dem Koaxialkabel wurde Ethernet um den

Einsatz von Twisted-Pair-Kabel der Kategorie 3 und 5 (UTP) erweitert. Es handelt sich dabei um 8-adrige Kabel, deren Adern jeweils paarweise verdrillt sind. Die Leitungsführung ist als Stern-Topologie mit Switches oder Hubs als Verteilstationen aufgebaut. Mit Switches kommt man ohne Kollisionserkennung aus und kann Vollduplex-Übertragung nutzen.

Twisted-Pair-Kabel haben allerdings eine Reichweite von nur 100 Metern, was es für die Vernetzung von Gebäuden oder als Backbone ungeeignet macht. Aus diesem Grund wurde Ethernet auch für Glasfaserkabel standardisiert. Heute spielt das Koaxialkabel keine Rolle mehr. Für Neuinstallationen werden generell Twisted-Pair-Kabel nach Kategorie 6 eingesetzt. Zur Überbrückung von längeren Strecken wird Glasfaserkabel verwendet.

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 breitet Ethernet Probleme bei allen Arten von zeitkritischen Anwendungen. Ethernet bietet keine Garantie, dass die Daten innerhalb einer bestimmten Zeit den Empfänger erreichen.

Dafür ist Ethernet eine einfach zu implementierende Vernetzungstechnik, die sich über die Jahrzehnte hinweg in lokalen Netzwerken bewährt hat.

Übersicht: Standards und Übertragungsgeschwindigkeit

Ethernet mit

10

100

1000

10 GBit/s

MBit/s

MBit/s

MBit/s

100Base- 1000Base- 10GBase-

10Base5 TX

T

T

100Base- 1000Base- 10GBase-

10Base2 T4

SX

CX4

10Base- 100Base- 1000Base- 10GBase-

T

T2

LX

LX4

10Base- 100Base- 1000Base- 10GBase-

FL

FX

LH

LW4

10Base-

1000Base- 10GBase-

FB

ZX

SR

10Base-

1000Base- 10GBase-

FP

CX

LR

10Base-

10GBase-

SX

ER

10GBase-

SW

10GBase-

LW

10GBase-

EW

CSMA/CD und

Kollisionen

(Ethernet)

CSMA/CD - Carrier Sense

Multiple Access with

Collision Detection

CSMA/CD (Carrier Sense Multiple Access with Collision Detection) ist ein Zugriffsverfahren von Ethernet, um auf das Übertragungsmedium zugreifen zu können.

Carrier Sense (Träger-Zustandserkennung): Jede Station kann feststellen, ob das Übertragungsmedium frei ist.

Multiple Access (Mehrfachzugriff): Mehrere Stationen können sich das Übertragungsmedium teilen.

Collision Detection (Kollisionserkennung): Wenn mehrere Stationen gleichzeitig senden, können sie die Kollision

erkennen.

Als Mehrfachzugriffsnetz können mehrere Ethernet-Stationen unabhängig voneinander auf das Übertragungsmedium zugreifen (Multiple Access). Alle Stationen hören permanent das Übertragungsmedium ab (Carrier Sense) und können zwischen einem freien und besetzten Übertragungsmedium unterscheiden. Bei einem freien Übertragungsmedium kann gesendet werden. Während der Datenübertragung wird überprüft, ob eine andere Station gleichzeitig gesendet hat und eine Kollision der Daten aufgetreten ist (Collision Detection). Ist keine Kollision aufgetreten wurde die Übertragung erfolgreich abgeschlossen. Verloren gegangene Pakete müssen durch Protokolle, wie z. B. TCP, neu angefordert werden. Tritt dies häufiger auf, werden mehr Datenpakete gesendet

und das drückt auf die effektive Übertragungsgeschwindigkeit des Netzwerks.

Ablauf von CSMA/CD

Das ursprüngliche Ethernet ist eine Bus-Topologie. Welche der angeschlossenen Stationen senden darf, wird durch das CSMA/CD-Verfahren bestimmt. Will eine Station senden, prüft sie, ob der Bus frei ist. Ist er frei, so beginnt die Station zu senden. Sie prüft allerdings weiterhin den Bus. Entsprechen die gesendeten Daten nicht den abgehörten Daten, so hat eine andere Station gleichzeitig gesendet. Eine Kollision wurde entdeckt und die Übertragung wird 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 verschickt werden konnten. Ist die Übertragung beendet und bis dahin keine Kollision aufgetreten, so nimmt die Station an, dass die Übertragung fehlerfrei verlaufen ist.

Kollisionen

Kollisionen gehören im Halbduplex-Betrieb zum normalen Betriebsablauf. Sie sind nicht als Störungen anzusehen. Allerdings werden Kollisionen zur größte Schwachstelle von Ethernet bzw. dem CSMA/CD-Verfahren, wenn die Anzahl der Kollisionen überhand nimmt. Die Anzahl der Kollisionen nimmt zu, je mehr Stationen auf das Übertragungsmedium Zugriff haben. Durch lange Kabel, 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. Beides darf nicht überschritten werden.

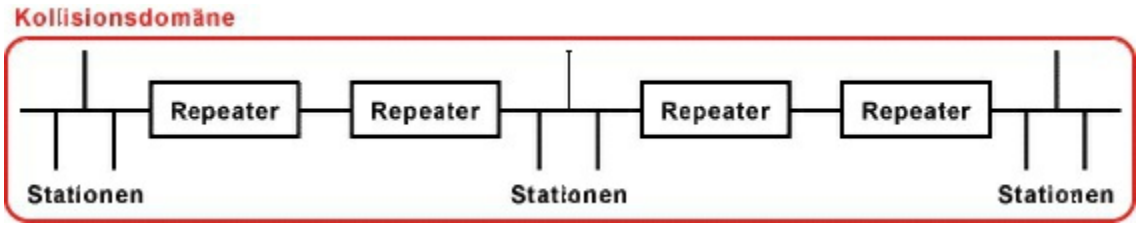
Solange die Bandbreite von Ethernet nicht mehr als zu 30 Prozent ausgereizt wird, machen sich Kollisionen kaum bemerkbar. Mit steigender Belastung des Netzwerks nehmen aber auch die Kollisionen zu. Hier hilft es nur, die Anzahl der Stationen zu reduzieren oder das gesamte Netzwerk in Teilnetz aufzuteilen.

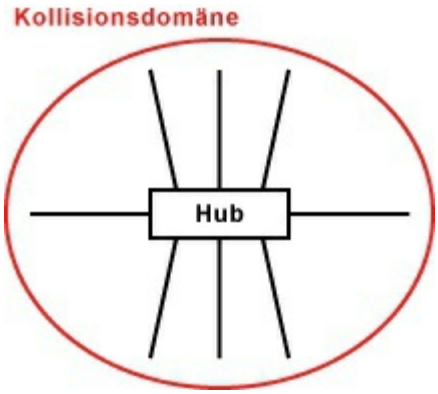
Kollisionsdomäne

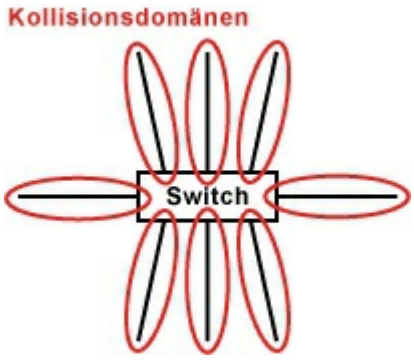
Die Kollisionsdomäne (collision domain) umfasst ein Netzwerk oder auch nur ein Teilnetzwerk aus Leitungen, Stationen und Kopplungselementen der Schicht 1 (OSI-Referenzmodell). In der Kollisionsdomäne müssen die Kollisionen innerhalb einer bestimmten Zeit jede Station erreichen. Das ist die Bedingung, 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 1023 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 werden. Dafür werden vier (4) Repeater eingesetzt. An nur drei (3) Segmenten dürfen Endstationen angeschlossen werden.

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.

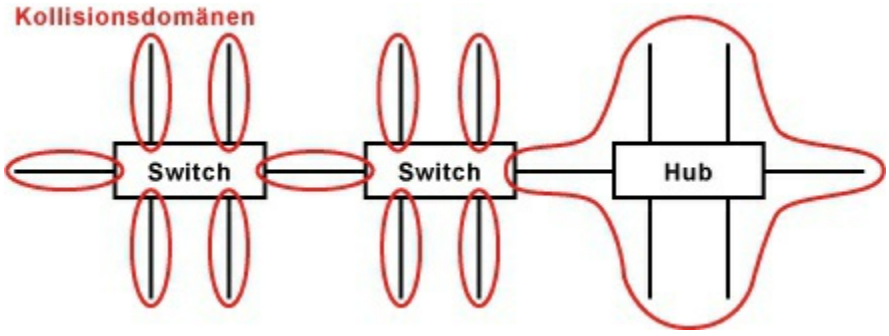






Beispiele für

Kollisionsdomänen



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 Switches 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 Switches 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).

Ethernet-Frame (Rahmenformat)

Ethernet ist ein paketvermittelndes Netzwerk. Die Daten werden in mehrere kleine Pakete aufgeteilt. Diese Pakete werden Frames genannt. Es gibt verschiedene Ethernet-Rahmenformate.

Ethernet II

Ethernet 802.3 raw

Ethernet 802.3

Ethernet 802.3 SNAP

Rahmenformate, die um VLAN-Tags erweitert sind

Grundsätzliches zu Ethernet-Rahmenformaten bzw. Ethernet-Frames

Dem Ethernet-Frame wird eine Präambel vorangestellt. Sie dient zur Synchronisation der Empfänger. Sie besteht aus einer Schwingung von 6,4 µs Länge. Es handelt sich dabei um eine Folge von 1010..., auf einer Länge von 8 Byte. Der Präambel folg Start Frame Delimiter (SFD). Es ist ein Bitfolge, die das Ethernet-Frame einleitet.
In einem Frame werden neben den Daten (Datenpakete aus den oberen Protokoll-Schichten) auch Zieladresse, Quelladresse und Steuerinformationen verpackt. Als Adressen dienen MAC-Adressen. Es handeln sich dabei um die Hardware-Adressen der Netzwerkadapter, die vom Hersteller vergeben werden. Für die MAC-Adressen stehen jeweils 6 Byte zur Verfügung. Die Steuerinformationen nehmen je nach Rahmenformat unterschiedlich viel Platz ein.

Das Ethernet-Frame muss eine Mindestlänge von 64 Byte haben. Wenn das Ethernet-Frame die erforderliche Minimalgröße von 64 Byte nicht erreicht, um genau zu sein, wenn die Nutzdaten weniger als 42 bzw. 46 Byte (mit bzw. ohne VLAN-Tag) betragen, dann muss der Rest aufgefüllt werden. Durch das PAD-Feld (Padding-Bits) wird das Ethernet-Frame auf die Minimalgröße gebracht. In der weiteren Betrachtung der verschiedenen Ethernet-Rahmenformate wird das PAD-Feld nicht berücksichtigt.

Das Ethernet-Frame endet mit der Frame Check Sequence (FCS). Es handelt sich dabei um eine 32-Bit-CRC-Prüfsumme. Sie wird über das gesamte Frame berechnet. Beginnend von der Ziel-MAC-Adresse bis zum PAD-Feld. Die Präambel und der SFD sind nicht in der Prüfsumme enthalten.

Nach dem Senden eines Frames erfolgt eine Pause von 9,6 µs. Diese Pause wird als Inter Frame GAP bezeichnet.

Ethernet II

Ethernet-Frame: min. 64 Byte / max.

Präambel SFD

1518 Byte

101010..

Zieladresse Quelladresse

8 Byte

6 Byte

6 Byte

Die klassische Frame-Struktur entspricht "Ethernet II". Das herausragende Merkmal ist das Typenfeld mit 2 Byte. Es kennzeichnet verschiedene Schicht 3 Protokolle. Andere Ethernet-Frames haben an dieser Stelle eine Längeninformation.

Ethernet 802.3 raw

Präambel

SFD

Ethernet-Frame: min. 64 Byte / max. 1518 Byte 101010.. 10101011
Zieladresse Quelladresse 8 Byte

6 Byte

6 Byte

"Ethernet 802.3 raw" ist das

Rahmenformat von Novell für IPX. Es

stammt noch aus der Zeit vor der

Normierung durch das IEEE. Es kann

ausschließlich IPX transportieren und

enthält deshalb auch keine Protokoll-

Kennung (Typenfeld).

Der Start Frame Delimiter (SFD) vor

dem eigentlichen Frame weist eine

Besonderheit auf. Sein letztes Bit ist

eine "1". Daran erkennt man, dass das Frame beginnt.

Dieses Rahmenformat erkennt man an

der Folge von Einsen nach dem

Längenfeld. Wäre dieses Feld nicht

vorhanden, dann würde man das

Längenfeld mit dem Typenfeld von

Ethernet II verwechseln.

Ethernet 802.3

Präambel

SFD

Ethernet-Frame: min. 64 Byte / max. 1518 Byte 101010.. 10101011 Zieladresse Quelladresse 8 Byte

6 Byte

6 Byte

"Ethernet-802.3"-Frames verzichten auf ein Typenfeld. Es folgen der Destination

Service Access Point (DSAP) und der

Source Service Access Point (SSAP).

Das Control-Feld enthält den Typ des

LLC-Frames.

Ethernet 802.3 SNAP

Präambel

SFD

Ethernet-Frame: min. 64 Byte / max. 1518 Byte 101010.. 10101011 Zieladresse Quelladresse 8 Byte

6 Byte

6 Byte

Dieses Ethernet-Frame hat als DSAP

und SSAP immer "0xAA" und im

Control-Feld immer "0x03". Vor dem Datenfeld wird ein zusätzliches Feld von

5 Byte hinzugefügt. Es wird als SNAP

bezeichnet. Das ist die Abkürzung für

Subnetwork Access Protocol. Die 5

Byte enthalten in 3 Byte den

Organizationally Unique Identifier (OUI)

des Herstellers und in den folgenden 2

Byte die Protokollnummer (Typenfeld).

Ethernet II tagged

Ethernet-Frame: min. 68 Byte / max. 1522

Präambel SFD

Byte

101010..

Zieladresse Quelladresse

8 Byte

6 Byte

6 Byte

Ethernet 802.3 tagged

Präambel

SFD

Ethernet-Frame: min. 68 Byte / max. 1522 Byte 101010.. 10101011 Zieladresse Quelladresse 8 Byte

6 Byte

6 Byte

Tagged-Frames enthalten nach der Quelladresse eine Kennzeichnung, die man als Tag bzw. VLAN-Tag bezeichnet. Dahinter steckt die Möglichkeit bestimmte Frames einem VLAN zuzuordnen. Das Ziel von VLANs ist, die Trennung von logischer und physikalischer Netzwerkstruktur. Anhand des Tags erkennen die Stationen auf dem Weg zum Empfänger, zu welchem VLAN das Frame gehört. VLANs werden nach IEEE 802.1q gebildet.

MAC-Adresse

In jedem Ethernet-Frame (Datenpaket) befinden sich auch die Adressen für Sender (Quelle) und Empfänger (Ziel). Die Adressen sollen die beiden Stationen eindeutig identifizieren. Sie werden als MAC-Adressen, Hardware-Adressen, Ethernet-Adressen oder

physikalische Adresse bezeichnet.
Die unterschiedlichen Bezeichnungen kommen daher, weil die MAC-Adresse den physikalischen Anschluss bzw. der Netzzugriffspunkt einer Station 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 vergeben werden. Jede Netzwerkkarte besitzt eine eigene, individuelle MAC-Adresse. Sie wird einmalig hardwareseitig vom Hersteller konfiguriert und lässt sich im Regelfall nicht verändern.
Beim Empfang eines Datenpakets vergleicht die Empfangseinheit der Netzwerk-Station die MAC-Zieladresse mit der eigenen MAC-Adresse. Erst wenn die Adressen übereinstimmen,

reicht die Empfangseinheit den Inhalt des Datenpakets an die höherliegende Schicht weiter. Wenn keine Übereinstimmung vorliegt, dann wird das Datenpaket verworfen.

Format einer MAC-Adresse

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

I/G U/L

OUI

OUA

1. Bit 2. Bit 3. - 24. Bit 25. - 48. Bit

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.

Die Bitfolge vom 25. bis zum 48. Bit

wird vom Hersteller vergeben. Man bezeichnet diese Bitfolge als Organizationally Unique Address (OUA).

Insgesamt stehen 7 bis 13 individuelle und eindeutige MAC-Adressen zur Verfügung.

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.

Beispiel für eine Umformung: 00110101

-> 10101100 = [1010][1100] = AC hex

Kanonische

Bitfolge

Form

00110101

01111011

Beispiel 00010010

AC-DE-48-

1

00000000

00-00-80

00000000

00000001

01001000

00101100

Beispiel 01101010

12-34-56-

2

00011110

78-9A-BC

01011001

00111101

MAC-Multicast- und MAC-Broadcast-Adressen

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

Kanonische Form	**Bitmuster**
Broadcast-	11111111 11111111 11111111

FF-FF-FF-

Adresse

11111111

FF-FF-FF

11111111

11111111

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.

Ethernet-

Standards

IEEE 802.3 umfasst eine ganze Reihe von Techniken, die einzeln standardisiert sind. Ihre Bezeichnungen ergeben sich aus:

{Datenrate}{Übertragungsverfahren}

{Segmentlänge oder Kabeltyp}

10Base5

10Base2

10Base-T

10Base-FL

100Base-T

100Base-TX

1000Base-T

1000Base-FX

...

Wie so häufig wurde nicht jeder Ethernet-Standard in eine fertiges Produkt umgesetzt. Aus diesem Grund ist diese Liste hier nicht vollständig. In der weiteren Beschreibung werden nur die wichtigsten und kommerziell erfolgreichen Ethernet-Standards erläutert.

10Base5 / Thick Ethernet / Yellow-Cable

Übertragungsgeschwindigkeit: 10 MBit/s

Physikalische Struktur: Bus

Maximale Länge eines Segmentes:

500 m

Maximal 100 Stationen pro

Segment

Mindestabstand zwischen zwei

Stationen: 2,5 m

Netzwerkkabel: Koaxialkabel

10Base5 ist eine Methode, Ethernet mit einer Bandbreite von 10 MBit/s über ein dickes Koaxial-Kabel (RG-8A/U) zu betreiben (Thick Ethernet). Die maximale Kabellänge eines Segments beträgt 500 Meter. Die beiden Kabelenden müssen mit Endwiderständen von 50 Ohm abgeschlossen werden. Pro Segment dürfen 100 Endgeräte angeschlossen werden. Die Transceiver in den Stationen müssen einen Mindestabstand von 2,5 m einhalten. Die jeweiligen Stichleitungen dürfen dabei nicht länger als 50 Meter lang sein.

10Base2 / Thin Ethernet /

Cheepernet

Übertragungsgeschwindigkeit: 10

MBit/s

Physikalische Struktur: Bus-

Topologie

Maximale Länge eines Segmentes:

185 m

Maximal 30 Stationen pro Segment

Netzwerkkabel: Koaxialkabel

10Base2 ist eine preisgünstige Ethernet-Variante (Thin Ethernet) mit einer Bandbreite von 10 MBit/s, die über ein dünnes Koaxialkabel (RG-58) betrieben wird. Die maximale Kabellänge eines Segments beträgt 185 Meter. Die beiden Kabelenden müssen mit Endwiderständen von 50 Ohm abgeschlossen werden. Das Netzwerkkabel wird direkt von Workstation zu Workstation geführt. Die Abzweigungen werden mit T-Stücken

(BNC) realisiert. Stichleitungen von der Netzwerkkarte zum Kabelstrang sind nicht zulässig. Das nachträgliche Anfügen zusätzlicher Workstations erfordert die kurzzeitige Unterbrechung des Netzwerks. Pro Segment können maximal 30 Geräte angeschlossen werden.

10Base-T / Ethernet / IEEE 802.3i

Übertragungsgeschwindigkeit: 10 MBit/s

Physikalische Struktur: Stern-Topologie

Maximale Kabellänge: 100 m

Netzwerkkabel: Twisted Pair der Kategorie 3

10Base-T ist ein Ethernet-Netzwerk in dem die Stationen über Twisted-Pair-Kabel stern- oder baumförmig an einem Hub oder Switch angeschlossen sind. Über ein Crossover-Kabel ist es

möglich, zwei Stationen oder Hubs direkt miteinander zu verbinden. Bei mehr als zwei Stationen ist jedoch zwingend ein Hub notwendig. Die maximale Kabellänge zwischen Station und Hub beträgt maximal 100 Meter. Als Anschlusstechnik kommt die RJ45-Technik zum Einsatz. Das sind breite 8-polige Western-Stecker, von denen aber nur 4 Pole verwendet werden.

Mit der Einführung von 10Base-T war es erstmals möglich, strukturierte Gebäudeverkabelungen auf der Basis von symmetrischen Kupferkabeln aufzubauen. Letztlich gab die Einführung von 10Base-T dem Ethernet über Koaxialkabel den Todesstoß. 10Base-T hat den Vorteil, dass sowohl Installation und Betrieb einfach sind und es keinerlei Probleme bereitet, Stationen in das Netz einzufügen oder wieder herauszunehmen. Auch der Ausfall einer einzelnen Station

hat keinen Einfluss auf den Betrieb des Netzwerks.

FOIRL und 10Base-FL

FOIRL (Fiber Optic Inter-Repeater Link) ist eine Methode, um Ethernet-Repeater mit 10 MBit/s über Glasfaserkabel zu verbinden. Dabei nutzt man die Vorteile der Glasfaser hinsichtlich Störanfälligkeit und EMV. FOIRL wurde offiziell von 10Base-FL abgelöst.

10Base-FL definiert Ethernet mit 10 MBit/s über eine sternförmige Glasfaserverkabelung mit zentralem Hub. Die maximale Länge des Kabels beträgt bei Multimode-Glasfaser mit einer Wellenlänge von 850 nm bis zu 2 km, bei einer Wellenlänge von 1300 nm bis zu 5 km und mit Monomode-Glasfaser bei einer Wellenlänge von 1300 nm bis zu 20 km. Die maximale Länge von FOIRL betrug nur 1 km.

100Base-T

100Base-T ist die allgemeine Bezeichnung für Ethernet mit 100 MBit/s. Die Stationen sind sternförmig über Twisted-Pair-Kabel an einen zentralen Switch angeschlossen. Die maximale Länge der Kabelverbindung beträgt 100 Meter (Kabellänge + Patchkabel).

100Base-TX / Fast Ethernet / IEEE 802.3u

Übertragungsgeschwindigkeit: 100 MBit/s

Physikalische Struktur: Stern-Topologie

Maximale Kabellänge: 100 m

Netzwerkkabel: Twisted-Pair-Kabel der Kategorie 5

100Base-TX ist die konsequente Weiterentwicklung von 10Base-T und umfasst dessen Eigenschaften mit der Möglichkeit einer

Übertragungsgeschwindigkeit von 100 MBit/s.

Gelegentlich wird fälschlicherweise die Bezeichnung 100Base-T statt 100Base-TX (mit X) verwendet und dabei unterschlagen, dass es noch weitere 100Base-T-Standards gibt. Die waren allerdings nicht ganz so erfolgreich, wie 100Base-TX.

100Base-T4

100Base-T4 ermöglicht Ethernet mit einer Bandbreite von 100 MBit/s über UTP-Kabel der Kategorie 3 zu betreiben. Der Unterschied zur normalen Ethernet-Verkabelung ist, dass alle 4 Adernpaare verwendet werden.

100Base-FX und 100Base-SX / IEEE 802.3u

100Base-FX ist eine Ethernet-Variante mit 100 MBit/s über Multimode- und Monomode-Glasfaserkabel. Diese Methode ist ähnlich wie FDDI

spezifiziert.

100Base-SX entspricht 100Base-FX mit einer Wellenlänge von 850 nm bei einer maximalen Kabellänge von 300 m. Die Komponenten dieser Technik sind wesentlich billiger als die von 100Base-FX.

1000Base-SX und 1000Base-LX / IEEE 802.3z

Ethernet mit 1000 MBit/s über Multimode- oder Monomode-Glasfaser bei einer Wellenlänge von 850 nm. Die maximale Kabellänge beträgt zwischen 220 und 550 m zwischen Verteiler und Station.

Ethernet mit 1000 MBit/s über Multimode- oder Monomode-Glasfaser bei einer Wellenlänge von 1270 (1300) nm. Die maximale Kabellänge liegt bei 550 und 5000 m zwischen Verteiler und Station.

1000Base-T / IEEE 802.3ab

Gigabit Ethernet mit 1000 MBit/s

Twisted-Pair-Kabel

Leitungslänge von max. 100 m

Stern-Topologie

1000Base-T setzt auf 100Base-T4 auf. Für die Übertragung werden alle 4 Adernpaare der Twisted-Pair-Kupferkabel genutzt. Die 1000 MBit/s werden auf die 4 Adernpaare zu je 250 MBit/s aufgeteilt.

Obwohl 1000Base-T nicht durchgängig bei der Arbeitsplatz-Vernetzung eingesetzt wird, 100 MBit/s reicht vollkommen aus, bauen die Neuinstallationen strukturierter Verkabelungen auf diesen Standard auf.

Ethernet-Standards im Überblick

Ethernet-Standard	**Bezeichnung**	**Jahr**	**Datenrate**
802.3	10Base5		

1983 10 MBit/s

802.3a

10Base2

1988 10 MBit/s

802.3i

10Base-T

1990 10 MBit/s

802.3j

10Base-FL

1992 10 MBit/s

100

802.3u

100Base-TX 1995 MBit/s

100Base-FX

100

802.3u

1995

100Base-SX

MBit/s

1000Base-

SX

802.3z

1998 1 GBit/s

1000Base-

LX

802.3ab

1000Base-T 1999 1 GBit/s

10GBase-SR

10GBase-

SW

10GBase-LR

10GBase-

802.3ae

LW

2002 10 GBit/s

10GBase-ER

10GBase-

EW

10GBase-

LX4

802.3an

10GBase-T

2006 10 GBit/s

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.

Übertragungstechnik

Fast-Ethernet ist die Weiterentwicklung des Ethernet-Standards 10Base-T, um über Twisted-Pair-Kabel 100 MBit/s zu übertragen. Durch den Leitungscode 4B5B wird die Übertragungsrate von 10 MBit/s auf 100 MBit/s angehoben. Dabei werden 4 Bit binäre Dateninformationen in 5 Bit binäre Übertragungsinformationen codiert. Die

Reichweite ist wie bei 10Base-T auf 100 Meter beschränkt.

IEEE 802.3x / Flow Control

Weil Fast-Ethernet in der Regel im Vollduplex-Modus arbeitet und damit auf CSMA/CD verzichtet, ist eine zusätzliche Flusskontrolle erforderlich. Der Grund: Wenn eine Ethernet-Station zu viele Datenpakete bekommt, dann besteht die Gefahr, dass die Datenpakete teilweise verworfen werden. Mit einer Flusskontrolle kann die Station der Gegenstelle signalisieren, eine Sendepause einzulegen. Die betroffene Station 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 Stationen mitteilen, dass sie mit einer geringeren Übertragungsrate senden sollen. Wenn die Stationen sich daran halten, dann verwirft der Switch auch weniger Datenpakete. So wird verhindert, dass das Netzwerk mit wiederholt gesendeten Datenpaketen überflutet wird.

Auto-Negotiation

Mit Auto-Negotiation können Datenendgeräte automatisch die Ethernet-Variante der Station am anderen Ende des Kabels 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 10Base-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 /

1GBase-T /

1000Base-T /

IEEE 802.3z /

IEEE 802.3ab

Gigabit-Ethernet gehört zu einer Familie von Netzwerktechniken, die vorwiegend

in lokalen Netzwerken zum Einsatz kommen. Aber auch für die Verbindung großer Netzwerke ist Ethernet 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 an ein Netzwerk anbinden 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. Server und Switches mit mehr Bandbreite zu verbinden, als es bei den übrigen Stationen üblich ist.

IEEE 802.3z / Gigabit Ethernet auf Glasfaser und Twinax-Kabel

1000Base-SX: Glasfaser mit einer Wellenlänge von 850 nm (Singlemode- oder Multimode-Glasfaser)

1000Base-LX: Glasfaser mit einer Wellenlänge von 1300 nm (Singlemode- oder Multimode-Glasfaser)

1000Base-CX: Twinax-Kabel bis maximal 25 Meter (Übergangslösung)

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 einfach so 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 den Steckern und Buchsen der RJ-45-Verbindungstechnik 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-Kabeln 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 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.

Übertragungstechnik von

1000Base-T

1 GBit/s auf Twisted-Pair-Kabel der Kategorie 5 (CAT5) zu erreichen, ist eigentlich ein Ding der Unmöglichkeit. Vor allem dann, wenn man die üblichen Distanzen bis zu 100 Meter überbrücken will. Das liegt daran, weil CAT5-Kabel nur für eine Übertragungsfrequenz bis 100 MHz ausgelegt sind. Was vor der Gigabit-Ethernet-Zeit mit üblicher Technik einer Übertragungsgeschwindigkeit von 100 MBit/s entsprach. Eine Übertragungsgeschwindigkeit über 1 GBit/s auf Twisted-Pair-Kabel ist deshalb nur mit ausgeklügelten Tricks möglich.

Das Entwicklungsziel von 1000Base-T war von Anfang an die Reduzierung der Übertragungsrate. Als erstes verzichtete man auf die übliche 8B/10B-Kodierung,

wodurch sich die Bitrate von 1.250 MBit/s (brutto) auf 1.000 MBit/s (netto) reduzierte. Die Übertragungstechnik nutzt alle vier Adernpaare des Twisted-Pair-Kabels. Bereits bei VG-AnyLAN und 100Base-T4 (Fast Ethernet über TP-Kabel der Kategorie 3) kam diese Technik zum Einsatz. Die üblichen Ethernet-Standards, wie 10Base-T und 100Base-T, nutzen ausschließlich zwei Adernpaare. Pro Adernpaar wird nur noch 250 MBit/s bzw. 250 MHz übertragen. Um die Übertragungsfrequenz noch weiter drücken zu können, setzt man auf eine Fünf-Level-Kodierung von PAM5. Statt der üblichen zwei (0 und 1) oder drei (-1, 0, +1) logischen Zustände, werden fünf (-1V, -0,5V, 0V, +0,5V, +1V) logische Zustände übertragen.
Durch die PAM5-Kodierung reduziert sich die Baudrate pro Adernpaar auf 125

MBit/s (bei 100 MHz). Das entspricht der Baudrate von Fast-Ethernet.
Damit der Vollduplex-Modus möglich ist, wird Echo Cancelation (Echo-Kompensation) eingesetzt, um Empfangssignal vom Sendesignal, dass auf dem gleichen Adernpaar gesendet wird, trennen zu können.

10-Gigabit-

Ethernet /

10GBase-T / 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) ablösen. 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 Probleme zu bekommen.

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 dadurch reduziert.

IEEE 802.3ae / 10-Gigabit-Ethernet über Glasfaserkabel

10GBase-LX4: Multimode- oder Singlemode-Glasfaser (300 m und 2 km) mit einer Wellenlänge von 1310 nm

10GBase-SR: Multimode-Glasfaser (bis 300 m) mit einer Wellenlänge von 850 nm

10GBase-LR: Singlemode-Glasfaser (bis 10 km) mit einer Wellenlänge von 1310 nm

10GBase-ER: Singlemode-Glasfaser (bis 40 km) mit einer Wellenlänge von 1550 nm

IEEE 802.3ak / 10-Gigabit-Ethernet über Twinax-Kabel

10GBase-CX4: 10 Gigabit über 8 Twinax-Paare auf 15 Meter (Verbindung für Switches)

IEEE 802.3an / 10-Gigabit-Ethernet über Twisted-Pair-Kupferkabel

10GBase-T: 10 Gigabit über CAT7- und CAT6a-Kabel

Übertragungstechnik von 10GBase-T

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- und CAT7-Kabel. Mit Abstrichen in der Reichweite auch CAT6e und CAT5e.
Um 10 GBit/s möglich zu machen, werden mit verbesserten Kodierverfahren mehr Zustände (Symbole) pro Übertragungsschritt übertragen. Mit ähnlichen Verfahren arbeiten bereits analoge Modems. Statt einfache binäre Verfahren, wird über viele Amplitudenwerten mehrere Bit pro Übertragungsschritt transportiert.
10GBase-T setzt auf PAM16, eine Puls Amplituden Modulation mit 16 Stufen. Sie bilden 4 Bit in einem Übertragungsschritt ab. Doch dieses und vergleichbare Verfahren haben ihre Grenzen. Mit zunehmender Anzahl der Bit pro Übertragungsschritt steigt die Anfälligkeit gegenüber Störungen.

Übersprechen am nahen Ende
(NEXT: Near End Crosstalk)
Übersprechen am entfernten Ende
(FEXT: Far End Crosstalk)
Übersprechen von benachbarten
Kabeln (AXTLK: Alien Crosstalk)
Der maximal erreichbare
Übertragungsgeschwindigkeit hängt vom
Signal/Rausch-Abstand ab. Deshalb
arbeitet man daran, die Störungen zu
eliminieren. Typischerweise wird mit
mathematischen Funktionen und
Algorithmen versucht typische
Störungsmuster zu erkennen und heraus
zu filtern. Die notwendige
Rechenleistung ist jedoch sehr hoch.
Weil das Übertragungsverfahren an das
Kabel angepasst werden muss, wird
nach dem physikalischen
Zusammenschalten zweier Stationen der
Übertragungsstrecke ausgemessen. Das
bedeutet, vor der Datenübertragung

gehen die Endstellen an den beiden Kabelenden in einen Trainingsmodus über. Danach stellen sie die Sendeleistung ein und parametrieren ihre Empfänger. Die Bedingungen für die Datenübertragung sind von der Kabellänge, der Kabelqualität, der Behandlung beim Verlegen und vielen anderen Parametern abhängig.

Kabelinstallation für 10GBase-T

Kategorie	**Grenzfrequenz**	**Reichweite**	**Anmerkung**
CAT5e	100 MHz	~ 22 m	nicht spezifiziert
CAT6	250 MHz	?	nicht
CAT6e	500 MHz		

~ 55 m

spezifiziert

CAT6a

625 MHz

100 m

CAT7

600 MHz

100 m

Einfach nur Cat-6a- oder Cat-7-Kabel zu verwenden, reicht für 10GBase-T nicht aus. Erschwerend kommt hinzu, dass auch die Bedingungen bei der Kabelinstallation eine große Rolle spielen. Hinzu kommen Maßnahmen, die sich durch die gesamte Installation ziehen müssen.

Der Betrieb von 10GBase-T auf CAT5e und CAT6e ist möglich. Aber nur mit Abstrichen bei der Reichweite. Wie weit genau, ist aber nicht spezifiziert. Im Einzelfall muss man das immer ausprobieren und nachmessen.

Nicht nur Fast- und Gigabit-Ethernet leiden unter Kopplungseffekte und Übersprechen. Insbesondere 10GBase-T leidet darunter, wenn bei der Installation unsauber gearbeitet wurde. Bei 10GBase-T dürfen sich die Kabel nicht zu nahe kommen. Andernfalls tritt erhöhtes Nebensprechen auf. Das Zusammenbinden der Kabelstränge mit Kabelbindern muss unterbleiben, weil die Kabel zusammengepresst werden und sich zu nahe kommen. Sowohl beim Verlegen als auch bei der festen Installation muss der Biegeradius eingehalten werden. Denn in der Biegung des Kabels werden die Adern gestaucht und gezogen, wodurch sie ihre Lage verändern können. Die Vorgaben von 10GBase-T haben auch Einfluss auf die Stecker und Buchsen. Beides muss geschirmt sein und weit genug auseinanderliegen. Konkret bedeutet das,

dass die üblichen RJ45-Steckverbindungen nicht mehr verwendet werden dürfen. Bisher gibt es aber noch keinen Standard-Steckverbinder für 10GBase-T.
Bei großen weitflächigen Installationen werden durchgängig metallische Kabeltrassen (ohne Löcher und Schlitze) empfohlen. Pro Kabeltrasse ist eine maximale Füllmenge und ein dazugehöriges Erdungskonzept vorgeschrieben. Zusätzlich sind Abdeckungen vorgesehen.
Bei diesem Aufwand erkennt man schnell, dass 10GBase-T nicht für die Arbeitsplatz-Vernetzung taugt. Und bei der Vernetzung übergeordneter Netzwerk-Stationen kommt man vom Preis und der Leistung her in die Regionen, wo sich Glasfaserkabel lohnen.

40- und 100-

Gigabit-Ethernet /

IEEE 802.3ba

100-Gigabit-Ethernet (100GE) gehört zu einer Familie von Netzwerktechniken, die vorwiegend in lokalen Netzwerken zum Einsatz kommt. Ethernet eignet sich auch zur Verbindung großer Netzwerke. Der Standard IEEE 802.3ba umfasst 40-Gigabit- und 100-Gigabit-Ethernet. Auf dem Weg zum 100-Gigabit-Ethernet ist 40 Gigabit nur ein Zwischenschritt. Der Zwischenschritt war deshalb notwendig, weil 100 Gigabit anfangs als technisch zu anspruchsvoll galt. Zudem gab es keine physikalischen Schnittstellen (Steckverbindungen) für diese Geschwindigkeit. IEEE 802.3ba ist somit der erste Ethernet-Standard, in dem zwei Geschwindigkeitsstufen definiert sind.

Die 40-GBit-Technik ist bei optischen Weitverkehrsstrecken (WAN) seit

Jahren etabliert. Mit ihr konnte der unterschiedliche Bandbreitenbedarf 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.

Übersicht: 100-Gigabit-Ethernet-Standards

40GBase-KR4: kurze Strecken im Backplane (4 Leitungspaare) bis 1 Meter

40GBase-CR4: Twinax-Kabel mit 4 Adernpaare für 10 Meter

100GBase-CR10: Twinax-Kabel mit 10 Adernpaare für 10 Meter

40GBase-SR4: Multimode-Faser mit vier Faserpaaren (OM3 für 100 Meter, OM4 für 125 m Reichweite)

100GBase-SR10: Multimode-Faser mit 10 Faserpaaren (OM3 für 100 Meter, OM4 für 125 m Reichweite)

40GBase-LR4: Single-Mode-Faserpaare mit 4 Wellenlängen a 10 GBit/s bei 10 km

100GBase-SR10: Single-Mode-Faserpaare mit 4 Wellenlängen a 25 GBit/s bei 10 km

100GBase-ER4: Single-Mode-Faserpaare mit 4 Wellenlängen a 25 GBit/s bei 40 km

100-Gigabit-Ethernet über Kupferkabel?

Die Übertragung von 10 GBit/s über Kupfer galt schon als technisch sehr anspruchsvoll. Eine weitere Steigerung gilt als schwierig. 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 sei.

Das Problem: Die heutigen Chips mit einer 65-nm-Strukturbreite sind für die 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) /

IEEE 802.af /

IEEE 802.3at

Hinter Power-over-Ethernet stehen standardisierte Verfahren, um Netzwerk-Endgeräte über das Netzwerk-Kabel mit Strom zu versorgen. Dadurch sollen Steckernetzteile für die Stromversorgung zum Beispiel für Webcams und WLAN-Access-Points entfallen.

Die Stromversorgung von Endgeräten in der Netzwerktechnik liegen im Einflussbereich der Herstellern der Endgeräte. Die lösen die Stromversorgung von Geräten mit geringen Leistungen meist über Steckernetzteile. Das bedeutete, neben jeder Netzwerkdose muss auch eine 230V-Steckdose sitzen. Mit Power-over-Ethernet (PoE) entfällt der separate Stromanschluss.

Für Power-over-Ethernet

gibt es zwei Standards:

PoE-

Leistung

nutzbare

Standard

pro Port

Leistung

IEEE

PoE

15,4 Watt

12,95 Watt

802.3af

IEEE

PoE+

60 Watt

ca. 50 Watt

802.3at

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 Twisted-Pair-Kabel sich 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

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 belegten Adern für die Datenübertragung 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 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.

Leistungsklassen von IEEE 802.3af

Der Standard IEEE 802.3af beschreibt einen Verbraucher, das Powered Device

(PD) und den Stromversorger, das

Power Source Equipment (PSE).

Max.

Klasse Typ

Klassifikationsstrom Speiseleistung

(PSE)

0

default

0 - 5 mA

1

optional

8 - 13 mA

2

optional

16 - 21 mA

3

optional

25 - 31 mA

4

reserviert

35 - 45 mA

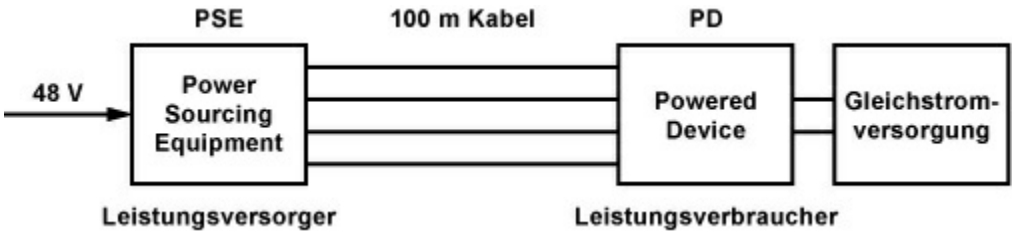
IEEE 802.at - Power-over-

Ethernet-Plus

Mit IEEE 802.at eignet sich Power-over-Ethernet auch für 1000Base-T. Hier werden alle vier Adernpaare für die Energieversorgung genutzt. IEEE 802.at verspricht eine Leistung bis 60 Watt pro Port. Dabei wird die Minimalspannung von 44 auf 50 Volt erhöht. Der maximale Strom wurde von 350 mA auf 720 mA erhöht. Bei diesen hohen Leistungen wird ein Cat5e/6-Kabel empfohlen. Das hat einen geringeren Widerstand.
Die 60 Watt Leistung steht dem Endgerät nicht direkt zur Verfügung. Man muss von den 60 Watt 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 50 Watt entspricht.
Für PoE+ gibt es momentan kaum

sinnvolle Anwendungen. Den meisten PoE-Geräten reichen 10 oder 100 MBit vollkommen aus. Viel interessanter ist die höhere Leistung bis ca. 60 Watt.

Varianten der Energieeinspeisung



Der Standard IEEE 802.3af beschreibt einen Verbraucher, das Powered Device (PD). Der Stromversorger ist das Power Source Equipment (PSE). Dabei handelt sich in der Regel um einen PoE-Switch, der auch für die Stromversorgung zuständig ist (Endspan-Verfahren).
Bis alle eingesetzten Switches und Hubs über PoE verfügen muss man noch auf eine Bastellösung zurückgreifen. Bei einzelnen Komponenten, die über Power-over-Ethernet mit Strom versorgt

werden können, tut es ein einfacher Power Injektor, der im Leitungsnetz zwischen einem normalen Switch und der abgehenden Netzwerkleitung zum Endgerät geschaltet wird (Midspan-Verfahren).
Gibt es in einem Netzwerk mehrere Power-over-Ethernet-Endgeräte, dann ist ein Power Hub nötig, der beim Hub/Switch installiert sein sollte.
Weil die Polarität nicht festgelegt ist und bei einem Cross-over-Kabel wiederum vertauscht werden kann, erkennt eine Eingangsbeschaltung im Endgerät die Polarität.

Spare-Pairs-Verfahren

Das Spare-Pairs-Verfahren verwendet die beiden unbenutzten Adernpaare im Kabel (4/5 und 7/8) für die Stromversorgung. Dieses Verfahren kommt bei 100Base-TX und 10Base-T zur Anwendung. Strom und Daten sind

hierbei sauber getrennt.

Phantom-Speisung

Bei der Phantom-Speisung werden alle Adern des Netzwerkkabels verwendet. Phantom-Speisung bedeutet, dass der Strom für die Energieversorgung dem Datensignal überlagert wird.
An dieser Stelle unterscheiden sich die beiden Standards IEEE 802.3af und 802.3at. Während der Standard, der nur 10Base-T und 100Base-TX berücksichtigt, die beiden benutzten Adernpaare (1/2 und 3/6), müssen bei IEEE 802.3at für 1000Base-T (Gigabit Ethernet) alle vier Adernpaare für die Stromversorgung und die Datenübertragung genutzt werden. Hier ist man zwangsläufig auf die Phantom-Speisung angewiesen, bei der der Stromfluss die Datensignale überlagert. Das Power-Device muss die Entkopplung übernehmen, was

fehleranfällig, aufwendig und teuer ist.

Auch bei der Phantom-Speisung ist der Strom auf 175 mA pro Adernpaar begrenzt. Bei Gigabit-Ethernet erreicht man per Phantom-Speisung auf allen vier Paaren ca. 60 Watt.

PoE-Erkennung

Wird die Netzwerkverkabelung auch für andere Anwendungen, z. B. für Telefonie, genutzt, dann ist Vorsicht beim Einsatz von Power-over-Ethernet-Netzwerk-Komponenten geboten. Mit einem Schutz-Mechanismus sollten die Power-over-Ethernet-Netzwerkkomponenten vor dem Einschalten der PoE-Stromversorgung alle angeschlossenen Endgeräte auf PoE-Unterstützung überprüfen. Auf einen Anschluss sollte nur dann Spannung geschaltet werden, wenn dort auch ein Endgerät mit PoE-Unterstützung angeschlossen ist.

Um PoE-taugliche Endgeräte von untauglichen Endgeräten unterscheiden zu können, kommt im PoE-Versorger ein Verfahren mit dem Namen Resistive Power Directory zum Einsatz. Auf der Engeräteseite sind dazu nur passive Bauteile notwendig. Die Stromquelle prüft mit einer Messschaltung den Innenwiderstand des Verbrauchers. Liegt er zwischen 19 und 26,5 kOhm und hat eine Kapazität von maximal 10 µF wird die Energieversorgung aktiviert. In einer zweiten Erkennungsphase wird die Leistungsklasse ermittelt. Power-over-Ethernet-Endgeräte müssen in jedem Fall beide Verfahren zur Stromaufnahme beherrschen. Dem Kopplungselement mit PoE-Stromversorgung steht es frei, welches Verfahren es unterstützt. Die gleichzeitige Nutzung beider Verfahren ist jedoch untersagt.

Belegung des RJ45-Steckers

bei Power-over-Ethernet

Spare-Pair- Phantom-Speisung

Pin Speisung Midi-x Midi

1 RX+

Rx+ / **V-** Rx+ / **V+**

2 RX-

Rx- / **V-** Rx- / **V+**

3 TX+

Tx+ / **V+** Tx+ / **V-**

4 V+

-

-

5 V+

-

-

6 TX-

Tx- / **V+** Tx- / **V-**

7 V-

-

-

8 V-

-

-

VLAN - Virtual

Local Area

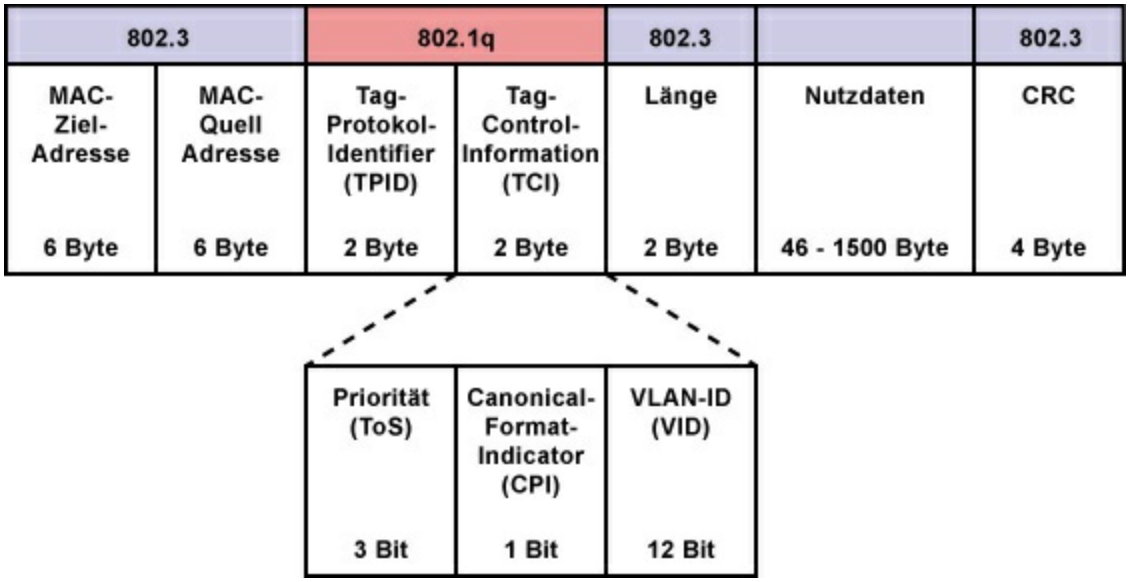
Network / IEEE

802.1q

VLANs sind virtuelle lokale Netze die in IEEE 802.1q standardisiert sind und auf der Schicht 2 des OSI-Schichtenmodells arbeiten. VLANs werden mit Switches realisiert, die auf der Schicht 3 arbeiten, also die Vorteile von Switching und Routing vereinen. Es gilt die Regel: Verbleibt der Netzwerkverkehr innerhalb eines VLANs, wird geswitcht, andernfalls wird in ein anderes VLAN geroutet. Wobei Switching schneller ist als Routing.

Ethernet-Frame nach IEEE

802.1q



Der Standard IEEE 802.1q sieht eine Veränderung von Ethernet-Frames vor. Insgesamt wird das Frame um 4 Byte verlängert und zusätzliche Informationen in den Header gepackt, die den Datenaustausch innerhalb des VLANs regeln (Tagging). Über das ToS-Feld (3 Bit) lässt sich zum Beispiel auch die Priorisierung bei der Beförderung des Frames festlegen. Die Veränderung wird von den Treibern des Netzwerk-Adapters vorgenommen und von netzübergreifenden VLAN-Switches ausgewertet.

Warum werden VLANs eingerichtet?

Neben Kollisionsdomänen gibt es auch Broadcastdomänen. Diese beziehen sich auf die Schicht 3 des OSI-Schichtenmodells und werden mit Subnetzen realisiert. Subnetze entstehen durch die Adressierung mit IP-Adressen und Subnetzmasken, die manuell oder von einem DHCP-Server an die Netzwerkstationen vergeben werden. Alle Stationen, die innerhalb eines Subnetzes liegen und nicht durch ein Gerät der Schicht 3 des OSI-Schichtenmodells getrennt sind, liegen innerhalb einer Broadcastdomäne. Die meisten modernen Ethernet-Netze basieren auf der Stern-Topologie und werden mit Switches realisiert. Diese Switches bilden an jedem ihrer Ports eine Kollisionsdomäne, indem sie den Datenverkehr nur an den Port

weiterleiten an dem sich die Ziel-MAC-Adresse befindet. Innerhalb einer Kollisionsdomäne befindet sich dann in der Regel eine einzelne Station, ein weiterer Switch oder ein Router in ein anderes Netz. Die Einrichtung von Kollisionsdomänen reduziert den Datenverlust, verursacht durch Kollisionen bei der Datenübertragung. Dieses wiederum reduziert den allgemeinen Netzwerkverkehr, der durch wiederholte Übertragungen verursacht wird. Von einem Subnetz in ein anderes Subnetz muss ein Datenpaket den Weg über einen Router gehen. Router arbeiten auf der Schicht 3 des OSI-Schichtenmodells. Mit Ihnen werden Kollisionsdomänen und Broadcastdomänen geschaffen. Broadcasts entstehen immer dann, wenn es für ein Datenpaket keinen bestimmten Empfänger gibt oder dessen Standort im

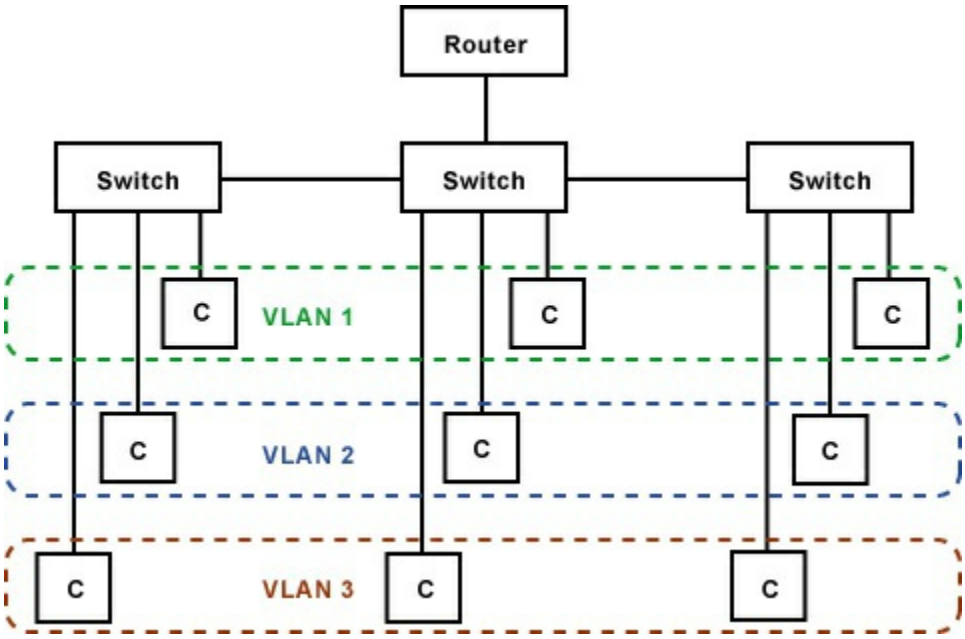
Netz unbekannt ist. Switches leiten in so einem Fall dieses Datenpaket an alle Ports weiter. Router verhindern die Weiterleitung von Broadcasts in ein anderes Subnetz.

Wie wird ein VLAN aufgebaut?

Router verhindern wirkungsvoll Broadcasts. Viele Router in einem lokalen Netz haben jedoch den Nachteil, dass sie sehr viel Netzwerkverkehr untereinander verursachen. Protokolle, die die Routing-Tabellen zwischen den Routern untereinander austauschen sorgen für viel Netzwerkverkehr und unnötige Fehlerquellen. Eine Lösung auf Basis von Switches hat Geschwindigkeitsvorteile gegenüber dem reinen IP-Routing. Deshalb werden Layer-3-Switches eingesetzt, die wie Router verschiedene Subnetze schaffen. Die Switches werden so konfiguriert,

dass ihre Ports nicht nur die MAC-Adresse kennen, sondern auf ein bestimmtes Subnetz, manchmal sogar auf eine bestimmte IP-Adresse konfiguriert sind. Dies führt zur Auflösung von physikalischen Strukturen, die durch den klassischen Switch gegeben sind. Doch größere Netze werden so schnell unübersichtlich und schwer zu administrieren.

Beispiel-Architektur eines lokalen Netzwerkes mit VLANs



Obwohl die Clients der VLANs 1, 2 und

3 an unterschiedlichen Switches angeschlossen sind, sind sie für unterschiedliche Subnetze adressiert.
Die Layer-3-Switches achten anhand der Subnetze auf die gezielte Weiterleitung von Broadcasts. Muss ein Datenpaket das Subnetz wechseln, wird es automatisch in ein anderes VLAN geroutet und der richtigen Station zugeordnet.

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. Wireless Local Area Network (WLAN).
Seit 1997 gibt es mit IEEE 802.11 eine verbindliche Luftschnittstelle für drahtlose Netzwerke. Davor war der

breite Einsatz drahtloser Datennetze 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 ohne Einschränkungen möglich, eine schnurgebundene Ethernet-Verbindung nach IEEE 802.3 gegen eine Wireless-LAN-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 (Wirless 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.

Im allgemeinen Sprachgebrauch hat es

sich durchgesetzt ein lokales

Funknetzwerk, dass auf dem Standard

"IEEE 802.11" basiert als Wireless LAN bzw. WLAN zu bezeichnen.

Übersicht:

Übertragungsgeschwindigkeit

Standard

802.11 802.11b 802.11a/h/j

2,4

2,4

Frequenzbereich

5 GHz

GHz

GHz

Übertragungsrate 2

11

54 MBit/s

(brutto)

MBit/s MBit/s

Übertragungsrate 0,5 - 1 1 - 5

bis 32

(netto)

MBit/s MBit/s MBit/s

Schaut man sich die Angaben der Hersteller und Händler zur Übertragungsgeschwindigkeit ihrer Produkte an (brutto) und vergleicht die Werte, die man damit in der Praxis erreicht (netto), riecht das fast schon nach einem Reklamationsgrund.

Tatsache ist, die Bruttodatenraten, wie sie auf den Produktverpackungen angegeben sind, werden in der Praxis nie erreicht. Die Bruttodatenrate sind nur unter optimalen Bedingungen und mit einer kurzen Entfernung zu erreichen. Je nach Umgebungsbedingungen, Anzahl der teilnehmenden Stationen und deren Entfernung erreicht man nur einen Bruchteil der angegebenen Datenrate.

Die Differenz zwischen theoretischer

Übertragungsgeschwindigkeit und dem, was in der Praxis übrig bleibt, ist der Tatsache geschuldet, dass es sich bei Funk um einen geteilten Übertragungskanal handelt, den mehrere Teilnehmer gleichzeitig nutzen wollen und deshalb ein spezielles Zugriffsverfahren (CSMA/CA) den Zugriff aushandelt. Das regelt, wenn einer sendet, müssen die anderen warten. Anschließend fällt dann noch eine Pause an. Die Funkschnittstelle ist deshalb auch nie zu 100% belegt. Für jeden einzelnen Teilnehmer bedeutet das, es bleibt nur ein Bruchteil der theoretischen Übertragungsgeschwindigkeit übrig.

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 unterschiedliche 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-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 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

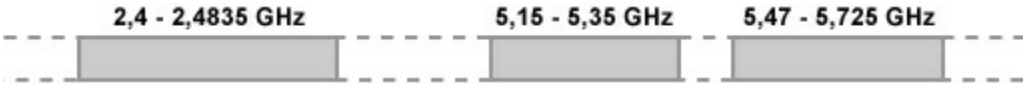
empfiehlt sich, gerichtliche Auseinandersetzungen im Voraus zu vermeiden. Deshalb sollte die Verschlüsselung immer aktiviert sein. Vorzugsweise WPA2. Die älteren Verschlüsselungsverfahren WPA und WEP sollte man nicht mehr verwenden. WLAN-Geräte, die WPA2 nicht beherrschen, sollte man dringend austauschen.

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.

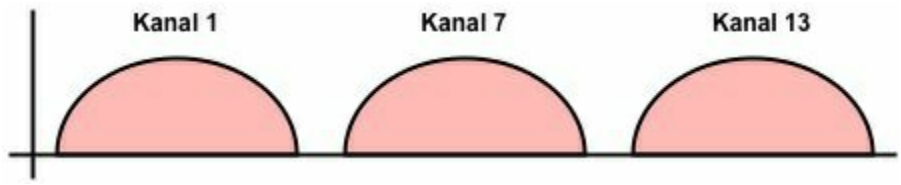


WLAN-Frequenzen

Für WLAN stehen zwei Frequenzbereiche zur Verfügung. Der eine Bereich liegt bei 2,4 GHz, der andere bei 5 GHz. Beide 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 beliebige Funktechniken tummeln. Insbesondere das ISM-Frequenzband (Industrial, Scientific, Medicine) um 2,4 GHz wird für Anwendungen in Industrie, Wissenschaft und Medizin intensiv genutzt.

In diesem Frequenzspektrum um 2,4 GHz konkurrieren viele Standards und proprietäre Funktechniken der unterschiedlichsten Hersteller und Anwendungen. Unglücklicherweise auch Geräte des täglichen Gebrauchs, z. B. Mikrowellenherde, Funkfernbedienungen und AV-Funksysteme. Die Realisierbarkeit eines Funknetzwerks mit IEEE 802.11 hängt also maßgeblich von der Nutzung anderer Funktechniken in diesem Frequenzspektrum ab.



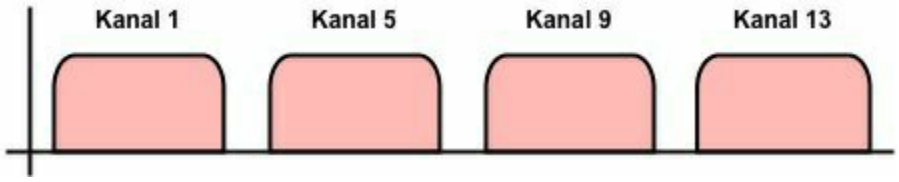
WLAN-Kanäle bei IEEE

802.11b (2,4 GHz, 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



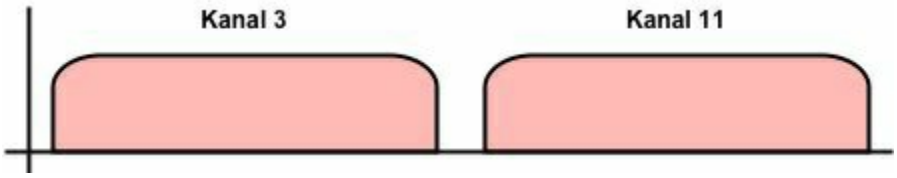
802.11g und 802.11n (2,4

GHz, 20 MHz Kanalbreite)

Bei einem WLAN mit IEEE 802.11g oder 802.11n empfiehlt es sich, die Kanäle 1, 5, 9 oder 13 einzustellen. Bei einer Kanalbreite von 20 MHz (OFDM)

und 16,25 MHz pro Träger wäre das Frequenzspektrum um 2,4 GHz optimal ausgenutzt.

Leider 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.



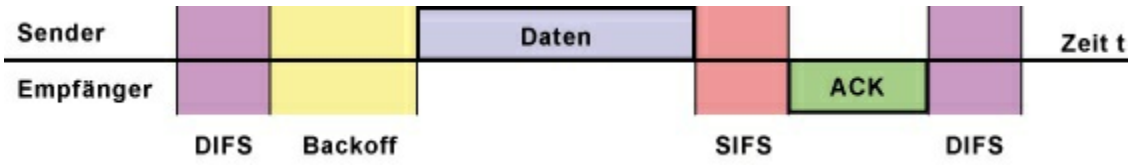
Weil Geräte nach IEEE 802.11b nahezu ausgestorben sein dürften gibt es keinen Grund mehr die Kanalaufteilung 1-7-13 zu nutzen.

WLAN-Kanäle bei IEEE 802.11n (2,4 GHz, 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 oder 11 einzustellen.

Bei einer Kanalbreite von 20 MHz

(OFDM) und 16,25 MHz pro Träger empfiehlt es sich die Kanäle 1, 5, 9 oder 13 einzustellen. In beiden Fällen erreicht man die optimale Ausnutzung des Frequenzspektrums um 2,4 GHz. In der Praxis vermeidet man es, ein WLAN mit IEEE 802.11n bei 2,4 GHz mit einer Kanalbreite von einzurichten. Dabei wäre das Frequenzspektrum mit 2 WLANs voll belegt. Damit auch WLANs mit IEEE 802.11g parallel betrieben werden können, werden WLANs mit IEEE 802.11n in der Regel auch mit 20 MHz Kanalbreite eingerichtet.



CSMA/CA -

Carrier Sense

Multible

Access/Collision

Avoidance

Das WLAN-Übertragungsmedium ist mit dem früheren Koax-Ethernet vergleichbar. Alle Stationen teilen sich das Übertragungsmedium und es kann nur eine Station senden. Wer wann senden darf, wird über das Zugriffsverfahren CSMA/CA geregelt. CSMA (Carrier Sense Multiple Access) ist ein Mehrfachzugriffsverfahren. Es sieht vor, dass jede Station vor dem Senden prüfen muss, ob das Medium frei ist. Erst dann ist die Übertragung erlaubt. Das schließt natürlich nicht aus, dass zwei Stationen das Medium als frei erkennen und gleichzeitig senden. Dann tritt eine Kollision auf. Dabei überlagern sich die Signale. Die Daten sind unbrauchbar. Beim Kabel-Ethernet können die Stationen mit CSMA/CD (Carrier Sense Multiple Access/Collision Detection) die

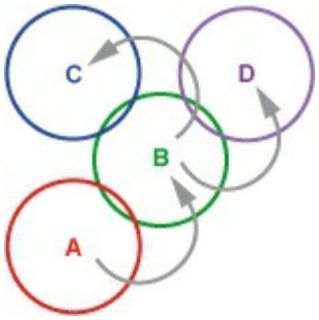
Kollision schon während der Übertragung erkennen, den Vorgang abbrechen und nach einer zufälligen Wartezeit einen erneuten Versuch starten. Beim Funk reicht das nicht aus. Mit 802.11 wurde deshalb ein Bestätigungspaket (ACK) eingeführt. Das ACK-Paket wird genauso behandelt, wie ein normales Datenpaket. Es besteht aus dem 802.11-Header und dauert 24 µs. Das ACK-Paket wird nach einer kurzen Wartezeit (SIFS) zurückgeschickt. Erst danach gehen andere Datenpakete auf die Reise. Zwischen den Datenpaketen koordinieren unterschiedlich lange Wartezeiten den Zugriff auf das Funkmedium. Das DIFS (Distributed Coordination Function Interframe Space) kennzeichnet die Backoffzeit, in der eine Station das freie Funkmedium erkennen kann. Das SIFS (Short Interframe Space)

kennzeichnet das ACK-Paket. Das ist das Bestätigungspaket des Empfängers für den Sender. Nach dem ACK-Paket folgt wieder ein DIFS.

CSMA/CA DCF

Die Distributed Coordination Function (DCF) verteilt die Zugriffsregeln auf die Stationen. Im DCF benutzt das MAC-Protokoll CSMA/CA (Carrier Sense Multible Access/Collision Avoidance). Durch das Übertragungsverfahren ergeben sich bei Funknetzen besondere Schwierigkeiten. Eine drahtlose Sendestation kann bspw. keine Signalkollision feststellen. Das eigene Signal überdeckt die Signale der anderen Stationen. Kollisionen lassen sich in einem Funknetzwerken von Störungen nicht unterscheiden. Deshalb wird im Vergleich zu den drahtgebundenen Ethernet-Varianten (mit CSMA/CD) auf eine

Kollisionserkennung (Collision Detection, CD) verzichtet. Stattdessen wird eine Kollisionsvermeidung (Collision Avoidance, CA) eingesetzt. Bevor eine WLAN-Station sendet stellt sie sicher, dass der Empfänger zum Empfang bereit und das Übertragungsmedium frei ist. Dieses Vorgehen wird als Listening before Talking (LBT) bezeichnet. Zu Deutsch: Hören vor dem Sprechen.
Bevor also eine Wireless-Station sendet hört sie in das Medium hinein, in diesem Fall die Funkschnittstelle, ob gerade eine andere Station sendet. Ist die Funkschnittstelle belegt, wartet die Station eine zufällige Zeit ab und hört erneut in das Medium hinein. Ist das Medium frei, kann die Station mit der Übertragung beginnen, andernfalls wird die Station erneut eine zufällige Zeit warten.



CSMA/CA und RTS/CTS

Durch Um das Risiko der mehrmaligen Funkschnittstellen-Belegung und Sende-Kollisionen zu vermeiden, muss jede Station die Funkschnittstelle explizit reservieren, bevor sie belegt werden darf. Dazu wird das RTS/CTS-Verfahren angewendet.

Für die Kollisionsvermeidung gibt es in der MAC-Schicht einen Virtual-Collision-Detection-(VCD-)Modus, der die Rahmen Request-to-Send (RTS) und Clear-to-Send (CTS) enthält. Bevor irgendwelche Daten gesendet werden erfolgt folgender Ablauf:

1. Die WLAN-Station verlangt einen freien Kanal.
2. Die WLAN-Station identifiziert

einen freien Kanal.

3. Die WLAN-Station sendet ein RTS auf diesen Kanal.

4. Der Access Point (AP) sendet ein CTS.

5. Die WLAN-Station sendet die Daten.

6. Der Access Point (AP) sendet ein Acknowledgement (ACK) zur Empfangsbestätigung.

Der Sender A schickt nach dem Erkennen eines freien Kanals ein RTS-Signal an Empfänger B. Erkennt der Empfänger B den Kanal als frei, sendet er ein CTS-Signal. Dieses Signal hören alle Stationen, die mit der Funkzelle des Empfängers B Kontakt haben. Damit ist dieser Kanal für eine bestimmt Übertragungszeit von Sender A zu Empfänger B reserviert.

Das Acknowledgement (ACK), die Empfangsbestätigung nach der

Datenübertragung, ist ein weiterer Teil des CSMA/CA. Beim Eintreffen des Paketes sendet der Empfänger dem Sender eine Empfangsbestätigung. Bleibt diese beim Sender aus, schickt er das Paket noch einmal. Ohne ACK ist der Sender bevorrechtigt das Funkmedium nochmals zu nutzen. Kurzzeitige Störungen (Interferenzen) auf dem Funkmedium werden so umgangen, ohne das der Anwender etwas davon mitbekommt. Länger andauernde Störungen durch andere Funk-Anwendungen im selben Frequenzbereich lassen erst die Übertragungsrate sinken. Wenn die Störungen sich auch so nicht umgehen lassen, bricht das Funknetzwerk zusammen.

CSMA/CA PCF

In einem WLAN kann es vorkommen, dass sich nicht alle WLAN-Stationen

kennen. Dieses Problem nennt sich Hidden-Node oder Hidden-Terminal. Besonders problematisch ist der Fall, wenn sich mehrere Stationen außerhalb der Reichweite anderer Stationen befinden. Dabei kann es zum fälschlichen Erkennen eines freien Kanals kommen.

Die PCF (Point Coordination Function) in IEEE 802.11 ist eine weitere Zugriffsregelung des MAC-Layers. Die PCF unterstützt Quality of Service (QoS), das bestimmte Charakteristiken bei der Übertragung für bestimmte Kommunikationsanforderungen garantiert.

Für PCF ist ein Access Point erforderlich, der mittels einer Kanalreservierung die Senderechte an die mobilen Stationen vergeben kann. Dieser Vorgang wird als Polling bezeichnet. Dabei fragt der Access Point

die Stationen innerhalb seiner Zelle nacheinander ab, ob sie Daten versenden wollen. PCF ist deshalb optimal für die Abwicklung von zeitkritischem Datenverkehr geeignet. DCF und PCF lassen sich auch parallel zueinander einsetzen. PCF hat allerdings eine höhere Priorität.

Nachteile durch CSMA/CA

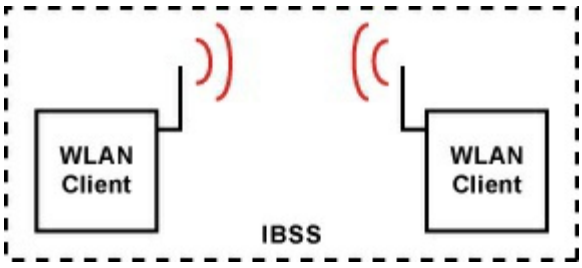
Die Sicherungsfunktionen, die durch CSMA/CA auf dem MAC-Schicht vorhanden sind, können in den oberen Protokoll-Schichten zu Problemen führen. Kommt es bereits auf dem MAC-Schicht zu Datenverlusten, verzögern sich die Datenpakete. Dies führt zu verlängerten Übertragungszeiten, die z. B. TCP/IP mit bestimmten Mechanismen zur Bestätigung von Datenpaketen durch den Empfänger erhöht. Dies führt zu erhöhtem Datenaufkommen durch die vermehrten Bestätigungsmeldungen.

Diese Schwierigkeiten sind häufig dafür verantwortlich, dass die Performance von drahtlosen Netzen deutlich unter der von drahtgebundenen Netzwerken liegt.

WLAN-Topologie

Die WLAN-Topologie besteht im wesentlichen aus den drahtlosen Netzteilnehmern, die als WLAN Clients bezeichnet werden, und den WLAN-Basisstationen, die als Access Point (AP) bezeichnet werden. Ein Access Point ist innerhalb eines Wireless LAN 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.

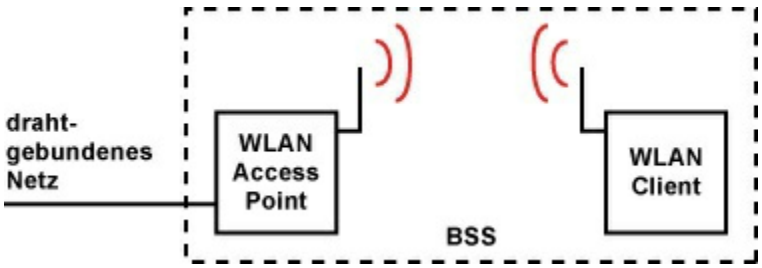
IBSS - Independent Basic Service Set

Schon mit zwei drahtlosen Stationen lässt sich ein einfaches Wireless LAN aufbauen. Bei der Einrichtung sind keine weiteren aktiven Elemente erforderlich. Die Stationen kommunizieren direkt über den WLAN-Adapter. In Notebooks ist das eine PCMCIA-Karte oder ein fest eingebauter WLAN-Adapter.
Die Topologie eines solchen Ad-hoc-Netzes nennt sich Independent Basic Service Set (IBSS). Jede Station bildet mit seiner Netzwerkkarte eine Funkzelle. Solange sich die Stationen in einer Zelle

befinden oder sich die Zellen überschneiden, ist eine Kommunikation zwischen den Stationen 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 Adhoc-Vernetzung ist mit Irda (Infrarot) oder Bluetooth schneller realisiert.

BSS - Basic Service Set

Ist die Reichweite einer Zelle zu gering,

lässt sie sich mit einem Access Point, kurz AP, erweitern. Doch nicht nur das. Der Access Point bildet auch den Übergang zum drahtgebundenen 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.

Die Topologie eines solchen Netzwerks mit Access Point nennt sich Basic Service Set (BSS).

Wird ein Access Point auf einen Kanal eingestellt, so versorgt er damit eine Funkzelle (räumliche Ausbreitung der Funksignale). Innerhalb der Funkzelle garantiert er eine festgelegte Übertragungsrate. Alle Funkteilnehmer in dieser Zelle, die auf dem selben

Kanal eingestellt sind, müssen sich diese Übertragungsrate teilen.
Rutscht ein Teilnehmer an den Rand der Funkzelle, wo die Übertragungsrate nicht mehr eingehalten werden kann, regelt der Access Point die Übertragungsrate herunter. Die neue Übertragungsrate gilt dann für alle anderen Teilnehmer auch. Egal ob sie sich näher am Access Point aufhalten oder nicht. Vor der Nutzung eines Access Points sollte seine Reichweite ausgiebig getestet werden, um die Randbereiche mit schlechtem Empfang herauszufinden.
Funkzellen, die QoS unterstützen werden als QBSS bezeichnet.

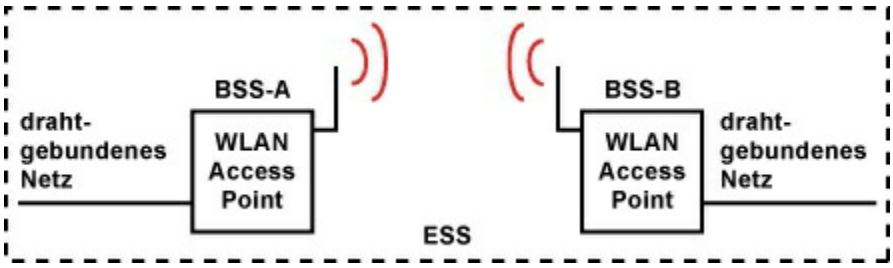
ESS - Extendet Service Set / IEEE 802.11c / Wireless Bridging

Mittels zweier Access Points lässt sich auch die Reichweite eines

kabelgebundenen Netzwerkes erhöhen.

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

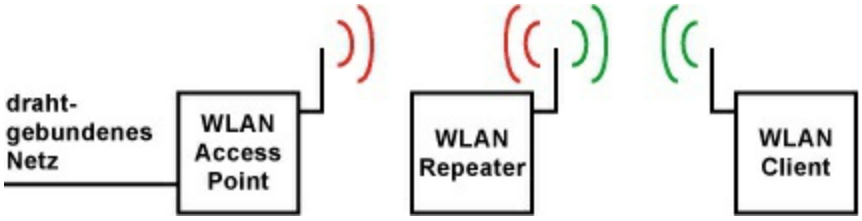


nicht erreicht werden können.

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.

Die Topologie eines solchen Netzwerks mit zwei Access Points nennt sich

Extendet Service Set (ESS). Es besteht aus zwei oder mehreren Basic Service Sets (BSS-A und BSS-B).
IEEE 802.11c ist der Standard zur drahtlosen Kopplung zweier Netzwerk-Topologien über WLAN. Im Bridging besteht zwischen zwei Access Points 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 ein Kabel.



WDS - Wireless

Distribution

System

WDS, neben Wireless Distribution System auch Wireless Distributed System genannt, bezeichnet die drahtlose Verbindung mehrerer Wireless Access Points untereinander.

Ein WDS ist eine WLAN-Basisstation, die schwache Funksignale empfangen, neu aufbereitet und verstärkt wieder abstrahlt. Im Prinzip handelt es sich dabei um eine Repeater-Funktion, die sich als Funkverlängerung eignet.

Da Access Point und Repeater die gleiche SSID haben, können sich die WLAN-Clients wahlweise mit der Funkzelle verbinden, deren Signal am stärksten ist.

WDS ist bereits im Basisstandard IEEE 802.11 definiert. Doch ist es etwas lasch definiert, so dass bei der Umsetzung große Freiheiten möglich sind. Sehr zum Nachteil der Kunden, die mit Geräten unterschiedlicher Hersteller, die nicht zusammenarbeiten, leben müssen. Damit man ein WDS einsetzen kann, muss der Repeater vom gleichen Hersteller wie der vom WLAN-Router sein. Nur so kann man Probleme ausschließen. Die WLAN-Access-Points kooperieren in der Regel nur zwischen den Geräten des gleichen Herstellers.

Reine WLAN-Repeater gibt es eher selten. Meist kann man einen einfachen Access Point als Repeater betreiben.

Prinzip-bedingte Probleme von Repeatern

Die Geräte senden ein Datenpaket auf dem selben Kanal, auf dem sie es empfangen haben. Das bedeutet, der

Übertragungskanal ist zweimal belegt. Somit reduziert sich die Datenrate auf mindestens die Hälfte. Kommen mehrere Repeater zum Einsatz, bricht die Datenrate noch stärker ein.
In der Praxis kann natürlich auch der umgekehrte Effekt eintreten. Denn zwei weit entfernte Stationen können nur eine Verbindung mit geringer Datenrate eingehen. Wenn ein Repeater dazwischengeschaltet ist, die Verbindung also verkürzt ist, dann geht auch die Datenrate deutlich nach oben.
Je nach örtlichen Begebenheiten und Platzierung des Repeaters steigert oder reduziert sich die Datenrate.

WDS und Verschlüsselung

Auch WDS sollte man verschlüsseln. Doch leider macht der Verschlüsselungsstandard IEEE 802.11i keine konkreten Vorgaben zur Umsetzung von WPA2 auf WDS.

Damit WPA2 funktioniert, braucht man eine Station, die sich um die Schlüsselverhandlung kümmert. Bei WDS gibt es allerdings keinen Chef. Alle Access Points agieren praktisch eigenständig. Die bei WPA2 übliche Aushandlung gibt es bei WDS-Verbindungen nicht.
Um dieses Problem zu umgehen, implementiert jeder Hersteller etwas anderes. Letztendlich sind dabei viele proprietäre Verfahren herausgekommen. In der Regel funktioniert die Verschlüsselung bei WDS herstellerübergreifend nur mit WEP. Um höchstmöglichste Sicherheit zu erreichen braucht man zwei Hersteller-gleiche Access Points mit WDS-Unterstützung, die eine eigene Verschlüsselungsverhandlung mitbringen.
Universal-Repeater lösen das

Verschlüsselungsproblem auf eine andere Art. Sie melden sich in Richtung Basisstation als Client an und weisen sich in Richtung den WLAN-Clients als Basisstation aus.

IEEE 802.11s / Wireless Mesh Network (WMN)

IEEE 802.11s ist ein Standard für ein WLAN Mesh Network (WMN) in dem WLAN-fähige Geräte für andere Geräte als Relaisstationen bis zum nächstgelegenen Access Point dienen. IEEE 802.11s regelt, wie WLAN-Stationen untereinander ein drahtloses Backbone aufbauen und Frames für die Stationen außerhalb der Funkzelle weiterleiten. Auf diese Weise wird die Reichweite einer Funkzelle vergrößert. Mesh-Network-fähige Endgeräte verbessern die Übertragungsrate und die Netzabdeckung der bestehenden Access-

Point-Infrastruktur. Zumindest theoretisch kann ein Mesh-WLAN einen allgegenwärtigen WLAN-Zugang möglich machen. Dazu ist nur ein einziger Access Point nötig, der eine Verbindung ins Internet haben muss.
Es gibt zwar schon im Basisstandard 802.11 das Wireless Distribution System (WDS), doch das lässt viele Fragen offen und funktioniert häufig nur mit den Geräten eines Chipsatz- oder Geräte-Herstellers. Mit IEEE 802.11s wird die drahtlose Vernetzung großer Flächen mit WLAN einfacher.
Der OLPC-Laptop (One Laptop per Child) ist die erste Implementierung von IEEE 802.11s für Mesh-Networking im großen Stil.

Merkmale von IEEE 802.11s

dynamisches Routing auf MAC-Ebene

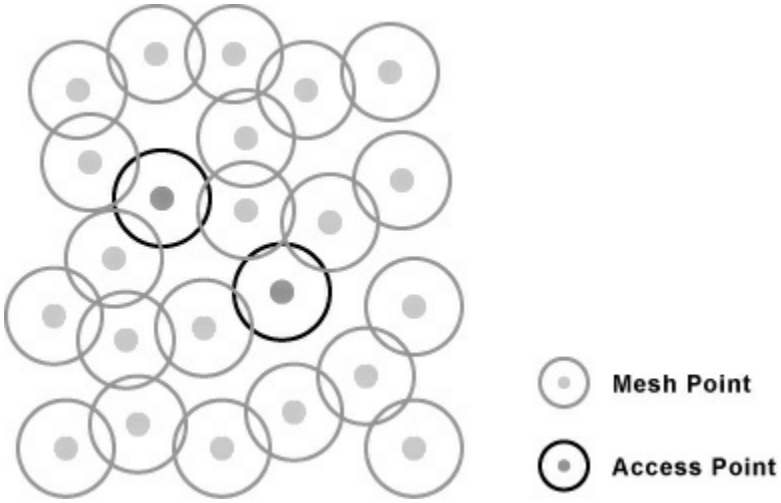
Änderungen am Kanalzugriff

Ergänzungen zum

Sicherheitskonzept

Grundlagen: Wireless Mesh

Networks (WMN)



In einem normalen WLAN kommunizieren die WLAN-Clients immer nur mit dem Access Point. In Wireless Mesh Networks sind die WLAN-Stationen untereinander vermascht. Mesh Networks agieren als Multi-Point-Netzwerke in denen die WLAN-fähigen Geräte im Ad-hoc-Modus als Relaisstationen bis zum nächstgelegenen Access Point dienen. Dabei verbessern Mesh-Network-fähige

Endgeräte die Reichweite des Access Points. Als Mesh-Points dienen Handys, PDAs und Notebooks.

In einem Mesh-WLAN bildet jeder Mesh-Point eine eigene Funkzelle. Während sich bei normalen WLANs die Funkzellen nur selten berühren, ist das bei Mesh-WLAN Absicht. Hier liegen die Mesh-WLANs in gegenseitiger Reichweite. Andernfalls würden sie kein Netzwerk bilden. Allerdings ist ohne Änderung am Zugriffsprotokoll keine brauchbare Performance möglich. Der Grund: Benachbarte Mesh-Points teilen sich einen gemeinsamen Funkkanal. Innerhalb des gemeinsamen Funkkanals kann immer nur ein Gerät senden. Jedes empfangene Paket muss zwischengespeichert werden, bevor es weitergesendet werden kann. Hier erkennt man auch das eigentliche Problem von Mesh-WLANs. Die

Störungen nehmen zu und das Zugriffsverfahren gerät an seine Grenzen.

Mesh Netzworks auf Basis von IEEE 802.11s

Herkömmliche Mesh-Verfahren für WLANs routen die Datenpakete auf IP-Ebene. Ein IP-Routing-Algorithmus, der einem WLAN übergestülpt ist, stößt sehr schnell an Performance-Grenzen. IEEE 802.11s verschiebt das Routing auf die MAC-Ebene. Das bedeutet, Mesh-WLANs mit IEEE 802.11s sind für Schicht-3-Protokolle wie IP transparent.
Um das Zwischenspeichern zu vermeiden, nutzt IEEE 802.11s EDCA (Enhanced Distributed Channel Access) für den Kanalzugriff. EDCA ist Bestandteil von IEEE 802.11e.
Um den Kanalzugriff noch effektiver zu gestalten, besitzen die meisten 802.11s-fähigen Basisstationen zwei

Funkmodule. So ist es möglich, dass Client- und Mesh-Network-Verkehr in unterschiedlichen Kanälen übertragen werden.

Besser ist MDA (Mesh Deterministic Access). Das ist ein Medienzugriffsverfahren, dass ähnlich wie das Distributed Reservation Protocol von WiMedia arbeitet. MDA ist aber nur als Option vorgesehen.

Verschlüsselung

WLANs nutzen WPA2 nur Absicherung des Netzwerks und der Datenübertragung. Bei Mesh-WLANs fehlt jedoch die übliche Hierarchie aus Authenticator (Beglaubiger) und Supplicant (Antragsteller). Deshalb müssen die Mesh-Points sich gegenseitig authentifizieren. Das bedeutet, sie durchlaufen die Prozedur einmal in jeder Rolle. Zur Authentifizierung kann ein zentraler Radius-Server (IEEE 802.1x)

dienen oder ein Passwort (Pre-shared Key, PSK) verwendet werden.

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. Im Außenbereich lassen sich Reichweiten bei Sichtkontakt bis 100 m oder mehr erreichen.

Hinweis: WLAN-Geräte, die dem Standard IEEE 802.11b entsprechen, sind veraltet. Man sollte sie nicht mehr verwenden. Zum Einen bieten sie keine ausreichende Verschlüsselung. Zum anderen 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.

DSSS - Direct Sequence Spread Spectrum

DSSS fasst die 79 schmalbandigen Kanäle im 2,4-GHz-Band in mehrere breitbandige Kanäle zusammen. In Europa gibt es 13, in den USA 11 und in

Japan 14 Kanäle. Diese Kanäle sind allerdings eng aneinander gereiht und überlappen sich.

Kanal Trägerfrequenz Frequenzbereich

2399,5 MHz -

1

2412 MHz

2424,5 MHz

2404,5 MHz -

2

2417 MHz

2429,5 MHz

2409,5 MHz -

3

2422 MHz

2434,5 MHz

2414,5 MHz -

4

2427 MHz

2439,5 MHz

2419,5 MHz -

5

2432 MHz

2444,5 MHz

2424,5 MHz -

6

2437 MHz

2449,5 MHz

2429,5 MHz -

7

2442 MHz

2454,5 MHz

2434,5 MHz -

8

2447 MHz

2459,5 MHz

2439,5 MHz -

9

2452 MHz

2464,5 MHz

2444,5 MHz -

10

2457 MHz

2469,5 MHz

2449,5 MHz -

11

2462 MHz

2474,5 MHz

2454,5 MHz -

12

2467 MHz

2479,5 MHz

2459,5 MHz -

13

2472 MHz

2484,5 MHz

14

2484 MHz

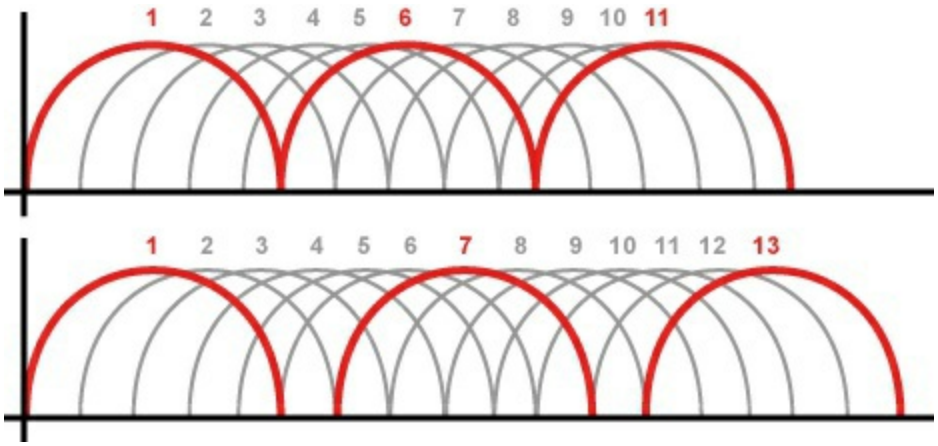
Kanalaufteilung

Insgesamt lassen sich von den 13 Kanälen (Europa) nur jeweils 3 Kanäle ohne Überlappung nutzen. Denn die 11 MBit/s von IEEE 802.11b stehen nur in diesen 3 Kanälen zur Verfügung. Das bedeutet auch, jedes Endgerät muss sich die Übertragungsleistung auf dem selben

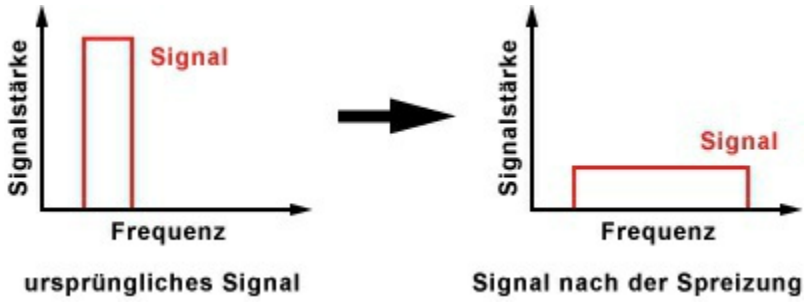
Kanal mit den anderen Endgeräten teilen (Shared Medium).

Bei der Konfiguration eines oder mehrerer Access Points muss darauf geachtet werden, dass die Kanäle nicht zu dicht beieinander liegen. Eventuell sollte noch sichergestellt werden, welche Kanäle in der Nachbarschaft genutzt werden, um eine ungewollte Überlappung zu vermeiden.

Überlappungen führen zu einer geringeren Übertragungsrate. Es wird empfohlen mindestens 5 Kanäle als Abstand zueinander einzuhalten. Um die Kanäle angrenzender WLANs herauszufinden wird ein WLAN-Sniffer benötigt, der in der Regel mit jedem WLAN-Adapter zusammenarbeitet. Manchmal liegt dem WLAN-Treiber auch ein Tool zur Anzeige benachbarter WLANs bei.



Um mehrere Access Points optimal nebeneinander betreiben zu können, ordnet man die Kanäle nach der 5er- bzw. 6er-Regel an. Die 5er-Regel verwendet die Kanäle 1, 6, 11 (Kanalbelegung für USA). Die 6er-Regel verwendet die Kanäle 1, 7, 13 (Kanalbelegung für Deutschland). Damit



überschneiden sich die Frequenzbereiche der Kanäle nicht und Verbindungsprobleme bleiben, aufgrund ungünstiger Kanalaufteilung, aus. Nur

wenn die Access Points über 30 Meter auseinanderstehen, darf sich die Kanalauswahl überschneiden.

Signalübertragung

Zur Übertragung des Funksignals wird

es auf die Spreizbandbreite gespreizt (Modulo-2-Multiplikation). Die Spreizung erfolgt mit einem Störcode, dem Pseudo-Noise-Code, der vor der Signalübertragung ausgehandelt wird. Dazu wird dem Originalsignal mehrere Bits, die sogenannten Chips, aufmoduliert und anschließend mit dem Trägersignal multipliziert. Das Signal wird auf die Gesamtbandbreite gespreizt und verschwindet im Rauschen.

Der Empfänger kehrt diesen Prozess um. Er multipliziert das empfangene Signal

mit den Spreizsignalen (Pseudo-Noise-Code). Diesen Vorgang nennt man Entspreizung. Anschließend werden durch einen Tiefpassfilter die unerwünschten schmalbandigen Störungen herausgefiltert. Das ursprüngliche Signal bleibt übrig.

Übersicht: Datenrate und Modulationsverfahren

Datenrate Verfahren Modulation Bit/Symbol 1 MBit/s

FHSS

2GFSK

1

2 MBit/s

FHSS

4GFSK

2

1 MBit/s

DSSS

DBPSK

1

2 MBit/s

DSSS

DQPSK

2

5,5

DSSS

DQPSK

4

MBit/s

11 MBit/s DSSS

DQPSK

8

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 benützt dafür das 2,4-GHz-

Frequenzband, wofür keine langwierigen Zulassungen notwendig sind. 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 Kompatibilität 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-

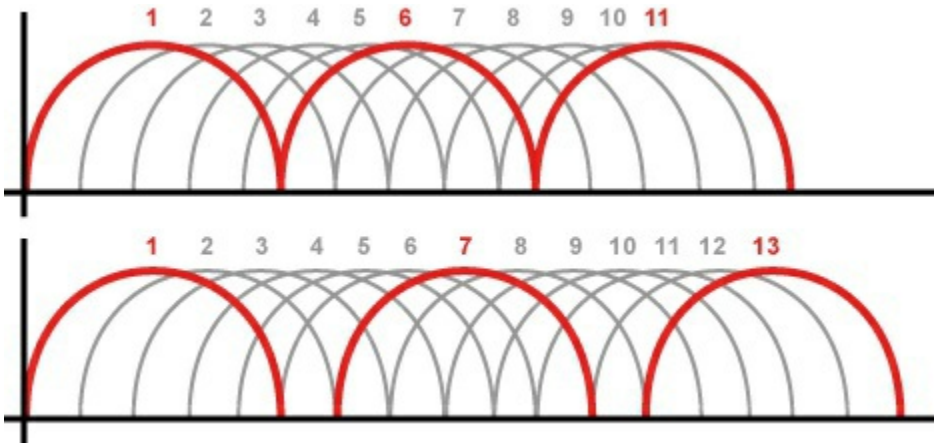
Steuerpaket (Clear-to-Send) voran. Das CTS-Paket reserviert das Medium für eine bestimmte Zeit. Es ist aber genauso lang, wie ein normales Datenpaket und drückt so die Datenrate. Das passiert immer dann, wenn 802.11g- und 802.11b-Stationen sich den selben Funkkanal teilen.

Kompatibilität zu IEEE 802.11a

Obwohl IEEE 802.11a und 802.11g mit 54 MBit/s dieselbe Übertragungsrate haben, ist die Kompatibilität nicht gegeben. 802.11a nutzt die Frequenzen über 5 GHz. Aufgrund der Abwärtskompatibilität zu 802.11b ist 802.11g dem Standard 802.11a vorzuziehen. Der Grund, IEEE 802.11a ist nicht auf der ganzen Welt identisch. Die Geräte sind teurer und evtl. wegen ihrer technischen Einschränkungen nur bedingt einsetzbar. Im Gegensatz dazu

lässt sich ein 802.11g-Gerät im Büro

oder im Heimnetzwerk mit 54 MBit/s



betreiben und an einem öffentlichen

WLAN-Hotspot notfalls auch mit 11

MBit/s.

Frequenznutzung und

Kanalaufteilung

Da IEEE 802.11g im gleichen

Frequenzband arbeitet, wie IEEE

802.11b, unterliegt es den gleichen

Beschränkungen. In Europa und Japan

lassen sich von den 13, in den USA 11,

Kanälen ohne Überschneidung nur 3

Kanäle nutzen. Im Prinzip wird das

Frequenzspektrum zusammengefasst. Nur

durch das Modulationsverfahren OFDM

erreicht IEEE 802.11g mehr

Übertragungsgeschwindigkeit.

Kanal Trägerfrequenz Frequenzbereich

2399,5 MHz -

1

2412 MHz

2424,5 MHz

2404,5 MHz -

2

2417 MHz

2429,5 MHz

2409,5 MHz -

3

2422 MHz

2434,5 MHz

2414,5 MHz -

4

2427 MHz

2439,5 MHz

2419,5 MHz -

5

2432 MHz

2444,5 MHz

2424,5 MHz -

6

2437 MHz

2449,5 MHz

2429,5 MHz -

7

2442 MHz

2454,5 MHz

2434,5 MHz -

8

2447 MHz

2459,5 MHz

2439,5 MHz -

9

2452 MHz

2464,5 MHz

2444,5 MHz -

10

2457 MHz

2469,5 MHz

2449,5 MHz -

11

2462 MHz

2474,5 MHz

2454,5 MHz -

12

2467 MHz

2479,5 MHz

2459,5 MHz -

13

2472 MHz

2484,5 MHz

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.

Turbo-Modus: 802.11g++ /

WLAN mit 108 MBit

Um dem Wunsch nach höherer Geschwindigkeit nachzukommen haben sich die Chipsatz-Hersteller einiges einfallen lassen. Beim Turbo-Modus unter 802.11g gibt es zwei Techniken, die den Datendurchsatz auf theoretisch 108 MBit/s, also eine Verdoppelung, hochtreiben können. Beide Techniken sind herstellerabhängig, also nur mit Geräten des selben Herstellers möglich, aber nicht als Standard festgelegt.

Channel Bonding

Nitro / Frame Bursting / Packet Aggregation / Packet Bursting

(Bezeichnung herstellerabhängig)

Verfahren, die 11g++ zugeordnet werden, entsprechen keinem offiziellen IEEE-Standard. Es handeln sich dabei um eigenmächtige Erweiterungen von Chipsatzherstellern. In der Praxis hat sich die eine oder andere Technik

bewährt und wurde deshalb später in neuen Spezifikationen offiziell berücksichtigt.

11g++ wird in Intels Centrino-Treiber als "Durchsatzverbesserung" bezeichnet. Das soll in etwa 30 Prozent mehr Datendurchsatz bringen. In der Praxis wird man nicht mehr als 10 Prozent erreichen.

Channel Bonding

Der Chipsatz-Hersteller Atheros verbreitert den Funkkanal von 20 MHz auf 40 MHz. Das Verfahren nennt sich Channel Bonding und verdoppelt die Einzelträger von 64 auf 128. Die maximale Bandbreite steigt so von 54 MBit/s auf 108 MBit/s. Channel Bonding liefert trotz Verdoppelung der Funkbandbreite nur etwa 10 MBit/s mehr. In der Praxis sogar deutlich weniger.

Atheros kombiniert Channel Bonding mit

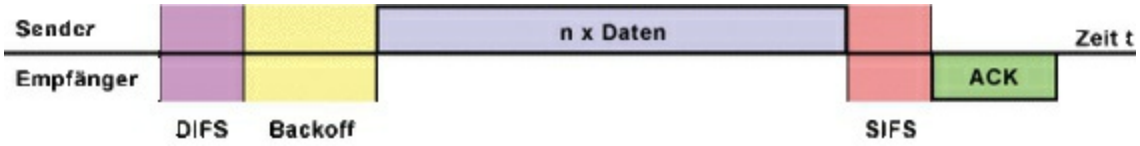
Kompression, Paketbündelung und Bursting. Damit sind Nutzdatenraten bis zu 60 MBit/s möglich.

Channel Bonding hat den Nachteil, dass es einen doppelt so breiten Anteil des bereits schmalen 2,4 GHz-Frequenzbandes belegt. Das so nahegelegene WLAN-Zellen gestört werden, ist nicht ausgeschlossen. Zwei 108-MBit-WLANs in räumlicher Nähe zueinander, schließen sich praktisch aus, wenn sich die Kanalbelegung nicht flexibel steuern lässt. Channel Bonding wird deshalb als Bandbreitenverschwendung verteufelt.

Die meisten WLAN-Hersteller nutzen Verfahren, die schonender mit der Bandbreite umgehen.

Der Atheros-Chipsatz ist weit verbreitet. WLAN-Komponenten unterschiedlicher Hersteller mit Atheros-Chipsatz können durchaus untereinander kommunizieren.

Nitro / Frame Bursting /



Packet Aggregation / Packet Bursting

Das zweite Verfahren ist je nach Hersteller unter einem anderen Namen bekannt. Allerdings haben alle eines gemeinsam. Sie optimieren das Zugriffsprotokoll der Funkschnittstelle. Beim Start ihrer Übertragung reservieren sich die Stationen die Sendezeit gleich für mehrere Datenpakete. Dadurch wird der Funkkanal effektiver ausgenutzt Die Zwangspausen und Synchronisationsprozesse nehmen weniger Zeit in Anspruch. So bleibt mehr Zeit für die Übertragung der Datenpakete.

Grundsätzlich sollten Produkte mit Frame Bursting von unterschiedlichen

Herstellern zusammenarbeiten, da sich die grundsätzlichen Zugriffe auf die Funkschnittstelle nicht verändert haben. Es ist sogar möglich, Geräte ohne Turbo-Modus mittels eines Firmware-Updates hochzurüsten und 108-MBit-fähig zu machen.

Frame Bursting hat einige Nachteile für Geräte ohne Unterstützung dieses Verfahrens. Geräte mit Frame Bursting können sich mehr Sendezeit reservieren. Geräte ohne Frame Bursting bekommen dann entsprechend seltener Zugriff auf die Funkschnittstelle.

In IEEE 802.11n ist Packet Aggregation offiziell eingeflossen.

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.

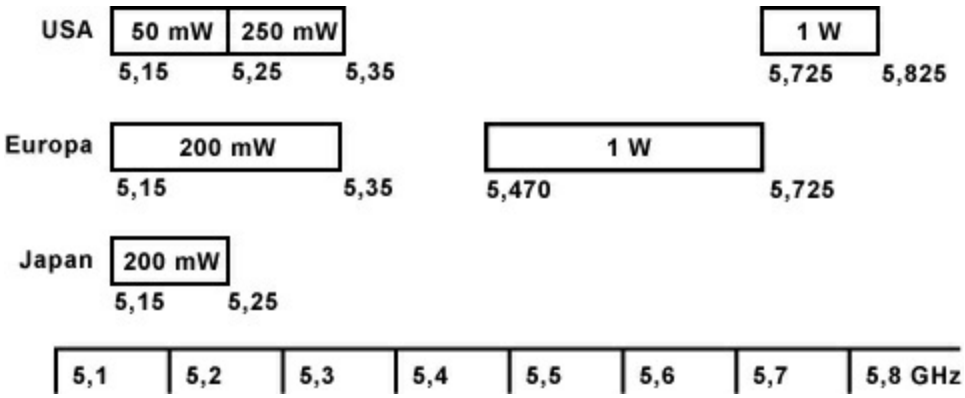
Der Grund für die parallele Entwicklung von 802.11a und 802.11g, liegt in der hohen Auslastung des 2,4-GHz-Bandes, in dem IEEE 802.11b und 802.11g funken. Drahtlose Fernbedienungen, AV-Brücken, Fernsteuerungen und viele private WLANs teilen sich die begrenzte Bandbreite im 2,4-GHz-Frequenzbereich. Mit 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.

Aufteilung und Nutzungserlaubnis des Frequenzbandes

IEEE 802.11a benutzt das 5-GHz-Frequenzband. 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 gibt es in Europa 19 Kanäle für 802.11a. Insgesamt ist das Frequenzspektrum in Europa 200 MHz groß (in Großbritannien sogar 455 MHz).

Kanalaufteilung des 5-GHz-

Bandes

IEEE 802.11a (USA)

IEEE 802.11h (Europa)

IEEE 802.11j (Japan).

IEEE

IEEE

IEEE

Träger-

Kanal

802.11a 802.11h 802.11j

Frequenz (USA) (EU)

(Japan)

5,180

36

ja

ja

ja

GHz

5,200

40

ja

ja

ja

GHz

5,220

44

ja

ja

ja

GHz

5,240

48

ja

ja

ja

GHz

5,260

52

ja

ja

nein

GHz

5,280

56

ja

ja

nein

GHz

5,300

60

ja

ja

nein

GHz

5,320

64

ja

ja

nein

GHz

5,500

100 GHz

nein

ja

nein

5,520

104

nein

ja

nein

GHz

5,540

108

nein

ja

nein

GHz

5,560

112

nein

ja

nein

GHz

5,580

116

nein

ja

nein

GHz

5,600

120

nein

ja

nein

GHz

5,620

124

nein

ja

nein

GHz

5,600

128

nein

ja

nein

GHz

132 5,660

nein

ja

nein

GHz

5,680

136

nein

ja

nein

GHz

5,700

140

nein

ja

nein

GHz

5,735

147

ja

nein

nein

GHz

5,755

151

ja

nein

nein

GHz

5,775

155

ja

nein

nein

GHz

5,835

167

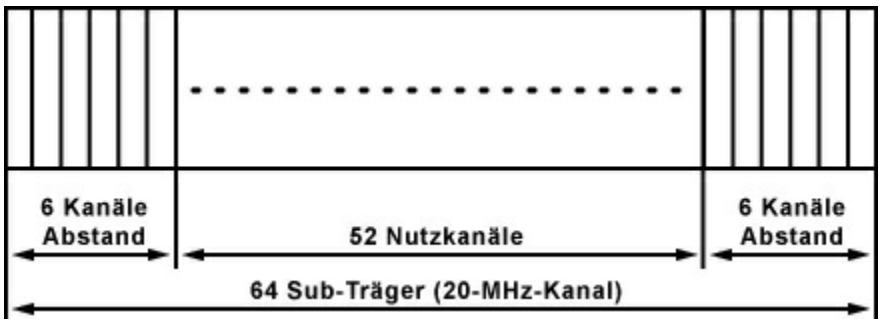
ja

nein

nein

GHz

Übertragungstechnik



Die hohe Datenrate von 54 MBit/s wird dadurch erreicht, dass mehrere Subträger mit geringem Datendurchsatz zu einen Hochgeschwindigkeitskanal innerhalb von 20 MHz kombiniert werden. Jeder 20-MHz-Kanal wird in 64-Sub-Träger aufgeteilt. Davon dienen 52 Kanäle zur Datenübertragung. Die anderen 12 Kanäle bleiben ungenutzt und dienen lediglich als Schutzabstand zu den anderen 20-MHz-Kanälen. Innerhalb der 52-Sub-Träger werden 48 zur Datenübertragung genutzt und die anderen 4 zur Übertragung von Signalen, die für die Phasensynchronisation gebraucht werden.

Es werden mehrere Modulationsverfahren und Kodierungsmechanismen unterstützt. Insgesamt sind 4 Modulationsverfahren möglich:

BPSK (Binary Phase Shift Keying),

2 Zustände

QPSK (Quad Phase Shift Keying),

4 Zustände

16-QAM (Quadratur Amplituden

Modulation), 16 Zustände

64-QAM (Quadratur Amplituden

Modulation), 64 Zustände

802.11a passt die Modulation an die

aktuelle Qualität jedes einzelnen

Subträgers an. Das Frequenzspektrum

wird also effektiv ausgenutzt. In

Abhängigkeit des verwendeten

Modulations- und Kodierungsverfahrens

ergeben sich unterschiedliche

Datenraten.

Datenrate Modulation Bits/Subcarrier

6 MBit/s

BPSK

1

9 MBit/s

BPSK

1

12 MBit/s QPSK

2

18 MBit/s QPSK

2

24 MBit/s 16-QAM

4

36 MBit/s 16-QAM

4

48 MBit/s 64-QAM

6

54 MBit/s 64-QAM

6

IEEE 802.11h

Am 13. November 2002 hat die RegTP in Deutschland für lokale Funknetze (Wireless Local Area Networks) den Frequenzen in den Bereichen 5150 MHz - 5350 MHz (innerhalb von Gebäuden) und 5470 MHz - 5725 MHz (innerhalb und außerhalb von Gebäuden) eine Allgemeinzuteilung erteilt.

Diese Frequenzbereiche sind nicht nur

für die Nutzung von IEEE 802.11a gedacht. Hier dürfen auch andere Funksysteme arbeiten. Diese Technologie-Neutralität soll es den Herstellern ermöglichen, flexible und innovative Lösungen im Markt zu platzieren und somit eine hohe Akzeptanz beim Verbraucher zu erzielen.
Um auch in Europa die Nutzung der Spezifikation IEEE 802.11a möglich zu machen, wurden diesem Standard mit IEEE 802.11h zwei Zusätze integriert:
dynamische Kanal- und Frequenzwahl: Dynamic Frequency Selection (DFS)
automatische Anpassung der Leistung: Transmit Power Control (TPC)
Die Kombination beider Verfahren erlaubt es den Netzelementen, die Kanäle mit der besten Verfügbarkeit zu ermitteln und eine möglichst kleine

Sendeleistung zu verwenden. Der Benutzer bekommt immer die Sendeleistung, die für die augenblickliche Entfernung zum Access Point benötigt wird. Die Übertragungsleistung wird von TPC auf ein Minimum beschränkt.

Die WLAN-Basisstationen müssen ihren Funkkanal beobachten und wechseln, wenn sie Nicht-WLAN-Signale feststellen. Dahinter steckt DFS (Dynamic Frequency Selection). Es dient dem Schutz anderer Systeme, wie beispielsweise Flughafenradar.

IEEE 802.11n / WLAN mit 100 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 mehrere 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 Laufe 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)

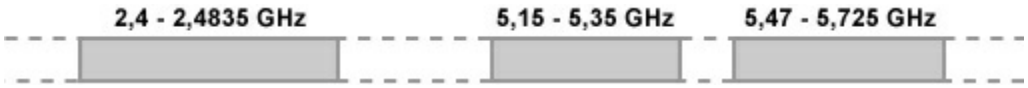
Bei IEEE 802.11n soll der Datendurchsatz über 100 MBit/s durch einen höheren Durchsatz auf der MAC-Schicht (Media Access Control) und einem geringeren Overhead erreicht werden. Deutliche Verbesserungen sollen adaptive MACs bringen, die die Bandbreite unter allen Teilnehmern besser aufteilt.

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

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 Begebenheiten 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 sind 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 also 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 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.

Kompatibilität zu Draft-N-tauglichen Geräten

Seit 2007 gibt es Draft-N-taugliche Geräte auf dem Markt. Diese Geräte sind durch die Wi-Fi Alliance (WFA) zertifiziert. Damit die Geräte, die dem offiziellen Standard IEEE 802.11n entsprechen, mit den alten Geräten kompatibel sind, durchlaufen die Standard-konformen Geräte das gleiche Zertifizierungsverfahren. Neue, nur im endgültigen Standard vorhandene Funktionen werden mit zusätzlichen Tests überprüft.

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.

Spatial Multiplexing

Spatial Multiplexing bezeichnet die parallel Übertragung mehrerer Datenströme in einem Funkkanal. Voraussetzung dafür ist der Einsatz mehrerer Antennen (MIMO). Pro Datenstrom ist eine Antenne notwendig. Der Einsatz mehrerer Antennen setzt einen Mindestabstand zwischen den Antennen voraus. Nur dann kann Spatial

Multiplexing funktionieren. In kleinen Geräten ist dieser Abstand nicht immer möglich.

Spatial Streams

Mit IEEE 802.11n ist es möglich, mehrere 10, 20 oder 40 MHz breite Kanäle innerhalb des freigegebenen Frequenzbandes bei 2,4 und 5 GHz zu nutzen. Pro 40-MHz-Kanal sind rein rechnerisch 150 MBit/s möglich. Mit zwei parallel betriebenen Datenströmen (Spatial Multiplexing) erreicht man theoretisch 300 MBit/s.

Anzahl der

Übertragungsrate

Datenströme

Brutto

Netto

150

1

ca. 90 MBit/s

MBit/s

300

ca. 120

2

MBit/s

MBit/s

450

ca. 180

3

MBit/s

MBit/s

600

ca. 240

4

MBit/s

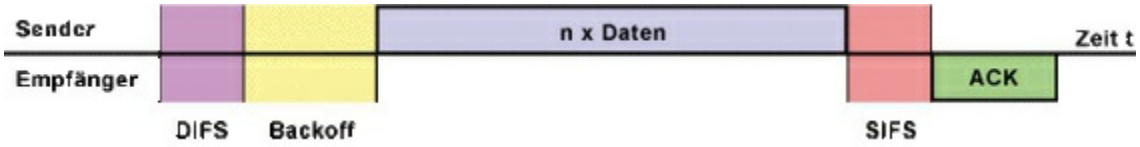
MBit/s

Um eine Übertragungsrate von 600 MBit/s (brutto) zu erreichen, müssen vier räumlich getrennte Datenströme auf der selben Frequenz parallel übertragen werden. Pro Datenstrom ist eine Antenne erforderlich und dafür ein hoher Hardware-Aufwand notwendig. Das

bedeutet, 4 Antennen mit eigenen Sender- und Empfangseinheiten. Das dürfte nur in sehr teuren Access Points möglich sein. In Smartphones und Tablets dürfte selten mehr als ein Datenstrom möglich sein. In der Konsequenz werden für den einzelnen Anwender nicht mehr als 150 MBit/s (brutto) bzw. ca. 90 MBit/s (netto) möglich sein.

Packet Aggregation

Packet Aggregation und Packet Bursting



sollen ebenso in den Standard enthalten sein. Dabei werden mehrere WLAN-Pakete zusammengefasst, um dabei die Header-Daten zu sparen.

Bei Packet Aggregation wird das WLAN-Frame vergrößert, so dass mehrere Ethernet-Pakete hinein passen. Mit diesem Verfahren wird der Paket-

Overhead reduziert, die Wartezeit zwischen den Datenpaketen verkürzt und somit der Durchsatz gesteigert.
Mit der zunehmenden Länge der Frames steigt aber auch die Wahrscheinlichkeit, dass durch Funkstörung die Pakete nochmal gesendet werden müssen. Hinzu kommt, dass andere Stationen länger auf das freie Medium warten müssen. Oder sie müssen die Datenpakete sammeln bis mehrere auf einmal gesendet werden können. Bei besonders vielen sendebedürftigen Stationen kann dadurch die Verzögerungszeit zwischen den Paketen deutlich größer werden. Die Übertragung von zeitkritischen Audio- oder Video-Übertragungen kann dabei gestört werden.

IEEE 802.11ac / Gigabit-WLAN

IEEE 802.11ac ist ein Standard für ein

WLAN mit Übertragungsgeschwindigkeiten im Gigabit-Bereich. Ein Entwurf des Standards definiert eine maximale Datenrate von 6.933 MBit/s. Die Beschleunigung erfolgt durch die Optimierung des Übertragungsprotokolls, verbesserte WLAN-Techniken und die konsequente Nutzung des Frequenzspektrums bei 5 GHz.

Hinweis: IEEE 802.11ac ist noch kein fertiger Standard, sondern befindet sich in der Entwurfsphase, in der es immer wieder Änderungen gibt. Daher mögen die folgenden Angaben und Ausführungen als vorläufig gelten. Obwohl der Standard noch nicht endgültig spezifiziert ist, gibt es bereits Hardware (so genannte 11ac-Draft-Geräte) in Form von WLAN-Routern und Notebooks. In Tablets und

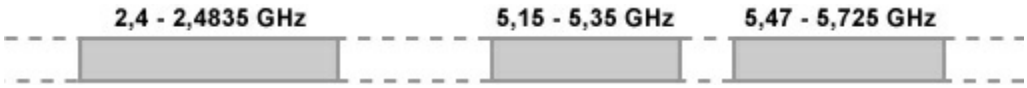
Smartphones wird 802.11ac

wahrscheinlich erst im Laufe 2013

auftauchen.

Technische Verbesserungen

Kanalbreiten von 20, 40, 80 und



160 MHz möglich.

Das Modulationsverfahren

256QAM kodiert pro

Übertragungsschritt 8 Bit.

Bis zu 8 simultan nutzbare

Antennen.

Mit Multiuser-MIMO (MU-MIMO)

können Basisstationen mehrere

Clients gleichzeitig bedienen.

Frequenzen

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 sein für mehrere parallel betriebene 11ac-WLANs.

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.

Nur mit DFS (Dynamic Frequency Selection) und TPC (Transmit Power Control) dürfen 5-GHz-Funksysteme die Kanäle oberhalb von Kanal 48 nutzen. Sonst dürfen sie nur die Kanäle zwischen 36 und 48 nutzen.

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.

Kanalbreiten von 20, 40, 80 und 160 MHz

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. Die Kanalbreite 160 MHz ist optional.

Ob in der Praxis ein 160 MHz breiter Kanal möglich ist, ist fraglich. Wenn wie im 2,4-GHz-Band auch im 5-GHz-Band mehrere WLANs parallel die Frequenzen nutzen, dann wird es eng und führt zu sinkenden Übertragungsraten. 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.

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

Weil IEEE 802.11ac noch in der Entwurfsphase steckt sind die folgenden Übertragungsgeschwindigkeiten als vorläufig anzusehen. Die traumhafte Übertragungsrate von bis zu 6.933 MBit/s darf jedoch nicht darüber hinwegtäuschen, das in der Praxis niedrigere Werte realisierbar sind.
In der Praxis wurden bereits über 400 MBit/s mit einem Datenstrom und einer Antenne, bei einem 80 MHz breiten Kanal und dem Modulationsverfahren 256QAM erreicht. Die Bruttorate steigt mit der Mehrantennen-Technik MIMO mit zwei räumlich getrennten Datenströmen auf über 800 MBit/s. Mit drei Streams steigt die Datenrate auf 1.300 MBit/s.
Das Ziel ist es mindestens 1 GBit/s zu erreichen. Unter guten Funkbedingungen dürfte das eine WLAN-Funkzelle durchaus erreichen. Wenn alle

Möglichkeiten ausgenutzt werden, dann ist ein Bruttodurchsatz von 3,5 GBit/s theoretisch möglich.
Berücksichtigt man, dass ein WLAN von mehreren Teilnehmern gleichzeitig genutzt wird, dann steht in der Praxis vielleicht 500 MBit/s bei einem 80-MHz-Kanal für eine Station zur Verfügung. Bei mehreren Stationen sollte zumindest ein Summendurchsatz von 1000 MBit/s möglich sein.
Ob alle WLAN-Clients diese Geschwindigkeit erreichen ist fraglich. Bei einem Smartphone ist davon auszugehen, dass nur eine Antenne vorhanden und damit nur ein Datenstrom möglich ist. Die Minimal-Unterstützung liegt bei den Kanalbreiten 20, 40 und 80 MHz, sowie die Modulationsstufen bis 7 MCS (64QAM). Alles Weitere ist optional. Ein WLAN-Client in einem 80-MHz-Kanal mit 64QAM kann

theoretisch nur 292,5 MBit/s erreichen.
Ein Gerät mit 293 MBit/s (brutto) gilt bereits als 11ac-fähig.
In Smartphones wird das üblich sein. Denn dort ist kein Platz für mehrere WLAN-Antennen und die Rechenleistung nicht groß genug, um höhere Modulationen und MIMO zu unterstützen. Die geringe Akkuleistung und knapper Platz sind die begrenzenden Elemente in mobilen Geräten.
USB-WLAN-Adapter arbeiten höchstens mit 2 Antennen, wobei bestenfalls 867 MBit/s (brutto) möglich sind. Wenn dieser USB-Stick aber lediglich per USB 2.0 angebunden ist dann sind höchstens 480 MBit/s erreichbar. Das ist die höchste Transferraten des USB-Ports.
In der ersten Ausbaustufe ist 1,3 GBit/s im 5-GHz-Band erreichbar.
Vorausgesetzt, die Funkverbindung ist

einwandfrei. Wenn alle Features zum Einsatz kommen, dann ist eine Bruttoübertragungsgeschwindigkeit von 3,5 GBit/s durchaus vorstellbar.

Anwendungen

Neben dem Betrieb eines schnurlosen Netzwerks ist es auch denkbar, zwei kabelgebundene Gigabit-Netzwerke drahtlos zu koppeln, ohne dass dabei ein nennenswerter Flaschenhals durch die Funkverbindung entsteht. Wenn die beiden Gegenstellen aufeinander abgestimmt sind, dann wäre es möglich die theoretische Übertragungsgeschwindigkeit zu erreichen.

Zur Zukunft von WLAN

Angesichts der Möglichkeiten, die IEEE 802.11ac mit sich bringt wären optimale Aussichten für die Zukunft vorprogrammiert. Hier kommt nun eine Begrenzung zum Tragen, die nur wenige

sehen.

Obwohl man im Optimalfall 1.300 MBit/s und mehr per WLAN erreichen könnte, ist damit auch das Ende der Fahnenstange erreicht. In einem Gigabit-Netzwerk per Ethernet (1.000 GBit/s) liegt die Grenze bei 930 MBit/s. Es ist davon auszugehen, dass in kleinen Netzwerken die Hersteller kein 10GBaseT für 10-Gigabit-Ethernet (10.000 MBit/s) einbauen werden, was aber notwendig wäre, wenn ein WLAN über 1.000 MBit/s betrieben wird.

MIMO - Multiple

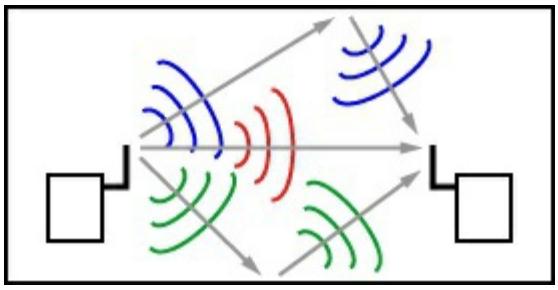
Input Multiple

Output

MIMO ist der Oberbegriff für Verfahren, die Funkverbindung mit mehreren Antennen verbessern. Mehrere Antennen liefern ein besseres Empfangssignal, vergrößern die mögliche Distanz oder erhöhen den Datendurchsatz.

Warum MIMO?

Bei der Entwicklung neuer



Funktechniken stößt man bei Ein-Antennen-Systemen immer öfter an das technisch Machbare. Die Strategie, ein immer höherstufiges Modulationsverfahren einzusetzen, lässt das Kosten-Nutzen-Verhältnis aus dem Ruder laufen. Denn die Hochfrequenzelektronik müsste eine deutlich höhere Genauigkeit aufweisen, um aus einem schlechten Funksignal noch ein brauchbares Datensignal erkennen zu können.

Mehrere Antennen verhelfen dem Empfänger zu räumlichen Informationen (Spatial Multiplexing), was zur Steigerung der Übertragungsrate genutzt

werden kann. Das ist besonders in Situationen vorteilhaft, wo keine Sichtverbindung zwischen den Sende- und Empfangsstationen besteht. Zum Beispiel in Gebäuden, wo sich die Signale aufgrund von Decken und Wänden mehrfach ausbreiten. WLANs mit MIMO-Technik profitieren dann durch die Mehrwegeausbreitung.

MIMO in Mobilfunknetzen

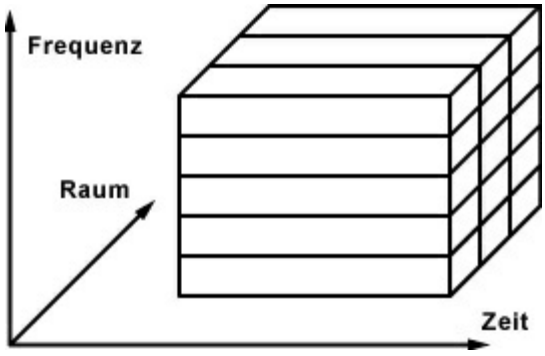
Seit dem Ausbau der Mobilfunknetze zu Breitbandnetzen sind die Entwickler auf der Suche nach Ansätzen zur Kapazitätssteigerung. Wegen der Bandbreitenbeschränkung aufgrund kleine Frequenzbereiche, verschiedener Funktechniken innerhalb des Frequenzspektrums und der unterschiedlichen Qualität der Funkschnittstelle, wird immer wieder an Verfahren gearbeitet, durch die Funktechnik grundlegend verbessert

wird. Als zukunftsweisend wird die Verwendung mehrere Antennen gesehen. Diese Technik, die MIMO genannt wird, kommt bereits in WLANs nach IEEE 802.11n zum Einsatz. Und auch die Arbeitsgruppen rund um die Standardisierung von WiMAX, HSPA und LTE sind an dieser Technik interessiert.

Ohne MIMO wird in Zukunft keine Funktechnik mehr auskommen. Egal ob WLAN, WiMAX, UMTS oder LTE.

MIMO-Prinzip

Das Prinzip, das bei MIMO zur Anwendung kommt, stammt aus der militärischen Radartechnik, die schon seit vielen Jahren genutzt wird. Dort setzt man nicht nur eine, sondern gleich mehrere baugleiche Antennen ein. Die Antennen haben zueinander mindestens eine halbe Wellenlänge (lambda/2) der Trägerfrequenz Abstand

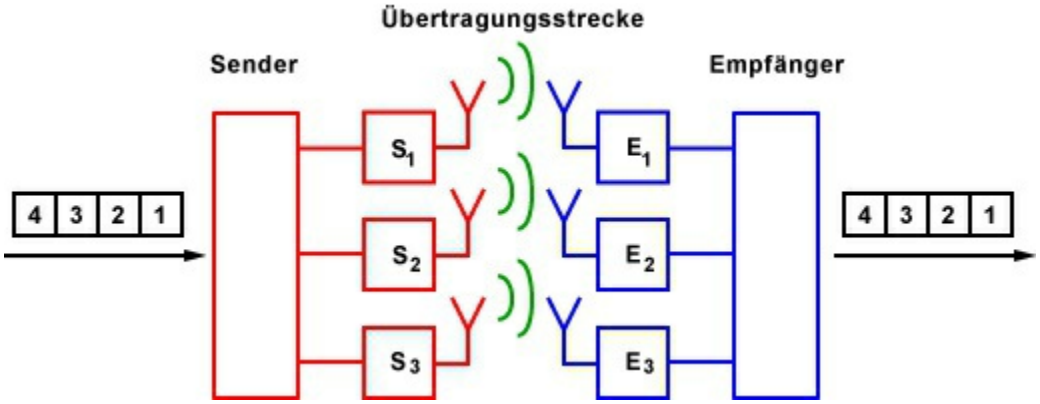


Der bis dahin üblichen Frequenz-Zeit-Matrix wird eine 3. Dimension, der Raum, hinzugefügt. Dabei wird das Datensignal über mehrere Antennen gesendet. Gleichzeitig werden auch mehrere Empfangsantennen verwendet. Die signalverarbeitende Empfangseinheit bekommt durch mehrere Funksignale eine räumliche Information. Denn bei zwei Antennen trifft das selbe Funksignal aus zwei verschiedenen Richtungen beim Empfänger ein. Jedes eingehende Funksignal weist in der Regel einen eigenen "räumlichen Fingerabdruck" auf, der auch "Spatial Signature" genannt wird. Der Empfänger setzt die Signale wieder passend zusammen. Dadurch verbessert sich die Leistung des ganzen

Funksystems erheblich.

MIMO in der Praxis

MIMO-Systeme müssen die Übertragung ständig an die wechselnden Eigenschaften des Funkkanals anpassen. Die komplexen Sende- und Empfangssysteme von Mehrantennensystemen in Hardware zu



implementieren ist eine große Herausforderung. Insbesondere deshalb, weil eine hohe Rechenleistung benötigt wird und in mobilen Geräten der Energiebedarf ansteigt.

Die einfachste MIMO-Hardware besteht aus zwei Sendeantennen und einer Empfangsantenne. Um die Leistungsfähigkeit optimal auszunutzen,

werden Antennen immer paarweise eingesetzt. Dadurch vereinfachen sich die MIMO-Signalverarbeitungsalgorithmen und führen zu einem optimalen Signal-Rausch-Abstand.
Die Bandbreite lässt sich mit der Anzahl der Sendeantennen linear erhöhen. Das Trennen der einzelnen Signale ist eine einfache lineare Matrizenrechnung, die von leistungsfähigen Prozessoren berechnet wird. Geht man von dieser Rechnung aus, dann ließe sich theoretisch die Übertragungskapazität ins unendliche steigern.
Jeweils 8 Sende- und Empfangsantennen gelten als das Maximum. Je mehr Sende- und Empfangsantennen, desto größer ist die Leistungsaufnahme durch die Hardware, desto größer die Wärmeentwicklung. Mal abgesehen vom enormen Platzbedarf. So spielt bei

kleinen tragbaren Geräten der Kompromiss zwischen Preis und Leistung eine große Rolle.

Mit jeweils 3 Sende- und Empfangsantennen erreicht man bereits optimale Systemvoraussetzungen für den Praxiseinsatz.

Vorteile durch Mehrfach-Antennen-Systeme

größere Empfangsleistung (Gruppengewinn)

Störerunterdrückung (Interferenzunterdrückungsgewinn)

bessere Verbindungsqualität (Diversitätsgewinn)

höhere Übertragungsraten (Multiplexgewinn)

Dabei muss man beachten, dass die 4 Gewinntypen nicht gleichzeitig maximiert werden können. Je nach Umgebung kann die Datenrate, die Verbindungsqualität oder die

Reichweite verbessert werden. Aus diesem Grund ist die MIMO-Technik noch ein großes Feld für Forschung und Entwicklung. Letztlich geht es darum, unter Berücksichtigung von Umgebung und den verschiedenen Mobilfunkstandards, die beste Kombination aus den vier Gewinntypen herauszubekommen.

Gruppengewinn

Der Gruppengewinn ergibt sich aus der Anzahl von Empfangsantennen. Mehr Antennen können aus den eintreffenden Funksignalen mehr Leistung herausholen und so die Funkverbindung verbessern. Mit einer Verdoppelung der Antennen erreicht man einen Gruppengewinn von maximal 3 dB.

Dazu müssen die empfangenen Funksignale durch lineare Überlagerungen (Spatial Combining) miteinander verknüpft werden. Dabei

spielt ein Verzögerungselement bei der Signalverarbeitung ein wichtige Rolle.
Die räumliche Trennung funktioniert jedoch nicht, wenn die Funkstationen zu dicht beieinander stehen. Die Grenze liegt in der Breite der Hauptkeule im Richtdiagramm. Die Breite wird in Grad angegeben. Stehen die Stationen zu dicht beieinander, dann muss man die üblichen Techniken, wie unterschiedliche Trägerfrequenzen, Zeitmultiplex und Übertragungscodes verwenden.
Weil die Antennen beim Senden und Empfangen das gleiche Verhalten aufweisen, kann man das MIMO-Verfahren nicht nur beim Empfangen, sondern auch beim Senden einsetzen.
Beim Senden führt die Verzögerung der Funkstrahlen zu einer Verformung (Beamforming). Die Antenne strahlt die Sendeleistung in die Richtung des

Empfängers ab. Davor muss natürlich der Winkel bestimmt werden, in dem sich der Empfänger befindet. Um das herauszufinden, wird das Funksignal in verschiedene Richtungen gesendet. Da in WLANs nach IEEE 802.11 jedes Datenpaket vom Empfänger bestätigt werden muss, weiß der Sender, wie stark seine Gegenstelle ihn empfangen kann. Die entsprechende Information wird als RSSI (Received Signal Strength Indication) übertragen. Und so bekommt der Sender auch heraus, wo sich der Empfänger befindet. Nämlich dort, in welche Richtung das Signal gesendet wurde, das er am besten empfangen konnte.

Doch auch beim Beamforming gilt es, die Vorschriften für die maximal erlaubte Sendeleistung (äquivalente isotrope Sendeleistung, EIRP) einzuhalten. Deshalb muss die

Sendeleistung auf alle Antennen aufgeteilt werden.

Interferenzunterdrückungsgewinn

Typisch für Funktechniken ist die Mehrwegeausbreitung (Multipath Propagation) der Funksignale durch Reflektionen und Abschattungen an Wänden und Gebäuden. Bei der Mehrwegeausbreitung trifft das Funksignal aus verschiedenen Richtungen mit unterschiedlichen Laufzeiten beim Empfänger ein. Der Empfänger muss dann versuchen das ursprüngliche Signal herauszufiltern. Im schlimmsten Fall wird das Trägersignal ausgelöscht. Der Empfänger befindet sich dann in einem Funkloch. Autofahrer kennen das, wenn sich der Radioempfang beim Anhalten deutlich verschlechtert und beim Anfahren wieder deutlich verbessert. Die Strecke des Funklochs ist gerade so kurz, wie

eine halbe Wellenlänge (lambda/2).
Beim UKW-Radio beträgt es etwas 1,5 Meter. Beim WLAN ist die Strecke etwa 6 cm lang. Bei einem MIMO-Funksystem kann das bedeuten, dass während eine Antenne sich im Funkloch befindet, eine andere Antenne das Funksignal in bester Qualität bekommt.
Diese Funklöcher können durch eine veränderliche Umgebung entstehen. Schon in einem Raum mit umhergehende Personen oder geöffnete Schranktüren kann es erheblichen Schwankungen bei der Signalstärke (Fading) kommen.
Diesen Effekt können WLAN-Empfänger bereits durch zwei Empfangsantennen ausgleichen, in dem sie das bessere Signal auswählen.
Intelligente Antennen können Funksignale aus bestimmten Richtungen, zum Beispiel von anderen Nutzern oder Störungen, ausblenden. Und schon allein

durch die Strahlformung (Beamforming) reduzieren sich die Interferenzen.

Diversitätsgewinn

Funklöcher entstehen dadurch, dass sich die elektromagnetischen Wellen des ursprünglichen Signals und die des reflektierten Signals gegenseitig auslöschen. Dass sich eine Antenne in einem Funkloch befinden könnte, lässt sich nicht vermeiden. Die Entstehung von Funklöchern ist nicht nur von der Umgebung, sondern auch von deren Veränderung abhängig. Um zu vermeiden, dass ein Funksystem durch Funklöcher Empfangsprobleme bekommt, arbeitet man mit mehreren Sende- und Empfangsantennen. Durch die Vielfalt (Diversität) wird die Ausfallsicherheit erhöht.

Schon allein mit 2 Antennen kann man einen Diversitätsgewinn von mehreren dB erreichen. Sind die Antennen in

einem Abstand von einer halben Wellenlänge angeordnet, dann eignet sich die Antennengruppe für Strahlformung (Beamforming). Ist der Abstand zwischen den Antennen größer, dann eignet sich die Gruppe für Diversität.

Nutzt man zwei Gruppen, eine für Strahlformung und eine für Diversität, dann kann man beides miteinander kombinieren. Dann profitiert man von Situationen, in denen Sichtverbindung zwischen den Stationen besteht und gleichzeitig Mehrwegeausbreitung durch ungünstig platzierte Stationen entstehen.

Multiplexgewinn

Der Multiplexgewinn steigert die Effizienz des MIMO-Verfahren vor allem in einer Umgebung mit erhöhter Mehrwegeausbreitung. Ein Vorteil dann, wenn Sender- und Empfänger keine direkte Sichtverbindung haben und die

Übertragung über Reflektionen erfolgt. Dann kommt auch die Teilnehmertrennung voll zum Tragen. Während bei einem herkömmlichen SISO-System, wie ein WLAN nach IEEE 802.11g bei guter Verbindung auf Anwendungsebene 3 MByte/s übertragen werden, erreicht man bei einem MIMO-System mit zwei Antennen rund 4 MByte/s. Verdreifacht man die Antennen auf Empfänger- und Senderseite, dann kann das zur Verdoppelung der Datenrate führen.

WLAN-Sicherheit

In physikalischen Netzen, mit Leitungen und Kabel, setzt das Abhören der Kommunikation das physikalische Anzapfen der Leitung voraus. Da Leitungen in der Regel durch gesicherte Gebäude oder unterirdisch verlaufen, ist das Abhören von Anfang an erschwert. In einem Funknetz sieht das ganz anders

aus. Hier dient der freie Raum als Übertragungsmedium. Sobald ein drahtloses Gerät seine Daten abstrahlt, benötigt ein Angreifer nur eine Antenne, um sich zumindest Zugang zum Signal zu verschaffen. Aus diesem Grund sind Sicherheitsvorkehrungen zu treffen, die das Signal für den Angreifer unbrauchbar macht.

In den Anfangszeiten des WLAN-Hypes war der IEEE-Standard 802.11 ein einziges Sicherheitsrisiko. Die Datenübertragung war abhörbar und unverschlüsselt. In Unternehmen ist das nicht akzeptabel. Zwar wurde mit WEP schnell ein Verschlüsselungsprotokoll nachgeliefert. Doch genauso schnell stellte sich heraus, dass es sich schnell knacken lässt. Das IEEE entwickelte deshalb den Standard IEEE 802.11i mit sicheren Verschlüsselungsverfahren.

Sniffing und War-Driving

Sniffing und War-Driving sind gängige Bezeichnungen für das Ausspionieren von WLANs. Dabei werden spezielle WLAN-Karten verwendet, die mittels eines Treibers zum Channel Hopping verwendet werden. So lässt sich das Frequenzspektrum nach WLANs absuchen. Über einen Monitor-Modus hören die Karten nur mit, nehmen aber keine Verbindung auf.

War-Driving ist die Bezeichnung für eine Tätigkeit, um Wireless-Netzwerke zu finden und mehr Informationen über deren Aufbau in Erfahrung zu bringen. Im einfachsten Fall ist War-Driving das Umherfahren mit einem Auto in dem sich ein Laptop mit eingebautem WLAN-Adapter und externer Antenne befindet. In Kombination mit einem GPS-Empfänger lässt sich der Standort eines WLANs protokollieren, um ihn später auf einer Karte wiederzufinden. Mit

einer speziellen Software, einem Sniffer, werden alle WLANs erkannt und protokolliert. Auch ob sie offen oder verschlüsselt sind, welches Access-Point-Equipment verwendet wird (bekannte Sicherheitslücken?) und welche Netzwerkgeschwindigkeit vorliegt. Offene WLANs ohne Verschlüsselung laden dann regelrecht zum Surfen im Internet ein, sofern das Netzwerk hinter dem Access-Point über einen solchen Zugang verfügt.

War-Driving war in der Anfangszeit der WLANs ein beliebter Sport, weil viele WLANs nicht verschlüsselt waren. Heute ist War-Driving uninteressant, weil auch private WLANs standardmäßig verschlüsselt sind, was den Zugang mit einfachen Mitteln erschwert.

Sicherheitsrisiko WLAN?

IEEE 802.11i bzw. WPA2 gilt seit

einiger Zeit als hinreichend sicher. Die Technik ist inzwischen ausgereift und vielfach im Einsatz. Wer nicht verschlüsselt oder immer noch WEP verwendet, der handelt nach Ansicht von Sicherheitsexperten grob fahrlässig. In der Regel gibt es auch rechtliche Probleme, wenn mit einem unverschlüsselten WLAN freier Zugang zum Internet möglich ist.

WLAN-Komponenten sind inzwischen so günstig zu haben, dass es für den Austausch der veralteten Geräte gegen neue mit WPA2-Verschlüsselung keine Ausrede gibt.

Im kommerziellen Einsatz sollten mit zusätzlichen Maßnahmen die übertragenen Daten geschützt werden. Mit SSH und IPsec lässt sich die Kommunikation zwischen Anwendungen sicherer machen. Windows-Clients lassen sich mit PPTP absichern.

Das Abhören und Entschlüsseln der Datenübertragung im WLAN ist dann nur mit unverhältnismäßig hohem Aufwand möglich. Wer ganz sicher gehen will, der lässt die Finger von WLAN und überträgt seine Daten ausschließlich über Kabelverbindungen.

10 Maßnahmen zur WLAN-Sicherheit

1. Eigene SSID vergeben
2. Eigenes Admin-Passwort für den Access Point vergeben
3. SSID-Broadcast abstellen (nicht empfehlenswert)
4. WPA2-Verschlüsselung einschalten
5. MAC-Adressfilter einsetzen
6. VPN einsetzen
7. WLANs von anderen Netzwerk-Segmenten logisch trennen
8. Firewall zwischen WLAN und LAN installieren
9. IDS im WLAN aufstellen

10. regelmäßige Audits mit aktuellen Hacker-Tools

Warum ein MAC-Adressfilter als alleiniges Sicherheits-Tool nichts taugt

Ein MAC-Adressfilter verschlüsselt die Daten nicht. Das Abhören der Verbindungen ist jederzeit möglich. Er verhindert nur, dass fremde Stationen so einfach das WLAN mitbenutzen dürfen. Weil die Verbindung nicht verschlüsselt ist, kann ein Angreifer die verwendeten MAC-Adressen mitlesen und übernehmen. MAC-Adressen können überschrieben werden. Das bedeutet, auf der MAC-Adressen-Ebene können Stationen sich für andere Stationen ausgeben. Und somit wäre der MAC-Adressfilter umgangen.

WLAN: Abschalten der SSID?

Das Abschalten oder Ausschalten der SSID im Access-Point gilt als Maßnahme zur Erhöhung der WLAN-Sicherheit. Diese Ansicht ist weit verbreitet. Es wird auf allerlei Internet-Seiten, so genannten Fachzeitschriften und auch in Büchern empfohlen. Tatsächlich handelt es sich dabei um einen Irrglaube.

Das Verstecken oder Abschalten der SSID ist ein Leistungsmerkmal, das nicht offiziell der Norm entspricht. Es wird nicht von jeder WLAN-Hardware unterstützt. Wenn die SSID im Access Point trotzdem abgeschaltet wird, kann es passieren, dass andere WLAN-Stationen den Access Point nicht mehr sehen und sich deshalb gar nicht erst dort anmelden.

Problematisch ist es auch, wenn ein Betreiber eines neuen WLAN-Access-Points ein bereits fremdes installiertes

WLAN nicht sehen kann und dummerweise den gleichen Funkkanal belegt. Dann funken zwei WLANs auf dem gleichen Kanal und können sich gegenseitig stören. Der Betreiber des neuen Access Points wundert sich dann, warum sein WLAN nicht richtig funktioniert. Den Fehler wird er ohne umfangreiches Know-how nicht finden. Und der Betreiber des bereits bestehenden WLANs wird sich wundern, warum sein WLAN auf einmal ständig Probleme macht. Das können niedrige Datenraten sein und sogar Totalausfälle.

Das Argument, dass versteckte WLANs von Wardrivern nicht gefunden werden ist falsch. Ein WLAN-Hacker oder Wardriver wird sich von der versteckten SSID nicht stören lassen. Mit den richtigen Tools kann man auch WLANs mit abgeschalteter SSID sichtbar

machen.

Rechtliche Bedeutung eines unverschlüsselten WLANs

Ein offenes WLAN stellt sich wie ein offenes Scheunentor dar. Beim Surfen über das offene WLAN hinterlässt die IP-Adresse des WLAN-Betreibers eine Spur im Netz. Diese IP-Adresse kann im nachhinein dem Anschlussinhaber zugeordnet werden. Der Anschlussinhaber wird daher im Rahmen einer Rechtsverletzung als erster Verdächtiger ermittelt. Schnell kann es vorkommen, dass man eine Straftat angehängt bekommt, obwohl Fremde den unverschlüsselten WLAN-Zugang missbraucht haben. Da hilft es dann auch nicht zu erklären, man habe nur seinen Nachbar ins Netz gelassen oder versehentlich die Verschlüsselung abgeschaltet.

IEEE 802.11i -

WPA/WPA2 -

WiFi Protected

Access

IEEE 802.11i ist ein Standard für die 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 gröbsten Sicherheitsmängel von WEP beseitigen.

WPA - WiFi Protected

Access

Noch vor der offiziellen Verabschiedung von IEEE 802.11i, brachte die Herstellervereinigung Wi-Fi Alliance auf Basis eines Entwurfes 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.

In WPA kommt TKIP (Temporal Key Integrity Protocol) als Verschlüsselungsmethode zum Einsatz. TKIP setzt auf den RC4-Algorithmus mit einer verbesserten Schlüsselberechnung (Fast Packet Keying, FPK).

WPA2 - WiFi Protected Access

Nach der Verabschiedung von IEEE 802.11i erweiterte die Herstellervereinigung Wi-Fi Alliance WPA um eine zweite Version. Damit basiert WPA2 auf dem Standard IEEE 802.11i. Zu beachten ist, dass WPA2 nicht gleich IEEE 802.11i ist. WPA2

gibt es in zwei Varianten, die beide nicht identisch mit IEEE 802.11i sind.

WPA-

WPA

Variante

Personal

Authentifizierung PSK

Mode

Verschlüsselung TKIP/MIC

Enterprise Authentifizierung 802.1x/EAP

Mode

Verschlüsselung TKIP/MIC

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.
Ab 2011 dürfen Access Points kein TKIP mehr unterstützen. Ab 2012 gilt das für alle WLAN-Geräte. Ab 2014 dürfen Access Points nur noch WPA2-AES anbieten.

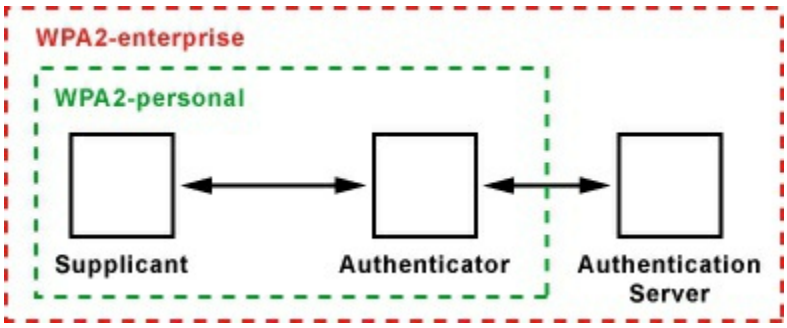
WPA2-enterprise

WPA2-enterprise 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.

WPA2-personal

WPA2-personal ist eine abgespeckte

WPA2-Variante, die hauptsächlich in SOHO-Geräten für Privatanwender und kleine Unternehmen gedacht ist und auf einige Funktionen verzichten können. Dazu gehören Funktionen, die in



größeren Netzwerken verwendet werden. Z. B. auch die RADIUS-Authentifizierung.

Funktionsweise von IEEE 802.11i und WPA/WPA2

Bei der WPA-Schlüsselverhandlung bekommen die Stationen Rollen zugewiesen. Der Access Point ist der Authenticator (Beglaubigter) und der Client der Supplicant (Antragsteller/Bittsteller). Dabei ist genau festgelegt, welche Seite welches

Paket zu welchem Zeitpunkt verschickt und wie darauf reagiert werden muss.
Bei WPA erfolgt die Netzwerk-Authentifizierung mit einem Pre-Shared-Key (PSK) oder alternativ über einen zentralen 802.1x/Radius-Server. Dabei wird ein Passwort mit 8 bis 63 Zeichen Länge verwendet. Das Passwort ist Teil eines 128 Bit langen individuellen Schlüssels, der zwischen WLAN-Client und dem Access Point ausgehandelt wird. Der Schlüssel wird zusätzlich mit einem 48 Bit langen Initialization Vector (IV) berechnet. Dadurch wird die Berechnung des WPA-Schlüssels für den Angreifer enorm erschwert.
Die Wiederholung des aus IV und WPA-Schlüssel bestehenden echten Schlüssels erfolgt erst nach 16 Millionen Paketen (2-24). In stark genutzten WLANs wiederholt sich der Schlüssel also erst alle paar Stunden. Um die Wiederholung

zu verhindern, sieht WPA eine automatische Neuaushandlung des Schlüssels in regelmäßigen Abständen vor. Damit wird der Wiederholung des echten Schlüssels vorgegriffen. Aus diesem Grund lohnt es sich für den Angreifer kaum den Datenverkehr zwischen Access Point und WLAN-Clients abzuhören.

Schwachstellen von WPA2

Die Schwachstelle von WPA2 ist der Schlüssel, der bei Broadcasts und Multicasts die Datenpakete verschlüsselt (Groupkey). Dieser Schlüssel ist allen Stationen bekannt. Bekommt eine nicht autorisierte Person diesen Schlüssel heraus, ist sie in der Lage den anfänglichen Schlüsselaustausch zwischen Client und Access Point zu belauschen. Die Aushandlung dieses Schlüssels ist zumindest bei IEEE 802.11i täglich vorgesehen (86400

Sekunden).

Eine weitere Schwachstelle ist das Passwort (PSK). Je kürzer oder simpler diese Phrase ist, desto schneller bekommt ein Hacker Zugriff auf das geschützte Netzwerk. Eine lange Phrase mit zufälligen Buchstaben, Zeichen und Zahlen, dürfte zumindest nicht zu erraten sein.

WLAN-Authentifizierung

Open System

Bei dieser Authentifizierung kann sich jede mobile Station mit einem WLAN-Access-Point verbinden, wenn die SSID miteinander übereinstimmen. Einige WLAN-Clients kenne die Option ALLE oder ANY, mit der unabhängig von der SSID mit jedem Access Point eine Verbindung hergestellt werden kann. Vorausgesetzt er ist als "Open System"

konfiguriert.

1. Die mobile Station schickt eine Authentifizierungsanforderung an den Access Point.

2. Der Access-Point überprüft die Identität der Station.

3. Die mobile Station stellt eine Verbindung zum Access-Point her.

Shared Key

Bei dieser Authentifizierung muss der Access-Point und die mobile Station über den gleichen WPA2-Passwort verfügen. Stimmt das Passwort mit dem eingestellten Passwort nicht überein,

dann verweigert der Access Point die Authentifizierung der Station. Eine Verbindung kann dann nicht aufgebaut werden.

Auto

Die Einstellung ist nicht eindeutig. Die

kann je nach Hersteller oder Access Point andere Auswirkungen haben. Die Einstellung der Authentifizierung ist in der Regel nicht mit dem setzen der Option getan. Es müssen noch Angaben zur Verschlüsselung, dem Code und evt. zur Verschlüsselungsstärke gemacht werden.

802.1x / Radius

Die Authentifizierung mit 802.1x erfordert einen Radius-Server.

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 und 500 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 (2 bis 68 MHz). Im praktischen Einsatz erreichen HomePlug-AV2-Adapter damit bis zu 150 MBit/s auf der Stromleitung.

Gigabit-Powerline (Gigle-Technik)

In den 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.

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.

Kritik an HomePlug-Powerline

Dadurch, dass Stromkabel und Steckdosen ungeschirmt sind, wirken sie wie Antennen. Wird dem Stromkabel ein hochfrequentes Signal aufmoduliert, dann senden die Kabel und Steckdosen elektromagnetische Signale aus. Da sich das Senden dieser Signale nicht verhindern lässt, gibt es vom Gesetzgeber Normen in denen Grenzwerte definiert sind. Solange die elektromagnetischen Signale unterhalb der Grenzwerte bleiben, gelten die Signale als unproblematisch. Dabei muss man berücksichtigen, dass jedes

elektrische Gerät elektromagnetische Strahlen sendet und das auch darf, solange die "Elektromagnetischen Verträglichkeit (EMV)" eingehalten wird.
Insbesondere Funkdienste, wie zum Beispiel Kurzwellenrundfunk, Amateurfunk und der NATO-Funk können durch die Abstrahlung der Powerline-Technik gestört werden. Das elektromagnetische Signal der Powerline-Adapter strahlt in diese Frequenzbereiche hinein. Damit die Powerline-Adapter bestimmte Frequenzen nicht stören können, sind unterhalb von 30 MHz ein paar Frequenzblöcke ausgespart.
Aber auch normale Geräte, die per Funk übertragen können durch die Abstrahlung der Powerline-Adapter gestört werden. So zum Beispiel drahtlose Mäuse und Tastaturen. Allerdings sind die

Störmeldungen, die sich auf Powerline-Adapter zurückführen lassen sehr gering. Bei einer Störungsmeldung prüft der Prüf- und Messdienst (PMD) der Bundesnetzagentur die Einhaltung der Grenzwerte des HomePlug-Systems. Bei einer Überschreitung erfolgt im Regelfall zunächst die Aufforderung an den Betreiber zur Nachbesserung, also Einhaltung der Grenzwerte. In der Regel bleibt dem HomePlug-Nutzer keine andere Möglichkeit, seine HomePlug-Powerline-Adapter wegen Überschreitung der Grenzwerte abzuschalten.

Höchstgeschwindigkeit nur bei optimalen Voraussetzungen

Den höchstmöglichen Datendurchsatz erreichen die Adapter, wenn sie direkt in die Wandsteckdose eingesteckt sind. Sie sollten keinesfalls mit anderen

Verbrauchern in Steckdosenleisten zusammen sein. Billige Ladegeräte und Netzteile von Kleingeräten erzeugen hochfrequente Störungen im Stromnetz, die das Powerline-Signal beeinträchtigen. Deshalb sollte man davon so wenig wie möglich betreiben oder ausgesteckt lassen, wenn man diese Netzteile gerade nicht braucht.

Wenn man sie über Verlängerungen oder Mehrfachsteckdosen betreibt muss man mit geringerem Durchsatz rechnen. Wem es an Wandsteckdosen mangelt kann auch auf Adapter zurückgreifen, die den Stromanschluss durchführen. Die kosten nur wenig mehr.

Die Übertragungsgeschwindigkeit ist unter anderem auch von der Elektroinstallation abhängig. Bei mangelhafter Ausführung kann schon innerhalb eines Zimmers die Übertragungsrate deutlich runter gehen.

Ungünstig ist es, wenn auch der Nachbar Powerline-Adapter in Betrieb hat. Dann sinkt der Datendurchsatz bei beiden Powerline-Netzen.

Eine hohen Übertragungsgeschwindigkeiten erreicht man mit Powerline nur auf kurzen Distanzen. Doch genau dann macht Powerline eigentlich keinen Sinn. Denn hier lässt sich gleich ein normales Netzwerkkabel verlegen. Das ist bei der Anschaffung günstiger und spart Stromkosten.

Stromkosten

Klar, wenn die Powerline-Adapter direkt am Stromnetz hängen, dann verbrauchen Sie auch Strom. Und das nicht zu knapp. Natürlich haben die Powerline-Adapter auch einen Stromsparmodus, der dann greift, wenn das am Adapter angeschlossene Gerät seine Ethernet-Schnittstelle abschaltet.

Trotzdem dürfte ein Powerline-Pärchen die Stromrechnung jährlich um ca. 15 Euro zusätzlich belasten.

Sicherheit

Powerline auf Stromleitungen ist ein shared Medium. Das bedeutet, alle die am Stromnetz dranhängen, können sich am Powerline-Netz beteiligen. Das gilt in der Regel fürs ganze Haus, in dem Powerline-Adapter betrieben werden. Häufig liest man, dass Powerline-Adapter nicht über Stromzähler hinweg miteinander kommunizieren können. Doch das stimmt nicht. Das Powerline-Signal breitet sich auch über Stromzähler aus. Das bedeutet, dass ein Nachbar das Powerline-Signal abgreifen kann.

Zukünftige Entwicklung

Ein weitere Steigerung der Übertragungsrate durch ein noch breiteres Frequenzspektrum ist eher

unwahrscheinlich. Die ITU will die obere Frequenz auf 80 MHz begrenzen. Um die Übertragungsrate weiter zu steigern wird über eine Art MIMO-Technik wie bei WLAN nachgedacht. Das bedeutet, man möchte unterschiedliche Signale in die Stromleitungen einspeisen. Da sich die Signale aber zwischen den Adern überkoppeln und somit vermischen, dürfte die Übertragungsrate nur etwas mehr, aber nicht doppelt so hoch steigen.

MPLS - Multi-Protocol Label Switching

Multi-Protocol Label Switching kombiniert die Vorteile von Switching mit Routing.
MPLS arbeitet zwischen den Schichten 2 und 3 des OSI-Schichtenmodells. Es baut sich also als Zwischenschicht ein.
Ein Beispiel für Schicht 2 ist das

Ethernet. Auf dieser Schicht werden die Frames (Datenpakete) geswitched. Ein Beispiel für Schicht 3 ist das Internet Protocol (IP). Auf dieser Schicht werden die Datenpakete geroutet. MPLS eignet sich um Datenpakete in einem IP-Netz priorisiert zu routen.

Wie war das noch mal mit dem Routing?

Router haben die Aufgabe, für Datenpakete anhand ihrer Zieladresse die Route an das Ziel zu bestimmen und es an den nächsten zuständigen Router weiterzuleiten. Zu diesem Zweck führt der Router intern sehr umfangreiche Tabellen von bekannten Netzen und den zuständigen Routern. Der Router muss für jedes eingehende Datenpaket die Tabellen durchlaufen und die Route heraussuchen, die am besten geeignet ist. Nicht immer ist die erstbeste Route geeignet. Deshalb werden die Tabellen

jedes mal komplett abgearbeitet.

Erschwerend ist, dass nicht jeder Router einen Überblick über das gesamte Routing hat. Das wäre auch weniger sinnvoll. Routen können sich ändern. Es wäre ein aufwendiger Abgleichvorgang zwischen allen Routern notwendig.

Wie funktioniert MPLS?

Statt für jedes Datenpaket in jedem Router die Route neu zu ermitteln, wird pro Route ein Label vergeben. Router analysieren die Zieladresse der Datenpakete und ermitteln dann, welche Route dazu am besten passt. Diese Entscheidung wird nur einmal, beim Eingang in das Netzwerk, getroffen. Dabei wird dem Datenpaket ein Label zugewiesen. Durch das Label wird festgelegt, welchen Weg dieses und alle weiteren Pakete nehmen sollen. Auf diese Weise entstehen Tunnel durch das Netzwerk.

In dem Label sind Routing- und Service-Informationen enthalten. MPLS-Router lesen diesen Header aus und leiten die Pakete in Abhängigkeit der Angaben weiter. Auf diese Weise kann man die MPLS-Router anweisen die Datenpakete immer über die gleiche Wegstrecke zu übertragen.

Kommt also ein Datenpaket mit MPLS-Header, nimmt sich der Router das Label aus dem MPLS-Header und vergleicht es mit seiner Label-Tabelle. Dort steht drin, welches Interface als Ausgang genommen werden muss. Gleichzeitig wird dem Datenpaket ein neues Label übergeben und dann an den nächsten Router übermittelt.

Hat ein Datenpaket keinen MPLS-Header wird der zuständige Router ermittelt und von diesem ein Label für die Ziel-IP des Paketes angefordert. Im MPLS-Header wird das Label dann

eingetragen und an den Router weitergeleitet.

Das Protokoll, mit dem Router die Label beantragen und Änderungen bekannt geben, nennt sich Label Distribution Protocol (LDP). Über BGP (Border Gatway Protocol) lassen sich Label auch austauschen. BGP wird bereits als Protokoll zwischen den Routern benutzt, mit dem sie ihre Routingtabellen miteinander austauschen.

Welche Vorteile bietet MPLS?

MPLS-Router haben den Vorteil, dass sie nur noch das Label im MPLS-Header betrachten müssen. Dadurch wird das Protokoll auf Schicht 3 austauschbar. Für das Routing mit MPLS spielt es keine Rolle mehr. Deshalb können MPLS-Router auch automatisch IPv6 routen.

Außerdem unterstützt MPLS Quality-of-

Service (QoS). Pakete mit höherer Priorität bekommen ein anderes Label mit dem die Route schneller zum Ziel führt. So ist es möglich Quality-of-Service-Parameter zu definieren. Zum Beispiel Transit Delay (Übertragungsverzögerung) und Packet Loss (Paketverlust). Der MPLS-Header besteht aus dem Label für das Forwarding, dem Class-of-Service-Feld (CoS) zur Unterscheidung von Dienste-Klassen, dem Bottom-of-Stack-Feld (S) und dem Time-to-Live-Feld (TTL). Weiterhin bietet MPLS ein Feature namens Label Stack. An einem Datenpaket können gleichzeitig mehrere Label angehängt werden. Geht bei einem Router ein solches Paket ein, dann verwirft er das erste Label und lässt das nächste nachrutschen. Dadurch wird die Route eines Datenpakets schon von Anfang an festgelegt. Normalerweise ist

das nicht sinnvoll, da sich Routen ändern oder kurzfristig ausfallen können. Handelt es sich dabei aber um ein Paket einer VPN-Verbindung, ist es besser, das Datenpaket kommt nicht beim Empfänger an, anstatt das es über eine unsichere Backup-Route weitergeleitet wird. Sofern man der Route hinsichtlich ihrer Sicherheit und Stabilität genug Vertrauen entgegen bringt, kann man dann auch auf die aufwendige und Performance-fressende Verschlüsselung verzichten. Was allerdings nicht zu empfehlen ist.

Wo sind MPLS-Router im Einsatz?

Die sogenannte Routing-Performance von Routern ist nur bei extrem hohen Bandbreiten mit z. B. Multi-Gigabit-Glasfaserstrecken der Carrier ein Problem. Hier bringt MPLS einen direkt sichtbaren Vorteil, um den

Geschwindigkeitsengpässe für ein paar Jahre weiter in die Ferne zu verschieben. Im Endkunden-Bereich mit typischen Dialup-Geräten über die analoge Telefonleitung oder ISDN spielt MPLS jetzt und in Zukunft keine Rolle. Aber wenn sich Breitband-Internet-Zugänge ohne Ausnahmen auf der ganzen Linie durchsetzen, dann ist MPLS-Routing gegenüber IP-Routing eine Ernst zunehmende Alternative.

T-MPLS - Transport Multiprotocol Label Switching

T-MPLS ist eine Weiterentwicklung von MPLS mit einer geringeren Komplexität und ein offener Standard der IETF. T-MPLS fließt zusätzlich in die ITU-T-Empfehlungen mit ein.

Eine Alternative zu MPLS und T-MPLS ist PBB-TE.

Quality of Service

RSVP - Resource Reservation Protocol

IEEE 802.1q / VLAN - Virtual Local Area Network

Priorisierung und Queuing

TCP/IP

IP - Internet Protocol Version 4

IP - Internet Protocol Version 6

TCP - Transmission Control Protocol

UDP - User Datagramm Protocol

TCP/IP

Zur Zeit des Kalten Krieges, in den 60er und 70er Jahren, entwickelten 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 Netzwerks verhindert werden.
1984 wurde das Projekt in einen militärischen und einen wissenschaftlichen Bereich aufgeteilt. Gleichzeitig wurde die TCP/IP-Protokollfamilie eingeführt.
TCP/IP ist die Abkürzung für Transmission Control Protocol und Internet Protocol. TCP/IP ist eine Protokoll-Kombination, die die Schichten Transport und Vermittlung aus dem OSI-Schichtenmodell verbindet.

Schicht

Dienste und Protokolle

Anwendung

Anwendungen

TCP - Transmission

Transport

Control Protocol

Internet

IP - Internet Protocol

Netzzugang

Übertragungssystem

Das Internet Protocol (IP) ist auf der Vermittlungsschicht (3. Schicht) des OSI-Schichtenmodells angeordnet. Das Transmission Control Protocol (TCP) ist auf der Transportschicht (4. Schicht) des OSI-Schichtenmodells angeordnet.

Das Aufkommen des Internets hat zu einem ungeahnten Erfolg für TCP/IP verholfen. Es ist damit weltweit der Netzwerkstandard im LAN (Local Area Network) und im WAN (Wide Area Network).

Vorteile von TCP/IP

TCP/IP hat mehrere entscheidende Vorteile. Jede Anwendung, ist mit

TCP/IP in der Lage über jedes Übertragungssystem Daten zu übertragen und auszutauschen. Dabei ist es egal, wo sich die Kommunikationspartner befinden. IP sorgt dafür, dass das Datenpaket sein Ziel erreicht und TCP kontrolliert die Datenübertragung und stellt den Datenstrom der Anwendung zu. Das bedeutet, TCP/IP ist an keinen Hersteller und kein Übertragungssystem gebunden.

TCP/IP ist 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 Datenpaket. Nur wenn Datenpakete von mehreren kByte gebildet werden, hält sich der Verwaltungsanteil im Vergleich zu den Nutzdaten gering.

TCP - Transmission Control Protocol

In der TCP/IP-Protokollfamilie übernimmt TCP, als verbindungsorientiertes Protokoll, die Aufgabe der Datensicherheit, der Datenflusssteuerung und ergreift Maßnahmen bei einem Datenverlust. Die

Funktionsweise von TCP besteht darin, den Datenstrom von den Anwendungen aufzuteilen, mit einem Header zu versehen und an das Internet Protocol (IP) zu übergeben. Beim Empfänger werden die Datenpakete sortiert und wieder zusammengesetzt.

Jedem Datenpaket, das TCP verschickt, wird ein Header vorangestellt, der die folgenden Daten enthält:

Sender-Port

Empfänger-Port

Paket-Reihenfolge (Nummer)

Prüfsumme

Quittierungsnummer

Datenpakete, die über IP ihr Ziel erreichen, werden von TCP zusammengesetzt und über die Port-Nummer an eine Anwendung übergeben. Dieser Port wird ständig von einem Prozess, Dienst oder einer Anwendung abgehört. Die Port-Nummer 1 bis 1023

sind jeweils einer Anwendung oder einem Dienst fest zugeordnet. Alle anderen Port-Nummern können frei belegt werden, sofern sie gerade von keinem anderen Dienst belegt sind. Durch die Port-Struktur ist es möglich, dass mehrere Anwendungen gleichzeitig über das Netzwerk Verbindungen zu Kommunikationspartnern aufbauen können.

IP - Internet Protocol

Das Internet Protocol, kurz IP, wird im Zusammenhang mit der Protokollfamilie TCP/IP genannt und verwendet. Es hat maßgeblich die Aufgabe, Datenpakete zu adressieren und in einem verbindungslosen paketorientierten Netzwerk zu vermitteln (Routing). Dazu haben alle Stationen und Endgeräte eine eigene Adresse im Netzwerk. Sie dient nicht nur zur Identifikation, sondern auch zum Erkennen eines Teilnetzes, in dem

sich eine Station befindet.

Jedes Datenpaket, das mit IP verschickt

wird, wird ein Header vorangestellt, der

die folgenden Daten enthält.

IP-Version

Paketlänge

Lebenszeit

Prüfsumme

Senderadresse

Empfängeradresse

Die IP-Adresse nach IP Version 4 ist 32

Bit groß/lang. Sie besteht aus 4 Byte und

wird durch Punkte voneinander getrennt.

Jedes Byte kann einen Wert von 0 bis

255 annehmen (z. B. 127.0.0.1).

IPv6-Adressen bestehen aus 128 Bit und

werden als Kette von 16-Bit-Zahlen in

Hexadezimalform getrennt durch einen

Doppelpunkt (":") dargestellt. Folgen von Nullen können einmalig durch einen

doppelten Doppelpunkt ("::") abgekürzt werden. Da in URLs der Doppelpunkt

mit der optionalen Portangabe kollidiert,

werden IPv6-Adressen in eckige Klammern gesetzt.

Adresse nach

IPv4 127.0.0.1

IPv6 FE80::0211:22FF:FE33:4455

IPv6- http://[FE80::0211:22FF:FE33:4455]:80/

URL

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 3. Schicht des OSI-Schichtenmodells und hat maßgeblich die Aufgabe, Datenpakete zu adressieren und in einem verbindungslosen paketorientierten Netzwerk zu vermitteln (Routing). Dazu haben alle Stationen und Endgeräte eine eigene Adresse im Netzwerk. Sie dient nicht nur zur Identifikation der Station, sondern auch des Netzes, in der sich die

Station befindet.

Das Internet Protocol (IP)

im TCP/IP-Protokollstapel

Dienste / Protokolle /

Schicht

Anwendungen

Anwendung HTTP IMAP DNS SNMP

Transport

TCP

UDP

Internet

IP (IPv4 / IPv6)

Netzzugang

Ethernet, ...

IP-Adressen nach IPv4

Hauptbestandteil von Internet Protocol (IP) sind die IP-Adressen, die alle Stationen in einem Netzwerk eindeutig kenntlich machen. Pro Hardware-Interface (Netzwerkkarte) wird eine IP-Adresse vergeben. In Ausnahmefällen lässt sich ein Interface auch über zwei

oder mehr IP-Adressen ansprechen oder mehrere Interfaces der gleichen Station haben die gleiche IP-Adresse.
Die IP-Adresse ist mit den Angaben zu Straße, Hausnummer und Ort einer Anschrift vergleichbar. Damit die IP-Adresse von Hardware und Software einfach verarbeitet werden kann, liegt sie in einem Bitcode (Duales Zahlensystem) vor. Der Bitcode ist 32 Stellen lang und kann wahlweise auch als hexadezimale oder dezimale Zahlenkombination dargestellt werden.

Zahlensystem Beispiel-Adresse

0111 0000 0000 0000

Binär/Dual

1111 0000 0000 0001

Hexadezimal

7F

00

00

01

Dezimal

127

0

0

1

Die typische Darstellung entspricht dem dualen Zahlensystem. Sie ist am einfachsten lesbar. Dazu wird der 32-Bitcode in jeweils 8 Bit (1 Byte) aufgeteilt und durch einen Punkt getrennt. Jedes Byte kann durch die achtstellige 1er- und 0er-Folge einen Wert von 0 bis 255 annehmen. Das sind 256 Werte pro Stelle. Die binäre IP-Adresse 01111111.00000000.00000000.00000001 ergibt umgerechnet in das dezimale Zahlensystem 127.0.0.1.

Subnetzmaske / Subnetmask

Das oben genannte Beispiel ergibt die IP-Adresse 127.0.0.1. Bei der Konfiguration von TCP/IP wird eine vergleichbare IP-Adresse verwendet.

Jede IP-Adresse besteht aus zwei Teilen. Jedes Teil hat eine bestimmte Bedeutung. Der vordere Teil ist die Adresse für das Netzwerk, indem sich die Station befindet. Der hintere Teil ist die Adresse für die Netzwerk-Station. Wo sich die IP-Adresse teilt, wird von der Subnetzmaske bzw. Subnetmask (engl.) bestimmt. Die Subnetzmaske besteht aus 32 Bit und 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 Teilung in eine Netz-Adresse und eine Stations-Adresse.

IP-Adresse

127.

0.

0. 1

Subnetzmaske

255. 255. 255. 0

Netz-Adresse

127.

0.

0. 0

Stations-Adresse

1

Der vordere Teil, die Netz-Adresse,

lautet 127.0.0.0. Der hintere Teil, die

Stations-Adresse, lautet 1.

Gültige

Ungültige

Subnetzmasken

Subnetzmasken

255.255.255. 0 250.255.255. 0

255.255. 0. 0 255.255. 0.255

255. 0. 0. 0 255. 0.255.255

255.255.255.252 255. 0. 0.255

255.255.255.128 255.255.255.200

Netz-Klassen

Die IP-Adressen werden in 5 Klassen eingeteilt. In jeder Klasse haben die Netz-ID und die Host-ID eine unterschiedliche Gewichtung.
Klasse-A-Netze sind Netze mit einer großen Anzahl an Stationen oder Subnetze. Das erste Bit ist immer "0". Der theoretische Adressbereich reicht von 0.0.0.0 bis 127.255.255.255. Der effektive Adressbereich reicht von 1.0.0.1 bis 127.255.255.254. Insgesamt sind also nur 126 Klasse-A-Netze möglich. Das ergibt eine rechnerische Anzahl von 16.777.214 möglichen Stationen pro Klasse-A-Netz.
Klasse-B-Netze sind Netze mit einer mittleren Anzahl an Stationen oder Subnetzen. Die ersten 2 Bit sind immer "10". Der theoretische Adressbereich reicht von 128.0.0.0 bis 191.255.255.255. Der effektive Adressbereich reicht von 128.0.0.1 bis 191.255.255.254. Insgesamt sind nur

16.384 Klasse-B-Netze möglich. Das ergibt eine rechnerische Anzahl von 65.534 mögliche Stationen pro Klasse-B-Netz.

Klasse-C-Netze sind Netze mit einer kleinen Anzahl an Stationen. Jedes Klasse-C-Netz ist gleichzeitig ein Subnetz. Eher selten wird es noch mal in mehrere Subnetze unterteilt. Die ersten 3 Bit des Adressbereiches sind immer "110". Der theoretische Adressbereich reicht von 192.0.0.0 bis 223.255.255.255. Der effektive Adressbereich reicht nur von 192.0.0.1 bis 223.255.255.254. Insgesamt sind 2.097.152 Klasse-C-Netze möglich. Das ergibt eine rechnerische Anzahl von 254 Stationen pro Klasse-C-Netz.

Klasse A (0.0.0.0 bis 127.255.255.255)

0 Netz-ID

Host-ID (24 Bit)

(7 Bit)

Klasse B (128.0.0.0 bis

191.255.255.255)

Netz-ID

1 0

Host-ID (16 Bit)

(14 Bit)

Klasse C (192.0.0.0 bis

223.255.255.255)

Netz-ID

1 1 0

Host-ID (8 Bit)

(21 Bit)

Klasse D (224.0.0.0 bis

239.255.255.255)

Multicast-Gruppen-ID (28

1 1 1 0

Bit)

Klasse E (240.0.0.0 bis

255.255.255.255)

1 1 1 1

0

Reserviert für zukünftige

Anwendungen (27 Bit)

IP-Adressen mit

besonderem Status

Die IP-Adresse 127.0.0.1 aus den oberen Beispielen ist die lokale IP-Adresse einer jeden Station. Diese IP-Adresse wird auch als Localhost (Name-Auflösung: localhost) bezeichnet, die einem virtuellen Interface, also keiner Hardware zugeordnet ist.
Wird ein Datenpaket mit der Ziel-Adresse 127.0.0.1 verschickt, so wird sie an den Absender selber verschickt. Man spricht dann vom einem Echo. Diese IP-Adresse macht im normalen Netzbetrieb nicht wirklich Sinn. Allerdings kann sie zum Testen verwendet werden. Zum Beispiel, ob TCP/IP korrekt installiert und konfiguriert ist. Das gilt für alle IP-Adressen im Bereich 127.0.0.0 bis

127.255.255.255.

Eine IP-Adresse, deren letzte Stelle eine 0 ist, ist keine gültige IP-Adresse (z. B. 127.0.0.0). Es handelt sich dabei um die Adresse eines Subnetzes.

Eine IP-Adresse, deren letzte Stelle die Nummer 255 ist (z. B. 127.0.0.255) ist ebenso keine gültige IP-Adresse. Es ist eine Broadcast-Adresse für das Netz 127.0.0.0. Die Datenpakete mit dieser Zieladresse werden in diesem Netz an alle Stationen geschickt.

Durch die Einschränkung von 0 bis 255 hat ein Subnetz 256 Adressen, aber mit der Adresse x.x.x.0 und der Subnetzmaske von 255.255.255.0 nur maximal 254 mögliche adressierbare Stationen.

Weitere Adressbereich sind

privaten Netzen zugeordnet. Diese IP-Adressen dürfen nicht im Internet zur Adressierung verwendet werden.

Private IP-Adressräume

Klasse Von

Bis

Subnetzmaske

Klasse-

10.0.0.0 10.255.255.255

A-Netz

Klasse-

B-

172.16.0.0 172.31.255.255

Netze

Klasse-

C-

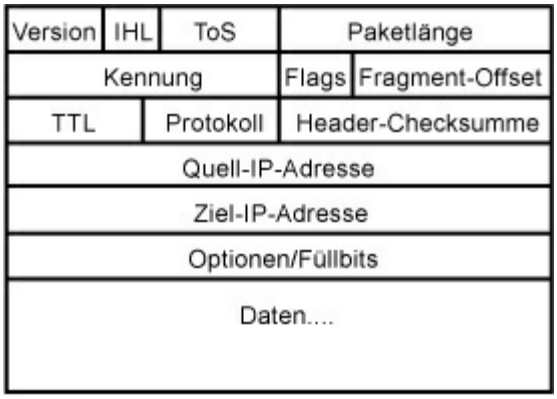
192.168.0.0 192.168.255.255 255.255.255.0

Netze

Die Verwaltung von IP-Adressen unterliegt einer zentralen Organisation, dem Network Information Center (NIC).

Will man sich mit dem Internet verbinden, benötigt man eine feste IP-Adresse, einen IP-Adressraum oder eine dynamisch von einem Provider zugewiesene IP-Adresse. Für kleine oder große private Netze gibt es Adressräume, die im Internet nicht verwendet werden dürfen, aber, innerhalb von privaten Netzen frei zur Verfügung stehen.
Für ein privates Klasse-A-Netz dürfen die Adressen von 10.0.0.0 bis 10.255.255.255 genutzt werden. Private Klasse-B-Netze befinden sich in dem Adressbereich 172.16.0.0 bis 172.31.255.255. Für private Klasse-C-Netze gibt es den Adressbereich von 192.168.0.0 bis 192.168.255.255. Letzterer wird gerne in kleinen privaten Netzen verwendet.

Aufbau des IPv4-Headers



Das IP-Datenpaket besteht aus einem Header (Kopf) und dem Bereich, in dem sich die Nutzdaten befinden. Der Header ist den Nutzdaten vorangestellt.
Der Header ist in jeweils 32-Bit-Blöcke unterteilt. Dort sind Angaben zu Servicetypen, Paketlänge, Sender- und Empfängeradresse abgelegt. Ein IP-Paket muss mindestens 20 Byte Header und 8 Byte Nutzdaten bzw. Nutz- und Fülldaten enthalten. Die Gesamtlänge eines IP-Pakets darf 65.535 Byte nicht überschreiten. Je nach Datenmenge und Übertragungsverfahren auf der Bitübertragungsschicht müssen die Nutzdaten in mehrere IP-Pakete aufgeteilt werden. Diesen Vorgang nennt

man Fragmentierung.

Der Begriff Fragmentierung ist auch von Dateisystemen und Festplatten bekannt.

IPv6 - Internet

Protocol Version 6

IPv6 ist als Internet Protocol (Version 6) für die Vermittlung von Daten durch ein paketvermittelndes Netz, die Adressierung von Netzknoten und -stationen, sowie die Weiterleitung von Datenpaketen zwischen Teilnetzen (Routing) zuständig. Mit diesen Aufgaben ist IPv6 der Schicht 3 des OSI-Schichtenmodells zugeordnet.

IPv6 ist der direkte Nachfolger von IPv4 und Teil der Protokollfamilie TCP/IP.

Der Grund für die Einführung des Internet Protocols Version 6 (IPv6) und Ablösung von IPv4 ist die Adressknappheit von nur 4 Milliarden IP-Adressen (Version 4), die bald aufgebraucht sind. Da weltweit immer

mehr Menschen, Maschinen und Geräte an das Internet mit einer eindeutigen Adresse angeschlossen werden wollen, reichen die IPv4-Adressen nicht mehr lange aus.

Internet Protocol Version 5?

IPv5 hieß offiziell ST-2 (Internet Stream Protocol Version 2) und war ein experimentelles Protokoll für Echtzeit-Datenströme. ST-2 wurde von RSVP (Resource Reservation Protocol) zur Bandbreitenanforderung bei Routern abgelöst. 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.

IP-Adressen nach IPv6

Die nächste Generation von IP, das IP

Version 6, erhöht den Adressumfang auf

2128. Damit wäre es möglich, jeden

Quadratmillimeter der Erde mit rund

600 Billionen Adressen zu belegen.

Doch nicht nur das, obendrein soll IPv6

Erleichterung bei der

Rechnerkonfiguration und Betrieb

bringen.

IPv6-Adressen bestehen aus 128 Bit.

Wegen dieser unhandlichen Länge hat

man sich für Hexadezimalzahlen als

Schreibweise entschieden. 16 Bit sind

jeweils durch einen Doppelpunkt (":") getrennt. Führende Nullen können in den

Blöcken wegfallen. Eine Folge von

Nullen kann man durch zwei

Doppelpunkte ("::") ersetzen. Da in URLs der Doppelpunkt mit der

Portangabe kollidiert, sind IPv6-

Adressen in eckige Klammern gesetzt.

Die Netzwerkmasken fallen ersatzlos

weg. Den Adressbereich bzw. das

Subnetz hängt man an und trennt ihn vom

Rest der Adresse durch ein "/". In IPv6 adressieren die ersten 64 Bit das Netz und die restlichen 64 Bit den Host.

Adresse nach

IPv4 127.0.0.1

IPv6 FE80:0000:0000:0211:020C:F1FF:FE8E:C1D8

IPv6- http://[FE80:0000:0000:0211:020C:F1FF:FE8E:C1D8]:80/

URL

Aufteilung des IPv6-

Adressraums

Man unterscheidet grob gesehen zwischen globalen Adressen (Global Scope) und lokalen Adressen (Local Scope). Pakete mit globale Adressen werden außerhalb des lokalen Netzwerks geroutet. Link-lokale Adressen sind nur innerhalb des lokalen Netzwerks gültig. Sie werden nicht extern, sondern nur intern geroutet. Hinter Link-Local Scope stecken Mechanismen wie Neighbor Discovery, das das Address Resolution Protocol

(ARP) ablöst oder Stateless Address Autoconfiguration (SAC oder SAA) als Alternative zu DHCP. Neighbor Discovery zeichnet sich vor allem durch Unabhängigkeit von der Übertragungstechnik aus.

Für private lokale Netze gibt es in IPv6 reservierte Adressbereiche (Unique Local Adressses, ULA). Sie haben eine ähnliche Funktion, wie die lokalen IPv4-Adressen. Die privaten IPv6-Adressen sind weltweit eindeutig, werden aber nicht geroutet.

Adressvergabe und Autokonfiguration

IPv6 kennt zwei verschiedene Wege, wie Clients an ihre eigene IP-Adresse kommen. Entweder über DHCPv6 oder Autokonfiguration. Letzteres hat den Nachteil, das damit nur die Kommunikation im lokalen Netz möglich ist. Standard-Gateway und DNS-Server

müssen immer noch manuell konfiguriert werden oder per DHCPv6 abgefragt werden.

Stateful Address Configuration (DHCPv6)

Stateless Address Configuration (Autokonfiguration)

Anders als bei IPv4 müssen die IP-Adressen im lokalen Netzwerk nicht zentral vergeben werden. Die Adressvergabe erfolgt automatisch und die Stationen prüfen selbständig, ob ihre Adresse im Netz schon vergeben ist. Unter IPv6 gibt es keine Netzwerkmaske und Broadcast-Adressen mehr. Die Einrichtung eines Netzwerks ist dadurch viel einfacher.

Stateless Address Configuration

Wird eine Station mit IPv6 gestartet, dann weist sie sich als erstes eine lokale Adresse zu. Die ersten 64 Bit sind fest

vorgegeben. Davon bestehen die ersten 16 Bit aus dem Prefix "fe80". Die restlichen 48 Bit werden mit Nullen aufgefüllt. Die zweiten 64 Bit werden als Suffix bezeichnet und bestehen aus der MAC-Adresse des Netzwerkadapters, die in das Nummerierungssystem EUI-64 des IEEE umgewandelt wird. Da MAC-Adressen in der Regel weltweit einmalig sind ist die lokale IP-Adresse es ebenso.
Bevor der PC diese Adresse nutzen kann, schickt er eine Anfrage ins lokale Netz (Neighbor Solicitation). Falls eine andere Station die Adresse bereits nutzt (Neighbor Advertisement), muss die IP-Adresse manuell umgeändert werden. In der Regel ist das nicht notwendig, weil jeder Netzwerkadapter in der Regel eine einmalig MAC-Adresse hat. Sollte doch einmal eine Doppelung vorkommen, dann sollte man das Netzwerk

überprüfen. Dann könnte es sein, dass jemand eine MAC-Adresse gekapert hat und per MAC-Spoofing ins Netzwerk eingedrungen ist.
Mit seiner lokalen Adresse kann die Station nur im lokalen Netzwerk kommunizieren. Für das Internet braucht sie eine zusätzliche Adresse, die sie sich ebenfalls selber generiert. Dazu muss die Station beim Standard-Gateway (Router) nachfragen, welche Netzwerk-Adresse sie verwenden soll (Präfix des öffentlichen Adressblocks). Mit der lokalen Adresse bittet (Solicitation Message) die Station auf der Multicast-Adresse "FF02::2" um den IPv6-Präfix. Der Router schickt daraufhin eine Ankündigung (Advertisement Message) mit einem Adress-Präfix für dieses Netzwerk und die Größe der Pakete (MTU). Aus dem Präfix und Suffix erzeugt die Station ihre öffentliche IPv6-

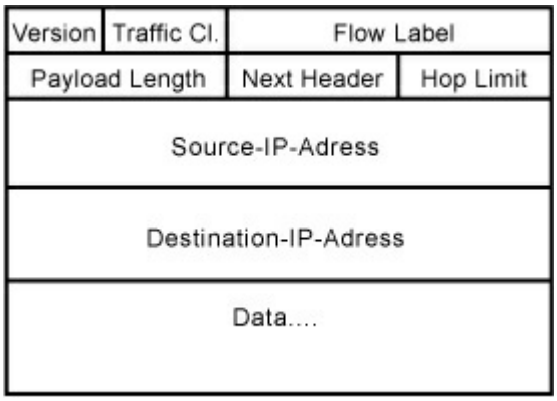
Adresse. Der Suffix ist eine EUI-64-Adresse, die aus der Hardware-Adresse (MAC-Adresse) erzeugt wird. Danach prüft die Station, ob diese Adresse im lokalen Netzwerk schon vergeben ist (Duplicate Address Detection). Wenn sie frei ist, weist sie die Adresse ihrer Netzwerkschnittstelle zu.

Die IP-Autokonfiguration ist allerdings nicht ganz vollständig. Es werden keine Adressen für DNS- oder NTP-Server erzeugt. Auch ein Hostname wird nicht zugewiesen. An diese Informationen kommt ein PC beispielsweise über Bonjour (Apple), PNRP (Microsoft) oder DHCPv6.

Privacy Extensions

Der Interface Identifier wird aus der MAC-Adresse errechnet. Weil die globale MAC-Adresse und die IPv6-Adressen durch den Interface Identifier nachverfolgbar ist wurden die Privacy

Extensions entwickelt. Damit wird ein Teil der Anonymität, wie es bei IPv4 möglich ist, wieder hergestellt werden, in dem die Kopplung von Interface Identifier und MAC-Adresse aufgehoben wird.
Privacy Extensions erzeugt ständig wechselnde Interface Identifiers, statt diesen aus der MAC-Adresse zu errechnen. Privacy Extensions erzeugt zusätzlich zu der festen IP-Adresse periodisch eine neue Adresse, bei der der hintere Teil verändert ist. Anschließend werden mit diesen



wechselnden Adressen ausgehende Verbindungen hergestellt. Auf diese Weise wird auf IP-Ebene die Erstellung

von Bewegungsprofilen verhindert.

Aufbau des IPv6-Headers

Zur weiteren Entlastung der Router wurde die Länge des IP-Headers fest definiert und die Adressfelder auf 64 Bit ausgerichtet (64 bit aligned). Dadurch findet der Router in jedem IPv6-Paket alles an der selben Stelle.

Obwohl der IPv6-Header weniger Felder als der IPv4-Header hat, ist er durch die längeren IPv6-Adressen trotzdem 40 Byte lang. Die Felder IHL, Type of Service, Kennung und Header-Checksumme wurden komplett gestrichen. Die Felder Fragment-Offset, Flags und Options sind in die optionalen Header-Erweiterungen verlagert.

Wechsel von IPv4 auf IPv6

Der Wechsel von IPv4 auf IPv6 in einem LAN gelingt in der Regel problemlos. In Windows XP/SP2, Windows Vista, Windows 7, MacOS und Linux ist IPv6

bereits enthalten. Einzig unter Windows XP muss IPv6 aktiviert werden. Eine Sache von nur wenigen Klicks.
Geräte, wie Hubs und Switche ist es egal ob IPv4 oder IPv6 zum Einsatz kommt. Sie kümmern sich um die Netzwerk-Kommunikation unterhalb des Internet Protokolls. Nur bei Routern stellt sich da noch ein Problem ein. Im Privat-Bereich gibt es so gut wie keine IPv6-Router. Eine "native" IPv6-Anbindung der DSL-Provider wäre ebenfalls nötig. Die ist jedoch bislang nicht in Sicht.

Änderungen gegenüber IPv4

IPv6 schafft die Adressknappheit und damit viele Netzwerkprobleme aus der Welt. IPv4 sieht nur 232 Adressen vor. Das sind rund 4,3 Milliarden IP-Adressen. IPv6 hat einen Adressraum von 2128. Das sind 340.282.366.900.000.000.000.000.000.000.000.000.000, also rund 340,28

Sextillionen Adressen.
Das 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. Der große Adressraum, also die hohe Anzahl an Präfixen, macht das Wegfallen von NAT möglich. Wobei das nicht bedeutet, dass es nicht doch irgendwann eine Implementierung für NAT in IPv6 geben wird.
Bei IPv6 hat man sich nicht nur um die Adresserweiterung gekümmert, sondern auch gleich eine Generalüberholung des Protokolls vorgenommen. Zählte zur Hauptaufgabe der heutigen IPv4-Routern das Prüfen von Checksummen und Fragmentieren von Daten, so ist die

Arbeit für IPv6-Router sinnvoll minimiert worden. IPv6 führt keine Prüfsumme mehr im Header mit. Stattdessen wird dem übergeordneten Transport-Protokoll TCP die Aufgabe überlassen, kaputte Pakete zu erkennen und neu anzufordern. Dieser Vorgang wird komplett beim Empfänger bearbeitet. Zu große Datenpakete werden von IPv6-Routern nicht mehr selber fragmentiert. Ist ein Paket zu groß wird dem Absender eine Fehlermeldung geschickt. Dieser muss dann die maximale Paketlänge (MTU - Maximum Transmissin Unit) anpassen. Dieses Verfahren nennt sich Path MTU Discovery und existiert in ähnlicher Form auch in IPv4. Dort muss im Datenpaket das Don't-Fragment-Flag (DF) gesetzt werden. War in IPv4 dieses Verfahren optional, ist es in IPv6 Pflicht. Kommt es zum Verlust eines

Datenpakets oder kommt es zu Fehlern bei der Fragmentierung, schlägt das Path MTU Discovery fehl. In IPv4 wurde der MTU dann auf 68 Byte abgesenkt. Das führte zu einer höheren Paketanzahl und einem unwirtschaftlichen Protokoll-Overhead. IPv6 hat als kleinste einstellbare MTU 1280 Byte. Dadurch werden die Router nicht mehr unnötig belastet. Selbstverständlich können auch kleinere Pakete als 1280 Byte übertragen werden.

IPv4-Router müssen Checksummen prüfen und Pakete fragmentieren. Das erfordert Rechenleistung und reduziert den Datendurchsatz. Um das Routing zu beschleunigen wird auf Fragmentierung und Checksummen verzichtet. Die Prüfsumme bleibt höheren Protokolle überlassen. Zum Beispiel TCP. Und für das Prüfen der Pakete auf IP-Ebene ist nur noch der Empfänger zuständig. Ist

ein Paket zu groß, wird es nicht mehr fragmentiert. Dafür wird es generell verworfen und der Sender per ICMP-Nachricht informiert. Der Sender setzt dann die maximale Paketgröße für diese Route herab (MTU, Maximal Transmission Unit).

Übersicht: Vorteile von IPv6

IP-Autokonfiguration anhand der MAC-Adresse der Netzwerkkarte

schnelleres Routing

Punkt-zu-Punkt-Verschlüsselung mit IPsec

gleiche Adresse in wechselnden Netzen

Multicast

Quality of Service

Datenpakete bis 4 GByte Größe

Vieles davon war auch mit IPv4 möglich. Doch dort wurde vieles erst nachträglich implementiert. IPv6 bringt

das alles integriert mit.

Privacy Extensions

(IPv6)

Privacy Extensions ist eine Erweiterung für IPv6, um IPv6-Adressen zu bilden, die keinen Rückschluss auf den Nutzer zulassen. Mit der Einführung von IPv6 ist die Angst um den Verlust der Privatsphäre gestiegen. Dahinter steckt die Vermutung, dass es mit IPv6 so viele Adresse gibt, dass jedem Nutzer eine Adresse lebenslang zugewiesen werden kann und er somit jederzeit identifizierbar ist. An dieser Stelle kommt die Frage auf, wie IPv6-Adressen gebildet werden?

Wie werden IPv6-Adressen

gebildet?

FE80:0000:0000:0211: 020C:F1FF:FE8E:C1D8

Interface Identifier (64

Präfix (64 Bit)

Bit)

IPv6-Adressen bestehen aus 128 Bit.

Die vorderen 64 Bit heißen Präfix.

Vereinfacht ausgedrückt, das ist die

Adresse des Netzwerks, in dem sich die

Station befindet. Der Präfix wird

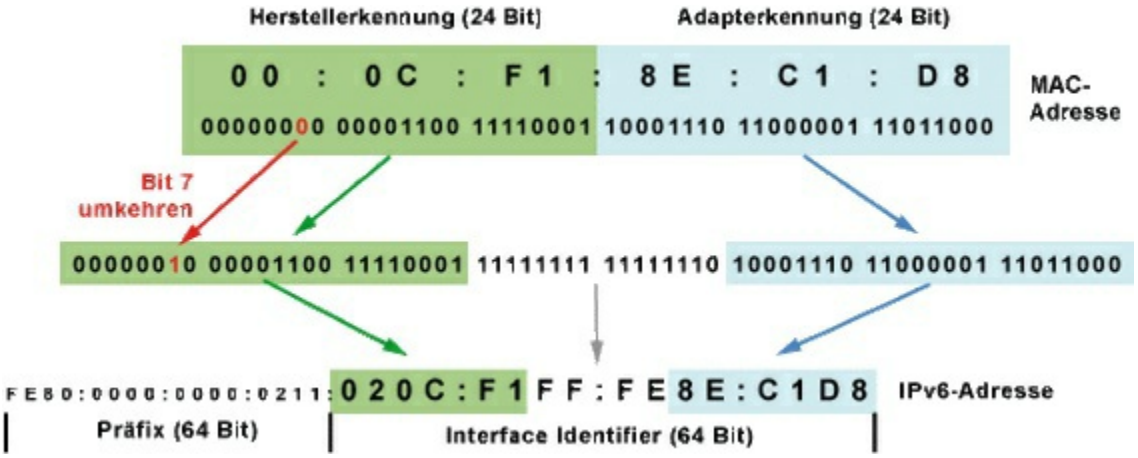
üblicherweise vom Provider

zugewiesen. Die hinteren 64 Bit werden

als Interface Identifier bezeichnet. Das

ist eine Adresse der

Netzwerkschnittstelle einer Station.



Die meisten Betriebssysteme erzeugen

einen Interface Identifier, der die MAC-

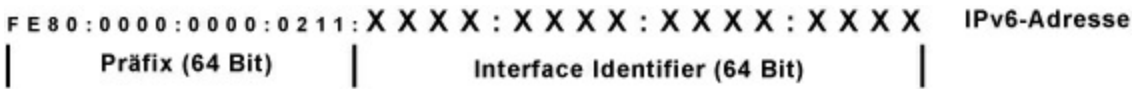
Adresse (Hardware-Adresse des

Netzwerkadapters) enthält. In der Mitte

der Hardware-Adresse wird zwei feste

Bytes (ff:fe) eingefügt. Das siebte Bit im

ersten Byte der MAC-Adresse wird umgekehrt. Aus der MAC-Adresse xxx



wird der Interface Identifier xxx. Eine gewissen Ähnlichkeit ist nicht zu übersehen. Das bedeutet, am Interface Identifier kann man eine bestimmte Station erkennen.

Mit Privacy Extensions die Privatsphäre schützen

Weil man mit dem üblichen Verfahren um eine IPv6-Adresse zu erzeugen eine bestimmte Station identifizieren kann, und das zu Bedenken bezüglich Datenschutz und Privatsphare führte, hat man "Privacy Extensions" eingeführt. Privacy Extensions erzeugen regelmäßig einen zufälligen Interface Identifier. Diese Adressen haben nur eine begrenzte Zeit Gültigkeit. Wenn Privacy Extension aktiv ist, dann kann eine IPv6-

Adresse über eine längere Zeit nicht zur Identifikation einer bestimmten Station benutzt werden.

Subnetting (Subnetmask / Subnetzmaske)

Die Aufteilung eines zusammenhängenden Adressraums von IP-Adressen in mehrere kleinere Adressräume nennt man Subnetting.
Ein Subnet, Subnetz bzw. Teilnetz ist ein physikalisches Segment eines Netzwerks, in dem IP-Adressen mit der gleichen Netzwerkadresse benutzt werden. Diese Teilnetze können mit Routern miteinander verbunden werden und bilden dann ein großes zusammenhängendes Netzwerk.

Warum Subnetting?

Wird die physikalische Netzstruktur bei der IP-Adressvergabe nicht berücksichtigt und die IP-Adressen

wahllos vergeben, müssen alle Router in diesem Netzwerk wissen in welchem Teilnetz sich eine Adresse befindet.
Oder sie leiten einfach alle Datenpakete weiter, in der Hoffnung, das Datenpaket kommt irgendwann am Ziel an. Dann müssen höhere Übertragungsprotokolle verloren geglaubte Datenpakete erneut anfordern bzw. senden. Das erhöht die Netzlast.
Kommt eine neue Station hinzu, dauert es sehr lange bis alle Router davon mitbekommen. Einzelne Stationen an den Rändern eines Netzwerkes laufen Gefahr nicht mehr erreichbar zu sein, weil am anderen Ende des Netzes ihre IP-Adresse nicht bekannt ist.
Um die Netzlast sinnvoll und geordnet zu verteilen, werden Netzwerke in Abhängigkeit der örtlichen Gegebenheiten und/oder nach organisatorischen Gesichtspunkten

aufgeteilt. Dabei wird auch berücksichtigt, wie viele Netzwerkstationen sich innerhalb eines Subnetz befinden.

Die Berücksichtigung der physikalischen Netzstruktur durch die gezielte Vergabe von IP-Adressen und damit eine logische Zusammenfassung mehrerer Stationen zu einem Subnetz reduziert die Routing-Informationen auf die Angabe der Netzwerk-Adresse. Die Netzwerk-Adresse gewährleistet den Standort einer IP-Adresse in einem bestimmten Subnetz. Ein Router benötigt dann nur noch die Routing-Information zu diesem Subnetz und nicht zu allen einzelnen Stationen in diesem Subnetz. Der letzte Router, der in das Ziel-Subnetz routet ist dann für die Zustellung des IP-Datenpakets verantwortlich.

Wie funktioniert Subnetting?

Jede IP-Adresse teilt sich in Netz-Adresse und Stations-Adresse. Die Subnetzmaske bestimmt, an welcher Stelle diese Trennung stattfindet. Die nachfolgende Tabelle enthält alle möglichen Subnetzmasken. Je nach verwendeter Netzwerk-Adresse und Subnetzmaske wird eine bestimmte Anzahl an Netzwerkstationen (Hosts) in einem Subnetz adressierbar.

32-

Hostanzahl Subnetzmaske

Bit- Präfix

Wert

1111

1111

0000

16.777.214

255.0.0.0 0000 /8

0000

0000

0000

0000

1111

1111

1000

0000

8.388.606

255.128.0.0

/9

0000

0000

0000

0000

1111

1111

1100

0000

4.194.302

255.192.0.0 0000 /10

0000

0000

0000

1111

1111

1110

0000

2.097.150

255.224.0.0

/11

0000

0000

0000

0000

1111

1111

1111

0000

1.048.574

255.240.0.0

/12

0000

0000

0000

0000

1111

1111

1111

1000

524.286

255.248.0.0 0000 /13

0000

0000

0000

1111

1111

1111

1111

1100

262.142

255.252.0.0

/14

0000

0000

0000

0000

1111

1111

1111

131.070

255.254.0.0 1110 /15

0000

0000

0000

0000

1111

1111

1111

1111

65.534

255.255.0.0

/16

0000

0000

0000

0000

1111

1111

1111

1111

32.766

255.255.128.0

/17

1000

0000

0000

0000

1111

1111

1111

1111

16.382

255.255.192.0

/18

1100

0000

0000

0000

1111

1111

1111

1111

8.190

255.255.224.0

/19

1110

0000

0000

0000

1111

1111

1111

1111

4.094

255.255.240.0

/20

1111

0000

0000

0000

1111

1111

1111

1111

2.046

255.255.248.0

/21

1111

1000

0000

0000

1111

1111

1111

1111

1.022

255.255.252.0

/22

1111

1100

0000

0000

1111

1111

1111

1111

510

255.255.254.0

/23

1111

1110

0000

0000

1111

1111

1111

254

255.255.255.0 1111 /24

1111

1111

0000

0000

1111

1111

1111

1111

126 255.255.255.128

/25

1111

1111

1000

0000

1111

1111

1111

1111

62 255.255.255.192 1111 /26

1111

1100

0000

1111

1111

1111

1111

30 255.255.255.224

/27

1111

1111

1110

0000

1111

1111

1111

1111

14 255.255.255.240

/28

1111

1111

1111

0000

1111

1111

1111

1111

6 255.255.255.248

/29

1111

1111

1111

1000

1111

1111

1111

1111

2 255.255.255.252

/30

1111

1111

1111

1100

Hinweis: Jeweils die erste und letzte IP-Adresse eines IP-Adressbereichs (z. B. 192.168.0.0 bis 192.168.0.255) kennzeichnen die Netzwerk-Adresse (192.168.0.0) und Broadcast-Adresse (192.168.0.255). Diese Adressen können keiner Station vergeben werden. Deshalb muss die Anzahl der IP-Adressen um zwei reduziert werden, damit man auf die richtige Anzahl nutzbarer IP-Adressen kommt.

Die 4 Dezimalzahlen jeder IP-Adresse entspricht einem 32-Bit-Wert. Die Subnetzmaske ist mit 32 Bit genauso lang, wie jede IP-Adresse. Jedes Bit der

Subnetzmaske ist einem Bit einer IP-Adresse zugeordnet. Die Subnetzmaske besteht aus einer zusammenhängenden Folge von 1 und 0. An der Stelle, wo die Subnetzmaske von 1 auf 0 umspringt trennt sich die IP-Adresse in Netz-Adresse und Stationsadresse.

Dezimal

Binär (Bit)

1100

IP-Adresse

192 .168

.0

.1 0000

1111

Subnetzmaske 255 .255 .255

.0 1111

Netzwerk-

1100

192 .168

.0

.0

Adresse

0000

0000

Stationsadresse

0

.0

.0

.1 0000

Broadcast-

1100

Adresse

192 .168

.0 .255 0000

Die Subnetzmaske wird also wie eine Schablone auf die IP-Adresse gelegt um die Netzwerk-Adresse und Stationsadresse herauszufinden. Die Informationen über die Netzwerk-Adresse ist wichtig bei der Zustellung eines IP-Datenpakets. Ist die Netzwerk-Adresse bei der Quell- und Ziel-Adresse gleich, wird das Datenpaket

innerhalb des gleichen Subnetzes zugestellt. Sind die Netzwerk-Adressen unterschiedlich muss das Datenpaket über das Standard-Gateway (Default-Gateway) in ein anderes Subnetz geroutet werden.

Schreibweise von IP-Adresse und Subnetzmaske

Es gibt zwei Formen der Schreibweise für die Subnetzmaske in Kombination mit der IP-Adresse.

IP-Adresse /

192.168.0.1 /

Subnetzmaske

255.255.255.0

IP-Adresse /

192.168.0.1 / 24

Präfix

Bei der ersten Schreibweise werden IP-Adresse und Subnetzmaske hintereinander geschrieben. Bei der zweiten Schreibweise wird statt der

Subnetzmaske der Präfix verwendet. Der Präfix nach der IP-Adresse gibt an, wie viele 1er innerhalb der Subnetzmaske in der Bit-Schreibweise nacheinander folgen. 24 bedeutet demnach 255.255.255.0. Weitere Präfixe sind in der Tabelle weiter oben nachzulesen.

Welche Subnetzmaske für welches Netz

Netzwerke werden in verschiedene Klassen eingeteilt. Je nach Klasse kann eine bestimmte Anzahl von Stationen adressiert werden.

Subnetzmaske Netz in Bit-Schreibweise	**Subnetzmaske**
1111 1111	
Klasse 0000 0000	255.0.0.0
A	

0000 0000

0000 0000

1111 1111

Klasse 1111 1111

255.255.0.0

B

0000 0000

0000 0000

1111 1111

Klasse 1111 1111

255.255.255.0

C

1111 1111

0000 0000

IP-Routing

Das Internet Protocol (IP) ist das wichtigste routingfähige Protokoll und aus keinem Netzwerk mehr weg zu denken. 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.

Was ist Routing?

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 Netzwerkstationen angeschlossen. Wenn eine Station Daten verschickt, dann werden die Daten im Hub an alle Stationen verschickt. Jedoch nimmt nur die adressierte Station die Daten entgegen. Das bedeutet, dass sich alle Stationen die Gesamtbandbreite dieses Hubs teilen (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 Stationen angeschlossen sind. Wollen nun zwei oder mehr Stationen gleichzeitig senden, kommt es zu einer

Kollision, die zu einer allgemeinen Sendepause auf dem Bus führt. Danach versuchen die Stationen erneut zu senden, bis die Übertragung erfolgreich war. Dieses Verfahren nennt man CSMA/CD. Die maximale Anzahl von Stationen an einem Ethernet-Bus ist 1024. Je mehr Stationen 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 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 ein Switch also nicht. Aus diesem Grund wird ein Netzwerk durch IP-Adressen in logische Segmente bzw. Subnetze unterteilt. Dazu dienen neben den IP-Adressen auch die Subnetzmaske. Sie teilen der Station mit, in welchem logischen Netzwerk sie sich befindet und welche Adresse sie hat. Die Adressierung durch das Internet Protocol ist so konzipiert, dass Stationen mit unterschiedlichen Subnetzmasken nicht einfach so kommunizieren können, obwohl es physikalisch durchaus

möglich wäre (gemeinsamer Hub/Switch). Stattdessen wird die Verbindung über einen oder mehrere Router hergestellt, die dafür sorgen, dass der Netzwerkverkehr innerhalb der Subnetze bleibt.

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 durch eine Firewall

Routing über Backup-Verbindungen bei Netzausfall

Vermeidung von Kollisionen und Broadcasts durch Begrenzung der Kollisions- und

Broadcastdomäne

Bei der Wegfindung von Sender- zu Empfänger-Station werden häufig rundspruchbasierte Protokolle eingesetzt. Zum einen NetBIOS in Microsoft-basierten Netzwerken und ARP des TCP/IP-Stacks. Die Protokolle schicken immer wieder Broadcasts raus, um den Weg zu einer unbekannten Station zu finden. Broadcasts belasten ein Netzwerk. Router verhindern die Weiterleitung von Broadcasts, sofern sie selber nicht auf deren Verwendung angewiesen sind. Router vermindern die Belastung des Netzwerkes durch Broadcasts.

Routing über unterschiedliche Netzarchitekturen und Übertragungssysteme

Netzwerkverkabelungen sind in der Regel strukturiert angelegt. Man

unterscheidet in der Primär-, Sekundär- und Tertiär-Verkabelung, die unterschiedliche Architekturen und Übertragungstechniken verwenden (Ethernet, Token Ring, FDDI, ATM, ISDN, WLAN, etc.). Ein Router kann in der Lage sein zwischen unterschiedlichen Architekturen zu vermitteln. Dazu gehört auch die Fragmentierung der Datenpakete.

Paket-Filter durch eine Firewall

Sicherheitsaspekte gehen auch an Routern nicht vorbei. Ungewünschter oder unsicherer Datenverkehr kann anhand von IP-Adressen oder TCP- und UDP-Ports gefiltert und unterbunden werden. Häufig kommen spezielle

Firewall-Router oder Router mit Firewall-Funktionen zum Einsatz.

Routing über Backup-Verbindungen bei Netzausfall

Durch den Einsatz von Routern entsteht häufig ein engmaschiges Netz, dass dem Datenpaket zum Ziel mehrere Wege zum Ziel bietet. Fällt ein Router aus, verständigen sich die Router untereinander und die Datenpakete nehmen einfach einen anderen Weg zu ihrem Ziel. Fällt eine Leitung zwischen zwei Routern aus, können diese z. B. eine Backup-Verbindung herstellen. Zum Beispiel eine Wählverbindung über das Telefonnetz.

In großen und modernen Netzwerken spielt die Fehlererkennung und -behandlung eine große Rolle. Router können den Netzwerkverkehr

protokollieren und über SNMP Meldungen an eine Netzwerk-Management-Station senden oder Befehle des Netzwerk-Administrators ausführen.

IP-Routing-Algorithmus

Der IP-Routing-Algorithmus gilt nicht nur für IP-Router, sondern für alle

Netzwerkstationen, die IP-Datenpakete empfangen können. Die empfangenen Datenpakete durchlaufen diesen Algorithmus bis das Datenpaket zugeordnet oder weitergeleitet werden kann.

Datenpaket

Frage: Ist das

Datenpaket für Ja Verarbeitung.

mich?

Nein

Frage: Ist das

Weiterleitung

Datenpaket für

ins Subnetz oder

Ja Verwerfung des

mein Subnetz?

Datenpakets.

Nein

Frage: Ist mir

die Route zum

Weiterleitung

Empfänger des

Ja über die

Datenpakets

bekannte Route.

bekannt?

Nein

Frage: Ist mir

ein Standard-

Gateway

Weiterleitung

bekannt,

über das

Ja

wohin ich das

Standard-

Datenpaket

Gateway.

weiterleiten

kann?

Nein

Fehlermeldung!

An erster Stelle des Routing-

Algorithmus steht die Frage "Ist das

Datenpaket für mich?". Wenn die Ziel-

Adresse des Datenpaketes 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

Subnetmaske 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

Stationen 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.

NAT - Network Address Translation

NAT ist ein Verfahren, dass in Routern eingesetzt wird, die lokale Netzwerke mit dem Internet verbinden. Während im lokalen Netzwerk jede Station eine private IP-Adresse hat, steht für das Internet oft nur eine öffentliche IP-Adresse zur Verfügung. Private IP-Adressen dürfen mehrfach verwendet werden und besitzen in öffentlichen Netzen keine Gültigkeit. Damit trotzdem alle Computer mit privater IP-Adresse Zugang zum Internet bekommen können,

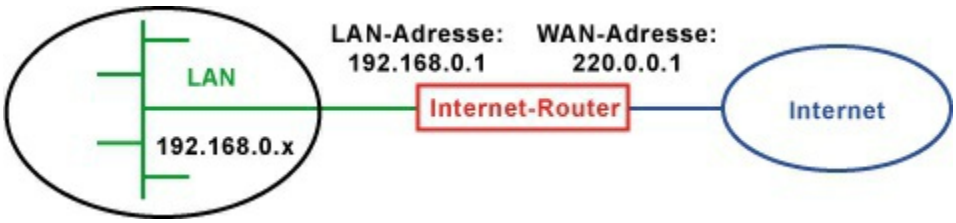
muss der Internet-Zugangs-Router in allen ausgehenden Datenpaketen die IP-Adressen der Stationen durch seine eigene, öffentliche IP-Adresse ersetzen. Damit die eingehenden Datenpakete dem richtigen Ziel zugeordnet werden, speichert der Router die aktuellen Verbindungen in einer Tabelle. Dieses Verfahren nennt man NAT (Network Address Translation).

Warum NAT?

Die ersten IP-Netze waren anfangs eigenständige Netz ohne Verbindung nach außen. Deshalb wurden die Stationen häufig mit IP-Adressen aus den privaten Adressräumen versehen. Doch irgendwann entstand der Bedarf, E-Mails über die Grenzen von Unternehmensnetzen auszutauschen und auch auf das World Wide Web (WWW) zuzugreifen. Weil die Stationen ohne eigene öffentliche IP-Adresse keine

Verbindung außerhalb des Netzwerks herstellen konnten, wurde mit NAT ein Verfahren eingeführt, dass es jeder Station möglich machte mit Rechnern außerhalb des lokalen Netzwerks zu kommunizieren.

Weil der Adressraum des Protokolls IPv4 zu verschwenderisch verteilt wurde, reichen die IP-Adressen nicht für jeden Computer aus. NAT ist also auch ein Ausweg, um die Adressknappheit



von IPv4 kurzfristig aufzulösen.

Langfristig muss jedoch ein Internet-Protokoll mit einem größeren Adressraum her. IPv6 ist ein solches Protokoll.

SNAT - Source Network Address Translation

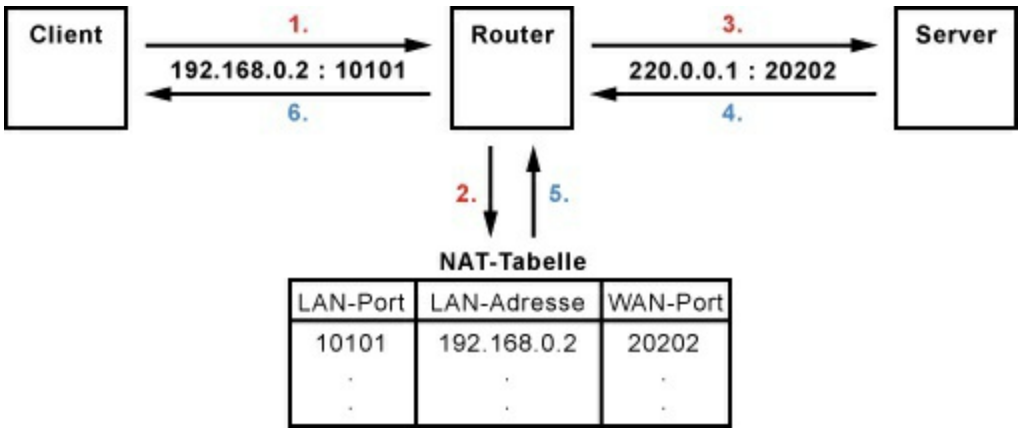
Das klassische Szenario für einen NAT-

Router ist ein gewöhnlicher 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. Innerhalb des lokalen Netzwerks hat der Router die IP-Adresse 192.168.0.1, die für den LAN-Port gilt. Mit der öffentlichen IP-Adresse tritt der Router als Stellvertreter für alle Stationen seines lokalen Netzwerks (LAN) auf. 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. Das bedeutet aber auch, dass diese Adressen nur innerhalb des privaten Netzwerks gültig sind. Private IP-Adressen werden in öffentlichen Netzen nicht geroutet. Das bedeutet, dass Stationen mit privaten IP-Adressen keine Verbindung ins Internet bekommen. Damit das trotzdem funktioniert, wurde NAT entwickelt.
Wenn nun ein Datenpaket mit einer Ziel-Adresse außerhalb des lokalen Netzwerks adressiert ist, dann ersetzt der NAT-Router die Quell-Adresse durch seine öffentliche IP-Adresse. Die Portnummer (TCP oder UDP) wird durch eine andere Portnummer ersetzt. Um später die Antwortpakete der richtigen Station zuordnen zu können führt der Router eine Tabelle mit den

geänderten Quell-Adressen und den dazugehörigen Portnummern. Wenn also Pakete mit einer bestimmten Portnummer zurück kommen, dann ersetzt NAT die Ziel-Adresse durch die richtige Adresse und Portnummer.
In der 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 Datenpaketes ändert, nennt man dieses Verfahren Source NAT (SNAT). SNAT bezeichnet man in der Regel einfach als NAT.

Ablauf von NAT



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 Portnummer (LAN-Port) aus und speichert beides mit der getauschten Portnummer (WAN-Port) in der NAT-Tabelle.

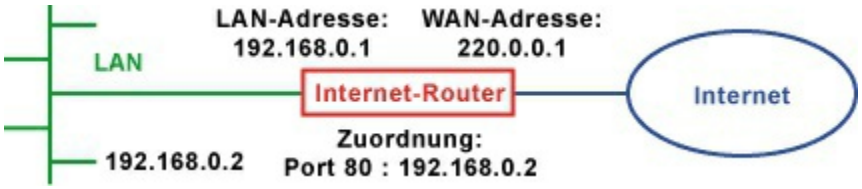
3. Dann leitet er das Datenpaket ins Internet weiter.

4. Der Empfänger (Server) des Datenpakets schickt seine Antwort

zurück.

5. Der NAT-Router stellt nun anhand der Portnummer 20202 (WAN-Port) fest, für welche IP-Adresse (LAN-Adresse) das Paket im lokalen Netz gedacht ist.

6. Dann tauscht er die IP-Adresse und die Portnummer von 20202 in 10101 aus und leitet das Datenpaket ins lokale Netz weiter,



wo es der Client entgegennimmt.

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 eine Station 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 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 diese Station 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 (unter 1024) 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

Die Einträge in der NAT-Tabelle sind nur für eine kurze Zeit gültig. Für Anwendungen, die nur sehr unregelmäßig Daten austauschen, bedeutet das, dass ständig die Verbindung abgebrochen wird. Das hat zur Folge, dass diese Anwendungen unter Umständen in einer NAT-Umgebung nicht funktionieren können.
Ein anderes Problem entsteht bei einer

hohen Anzahl ausgehender Verbindungen. Dann können NAT-Tabellen schon mal überlaufen. Das bedeutet, dass einzelne Verbindungen aus der NAT-Tabelle fliegen und demzufolge Verbindungen abbrechen. Für manche Anwendungen besteht ein hohes Risiko der Fehladressierung wegen fehlender Adresszuordnungen. Für viele Protokolle wurden Umgehungsmechanismen für NAT entwickelt. Das hat zu einer Verkomplizierung von Internet-Anwendungen und -Diensten und auch Sicherheitslücken geführt.

NAT als Sicherheitsfeature?

NAT wird besonders in Produkt-nahen Beschreibungen als Sicherheitsmerkmal beschrieben. Dahinter steckt ein Mechanismus, der als Nebenprodukt verhindert, dass Stationen hinter dem NAT-Router von außerhalb direkt

ansprechbar sind. Von außen initiierte Verbindungsversuche werden verworfen und bekommen keinen Zugang zum lokalen Netzwerk. Hacker, die zyklisch alle TCP-Ports einer IP-Adresse nach offenen Ports absuchen (Port-Scan) bekommen keine Antwort vom Router. Man kann sagen, NAT wirkt wie eine rudimentäre Firewall, die alle unberechtigten Zugriffe von außen blockt. Es handelt sich dabei um eine gewollte Schutzfunktion vor unaufgefordertem und unsicherem Datenverkehr. Doch eher zufällig erweist sich NAT als Sicherheitsmerkmal für lokale Netzwerke. NAT ersetzt keinen Paketfilter und schon gar keine vollwertige Firewall. NAT als Sicherheitsmerkmal zu bezeichnen ist irreführend und fahrlässig. Trotzdem wird dem Laien NAT immer wieder

gerne als Sicherheitsfeature verkauft.

Doch das ist falsch.

NAT und IPv6

Durch IPv6 wird NAT praktisch überflüssig. Der Wegfall von NAT verbessert den Betrieb von Netzwerken erheblich. Fehler, die NAT verursacht fallen dann einfach weg. Außerdem lassen sich Fehler schneller finden und beheben.

Ohne NAT werden Protokolle, wie STUN überflüssig. Das freut besonders Entwickler, weil jedes Protokoll, dass nicht implementiert werden muss, erst gar keine Sicherheitslücken aufreißen kann. Doch ohne NAT wird in Zukunft eine gut konfigurierte Firewall wichtiger werden.

DHCP - Dynamic

Host

Configuration

Protocol

DHCP ist ein Protokoll, um IP-Adressen in einem TCP/IP-Netzwerk zu verwalten und an die Stationen zu verteilen. Mit DHCP ist jede Netzwerk-Station in der Lage sich selber vollautomatisch zu konfigurieren.

Warum DHCP?

Um ein Netzwerk per TCP/IP aufzubauen ist es notwendig jede einzelne Station zu konfigurieren. Für ein TCP/IP-Netzwerk müssen folgende Einstellungen bei jeder Station vorgenommen werden:

Vergabe einer eindeutigen IP-Adresse

Zuweisen einer Subnetzmaske (Subnetmask)

Zuweisen des Default- bzw. Standard-Gateways

DNS-Serveradressen

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 lauter. Hier war sehr viel Planungs- und Arbeitszeit notwendig. Um dem zu entgehen, wurde DHCP entwickelt.
Mit DHCP kann jede Netzwerk-Station die Adresskonfiguration von einem DHCP-Server anfordern und sich selber automatisch konfigurieren. So müssen IP-Adressen nicht mehr manuell verwaltet und zugewiesen werden.

DHCPv6

Bei IPv6 gibt es die Stateless

Autoconfiguration. Doch diese berücksichtigt keine Informationen über Host-, Domainnamen und DNS. Diese Angaben und noch mehr können durch den Einsatz eines DHCPv6-Servers ergänzt werden. Dieser liefert die gewünschten Zusatzinformationen, kümmert sich dabei aber nicht um die Adressvergabe. Man spricht von Stateless DHCPv6.

Funktionsweise von DHCP

DHCP ist eine Client-Server-Architektur. 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-Gateway es gibt. In der Regel ist der DHCP-Server ein Router.

Wird eine Station gestartet und ist dort ein DHCP-Client aktiviert, wird ein in seiner Funktion 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. 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.

Der DHCP-Server antwortet auf den Broadcast mit einer freien IP-Adresse und weiteren Parametern. Danach wird die Datenübergabe bestätigt.

Mit DHCP werden nicht nur die IP-Adressen verteilt. Bei der Gelegenheit werden weitere Parameter übergeben, um die IP-Konfiguration im Client 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

Subnetzmaske

IP-Adresse des DHCP-Servers / Server-ID

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. Anschließend muss die Vergabe der IP-Adresse vom DHCP-Server bestätigt werden. Sobald der DHCP-Client die Bestätigung erhalten hat, speichert er die Daten lokal

ab. Abschließend wird der TCP/IP-Stack vollständig gestartet.

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:

Time Server

Name Server

Domain Name Server (Alternative)

WINS-Server

Domain Name

Default IP TTL

Broadcast Address

SMTP Server

POP3 Server

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 nun ein IP-Paket an sein Ziel findet, muss die Hardware-Adresse des Ziels bekannt sein.

Jede Netzwerkkarte besitzt eine einzigartige und eindeutige Hardware-Adresse, die fest auf der Karte eingestellt ist.

Bevor nun ein Datenpaket verschickt werden kann, muss durch ARP eine Adressauflösung erfolgen. Dazu benötigt ARP Zugriff auf IP-Adresse und Hardware-Adresse. Um an die Hardware-Adresse einer anderen Station zu kommen verschickt ARP z. B. einen Ethernet-Frame als Broadcast-Meldung mit der MAC-Adresse "FF FF

FF FF FF FF". Diese Meldung wird von jedem Netzwerkinterface entgegengenommen und ausgewertet. Der Ethernet-Frame enthält die IP-Adresse der gesuchten Station. Fühlt sich eine Station mit dieser IP-Adresse angesprochen, schickt sie eine ARP-Antwort an den Sender zurück. Die gemeldete MAC-Adresse wird dann im lokalen ARP-Cache des Senders gespeichert. Dieser Cache dient zur schnelleren ARP-Adressauflösung.

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 kein Schicht 3 Protokoll ist. Da ARP und IP aber so eng verzahnt sind, wäre ARP eigentlich irgendwo zwischen Schicht 3 und Schicht 2 richtig angesiedelt.

Ablauf einer ARP-

Adressauflösung

Eine ARP-Auflösung unterscheidet zwischen lokalen IP-Adressen und IP-Adressen in einem anderen Subnetz. Als erstes wird anhand der Subnetzmaske festgestellt, ob sich die IP-Adresse im gleichen Subnetz befindet. Ist das der Fall, wird im ARP-Cache geprüft, ob bereits eine MAC-Adresse für die IP-Adresse hinterlegt ist. Wenn ja, dann wird die MAC-Adresse zur Adressierung verwendet. Wenn nicht, setzt ARP eine Anfrage mit der IP-Adresse nach der Hardware-Adresse in das Netzwerk. Diese Anfrage wird von allen Stationen im selben Subnetz entgegengenommen und ausgewertet. Die Stationen vergleichen die gesendete IP-Adresse mit ihrer eigenen. Wenn sie nicht übereinstimmt, wird die Anfrage verworfen. Wenn die IP-Adresse übereinstimmt schickt die betreffende

Station eine ARP-Antwort direkt an den Sender der ARP-Anfrage. Dieser speichert die Hardware-Adresse in seinem Cache. Da bei beiden Stationen die Hardware-Adresse bekannt sind, können sie nun miteinander Daten austauschen.

Befindet sich eine IP-Adresse nicht im gleichen Subnetz, geht ARP über das Standard-Gateway. Findet ARP die Hardware-Adresse des Standard-Gateways im Cache nicht, wird eine lokale ARP-Adressauflösung ausgelöst. Ist die Hardware-Adresse des Standard-Gateways bekannt, schickt der Sender bereits sein erstes Datenpaket an die Ziel-Station. Der Router (Standard-Gateway) nimmt das Datenpaket in Empfang und untersucht den IP-Header. Der Router überprüft, ob sich die Ziel-IP-Adresse in einem angeschlossenen Subnetz befindet. Wenn ja, ermittelt er

anhand der lokalen ARP-Adressauflösung die MAC-Adresse der Ziel-Station. Anschließend leitet er das Datenpaket weiter. Ist das Ziel in einem entfernten Subnetz, überprüft der Router seine Routing-Tabelle, ob ein Weg zum Ziel bekannt ist. Ist das nicht der Fall steht dem Router auch ein Standard-Gateway zu Verfügung. Der Router führt für sein Standard-Gateway eine ARP-Adressauflösung durch und leitet das Datenpaket an dieses weiter.

Die vorangegangenen Schritte wiederholen sich so oft, bis das Datenpaket sein Ziel erreicht oder das IP-Header-Feld TTL auf den Wert 0 springt. Dann wird das Datenpaket vom Netz genommen.

Erreicht das Datenpaket irgendwann doch sein Ziel, schreibt die betreffende Station seine Rückantwort in ein ICMP-Paket an den Sender. In dieser Antwort

wird falls möglich ein Gateway vermerkt, über das die beiden Stationen miteinander kommunizieren. So werden weitere ARP-Adressauflösungen und dadurch Broadcasts vermieden.

ARP-Cache

Durch den ARP-Cache wird vermieden, dass bei jedem Datenpaket an das selbe Ziel wieder und immer wieder ein ARP-Broadcast ausgelöst wird. Häufig benutzte Hardware-Adressen sind im ARP-Cache gespeichert. Die Einträge im ARP-Cache können statisch oder dynamisch sein. Statische Einträge können manuell hinzugefügt und gelöscht werden. Dynamische Einträge werden durch die ARP-Adressauflösung erzeugt. Jeder dynamische Eintrag bekommt einen Zeitstempel. Ist er nach zwei Minuten nicht mehr abgerufen worden, wird der Eintrag gelöscht. Wird eine Adresse auch nach zwei Minuten noch

benutzt, wird der Eintrag erst nach zehn Minuten gelöscht. Ist der ARP-Cache für neue Einträge zu klein, werden alte Einträge entfernt.

Wird die Hardware neu gestartet oder ausgeschaltet, wird der ARP-Cache gelöscht. Es gehen dabei auch die statischen Einträge verloren.

Fehler und Probleme mit ARP

Grundsätzlich gibt es keine Probleme oder Fehler mit ARP, solange keine statischen Einträge im ARP-Cache vorgenommen werden oder Hardware-Adressen von Netzwerkkarten verändert werden.

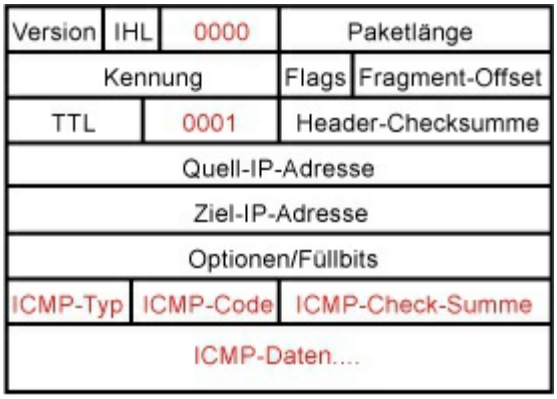
ARP läuft für den Benutzer ganz im Verborgenen.

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.

Aufbau des ICMP-Headers (IPv4)



ICMP hat keine eigene Header-Struktur.

Stattdessen wird der Standard-IP-

Header zur Übertragung von ICMP-

Meldungen genutzt.

Für die Nutzung durch ICMP werden

einige Felder des IP-Headers angepasst.

Das IP-Header-Feld Type-of-Service

wird auf den Wert "0000" gesetzt. Das IP-Header-Feld Protokoll wird auf den

Wert "0001" (=ICMP) gesetzt. Der

Daten-Bereich des IP-Headers wird zum

ICMP-Bereich, in dem sich die Felder

ICMP-Typ (Meldungstyp), ICMP-Code

(Zusatzinformationen zur Behandlung der

Nachricht), die ICMP-Check-Summe

und der ICMP-Daten-Bereich befinden.

Der ICMP-Daten-Bereich enthält den IP-

Header und die ersten 64 Bit IP-Daten des IP-Pakets, dass die ICMP-Meldung ausgelöst hat.

Aufbau des ICMP-Headers (IPv6)

Eine ICMPv6-Nachricht besteht aus mindestens drei Feldern:

8 Bit für den Typ der ICMPv6-Nachricht

8 Bit für den Code der ICMPv6-Nachricht

16 Bit für die Prüfsumme der ICMPv6-Nachricht.

Die Prüfsumme wird über die gesamte ICMPv6-Nachricht und einem Pseudoheader gebildet. Der Pseudoheader besteht aus Quell- und Zieladresse, sowie der Länge des ICMPv6-Datagramms und dem Next-Header-Eintrag.

Anwendung von ICMP

Die meisten Internet- und Netzwerk-

Benutzer kommen mit ICMP selten direkt in Kontakt. Die meisten ICMP-Meldungen werden von Stationen im Netzwerk verursacht, die Probleme mit IP-Paketen der auslösenden Station 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.
Neben den Netzwerkanalyse-Tools bei Netzwerk-Problemen gibt es auch die Möglichkeit den Datenverkehr und die ICMP-Meldungen mit einem Netzwerkmonitor zu überwachen.

IGMP - Internet Group Management

Protocol

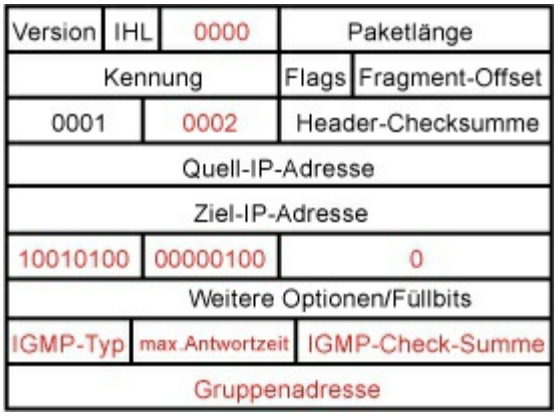
Das Internet Group Management Protocol (IGMP) ist eine Erweiterung des Internet Protocols (IPv4). Mit IGMP ist IP-Multicasting (Gruppenkommunikation) im Internet möglich. IP-Multicasting ist die Verteilung von IP-Paketen mit einer Ziel-IP-Adresse an mehrere Stationen gleichzeitig. Das Gegenstück von IGMP von IPv4 ist bei IPv6 MLD (Multicast Listener Discovery).

Funktionsweise von IGMP

Um die Datenmenge auf das notwendigste zu reduzieren, bietet IGMP die Möglichkeit dynamisch Gruppen zu verwalten. Die Verwaltung findet nicht in der Sende-Station statt, sondern in den Routern auf dem Weg zum Empfänger. Dazu merkt sich der Router, an welcher ausgehenden Schnittstelle sich eine Station befindet, die bestimmte

Multicast-IP-Pakete erhalten wollen. IGMP bietet Funktionen, mit denen sich Router untereinander verständigen und über die eine Station einem Router mitteilt, dass sie Multicast-IP-Pakete empfangen will. Der Sender von Multicast-IP-Paketen weiß dabei nicht, welche und wie viele Stationen seine Pakete empfangen. Denn er verschickt nur ein einziges Datenpaket an seinen übergeordneten Router. Der dupliziert das IP-Paket bei Bedarf, wenn er mehrere ausgehende Schnittstellen mit Empfängern hat. Damit Multicast-IP funktioniert, müssen auf dem Weg zwischen Sender und Empfänger alle Netzknoten IGMP unterstützen.

Aufbau des IGMP-Headers (IPv4)



IGMP verwendet den Standard-IP-

Header zur Übertragung von IGMP-

Meldungen. Der IP-Header wird nur um

ein paar Zusatzinformationen für IGMP

erweitert.

Das IP-Header-Feld Type-of-Service

wird auf den Wert "0000" gesetzt. Das IP-Header-Feld Protokoll wird auf den

Wert "0002" (=IGMP) gesetzt. IGP-

Meldungen werden nur zwischen direkt

miteinander verbundenen Netzwerk-

Stationen ausgetauscht. Deshalb wird

der TTL-Wert fest auf 1 gesetzt. Damit

wird sichergestellt, dass Router ohne

IGMP die IGMP-Pakete nicht

weiterleiten. Im Option-Feld des IP-

Headers wird dem Router mitgeteilt,

dass er dieses Paket auswerten muss.
Der Daten-Bereich des IP-Headers wird zum IGMP-Bereich, in dem sich die Felder IGMP-Typ (Meldungstyp), Max. Response Time (maximale Antwortzeit), die IGMP-Check-Summe und das Feld für die Multicast-IP-Adresse (Gruppenadresse) befinden.

Anwendung von IGMP

Das Internet mit der Protokoll-Familie TCP/IP setzt bei der Adressierung einen Sender und Empfänger pro Verbindung voraus. Für Verbindungen mit einem Sender und mehreren Empfängern, wie sie bei Fernseh- und Rundfunkübertragungen bekannt sind, ist mit IP nur mit IGMP möglich.
IGMP findet Anwendung im Mbone, einem Internet-Broadcast-System, das Rundfunk-Programme (Web-Radio, Streaming) über das Internet überträgt.

TCP -

Transmission

Control Protocol

Das Transmission Control Protocol, kurz TCP, ist Teil der Protokollfamilie TCP/IP. TCP übernimmt, als verbindungsorientiertes Protokoll, innerhalb von TCP/IP die Aufgabe der Datensicherheit, der Datenflusssteuerung und ergreift Maßnahmen bei einem Datenverlust. Die Funktionsweise von TCP besteht darin, den Datenstrom verschiedener Anwendungen aufzuteilen, mit einem Header zu versehen und an das Internet Protocol (IP) zu übergeben. Beim Empfänger werden die Datenpakete in die richtige Reihenfolge gebracht und an die adressierte Anwendung übergeben.

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

Dienste / Protokolle /

Schicht

Anwendungen

Anwendung HTTP IMAP DNS SNMP

Transport

TCP

UDP

Internet

IP (IPv4 / IPv6)

Netzzugang

Ethernet, ...

Eigenschaften von TCP

Verbindungsmanagement

Flusskontrolle

Zeitüberwachung

Fehlerbehandlung

Funktionsweise von TCP

Durch TCP stehen Sender und
Empfänger ständig in Kontakt
zueinander. Obwohl es sich eher um eine
virtuelle Verbindung handelt, werden
während der Datenübertragung ständig
Kontrollmeldungen ausgetauscht. So

werden zum Beispiel verloren gegangene Pakete von TCP erkannt und erneut angefordert.

TCP hat außerdem einen Algorithmus, der die Datenrate dynamisch an die Netzauslastung anpasst. TCP erhöht nach dem Verbindungsaufbau die Übertragungsrate kontinuierlich, bis irgendwo auf dem Weg zum Empfänger Pakete verloren gehen. TCP reagiert dann umgehend mit der Halbierung der Datenrate.

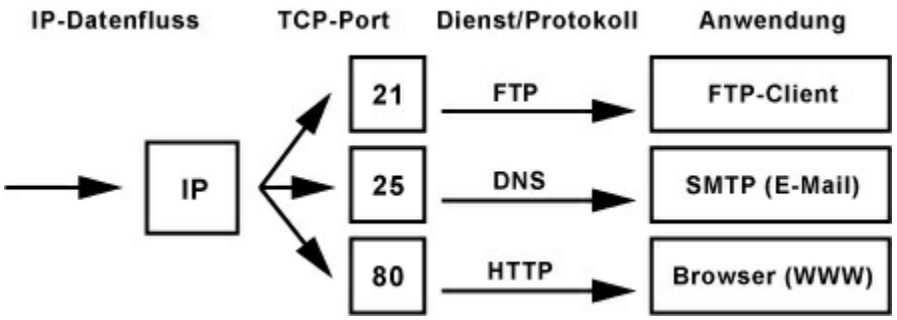
Zum einen nutzt TCP freie Kapazität aus. Zum anderen, wenn andere Nutzer die Kapazität ebenfalls beanspruchen, dann gibt TCP sie wieder frei. Diese Steuerung findet in den Endgeräten statt. Die IP-Router im Netz haben damit nichts zu tun.

Ein Problem ist das dann, wenn Anwendungen einfach mehrere TCP-Verbindungen öffnen. Das ist zum

Beispiel bei P2P-Filesharing in der Regel der Fall. Das Problem dabei ist aber nicht das Filesharing, sondern die Zuteilungsregeln von TCP.

Der kleine Bruder: UDP - User Datagram Protocol

Neben dem verbindungsorientierten TCP gibt es auch das verbindungslose und unsichere UDP. Das User Datagram Protocol (UDP) ist auf der 4. Schicht, der Transportschicht, des OSI-Schichtenmodells angeordnet. Es hat die selbe Aufgabe wie TCP, nur das ihm



nahezu alle Kontrollfunktionen fehlen und dadurch schlanker daher kommt und einfacher zu verarbeiten ist.

TCP-Port-Struktur

In jedem TCP-Datenpaket ist eine

Nummer hinterlegt, die einen Port definiert, hinter dem sich eine Anwendung oder ein Dienst befindet, die diesen Port abhören und die Daten von TCP entgegennehmen. Datenpakete, die über IP ihr Ziel erreichen, werden von TCP zusammengesetzt und über die Port-Nummer an eine Anwendung übergeben. Dieser Port wird ständig von einem Prozess, Dienst oder einer Anwendung abgehört.

Die Port-Nummer 0 bis 1023 sind jeweils einer Anwendung oder einem Dienst fest zugeordnet. Die darüber liegenden Port-Nummern können frei belegt werden, sofern sie gerade von keinem anderen Dienst belegt sind. Zum Beispiel nehmen Programme einen freien Port, um damit Kontakt zu einem Server aufzunehmen. Der Server schickt dann die Daten an diesen Port zurück. Damit wird sichergestellt, dass die

Daten nicht an die falsche Anwendung übergeben werden.

Mit der Port-Struktur ist es möglich, dass mehrere Anwendungen gleichzeitig über das Netzwerk Verbindungen zu mehreren Kommunikationspartner aufbauen.

TCP-Port-Übersicht

Diese Ports sind fest einer Anwendung oder einem Protokoll zugeordnet. Die feste Zuordnung ermöglicht eine einfachere Konfiguration

Well Known 0 - **Ports**

durch den 1023 Benutzern. Er kommt so mit dem

Protokoll TCP in

Kontakt.

Die Verwaltung

dieser Ports

übernimmt die

Internet Assigned

Numbers Authority

(IANA).

1024 Diese Ports sind

Registered -

für Dienste

Ports

49151 vorgesehen.

Diese Ports werden

dynamisch

zugewiesen. Jeder

Dynamically 49152 Client kann diese

Allocated

-

Ports nutzen. Wenn

Ports

65535 ein Prozess einen

Port benötigt,

fordert er diesen

bei seinem Host an.

Beispiele für TCP-Ports

Port-

Protokoll Anwendung

Nummer

21

FTP

Dateitransfer

23

Telnet

Konsole

25

SMTP

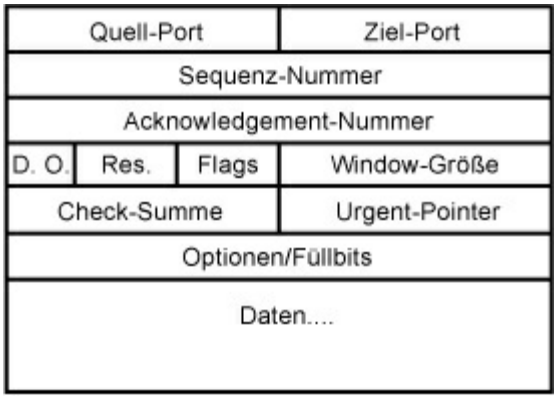
Postausgang

World Wide

80

HTTP

Web



110

POP3

Posteingang

119

NNTP

Usenet

Aufbau des TCP-Headers

Jedem Datenpaket, das TCP verschickt,

wird ein Header vorangestellt, der die

folgenden Daten enthält:

Sender-Port

Empfänger-Port

Paket-Reihenfolge (Nummer)

Prüfsumme

Quittierungsnummer

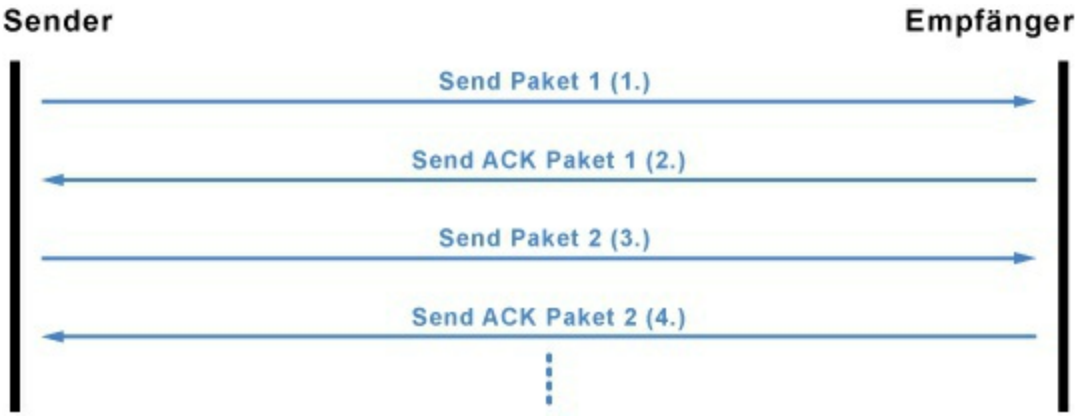
Aufbau des TCP-Headers TCP-Pakete

setzen sich aus dem Header-Bereich und

dem Daten-Bereich zusammen. Im Header sind alle Informationen enthalten, die für eine gesicherte TCP-Verbindung wichtig sind. Der TCP-Header ist in mehrere 32-Bit-Blöcke aufgeteilt. Mindestens enthält der Header 5 solcher Blöcke. Somit hat ein TCP-Header eine Länge von mindestens 20 Byte.

TCP-Verbindungsaufbau

Der Verbindungsaufbau läuft nach dem Three-Way-Handshake ab. Zuerst schickt der Client an den Server einen Verbindungswunsch (SYN). Der Server bestätigt den Erhalt der Nachricht (ACK) und äußert ebenfalls seinen Verbindungswunsch (SYN). Der Client



bestätigt den Erhalt der Nachricht (ACK). Danach erfolgt die Kommunikation zwischen Client und Server.

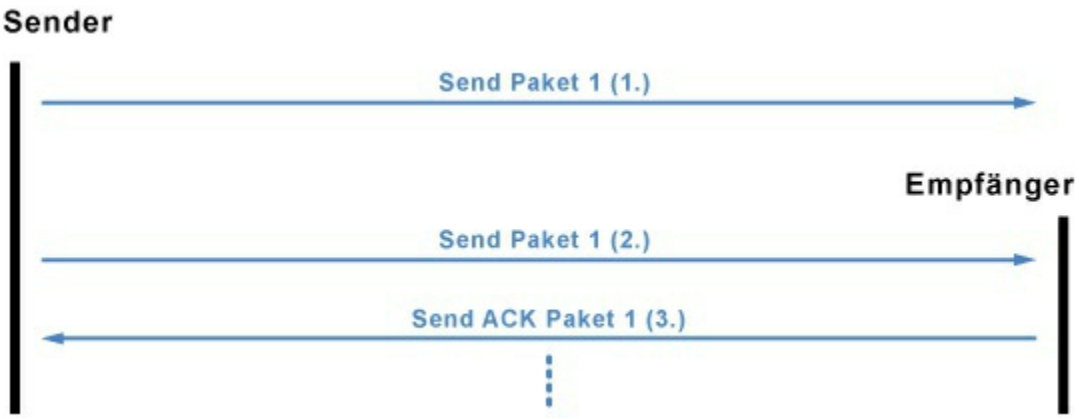
TCP-Kommunikation

Der Sender beginnt mit dem Senden des ersten Datenpakets (Send Paket 1). Der Empfänger nimmt das Paket entgegen (Receive Paket 1) und bestätigt den Empfang (Send ACK Paket 1). Der Sender nimmt die Bestätigung entgegen (Receive ACK Paket 1) und sendet das zweite Datenpaket (Send Paket 2). Der Empfänger nimmt das zweite Paket entgegen (Receive Paket 2) und bestätigt den Empfang (Send ACK Paket 2). Der

Sender nimmt die zweite Bestätigung entgegen (Receive ACK Paket 2).

Und so läuft die Kommunikation weiter, bis alle Pakete übertragen wurden.

TCP-Kommunikation mit Timer



Um festzustellen, ob Datenpakete ankommen, wird ein Timer gesetzt. Läuft der Timer ab, dann muss der Sender das Datenpaket nochmal schicken.

Im Prinzip läuft die Kommunikation wie gewohnt. Der Sender beginnt mit dem Senden des ersten Datenpakets (Send Paket 1). Gleichzeitig setzt er einen Timer. Bekommt er die Bestätigung

(Send ACK Paket 1) des Empfängers, dann sendet er das zweite Paket. Läuft der Timer jedoch ab, dann geht der Sender von einem Paketverlust aus und sendet das Datenpaket noch mal (Send Paket 1).

TCP-Verbindungsabbau

Der Verbindungsabbau kann sowohl vom Client als auch vom Server vorgenommen werden. Zuerst schickt einer der beiden der Gegenstelle einen Verbindungsabbauwunsch (FIN). Die Gegenstelle bestätigt den Erhalt der Nachricht (ACK) und schickt gleich darauf ebenfalls einen Verbindungsabbauwunsch (FIN). Danach bekommt die Gegenstelle noch

mitgeteilt, dass die Verbindung abgebaut ist (ACK).

Flusskontrolle

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.

Ein weiteres Problem sind die Wartezeiten zwischen Datenpaket, Bestätigung und nächstes Datenpaket. Die Wartezeit kann manchmal sehr lange dauern. Insbesondere dann, wenn die Quittierung eines gesendeten Pakets nicht kommt. Deshalb können auch mehrere TCP-Pakete hintereinander verschickt werden (Sliding Window). Weitere Datenpakete folgen dann, wenn

das erste ACK zurück kommt.

UDP - User

Datagram

Protocol

UDP ist ein verbindungsloses Transport-Protokoll und arbeitet auf der 4. Schicht, 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.

Das User Datagram Protocol

(UDP) im TCP/IP-

Protokollstapel

Dienste / Protokolle /

Schicht

Anwendungen

Anwendung HTTP IMAP DNS SNMP

Transport

TCP

UDP

Internet

IP (IPv4 / IPv6)

Netzzugang

Ethernet, ...

Eigenschaften von UDP

kein Verbindungsmanagement

keine Flusskontrolle

keine Zeitüberwachung

keine Fehlerbehandlung

Funktionsweise von UDP

UDP hat die selbe Aufgabe wie TCP,

nur das ihm nahezu alle

Kontrollfunktionen fehlen und dadurch

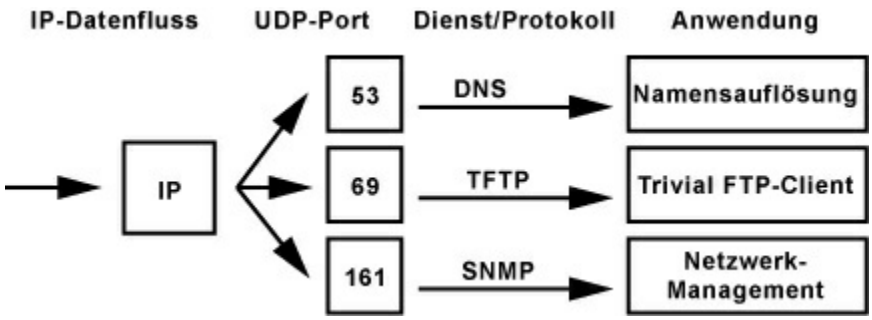
schlanker daher kommt und einfacher zu

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 den Datenstrom 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. Typisch sind DNS-Anfragen, VPN-Verbindungen, Audio- und Video-Streaming.

Port-Struktur



Die Gemeinsamkeit von UDP und TCP ist die Port-Struktur, die mehreren Anwendungen gleichzeitig mehrere Verbindungen über das Netzwerk ermöglicht.

In jedem UDP-Datenpaket ist eine Nummer hinterlegt, die einen Port definiert, hinter dem sich eine Anwendung oder ein Dienst befinden, die diesen Port abhören und die Daten von UDP entgegennehmen. Die Port-Nummern beginnen von 0 an zu zählen und sind bis zur Port-Nummer 1023 fest einer Anwendung zugeordnet. Alle anderen Port-Nummern, die darüber liegen, können frei von anderen Programmen verwendet werden. Z. B. nehmen Programme einen freien Port, um

damit Kontakt zu einem Server aufzunehmen. Der Server schickt dann die Daten an den frei gewählten Port zurück.

Mit der Port-Struktur ist es möglich, dass mehrere Anwendungen gleichzeitig über das Netzwerk Verbindungen zu mehreren Kommunikationspartner aufbauen. Mit UDP wird sichergestellt, dass die Daten nicht an die falsche Anwendung übergeben werden.

Beispiele für UDP-Ports

Port-Nummer	**Protokoll**	**Anwendung**
53	DNS	Domain Name Server
69	TFTP	Trivial File

Transfer Protocol

NetBIOS- NetBIOS

137

ns

Nameserver

NetBIOS- NetBIOS-

138

DGM

Datagramm-Dienst

Simple

161

SNMP

Management

Network Protocol

Aufbau des UDP-Headers

UDP-Pakete setzen sich aus dem

Header-Bereich und dem Daten-Bereich

zusammen. Im Header sind alle

Informationen enthalten, die eine einigermaßen geordnete Datenübertragung zulässt und die ein UDP-Paket als ein solches erkennen lassen. Der UDP-Header ist in 32-Bit-Blöcke unterteilt. Er besteht aus zwei solcher Blöcke, die den Quell- und Ziel-Port, die Länge des gesamten UDP-Pakets und die Check-Summe enthalten. Der UDP-Header ist mit 8 Byte sehr schlank und lässt sich mit weniger Rechenleistung verarbeiten.

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. Je nach Codec sind 1-20%

Paketverlust tolerierbar. Allerdings garantiert RTP nicht die Dienstqualität der Übertragung (Quality of Service).

Das Realtime Transport Protocol (RTP) im TCP/IP-Protokollstapel

Dienste / Protokolle / Schicht

Anwendungen

Anwendung

RTP

Transport

UDP

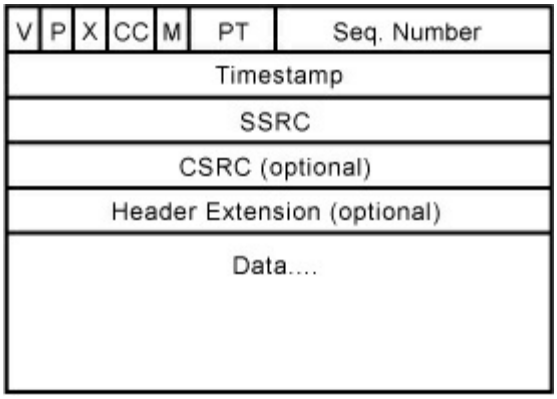
Internet

IP (IPv4 / IPv6)

Netzzugang

Ethernet, ...

Aufbau des RTP-Headers



Mit RTP wird der Medienstrom in Datenpakete aufgeteilt. Im Header der Datenpakete sind Informationen über den Codec, Sequenznummer, Zeitstempel, Synchronisation und evt. Verschlüsselung (SRTP) enthalten. Trotzdem wird dabei unnötiger Protokoll-Overhead vermieden.

SRTP - Secure Realtime Transport Protocol

Nach dem Verbindungsaufbau mit SIP, SIPS oder H.323 werden die Sprachdaten mit RTP übertragen. Diese Datenpakete können von einem Dritten mitgeschnitten oder herausgeschnitten werden. Dadurch kann die Gesprächsverbindung belauscht oder

manipuliert werden. Mit SRTP werden die Sprachdaten verschlüsselt. Das Abhören ist dann nicht mehr möglich.

Ping - Paket Internet Groper / pathping

Ping steht für Paket Internet Groper und ist das meistgenutzte Tool um eine Netzwerkverbindung zu einer anderen Station zu testen oder einfach nur um den lokalen TCP/IP-Stack zu prüfen.
Ping steht auf der Kommandozeile/Konsole als Befehl ping zur Verfügung. Die entfernte Station kann über die IP-Adresse oder den Domain- bzw. WINS-Namen angesprochen werden. Bei Bedarf übernimmt ping die Namensauflösung.
Ping kennt mehrere Optionen, die mehr Informationen liefern. Hierauf wird hier nicht weiter eingegangen. Das Hilfesystem des verwendeten

Betriebssystems gibt weitere Auskunft.

Unter Windows führt der ping-Befehl den Ping nur insgesamt 4 mal hintereinander aus. Bei Unix oder Linux führt der ping-Befehl den Ping so oft aus, bis der Befehl abgebrochen wird. Zum Abbruch muss CTRL und C (CTRL + C) gedrückt werden.

Was passiert bei einem Ping?

Bei der Ausführung des Befehls ping wird ein ICMP-Paket vom Typ ICMP Echo Request an die Netzwerk-Station gesendet. Wenn die Station des ICMP-Paket empfangen hat, sendet sie ein ICMP-Paket vom Typ ICMP Echo Reply zurück. Ein Windows-Betriebssystem führt insgesamt 4 ICMP-Meldungen aus. Bei Unix/Linux muss ping durch STRG+C abgebrochen werden.

Anwendung von Ping

1. Mit Ping kann man die Laufzeit

eines Paketes vom Sender zum Empfänger ermitteln. Dazu wird die Zeit, bis das Echo Reply eintrifft, halbiert.

2. Mit Ping kann geprüft werden, ob eine Station Kontakt zum Netzwerk hat: mit ping auf eine Nachbarstation oder dem Standard-Gateway.

3. Mit Ping auf den localhost oder 127.0.0.1 kann geprüft werden, ob der TCP/IP-Stack auf der lokalen Station überhaupt installiert ist.

4. Wichtige Stationen (z. B. Server) können mit regelmäßigen Pings auf Verfügbarkeit überprüft werden. Allerdings bezieht sich das auf die Verfügbarkeit des TCP/IP-Stacks oder aber die Server-Erreichbarkeit.

pathping

pathping ist eine Erweiterung von ping.

Es analysiert die Stationen ähnlich wie tracert oder traceroute über die gesamte Strecke, die ein Datenpaket zum Ziel nehmen muss.
In Abhängigkeit der überwundenen Stationen liefert pathping nach ein paar Minuten eine Statistik über die Erreichbarkeit der einzelnen Stationen.

Trace Route (traceroute, tracert)

Trace Route ist ein Kommandozeilen-Tool, um in einem IP-Netzwerk den Weg von Datenpaketen zu verfolgen und sichtbar zu machen. Es geht darum festzustellen, welche Stationen ein Datenpaket bis zum Ziel nimmt. Trace Route funktioniert ähnlich wie Ping. Mit diesem Tool bekommt man jedoch noch mehr Informationen über die Netzwerkverbindung zwischen der lokalen Station und der entfernten

Station.

Trace Route steht auf der Kommandozeile/Konsole als Befehl traceroute unter Unix/Linux und tracert unter Windows zur Verfügung. Die entfernte Station kann unter der IP-Adresse oder dem Domain- bzw. WINS-Namen angesprochen werden. Bei Bedarf übernimmt Trace Route die Namensauflösung.

Trace Route hat mehrere Optionen, die mehr Informationen liefern. Darauf wird hier nicht weiter eingegangen. Das Hilfesystem des Betriebssystems gibt darüber Auskunft.

Beispiel für die Anwendung von Trace Route (tracert)

C:\>tracert -d www.elektronik-kompendium.de

Routenverfolgung zu www.elektronik-kompendium.de [212.227.253.68]

über maximal 30 Abschnitte:

1 1 ms 1 ms 1 ms

192.168.168.8

2 64 ms 68 ms 70 ms

217.5.98.159

3 60 ms 60 ms 61 ms

217.237.156.234

4 62 ms 63 ms 63 ms

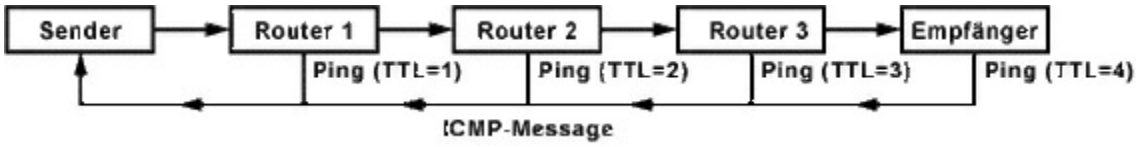
62.154.18.22

5 70 ms 71 ms 71 ms

212.227.112.18

6 69 ms 71 ms 71 ms

212.227.120.6



7 69 ms 71 ms 71 ms

212.227.116.210

8 81 ms 73 ms 72 ms

212.227.34.194

9 71 ms 71 ms 70 ms

212.227.253.68

Ablaufverfolgung beendet.

Was passiert bei Trace

Route?

Bei der Ausführung des Befehls tracert bzw. traceroute werden mehrere ICMP-Befehle (Ping) hintereinander verschickt an die Ziel-Adresse geschickt. Beim ersten ICMP-Befehl wird der TTL-Wert des IP-Pakets auf "1" gesetzten. Der TTL-Wert gibt an, nach wie vielen Stationen die Lebenszeit eines IP-Pakets verfällt. Der Station, die die abgelaufene Lebenszeit des Datenpakets erkennt, verwirft das Paket und schickt eine ICMP-Meldung vom Typ 11 "Time Exceeded" zurück. Nach der Ankunft der ICMP-Meldung "Time Exceeded" wird erneut ein ICMP-Befehl mit um eins erhöhten TTL-Wert verschickt. Das wird so lange wiederholt, bis alle Stationen bzw. die Route zur Ziel-Adresse ermittelt ist. Das Ergebnis wird auf dem Bildschirm ausgegeben.

Anwendung von Trace

Route

1. Trace Route kann dazu verwendet werden, um zu prüfen, ob die Datenpakete auf dem Weg zum Ziel die richtige Route verwenden. Ein Umweg kann z. B. auf einen Ausfall eines Routers hindeuten.
2. Mit Trace Route kann man die Laufzeit zwischen den einzelnen Stationen prüfen. So kann ein Engpass auf der Übertragungsstrecke ermittelt werden.
3. Erreichen IP-Pakete ihr Ziel nicht, dann kann man mit Trace Route die Station ermitteln, die ausgefallen ist.
4. Kommen innerhalb einer Route eine oder mehrere Stationen mehrfach vor, liegt es nahe, dass der entsprechende Router durch einen fehlerhaften Routing-Eintrag eine

Routing-Schleife verursacht.

ipconfig / winipcfg

(Windows)

ipconfig und winipcfg sind Tools, die unter Windows die Einstellungen zu TCP/IP übersichtlich darstellen.

ipconfig

Auf der Kommandozeile/Konsole von Windows steht der Befehl ipconfig zur Verfügung, um Informationen des lokalen TCP/IP-Stacks zu erhalten. Alle Informationen lassen sich auch über die Netzwerkeinstellungen der Systemsteuerung einsehen. Allerdings nicht so schön übersichtlich und ohne die IP-Adresse, wenn diese per DHCP bezogen wurde.

ipconfig /all kann folgende Informationen liefern:

Hostname

DNS-Server

Knotentyp

NetBIOS-Bereichs-ID

IP-Routing aktiviert

WINS-Proxy aktiviert

NetBIOS-Auflösung durch DNS

Dazu werden Informationen zu allen Netzwerkadaptern inklusive Modems und ISDN-Karten geliefert:

Beschreibung

Physische Adresse (Hardware-Adresse)

DHCP aktiviert

Subnet Mask

Standard-Gateway

DHCP-Server

Erster WINS-Server

Zweiter WINS-Server

Gültig seit

Gültig bis

winipcfg (winipcfg.exe)

Wer nicht mit der DOS-Box hantieren will, der kann auch mit dem Windows-eigenen Tool (Windows 9x)

winipcfg.exe arbeiten. Alternativ ist es im c:\windows\-Pfad zu finden oder über die Ausführen-Dialog-Box mit winipcfg.exe ausführbar.

winipcfg bietet die gleichen Informationen und Funktionen wie ipconfig. Doch Vorsicht bei dieser Klicki-Bunti-Variante. Beim Klicken der Buttons sollte man wissen was man tut.

Anwendungen und

Dienste

Internet

Namensauflösung

World Wide Web

E-Mail

Verzeichnisdienste

Storage

Internet

Das Internet ist eine unermessliche Vielzahl von kleinen, mittleren und großen Netzen, die alle zum weltweiten uneingeschränkte Austausch von

Informationen zusammen geschaltet

werden.

Obwohl das Internet verschiedene

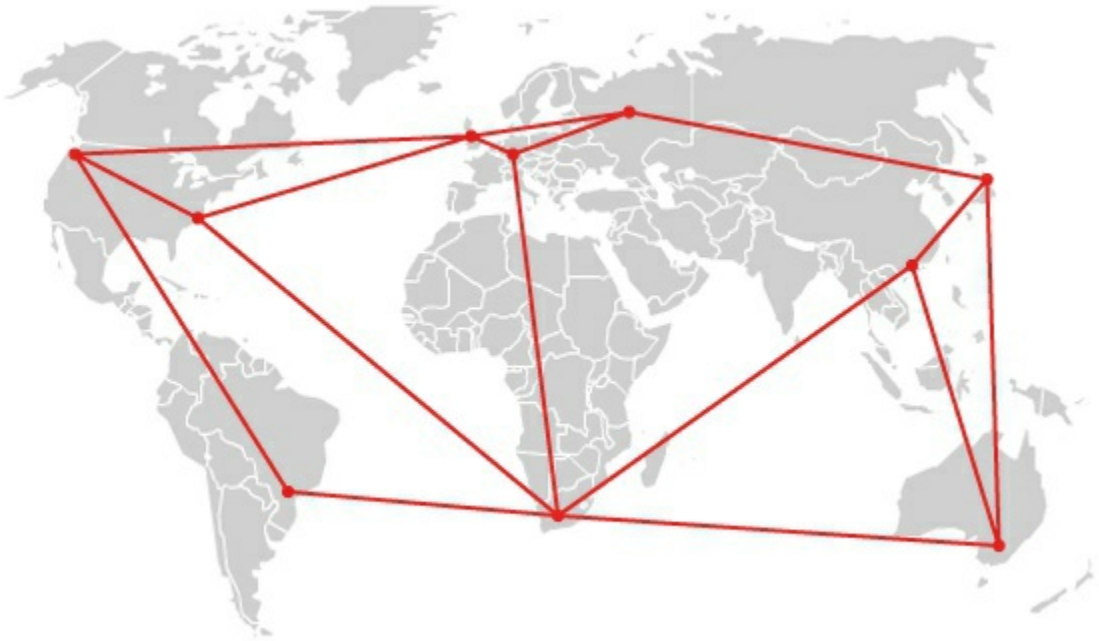
Dienste und Anwendungen hat,

verwendet man den Begriff "Internet"

heute synonym für das "World Wide

Web (WWW)", dass man sich mit einem

Browser zugänglich macht.



Das Internet unterliegt keiner bestimmten

Struktur und es gibt auch keine Zentrale.

Stattdessen sind alle Computer

irgendwie miteinander verbunden. Das

zentrale Vermittlungsprotokoll ist das

Internet Protocol (IP), das für die Vermittlung und Adressierung der Datenpakete zuständig ist. 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 TCP/IP-Protokollfamilie, die auch in kleinen lokalen Netzwerken für die Steuerung des Netzwerkverkehrs verantwortlich sind.

Internet-Dienste

Das Internet ist ein Informations- und Kommunikationsmedium über das Informationen und Daten übermittelt und ausgetauscht werden. Dazu gibt es verschiedene Dienste, die über Anwendungen, die auf einem Computer installiert sind, benutzt werden können. Klassische Internet-Anwendungen sind

das World Wide Web, E-Mail, Usenet (Diskussionsforen), Chat (IRC) und File-Transfer (FTP). Der Zukunft gehören Peer-to-Peer-Anwendungen (P2P), Internet-Telefonie und Cloud Computing.

Internet-Adresse

Die Internet-Adresse ist ein Überbegriff für die verschiedenen Adressen, mit denen man im Internet Dienste adressiert und dadurch erreichbar sind. Allerdings werden WWW-Adressen im allgemeinen Sprachgebrauch als Internet-Adressen bezeichnet.

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 Netzwerkes verhindert werden. Dank der Protokolle TCP und IP konnten an das ARPANET immer mehr Netzwerke angeschlossen werden. Dabei entstand das Internet.

1984 wurde das Projekt in einen militärischen Bereich und einen wissenschaftlichen Bereich aufgeteilt. 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.

Heute

Heute hat das Internet für Wirtschaft und Gesellschaft, sowie dem internationalen Austausch eine wichtige Bedeutung. So spielen sich große Teile der Kommunikation, Unterhaltung und des Informationsaustauschs im Internet ab.

Zukunft

Neben gesellschaftlichen Veränderungen, vor allem bei der Mediennutzung, beeinflussen die Netzneutralität, Konvergenz und das Internet-Protokoll IPv6 die Zukunft des Internets.

URI - Uniform Resource Identifiers

Uniform Resource Identifiers (URI) ist der Überbegriff für einheitliche und unverwechselbare Adressierungsmöglichkeiten in einem unsortierten und dezentralen

Informationsraum. Bemerkenswert ist, dass URI aus dem Jahr 1998 stammt und alle darunter fallende Einzelkonzepte wesentlich älter sind, aber darin berücksichtigt wurden.

Übersicht der Einzelkonzepte

URL - Uniform Resource Locator

URN - Uniform Resource Names

PURL - Peristent Uniform Resource Locator

URC - Uniform Resource Characteristics

Grundsätzlicher Aufbau eines URI

Schema : Schemaspezifisch

Der Aufbau setzt sich aus der Bezeichnung des Schemas zusammen, gibt also an, um was es sich für eine Ressource handelt. Schemaspezifisch ist der Zeiger bzw. die Angabe des Standorts, wo sich die Ressource

befindet.

URL - Uniform Resource

Locator

Ressourcentyp://User:Passwort@Host.Domain.TLD:Port/Pfad/Datei Paramter

Die oder 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.

Beispiele für URL:

http://www.elektronik-

kompendium.de/

mailto:name@beispiel.de

file:///c:/temp/

URN - Uniform Resource

Names

URN:Bezeichnung:Ressourcenbezeichnung

Die URN bezeichnen ein Objekt mit

einem eindeutigen Namen in einem

bestimmten Informationsraum. Der Name enthält weder Informationen über Standort noch Inhalt, sondern eine unverwechselbare Bezeichnung.
Klassische URN-Objekte sind Produkte, die mit dem EAN-Code (European Article Nummber) ausgezeichnet sind, Bücher, die den ISBN-Code (International Standard Book Number) tragen, oder auch periodisch erscheinende Publikationen wie Zeitungen und Zeitschriften mit dem ISSN-Code (International Standart Serial Number).

Beispiele für URN:

URN:ISSN:1610-0085

URN:ISBN:3-8334-1681-5

PURL - Persistent Uniform Resource Locator

PURL ist eine eigene URN-Struktur, die per URL aufgerufen wird. Die Anfrage wird von einem PURL-Server

ausgewertet und auf die eigentliche Ressource umgeleitet.

PURL ist sehr theoretisch und will in das etablierte URL-System nicht hineinpassen. Es ist deshalb auch nur ein Beispiel, wie URN-Anwendungen in das URL-System hineingeplanzt werden.

URC - Uniform Resource Characteristics

Die URC beschreibt die Eigenschaften und bietet weitere Informationen zu einer Ressource an. Diese Informationen werden in der Regel als Metadaten bezeichnet. In ihnen werden die Informationen zu einer Ressource einheitlich beschrieben.

Umsetzungen von URC betreffen z. B. die Katalogisierung von Internet-Ressourcen. Jedoch unterliegen die Informationen im Internet einer außergewöhnlichen Dynamik, der selbst moderne Suchmaschinen nicht Herr

werden.

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 heißt es korrekterweise als "der" URL.

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 an die Ressource übertragen!

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.
Nicht jeder Ressourcentyp kennt diese
Paramter. Außerdem gibt es
unterschiedliche Verfahren und nicht alle
Parameter sind für das entfernte
Zielsystem bestimmt.

WWW - World
Wide Web

Das World Wide Web, kurz WWW oder
Web, ist eine Ansammlung von Servern,
auf denen Informationen abgelegt sind.
Die Informationen in Form von Text,
Bild, Audio und Video greift man mit
Hilfe einer Software (Browser) zu. Um

die 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 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 Informationsseite zu Informationsseite.

Bei jedem Klick auf einen Link kontaktiert der Browser (HTTP-Client) einen HTTP-Server, auf dem die Ressource liegt. Jeder Link besteht aus einer Adresse, die aus der Server-Adresse und einem Verzeichnis und Dateinamen besteht. Der HTTP-Server liefert dann die aufgerufene Seite an den Browser zurück. 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. In 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:

Internet Explorer (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)

...

Der HTTP-Server ist ein Server-Dienst (z. B. httpd), 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 Internet, um genauer zu sein, 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 (Windows, Unix,

Linux, MAC, etc.) Dokumente zu erstellen. Zur Übertragung von HTML zwischen Browser und Webserver wird HTTP verwendet.

E-Mail

E-Mail ist die Abkürzung für Electronic Mail, was auf Deutsch "Elektronische Post" oder "Elektronischer Brief" bedeutet. Das Erstellen, Versenden und Darstellen einer E-Mail erfolgt ausschließlich in elektronischer Form. E-Mail ist neben dem Telefon ein zentrales Kommunikationsmittel in unserer Gesellschaft. Kurzmitteilungen, Diskussionen und Dateiaustausch, das alles wird mit E-Mails möglich.
Das Bearbeiten durch den Benutzer findet auf einem Computer oder einem anderen dafür vorgesehenen Endgerät statt. Nach dem Absenden wird die E-Mail innerhalb eines Netzwerkes oder über das Internet verschickt. Beim

Empfänger wird die E-Mail wieder auf dem Computer oder einem vergleichbaren Endgerät angezeigt.
Im Jahr 1971 wurde erstmals eine E-Mail zwischen zwei Computer im damaligen ARPANET übertragen.
Danach wurden E-Mail 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 ersetzte bzw. ergänzte Telefon, Fax und Brief und eine schnelle Möglichkeit Nachrichten und Dokumente digital zu übertragen. In der heutigen Zeit ist die Elektronische Post nicht mehr weg zu denken.

E-Mail-Adresse

E-Mail-Adressen erkennt man am dem ungewöhnlichen Satzzeichen "@"

(Klammeraffe). Es wird als Trennzeichen zwischen Benutzername und Ziel-Computer verwendet. Es kennzeichnet eine E-Mail-Adresse und unterscheidet sich dadurch von einer WWW-Adresse.

Spamming, Phishing, Pharming

E-Mail wäre an sich ein perfektes Kommunikationsmittel, wenn die ständigen Missbrauchsversuche krimineller Personen nicht wären. So wird massenhaft Werbe-E-Mails verschickt und dabei noch die E-Mail-Adresse fremder Personen missbraucht. Zusätzlich werden über Phishing und Pharming unbedarfte Personen dazu aufgefordert Zugangsdaten von Online-Banking-Accounts in fast perfekt nachgemachten Webseiten einzugeben, um danach Konten leer zu räumen. Obwohl weite Teile der Gesellschaft

inzwischen über solche Machenschaften aufgeklärt ist, nutzen Betrüger immer wieder arglose Personen aus, um sie unrechtmäßig zu bereichern.

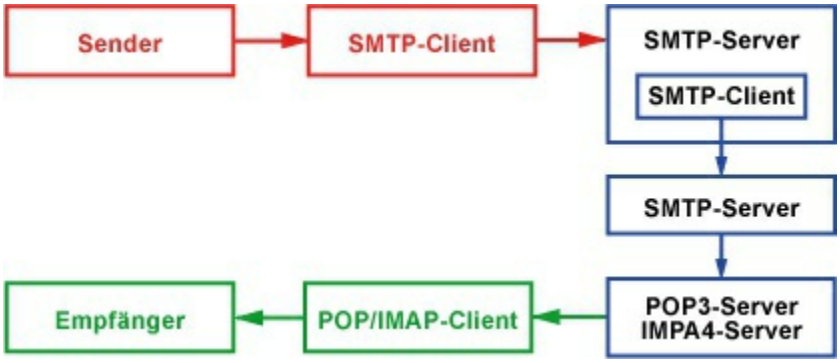
Aus diesen Gründen kommt kein E-Mail-Account ohne Spam-Filter und Antivirus-Funktion aus.

Die gesamte E-Mail-Kommunikation basiert auf drei Protokollen:

SMTP - Simple Mail Transfer Protocol

POP3 - Post Office Protocol Version 3

IMAP4 - Internet Mail Access Protocol Version 4



SMTP - Simple Mail

Transfer Protocol

Das SMTP-Protokoll ist für die Übertragung von E-Mails vom Sender zum Posteingang-Server (POP3 oder IMAP4) des Empfängers zuständig. Dazu kontaktiert der E-Mail-Client des Absenders seinen eigenen SMTP-Server (Postausgang-Server) und übergibt ihm die E-Mails, die zum Versand anstehen. Der Austausch der Nachrichten übernimmt der MTA (Mail Transport Agent) mit dem der Benutzer nicht in Kontakt kommt. Untereinander verständigen sich die E-Mail-Clients und MTAs mit Klartext-Kommandos, ähnlich wie bei HTTP oder FTP.

POP3 - Post Office Protocol

Version 3

Da E-Mail-Nutzer in der Regel nicht ständig online sind, um einen eigenen SMTP-Server zu betreiben, gibt es den Posteingangs-Server, z. B. mit POP3.

Auf dem Posteingangs-Server werden alle eingehenden Nachrichten einem Benutzer zugewiesen und zwischengespeichert, bis der Benutzer die E-Mails über das POP3-Protokoll abruft. Die Kommunikation übernimmt für den Benutzer der E-Mail-Client, der sich am POP3-Server anmeldet und die E-Mails danach abholt.

IMAP4 - Internet Mail Access Protocol Version 4

IMAP4 hat vom Prinzip die selbe Aufgabe wie POP3. 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 POP3 kann der

Benutzer selber vorab wählen, welche E-Mails er zum Lesen herunterladen will. Das ist vor allem bei der Benutzung einer Verbindung mit geringer Bandbreite (z. B. Remote über Handy, Modem oder ISDN) ein Vorteil.

POP3 oder IMAP4

Üblicherweise werden E-Mails vom Posteingangsserver über POP heruntergeladen und anschließend auf dem Server gelöscht. Das bedeutet, POP eignet sich hauptsächlich 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 POP3 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 bietet die Möglichkeit Ordner auf dem E-Mail-Server anzulegen, um dort die E-Mails zu speichern. 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 immer Zugriff auf die E-Mails.

POP ist veraltet und entspricht nicht mehr dem Umgang mit Daten. Die Daten werden lokal und nicht zentral gespeichert. Und trotzdem hat sich IMAP nicht wirklich durchgesetzt.
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. Wahlweise kann man 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.

IM - Instant Messaging

Instant-Messaging bedeutet soviel wie "sofortige Nachrichtenübermittlung" oder "Nachrichtensofortversand". Es ist eine Kommunikationsform, bei

sich zwei
oder mehr Teilnehmer per Textnachricht unterhalten. Unter Instant-Messaging versteht man im allgemeinen "Chatten". Also das Austauschen von Kurznachrichten in Dialogform. Während der Eine seine Nachricht mit der Enter-Taste abschickt, erscheint sie in Sekundenbruchteilen beim Anderen auf dem Bildschirm. Natürlich wäre eine solche Unterhaltung per Telefon wesentlich schneller und effektiver. Der Vorteil beim Chatten liegt in der Kürze. Einsteiger gewöhnen sich schnell daran, sich kurz zu fassen. Dröge Unterhaltungen bleiben in der Regel aus und es können jederzeit mehrere Personen zum Chat eingeladen werden. Eine vergleichbare Telefonkonferenz wäre für alle Beteiligten teuer, erfordert eine entsprechende Infrastruktur und erfordert ein diszipliniertes

Kommunikationsverhalten bei allen Teilnehmern.

Bei Instant-Messaging müssen die Teilnehmer über eine Software, den Chat-Client, verfügen und neben einer Verbindung zum Internet an einem Server angemeldet sein, der die Textnachrichten zwischen den Teilnehmern austauscht.

Die direkte persönliche Kommunikation ist nicht durch diese Art von digitalen oder elektronischen Medien zu ersetzen. Nur der direkte zwischenmenschliche Kontakt schafft Vertrauen. Über Instant-Messaging kommen auch Menschen zusammen, die räumlich und zeitlich voneinander getrennt sind.

Insbesondere im Privatbereich und unter Jugendlichen ist Instant-Messaging sehr beliebt. Über eine Kontaktliste sieht man sehr schnell wer gerade online ist und angechattet werden kann. Vor allem

öffentliche und kostenlose IM-Dienste von Yahoo, AOL (AIM und ICQ), Skype und Microsoft haben zur schnellen Verbreitung geführt.

Client: Instant-Messenger

Für die ganzen Kommunikationsformen wird ein Client, der Instant Messenger verwendet. Er wird vom IM-Anbieter kostenlos bereitgestellt. Alle Clients haben Grundfunktionen. In der Regel unterstützen alle Clients zusätzlich die Übertragung von Dateien und Audio- und Video-Streams. Benutzer können sich gegenseitig in ihrer Kontaktliste führen und sehen dann an der Präsenzinformation, ob andere online und für Gespräch bereit sind.

Kurznachrichten (Chat)

Voice-over-IP

Video-Telefonie

Dateiaustausch

Adressbuch

Standardmäßig werden die IM-Clients beim Start des Betriebssystems automatisch geladen. Zum Standard gehört die Abfrage, ob ein anderer die eigenen Kontaktdaten in seine Kontaktliste aufnehmen darf. Diese Funktion ist sehr wichtig. Denn darüber lässt sich steuern, wer einem eine Nachricht schicken darf oder sieht, ob man gerade online ist. So lassen sich zum Beispiel unerwünschte Gesprächspartner ausgrenzen.

AIM (AOL)

ICQ (AOL)

Google Talk

Windows Live Messenger

Yahoo Messenger

Skype

...

Eine netzübergreifende Kommunikation zwischen den verschiedenen IM-Anbietern ist nur selten möglich. Die

Ausnahme bildet AIM und ICQ und auch Microsoft und Yahoo haben sich testweise zusammen geschaltet. Wer sich in verschiedenen Netzen bewegt, der kann einen Multi-Protokoll-Client nutzen, der aber meist nur das Chatten beherrscht.

Internet-Telefonie

Internet-Telefonie ist eine Kommunikationstechnik um Sprache zwischen zwei Gesprächspartner über das Internet zu übertragen. Dabei bedient man sich eines Computers oder eines Telefons. Bei Benutzung eines Computers muss dieser eine spezielle Hardware- und Software-Ausstattung haben.

Als Internet-Telefonie aufkam war die Technik noch nicht ausgereift. Nach einem ersten Hype verschwand die Technik fast spurlos von der Bildfläche. Breitbandige Internet-Anschlüsse und

das einfache Vermittlungsprotokoll SIP waren dann die Faktoren, die erneut Dynamik in den Markt gebracht haben. Während die ersten Internet-Telefonie-Angebote qualitativ auf niedrigem Niveau lagen, kann man heute Internet-Telefonie fast uneingeschränkt empfehlen. Dank Breitband-Internet-Zugänge und der gut ausgebaute IP-Netze der Provider steht fast überall ausreichend Bandbreite für Internet-Telefonie zur Verfügung. Allerdings ist Internet-Telefonie immer noch etwas für Technik-Freaks oder Menschen mit hoher Frustrationsgrenze. Denn so gut Internet-Telefonie funktioniert, so kompliziert ist es einzurichten. In der Regel reicht es nicht aus, einfach nur ein Telefon in eine Telefondose zu stecken.

SIP-Provider

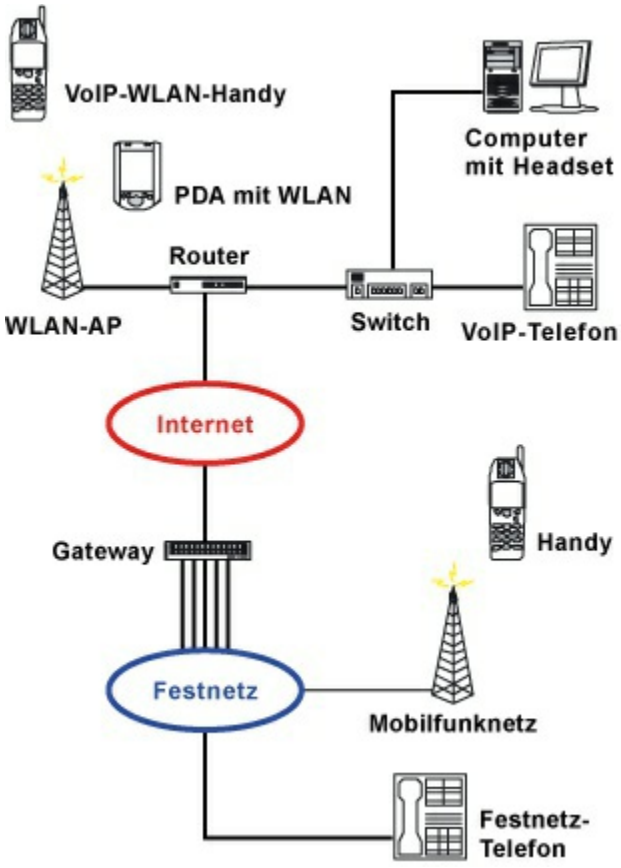
Es ist sehr einfach einen VoIP-Zugang für Internet-Telefonie zu bekommen.

Dazu meldet man sich bei einem VoIP-Anbieter an, der SIP-Provider genannt wird. Danach muss man nur noch den VoIP-Adapter, -Router oder -Client konfigurieren. Dann kann es auch schon losgehen.

Da die SIP-Provider häufig auch Internet-Provider sind fällt für die netzinternen Gespräche nur zusätzlicher Datenverkehr an, der sehr günstig im Netz des Providers abgewickelt wird. Die Nutzung der Infrastruktur ist durch den Internet-Zugang des Kunden schon bezahlt. Ein paar Gigabyte Daten mehr fallen kaum ins Gewicht. Deshalb sind netzinterne Telefongespräche in der Regel kostenlos. Nur die ausgehenden Gespräche in das herkömmliche Telefonnetz müssen vom Kunden bezahlt werden. Diese Verbindungen muss der SIP-Provider dem Unternehmen bezahlen, dass ihm den Zugang zum

Telefonnetz stellt. Sofern der Kunde eine eigene Ortsnetzrufnummer zugewiesen bekommen hat, sind auch eingehende Gespräche aus dem Telefonnetz möglich.

Endgeräte



Ein mögliches Endgerät wäre ein Computer mit SIP-Client und Headset, alternativ Lautsprecher und Mikrofon. Neben diesen klassischen Softphones gibt es auch telefonähnliche Endgeräte, die am USB angeschlossen werden und

zwingend einen eingeschalteten Computer erfordern.

Selbstverständlich lassen sich auch analoge Telefone als Endgerät nutzen. Zusammen mit einem Analog Telephone Adapter (ATA) kann jedes analoge Telefon zu einem VoIP-Telefon umgerüstet werden. Wer mehrere VoIP-Accounts nutzt, benötigt ein eigenes VoIP-Gateway, das man auch als VoIP-Telefonanlage bezeichnet.

Richtige VoIP-Telefone werden direkt an einem IP-Router bzw. einem Switch angeschlossen. Vorkonfiguriert lässt sich darüber genauso einfach telefonieren, wie mit einem herkömmlichen Telefon.

Wer es gerne schnurlos hat, der ist auf ein analoges Schnurlostelefon mit einem ATA angewiesen oder verwendet ein VoIP-Handy für WLAN.

Wer nicht nur zu hause, sondern auch unterwegs über WLAN-Hotspots

telefonieren will, muss einen PDA oder Laptop zusammen mit einem Softphone und Headset benutzen.

Internet-Telefonie mit dem PC

Internet-Telefonie über einen Computer dürfte von den Investitionskosten her, die günstigste Art sein um über das Internet zu telefonieren. In der Regel ist jeder Computer heute mit der nötigen Hardware (Lautsprecher, Mikrofon, Headset, vollduplexfähige Soundkarte) ausgestattet. Die Software (für H.323 oder SIP) erhält man meist als Freeware oder sie liegt dem Betriebssystem bei. Sobald man online ist, kann man billig über das Internet telefonieren.
Nachteilig ist jedoch, dass man nur dann erreichbar ist, wenn der Computer eingeschaltet, die Software geladen und der Computer mit dem Internet verbunden ist.

Datenvolumen und Traffic

Technisch bedingt wird bei VoIP bzw. Internet-Telefonie keine Leitung belegt. Zumindest nicht über die gesamte Strecke. Stattdessen wird die Bandbreite eines Internet-Anschlusses belastet, die in irgendeiner Weise bezahlt werden muss. Entweder als Flatrate, volumenbasiert oder minutenbasiert. Im Fall der Flatrate und der Abrechnung nach Minuten spielt das verbrauchte Volumen keine Rolle. Wird der Internet-Anschluss allerdings nach übertragenen MByte oder GByte abgerechnet, dann ist es schon von Interesse wie viel ein Internet-Telefonat an MByte kostet. Grundsätzlich ist es schwierig das Volumen bzw. die Kosten dafür im Voraus abzuschätzen oder zu berechnen.

Protokoll-Overhead durch RTP:

Bit

64

Protokoll-Overhead durch UDP:

Bit

160

Protokoll-Overhead durch IP:

Bit

Protokoll-Overhead durch PPP

16

(bei T-DSL):

Bit

Protokoll-Overhead durch

48

PPPoE (bei T-DSL):

Bit

Protokoll-Overhead durch

144

Ethernet (bei T-DSL):

Bit

Summe Protokoll-Overhead pro

528

Datenpaket:

Bit

Man kann sich aber an einem Richtwert halten, der so ungefähr gelten kann: Jedes Datenpaket enthält die Sprache von 20 ms, so das pro Sekunde 50 Datenpakete anfallen. Das ist ein Protokoll-Overhead von insgesamt 26,4 kBit pro Sekunde.

Bitrate

Bitrate

Codec

Codec

Ethernet

G.711

64 kBit/s

88 kBit/s

G.722

64 kBit/s

88 kBit/s

G.723

6,4 kBit/s

22 kBit/s

G.726- 24 kBit/s

47 kBit/s

24

G.726- 32 kBit/s

55 kBit/s

32

G.726- 40 kBit/s

64 kBit/s

40

G.728

16 kBit/s

32 kBit/s

G.729

8 kBit/s

32 kBit/s

iLBC

13,3 kBit/s

27 kBit/s

GSM

13 kBit/s

35 kBit/s

2 bis 44

Speex

variabel

kBit/s

Für VoIP werden in der Regel zwei verschieden Sprach-Codecs verwendet. Entweder einer mit 8 kBit/s (G.729) oder einer mit 64 kBit/s (G.711). Je nach Codec muss man also mit 34 oder 90 kBit/s rechnen. Da Sprache immer in zwei Richtungen übertragen wird, muss dieser Wert nochmals verdoppelt werden.

In Summe kommt man pro Gesprächsminute auf 0,5 bis 1,4 MByte, je nach dem, welcher Codec verwendet wird.

Bandbreite und Latenzzeit

Für Internet-Telefonie ist ein Breitbandanschluss mit mindestens 100 kBit/s in beide Richtungen (Downstream und Upstream) notwendig. T-DSL light und ISDN sind nur unter der Voraussetzung nutzbar, wenn der

verwendete Sprachcodec sich mit einer geringeren Bandbreite zu Frieden gibt. Schlimmer noch als ungenügende Bandbreite, ist eine schwankende oder sogar ganz schlechte Latenzzeit. Immer dann, wenn sich auf der gesamte Übertragungsstrecke mehrere Teilnehmer die Bandbreite teilen, kommt es zu Verzögerungen der Datenpakete. Es kommt zu Aussetzern und es besteht die Gefahr, dass die Verbindung ganz abbricht.

Komplett ungeeignet sind Satellitenverbindungen. Dort sind die Laufzeiten der Signale sehr lang und die Latenzzeit stark schwankend.

Internet-Fax

Für Fax-Übertragungen per VoIP ist zwingend der Codec G.711 notwendig. Nur er bietet die notwendige Übertragungsqualität, um mit der Standardgeschwindigkeit von 9600 Bit/s

Faxe zu übertragen.

Mit Codecs wie G.729 funktioniert Faxen nicht, da dieser Codec für Sprachübertragung optimiert ist. Für digitale Fax-Übertragungen ist T.38 vorgesehen.

VoIP als Festnetz-Ersatz

Mit Anbietern, die ein NGN betreiben und Telefonie intern auf Basis von VoIP abwickeln ist die bequemste und einfachste Art Internet-Telefonie zu nutzen. Außerdem ist es für den Kunden vollkommen transparent. Er kann seine alten Endgeräte ohne Probleme weiter betreiben. So kann er störungsfrei und zuverlässig telefonieren und faxen. Begünstigt durch breitbandige Internet-Anschlüsse, Pauschaltarife, offene Standards für Voice over IP und die einfachere Vergabe von Festnetzrufnummern steigen viele Internet-Dienstleister auf den VoIP-Zug

mit auf. Und auch große Netzbetreiber wollen ihre Netze auf Internet-Übertragungstechniken umstellen. Mit der Einführung und Umstellung auf ein NGN sollen die Kosten gesenkt und die Netzstruktur vereinfacht werden.
Das größte Problem ist, dass Teile der Verbindungsvermittlung zum Kunde gewandert ist. Auf das, was dort passiert hat der Provider keinen Einfluss.
Minderwertige VoIP-Adapter mit instabilen DSL-Anschlüssen können nicht mit der guten alten Telefontechnik konkurrieren. Gelegentlich muss man mit Verbindungsabbrüche, Aussetzer und Echos leben. Die Qualität von VoIP kommt also an das zuverlässige und qualitativ hochwertige Telefonnetz nicht heran. Ein besonderer Knackpunkt, wenn die Internet-Verbindung ausfällt, dann ist zwangsläufig auch das Telefon tot.
Kein VoIP-Provider unterstützt alle

Sonderrufnummern oder Notrufe. Man hat den Eindruck, die VoIP-Angebote befinden sich im Beta-Stadium. Möglicherweise wird das noch eine ganze Weile so bleiben. Das Problem mit der ortsunabhängigen Rufnummer soll durch eine bundeseinheitliche Notrufabfragestelle mit automatisierter Standortbestimmung gelöst werden.

P2P - Peer-to-Peer

Peer-to-Peer-Netze haben einen zweifelhaften Ruf. Bekannt geworden durch die Nutzung in Dateitauschbörsen zum illegalen Tauschen von Musik- und Video-Dateien, scheint diese Technik für nichts anderes brauchbar zu sein. Allerdings ist die Mächtigkeit dieser Technik bei weitem nicht ausgeschöpft. Auf einen Nenner gebracht, ermöglicht P2P das massenhafte verteilen von Dateien.

Die Peer-to-Peer-Technik ist eine

zukunftsträchtige Technik und für eine Vielzahl von Anwendungen geeignet.

Informationsrecherche und Suchmaschinen

In Zukunft werden sich weitere Anwendungen finden. Denkbar ist ein Suchsystem, das über die klassischen Suchsysteme mit ihren Spidern und Robotern hinausgeht. Da sich klassische Suchmaschinen mit Metadaten und Katalogisierungsinformationen schwer tun (hohe Manipulationsgefahr), wird mit einem geeigneten Werkzeug Datensammlungen katalogisiert und anderen zu Verfügung gestellt. Was mit MP3-Dateien hervorragend funktioniert, ist auch mit Word-, PDF-, Excel- und anderen Dateien möglich.

Software-Vertrieb

Auch der Software-Vertrieb, egal ob kommerziell oder Freeware lässt sich mit P2P vereinfachen. Bisher wurden

Downloads auf Serverfarmen gespeichert und angeboten. Mit P2P lassen sich Dateien auf viele einzelne Computer verteilen, die dann regionale Netzwerke bedienen. So lässt sich viel Übertragungskapazität auf den Überland-Backbones vermeiden.

Spam-Bekämpfung

Ebenso eignet sich P2P bei der Spam-Bekämpfung. Ein kleiner Software-Agent analysiert eingehenden E-Mail-Verkehr. E-Mails, die an verschiedenen Orten zugleich auftreten, werden als Spam erkannt und herausgefiltert. Diese Funktion ist bereits im Anti-Spam-Produkt SpamAssassin integriert.

Datensicherung / Backup

Eine weitere Möglichkeit von P2P ist die Datensicherung. Ein installierter Client prüft den freien Speicherplatz und tauscht lokale Dateien mit anderen beteiligten Systemen aus. Müssen

Dateien wieder hergestellt werden, werden die Dateien von den anderen Systemen zurück gesichert.

Namensauflösung

Im TCP/IP-Netzwerk werden Stationen mit ihrer IP-Adresse angesprochen. Die IP-Adresse in binärer Form ist eine 32-Bit-Folge von 1en und 0en. Dadurch können digital arbeitenden elektronischen Schaltungen und Programmen de IP-Adressen schneller verarbeiten. Doch weder die 32-Bit-Folge, noch die IP-Adresse sind für das menschliche Gehirn einfach zu erfassen und zu merken. Der Mensch verwendet lieber Namen um eine Sache zu benennen und zu identifizieren. Diese Tatsache ist in den 70er-Jahren in das ARPANET, dem ursprünglichen Vorgänger des Internets, mit eingeflossen. Statt der IP-Adressen wurden Namen zur Adressierung von

Computern verwendet. Diese waren 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. Für ihn besteht die Welt immer noch aus Bit und Byte. Und deshalb braucht er immer eine binäre Adresse. Aus diesem Grund wurden mehrere Methode entwickelt, um eine Namensauflösung von Namen in numerische Adressen zu realisieren.

hosts

Jedes TCP/IP-Betriebssystem hat eine Datei mit dem Namen hosts. In ihr sind die IP-Adressen und Namen tabellenartig aufgelistet.

lmhosts

Die Datei lmhosts ist ausschließlich in Windows-Betriebssystemen zu finden. Neben den IP-Adressen sind dort NetBIOS-Namen enthalten.

DNS - Domain Name System

DNS ist eine servergestützte Struktur zur Auflösung von Namen in IP-Adressen. Der Client, der einen DNS-Namen in eine IP-Adresse aufgelöst haben will, stellt eine Anfrage an den DNS-Server. Der DNS-Server verwaltet IP-Adressen und die dazugehörigen Namen in einer Datenbank. Ist ein Name dort nicht enthalten, befragt er einen übergeordneten DNS-Server, bis eine IP-Adresse an den anfragenden Client zurück geliefert werden kann.

WINS - Windows Internet Name Service

WINS ist ein plattformabhängiges, auf Windows-basierendes, System zur Namensauflösung. Es baut auf den NetBIOS-Dienst der Windows-Betriebssysteme auf. WINS wurde eingeführt, um die NetBIOS-

Rundsprüche zur Namensauflösung zu reduzieren. Wie bei DNS greift der Client auf den WINS-Server zu, um einen Namen in eine IP-Adresse umzuwandeln.

Ablauf einer Namensauflösung

1. Als erstes prüft der Client in seinem lokalen Cache, ob eine Adresse für den Namen vorliegt.
2. Wenn nicht, sieht er in der Datei hosts nach.
3. Findet er auch dort den Namen nicht stellt er eine Anfrage an den DNS-Server.

Zusätzliche Namensauflösung in Windows

Findet die Suche über den DNS-Server die IP-Adresse nicht, wird der WINS-Server befragt.

Kennt auch dieser den Namen nicht,

wird ein NetBIOS-Rundspruch

abgesetzt.

Als letzter Strohhalm bei der

NetBIOS-Namensauflösung ist die

lmhosts-Datei.

DNS - Domain

Name System

Um einen Server im Internet adressieren

zu können benötigt man seine IP-

Adresse. Üblicherweise sind aber nur

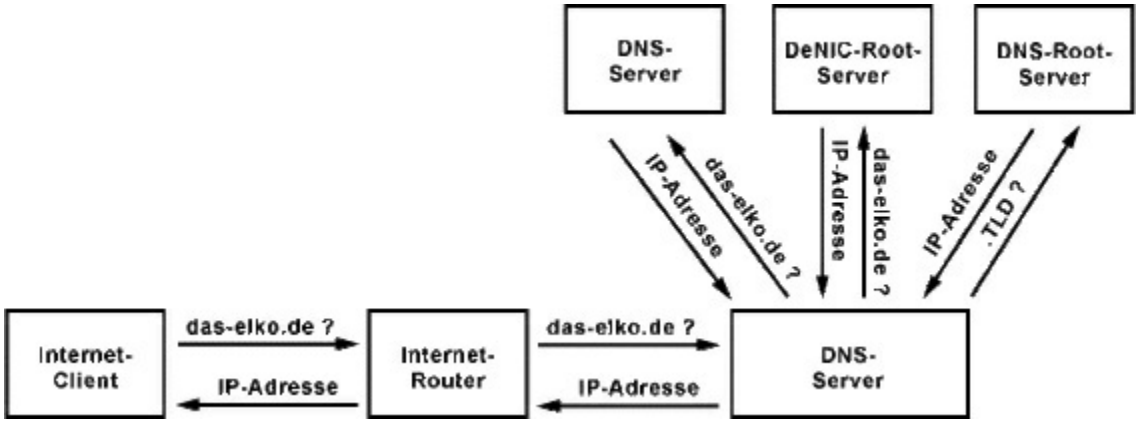
Domain-Namen und Computernamen der

Server bekannt. Das Domain Name

System, kurz DNS, ist ein System zur

Auflösung von Computernamen in IP-

Adressen und umgekehrt.



Möchte man zum Beispiel die Webseite

www.elektronik-kompendium.de

besuchen, dann fragt der Browser zuerst seinen DNS-Server. Bei einem normalen Internet-Nutzer ist das der DNS-Server des Internet-Providers. Unternehmen mit großen Netzen betreiben häufig einen eigenen DNS-Server. Wenn der angefragte DNS-Server die IP-Adresse zu diesem Domain-Namen weiß, dann liefert er sie zurück. Wenn nicht, dann befragt der DNS-Server weitere DNS-Server. Das macht er so lange, bis er die IP-Adresse des Domain-Namens an den Browser zurückliefern kann.

Da ohne DNS das Internet praktisch nicht existieren kann, gibt es viele tausend DNS-Server auf der ganzen Welt, die zusätzlich hierarchisch angeordnet sind und sich gegenseitig auf dem Laufenden halten und über Änderungen informieren.

DNS geht auf die Datei hosts zurück,

deren Inhalt zur Namensauflösung im ARPANET diente und händisch gepflegt werden musste. Mit zunehmender Anzahl der Hosts im ARPANET wuchst der Bedarf für ein verteiltes und hierarchisches 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.

Domain-Name

Domain-Namen dienen dazu, um Computer, die mit kaum merkbaren IP-Adressen adressiert sind, richtige Namen zu geben und gleichzeitig in eine hierarchische Struktur zu unterteilen.

Das DNS kümmert sich im Hintergrund um die Zuordnung von IP-Adresse zu Domain-Name.

Domain-Namen haben eine bestimmte

Struktur und sind Teil einem Uniform Resource Locator (URL). Der, nicht die, wird zu Deutsch als "einheitliche Angabeform für Ressourcen" bezeichnet. Die für DNS verwendete Struktur (URL) besteht aus drei oder mehr Teilen:

Second-Level-Domain (SLD)	**Top-Level-Domain (TLD)**	**Computername (Host oder Dienst)**
elektronik-kompendium.	de	www.
elektronik-kompendium.	de	ftp.

kompendium.

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)**
www.	dse-faq.	kompendium.

Eine URL 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 in Englisch als Country-Code Top-Level-Domains (ccTLD) bekannt sind. Dann gibt es noch die organisatorischen oder generischen Top-Level-Domains (Generic Top-Level-Domain, gTLD).
An letzter Stelle, jedoch nicht zwingend erforderlich, steht der Computername oder Hostname, der meistens auf einen Dienst hindeutet.
Die einzelnen Unterteilungen bzw. Ebenen werden durch Punkte voneinander getrennt. Zur Vervollständigung hat eine URL ein vorangestelltes Kürzel, das den verwendeten Dienst kennzeichnet (http:// oder ftp://). Es handelt sich dabei um eine optionale Angabe, die auch nur für Anwendungsprogramme wichtig ist.

Organisatorische Top-Level-Domains (TLD)

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 Vereinigten Staaten von Amerika
.info	

Informationsdienste

International tätige

.int

Institutionen

Militär der Vereinigten

.mil

Staaten von Amerika

.museum Museen

.name

Privatpersonen

Netzspezifische Dienste und

.net

Angebote

Nichtkommerzielle

.org

Unternehmungen und Projekte

Professionals, spezielle

.pro

Berufsgruppen

...

Geografische Top-Level-

Domains (TLD)

Domain	**Land**
(ccTLD)	
.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

Vereinigtes

.uk

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.
Einige Länder bilden Second-Level-

Domains unterhalb des Ländercodes ähnlich der generischen Top-Level-Domains (z. B. .co.uk).
Unterhalb der Second-Level-Domain können weitere Sub-Level-Domains (Subdomains) vorhanden sein, für die der Inhaber der Second-Level-Domain verantwortlich ist.

Nameserver / DNS-Server

Ein DNS-Server tritt selten alleine auf. Es gibt immer einen Primary und einen 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.
Damit nicht bei jeder DNS-Anfrage das Netzwerk belastet werden muss, hat jeder DNS-Server einen Cache, in dem

er erfolgreiche DNS-Anfragen speichert. Bei wiederholtem Aufruf holt er die IP-Adressen bereits erfolgreich aufgelöste Domain-Namen aus dem Cache. Die gespeicherten Informationen haben eine Lebensdauer (Time-To-Live, TTL) von ca. 2 Tagen. Wird eine IP-Adresse durch den Umzug eines Domain-Namens geändert, ist die Domain nach spätestens 2 Tagen wieder im ganzen Internet erreichbar.

Neben den ganz normalen DNS-Servern gibt es auch die Root-Server, von denen es weltweit nur 13 Stück gibt. 10 davon stehen in den USA. Die 3 anderen befinden sich in London, Stockholm und Tokio.

Resolver / DNS-Client

Der DNS-Client (Resolver) ist direkt in TCP/IP integriert und steht dort als Software-Bibliothek für die DNS-Namensauflösung zur Verfügung. Der

DNS-Client wird als Resolver bezeichnet und ist der Mittler zwischen DNS und dem Anwendungsprogramm. 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-Server, die in den TCP/IP-Einstellungen eingetragen oder über DHCP angefordert werden müssen.

Ablauf der Namensauflösung mit DNS

Grundsätzlich unterscheidet man zwischen der rekursiven und der iterativen Namensauflösung. Einer der beiden Abfragetypen wird zusammen mit dem Domain-Namen an den Resolver übermittelt.

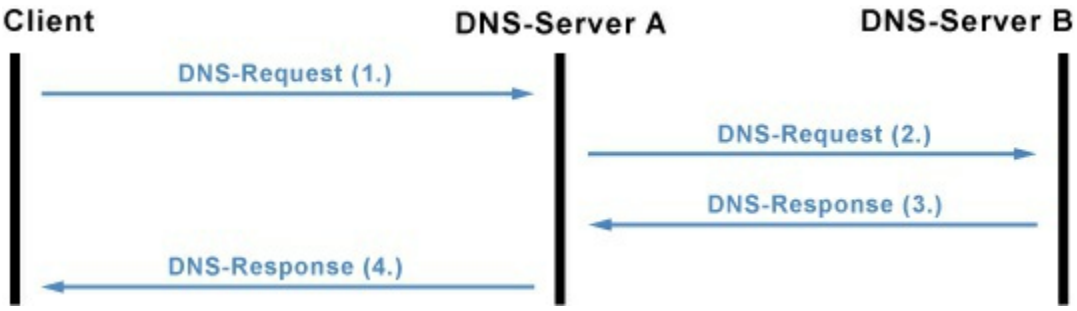
Rekursion / rekursive DNS-

Abfrage

Iteration / iterative DNS-Abfrage

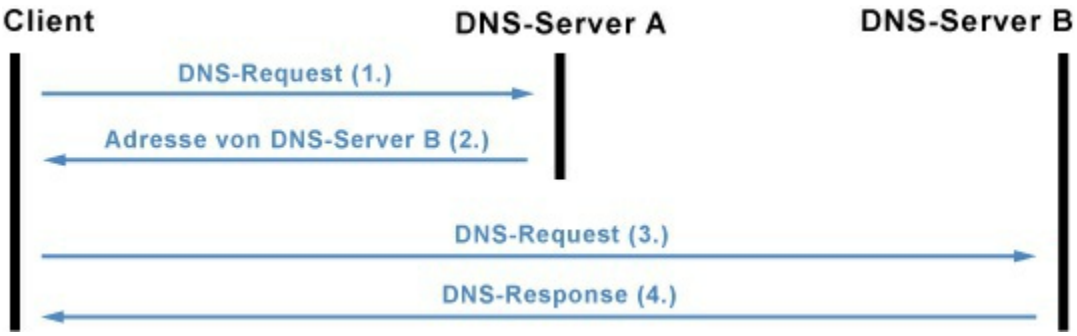
Damit ein beliebiger Server, über den nur der Domain-Name bekannt ist, kontaktiert werden kann, muss seine IP-Adresse bekannt sein. Dazu befragt der Resolver des TCP/IP-Clients den hinterlegten DNS-Server (1.).

Rekursion



Bei der rekursiven Abfrage übergibt der Resolver (Client) die Namensauflösung an einen DNS-Server (1.). Wenn dieser den Domain-Namen nicht auflösen kann, fragt der DNS-Server bei weiteren DNS-Servern nach (2.), bis der Domain-Name aufgelöst ist (3.) und die Antwort vom DNS-Server an den Resolver

zurückgeliefert werden kann (4.). Der Resolver übergibt die Antwort dann an das Anwendungsprogramm.



Iteration

Bei der iterativen Abfrage liefert der DNS-Server nur die Adresse des nächsten abzufragenden DNS-Servers zurück (2.). Der Resolver muss sich dann um die weiteren Anfragen kümmern (3.), bis der Domain-Name vollständig aufgelöst ist (4.).

DNS-Protokoll

DNS ist auf der Anwendungsschicht des OSI-Schichtenmodells angeordnet. Deshalb nutzt es zur Übertragung TCP und UDP auf dem Port 53. In der Regel verwendet der Resolver das UDP-

Protokoll. Wenn die Antwort größer als 512 Byte ist, werden nur 512 Byte übertragen. Anschließend muss der Resolver seine Anfrage noch mal über TCP wiederholen, damit die Antwort in mehrere Segmente aufgeteilt werden kann. Der Datenaustausch zwischen dem Primary und Secondary DNS-Server wird ausschließlich mit TCP geregelt.

OpenDNS

OpenDNS ist ein kostenloser Dienst, der DNS-Abfragen beantwortet. OpenDNS bietet Auflösung von DNS-Namen für Privatpersonen und Firmen an. Es handelt sich dabei um eine Alternative zur Nutzung des DNS-Servers des eigenen Internet Service Providers (ISP).

WINS - Windows Internet Name Service

Der WINS Internet Name Service

(WINS) ist ein Dienst unter Windows NT und Windows 2000, der die Namensauflösung von NetBIOS-Computernamen vornimmt. Der Einsatz eines WINS-Servers macht die Nutzung und Verwaltung der Datei lmhosts überflüssig und verhindert die netzbelastenden Rundsprüche bei der NetBIOS-Namensauflösung.

Funktionsweise

WINS ist ein dynamischer Namensdienst, der die Verwaltung in Verbindung mit den WINS-Clients selbständig abwickelt und so gut wie keinen Eingriff eines Administrators erfordert. Im Prinzip ist es so, dass sich WINS-Server und WINS-Client die Arbeit teilen. Wenn der WINS-Client gestartet wird, meldet er seinen NetBIOS-Computernamen und seine IP-Adresse an den WINS-Server. Dieser trägt Name und Adresse in seine

Datenbank ein. Will eine Station einen Computernamen aufgelöst haben, nimmt sie Kontakt zum WINS-Server auf. Der sieht in seiner Datenbank nach und liefert gegebenenfalls die IP-Adresse zurück.

Generell gilt, dass jeder Name in die WINS-Datenbank eingetragen wird, sofern er nicht bereits verwendet wird. Üblicherweise melden sich die Stationen z. B. beim Herunterfahren wieder vom WINS-Dienst ab. Dadurch wird der NetBIOS-Name wieder freigegeben und kann von einer anderen Station verwendet werden. Wenn durch einen Computerabsturz oder Netzwerkausfall das Abmelden nicht erfolgt ist, entsteht eine Leiche im Datenbestand des WINS-Servers. Der verwendete Computername ist dann blockiert. Aus diesem Grund haben alle NetBIOS-Namen eine begrenzte

Gültigkeit. In der Datenbank des WINS-Servers werden die Einträge mit einem Laufzeit-Wert (Time-To-Live, TTL) versehen. Vor Ablauf der Laufzeit muss der Client seinen Namen erneut beim WINS-Server anmelden und die Lebensdauer verlängern.
Die Kommunikation des WINS-Dienstes erfolgt mit UDP über den Port 137.

WINS-Server

In der Regel reicht die Verwendung eines WINS-Servers aus. Fällt dieser aus, steht ein großer Teil des Netzwerkes, weil die meisten Stationen über die Computernamen miteinander kommunizieren. Ist eine Auflösung der NetBIOS-Namen nicht mehr möglich, wird das Netzwerk dadurch empfindlich gestört. Deshalb empfiehlt sich in großen Netzwerken einen Primary und einen Secondary WINS-Server zu installieren. Die Server sollten voneinander

unabhängig und redundant ausgelegt sein. Da die beiden WINS-Server ihren Datenbestand regelmäßig abgleichen, führt der Ausfall eines Servers nicht zum Ausfall des gesamten Netzwerks.

Bonjour / Zeroconf

Bonjour ist eine Protokoll-Sammlung auf Basis von IP, DNS und NAT, um Netzwerkdienste, die in einem IP-Netz bereitgestellt werden, automatisch erkennen zu können. Bonjour, dass auch als Zeroconf bezeichnet wird, ist der Nachfolger von AppleTalk. Bonjour wurde von Apple im Jahr 2002 ins Leben gerufen und gibt es nicht nur für Mac OS X, sondern auch für Linux (Avahi) und Windows (Bonjour).
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 er von anderen Stationen automatisch gefunden werden kann. Dabei kommt man ohne zentralen Server aus, der die Adressen, Portnummern und Servernamen verteilt. Die Dienste melden sich dynamisch an und ab.
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. Multicast-Pakete werden nicht zwischen den Segmenten geroutet. Damit Bonjour-Informationen 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.

DynDNS

DynDNS oder DDNS ist ein System, das Domain-Name-Einträge in Echtzeit aktualisieren kann. Unter DynDNS versteht man in der Regel einen DNS-Dienst, der die ständig wechselnden IP-Adressen für einen festen Domain-Namen bereithält. Unter DDNS versteht man in der Regel einen Aktualisierungsmechanismus für DNS-Einträge.

Warum braucht man DynDNS?

Will man das eigene Netzwerk zum Beispiel über einen DSL-Anschluss dauerhaft im Internet erreichbar machen, zum Beispiel einen Server, dann braucht man eine ständig gültige einmalige Adresse. Doch das scheitert in der Regel an der Vergabe dynamischer IP-Adressen durch den Internet-Provider. Gemeint ist, dass der eigenen Internet-Anschluss regelmäßig eine neue IP-

Adresse bekommt. Das bedeutet, diese IP-Adresse ändert sich ständig und kann deshalb nicht als Ziel-Adresse dauerhaft genutzt werden. In der Konsequenz wäre das Netzwerk dauerhaft nicht erreichbar. Dienste, wie DynDNS sorgen nun dafür, dass Netzwerke oder Stationen im Internet mit wechselnden IP-Adressen über einen Domain-Namen erreichbar sind.

Wie funktioniert DynDNS?

Da man in der Regel mit Domain-Namen und nicht mit IP-Adressen bei der Adressierung arbeitet, benötigt man einen Dienst, der die IP-Adresse ständig aktualisiert und einem Domain-Namen zuordnen kann.

Dienste, wie zum Beispiel DynDNS.org, bieten Subdomain-Adressen kostenlos an, die man im eigenen Internet-Zugangs-Router einträgt. Immer dann, wenn sich die IP-Adresse des Routers ändert,

meldet der Router die IP-Adresse an DynDNS.org. Von diesem Dienst wird bei einer DNS-Anfrage mit dem eigenen Domain-Namen immer die aktuelle IP-Adresse zurückgeliefert. Das setzt voraus, dass der Router DynDNS unterstützt.

Anwendungen von DynDNS

DynDNS eignet sich zum Beispiel zum Verbindungsaufbau eines VPN-Zugangs zu einen LAN, welches über keine eigene feste IP-Adresse verfügt. Ebenso kann über den Domain-Namen ein Web- oder FTP-Server erreichbar sein. Die Möglichkeiten sind vielfältig.

HTTP - Hypertext Transfer Protocol

HTTP ist das Kommunikationsprotokoll im World Wide Web (WWW). Die wichtigsten Funktionen sind Dateien vom Webserver anzufordern und zum Browser zu schicken. Der Browser

übernimmt dann die Darstellung von

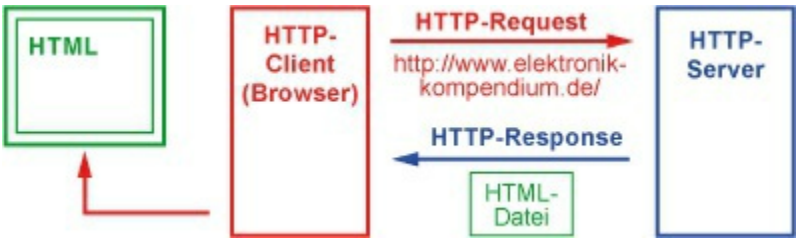
Texten und Bilder und kümmert sich um

das Abspielen von Audio und Video.

Das Hypertext Transfer

Protocol (HTTP) im

Schichtenmodell



Dienste / Protokolle /

Schicht

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 an den HTTP-Server. Dieser bearbeitet die Anfrage und schickt seine Antwort zurück. Diese Kommunikation zwischen Client und Server findet auf Basis von Meldungen im Text-Format statt. Die Meldungen werden standardmäßig über TCP auf dem Port 80 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.

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 eine URL 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*

Die 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 die 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-Request-Header

Methode URL HTTP/Version

General Header

Request Header

Entity Header (optional)

Leerzeile (!)

Request Entity (falls vorhanden)

Beispiel für einen HTTP-Request-Header

Im folgenden wird der HTTP-Request-Header dargestellt, den der Browser an den Webserver schickt.

GET / HTTP/1.1

Host: www.elektronik-kompendium.de

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.9.1.2) Gecko/20090729 Firefox/3.5.2 (.NET CLR 3.5.30729)

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: de-de,de;q=0.8,en-us;q=0.5,en;q=0.3

Accept-Encoding: gzip,deflate

Accept-Charset: ISO-8859-1,utf-

8;q=0.7,*;q=0.7

Keep-Alive: 300

Connection: keep-alive

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-Header

HTTP/Version Response-Code (Status)
Klartext-Meldung (Reason)
General Header
Response Header
Entity Header (optional)
Leerzeile (!)
Resource Entity (falls vorhanden)

Beispiel für einen HTTP-Response-Header

Im folgenden wird der HTTP-Response-Header dargestellt, den der Webserver an den Browser schickt und dem eine Datei folgt. Im folgenden wird nur die

HTML-Datei zurück geliefert. Aufgrund Referenzierungen in der HTML-Datei schickt der Browser weitere HTTP-Requests an den Server. Er fordert weitere Dateien an. Zum Beispiel CSS, Javascript, Bilder, Audio oder Video.

```
HTTP/1.x 200 OK
Date: Tue, 08 Sep 2009 15:47:06 GMT
Server: Apache/1.3.34 Ben-SSL/1.55
Keep-Alive: timeout=2, max=200
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html
```

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.

Status-Codes	**Beschreibung**
Status-Codes im 100er Bereich	
100-199	sind Meldungen informeller Art.
Status-Codes im 200er Bereich	
200-299	informieren den Client über eine erfolgreiche Anfrage.
Status-Codes im 300er Bereich	

deuten auf eine Umleitung hin

und weisen den Client an, seine

300-

Anfrage auf das

399

zurückgelieferte Ziel zu

wiederholen oder den Benutzer

die Entscheidung treffen zu

lassen.

Status-Codes im 400er Bereich

sind Fehlermeldungen, die vom

400-

Client ausgelöst werden.

499

Meistens handelt es sich um

eine Anfrage, die vom Server

nicht beantwortet werden kann.

Status-Codes im 500er Bereich

500-

sind Fehlermeldungen, die vom

599

Server direkt ausgelöst werden.

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)
	Immer dann, wenn keine HTML-Datei zurückgeliefert werden kann, dann erfolgt die

404

Rückmeldung eines 404-Errors.

Meistens liefert der Server eine

Standard-Fehlerseite zurück.

Ein HTTP-Server kann nicht

nur HTML-Dateien schicken,

sondern auch Programme und

Skripte ausführen, die HTML-

500

Daten zurückliefern. Kommt es

bei der Ausführung zu einem

Fehler, bricht der Server den

Vorgang ab und liefert diese

Fehlermeldung zurück.

HTTP-Authentifizierung

Manche Informationen und Daten auf

einem Webserver sind nicht für

jedermann bestimmt und sollen nur einer

begrenzten Zahl von Personen zugänglich

sein. Dazu gibt es das Basic-HTTP-

Authentication-Schema, das einen

Benutzernamen und ein Passwort für die

Authentifizierung verwendet.

Der Ablauf der Authentifizierung beginnt mit einem normalen HTTP-Request durch den HTTP-Client. Ist der Zugriff auf das angefragte Verzeichnis durch Basic-HTTP-Authentication beschränkt, sendet der HTTP-Server den HTTP-Response mit einem WWW-Authentication-Header-Feld und dem Status-Code 401 (Nicht autorisiert). Der HTTP-Client wird damit zum Senden von Benutzernamen und Passwort aufgefordert. Der HTTP-Client öffnet dann ein Fensterchen, das den Benutzer zur Eingabe von Benutzername und Passwort auffordert. Nach abgeschlossener Eingabe schickt der HTTP-Client die Zugangsdaten an den Server. Sind die Daten korrekt, wird der Zugriff auf die angeforderten Inhalte freigegeben und vom Server ausgeliefert. Bei jedem erneuten HTTP-

Request werden die Anmeldedaten erneut vom Client an den Server übermittelt.
Sind die Zugangsdaten inkorrekt, hat der Benutzer mehrmals die Möglichkeit für eine korrekte Eingabe zu sorgen. Gehen diese Anfragen alle schief, wird ein Status-Code von 403 und einer entsprechenden HTML-Datei vom Server geschickt, die den Besucher auf den fehlerhaften Zugriff des passwortgeschützten Bereichs hinweist.
Der Authentifizierungsvorgang mit Basic-HTTP-Authentication ist alles andere als sicher. Die Anmeldedaten werden in Klartext und damit protokollierbar und abhörbar übertragen. Um diese Schwäche zu vermeiden empfiehlt sich das Digest Access Authentication. Dieses benutzt mehrere Parameter zur Verschlüsselung.

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 Medium. WebDAV eignet sich für das Hochladen und Herunterladen von Dateien. Denkbare Anwendungen sind virtuelle Festplatten oder auch der E-Mail-Transport. WebDAV soll die Einschränkungen von HTTP aufheben. Es ist in der Lage Dateien entgegen zunehmen und auf einen Datenträger abzulegen. Diese Disziplin war lange Zeit dem FTP-Protokoll überlassen. Z. B. um Websites zu aktualisieren und zu verwalten.

WebDAV ist darauf ausgelegt, Webseiten im Team zu entwickeln. Es stellt Funktionen für die Namens- und Versionsverwaltung zur Verfügung. WebDAV-Zugänge lassen sich nahtlos in jedes Betriebssystem integrieren. Der Zugriff darauf ist so einfach, wie das Arbeiten mit Dateien auf dem lokalen System.

Sperrmechanismus und Versionsverwaltung

Das Überschreiben von Änderungen bei gleichzeitigem Zugriff mehrere Personen wird verhindert. Eine in Bearbeitung befindliche Datei kann von anderen Personen nur gelesen aber nicht überschrieben werden.

Ältere Versionen von Dateien werden gespeichert. Ist eine neue Datei unbrauchbar, kann die alte Datei wieder hergestellt werden.

Metadaten und Properties

WebDAV erweitert die Metadaten um Properties, die jeweils aus einem Namen und einem Wert bestehen. Das sind zum Beispiel Speicherdatum, bearbeitende Person und Content-Type (Inhalt). Es lassen sich beliebig weitere Properties definieren.

Neben reinem HTTP beherrscht WebDAV auch XML für die Übertragung von Parametern.

Namensverwaltung und Collections

Mit den Collections lassen sich Dateien in Ordnern organisieren. Neben dem Lesen und Schreiben von Dateien ist es möglich, die gesamte Ordnerstruktur einzusehen, Ordner zu kopieren und zu verschieben. Genauso wie in einem Dateimanager.

WebDAV-Befehle

Befehl

Beschreibung

PROPFIND Properties auslesen

PROPATCH Propertie ändern

MKCOL

Collection anlegen

Herunterladen einer

GET

Datei

PUT

Hochladen einer Datei

DELETE

Löschen einer Datei

COPY

Kopieren einer Datei

MOVE

Verschieben einer Datei

Sperren von Dateien oder

LOCK

Collections

Entsperren von Dateien

UNLOCK

oder Collections

FTP - File

Transfer Protocol

FTP ist ein Kommunikationsprotokoll, um Dateien zwischen zwei 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

Dienste / Protokolle / Schicht

Anwendungen

Anwendung FTP HTTP DNS SNMP

Transport

TCP

UDP

Internet

IP (IPv4 / IPv6)

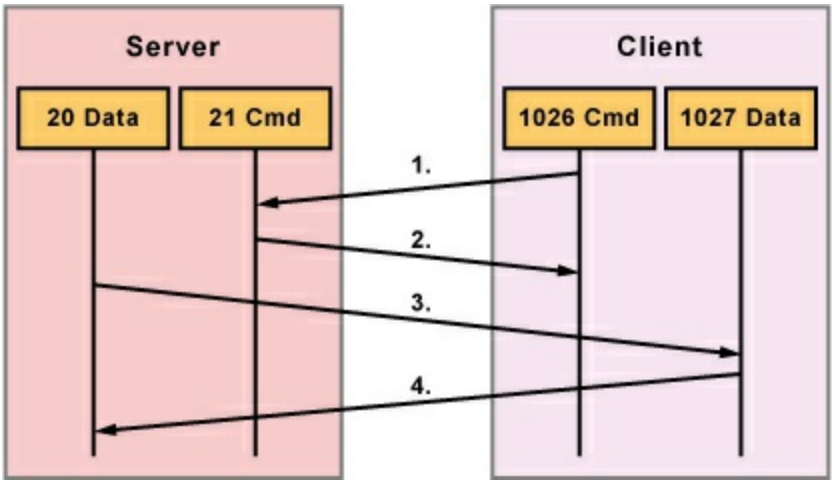
Netzzugang

Ethernet, ...

Wie funktioniert FTP?

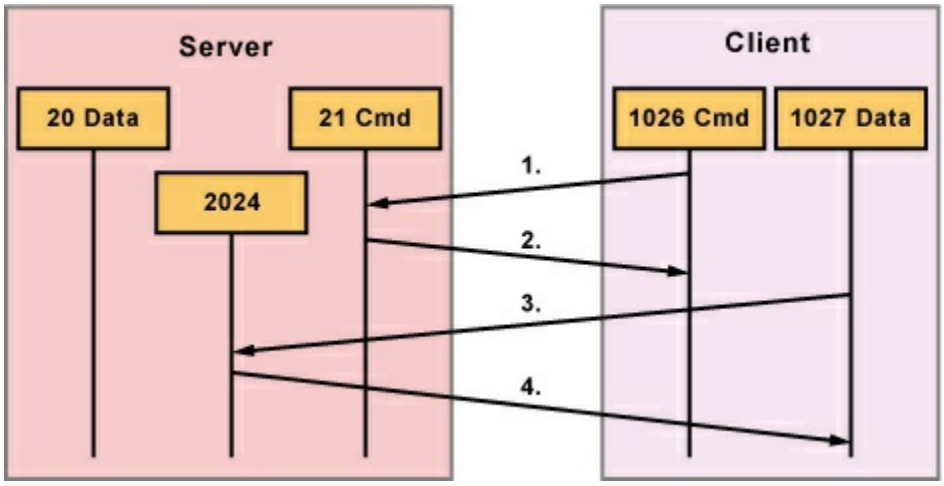
Die Kommunikation findet nach dem Client-Server-Prinzip statt. Zusätzlich erzeugt FTP zwischen Client und Server zwei logische Verbindungen. Die erste Verbindung ist der Steuerkanal (command channel) über den TCP-Port 21. Dieser Kanal dient ausschließlich zur Übertragung von FTP-Kommandos

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 Steuerkanal wird vom FTP-Client aufgebaut. Steht der Steuerkanal wird der Datenkanal vom FTP-Server initiiert. Befindet sich der FTP-Client hinter einem NAT-Router oder einer Firewall kommt die Verbindung nicht zustande. Die Verbindungsanforderung vom Server an den Client wird von der Firewall bzw. dem Router abgeblockt. Für diesen Fall gibt es das passive FTP, bei dem der Client den Datenkanal initiiert.



FTP Active Mode

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

Da ein FTP-Client in der Regel 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.

FTP-Verbindung

Am Anfang jeder FTP-Verbindung steht die Authentifizierung des Benutzers. Danach erfolgt der Aufbau des Steuerkanals über Port 21 und des Datenkanals über Port 20. Wenn die Dateiübertragungen abgeschlossen sind, werden die Verbindungen vom Benutzer oder vom Server (Timeout) beendet.
Das FTP-Protokoll kennt zwei verschiedene Übertragungsmodi. Den ASCII-Modus und den Binary-Modus. Die beiden Modi unterscheiden sich in der Art der Codierung. Der ASCII-Modus wird zur Übertragung von reinen Text-Dateien verwendet. Hier muss die Zeilenstruktur des Textes umcodiert werden. Bei diesem Vorgang wird der Zeichensatz dieser Datei an das Zielsystem angepasst. Der Binary-Modus überträgt die Dateien byteweise ohne die Daten zu ändern. Dieser Modus wird am häufigsten genutzt.

Vorzugsweise natürlich bei Binär-

Dateien.

Die Fehlerkontrolle bei der

Datenübertragung überlässt FTP

komplett dem TCP-Protokoll. Kommt es

doch zu einem Verbindungsabbruch,

sieht die FTP-Spezifikation die

Wiederaufnahme von unterbrochenen

Übertragungen vor. Die Header der

einzelnen Datenpakete enthalten Restart-

Markierungen. Versucht der FTP-Client

die Übertragung wieder aufzunehmen,

gleichen Client und Server die

Markierungen ab. Anschließend wird

die Übertragung wieder aufgenommen.

Eine Besonderheit von FTP ist der frei

Zugriff für alle Besucher: das

Anonymous-FTP. Da das FTP-Protokoll

Anmelde-orientiert arbeitet, kann der

Besucher als Benutzername

"anonymous" angeben und ein Passwort frei wählen. Zum guten Ton gehört die

Verwendung einer gültigen E-Mail-Adresse.
Nach erfolgreicher Anmeldung kann der Besucher sich in der Verzeichnisstruktur frei bewegen. Im Regelfall ist das Löschen von Dateien nicht möglich. Der Upload von Dateien ist nur über ein spezielles, für den Besucher ständig leeres Verzeichnis möglich. Der Download ist innerhalb der restlichen Verzeichnisse jederzeit möglich.

FTP-Befehle

FTP-Befehle gibt es für das Senden, Empfangen, Löschen und umbenennen von Dateien, das Einrichten, Löschen und Wechseln von Verzeichnissen.
Die Kommunikation zwischen FTP-Client und FTP-Server findet als Austausch von textbasierten Kommandos statt. In der einfachsten Form ist der FTP-Client ein Terminal-Programm über das der Benutzer sich mit dem

Server verständigt. Inzwischen verwendet man Programme, die ähnlich wie ein Dateimanager mehr Komfort bieten. Z. B. die Unterscheidung zwischen Text-Dateien und Binär-Dateien. Dazu gibt es zwei verschiedene Übertragungsmodi, die vor der Übertragung eingeleitet werden müssen. Gute FTP-Clients erkennen anhand der Datei-Endung den Datei-Typ und kümmern sich automatisch um die Einleitung des richtigen Übertragungsmodus.

FTP-Status-Codes

Jeder, vom FTP-Client, gesendete Befehl führt zu einer Rückmeldung des FTP-Servers in Form eines Status-Codes und einer Meldung im Klartext. Der Status-Code ist eine 3-stellige Nummer, die für den FTP-Client Informationen über die Verfügbarkeit der angeforderten Daten enthält. 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.

Status-Codes	**Beschreibung**
100-199	Die Status-Codes aus diesem Bereich weisen auf eine erfolgreiche Ausführung des Kommandos hin. Der Server erwartet aber vom Client die Fortführung durch einen weiteren Befehl.
200-299	Die Status-Codes aus diesem Bereich weisen auf eine erfolgreiche Ausführung des Kommandos hin.

Die Status-Codes aus diesem Bereich weisen auf eine erfolgreiche Ausführung des

300-

Kommandos hin. Der Server

399

erwartet zur weiteren Ausführung weitere Angaben um die Bearbeitung abzuschließen.

Die Status-Codes aus diesem Bereich weisen auf die Nichtausführung des Kommandos hin. Es handelt

400-

sich aber um ein temporäres

499

Problem. Eventuell wird bei erneuter Ausführung des Kommandos, die Bearbeitung erfolgreich abgeschlossen.

Die Status-Codes aus diesem

Bereich weisen auf die

500-

Nichtausführung des

599

Kommandos hin. Die erneute Ausführung würde zur selben Fehlermeldung führen.

TFTP - Triviale File Transfer Protocol

TFTP ist ähnlich wie FTP ein Protokoll für den Datei-Transfer über das Internet. Im Gegensatz zu FTP hat TFTP deutlich weniger Kommandos und verwendet nur den UDP-Port 69. Wegen der Verwendung des ungesicherten Transport-Protokolls UDP übernimmt TFTP selber die Sicherung der Datenpakete und kümmert sich eigenständig um die wiederholte Sendung bei Paketverlusten. Eine Authentifizierung entfällt. Stattdessen

wird auf die Zugriffsbeschränkung des Betriebssystems gebaut. So dürfen nur Dateien gelesen und geschrieben werden, die für alle Benutzer lesbar oder schreibbar sind.

TFTP wird sehr häufig benutzt um neue BIOS- und Firmware-Versionen auf aktive Netzwerkkomponenten zu laden.

TFTP-Befehle

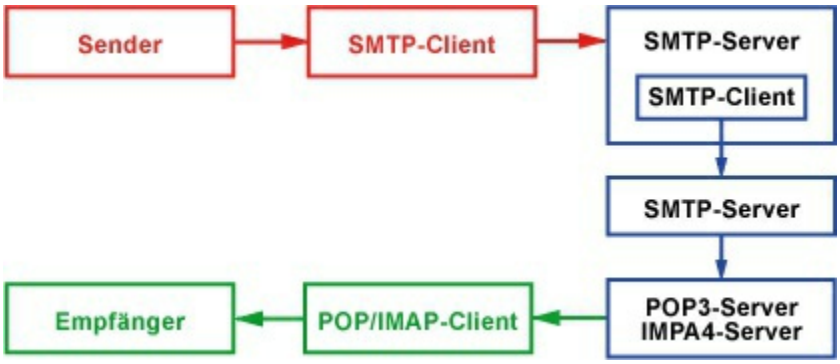
TFTP-Kommandos sind in ihrer Funktion identisch mit den FTP-Kommandos. Unterstützt werden nur die folgenden Kommandos: CONNECT, MOD, PUT, GET, QUIT, VERBOSE, TRACE, STATUS, BINARY, ASCII, RESMT TIMEOUT.

SMTP - Simple Mail Transfer Protocol

SMTP ist ein Kommunikationsprotokoll für die Übertragung von E-Mails. Die Kommunikation erfolgt zwischen einem

E-Mail-Client und einem SMTP-Server (Postausgangsserver) oder zwischen zwei SMTP-Server.

Neben SMTP gibt mit POP und IMAP noch zwei weitere Protokolle für den E-Mail-Austausch. Diese beiden Protokoll dienen jedoch nur dazu, um E-Mail



abzuholen oder online zu verwalten.

SMTP dagegen ist ein Kommunikationsprotokoll, das E-Mails entgegennehmen und weiterleiten kann.

Wie funktioniert SMTP?

Für den Austausch der E-Mails sind die Mail Transfer Agents (MTAs) zuständig. Untereinander verständigen sich die MTAs mit Kommandos. Dabei sendet der SMTP-Client dem SMTP-Server ein

Kommando, und dieser antwortet mit einem Status-Code und einer Klartext-Meldung.

Nachteile von SMTP

SMTP hat mehrere große Nachteile. Zum einen wird für versendete E-Mails keine Versandbestätigung zurückgeliefert. Geht eine E-Mail verloren, werden weder Sender noch Empfänger darüber informiert.

Kann eine E-Mail nicht zugestellt werden, sieht die SMTP-Spezifikation die Benachrichtigung des Senders vor. Es gibt zwar eine SMTP-Erweiterung für standardisierte Fehlermeldungen, allerdings unterstützen nicht alle SMTP-Server diese Erweiterung. Die meisten unzustellbaren E-Mails enthalten nur eine mehr oder weniger verständliche Fehlermeldung in englischer Sprache und den Header der gesendeten E-Mail.

Ein weiteres Problem von SMTP ist die

nicht vorhandene Authentifizierung des Benutzers beim Verbindungsaufbau zwischen SMTP-Client und SMTP-Server. Das führt dazu, dass eine beliebige Absenderadresse beim Versand einer E-Mail angegeben werden kann. In der Praxis sieht das dann so aus, dass über offene SMTP-Server massenhaft Werbe-E-Mails, der sogenannte Spam, versendet wird. Aufgrund der gefälschten Absender-Adressen kann der eigentliche Urheber nur mit viel Mühe ermittelt werden.

Aufbau einer E-Mail

Eine E-Mail besteht aus drei Teilen. Der Envelope beinhaltet Sender-Adresse und Empfänger-Adresse, die der MTA benötigt. Es folgt der Header mit Informationen über den E-Mail-Client und die Message-ID. Diese besteht aus einer Zahlen-/Buchstaben-Kombination, gefolgt von der Host-Adresse (Domain)

des Senders. Der Body enthält den Nachrichten-Text der E-Mail.

SMTP-Befehle

Die Kommunikation zwischen SMTP-Client und SMTP-Server basiert auf ASCII-Kommandos.

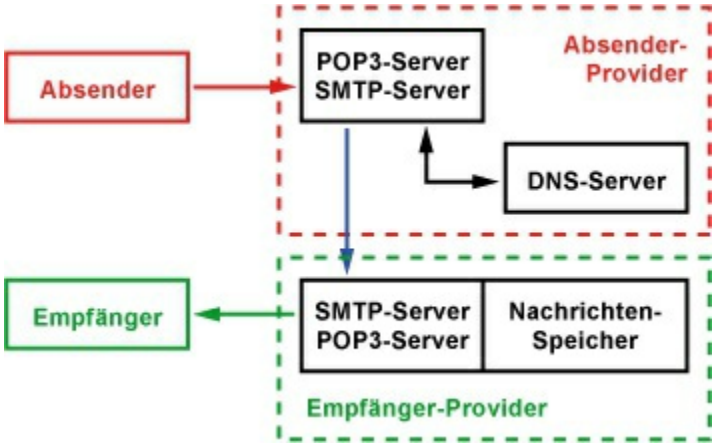
SMTP-Status-Code

Auf jedes Kommando vom SMTP-Client an den SMTP-Server schickt der Server einen 3-stelligen Status-Code mit Klartext-Meldung zurück.

E-Mail-Routing über SMTP und DNS

Nachdem der SMTP-Server eine E-Mail von einem E-Mail-Client entgegengenommen hat, ist er für das Weiterleiten an den Ziel-SMTP-Server verantwortlich. Das DNS spielt wie bei den Protokollen HTTP und FTP eine zentrale Rolle. Im DNS sind spezielle Einträge für die elektronische Post vorhanden. Das sind die Mail Exchange

Records (MX-Records). Über diese Einträge identifiziert der SMTP-Server den Ziel-SMTP-Server der Domain, die in der E-Mail-Adresse des Empfängers angegeben ist.



Der Ablauf des E-Mail-Routings sieht in etwa so aus: Der SMTP-Server fragt einen DNS-Server ab und erhält eine Aufstellung von Mail-Servern, die E-Mails für den Ziel-SMTP-Server entgegennehmen. Jeder dieser Mail-Server (Mail Exchanger) ist mit einer Priorität versehen. Der SMTP-Server versucht die Mail-Server in der vorgegebenen Reihenfolge zu kontaktieren, um die E-Mail zu

übermitteln. Theoretisch ist es möglich, das eine E-Mail über mehrere dieser Mail Exchanger läuft. Die MX-Records sollen das Entstehen dieser Mail-Schleifen verhindern. Trotzdem kann es zu Mail-Schleifen kommen, wenn die MX-Records unvollständig sind oder die Domain zu einem anderen Hoster oder Provider umgezogen ist.

ESMTP - Extended SMTP

ESMTP ist die Erweiterung von SMTP. Nutzt ein E-Mail-Client die Erweiterungen von ESMTP, meldet er sich beim SMTP-Server mit dem Kommando EHLO an. Antwortet der Server mit einer Fehlermeldung kennt er ESMTP nicht und der Client muss sich mit HELO anmelden. Beherrscht der SMTP-Server die ESMTP-Erweiterungen meldet er mehrere Antwortzeilen mit dem Status-Code 250. Der Status-Code und die Meldung sind

durch einen Bindestrich voneinander getrennt. In jeder Zeile steht eine spezifizierte Erweiterung, die der SMTP-Server unterstützt.

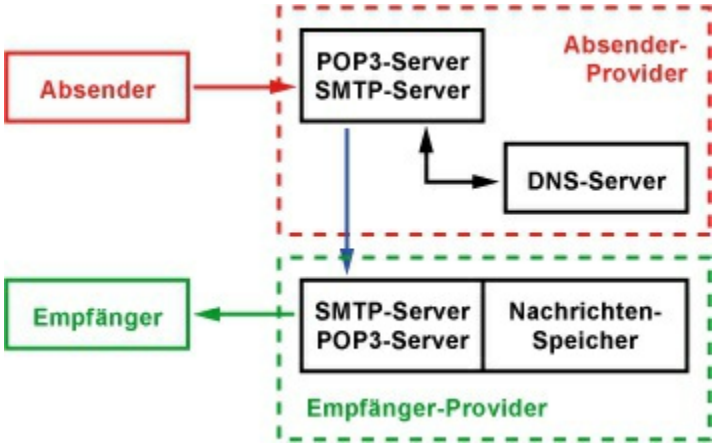
POP3 - Post Office Protocol Version 3

POP ist ein Kommunikationsprotokoll, um E-Mails von einem Posteingangsserver (POP-Server) abzuholen. Die Kommunikation erfolgt zwischen einem E-Mail-Client und einem E-Mail-Server (Posteingangsserver). Das Protokoll, das diesen Zugriff regelt, nennt sich POP (aus dem Jahr 1984), das in der aktuellen Version 3 vorliegt.

Bedeutung des Posteingangsservers

Der Empfang einer E-Mail setzt den Betrieb eines SMTP-Servers voraus. Dazu muss die Hardware aber auch rund um die Uhr laufen und funktionieren. Das

ist bei nahezu allen Anwendern des Internets nicht der Fall. Viele wählen sich über Wählverbindungen (analoges Modem oder ISDN-Karte) ins Internet ein. Oder sie hängen mit ihrem Computer in einem Netzwerk und haben über einen Benutzer-Account Zugriff auf das Internet. Auch in diesem Fall ist der Computer nur dann an, wenn der Benutzer gerade arbeitet. Im Normalfall würde also selten ein SMTP-Server eines Anwenders erreichbar sein. Um



diese Problematik zu umgehen werden E-Mails im letzten SMTP-Server zwischengespeichert.

Wie funktioniert POP?

Per Fernzugriff werden die gespeicherten E-Mails abgerufen und auf dem lokalen Computer gespeichert. POP sieht das Prinzip der Offline-Verarbeitung von E-Mails vor. Online werden die E-Mails vom Posteingangsserver vom E-Mail-Client heruntergeladen. Wenn sich darunter E-Mails mit einem großen Dateianhang befinden, kann der Download schon mal etwas länger dauern. Erst nach erfolgreichem und vollständigem Zugriff werden die E-Mails auf dem Server gelöscht. Die Bearbeitung der eingegangenen E-Mails erfolgt anschließend auf dem lokalen Computer des Benutzers ohne Verbindung (offline) POP-Server.
Die Verbindung zwischen POP-Server und E-Mail-Client erfolgt über TCP auf Port 110.

POP3-Befehle

Ist eine Verbindung zwischen POP3-Server und E-Mail-Client zustande gekommen, werden zur weiteren Kommunikation Kommandos ausgetauscht. Die POP3-Kommandos bestehen aus 3 bis 4 Zeichen und einen oder mehreren Parametern. Die Antwort des Servers auf ein Kommando enthält einen Status und optionale Informationen. Der Status ist entweder positiv (+OK) oder negativ (-ERR).

POP3-Sitzungen

Eine POP3-Verbindung umfasst mehrere Sitzungsstufen. Nach dem der POP3-Server die Verbindung mit einer positiven Meldung bestätigt hat, beginnt der "Authorization State", die Sitzung zur Benutzeranmeldung. Hier muss sich der E-Mail-Client gegenüber dem Server mit Benutzername und Passwort identifizieren. Nach erfolgreicher Identifizierung erfolgt der "Transaction State", die Sitzung zur Anforderung und Übermittlung der E-Mails. Hier werden

alle Befehle zur Bearbeitung von E-

Mails ausgeführt. Sendet der E-Mail-

Client den Befehl QUIT, beginnt der

"Update State", in dem alle vom E-Mail-Client angegebenen Änderungen

ausgeführt werden. Die Verbindung über

TCP ist zu diesem Zeitpunkt schon

beendet. Der letzte Vorgang, der

"Update State" stellt sicher, dass E-Mails nur dann auf dem Server gelöscht

werden, wenn die Verbindung vom E-

Mail-Client ordnungsgemäß beendet

wurde. Ist die TCP-Verbindung während

einer E-Mail-Übertragung

zusammengebrochen oder ist es zu einem

Timeout gekommen, dann sind noch nicht

alle geladenen E-Mails verloren. Sie

können nach einem nochmaligen

Verbindungsaufbau heruntergeladen

werden.

IMAP 4 - Internet

Mail Access

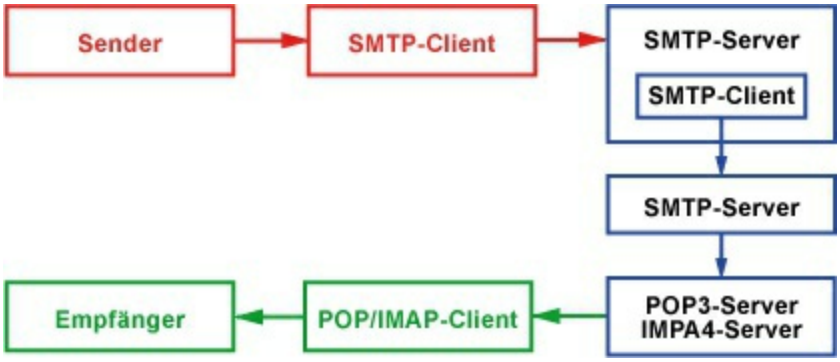
Protocol Version 4

IMAP ist ein Kommunikationsprotokoll, um E-Mails auf einem entfernten Server ähnlich wie Dateien zu verwalten. Dabei bleiben alle E-Mails auf dem IMAP-Server. Erst wenn eine E-Mail gelesen werden soll, wird sie heruntergeladen.

Unterschied IMAP zu POP

IMAP erlaubt den Zugriff auf eine Mailbox, ähnlich wie mit POP. Der entscheidende Unterschied zwischen beiden Protokollen ist der Online-Modus von IMAP, über den der E-Mail-Client ständig in Verbindung mit dem E-Mail-Server steht. Während einer IMAP-Sitzung kann auf einzelne E-Mails zugegriffen werden, die so lange auf dem Server bleiben, bis sie gelöscht werden. Dadurch kann von überall auf dem Server zugegriffen werden. Auch mit einem Endgerät, das nur mit geringer Bandbreite am Netzwerk angeschlossen ist. Die E-Mails werden nur dann

heruntergeladen, wenn der Anwender diese Lesen will. E-Mails mit einem großen Dateianhang verstopfen dann nicht mehr ungewollt den Zugang zum



Netzwerk.

Wie funktioniert IMAP?

Die Verbindung zwischen E-Mail-Client und Server findet über TCP auf Port 143 statt. Die Kommunikation basiert auf Textmeldungen im ASCII-Format. Im Gegensatz zu SMTP und POP wartet der E-Mail-Client bei IMAP keine Antwort auf gesendete Kommandos ab. Er kann mehrere Befehle hintereinander senden. Um eine eventuell spätere Rückmeldung vom Server identifizieren zu können, schickt der Client eine Kennung mit, die

der Server bei seiner Antwort zurück liefert. Mit einem Plus-Zeichen am Anfang der Antwort-Zeile signalisiert der Server, dass er weitere Informationen zum gesendeten Kommando erwartet. Mit einem Sternchen am Anfang der Zeile sendet der Server mehrere Informationen zum Client zurück. In der Antwort ist der Erfolg oder Misserfolg eines Kommandos gekennzeichnet. "OK" deutet auf die erfolgreiche Ausführung des Kommandos hin. Bei "NO" ist ein Fehler aufgetreten und "BAD" informiert über ein unbekanntes Kommando oder einen Syntax-Fehler.

IMAP-Sitzungen

Während einer IMAP-Verbindung werden mehrere Sitzungsstufen durchlaufen. Direkt nach dem Verbindungsaufbau über TCP wird während dem "Non-Authenticated State" der Benutzer vom Server identifiziert.

Hat sich der Benutzer erfolgreich

identifiziert, kann er sich im

nachfolgenden "Authenticated State"

eine Mailbox wählen. Im

darauffolgenden "Selected State" kann der Benutzer die E-Mails in seiner

Mailbox lesen und bearbeiten. Beendet

der E-Mail-Client die Verbindung zum

Server, wechselt er in den "Logout

State" oder "Update State", in dem er noch anstehende Änderungen ausführt.

MIME-Types -

Multipurpose

Internet Mail

Extensions

MIME ist die Abkürzung für

Multipurpose Internet Mail Extensions.

Es handelt sich um eine Kodierung, die

den Anwendungsprogrammen im Internet

einen Hinweis auf den verwendeten

Datentyp geben soll. Ursprünglich

wurde dieses Schema für Datei-Anhänge

(Attachments) in E-Mails eingeführt.

Innerhalb dieser Multipart-Mails trennt MIME die Datei vom Rest der E-Mail und gibt den empfangenden E-Mail-Clients einen Hinweis auf den Datentyp. Diese Information ist wichtig, damit der Empfänger weiß, mit welchem Programm er die Datei öffnen kann.
Was sich für E-Mails als nützlich erwiesen hat, wurde dann für andere Protokolle eingeführt, die zwischen zwei Stationen Daten übertragen. So haben verschiedene HTML-Elemente Attribute, die den MIME-Type als Angabe enthalten. Auch im HTTP-Header hat der MIME-Type seinen Platz gefunden. Sowohl der Browser, als auch der Web-Server führen eine Liste mit ihren bekannten MIME-Types. Bei jeder Kommunikation zwischen Browser und Web-Server wird der MIME-Type ausgehandelt. In der Regel akzeptiert ein Browser jeden MIME-Type. Kennt er

ihn nicht, bietet er dem Anwender den Download dieser Datei an. Der Anwender kann sich dann später entscheiden, welches Programm für die Datei geeignet ist.

Medientypen und Subtypen

Der MIME-Type besteht aus der Angabe eines Medientyps und eines Subtyps, die durch einen Schrägstrich voneinander getrennt sind. Z. B. text/html oder image/jpeg.

Der Medientyp weist daraufhin, um welche Art es sich handelt. Typische Beispiele sind Text, Bilder, Video und Audio.

Medientypen	**Beschreibung**
text	Dateien mit ASCII-Text
image	Bilder, Grafiken, Fotos
video	Video-Dateien

audio

Audio-Dateien

Dateien, die an ein

bestimmtes

application

Anwendungsprogramm

gebunden sind

mulitpart

mehrteilige Daten

message

Nachrichten

Dateien mit

model

mehrdimensionalen

Strukturen

Beispiel-Medientyp für

example

Dokumentationen

Aus dem Medientyp ergibt sich die Art

der Datenstruktur, also ob die Datei

Binär oder nach ASCII abgelegt sind.

Der Subtyp bezieht sich auf ein oder

mehrere Dateiformate, die an ein bestimmtes Programm gebunden sind oder mit speziellen Programmen oder Plugins ausgeführt werden müssen.

Subtypen, die mit einem "x-" anfangen, sind Dateien, die auf einem Server ausgeführt werden. Da es sehr viele MIME-Types gibt, ist die folgende Tabelle nur eine kleine Auswahl der wichtigsten und am häufigsten vorkommenden MIME-Types.

MIME-Type	**Dateiendung**
application/gzip	*.gz
application/msexcel	*.xls *.xla
	*.ppt *.ppz
application/mspowerpoint	*.pps *.pot
application/msword	*.doc *.dot
	*.bin *.exe
application/octet-stream	

*.com *.dll

*.class

application/pdf

*.pdf

*.ai *.eps

application/postscript

*.ps

application/rtf

*.rtf

application/x-javascript

*.js

application/x-httpd-php

*.php *.phtml

application/zip

*.zip

audio/x-pn-realaudio

*.ram *.ra

audio/x-pn-realaudio-

*.rpm

plugin

audio/x-qt-stream

*.stream

audio/x-wav

*.wav

image/gif

*.gif

*.jpeg *.jpg

image/jpeg

*.jpe

image/tiff

*.tiff *.tif

multipart/alternative

multipart/byteranges

multipart/digest

multipart/encrypted

multipart/form-data

multipart/mixed

text/css

*.css

*.htm *.html

text/html

*.shtml

text/javascript

*.js

text/plain

*.txt

*.mpeg

video/mpeg

*.mpg *.mpe

video/quicktime

*.qt *.mov

video/x-msvideo

*.avi

Telnet

Telnet ist ein Protokoll um Zugriff auf einen anderen entfernten Computer oder Netzwerkkomponente zu erhalten. Der Zugriff erfolgt auf der Kommandozeile, über den Telnet-Client, der eine Verbindung zum Telnet-Server aufbaut. Telnet ist der älteste Dienst im Internet und stammt noch aus den Ursprüngen des ARPANET. Telnet ist ein Kunstwort und bildet sich aus den ersten drei Buchstaben von Telecommunication Network.

Wie funktioniert Telnet?

Die Öffnung einer Telnet-Sitzung erfolgt durch Eingabe des Computernamens oder der IP-Adresse. Die Daten werden über TCP Port 23 übertragen. In der Regel wird nach dem Verbindungsaufbau ein Passwort abgefragt.

Neben dem Zugriff auf einen entfernten Rechner per Terminal-Emulation ist es möglich auf TCP aufsitzende Protokolle wie POP3, SMTP, HTTP, FTP direkt anzusprechen. Auf diese Weise lassen sich Verbindungen zu entfernten Servern mittels der Befehle dieser Protokolle aufbauen. Dazu muss man nur den Port des entsprechenden Dienstes kontaktieren und mittels der Klartext-ASCII-Befehle die Kommunikation

steuern. Es ist zwar äußerst umständlich E-Mails per Telnet abzuholen oder Dateien auf eine Server zu laden, aber es ist theoretische möglich und damit zum Testen der Dienste geeignet.

Arbeitsweise des Telnet-Protokolls

Die Bedienung und Fähigkeiten der unterschiedlichen Betriebssysteme erfordern ein Protokoll, das entweder auf die Grundfunktionen reduziert ist oder in seiner Anpassungsfähigkeit sehr flexibel ist. Telnet ist beides.

Die Telnet-Sitzung wird durch das Network Virtual Terminal (NVT) beschrieben. Hier sind die Fähigkeiten der Datenquelle und des Datenempfängers beschrieben. Das NVT besteht aus einer virtuellen Tastatur und einem virtuellen Drucker, die nur bestimmte Zeichen erzeugen bzw. anzeigen können. Jede Telnet-Sitzung hat

an ihren Endpunkten eine NVT-Tastatur und einen NVT-Drucker. Vor Beginn einer Telnet-Sitzung verhandeln Client und Server auf Basis des NVT alle weiteren Protokoll-Elemente, die ein- und ausgeschaltet werden können. Von dieser Verhandlung bekommt der Anwender in der Regel nichts mit.

Telnet in der Praxis

Telnet ist ein unsicheres Protokoll. Die Übertragung erfolgt in Klartext und ist damit abhörbar bzw. protokollierbar. Für Telnet-Sitzungen innerhalb eines lokalen Netzwerkes dürfte das kein Problem sein. Für Verbindungen ins Internet empfiehlt sich das gesicherte SSH (Secure Shell).

Verzeichnisdienste

(X.500)

Ein Verzeichnis ist eine Sammlung von Informationen und Objekten, die in einer bestimmten Reihenfolge gespeichert sind

und auf die zugegriffen werden kann. Die Benutzeroberfläche (Interface) mit der auf die Informationen und Objekte zugegriffen werden (Suchen, Ändern, Hinzufügen, Löschen) nennt man Verzeichnisdienst.

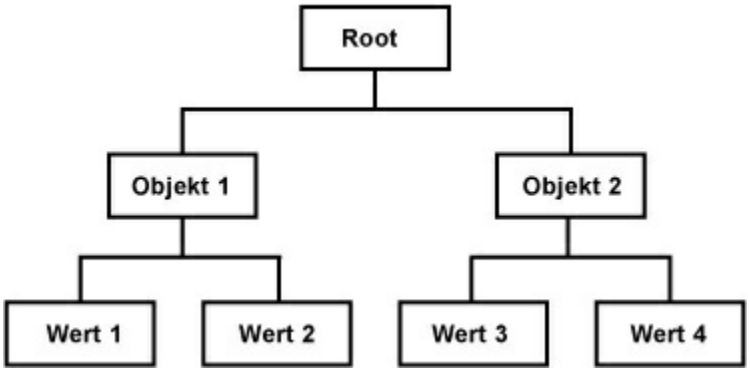
Ein Verzeichnis nach ISO 9594-1 ist baumartig strukturiert. Dort sind die Daten statisch abgelegt. Jeder Eintrag kann beliebig viele Werte oder Attribute haben. Und jede Ebene kann beliebig viele Einträge haben.

Das Verzeichnis ist eine spezielle Datenbank, in der die Benutzer, Anwendungen und Ressourcen und deren Eigenschaften und Standort gespeichert sind. Ein Benutzerverzeichnis enthält z. B. die Adresse, die Telefonnummer und E-Mail-Adresse. Ein Druckerverzeichnis enthält z. B. Informationen über Standort, Druckerart, druckbare Seiten pro Minute und

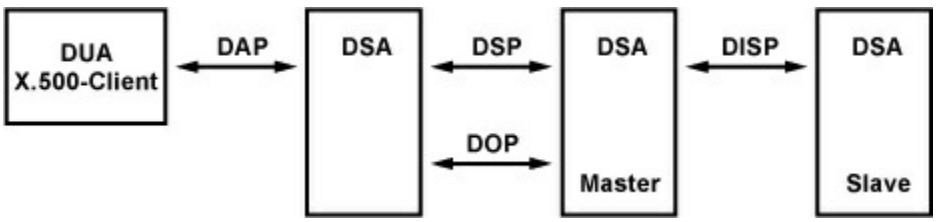
Zugriffsrechte.

X.500

Im Rahmen der X-Serie der ITU



(International Telecommunication Union) wurde 1988 eine Empfehlung für Verzeichnisdienste veröffentlicht. Die Empfehlung von X.500 wurde als Standard von der ISO (International Standards Organization) aufgenommen. 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 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.

Der Zugriff auf das Verzeichnis erfolgt mit dem Directory User Agent (DUA). Dafür stehen einige Operationen zu Verfügung. Z. B. Lesen, Vergleichen, Suchen Hinzufügen, Löschen und Ändern. Um den Zugriff für Personen und Objekte einzuschränken steht für die Authentifizierung je eine Variante mit Passwort und Public-Key-Zertifikat zu

Verfügung.

Die dezentrale Datenhaltung kann auf mehreren Servern realisiert werden. Diese kommunizieren miteinander, um Anfragen für einen anderen Datenbestand weiterzuleiten. Die einzelnen Server werden als Directory System Agents (DSA) bezeichnet. Um die Lesezugriffe auf das Verzeichnis zu beschleunigen, wird das Verzeichnis auf mehreren Servern gespiegelt. 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 Datenbestandes gespeichert. Diesen Vorgang (Spiegelung) nennt man Replikation. Dadurch erhöht sich auch die Ausfallsicherheit des Verzeichnisses.

X.500-Protokolle

Protokoll	Abkürzung	Beschreibung
Access Directory Protocol	DAP	Definiert die Kommunikation zwischen Directory User Agent (DUA) und Directory System Agent (DSA).
System Directory Protocol	DSA	Definiert die Kommunikation zwischen den Directory

System Agents

(DSA).

Definiert die

Directory

Replikation

Information DISP

zwischen

Shadowing

Master- und

Protocol

Slave-Server.

Definiert die

Directory

administrative

Operational

Kommunikation

Binding

DOP

zwischen zwei

Management

Directory

Protocol

System Agents

(DSA).

Übersicht: X.500-konforme

Verzeichnisdienste

Nahezu alle verfügbaren

Verzeichnisdienste basieren auf X.500.

Microsoft Active Directory

Novell eDirectory

LDAP - Lightweight Directory

Access Protocol

Siemens DirX

Storage

Storage ist die Bezeichnung für eine

große Menge zusammenhängenden

Speicherplatz in einem Netzwerk.

Storage heißen auch die große Miet-

Garagen-Parks in den USA. Ein Storage

im Netzwerk arbeitet mit dem selben

Prinzip. Im Storage bekommt jeder

Netzwerkbenutzer einen bestimmten

Speicherplatz reserviert, auf dem er

eigene Dateien speichern kann.

Storage-Kategorien

DAS - Direct Attached Storage

NAS - Network Attached Storage

SAN - Storage Area Network

DAS - Direct Attached

Storage

Mit DAS bezeichnet man eine Festplatte, die mit einem Server direkt verbunden ist. Dabei spielt es keine Rolle, ob die Festplatte innerhalb des Gehäuses mit SATA oder SAS angeschlossen ist oder extern über USB, FireWire oder eSATA. In jedem Fall kontrolliert der Server den Zugriff auf den Speicherplatz. Andere Server und Workstations erhalten über Benutzerrichtlinien oder auf Freigabeebene Zugriff auf den Speicher. Bei diesem Speichersystem besteht immer die Gefahr einer Downtime (Ausfallzeit). Fällt der Server aus, dann steht der Speicherplatz mit den gesamten

Daten nicht mehr zur Verfügung. Ist eine Festplatte defekt, sind die Daten verloren und müssen mit einem Backup wieder hergestellt werden. Das erste Problem kann durch einen zweiten Server gelöst werden, der seine Daten mit dem ersten Server abgleicht und so die Performance und Ausfallsicherheit verbessert. Das zweite Problem wird durch ein RAID gelöst. Hier werden die Daten auf zwei Festplatten gespiegelt. Fällt eine Festplatte aus, kann sie entfernt und durch eine neue ersetzt werden. Danach werden die Daten auf die neue Festplatte automatisch gespiegelt.

NAS - Network Attached Storage

Bei NAS sind die Festplatten vom Server losgelöst. Sie sind als eigenständige Einheit zu sehen. Im Prinzip besteht eine NAS-

Speicherlösung aus einer oder mehr Festplatten, einem Netzteil für die Stromversorgung und dem Netzwerkinterface. Alles zusammen in einem Gehäuse steht an einer zentralen Stelle in der Netzwerkinfrastruktur und stellt auf Basis von TCP/IP Speicherplatz zur Verfügung. Der Zugriff wird nicht zentral, sondern im NAS geregelt. Entweder steht der Speicherplatz allen Netzwerkteilnehmern zur Verfügung oder wird benutzerabhängig aufgeteilt. Da NAS direkt über TCP/IP im Netzwerk zur Verfügung steht, lassen sich sehr leicht HTTP- und FTP-Server-Dienste implementieren.

SAN - Storage Area Network

Ein SAN ist ein Netzwerk in dem große Datenmengen gespeichert und bewegt werden und wo eine zeitnahe Datensicherung erforderlich ist.

Speichernetze entkoppeln Server und Speicher räumlich voneinander. Der Server wird zur reinen Verwaltung des Speichers und der Daten eingesetzt. So kann man den Speicher bedarfsgerecht verteilen und besser skalieren. Der Speicher muss dann auch nicht am gleichen Ort stehen, an dem sich der Server befindet.

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 liegt 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. Für VoIP-Kunden sieht das anders aus. Sie müssen Einschränkungen in Kauf nehmen. Zuverlässigkeit, Komfort und Sprachqualität lassen zu wünschen übrig. Während die Festnetz-Telefonie aus möglichst wenigen Komponenten besteht, sind bei VoIP über das Internet

sehr viele Komponenten im Spiel.

VoIP-

Call-Manager,

Anwendungen

Softphone, ...

SIP, H.323, RTP,

VoIP-Protokolle UDP, ...

VoIP

DNS, NAT, QoS,

unterstützende AAA, ...

Dienste

Linux, Unix,

Betriebssysteme Windows, ...

Breitbandmodem,

Hardware

Router, Server, IP-

Telefon, Smartphone,

...

LAN, WAN, DSL,

Netze

TV-Kabel, ...

Viele Faktoren spielen beim

Verbindungsaufbau und auch danach eine große Rolle. Zwar sind Störungen meist nur von kurzer Dauer. Doch wer auf einen Anruf wartet oder dringend telefonieren muss, der möchte sich darauf verlassen können, dass der Telefonanschluss problemlos funktioniert.

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 Inhaber. 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.

Voice over IP: Protokolle und Standards

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, stellen sich einem einige Hürden in den Weg.

Call Control Audio Video

G.711 H.261

G.723

SIP

H.263

G.729

H.323

RTP

RTCP

TCP

UDP

IP

LAN

Voice over IP im OSI-Schichtenmodell

Schicht

Protokoll

VoIP-Anwendung

7. Anwendung

Softphone / Call-

Manager

Sprachcodecs

6. Präsentation

G.729 / G.723 /

G.711

Signalisierung

5. Session

H.323 / SIP

Transport-

Protokolle

4. Transport

RTP / UDP / RSVP

Netzwerk-Protokoll

3. Netzwerk

IP

2. Verbindung

ATM / Ethernet

Physikalische

1.

DSL / Ethernet

Ebene

Transport-Protokolle

Bei Voice over IP muss man zwischen den Datenpaketen zum Verbindungsauf- und abbau (Signalisierung) 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 um so 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, 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.

Laufzeit mit Ping messen

Um Verzögerungen auf einer Übertragungsstrecke zu messen, bietet sich der Ping als grobe Abschätzung an. Dabei muss man beachten, dass der Ping

die Gesamtverzögerung von Hinweg und Rückweg (Round-Trip-Time, RTT) misst. Sprachdaten dagegen werden nur in eine Richtung übertragen und enden beim Empfänger. Der Empfang der Pakete wird auf Transportebene nicht bestätigt. Deshalb muss der Wert, den Ping liefert, halbiert werden. Dabei muss man berücksichtigen, dass die Zeiten von Hinweg und Rückweg unterschiedlich sein können. Doch Ping weist diese Zeiten nicht getrennt voneinander aus. Deshalb kann man Ping auch nur als grobe Abschätzung nehmen. Eine Messung mit aussagekräftigen und korrekten Werten muss in der Praxis anders erfolgen.

Um die Messung mit Ping trotzdem einigermaßen realistisch zu gestalten muss die Paketgröße von Ping eingestellt werden. Geht man von der Kodierung mit G.711 und 20 ms Sprachdaten pro

Paket aus, dann entspricht das 160 Byte (64 kBit/s x 0,02 s). Hinzurechnen muss man noch 40 Byte für den IP/UDP/RTP-Header-Anteil. Der Ping sollte also 200 Byte pro Paket verschicken.
Unter Windows würde das Ping-Kommando demnach **ping -l 200 -t {Hostname}** lauten. Durch das Attribut -t wird der Ping so lange wiederholt, bis die Tastenkombination Strg + C gedrückt wird. Unter Linux würde das Ping-Kommando **ping -s 200 {Hostname}}** lauten.

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 Ausfällen 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 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.
In H.323 ist H.235 definiert. Es umfasst Verfahren zur Authentifizierung und Verschlüsselung der Datenströme. Die Verschlüsselung ist optional. Die Verschlüsselung erfolgt mit SRTP.
SIP sieht die Verschlüsselung der Authentifizierung mit PGP vor. Bei SIP wird der Datenstrom auch mit SRTP verschlüsselt.
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.
SIPS - SIP über TLS/SSL für den Verbindungsaufbau
SRTP - Secure RTP für die

Übertragung der Sprachdaten

H.323 (Voice over

IP)

H.323 ist eine Rahmenspezifikation für paketbasierte Multimedia-Dienste in lokalen Netzwerken (LAN). Es hat seinen Ursprung in der Videokommunikation über TCP/IP. Dazu wurde die Protokollfamilie rund um H.323 für Enterprise und LAN-Lösungen entwickelt. H.323 wurde für Netze entwickelt, die kein Quality of Service (QoS) zu bieten haben.

1996 führte die ITU den H.323-Standard ein. Es ist das älteste Protokoll für Voice over IP. Die ersten VoIP-TK-Anlagen basierten auf diesem Standard.

1998 folgte die Version 2 von H.323, für die auch Hardware entwickelt wurde.

Schon 1999 folgte die 3. und 2000 die 4. Version.

H.323-Systemarchitektur

In H.323 sind Gateway- und Gatekeeper-Funktionen definiert. Über das Gateway wird der Übergang in andere Sprachnetze ermöglicht. Und der Gatekeeper regelt das Bandbreitenmanagement und die Umsetzung von der symbolischen Adresse in die IP-Adresse.

H.323-Protokolle

H.323 stammt aus der Welt der Telekommunikation. Es besteht aus vielen Teilprotokollen, die verschiedene Aufgaben bei der Signalisierung und Datenübertragung haben und die in jeweils eigenen Standards definiert sind. Innerhalb von H.323 sind die Protokolle H.225.0 (Setup), Q.931 (Signalisierung), H.245.0 (Telefonie) und weitere Dienste und Leistungmerkmale definiert. Mit H.450 werden fast alle Leistungsmerkmale traditioneller TK-Systeme unterstützt.

Audio Video Steuerung & User-

Data

Codec Codec

Interface

G.711

T.125

Call

H.450

G.722 H.261

T.124

RAS Control

G.723 H.263 Control H.225.0

G.728

H.245

H.225.0 (Q.931)

G.729

T.123

RTP

RTCP

UDP

TCP

IP - Internet Protocol (Network Layer)

Ethernet (Link Layer)

Physical Layer

H.323 definierte die paketvermittelte Kommunikation, die Nutzung von Kodierungs- und Signalisierungsverfahren und basiert auf den Übertragungsprotokollen RTP und RTCP. Trotzdem ist H.323 unabhängig vom Transport-Protokoll (RTP, TCP, UDP, etc.). Der für die Signalisierung erforderliche Datenaustausch erfolgt über die Transport-Protokolle TCP oder UDP. Der Datenstrom für die Sprache wird über RTP übertragen.

H.225.0 und H.245.0

H.225.0 (Setup) und H.245.0 (Telefonie) sind unter H.323 für die Signalisierung zuständig. H.225 definiert Registrierungs-, Authentifizierungs- und Status-Prozeduren (RAS) für die Gatekeeper-Signalisierung und die Steuerung des Verbindungsaufbaus. Das

RAS-Protokoll (Registration Admission Status) ist ein Verfahren zur Anmeldung von Endgeräten, Verbindungsanforderungen und Bandbreitenzuteilung. Die Anrufinformationen sind in einem Binärcode geschrieben.
In paketvermittelten Netzen ist es üblich dem Datenpaket die Zieladresse mitzugeben. Beim Verbindungsaufbau von VoIP-Gesprächen besteht jedoch das Problem, dass IP-Telefone des Ende der eingetippten Rufnummer nicht erkennen können. Gelöst wird das von "Overlap Sending", bei der die Rufnummer schon während des Eintippens gesendet wird. So kann der Gatekeeper das Ende schneller erkennen und zügig die Verbindung herstellen.
Wenn die Verbindung aufgebaut ist, übernimmt H.245 mit einem Handshaking-Verfahren die Arbeit.

H.245 definiert den logischen Kanal und weitere Verbindungssteuerungsfunktionen (Anrufkontrolle). Dabei werden Audio- und Videocodecs für Sprach- und Videokompression auf Verfügbarkeit geprüft. Es gibt verschiedene Sprach-Codecs. Aber nur der G.711-Codec ist in H.323 als Muss definiert. Alle anderen Codecs können von den Herstellern zusätzlich in ihre Produkte implementiert werden. Haben sich zwei Endgeräte auf einen Codec geeinigt, dann erfolgt die Sprachübertragung über das Realtime Transport Protocol (RTP).

H.450 - Supplementary Services (Leistungsmerkmale)

H.450 ist eine Serie von Standards zur Definition und Funktionen der Signalisierungsprotokolle, die bei H.323 genutzt werden. Diese Funktionen gehen

über die Grundfunktionen von H.323 hinaus und haben mit dem Verbindungsaufbau nichts zu tun.

H.450 umfasst Leistungsmerkmale, die von klassischen Telefonanlagen und vom ISDN bekannt sind. Um diese Leistungsmerkmale auch im VoIP zu integrieren gibt es den H.450-Standard (Supplementary Services), der allerdings nur 8 Leistungsmerkmale umfasst:

Call Transfer (Weiterverbinden)

Call Division (Rufweiterleitung)

Call Hold (Halten von Anrufen)

Call Park (Anruf parken)

Call Waiting (Zweitanruf)

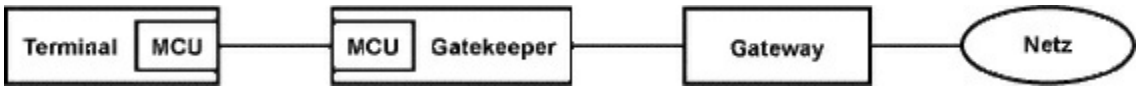
Message Waiting (Nachrichten übermitteln)

Name Identification (Namensübermittlung)

Call Competition (Rückruf)

Zusätzlich haben die Hersteller die

Möglichkeit ihre propritären Leistungsmerkmale über einen standardisierten Signalisierungsmechanismus zu implementieren. Allerdings verwenden die Hersteller zur Realisierung ihrer Leistungsmerkmale meist ein proprietäres Protokoll. Die Zusammenarbeit zwischen den Endgeräten und Gatekeepern unterschiedlicher Hersteller ist meistens nicht gegeben. Es reicht meist nur für die Grundfunktionen.



H.323-Systemarchitektur

In der H.323-Systemarchitektur sind 4 Elemente definiert:

Terminal (Endgeräte)

MCU - Multipoint Controller Unit

Gateway

Gatekeeper

In der H.323-Systemarchitektur spielt

der Gatekeeper die zentrale Rolle. Und

das Gateway übernimmt die Anbindung

an externe Netze.

Bei H.323 gibt es bestimmte "Zonen", in denen festgelegt ist, welche MCUs,

Endgeräte und Gateways von einem

Gatekeeper kontrolliert werden. Eine

solche Zone kann mehrere Router und

sogar mehrere miteinander verknüpfte

lokale Netzwerke (LAN) umfassen.

Gateway, Gatekeeper und MCU sind

voneinander unabhängig. Das bedeutet,

dass sie getrennt oder als eine Einheit

implementiert werden können. Ein

System aus Gateway, Gatekeeper und

MCU lässt sich auf einem Server

installieren. Diese Konstellation gilt als

deutlich preiswerter als klassische

Telefonanlagen. Das System übernimmt

dann in einem Netzwerk die Telefonie-

Funktion. Ist die Last auf dem System zu groß, dann lässt es sich auf mehreren Systemen verteilen.

Terminals / Endgeräte

Das Terminal ist eine Hardware oder Software, die den Endpunkt in der H.323-Systemarchitektur darstellt.
Als Terminal eignet sich jedes Gerät, auf dem der H.323-Stack läuft. Die Hauptaufgabe des Terminals ist der Informationsaustausch mit anderen Terminals. Dafür stehen Punkt-zu-Punkt- und Multipunkt-Verbindungen zur Verfügung.

MCU - Multipoint

Controller Unit

Ein MCU ist Bestandteil des Gatekeepers und der Terminals. Ein MCU besteht aus einem Multipoint Controller (MC) und optional aus einem Multipoint Processor (MP). Der MC ist für die Anrufsignalisierung und

Verwaltung der Ressourcen verantwortlich. Der MP wandelt Audio- und Video-Streams in Echtzeit um.

Gateway

Das Gateway unterstützen die Echtzeit-Kommunikation zwischen zwei Terminals mit unterschiedlichen Protokollen. Es übersetzt die Protokolle und wandelt unterschiedliche Medienformate um. Außerdem steuert es den Informationsaustausch zwischen den Netzen.

Beispielsweise verbindet das Gateway H.323-Terminals mit SIP-Terminals. Über das Gateway wird auch der Übergang in andere Sprachnetze ermöglicht. Dabei regelt der "Gatekeeper" das Bandbreitenmanagment und die Umsetzung von der symbolischen Adresse in die IP-Adresse. Das Gateway ist auch für den Auf- und

Abbau der Sprachkanäle zwischen dem H.323-LAN und dem Telefonnetz zuständig. Im Gateway werden die Sprach-Daten von verschiedenen Sprach-Codecs in G.711 (64 kBit/s) umgesetzt.
Auf der einen Seite ist das Gateway mit dem LAN verbunden. Auf der anderen Seite ist das Gateway über mehrere ISDN-B-Kanäle mit dem Telefonnetz verbunden. Das Gateway ist der Netzwerk-/Systemknoten, der für den Jitter-Puffer, die Laufzeitoptimierung, Echo-Unterdrückung und andere Verfahren zur Verbesserung von Quality-of-Service (QoS) zuständig ist. Das Gateway kann entfallen, wenn keine Verbindung zum klassischen Telefonnetz oder in andere Netze erforderlich ist.

Gatekeeper

Die zentrale Rolle spielt der Gatekeeper (Torwächter). Er ist die

Schnittstellenfunktion des H.323-Standards und dient der Emulation des PSTN-Verbindungsaufbaus zwischen den Endgeräten über das IP-Netz. Der Gatekeeper übernimmt die...

...Anrufsteuerung (Signalisierung) und die dafür notwendigen Übersetzung von IP-Adresse in PSTN-Rufnummer bzw. umgekehrt. Die Steuerungsfunktionen sind im H.225 festgelegt.

...Signalisierung auf den Teilnehmeranschlussleitungen zum Auf- und Abbau von Verbindungen (Q.931).

...Umwandlungen des synchronen Datenstroms, aus dem PSTN, in IP-Pakete.

Der Gatekeeper ist nicht zwingend vorgesehen. Prinzipiell können sich zwei H.323-Terminals direkt miteinander verbinden. Doch der Gatekeeper bietet

mehr Kontrolle über die Anrufe und eine bessere Lastverteilung innerhalb eines Netzes. Steht nicht genügend Bandbreite für eine Verbindung zur Verfügung, dann kann er eingehende Anrufe abweisen.
Steht ein Gatekeeper zur Verfügung, dann müssen Terminals, MCUs und Gateways seine Dienste benutzen.
Wir ein Gatekeeper eingesetzt, dann kümmert er sich um die Adressierung, Autorisierung und Authentifizierung der Terminals. Die Bandbreitenverwaltung gehört auch zu seinen Aufgaben.
Optional beherrscht er Routing, die Autorisierung und das Verwalten von Anrufen. Ist das Netzwerk über ein Gateway an das klassische Telefonnetz angeschlossen, dann übernimmt der Gatekeeper die Übersetzung der Telefonnummern in IP-Adressen.

H.323-Kommunikation

Die H.323-Kommunikation gliedert sich

in 5 Phasen:

1. Gesprächsaufbau

2. Austausch der Endgeräte-Merkmale

3. Gesprächsbeginn

4. Kommunikation

5. Gesprächsabbau

Gesprächsaufbau bei H.323

mit H.225 und RAS

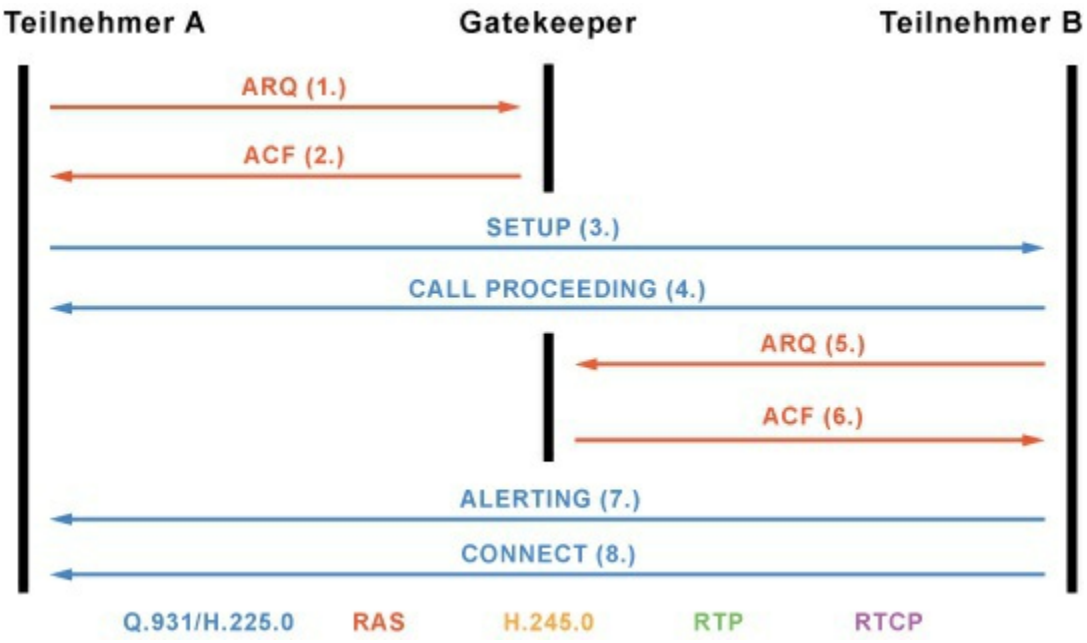
Den Rufaufbau bei H.323 übernimmt

H.225 und RAS. Dazu gehört die

Anmeldung der Teilnehmer und die

Übermittlung der Adresse an die

Gegenseite.



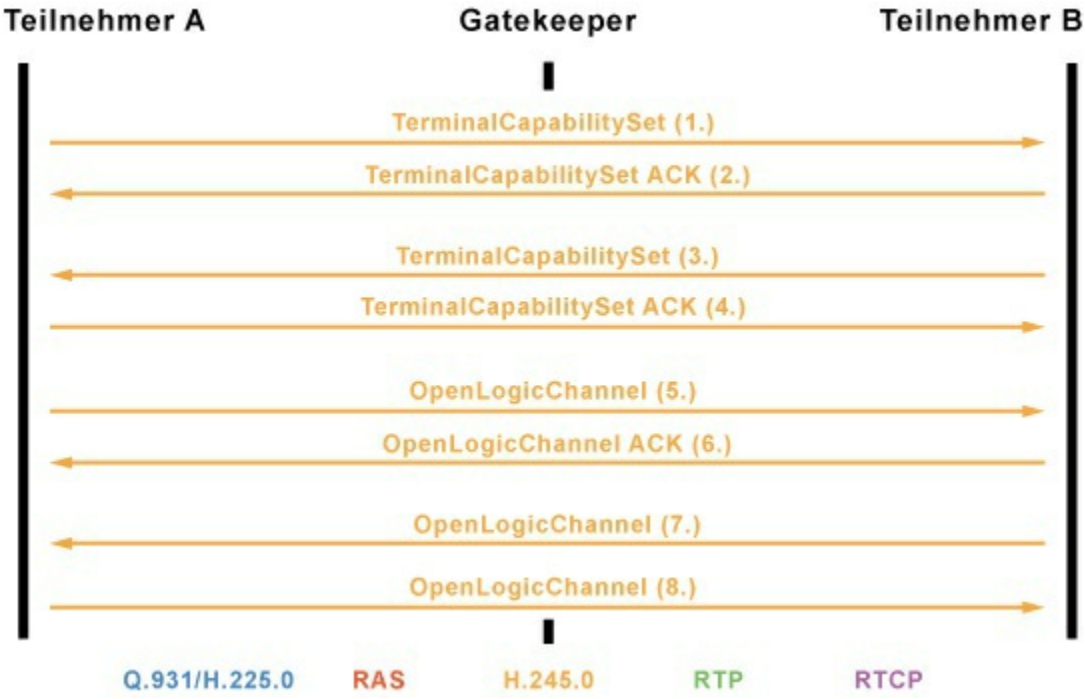
Zur Einleitung eines Anrufs schickt das Terminal von Teilnehmer A einen ARQ (Admission Request) an den Gatekeeper. Damit meldet sich das Terminal von Teilnehmer A an und übermittelt den Verbindungswunsch für Teilnehmer B. Der Gatekeeper schickt daraufhin ein ACF (Admission Confirmation) zur Bestätigung zurück. Dabei wird auch die Adresse von Teilnehmer B übermittelt. Das Terminal A schickt eine Signalisierungsnachricht (Setup) an das Terminal B mit der Adresse, die es vom Gatekeeper bekommen hat. Terminal B beantwortet den Verbindungswunsch mit einem "Call proceeding". Danach meldet sich Terminal B mit einem ARQ (Admission Request) ebenfalls beim Gatekeeper an und bekommt das mit einem ACF (Admission Confirmation) bestätigt. Daraufhin schickt Terminal B zwei Nachrichten an Terminal A. Zum einen "Alert", um die Verbindung

einzurichten und "Connect" um die

Verbindung herzustellen.

Austausch der Endgeräte-

Merkmale



Im Anschluss des Gesprächsaufbaus

informieren sich die beiden Teilnehmer

mit H.245-Nachrichten über ihre

Fähigkeiten. Sie einigen sich dabei auf

den kleinsten gemeinsamen Nenner. Die

Fähigkeiten werden mit

"TerminalCapabilitySet" zwischen den Terminals ausgetauscht und mit

"TerminalCapabilitySet ACK" bestätigt.

Danach wird mit H.245 ein Kanal zur

Übertragung für Audio und Video

eingerichtet. Dazu schicken sich die

beiden Teilnehmer ein

"OpenLogicChannel" mit der Adresse des RTCP-Kanals. In einem IP-Netz ist

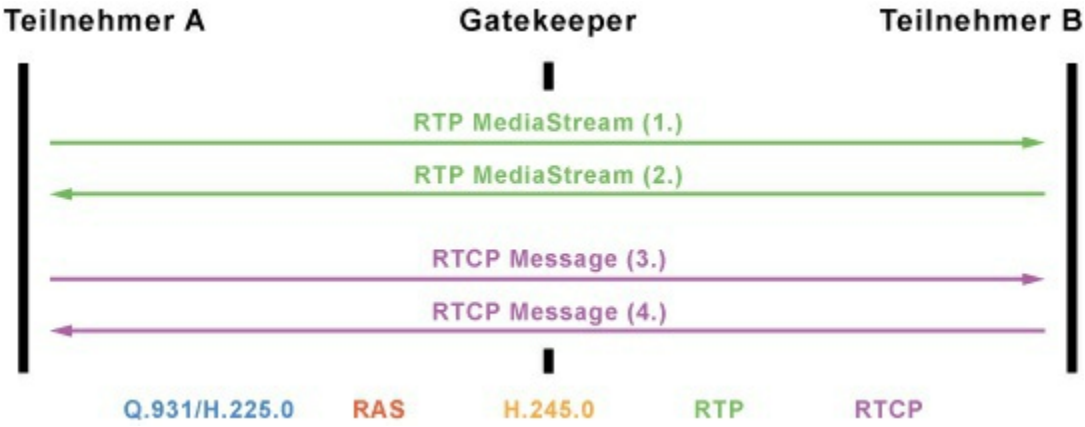
das die IP-Adresse. Die beiden

Teilnehmer bestätigen das jeweils mit

einem "OpenLogicChannel ACK", das

auch die RTP-Adresse enthält.

Gesprächsbeginn und



Kommunikation

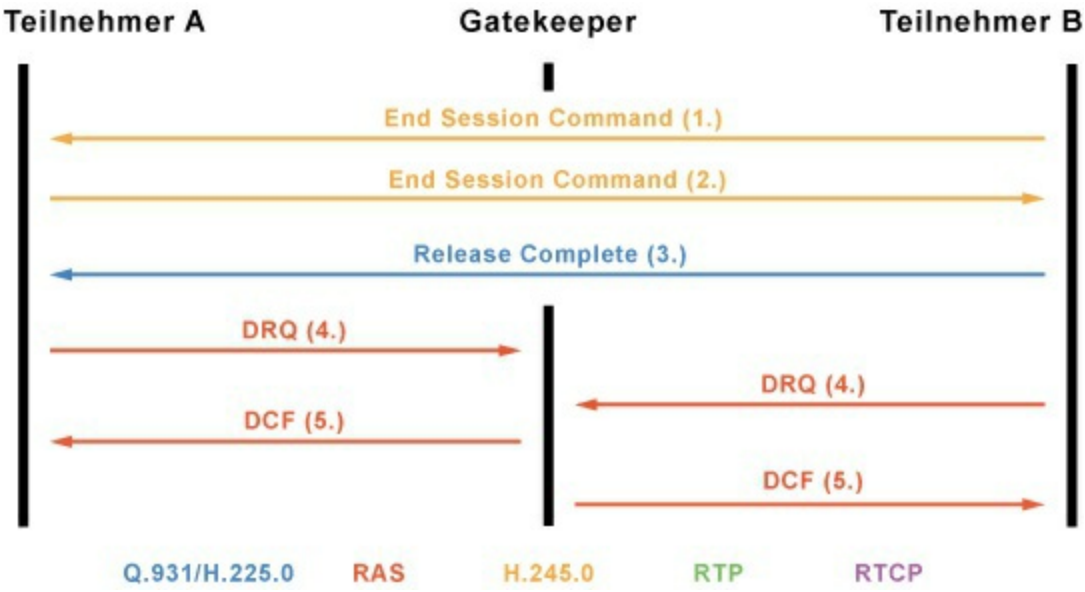
Jetzt beginnen die beiden Teilnehmer

damit die Sprach- und Video-Daten über

RTP miteinander auszutauschen. Die

Überwachung dieser Verbindung und

deren Qualität übernimmt RTCP.



Gesprächsabbau

Bei der Beendigung des Gesprächs tritt

wieder H.245 in Kraft. Beide

Teilnehmer schicken sich ein "End

Session Command". Das

Verbindungsende wird vom Terminal B

mit einem "Release Complete" bestätigt (H.225). Dann kommt der Gatekeeper

wieder ins Spiel. Beide Teilnehmer

müssen ihre Verbindung abmelden. Über

H.225-RAS schicken beide Teilnehmer

einen DRQ (Disengage Request) und

bekommen das mit einem DCF

(Disengage Confirmation) bestätigt.

Danach ist die Verbindung komplett

abgebaut.

SIP - Session

Initiation Protocol

Das SIP wurde entwickelt, um Teilnehmer zu Mehrpunktkonferenzen im Mbone zusammenzuschalten. Es wurde zur Verteilung von Multimedia-Content eingesetzt. Schnell erkannte man damals 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 und 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

Teilnehmer

G.711 / G.729 / G.723 / ...

SAP

SIP

SDP

TCP

UDP

IP

Data Link

Physical Link

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.

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.

SIP-Systemarchitektur

SIP basiert auf einer kombinierten Client-/Server-Architektur. Sie besteht aus vier Komponenten:

User Agent (UA)

Proxy Server

Redirect Server

Registrar Server

Der Registrar, Proxy und Redirect

Server können auf dem gleichen Server installiert sein.

User Agent

Die User Agents sind die Terminals bzw. Endgeräte. Das können Computer, Telefone oder Handys sein. Sofern die Adressen gegenseitig bekannt sind, könne sich zwei User Agents gegenseitig direkt anrufen.
Man unterscheidet zwischen User Agent Client (UAC) und User Agent Server (UAS). In einer SIP-Verbindung wird der Anrufer als User Agent Client (UAC) und der Angerufene als User Agent Server (UAS) bezeichnet.

Registrar Server

Der Registrar Server ist die zentrale Schaltstelle in der Systemarchitektur von SIP. Jeder SIP-Teilnehmer schickt in regelmäßigen Abständen eine REGISTER-Nachricht an den Registrar

Server. Die Nachricht enthält die SIP-Adresse und die IP-Adresse des User Agents. Diese Informationen dienen dem Proxy-Server später zum Auffinden des Teilnehmers. Beide Informationen werden in einer Datenbank, dem "Location Service" gespeichert.
Es ist sogar möglich, dass sich ein Anwender mit verschiedenen User Agents mit der gleichen SIP-Adresse registriert. Zum Beispiel an seinem Arbeitsplatz und bei sich zu Hause. Bei einem Anruf klingeln beide Telefone.

Proxy Server

Der Proxy Server arbeitet als Client oder als Server. Er kann in Vertretung anderer Clients Anfragen starten. Zum Beispiel um die IP-Adresse eines Teilnehmers zu erfahren.
Damit der Proxy Server die IP-Adresse des User Agent Server bekommen kann, muss der "Location Service" mit

möglichst vielen Datenbanken anderer

SIP-Provider zusammengeschaltet sein.

Redirect Server

Der Redirect Server entlastet den Proxy

Server. Er übergibt die Routing-

Informationen direkt an den User Agent

Client. Der kümmert sich dann selber um

den Verbindungsaufbau zum User Agent

Server.

Damit der Redirect Server die IP-

Adresse des UAS bekommen kann, muss

der "Location Service" mit möglichst vielen Datenbanken anderer SIP-Provider zusammengeschaltet sein.

SIP-

Kommunikation

SIP stellt mehrere Dialoge zur

Verfügung um eine Sitzung zwischen

zwei Teilnehmern (User Agent)

aufzubauen. Die Dialoge bestehen aus

einer Anforderung/Anfrage (Request)

und einer Rückmeldungen/Antwort

(Response).

Requests werden vom User Agent Client erzeugt und an den User Agent Server gesendet. Responses werden vom User Agent Server erzeugt und an dem User Agent Client gesendet.

Prinzip des Verbindungsaufbaus

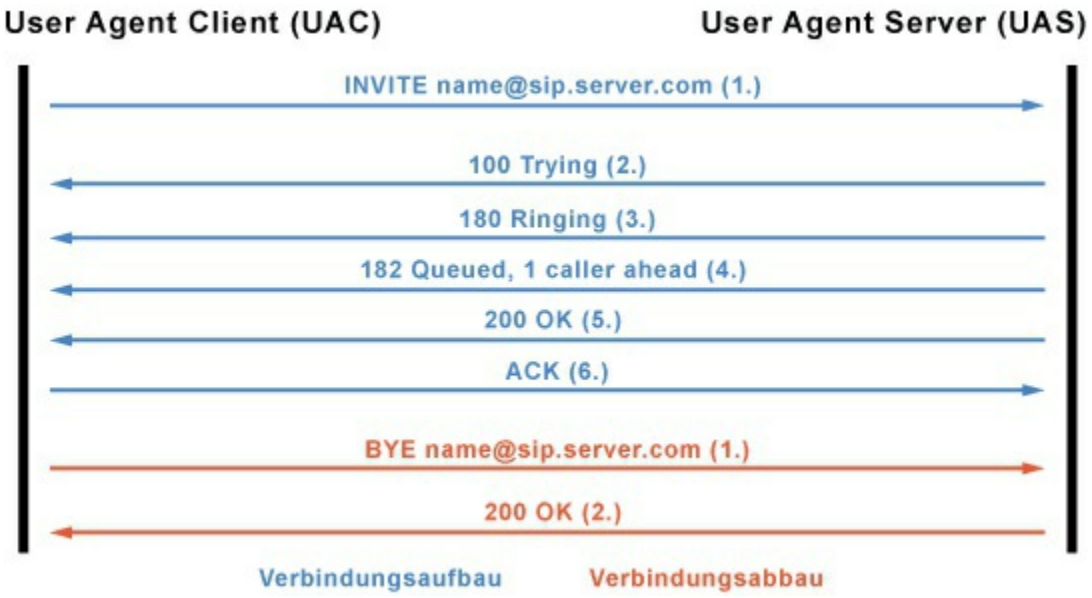
In einer SIP-Verbindung wird der Anrufer als User Agent Client (UAC) und der Angerufene als User Agent Server (UAS) bezeichnet.

Die Sitzungsabläufe können direkt zwischen den User Agents ablaufen. Allerdings ist nicht immer gewährleistet, dass ein User Agent erreichbar ist und immer dieselbe IP-Adresse hat. Daher meldet sich ein User Agent in der Regel an einem SIP-Server (Registrar) an, der als Proxy fungiert. Der SIP-Server registriert die IP-Adresse. Wenn ein Anruf auf die SIP-Adresse des SIP-Clients erfolgt, wird die SIP-Adresse

aufgelöst und ermittelt, wo der Client erreichbar ist. Anschließend wird der Anruf und alle anderen Anfragen an den Client weitergeleitet.

SIP bedient sich beim Rufaufbau eines SIP-Proxys. Um erreichbar zu sein, muss sich jeder SIP-Teilnehmer bei einem SIP-Registrat anmelden. Meistens sind der SIP-Proxy und der SIP-Registrar der gleiche Server. Der SIP-Registrar hat eine ähnliche Funktion, wie der DNS-Server. Der SIP-Proxy greift auf den SIP-Registrat zu, um den Standort des Teilnehmers herauszufinden.

Verbindungsaufbau bei



einer direkten Verbindung

zwischen UAC und UAS

Der UAC leitet den Verbindungswunsch

durch ein INVITE ein. Der UAS

bestätigt dem UAC den

Verbindungswunsch mit einem "Trying".

Mit "Ringing" wird dem UAC bestätigt, dass dem Angerufenen der

Verbindungswunsch signalisiert wird. Ist

der Gesprächspartner belegt, dann

schickt der UAS dem UAC ein "Busy

here".

Nimmt der gewünschte

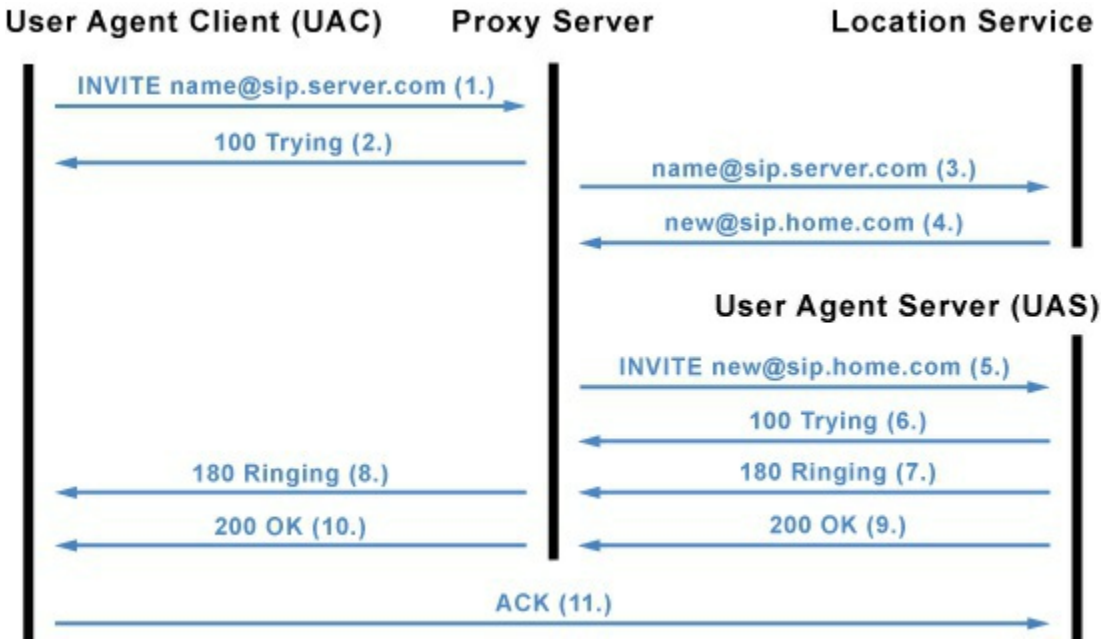
Gesprächspartner den

Verbindungswunsch an, dann schickt der

UAS dem UAC ein "OK". In diesem Response werden auch die SDP-Verbindungsparameter mitgeschickt. Der UAC bestätigt dem UAS den Verbindungsaufbau und die Verbindungsparameter mit einem "ACK". Das Gespräch ist aufgebaut.

Wenn einer der beiden Teilnehmer das Gespräch beendet, schickt der User Agent ein "BYE" und bekommt das von der Gegenseite mit einem "OK" bestätigt.

Verbindungsaufbau über einen Proxy-Server



Der UAC leitet seinen

Verbindungswunsch mit einem INVITE
an seinen Proxy-Server ein. Zur
Bestätigung bekommt der UAC ein
"Trying" zurück.
Der Proxy-Server befragt seinen
"Location Service" nach der IP-Adresse des gewünschten Teilnehmers. Er
bekommt die Adresse des Teilnehmers
zurück. Wenn es für den UAS mehrere
IP-Adressen gibt, dann bekommt jede
IP-Adresse eine Verbindungsanfrage.
Demzufolge signalisiert jeder UAS den
Verbindungswunsch. Im einfachsten Fall
klingeln die SIP-Telefone.
Damit der Proxy-Server die IP-Adresse
des UAS aus einem fremden Netz
bekommen kann, muss der "Location
Service" mit möglichst vielen
Datenbanken anderer SIP-Provider
zusammengeschaltet sein.
Der Proxy-Server leitet die
Verbindungsanfrage an den UAS weiter.
Dabei spielt es keine Rolle, ob der UAS

im gleichen Domain-Bereich oder an

einer anderen Domain hängt. Der UAS

schickt dem Proxy-Server darauf ein

"Trying" zur Bestätigung. Wenn es beim UAS klingelt folgt ein "Ringing", das der Proxy-Server an den UAC weiterreicht.

Nimmt der Teilnehmer beim UAS ab,

dann schickt er ein "OK" an den Proxy-Server, der auch das an den UAC

weiterreicht. In der OK-Meldung sind

zusätzlich alle SDP-

Verbindungsparameter enthalten. Der

UAC bestätigt dem UAS den

Verbindungsaufbau und die

Verbindungsparameter mit einem

"ACK". Das Gespräch ist aufgebaut.

Wenn einer der beiden Teilnehmer das

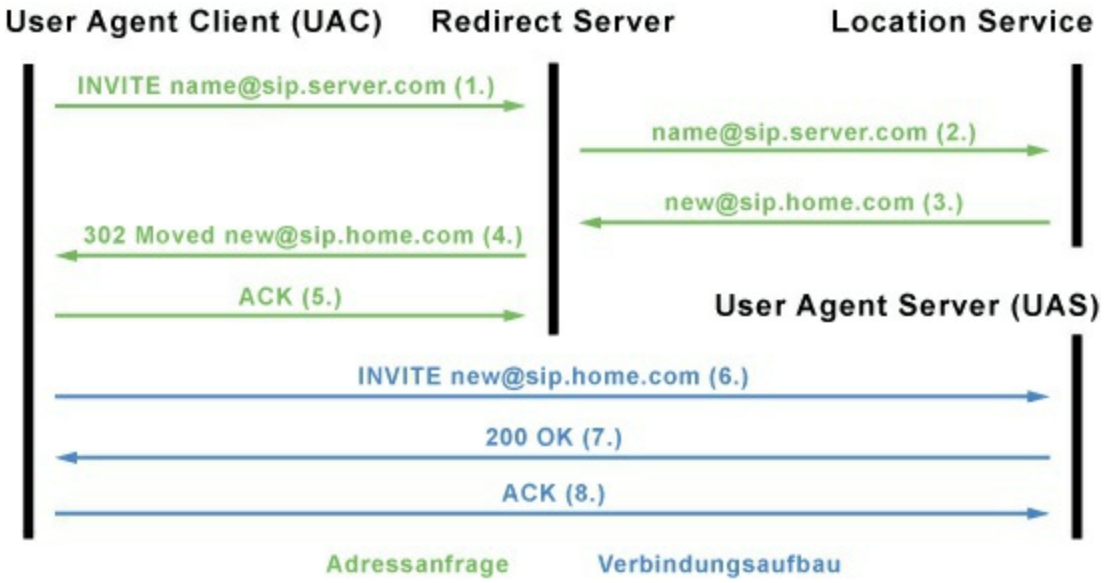
Gespräch beendet, schickt der User

Agent ein "BYE" und bekommt das von der Gegenseite mit einem "OK"

bestätigt.

Verbindungsaufbau über

einen Redirect-Server



Der UAC leitet seinen Verbindungswunsch mit einem INVITE an seinen Redirect-Server ein. Der Server befragt seinen "Location Service" nach der IP-Adresse des gewünschten Teilnehmers. Er bekommt die Adresse des Teilnehmers zurückgeliefert. Der Redirect-Server meldet dem UAC die Adresse des gewünschten Teilnehmers. Der UAC bestätigt den Erhalt der Adresse mit einem "ACK".
Dann kontaktiert der UAC den UAS direkt mit einem "INVITE". Danach

verläuft der weitere Verbindungsaufbau, wie bei einer Direktverbindung.

SIPS - Session Initiation Protocol Security

SIPS ist ein Erweiterung für SIP um eine Verschlüsselung mit TLS/SSL. Mit SIPS kann der Verbindungsaufbau mit nicht mehr abgehört werden. Die Daten werden verschlüsselt im Internet übertragen.

SIP ist dem HTTP-Protokoll sehr ähnlich. Für die Sicherheit stellt das ein Problem dar. Die Verbindungsdaten werden in Klartext im Internet übertragen und können abgehört und eingesehen werden. Für das ganz normale Surfen mit dem Protokoll HTTP ist das kein Problem. Nur bei eCommerce-Anwendungen wie Online-Shopping oder Online-Banking wird der Datenaustausch verschlüsselt, damit

niemand die Kundendaten mitprotokollieren kann.

SIPS funktioniert so ähnlich wie HTTPS. Es handelt sich dabei um die Verschlüsselung von SIP mit TLS/SSL. Mit SIPS wird eine verschlüsselte Verbindung aufgebaut.

Die Verbindung zwischen Telefon und Proxy kann zwar immer noch abgehört werden. Die Daten werden jedoch verschlüsselt und können nicht mehr eingesehen werden. Bei den Server- und Proxy-Herstellern ist SIPS sehr häufig implementiert. Bei den Telefon-Herstellern und SIP-Providern ist es dagegen weniger verbreitet.

Ob man die Verschlüsselung der Verbindung zwischen Telefon und SIP-Server braucht, muss jeder Anwender selber entscheiden. Ohne Verschlüsselung kann der Verbindungsaufbau mit SIP von einem

Dritten abgehört und sogar gestört werden.

H.323 und SIP im Vergleich

Hauptvorteil von SIP ist die einfache Integration in bestehende IP-Netze. SIP nutzt die vorhandenen Dienste im Internet, wie HTTP, SMTP, MIME, URL und DNS mit. Bei SIP kann die Kommunikation vollständig von den Clients abgewickelt werden. Bei Voice over IP mit H.323 ist in der Regel ein Gatekeeper erforderlich.

Gegenüberstellung von H.323 und SIP

VoIP-Standard	**H.323**
Philosophie	Genau definierte Systemarchitektur und Implementierungsrichtlinien.
	Regelung von Anrufaufbau,

-abbau, Steuerung und

Medium.

Anforderung

Telekommunikationstechnik

Leistungsmerkmale werden

Rückwärtskompatibilität als Ergänzung zu den vorhandenen hinzugefügt.

Steuerung durch einen

Architektur

Server.

Protokolle im Vergleich:

H.323 und SIP

H.323

SIP

Teilnehmer

E.164

Teilnehmer

G.711 / G.729 /

G.711 / G.729 /

G.723 / ...

G.723 / ...

H.225 /

SAP

H.245

RTP

SDP

RTCP

SIP

TCP

UDP

TCP

UDP

IP

IP

Ethernet / ATM /

Data Link

...

Physical Link

T1 / T3 / H.221 /

H.224

Verbindungsaufbau

zwischen H.323 und SIP

Die folgende Beschreibung geht von

einer Verbindung von H.323 zu SIP aus.

Für die Standardisierung ist das IETF

verantwortlich, die auch SIP

standardisiert hat.

Am Verbindungsaufbau und der

Verbindung selber sind drei

Komponenten beteiligt:

Teilnehmer aus dem H.323-Netz

Teilnehmer mit SIP-Telefon

IWF (Interworking Function)

Die IWF ist eine "Black Box", die für die Umsetzung der beiden Protokolle

H.323 und SIP zuständig ist. Die IWF

übernimmt die Anmeldung der

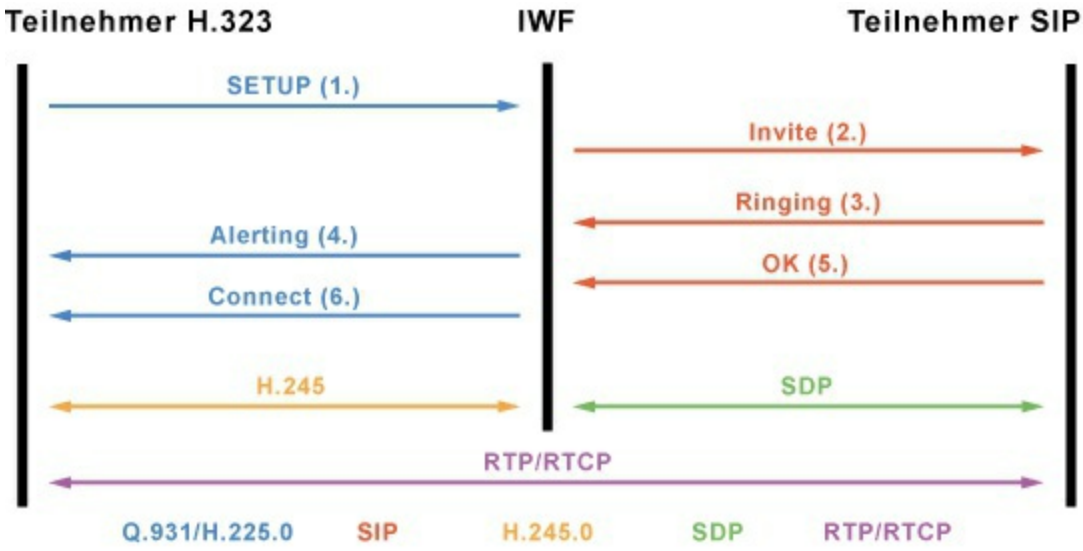
Teilnehmer, die Adressumsetzung und

die gegenseitige Anrufsignalisierung.

Die IWF kann sowohl in einem H.323-

Gatekeeper, als auch in einem SIP-Proxy

implementiert sein.



Für die Beschreibung der Verbindung (Session) wird zwischen Teilnehmer A und IWF H.245 und zwischen Teilnehmer B und IWF SDP (Session Description Protocol) verwendet. Der IWF-Server übernimmt jeweils die Übersetzung. Für den Austausch der Sprach- und Video-Daten wird RTP und RTCP verwendet.

Teilnehmer A leitet den Verbindungswunsch mit einem SETUP (H.323) ein, den er an den IWF-Server schickt. Der übersetzt das SETUP in eine INVITE-Nachricht (SIP) für Teilnehmer B. Dann wird die

Anrufsignalisierung von Teilnehmer B

eingeleitet und mit "Ringing" an den IWF-Sever gemeldet. Der übersetzt das

für den Teilnehmer A in "Alerting". Die Verbindungsannahme wird vom

Teilnehmer B mit "OK" und für

Teilnehmer A mit "Connect" bestätigt.

STUN - Simple

Traversal of UDP

through NAT

Simple Traversal of UDP through NAT,

kurz STUN, ist ein Protokoll, mit dem

zwei SIP-Endgeräte mit integriertem

STUN-Client unter Mithilfe eines

STUN-Servers die Beschränkungen von

NAT in vielen Fällen umgehen können.

Probleme durch NAT für

Voice-over-IP mit SIP im

Internet

Voice over IP mit SIP setzt immer

voraus, dass die Endgeräte über ihre IP-

Adresse erreichbar sind. Steht das

Endgerät hinter einem Router mit NAT

(Network Address Translation), dann kann dieses Endgerät von außen nicht erreicht werden. Der Router leitet den Datenverkehr von außen nur dann durch, wenn der Datenverkehr von innen initiiert wurde. Denn sonst ist ihm nicht bekannt, für welches Endgerät die Daten von außen bestimmt sind. Dazu kommt noch, das Endgerät kennt noch nicht einmal seine eigene Adresse im Internet.
Folgende Problematik kommt erschwerend hinzu: Der Datenstrom wird über RTP übertragen und mit RTCP gesteuert. Dabei werden dynamisch die Ports genutzt. Bei NAT-Routern und Firewalls führt das zu Problemen. Dort besteht die Gefahr, dass die Verbindungen blockiert werden.
Um diese Probleme zu umgehen, betreibt der SIP-Provider einen STUN-Server.
Er teilt dem Endgerät auf Anfrage mit,

mit welcher IP-Adresse er im Internet erreichbar ist und hinter welcher Art von Firewall er sich befindet.

Funktionsablauf bei STUN

Der STUN-Server bekommt vom Endgerät eine Nachricht geschickt. Er sendet ein Paket zurück, in der IP-Adresse und Port des gesendeten Pakets enthalten sind. Das Endgerät, das sich hinter dem NAT-Router befindet, kann dann diese Informationen für alle folgenden Verbindungen in den SIP- und SDP-Paketen verwenden. Dadurch kann ein Endgerät auch herausfinden, ob Zugang zum Netzwerk besteht, ob die Firewall UDP-Pakete blockiert und ob NAT zum Einsatz kommt.

Audio-Codecs zur Sprachdigitalisierung

Wie bei der Digitalisierung der Sprache für die Fernsprechübertragung arbeiten Codecs nach dem Prinzip Sampling,

Quantisierung und Kodierung. Dadurch erreicht man eine optimale Sprachqualität, um das analoge Sprachsignal über digitale Systeme zu übertragen.
Bei 8.000 Abtastungen pro Sekunde (Sampling), mit einer Quantisierung von 8 Bit pro Abtastung ergibt sich eine Bitrate von 64 kBit pro Sekunde (nach µ-Law/a-Law). Diese Technik wird als PCM bezeichnet. Sie wird im leitungsvermittelten ISDN für die Digitalisierung der Sprache verwendet.
In einem paketvermittelten Netz ist man immer bestrebt Bandbreite zu sparen. Deshalb werden die Sprachdaten meistens noch komprimiert. Bei zunehmender Komprimierung nimmt die Sprachqualität ab, die Dekomprimierungszeit und die erforderliche Rechenleistung nehmen zu.
Es gilt: Je höher die Bitrate eines

Codecs ist, desto besser die Tonqualität. Je niedriger die Bitrate, desto schlechter die Tonqualität und höher der Bedarf an Rechenleistung. Das gilt jedoch nicht immer. Die meisten Codecs machen sich die Eigenschaften der menschlichen Sprache zu nutze um möglichst verlustfrei zu komprimieren.
Es gibt verschiedene Codecs, die für Multimedia-Übertragung im IP-Netzwerk geeignet sind. G.711 (PCM) bietet die beste Sprachqualität. Es kommt ohne rechenintensive Kompression aus und braucht deshalb auch relativ viel Bandbreite. Werden die Sprachdaten mit einem anderen Codec komprimiert, dann wird G.711 beim Qualitätsvergleich herangezogen.
Codecs zur Sprachdigitalisierung müssen einige Bedingungen erfüllen. Bedingt durch die Struktur des Internets (paketorientierte Übertragung und

Vermittlung) müssen sie Paketverluste (bis zu 5%) verkraften und Laufzeitunterschiede der einzelnen Pakete ausgleichen und in die richtige Reihenfolge sortieren können (Forward Error Correction und Jitter Buffering). Das bedeutet, dass Paketverluste und Laufzeitschwankungen keinen Einfluss auf die Sprachqualität haben dürfen.
Die Auswahl eines Codecs ist immer ein Kompromiss zwischen Sprachqualität, Bitrate, Bandbreite und Rechenleistung. Muss die Sprachqualität sehr gut sein, dann ist die Bitrate sehr groß. Entsprechend muss eine ausreichende Bandbreite über die gesamte Übertragungsstrecke zur Verfügung stehen. Reicht eine geringere Sprachqualität aus, dann sinkt dadurch die Bitrate und der Bedarf an Bandbreite. Gleichzeitig steigt dabei der Bedarf an Rechenleistung, um die

Sprachdaten zu dekomprimieren.

MOS - Mean Opinion Score

MOS

kleiner

größer

4

vergleichbar mit

vergleichbar mit

der

der

Sprachübertragung

Sprachübertragung

im Mobilfunknetz

im Festnetz

Von Bell Labs wurde der "Mean Opinion Score" (MOS) definiert. Der MOS ermittelt das statische Empfinden der Sprachqualität eines Benutzers. Der MOS 4 gilt als Grenzwert. Darüber wird die Sprachqualität besser, darunter schlechter.

MOS-

Bedeutung

Wert

keine Anstrengung zum

5 /

Verständnis der Sprache

excellent notwendig

keine Anstrengung notwendig,

4 / good aber Aufmerksamkeit

notwendig

leichte Anstrengung

3 / fair

notwendig

2 / poor merkbare, deutliche

Anstrengung notwendig

trotz Anstrengung kein

1 / bad

Verständnis

G.711

G.711 ist der älteste Codec. Er wurde

bereits 1965 von der ITU zugelassen. Er

benötigt nur eine geringe Rechenleistung,

erzeugt dafür einen Datenstrom von 64

kBit/s.

IP-Telefonie-Anbieter setzen häufig auf G.711. Es ist dasselbe Verfahren wie bei ISDN. Der Vorteil liegt in der einfachen Durchleitung der Sprachdaten vom Festnetz ins IP-Netz bzw. umgekehrt. Eine Umkodierung der Sprachdaten ist nicht notwendig.
Für schmalbandige Internet-Zugänge oder Netzwerkverbindungen ist dieser Codec jedoch ungeeignet.

G.722

Der Codec G.722 bewertet die Signaldifferenz zwei aufeinanderfolgender Signale. So lässt sich mit der selben Bitrate von G.711 ein Sprachsignale bis 7 kHz mit einer Abtastrate von 16 kHz digitalisieren.
Das Frequenzband reicht von 50 Hz bis 7.000 Hz. Der Bandbreitenbedarf liegt bei 48, 56 oder 64 kBit/s.

G.723.1

Durch ein Prädiktionsverfahren erreicht dieser Codec mit einer Bitrate von 5,6 oder 6,3 kBit/s, einer Audiobandbreite von 3,1 kHz und einer Bitbreite von 8 Bit eine etwas geringere Sprachqualität als G.711. Dabei ist die erforderliche Rechenleistung bei G.723 nicht zu unterschätzen. Das ist der Kompression geschuldet, die die Datenrate im Vergleich zu G.711 auf 10% drückt.

G.729 / G.729A

Bei G.729 handelt es sich um die optimierte Variante des CELP-Algorithmus für Sprachübertragungen. G.729 ist mit G.723 vergleichbar. Der Bandbreitenbedarf liegt bei nur 8 kBit/s, wodurch eine geringere Rechenleistung im Vergleich zu G.723 erforderlich ist. Für VoIP-Anwendungen wird der Codec G.729A verwendet. Er ist die Grundlage für eine gute Sprachqualität in VoIP-Verbindungen. Unter Berücksichtigung

des IP-Overheads, der Sprachkomprimierung und der Sprechpausenunterdrückung wird eine Bandbreite von ca. 10 kbit/s (1,25 kByte/s) pro Sprachverbindung benötigt. Diese Bandbreite muss das Datennetz für jedes Gespräch gewährleisten. Alternativ stellen VoIP-Anbieter Verbindungen mit G.729 zur Verfügung. Die eingesetzte Kompression drückt die Datentransferrate auf fast 10%. Obwohl das Abstriche bei der Sprachqualität bedeutet, ist das deutlich besser als die Sprachqualität im Mobilfunknetz.

Linear-PCM 16 (L16)

Linear-PCM 16 (L16) ist von der TIA (Telecommunications Industry Association) im Rahmen der Spezifikation TIA 920 für Breitband-Kommunikation definiert (Breitband-Internet-Anschlüsse). Das Sprachsignal wird 16.000 mal pro Sekunden

abgetastet (Sampling). Die Sprachdaten werden mit 16 Bit aufgelöst (Quantisierung). Die Übertragung findet ohne Kompression, ohne Latenz und ohne Umwandlung statt. Damit bietet L16 die beste Sprachqualität.

PCMA-16

PCMA-16 ist eine 16-kHz-Variante des G.711-Codecs. PCMA-16 bietet eine Abtastrate von 16.000 Samples pro Sekunde (Sampling). Die Sprachdaten werden nach dem A-Law in 8 Bit aufgelöst (Quantisierung).

GSM

GSM ist der Codec für die Sprachübertragung im Mobilfunknetz. Die Bandbreite beträgt 13,2 kBit/s.

iLBC

Der Codec iLBC wurde für schmalbandige Übetragungsstrecken im Internet entwickelt. Er ist darauf optimiert, im Falle von verloren

gegangenen und verzögert eingetroffenen Datenpaketen, eine gleichbleibende Sprachqualität und -verständlichkeit zu liefern. Der Codec besitzt eine höhere Qualität als G.729. Die Bandbreite liegt bei 13,33 kBit/s.

Speex (SPX)

Speex zeichnet sich dadurch aus, dass er eine variable Bitrate hat und somit optimal an die Sprachübertragung angepasst ist. So zum Beispiel an Sprechpausen, in denen so gut wie keine Daten anfallen. Die Bandbreite variiert zwischen 2,15 und 24,6 kBit/s.

Skype

Skype verwendet einen propritären Codec, der Audiosignale bis etwa 12 kHz übertragen kann.

Übersicht und Vergleich der Audio-Codecs

Codec Bandbreite MOS MIPS Delay

56 oder 64

0,25

G.711

4,10 1

kbit/s

ms

5,6 - 6,3

67,5

G.723.1

3,90 18

kbit/s

ms

G.723

5,3 kbit/s

3,65

16 - 40

G.726

3,85

kbit/s

1,25

G.728

16 kbit/s

3,61 30

ms

G.729

8 kbit/s

3,92 20

25 ms

G.729A 8 kbit/s

3,70 11

25 ms

GSM

13 kBit/s

iLBC

15 kBit/s

2,15 - 44,2

Speex

kBit/s

LPC10 2,4 kBit/s

FoIP - Fax over IP

Telefonverbindungen werden nicht nur

für Telefongespräche, sondern auch zum

Übertragen von Fax-Dokumenten

genutzt. Doch diese Anwendung ist in

Voice-over-IP-Umgebungen technisch

nicht vorgesehen. Dokumente als Fax mit Voice over IP zu übertragen ist in der Regel schwierig. Im Gegensatz zu Telefonen reagieren Faxgeräte empfindlich auf noch so kleine Störungen. Sie führen zu einem sofortigen Abbruch der Verbindung. Unvollständig übertragene Dokumente, die etwa ab der Hälfte abgeschnitten sind, sind die Regel. Dasselbe trifft auch bei dem Versuch zu, eine VoIP-Übertragungsstrecke zur Datenübertragung mit analogen Modems zu verwenden. Auch hier bricht die Verbindung ab.

Aus diesem Grund gibt es Standards, um Fax-Dokumente per Voice over IP zu übertragen. Man ordnet diese Standards Fax over IP zu. Fax over IP kennt zwei Standards. Einmal T.37 für die Store-and Forward-Übermittlung von Facsimilies und T.38 für die

Faxübermittlung in Echtzeit.

Auch wenn es T.37 und T.38 gibt, muss man von einer Faxübertragung per VoIP eher abraten. Die meisten VoIP-Provider unterstützen T.37 und T.38 nicht.

Technischer Hintergrund:

Warum Fax via VoIP nicht funktioniert?

Bei der Übertragung von Sprache wird das analoge Sprachsignal in ein digitales Signal umgewandelt. Jeweils 20 ms der Sprache wird in einem Datenpaket per UDP bzw. RTP auf die Reise geschickt. Der Empfänger setzt die erhaltenen Pakete in der richtigen Reihenfolge wieder zusammen und wandelt das digitale Signal in ein analoges Signal zurück.

Um die Sprache in guter Qualität wiedergeben zu können ist der Empfänger auf einen kontinuierlichen Datenstrom angewiesen. Kommt ein

Paket nicht an, dann fehlen 20 Millisekunden oder mehr. Wenn das digitale Signal wieder in ein analoges Sprachsignal zurückgewandelt wird, dann ist ein Knackser hörbar. Allein das fehlen eines Datenpakets führt zum Abbruch einer Fax-Verbindung. Denn die Faxgeräte sind nicht nur auf einen kontinuierlichen, sondern auch auf einen vollständigen Datenstrom angewiesen. Fehlende oder fehlerhafte Paket einfach noch mal beim Sender anzufordern, würde zu lange dauern. Die Verzögerung verschlechtert die Übertragungsqualität noch mehr.

Das nächste Problem wird durch Laufzeitschwankungen hervorgerufen. Das bedeutet, zwischen den Datenpaketen darf nur eine gleichmäßige Verzögerung auftreten. Eine Fax-Verbindung braucht einen kontinuierlichen Datenstrom. Um die

Laufzeitschwankungen zwischen den Paketen auszugleichen kommen die empfangenen Pakete zuerst in einen Jitter-Puffer. Der Jitter-Puffer verzögert die Pakete, um am Ausgang eine gleichmäßige Verzögerung und damit einen gleichmäßigen Datenstrom zu erreichen. Eine Verzögerung von 100 bis 200 ms stellt kein Problem dar. Auch wenn die Pufferzeit ab und zu angepasst wird und zum Beispiel ein Aussetzer von 100 ms entsteht, nimmt man das bei einer Sprachverbindung kaum war.
Aber, ein Faxmodem verliert dadurch die Synchronisierung zur Gegenstelle und bricht die Verbindung ab.
Erschwerend kommt hinzu, dass je länger ein Übertragung dauert, desto eher bricht die Verbindung ab.
Eine weitere Schwierigkeit ist die Tatsache, dass die üblichen VoIP-Adapter für die Sprachübertragung

optimiert sind. Das bedeutet, sie minimieren die Datenmenge, unterdrücken Rauschanteile und passen den Frequenzgang an die menschliche Sprache an. Zusätzlich wird in Sprechpausen ein künstliches Rauschen eingestreut, damit die Nutzer das Gefühl haben, dass die Verbindung noch steht, auch wenn nicht gesprochen wird.
Alle diese Maßnahmen sind Gift für eine Fax-Übertragung. Wenn dann noch ein verlustbehafteter Codec für die Analog/Digital-Wandlung eingesetzt wird, dann kann das Faxmodem auf der Gegenseite mit dem Signal nichts mehr anfangen.

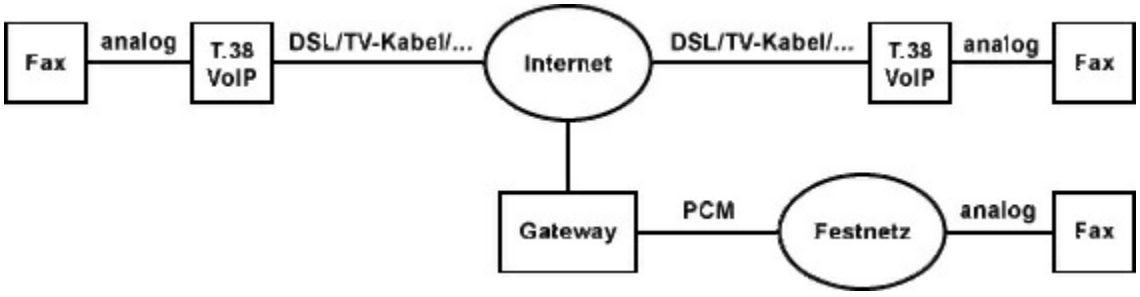
Lösung ohne zusätzliche Protokolle

Gelegentlich kann man VoIP-Adapter und VoIP-Gateways für Fax-Übertragungen konfigurieren. In diesem Fall verzichtet der VoIP-Adapter auf

Signalaufbereitung, Echo-Unterdrückung, Rauschunterdrückung und andere Signalbearbeitungen. Zusätzlich wird die Größe des Jitter-Puffers optimiert und der komprimierungsfreie Codec G.711 verwendet. Manche VoIP-Adapter sind sogar so gut, dass sie den Faxträger erkennen und dann automatisch alle Einstellungen für die Fax-Übertragung optimieren.

T.37

T.37 basiert auf der Übertragung per E-Mail. Das Fax wird in eine TIFF-Bilddatei umgewandelt. Dann wird eine



E-Mail mit der Bilddatei als Anhang und mit der Empfänger-Faxnummer als Adresse verschickt. Die Übertragung ist

unabhängig von Zeit und Bandbreite.
Aber die Umwandlungsprogramme
müssen ständig aktuell sein.

T.38

Für zuverlässige Faxübertragungen ist
das Protokoll T.38 geeignet. Ein VoIP-
Adapter mit T.38 kann als Gateway für
ein Fax dienen. Es nimmt die die
Faxsignale entgegen und stimmt sich mit
der Gegenstelle ab. Die Daten werden in
digitaler Form übertragen. Die
Gegenstelle kann wiederum ein T.38-
VoIP-Adapter sein oder ein Gateway
zum Festnetz. Faxgeräte beherrschen
üblicherweise kein T.38.
Bei T.38 wird eine Echtzeit-Verbindung
zwischen den Gegenstellen
vorausgesetzt. T.38 basiert auf H.323.
Zuerst wird eine H.323-Verbindung
aufgebaut und dann die Faxe mit T.38
übertragen.

QoS - Quality of

Service

Standardmäßig werden in einem Netzwerk alle Datenpakete gleich behandelt. In einem Paket-orientierten Netzwerk können die einzelnen Datenpakete unterschiedliche schnell unterwegs sein. So lange hauptsächlich Nachrichten und Dateien übertragen werden, kommt es hierbei zu keinem Problem. Werden jedoch Echtzeitanwendungen, wie Voice over IP oder Videostreaming genutzt, dann wirkt sich die Verzögerung oder Paketverlust auf die Übertragungseigenschaften zwischen den Teilnehmern negativ aus. 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 verzögerter Auslieferung der Datenpakete. 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, sind die Übertragungssysteme nicht in der Lage zwischen einem Sprachpaket und einem normalen Datenpaket zu unterscheiden. Viele QoS-Maßnahmen versuchen diesen Mangel auszumerzen und Datenpakete mit Diensteklassen zu kennzeichnen, die bestimmten Anwendungen zugeordnet sind.
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 Switches 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.
Achtung: 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 wichtige Daten bevorrechtigt 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 am 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 werden 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.

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. Das liegt daran, dass Datenverkehr und Bandbreite sehr billig sind. Bei den

meisten Netzbetreibern wird QoS ganz einfach durch eine überdimensionierte Bandbreite umgesetzt.

Netzwerk-Sicherheit

Grundlagen der Netzwerk-Sicherheit

Firewall

VPN - Virtual Private Network

AAA - Authentication Authorization Accounting

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 End-to-End-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.

In diesem Zusammenhang steigen auch die Anforderungen an Unternehmensnetzwerke. Auf sie sollen extern arbeitende 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 aber auch Tribut in 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 die mobilen Geräte ursprünglich für den Privatgebrauch und

nicht für Unternehmenszwecke
entwickelt wurden.

Die 3 Pfeiler der Netzwerk-Sicherheit

Integrität
Vertraulichkeit
Authentizität

Integrität // Vertraulichkeit // Authentizität

Netzwerksicherheit umfasst drei wesentliche Merkmale. Das eine ist die Integrität. Dahinter verbergen sich Mechanismen, die die Echtheit von Daten prüfen und sicherstellen können. Dazu zählen auch Mechanismen und Verfahren, die Daten vor Manipulation schützen.

Das zweite ist die Vertraulichkeit der Kommunikation. Hier geht es darum dafür zu sorgen, dass niemand Einblick in die Daten und Kommunikation erhält.

Hier steht die Authentifizierung der

Kommunikationspartner und die Verschlüsselung der Kommunikation im Vordergrund.

Das zweite ist die Authentizität der Kommunikationspartner. Hier geht es darum festzustellen, ob der Kommunikationspartner auch tatsächlich der ist, für den er sich ausgibt.

Authentifizierung und Autorisierung

Authentifizierung ist der Vorgang um festzustellen wer die Person oder Maschine ist. Autorisierung ist der Vorgang, bei dem ermittelt wird, was die Person oder Maschine machen darf (Berechtigung).

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.

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 fehlerhafte 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

HTTPS

Application Layer

6

SSH

Anwendungsschicht

SSL

5

4

Network Layer

IPsec

3

Netzwerkschicht

2

Data Link Layer

PPTP

1 Übertragungsschicht

L2TP

Maßnahmen auf der Übertragungsschicht

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

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

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.

Sicherheitssoftware

Sicherheitssoftware soll vor unberechtigten Zugriffen durch Schadsoftware schützen. Die meisten Angriffe und Zugriffe erfolgen über den Versuch Schadsoftware durch Unachtsamkeit des Nutzers einzuschleusen, zu installieren und zu aktivieren und somit Zugriff auf das System zu bekommen.

Virus

Wurm

Trojaner

Malware

Rootkit

Fakeware/Ransomware

Virenscanner

Virenscanner sind Bestandteil einer

Sicherheitssoftware, die einen Computer im laufenden Betrieb auf Viren, Würmer und Trojaner untersucht. Dabei wird neben dem Arbeitsspeicher auch die Festplatte nach verdächtigen Datenfolgen durchsucht. Zusätzlich klinken sich Virenscanner dort im Betriebssystem ein, wo Daten zwischen Massenspeicher und Arbeitsspeicher übertragen werden, um zu verhindern, dass Schadsoftware zur Ausführung kommt. Weil Schadsoftware ist im Laufe der Zeit erheblich weiterentwickelt hat und von einem normalen Programm teilweise nicht mehr zu unterscheiden ist, eignen sich herkömmliche Mittel, wie der klassische Virenscanner nicht mehr, um einen Großteil der Schadsoftware zu erkennen.
Deshalb baut moderne Sicherheitssoftware immer öfter auf Verhaltenserkennung. Also typische

Aktivitäten von Schadsoftware, die von normalen Programmen und deren Nutzung abweicht.

Dynamic Malware Detection erkennt Schädlinge an ihrem Verhalten. Das hilft bei Malware, für die es noch keine Erkennung gibt. Die Verhaltenserkennung wertet protokollierte Aktivitäten von Prozessen aus und versucht Unregelmäßigkeiten zu erkennen.

Was bringen Desktop-Firewalls, Security-Suiten und Virenscanner?

Grundsätzlich gilt, jede Software, die Daten aus unsicheren Quellen (z. B. Internet) liest, ist als Angriffsfläche missbrauchbar. Dazu zählen von außen erreichbare Server-Dienste, aber auch Client-Software wie Browser, Mail-Clients, Messenger und so weiter. Ungeachtet ihrer Sicherheitsfunktionen

fallen auch Personal Firewalls und Virenscanner darunter.

Jede Software, auch die eigentlich die Sicherheit erhöhen soll, vergrößert die Angriffsfläche. Deshalb sollte man immer abwägen, wo die Vor- und Nachteile einer Sicherheitssoftware liegen. In der Regel macht ein Virenscanner Sinn. Eine Personal Firewall ist in der Regel unnötig und gaukelt nur Sicherheit vor. Die Firewall, die zum Beispiel in Windows XP (SP2), Windows 7 oder Mac OS enthalten ist, ist schlank, fest ins System integriert und gilt als sicherer als so manche Security-Suite.

Das bedeutet nicht, dass sich die Firewall eines Betriebssystems nicht verbessern lässt. Im Gegenteil. In der Regel darf sich jede Applikation bei der Installation selbst in die Ausnahmeliste der Firewall eintragen. Die

Applikationen sind dabei sehr freigiebig bei der Eintragung. Eine Personal Firewall kann die Ausnahmen deutlich einschränken. Sofern sie gut gepflegt wird, spricht nichts gegen den Einsatz einer zusätzlichen Desktop-Firewall.

Mit steigender Komplexität einer Software nimmt die Wahrscheinlichkeit von Fehlern zu. Ab einer gewissen Komplexität ist eine Software nicht mehr fehlerfrei. Es ist davon auszugehen, dass "jede" Software fehlerhaft ist. Eine fehlerhafte Software, die mit Daten aus unsicheren Quellen arbeitet, ist mit einer besonders großen Angriffsfläche gleichzusetzen. Und diese Angriffsfläche steigt mit der Komplexität der Software.

Für jedes Betriebssystem, egal ob Windows, Linux oder Mac OS, gilt:

Jede nicht in Gebrauch befindliche Software deinstallieren.

Jeden nicht benötigten Server-Dienst abschalten.

Anzahl der Software-Fehler durch regelmäßige Updates reduzieren.
Bei Software-Alternativen diejenige mit den geringsten Fehlern wählen.
Tendenziell die weniger komplexe Lösung einsetzen.
Bis hierher ist noch keine spezielle Sicherheitssoftware erforderlich. Das bedeutet, ein hohes Maß an Sicherheit kann "jeder" schon mit einfachen Maßnahmen erreichen.
Das Computermagazin ct stellte in seiner Ausgabe 5/2010 fest, "dass jedes Paket (Security-Suite) in fast jeder Kategorie so ernste Defizite aufweist, dass man von ihrem Einsatz abraten muss." Zuvor wurde festgestellt, "das keines der (getesteten) Programme dem Anspruch gerecht wird, besser zu sein als das, was Windows und Mail-Clients eh schon bereitstellen."

Im Editorial des selben Hefts finden sich klare Worte: "Andererseits entpuppen sich die Suiten bei näherem Hinsehen als Pappkameraden." und "Der versprochene Rundumschutz findet nicht statt."

Durch den Test kommen die Redakteure zu der Empfehlung: "Ein reiner Virenscanner reicht nicht nur aus. Man sollte ihn gegenüber einer Security-Suite sogar unbedingt vorziehen."

Was 2010 getestet wurde hat sich bis heute nicht wirklich entscheidend verbessert. Vor diesem Hintergrund sollte man der installierten Security-Software nicht vertrauen.

Das Hauptproblem ist der Nutzer

Das größte Sicherheitsproblem ist immer noch der Nutzer selber. Die wichtigste Maßnahme ist die Sensibilisierung für

Sicherheitsprobleme. Dadurch reduziert sich die Angriffsfläche automatisch.
Richtig böse ist es, wenn der Nutzer die Schadsoftware meist unwissentlich selbst installiert. Zum Beispiel durch das Öffnen eines E-Mail-Anhangs. Doch Otto-Normal-Nutzer ist sehr schwer von einem sehr vorsichtigen Umgang mit fremden Dateien zu überzeugen. Deshalb ist der Sicherheitsgewinn durch einen Virenscanner höher zu bewerten, als die zusätzlich entstehende Angriffsfläche durch den Virenscanner selber.
Doch Vorsicht, ein Virenscanner ist ein Tool zum Überprüfen von Dateien auf Schadsoftware. Mehr Sicherheit bietet er nicht. Er kommt immer nur dann zum Einsatz, wenn es eigentlich schon zu spät ist. Ein Virenscanner kann im Zweifelsfall den Virenbefall nicht verhindern, wenn er den Virus nicht kennt.

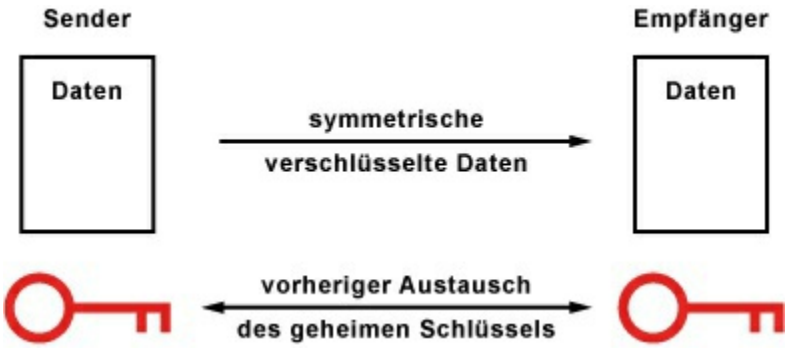
Verschlüsselung

Die moderne Verschlüsselung von Daten basiert auf einem digitalen bzw. elektronischen Schlüssel. Die Verschlüsselungsverfahren (Algorithmen) benötigen den digitalen Schlüssel als individuellen Bestandteil, der bei der Verschlüsselung und bei der Entschlüsselung vorhanden sein muss. Der digitale Schlüssel ist eine Folge von Zeichen, dessen Länge in Bit angegeben wird. Je länger dieser Schlüssel ist, desto schwieriger ist es eine verschlüsselte Information zu knacken. Die bekannten Verschlüsselungsverfahren teilen sich in symmetrische, asymmetrische und hybride Verschlüsselungsverfahren auf. Weil mit asymmetrischen Verschlüsselungsverfahren verwandt, findet die Digitale Signatur hier ebenfalls Erwähnung.

Symmetrische

Verschlüsselungsverfahren

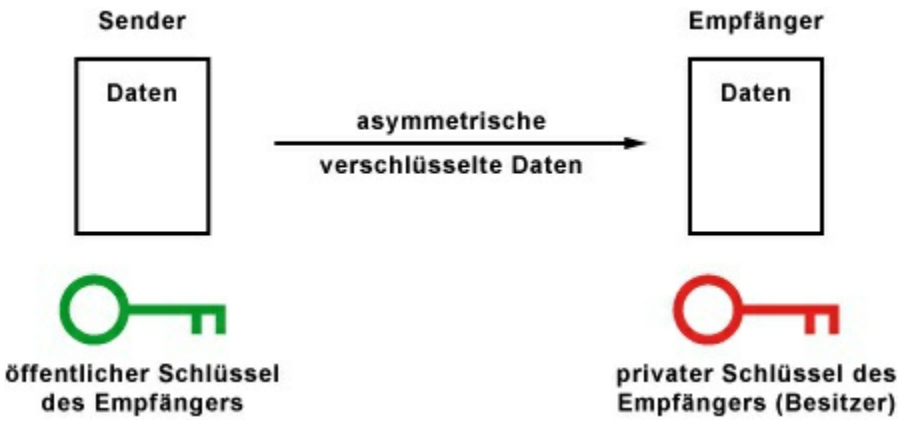
(Secret-Key-Verfahren)



Symmetrische Verschlüsselungsverfahren arbeiten mit einem einzigen Schlüssel, der bei der Ver- und Entschlüsselung vorhanden sein muss. Diese Verfahren sind schnell und bei entsprechend langen Schlüsseln bieten sie auch eine hohe Sicherheit. Der Knackpunkt liegt in der Schlüsselübergabe zwischen den Stationen. Am sichersten ist die Schlüsselübergabe, wenn sich zwei Personen persönlich treffen und den Schlüssel austauschen oder der Schlüssel einen anderen Weg geht, wie

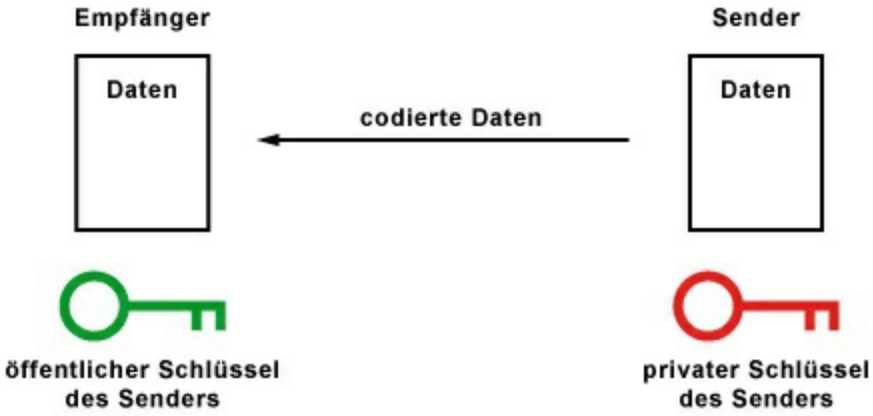
es die Daten tun. Ein Möglichkeit wäre der postalische Weg (Brief, Einschreiben mit Rückschein).

Asymmetrisches Verschlüsselungsverfahren (Public-Key-Verfahren)



Asymmetrische Verschlüsselungsverfahren arbeiten mit Schlüsselpaaren. Ein Schlüssel ist der öffentliche Schlüssel (Public Key), der andere ist der private Schlüssel (Private Key). Dieses Schlüsselpaar hängt über einen mathematischen Algorithmus eng zusammen. Daten, die mit dem öffentlichen Schlüssel verschlüsselt wurden, können nur noch mit dem

privaten Schlüssel entschlüsselt werden. Der konkrete Anwendungsfall sieht so aus: Will der Sender Daten verschlüsselt an den Empfänger senden, benötigt er den öffentlichen Schlüssel des Empfängers. Mit dem öffentlichen Schlüssel können die Daten verschlüsselt, aber nicht mehr entschlüsselt werden (Einwegverschlüsselung). Nur noch der Besitzer des privaten Schlüssels, also der richtige Empfänger kann die Daten entschlüsseln. Wichtig bei diesem Verfahren ist, dass der private Schlüssel vom Schlüsselbesitzer absolut geheim gehalten werden muss. Kommt eine fremde Person an den privaten Schlüssel



muss sich der Schlüsselbesitzer ein neues Schlüsselpaar besorgen.

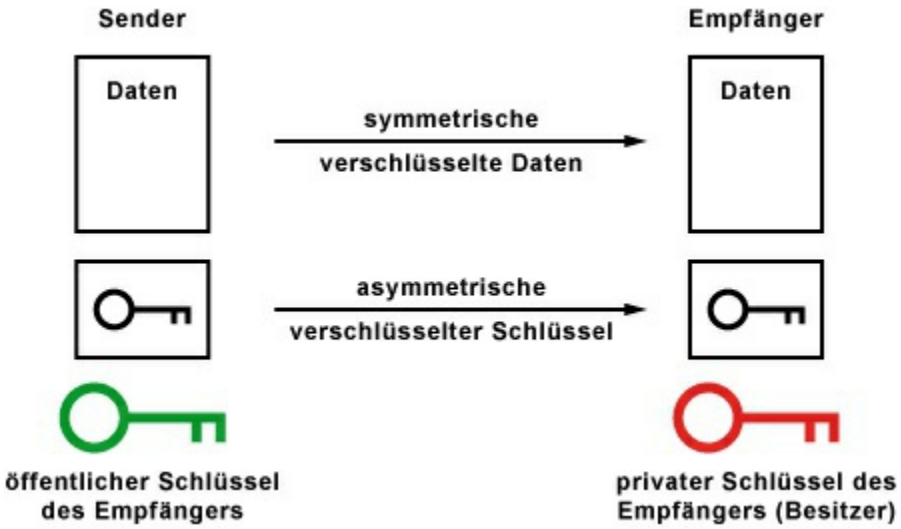
Digitale Signatur

Die Digitale Signatur ist kein Verschlüsselungsverfahren, sondern eine Codierung. Das bedeutet, die Daten sind mit Kennzeichen versehen, die durch den privaten Schlüssel hinzugefügt wurden. Mit dem öffentlichen Schlüssel kann man feststellen, ob die Daten von demjenigen sind, der den privaten Schlüssel besitzt. Die Tatsache, dass der private Schlüssel nur im Besitz des Senders ist, erlaubt die Annahme, dass Daten, die mit dem privaten Schlüssel codiert sind, tatsächlich vom Schlüsselbesitzer

stammen. Ganz ähnlich wie bei der Beglaubigung eines Dokumentes durch einen Notar. Mittels des öffentlichen Schlüssels können die codierten Daten auf ihre digitale Beglaubigung überprüft werden.

Dieses umgekehrte Public-Key-Verfahren macht man sich für die Digitale Signatur zu nutze, um festzustellen, ob die erhaltenen Daten tatsächlich vom angegebenen Sender stammen. Vorher muss der Sender die Daten mit seinem privaten Schlüssel codiert haben.

Hybride Verschlüsselungsverfahren



Hybride Verschlüsselungsverfahren arbeiten mit symmetrischen und asymmetrischen Verfahren um Daten zu verschlüsseln. Damit werden die Schwachpunkte beider Verfahren ausgeglichen.

Zunächst wird ein zufälliger, digitaler Schlüssel generiert. Mit diesem Schlüssel werden die Daten vom Sender verschlüsselt. Der Empfänger wird mit demselben Schlüssel die Daten wieder entschlüsseln. Die Verschlüsselung der Daten erfolgt also symmetrisch. Der Schlüssel wird mit einem asymmetrischen

Verschlüsselungsverfahren, also mit dem öffentlichen Schlüssel des Schlüsselpaares verschlüsselt. Die verschlüsselten Daten und Schlüssel werden dann an den Empfänger geschickt. Mit Hilfe seines privaten Schlüssels kann der Empfänger den eigentlichen Schlüssel entschlüsseln. Danach ist es ihm möglich mit dem entschlüsselten Schlüssel die eigentlichen Daten zu entschlüsseln.
Bei diesem Verschlüsselungsverfahren werden die Daten symmetrisch Verschlüsselt. Die Schlüsselübergabe erfolgt mit der asymmetrischen Verschlüsselung. Es handelt sich also um ein sichere Schlüsselübergabe. Wichtig ist jedoch, das ein wirklich zufällig Schlüssel generiert wird.

Übersicht:

Verschlüsselungsverfahren

DES - Data Encryption Standard

Triple-DES

CBC - Cipher Block Chaining

AES - Advanced Encryption

Standard

Rijndael (Algorithmus)

RC4

Public-Key-Kryptografie

Diffie-Hellmann-Verfahren

RSA-Verfahren

ECC - Elliptic Curve Cryptography

Hash-Funktionen (MD5, SHA1,

HMAC)

SSL - Secure

Socket Layer

SSL ist ein Protokoll, das der Authentifizierung und Verschlüsselung von Internetverbindungen dient. SSL schiebt sich als eigene Schicht zwischen TCP und den Protokollen der Anwendungs- und Darstellungsschicht. 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 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 Symbol in der Statusleiste eingeblendet wird oder die Adresszeile ihre Farbe ändert.

Weil SSL unterhalb der Anwendungsprotokolle sitzt, können es

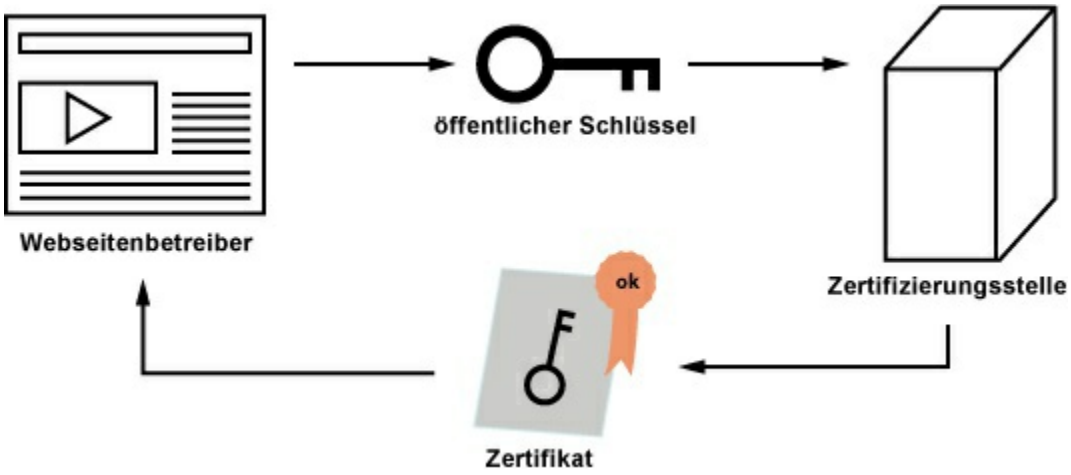
auch andere Anwendungsprotokolle zum Verschlüsseln benutzen. Dabei muss jedes Anwendungsprotokoll SSL explizit beherrschen. So wird aus HTTP (Hypertext Transfer Protocol) HTTPS (Hypertext Transfer Protocol Secure). Ebenso ist es möglich E-Mails über SSL beim POP3-Server abzurufen oder an den SMTP-Server zu übermitteln. Auch hier bekommen die Protokolle einen "Secure"-Zusatz (SMTPS, POP3S, 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.

SSL wurde ursprünglich von Netscape in den 90er Jahren für den Browser "Netscape Navigator" entwickelt. Die Weiterentwicklung von SSL wurde mit der Version 3 beendet. Die IETF hat

SSL 3.0 übernommen, ein paar kleine Änderungen vorgenommen und anschließend TLS 1.0 genannt. In der Regel arbeiten die Anwendungsprotokolle mit TLS, wenn von SSL die Rede ist. Der Grund, warum statt der Bezeichnung TLS immer noch SSL verwendet wird, liegt daran, dass sich TLS bei der Kommunikation als SSL Version 3.1 zu erkennen gibt.

Zertifizierung



Eine verschlüsselte Verbindung, wie bei SSL, bietet keinen Schutz, wenn nicht sichergestellt ist, dass der öffentliche Schlüssel von der tatsächlichen Domain kommt, mit der eine verschlüsselte

Verbindung bestehen soll. Deshalb gehören zum SSL-Protokoll ein öffentlicher und privater digitaler Schlüssel des Servers. Der öffentliche Schlüssel darf jedem bekannt und zugänglich sein. Z. B. bei einer Anfrage durch den HTTP-Client. Der private Schlüssel (Private Key) verbleibt auf dem Server und muss geheim bleiben. Nur der Server mit dem passenden privaten Schlüssel ist in der Lage die Daten zu entschlüsseln.
Um die Gültigkeit des Schlüssels zu unterstreichen, lässt sich der Webseiten-Betreiber und Domain-Inhaber ein Zertifikat ausstellen, in dem Domainname, der öffentliche Schlüssel und ein Ablaufdatum enthalten ist. Das Zertifikat wird von einer Zertifizierungsstelle, auch Certificate Authenticity (CA) genannt, ausgestellt. Die Zertifizierungsstelle signiert das

Zertifikat mit ihrem privaten Schlüssel, womit die Echtheit der Daten bestätigt sind. Im Vorfeld prüft die Zertifizierungsstelle die Informationen im Zertifikat und die Identität des Zertifikatsinhabers. Der kann zwischen drei Zertifikatstypen wählen, die einen unterschiedlichen Prüfaufwand haben und 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 wenig Euro oder sogar kostenlos bekommen kann, kommen wegen des erheblichen Prüfaufwands bei EV-Zertifikaten mehrere hundert Euro zusammen.
Allerdings kann man bei EV-Zertifikaten von einer höheren Vertrauenswürdigkeit ausgehen.
Welches Zertifikat bei einer verschlüsselten Verbindung zum Einsatz kommt, erkennt man beim Browser an der Adresszeile. Je nach Browser ist sie gelb, blau oder grün eingefärbt.
Manchmal ist eine verschlüsselte Verbindung auch nur an einem Schloss-Symbol zu erkennen.
Auch die Zertifizierungsstelle besitzt ein Zertifikat, indem sich deren öffentlicher Schlüssel befindet. Dabei handelt es sich um ein Wurzelzertifikat, das in Browsern und Betriebssystemen

hinterlegt ist und dem sie bedingungslos vertrauen. Anhand der Signatur der Zertifizierungsstelle und dem Wurzelzertifikat kann ein Browser feststellen, ob das Zertifikat einer

Domain wirklich von der angegebenen Zertifizierungsstelle ausgestellt wurde.

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 authentifiziert sich der Webserver gegenüber dem Client. Schlüssel und Zertifikat werden vom Client auf

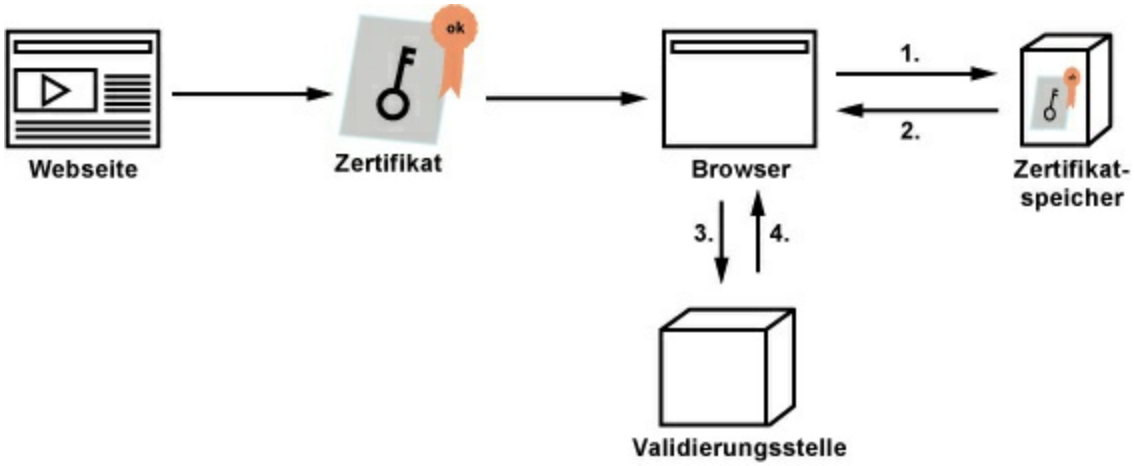
Glaubwürdigkeit überprüft. Je nach Einstellung des Clients muss der Benutzer zuerst die Glaubwürdigkeit bestätigen.
Nach erfolgreicher Authentifizierung des Servers, generiert der Browser einen symmetrischen Schlüssel, den er mit dem öffentlichen Schlüssel des Servers verschlüsselt. Den symmetrischen 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.

Ablauf der Validierung



Bei der Validierung prüft ein Browser zuerst, ob er dem Aussteller des Zertifikats vertraut. Dazu muss das entsprechende Wurzelzertifikat der Zertifizierungsstelle im Browser hinterlegt sein. Im zweiten Schritt kontaktiert der Browser die angegebene Validierungsstelle. Diese prüft, ob das Zertifikat gültig ist. Erst wenn der Browser die Gültigkeit eines Zertifikats feststellen kann, gilt die Verbindung mit dem öffentlichen Schlüssel als sicher.

Sicherheitsrisiken beim Einsatz von SSL

Wurde eine Verbindung mit SSL oder TLS aufgebaut, dann ist die Übertragung

verschlüsselt und vor Dritten geschützt.
Es ist nicht mehr möglich die
Verbindung passiv zu belauschen oder
aktiv zu manipulieren. Doch man sollte
nicht denken, dass SSL so bombensicher
ist, wie es hier dargestellt wurde.
Deshalb im folgenden, ein paar
Sicherheitsrisiken, die man im
Zusammenhang mit SSL beachten sollte.
Wenn ein privater Schlüssel gestohlen
wurde, dann muss dieser Schlüssel in
eine Blacklist (Sperrliste) aufgenommen
werden, damit die Validierungsstelle
diesen Schlüssel bei einer Abfrage als
ungültig erklären kann.
Ein weiteres Risiko entsteht, wenn es
einem Angreifer gelungen ist, die
Prüfinstanzen einer Zertifizierungsstelle
zu umgehen und Zertifikate für beliebige
Domains auszustellen. Kann sich ein
Angreifer Zugriff auf eine
Zertifizierungsstelle verschaffen und

beliebige Zertifikate erstellen, dann hilft nur noch, das Wurzelzertifikat der Zertifizierungsstelle aus Browsern und Betriebssystemen zu entfernen. Nur das stellt die nötige Sicherheit wieder her.
Leider akzeptieren manche Browser ein Zertifikat auch dann, wenn sie keine Antwort von der Validierungsstelle bekommen. Bei einer ausbleibenden Antwort könnte die Verbindung auch durch eine Man-in-the-Middle-Aktion gesteuert werden und eine offensichtlich verschlüsselte Verbindung durch eine dritte Person abgehört werden.
Um sicher zu gehen, nehmen die Browserhersteller ungültig gewordene Zertifikate in ihre Browsereigenen Blacklisten auf.

Wie sicher ist SSL?

Generell hängt die Sicherheit von Kryptographie und Verschlüsselung davon ab, dass zum einen die Verfahren

sicher sind und zweitens die Verfahren korrekt verwendet werden. Doch Krypto- und Verschlüsselungsalgorithmen korrekt zu benutzen ist nicht so einfach. Dazu braucht es Hintergrundwissen und Erfahrung. Um es sich einfacher zu machen nutzen viele Entwickler Software-Bibliotheken. Im Fall von SSL zum Beispiel JSSE, OpenSSL oder GnuTLS. Diese Bibliotheken bieten dem Programmierer eine Vielzahl von Optionen und Einstellungen, die bei einer ungünstigen Konstellation eine wirksame Verschlüsselung außer Kraft setzen können. Wenn diese Bibliotheken fehlerhaft genutzt werden ist die Verschlüsselung unwirksam.
Leider ist sind die Schnittstellen vieler Bibliotheken schlecht entwickelt und überfordern die Programmierer.
Erschwerend kommt hinzu, dass es an

vernünftigen Testmöglichkeiten für Programme fehlt, die SSL-Funktionen nutzen.

SSL ist nur so sicher, wie ein Programm die Identität der Gegenstelle, also deren Zertifikat, überprüft. Das bedeutet, dass Programme und Anwendungen mit SSL-Verschlüsselung nicht zwangsläufig sicher sind. Unterschiedliche Studien haben gezeigt, dass die Überprüfung von Zertifikaten in vielen wichtigen Programmen und Bibliotheken nicht richtig funktioniert. Das öffnet Tür und Tor für Man-in-the-Middle-Angriffe.

Das betrifft Online-Shops, Messaging-Dienste, Cloud-Dienste, Mobile-Apps, bis hin zu kritischen Geschäftsanwendungen, die sensible Kundendaten transportieren.

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 Authentisierung 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.

SSH - Secure Shell

SSH bzw. Secure Shell ist ein kryptografisches Protokoll mit dem man auf einen entfernten Rechner mittels einer gesicherten Kommunikationsverbindung 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 in 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 Netzwerkes. SSH bietet dazu eine kryptografisch gesicherte Kommunikation über das unsichere Netzwerk, eine zuverlässige

gegenseitige Authentifizierung,
Verschlüsselung des gesamten
Datenverkehrs auf Basis eines
Passworts oder Public/Private-Key-
Login-Methoden.
In den meisten Fällen ersetzt Secure
Shell Telnet, FTP und die r-Utilities.

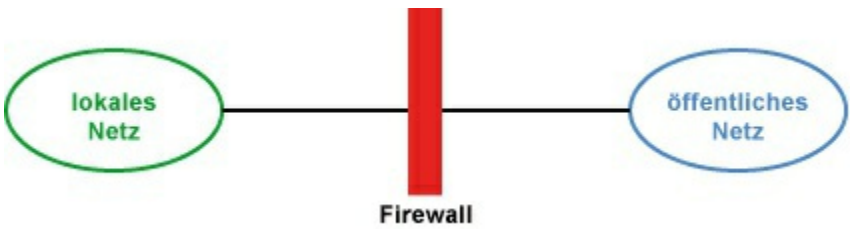
SSH 1.x und SSH 2.x

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 2.x wurde durch eine
Arbeitsgruppe der IETF erarbeitet. Es

empfiehlt sich diese Version von SSH zu verwenden. 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.

OpenSSH

OpenSSH ist eine Entwicklung des OpenBSD-Projekts und basiert auf 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. OpenSSH ist eine Implementierung von SSH für Unix/Linux. Für Windows-Betriebssysteme gibt es die Freeware putty, die eine grafische Benutzeroberfläche für SSH 1.x und SSH 2.x hat.



Firewall

Eine Firewall ist eine Schutzmaßnahme vor fremden und unberechtigten Verbindungsversuchen 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 als eine Sicherheitsstrategie zu verstehen, die

unerwünschte, unsichere und schädigende Verbindungen verhindern soll. 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.

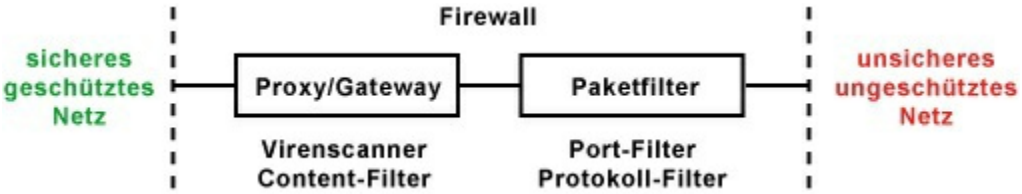
Firewall-Strategie: Alles

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

aktives Gateway (Proxy)

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!

Sicherheitsvorkehrungen?

Keine Sicherheitsvorkehrungen oder Sicherheitsmechanismen zu verwenden ist fahrlässig. Allerdings sollte man schon genau hinschauen, was einem so als Sicherheitsfunktion angeboten wird. Ein MAC-Filter, wie er in WLAN-Access-Points angeboten wird, ist als Sicherheitsfunktion bedingt tauglich. Zum einen ist der Verwaltungsaufwand groß und zweitens für einen Hacker kein wirkliches Hindernis. Jeder Netzwerk-Adapter kann mit einer anderen MAC-Adresse versehen werden.

NAT wird besonders in Produkt-nahen Beschreibungen als Sicherheitsmerkmal beschrieben. Hinter NAT steckt ein Mechanismus, der als Nebenprodukt verhindert, dass Stationen hinter dem NAT-Router von außerhalb direkt ansprechbar sind. Von außen initiierte Verbindungsversuche werden verworfen

und bekommen keinen Zugang zum lokalen Netzwerk.

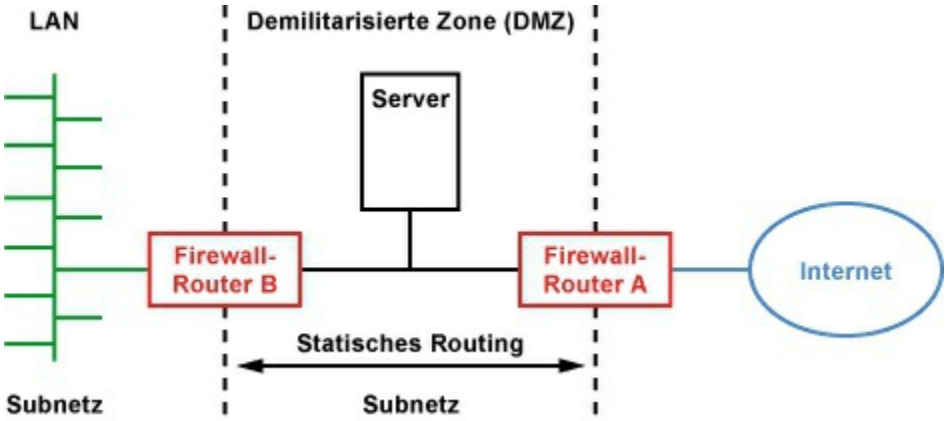
NAT als Sicherheitsmerkmal zu bezeichnen ist irreführend, weil es nicht die Aufgabe von NAT ist, die Sicherheit zu erhöhen.

Ein weiterer gut gemeinter Ratschlag ist das Blockieren von Ports. Dadurch soll verhindert werden, dass über nicht blockierte Ports irgendwelche Dienste angesprochen werden können.

Allerdings erreicht man dadurch nicht mehr Sicherheit. Protokolle sind nicht an bestimmte Ports gebunden. Sie können irgendwelche Ports verwenden.

Ziel sollte es sein, alle nicht in Gebrauch befindlichen Dienste abzuschalten. Denn dann braucht man sich um offene Ports keine Sorgen machen. Ports sperrt nur derjenige, der seine Server- und Netzwerk-Dienste nicht im Griff hat.

Trotz aller Sicherheitsmaßnahmen ist die beste Firewall die Isolation. Computer mit sensiblen oder datenschutzrechtlichen Daten sollten autark und vom jedem Netzwerk getrennt laufen.



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

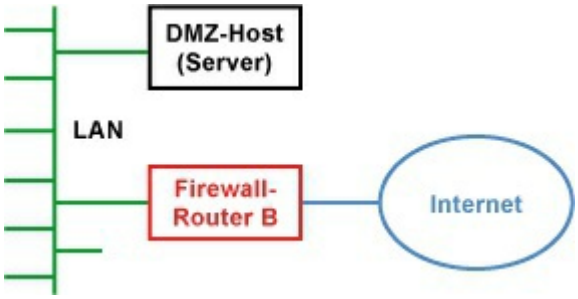
der Konfigurationsaufwand sind nicht

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 NAT-Vorgabe (Port-Forwarding) 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 Stationen 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.

SPI - Stateful Packet Inspection

SPI ist ein Firewall-Leistungsmerkmal.

Dieses Verfahren entscheidet anhand mehreren Kriterien, ob ein eingehendes Datenpaket weitergeleitet oder verworfen wird. Z. B. wird der Zielport als Kriterium verwendet. Ist in der Firewall für diesen Port kein Server angegeben, werden die Datenpakete für diesen Port verworfen. SPI überprüft auch, ob eingehende Datenpakete zu zuvor gesendeten Datenpaketen in Beziehung stehen. Also zu einer Sitzung gehören, die durch das sichere lokale Netzwerk ausgelöst wurden. Datenpakete, die sehr häufig eintreffen werden identifiziert. Liegt der Verdacht nahe, dass es sich um eine DoS-Attacke (Denial-of-Service) handelt werden diese Datenpakete automatisch verworfen.

DoS - Denial of Service

Denial of Service, kurz DoS, sind

Angriffsversuch auf einen Rechner, Server oder ein ganzes Netzwerk. In der Regel wird dabei ein Dienst, ein Server oder ein ganzes Netzwerk mit Verbindungsversuchen überflutet. Die Folge ist, dass der Dienst, der Server oder das Netzwerk nicht mehr erreichbar sind. Der Angriff ist in der Regel beabsichtigt, kann aber auch durch eine fehlerhafte Software ausgelöst werden. Große Firmen schützen ihre IT-Infrastruktur gegen DoS-Angriffe, in dem sie es entsprechend dimensionieren und Maßnahmen ergreifen, um schädliche Angriffe herauszufiltern. Einen absoluten Schutz gegen DoS-Angriffe gibt es jedoch nicht. Das Fluten von Schnittstellen mit Datenpaketen ist immer möglich.

DDoS - Distributed Denial of Service

Eine besonders böswillige Variante von

DoS-Angriffen sind Distributed Denial of Service, kurz DDoS. Dahinter stecken Programme zum Starten von DoS-Angriffen. Diese Programme enthalten Anweisungen von einem Steuerprogramm, um den Angriff auszuführen.

Über Trojaner und Würmer werden DDoS-Programme auf die Computer argloser Nutzer eingeschleust, um in Summe ein Bot-Netzwerk zu bilden, dass für DoS-Angriff missbraucht werden kann. Bei DDoS werden sehr viele Zugriffe von mehreren Rechnern auf den Zielrechner ausgeführt. Ziel ist es, das System durch Überlastung zum Absturz zu bringen, oder es zumindest unerreichbar zu machen.

Dazu startet der Angreifer über ein Netz von DDoS-verseuchten Computern eine große Anzahl von Anfragen. Zum Beispiel auf einen Webserver. Dabei

wird eine einzelne Webseite so oft aufgerufen, dass der Server komplett ausgelastet ist und keine neuen Anfragen entgegen nehmen kann. Die angegriffene Webseite ist nicht mehr erreichbar. Selbiges kann man mit jedem Service oder Dienst machen, der über das Internet erreichbar ist.

FDoS - Flooder Denial of Service

Eine weitere Variante von DoS-Angriffen sind Flooder Denial of Service, kurz FDoS. FDoS-Programme arbeiten im Gegensatz zu DDoS-Programmen eigenständig. Sie versuchen Netzwerkdienste auszuschalten. Das erreicht man in der Regel dadurch, dass man den Netzwerkdienst mit Zugriffen überflutet, der dann aufgrund der hohen Zahl an Zugriffen kollabiert. Zum Beispiel dann, wenn die Hardware-Ressourcen nicht mehr ausreichen.

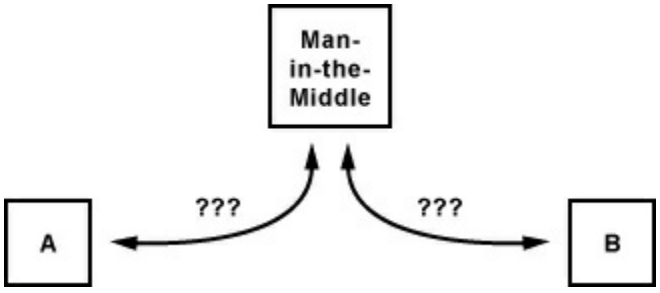
Maßnahmen gegen DoS,

DDoS und FDoS

Firewall

DPI - Deep Packet Inspection

SPI - Stateful Packet Inspection



Man-in-the-

Middle

Bei einer Man-in-the-Middle-Attacke klinkt sich der Angreifer in die Kommunikation zwischen zwei Stationen ein, die sich einander vertrauen. Dabei täuscht der Angreifer vor, dass seine Pakete von einem Rechner kommen, denen der angegriffene Rechner vertraut. Mit dieser Methode verbergen Angreifer ihre Identität und um gleichzeitig Zugriff auf die Datenpakete zu erhalten. Der Angreifer kann dabei die Pakete

auswerten und gegebenenfalls manipulieren.

Aufgrund einer falschen Identität kann der Angreifer die Stationen auch dazu bringen, vertrauliche Informationen herauszugeben. Das geht sogar soweit, dass der Angreifer Zugriff auf die Rechner der Kommunikationspartner bekommen kann.

Für Man-in-the-Middle-Attacken gibt es verschiedene Angriffspunkte. Meist ist der Vorgang sehr komplex und funktioniert deshalb in der Regel nur bei einer vorhersehbaren Kommunikation. Das allein reicht für ein erhebliches Gefahrenpotential und Sicherheitsproblem aus. Unsichere Passwörter und öffentlich bekannte Sicherheitslücken in der Software bieten einige Angriffspunkte.

IP-Spoofing

IP-Spoofing zählt zu den Man-in-the-

Middle-Angriffen. IP-Spoofing ist wegen einer systembedingten Schwäche von TCP/IP möglich. Im Prinzip geht es dabei um das Versenden von IP-Paketen mit gefälschter Quell-IP-Adresse.

ARP-Spoofing

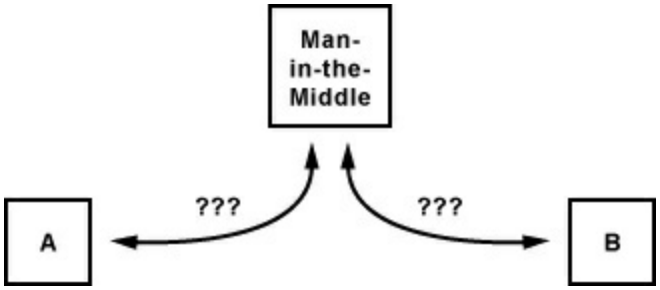
ARP-Spoofing ist eine Variante von IP-Spoofing. Nur das hierbei die systembedingten Schwächen von Ethernet ausgenutzt werden. Beim ARP-Spoofing werden ARP-Abfrage vorgetäuscht und die MAC-Adresse gefälscht, um den Datenverkehr umzuleiten und abzuhören.

Maßnahmen gegen Man-in-the-Middle

Verschlüsselung

sichere Passwörter

aktuelle Software



IP-Spoofing

IP-Spoofing zählt zu den Man-in-the-Middle-Angriffen. IP-Spoofing ist wegen einer systembedingten Schwäche von TCP/IP möglich. Im Prinzip geht es dabei um das Versenden von IP-Paketen mit gefälschter Quell-IP-Adresse.
Mit dieser Methode verbergen Angreifer ihre Identität und um gleichzeitig Zugriff auf einen geschützten Rechner zu erhalten. Dabei täuscht der Angreifer vor, dass seine Pakete von einem Rechner kommen, denen der angegriffene Rechner vertraut.

Warum IP-Spoofing

möglich ist

Der IP-Header beinhaltet eine Quell- und eine Ziel-IP-Adresse. Es gibt leider

keinerlei Mechanismen, die diese Angaben verschlüsseln oder vor Manipulation schützen. Außerdem gibt es keinen Mechanismus, mit dem man die Angaben im IP-Header auf Korrektheit prüfen kann. Das bedeutet, jedes IP-Paket kann beliebig manipuliert werden. Der Empfänger eines Datenpakets muss praktisch darauf vertrauen, dass das Paket tatsächlich von dem Absender der IP-Adresse stammt.
Kern des Problems ist die Sequenznummer, die ein TCP-Paket kennzeichnet. Befindet sich der Angreifer innerhalb des Kommunikationswegs zwischen den beiden Teilnehmern, dann kann er die nächsten Sequenznummern vorhersagen und sich in die Kommunikation zweier Stationen einklinken (Session Hijacking).
Der Grund, warum das möglich ist, ist

dass die beiden Teilnehmer sich nur am Anfang der Kommunikation gegenseitig authentifizieren. Danach gehen sie davon aus, dass sie mit der richtigen Gegenstelle kommunizieren. Tritt ein Angreifer an die Stelle eines der beiden Teilnehmer, bleibt das unbemerkt.
Damit das Eindringen in ein System per IP-Spoofing gelingt, muss das System zusätzliche Sicherheitslücken aufweisen.
Mit IP-Spoofing lässt sich also keine normale Internet-Verbindung aufbauen.
Anonymisierung ist per IP-Spoofing nicht möglich.

Non-Blind Spoofing

Hierbei muss sich der Angreifer im gleichen Subnetz befinden, wie das Opfer. Dabei macht sich der Angreifer die Tatsache zu Nutze, dass die IP-Pakete aus dem gleichen Subnetz auf alle Fälle bei ihm vorbei kommen. Anstatt sie zu verwerfen, greift er sie sich

einfach heraus.

Blind Spoofing

Beim Blind Spoofing befindet sich der Angreifer außerhalb des Subnetzes des Opfers. Diese Form des Angriffs ist deshalb um einiges aufwändiger. Diese Angriffsart ist daher eher selten.
Beim Blind Spoofing schickt der Angreifer einfach Pakete an das Opfer, um dabei aus den Empfangsbestätigungen Sequenznummer zu sammeln, um die nächsten Sequenznummern vorhersagen zu können.

SYN-Flooding

In der Regel schert sich der Angreifer bei DoS-Attacken nicht um die Einhaltung von Protokoll-Regeln. Das Opfer soll nur mit einer möglichst großen Zahl an Paketen überflutet werden. Hier wird IP-Spoofing eingesetzt, damit die eigentlich

angreifenden Rechner nicht ohne weiteres aufgespürt werden können.
Ein typischer DoS-Angriff per IP-Spoofing ist das SYN-Flooding (TCP). Hierbei sendet der Angreifer ein SYN an das Opfer. Verwendet allerdings eine gefälschte Quell-IP-Adresse (IP-Spoofing). Das ACK des Opfers kommt aber nie an. Die Verbindung beim Opfer bleibt aber trotzdem noch eine Zeit lang offen. Der Angreifer überflutet (DoS-Attacke) jetzt das Opfer mit weiteren SYN-Paketen, die alle nicht bestätigt werden können und geöffnete Verbindungen hinterlassen. Irgendwann kann das Opfer keine weiteren Verbindungen mehr annehmen und ist somit auch für andere Stationen nicht mehr erreichbar.
Diese Art von Angriffen versucht man mit einer vorgeschalteten Firewall zu erkennen und zu blocken. Die dazu

erforderliche Gegenmaßnahme ist denkbar einfach. Die Firewall überprüft die eingehenden Datenpakete, ob deren IP-Adressen aus dem internen Netz stammen. Dann muss man mit Sicherheit von einem Angriffsversuch ausgehen. Denn die internen IP-Adressen befinden sich im lokalen Netz, nicht im öffentlichen Netz.

Die umgekehrte Maßnahme, als IP-Spoofing aus dem eigenen Netz zu verhindern, ist die, nur die Pakete weiterzugeben, die mit einer Quell-IP-Adresse aus dem eigenen Netz versehen sind.

Drive-by-Angriffe

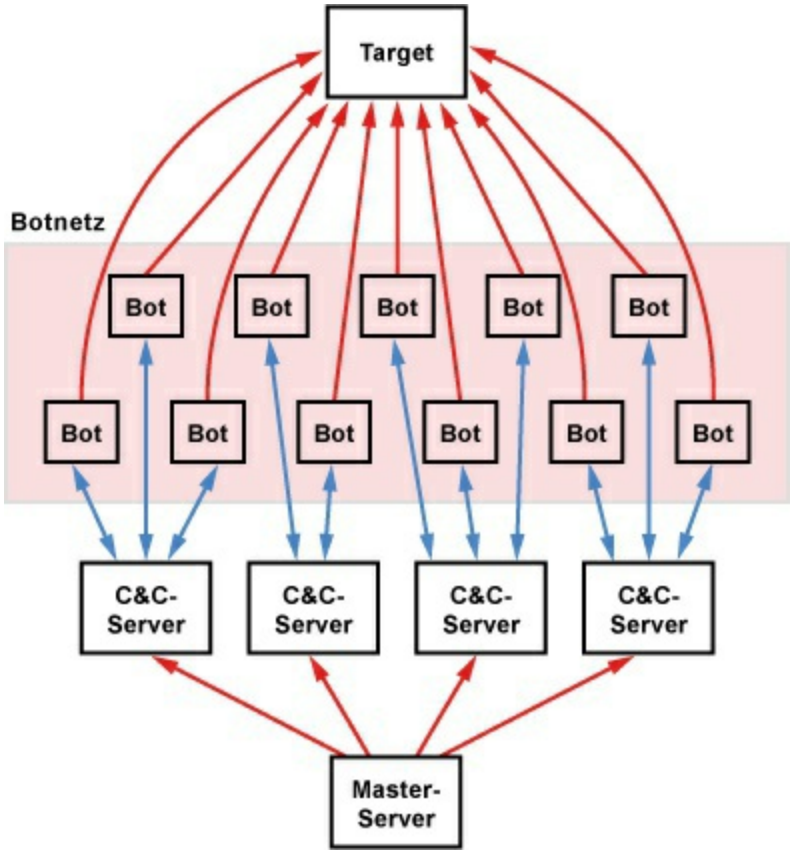
Bei Drive-by-Angriffen geht es für den Angreifer darum, sich Huckepack auf einen Dienst oder ein Anwendung draufzusatteln, um darüber auf die Computer argloser Nutzer Schadsoftware zu installieren.

Für gewöhnlich richten die Online-Gauner Webseiten ein, auf die eine Vielzahl von Nutzer freiwillig und unter Ausschaltung von Hirn und Verstand zugreifen. Zwar sind insbesondere Pornoangebote besonders erfolgreich beim Verteilen von Schadsoftware, zum Beispiel Malware, doch gewöhnliche Webseiten dürften in der Mehrzahl sein. Das bedeutet, dass längst nicht mehr nur zwielichtige Angebote zum Opfer von "Drive-by"-Attacken werden können. Auch wer sich nicht auf Rotlichtseiten herumtreibt, kann angegriffen werden. heimgesucht werden. Dazu hacken die Online-Gauner zunächst Webserver von seriösen Webseiten, von denen aus Nutzer dann auf Webseiten mit Schadcode umgeleitet werden, die dann wiederum versuchen, den Rechner des arglosen Nutzers zu infizieren.
Die Online-Gauner nutzen eine Reihe

von Methoden, um normale Webseiten nach ihren eigenen Wünschen zu verändern. Zum Beispiel mit einem speziellen JavaScript-Code, der Nutzer automatisch auf eine andere Adresse umleitet und die sich regelmäßig ändert. Dort versucht dann der Server, den Rechner des Benutzers mit Schadsoftware zu infizieren, die es dem Gauner erlaubt, diesen später fernzusteuern.

Die Infizierung durch Schadsoftware ist in der Regel auf Browser- und Windows-Sicherheitslücken abgestimmt. Hier verdeutlicht sich, wie wichtig es ist, sein System auf dem neuesten Stand zu halten. Automatische Updates von Betriebssystem und Software vermindern das Risiko sich Schadsoftware einzufangen.

Botnetze



Ein Botnetz ist ein hierarchisch aufgebautes Rechnernetzwerk mit einem Master-Server an der Spitze. Von ihm aus werden Befehle und Anweisungen über Command&Control-Server an Bots bzw. Zombies verteilt. Das ganze System bezeichnet man als Botnetz. Es eignet sich für die unterschiedlichsten Dinge. Zum Beispiel für DDoS-Attacken oder massenhaften Spam-Versand.

Der Botnetz-Betreiber ist in der Regel

nicht der Eigentümer der Zombies oder Server. Er hat sie nur gehackt und dort seine Software platziert. Auf diese Weise bleibt er als Person oder Organisation im Hintergrund.

Master-Server

Der Master-Server steht irgendwo auf der Welt. Er steuert die Command&Control-Server aus dem Hintergrund. Von hier aus werden alle Aktionen im Botnetz ausgelöst.

Command&Control-Server

Command&Control-Server stehen irgendwo auf der Welt. Häufig sind sie auch gekaperte Rechner, die über eine gute Internet-Anbindung verfügen. Von ihnen holen sich die Bots bzw. Zombies ihre Anweisungen oder laden sich weitere Schadsoftware herunter. Command&Control-Server liefern auch Trojaner aus und kontrollieren sie.

Sichere Standorte für

Command&Control-Server sind Südkorea, China und Brasilien. Dort interessiert sich niemand über die Beschwerden gegen Botnetz-Betreiber.

Bots und Zombies

Bot ist eine Abkürzung und kommt von Robot. Die Bezeichnung Bot steht für einen Rechner, auf dem ein Programm ohne Einwilligung des Besitzers vollständig automatisch läuft. Manchmal bezeichnet man Bots auch als Zombies, weil sie unkontrolliert vom eigentlichen Besitzer agieren.

Bots bzw. Zombies befinden sich überall auf der Welt. Es handelt sich dabei um Computer auf denen ein Trojaner eingeschmuggelt wurde und der im Hintergrund Spam-Mails verschickt oder DDoS-Angriffe ausführt.

Üblicherweise sind Bots in der Lage, in weiten Teile autonom zu arbeiten. Ihre Anweisungen holen sich die Bots von

den Command&Control-Servern. Die Kommunikation mit diesem Steuerserver (Command&Control-Server) ist verschleiert.

Weil es aufwendig ist, einen Trojaner auf einem Rechner einzuschleusen und das "Inventar" eines Botnetzes sehr wertvoll für den Betreiber ist, sind in vielen Bots Fallback- bzw. Backup-Maßnahmen implementiert. Das bedeutet, verliert ein Bot den Kontakt zu einem seiner fest einkodierten Command&Control-Server, beginnt er ein Notfallprogramm, bei dem er anhand eines vorgegebenen Algorithmus neue Domainnamen generiert und diese versucht, zu kontaktieren. Der Botnetz-Betreiber registriert anhand des Algorithmus die Domainnamen und sorgt für die Erreichbarkeit eines Servers.

Target

Der Target ist das Angriffsziel irgendwo auf der Welt. Beispielsweise für eine

DDoS-Attacke. Voraussetzung für eine DDoS-Attacke ist, dass sehr viele Bots bzw. Zombies online sind.

Anwendungen von Botnetzen

In der Regel werden Botnetze von modernen Kriminellen verwendet, um Geld zu verdienen. Ist der Betreiber an kriminellen Machenschaften nicht interessiert, dann vermietet er sein Botnetz.

Denial-of-Service-Angriffe

Diebstahl von Bank- und Identitätsdaten

Versand von Spam

Maßnahmen gegen Botnetz-Betreiber

Die infizierten PCs (Zombies oder Bots) verbinden sich mit einem zentralen IRC-Server. Von dort bekommen sie Anweisungen. Das kann das Versenden von Spam-Mails sein, sich an einer

DDoS-Attacke zu beteiligen oder eine neue Version nachzuladen. Durch das Sperren oder Filtern von IRC-Kommunikation ließen sich Botnetze ausschalten. Doch genau deshalb arbeiten Botnetz-Betreiber bevorzugt mit HTTP. HTTP-Aufrufe lassen sich nicht so ohne Weiteres aufspüren und filtern. Denn HTTP-Aufrufe sehen aus, wie Aufrufe normaler Webseiten.

Um dem Treiben Einhalt zu gebieten ist die Zusammenarbeit von Malware-Experten, Strafverfolgern und Providern auf internationaler Ebene erforderlich. Außerdem sind die Internetanwender in der Pflicht, zumindest die wichtigsten Sicherheitsregeln zu befolgen.

Fast-Flux-Netz

Bot-Netze lassen sich nur dann stilllegen, wenn man den zentralen Master-Server oder die Command&Control-Server abschaltet.

Um das zu erschweren arbeiten die Botnetz-Betreiber mit Arbeitsteilung und Dezentralisierung. So kommunizieren die infizierten PCs nicht direkt mit dem Command&Control-Server, sondern mit einer Zwischenstation (Proxy). Davon gibt es sehr viele. Sie bekommen aus dem Hintergrund vom Command&Control-Server ihre Anweisungen. Sucht ein Zombie seinen Master-Server, dann kontaktiert er eine Domain und bekommt mehrere IP-Adressen zurückgeliefert. Die geht er so lange durch, bis er einen Kontakt herstellen kann. Ist zwischenzeitlich ein Server abgeschaltet, steht bestimmt noch ein anderer zu Verfügung. So verteilt sich auch die Anzahl der Anfragen pro Server. Die IP-Adressen gehören jedoch nicht dem Botnetz-Betreiber, sondern ebenso infizierten PCs. Die DNS-Einträge ändern sich ständig. Im Prinzip

sind daran mehrere hundert oder tausend Stationen beteiligt. In diesem Szenario bleibt das außer Betrieb setzen der Proxies ohne Wirkung.

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 gibt es für VPN nicht. VPN steht für eine Vielzahl unterschiedlicher Techniken. So wird manche Technik, Protokoll oder Produkt zu VPN zugeordnet, obwohl keinerlei Verschlüsselung oder Authentifizierung zum Einsatz kommt. Beides ist allerdings Voraussetzung für ein VPN.

VPN - Virtual Private Network

Authentizität Vertraulichkeit Integrität

VPNs müssen Sicherheit der Authentizität, Vertraulichkeit und Integrität sicherstellen. 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 eine angemessene Sicherheit der Daten, die darüber übertragen werden.

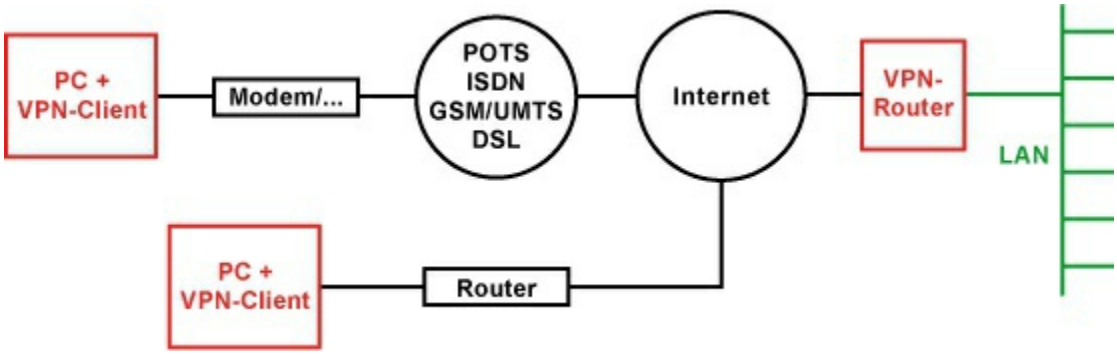
VPN-Typen

Remote-Access-VPN

Branch-Office-VPN / Site-to-Site-VPN / LAN-to-LAN-VPN

Extranet-VPN

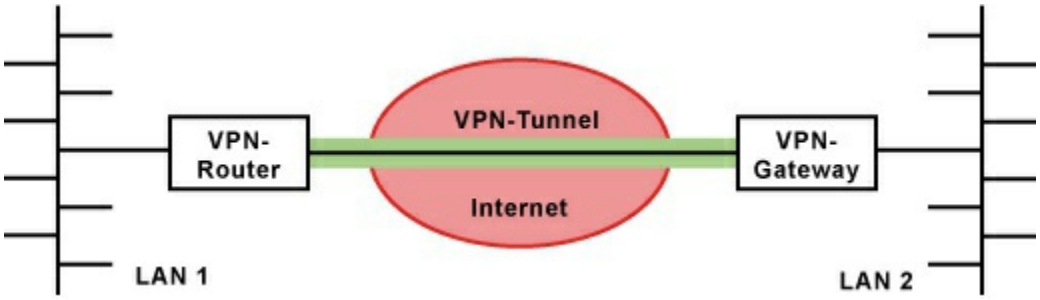
Remote-Access-VPN



Remote-Access ist 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. Die VPN-

Technik stellt eine logische Verbindung zum lokalen Netzwerk über das öffentliche Netzwerk her. Im Vordergrund steht ein möglichst geringer, technischer und finanzieller Aufwand für einen sicheren Zugriff auf das Unternehmensnetzwerk.
Hierbei ist zwangsläufig ein VPN-Client auf dem Computer des externen Mitarbeiters zu installieren, wenn diese Software nicht bereits im Betriebssystem verankert ist.

Branch-Office-VPN / Site-to-Site-VPN / LAN-to-LAN-VPN



Branch-Office-VPN, Site-to-Site-VPN oder LAN-to-LAN-VPN sind Anwendungs-Szenarien, um

Außenstellen oder Niederlassungen (Filialen) zu einem dynamischen, virtuellen Firmennetzwerk über das öffentliche 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 sehr schnell hohe Kosten durch relativ hohe Verbindungsgebühren zusammen. Je nach Anzahl, Entfernung, Bandbreite und Datenmenge, kommen sehr schnell hohe Kosten zusammen.

Da jedes Netzwerk in der Regel auch eine Verbindung zum Internet hat, bietet sich diese Verbindung zur Zusammenschaltung von zwei oder mehr Netzwerken mit VPN-Technik an (LAN-

to-LAN-Kopplung). Bei VPNs über das Internet entstehen nur die Kosten, die für den Internet Service Provider zu bezahlen sind.

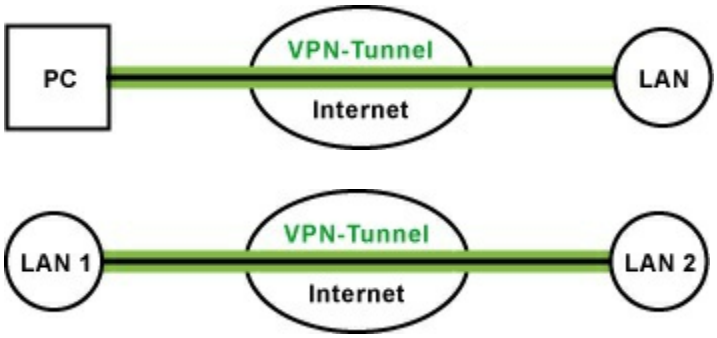
Virtuelle private Netze benutzen das Internet als Weitverkehrsnetz. Das Internet wird so zur Konkurrenz zu klassischen WAN-Diensten der Netzbetreiber. VPN-Technik löst zunehmend leitungsgebundene WAN- und Remote-Access-Lösungen ab. VPNs lassen sich über das Internet billiger und flexibler betreiben.

Extranet-VPN

Während Branch-Office-VPNs nur die verteilten Standorte einer Firma verbinden, ist ein Extranet-VPN ein virtuelles Netzwerk, das die Netzwerke unterschiedlicher Firmen miteinander verbindet. In der Regel geht es darum die Intranets fremder Unternehmen zusammenzuschließen. Zum Beispiel

Geschäftspartner, Lieferanten und Support-leistende Unternehmen. Dabei gewährt man dem externen Unternehmen Zugriff auf Teilbereiche des Unternehmensnetzwerks. Die Zugriffsbeschränkung erfolgt mittels einer Firewall. Extranet-VPNs ermöglichen eine sichere Kommunikation bzw. einen sicheren Datenaustausch zwischen den beteiligten Unternehmen.

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 die Station, die für die Einhaltung von Authentizität, Vertraulichkeit und Integrität zuständig ist.

Ein VPN-Endpunkt kann ein Router, Gateway oder Software-Client sein.

VPN-Router / VPN-Gateway

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 werden. Diese VPN-Server dienen dann als VPN-Endpunkte. Ein VPN-Server ist eher selten nötig. VPN-Gateway-Funktionen finden sich immer öfter auch in normalen 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

OpenVPN

Hamachi

Systemanforderungen

Sicherheit

Datenvertraulichkeit

Schlüsselmanagement

Paketauthentifizierung

Datenintegrität

Benutzerauthentifizierung

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.

Eigenes VPN aufbauen oder Outsourcing?

Bei der Planung eines VPN kommt man nicht herum, heute schon an morgen zu denken. Doch langfristige Aussagen sind immer schwierig. Die Rahmenbedingungen sind ständigen Änderungen unterworfen. Zum Beispiel die Zahl der Benutzer, die benötigte Bandbreite, Qualitätsmerkmale, rechtliche Aspekte, neue Geschäftsfelder und Akquisitionen, an die man heute noch nicht denkt. Am Anfang groß zu denken, aber klein und bedarfsgerecht zu

starten, ist deshalb eine gute Strategie.
Grundsätzlich ist auf die Offenheit des Systems zu achten. Zum Beispiel auf die Einhaltung von Standards. Das erleichtert die Integration in existierende Netze. Der Sicherheitsstandard auf IP-Ebene heißt IPsec. Virtuelle, private Netze sind aber nicht auf IP beschränkt, obwohl IP-VPNs heute vorherrschend sind.
Ein eigenes VPN aufzubauen bedeutet ein eigenes VPN-Gateway inklusive Access-Router zu betreiben. Hierbei entsteht ein relativ hoher Aufwand, weil man sich um alles selber kümmern muss. Die Management-Kosten werden in der Regel unterschätzt. Dabei geht es nicht nur um Geld. Viel vergeudete Zeit durch selbst verursachte Fehler, inkompatible Komponenten und fehlendes Know-how treiben den Frustfaktor nach oben.
Obwohl man mit standardisierten

Protokollen und Einrichtungen arbeitet, ist vieles so flexibel konfigurierbar, dass unter Umständen eine Zusammenarbeit unterschiedlich konfigurierter Geräte nicht zustande kommt. Zusatzkosten durch nachträgliches Eliminieren von Fehlerquelle sollte man nicht unterschätzen. So ist die Integration einer VPN-Technik häufig auch mit IP-Adressänderungen gekoppelt. Über ein externes VPN eines Dienstleisters spart man sich die Probleme häufig, weil der für die notwendige Adressumsetzung sorgen kann.

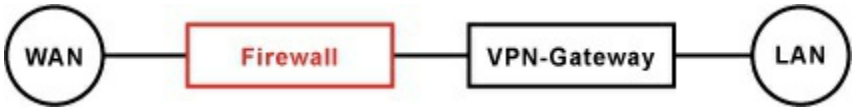
Eventuell ist die Rundumsorglos-Lösung eines Fernwartungsspezialisten für den Anfang die beste Lösung. Der Einstieg gelingt hier auf der Know-how-Seite relativ schmerzfrei. Hierbei muss man berücksichtigen, dass man sich von den Diensten eines Service-Providers je

nach Outsourcing-Weite abhängig macht und wenig Einfluss hat. Es macht durchaus Sinn vor dem Outsourcing eine Exit-Strategie für den Betrieb eines eigenen Gateways in der Schublade zu haben.

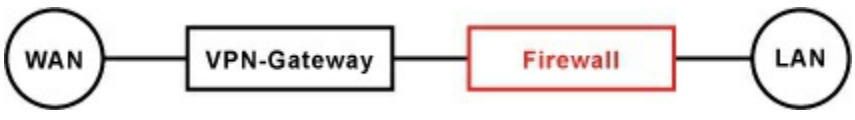
VPN und Firewall, eine unheimliche Begegnung!

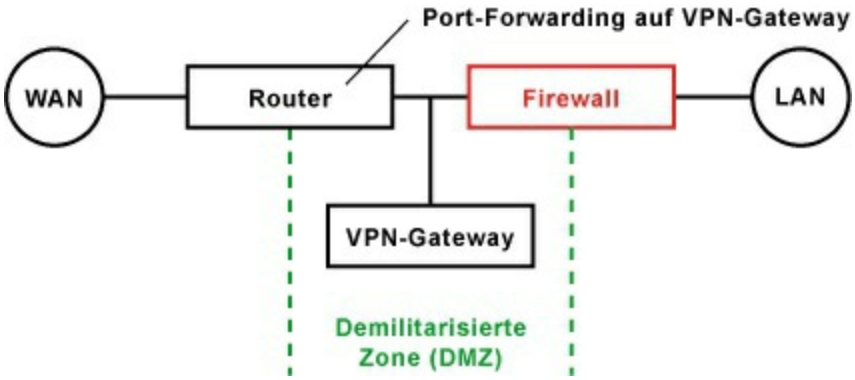
VPN im Zusammenhang mit einer Firewall führt häufig zu ungeahnten Problemen. In der Regel sollte eine Firewall gekapselten Datenverkehr verhindern. Denn der gekapselte Datenverkehr könnte unberechtigte und unsichere Daten enthalten. Deshalb lässt man in der Regel eine Tür im Sicherheitskonzept geöffnet, wenn man ein VPN betreibt.

Beim Aufbau eines VPNs ist die Platzierung des VPN-Endpunktes,



üblicherweise ein VPN-Router oder VPN-Gateway, eine wichtige Entscheidung. Es steht dabei die Frage im Raum, ob das VPN-Gateway vor oder hinter der Firewall sitzen soll. Eigentlich soll eine Firewall vor ungewollten Zugriffen aus dem Netz schützen. Wenn nun das VPN-Gateway hinter der Firewall sitzt, dann ist die Firewall nicht in der Lage in die verschlüsselten Pakete hineinzusehen. Die verschlüsselten IP-Pakete (mit IPsec und IKE) werden auf Port 500 an das VPN-Gateway durchgelassen. Ein VPN-Teilnehmer könnte auf diese Weise unkontrolliert das Netzwerk angreifen





oder ungewollte Daten ins Netzwerk einschmuggeln.

Ein bessere Lösung ist, das VPN-Gateway vor die Firewall zu setzen und alle verschlüsselten Datenpakete zu entschlüsselt und erst danach die Prüfung auf ungewollte Verbindungen zu prüfen

Die beste Lösung ist jedoch, das VPN-Gateway oder den VPN-Server in eine demilitarisierte Zone (DMZ), zwischen Netzzugangsrouter und Firewall, zu setzen. Auf diese Weise kann der entschlüsselte Datenverkehr in einer zweiten Filterstufe durch die Firewall nochmals überprüft werden.

Wer Sicherheits- und

Verbindungsprobleme vermeiden will, der wird in der Regel einen Router mit integrierter Firewall einsetzen, der gleichzeitig als Endpunkt einer VPN-Verbindung arbeitet.

Problem: Fragmentierte IP-Pakete

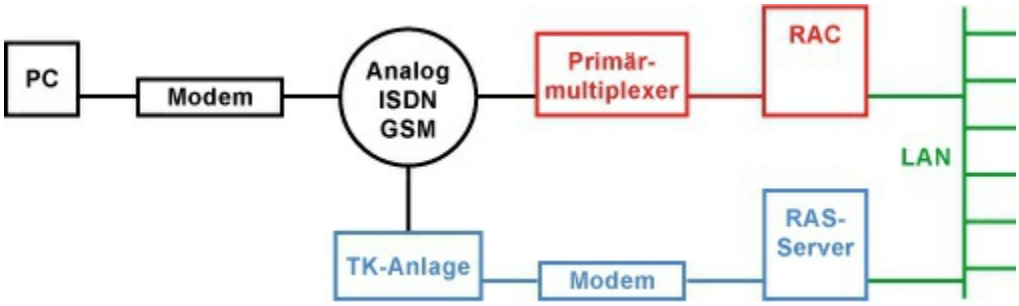
Gelegentlich kommt es vor, dass VPN-Verbindungen hergestellt werden können, aber keine Datenübertragung möglich ist. In der Regel liegt es daran, dass die Firewall auf der Gegenseite aus Sicherheitsgründen fragmentierte Datenpakete verwirft. Das ist dann der Fall, wenn IP-Pakete auf mehrere VPN-Pakete verteilt werden. In diesem Fall muss man in der betreffenden Firewall diese Funktion abschalten (drop fragmented packets).

RAS - Remote Access Service

Remote Access Service ist ein Dienst

für den Zugriff auf einen Computer oder ein Netzwerk aus der Ferne. In der Regel findet eine Einwahl über eine Wählleitung via analogem Modem oder ISDN statt.

Das analoge, wie auch das ISDN-Wählnetz haben den Nachteil, dass die Bandbreite auf wenige kByte beschränkt sind. Analog ist mit maximal 56 kBit/s (7 kByte/s) und ISDN mit 64 kBit/s (8 kByte/s) bzw. 128 kBit/s (16 kByte/s) möglich. Auf Dauer und bei weit



entfernten Stationen kann das teuer werden. Denn Wählverbindungen werden in der Regel minutenweise abgerechnet.

VPN-Technik (Remote-Access-VPN) löst zunehmend leitungsgebundene

WAN- und Remote-Access-Lösungen ab.

RAS-Architektur

Ein klassischer Remote Access Service besteht aus einem System, dass am öffentlichen Telefonnetz angeschlossen ist. Es wird als Remote Access Concentrator (RAC) bezeichnet. Der RAC ist mit dem Telefonnetz über einen oder mehr Primärmultiplexanschlüsse verbunden. Ein Primärmultiplexanschluss hat eine Bandbreite von 2,048 MBit/s oder 30 Nutzdatenkanäle mit jeweils 64 kBit/s. Die Anzahl der Einwahlports ist praktisch nur in 30er Schritten skalierbar.

Beim Primärmultiplexer kommen die Einwahlen über das Telefon- und Mobilfunknetz an. Das können ISDN-Verbindungen oder Anrufe von analogen Modems und GSM-Modems sein.

Im einfachsten Fall ist der RAC ein RAS-Server, der über mehreren Modems oder ISDN-Karten an einer Telefonanlage angeschlossen ist.
Nach der Einwahl kann neben den Protokollen TCP/IP auch IPX/SPX oder NetBEUI genutzt werden, um z. B. die Datei- und Druckerfreigabe im entfernten Netzwerk zu nutzen. In der Regel werden folgende Protokolle unterstützt:

V.34

V.90/V.92

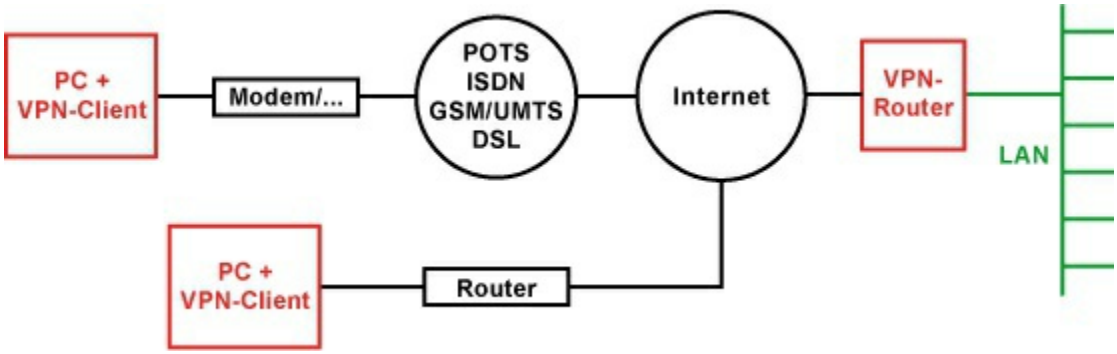
V.120 (asynchrones ISDN)

V.110 (Mobilfunk)

Die Unterstützung aller möglichen Modemprotokolle, Telefonsignalisierung und Übertragungssysteme macht RACs technisch sehr komplex und in der Regel sehr teuer.
RAS ist sehr leicht einzurichten. Jedoch darf der Sicherheitsgedanke keine große

Rolle spielen. Die Authentifizierung wird über einfache Benutzerzugänge mit Benutzername und Passwort erreicht. Die Einwahlnummer für den RAS-Server sollte nur den Personen bekannt sein, die den RAS-Zugang benützen müssen.

Remote-Access-VPN



Die Weiterentwicklung von RAS ist Remote-Access-VPN. VPN bietet Verfahren und Protokolle, um sich in ein entferntes Netzwerk einzuwählen. Hier muss sich der User zuerst ins Internet einwählen. Das hat den Vorteil, dass es überhaupt keine Rolle spielt, auf welche Weise der Zugang erfolgt. Egal ob analoges Modem, ISDN, DSL, TV-

Kabel, Mobilfunk oder WLAN-Hotspots.

Als VPN-Gegenstellen dient ein Software-Client und ein VPN-Gateway bzw. VPN-Router der am Internet angebunden ist. Einen RAC, wie bei RAS kann man sich sparen.

Um Verbindungsproblemen im Bereich Remote-Access aus dem Weg zu gehen, hat sich dort eine Alternative zu IPsec, PPTP und L2TP herauskristallisiert.

SSL-VPN mit einer TCP-Verbindung, die durch jede Firewall hindurch kommt.

VPN-Verfahren, die nur einen Port öffnen, wie zum Beispiel OpenVPN oder SSL-VPN, sind in Verbindung mit einer Firewall grundsätzlich unproblematisch.

PPP - Point-to-Point Protocol

PPP hat die Aufgabe, Punkt-zu-Punkt-Verbindungen zu initialisieren, aufrecht zu erhalten und auch wieder zu beenden.

PPP ist für die Authentisierung, die Aushandlung der Paketgröße, die Vergabe von IP-Adressen und die Verschlüsselung der Daten zuständig. Prinzipiell kann PPP beliebige Protokolle aus höheren Schichten, wie IP, IPX, NetBIOS oder AppleTalk übertragen. Bei der Einwahl ins Internet werden aber nur IP-Pakete weitergeleitet. Wenn man andere Protokolle in ein anderes Netzwerk transportieren will, dann benötigt man PPTP, das PPP-Pakete über GRE in IP-Pakete verpackt.

Dienste / Protokolle / Schicht

Anwendungen

Vermittlung

LCP

IP

IPCP

Sicherung

PPP

Bitübertragung Übertragungsverfahren

Typischerweise arbeitet das Point-to-Point Protocol (PPP) auf der Schicht 2 des OSI-Schichtenmodells und wurde für die Übertragung von Schicht-3-Protokollen über eine Punkt-zu-Punkt-Verbindung entwickelt. Typische Punkt-zu-Punkt-Verbindungen sind Verbindungen in leitungsvermittelnde Netze.

Wählverbindungen über das analoge Telefonnetz (mit Analog-Modem)

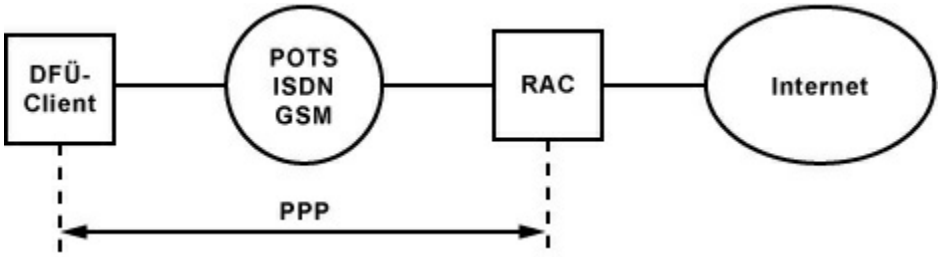
Wählverbindungen über GSM (Mobilfunk)

Wähl- oder Festverbindungen über ISDN

serielle Verbindungen

ATM-Verbindungen (PPP over Ethernet bei DSL)

PPP-Architektur



Die typische PPP-Verbindung entspricht einer RAS-Verbindung. Ein DFÜ-Client wählt sich über das öffentliche Telefonnetz in einen Remote Access Concentrator (RAC) ein und erhält auf diese Weise eine Verbindung zum Internet. PPP sorgt in diesem Szenario dafür, dass die IP-Datenpakete über die Wählverbindung übertragen werden.

Wie funktioniert PPP?

Das PPP-Protokoll sieht eine Methode vor, die Datenpakete verschiedener anderer Protokolle einzukapseln und über eine physikalische Verbindung zu übertragen. Man spricht in diesem Zusammenhang auch von Tunneling.
Die Verbindung wird mit dem Link Control Protocol (LCP) aufgebaut,

konfiguriert, getestet und auch wieder abgebaut. Außerdem enthält das PPP-Protokoll mehrere Network Control Protocols (NCPs), z. B. IPCP, die Schicht-3-Protokolle über eine Punkt-zu-Punkt-Verbindung aufbauen und konfigurieren können.

PPP-Rahmen/-Frame

Vor PPP wurden Punkt-zu-Punkt-Verbindungen mit HDLC (High-Level Data Link Control) betrieben. Mit PPP waren dann erstmals Punkt-zu-Punkt-Verbindungen zwischen Gegenstellen unterschiedlicher Hersteller möglich.
PPP ist in jedem Betriebssystem implementiert.
PPP benutzt die Rahmenstruktur von HDLC. Ansonsten haben beide Protokolle nichts gemeinsam.

LCP - Link Control

Protocol

Beim Aufbau der Punkt-zu-Punkt-Verbindung werden LCP-Konfigurationspakete zwischen den zwei Systemen ausgetauscht. Hier wird bereits festgelegt, welche Protokolle für die Authentisierung, Datenkompression und Netzwerk-Protokolle verwendet werden. Die Qualität der Verbindung wird geprüft und bei Bedarf erfolgt eine Authentisierung zwischen den Gegenstellen.

Authentisierung

Authentisierung bedeutet, die Identität zu überprüfen. 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.

PAP - Password Authentication Protocol

CHAP - Challenge Handshake Authentication Protocol

MS-CHAP - Microsoft CHAP

CCP

Mit CCP handeln die Gegenstellen ein Datenkompressionsverfahren aus. Es gibt zwar einige Kompressionsverfahren, doch nicht alle werden von jeder Gegenstelle unterstützt.

STAC/LZS

MPPC - Microsoft Point-to-Point-Compression

NCP - Network Control Protocol

Für jedes Schicht-3-Protokoll, das in PPP übertragen werden kann, gibt es ein Kontrollprotokoll, das als Network Control Protocol (NCP) bezeichnet wird. Es enthält Kontrollfunktionen und

dient zur Konfiguration des zu übertragenden Protokolls.

IPCP für das Internet Protocol (IP)

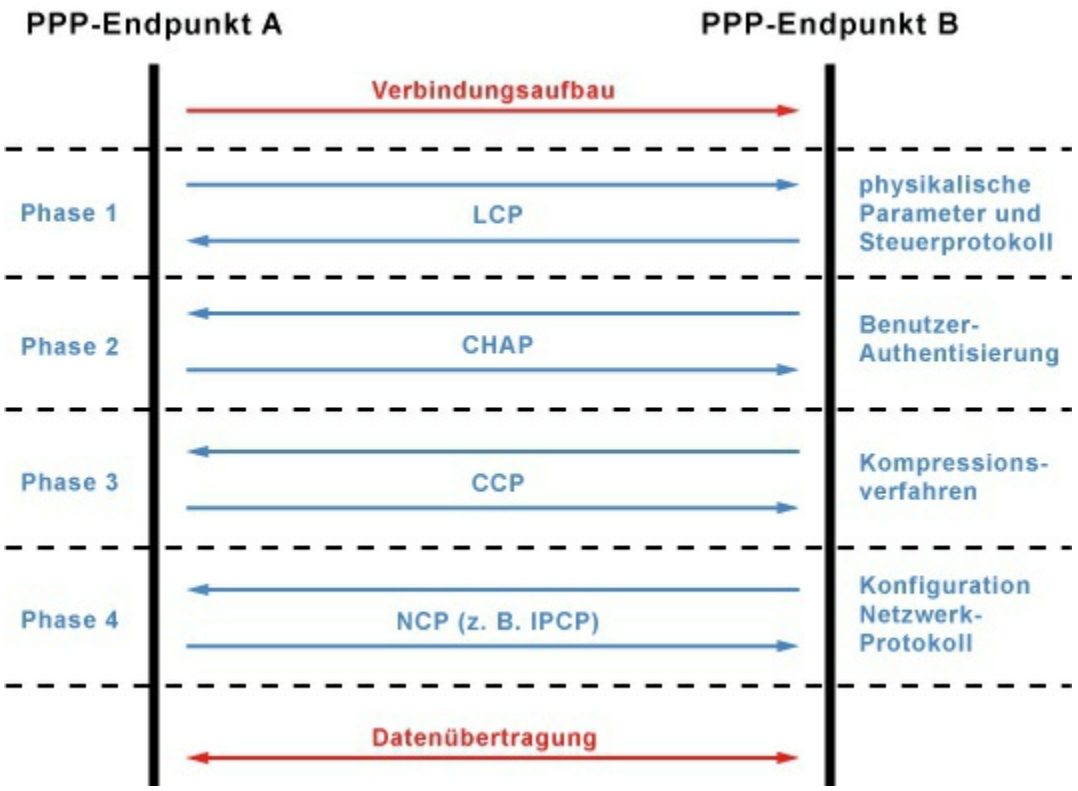
IPXCP für IPX

IPCP - IP Control Protocol

Wird das Internet Protocol (IP) über PPP getunnelt, dient das IP Control Protocol (IPCP) als NCP. Ein konkreter Anwendungsfall ist der Internet-Zugang per Analog-Modem oder ISDN. Nach dem Verbindungsaufbau wird der einwählenden Station über ein IPCP-Paket eine IP-Adresse, die Subnetzmaske, der DNS-Server und das Standard-Gateway zugewiesen.

Bei IPCP handelt es sich demnach um eine Art DHCP, speziell für Wählleitungen bzw. Punkt-zu-Punkt-Verbindungen.

PPP-Verbindungsaufbau



Der Ablauf des PPP-Verbindungsaufbaus setzt voraus, dass vorher eine physikalische Verbindung hergestellt wurde. Zum Beispiel eine geschaltete Festverbindung oder eine durch Einwahl hergestellte Wählverbindung über das öffentliche Telefonnetz. Erst danach werden die Parameter für die PPP-Verbindung in mehreren Phasen ausgehandelt.

1. Zuerst werden mit LCP die physikalischen Parameter und

Steuerprotokolle ausgehandelt.

2. Danach erfolgt die Authentisierung, beispielsweise mit CHAP oder MS-CHAP. Wenn sie erfolgreich war, dann werden weitere Protokolle ausgeführt. Wenn nicht, dann wird die Verbindung an dieser Stelle beendet.

3. Im Anschluss konfiguriert CCP das Datenkompressionsverfahren. Können sich die Gegenstellen nicht einigen, dann werden die Daten unkomprimiert übertragen.

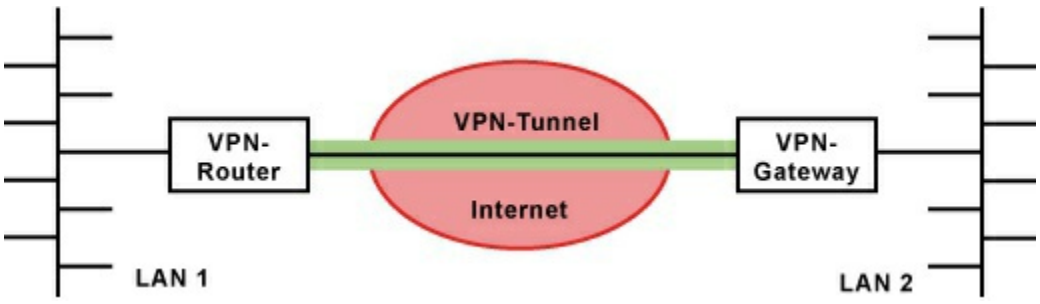
4. Dann als letzter Schritt wird IPCP ausgeführt, dass die beiden Gegenstellen für die Übertragung von IP-Paketen über die PPP-Verbindung konfiguriert. Während dieser Verbindung können mehrere Netzwerkprotokoll wie IPX oder NetBEUI übertragen werden.

Sofern eine physikalische Verbindung

möglich ist und die Authentisierung erfolgreich war, kommt in der Regel immer eine PPP-Verbindung zustande. Hier zeigt sich PPP sehr flexibel und robust.

Tunneling-Protokolle (VPN)

Das Internet hat den Nachteil, dass dessen Infrastruktur im Detail nicht bekannt ist und der Weg zwischen zwei Kommunikationspartnern nicht nachvollziehbar, vorhersagbar und kontrollierbar ist. So ist es an jedem Knoten, den ein Datenpaket überquert, möglich, dass es abgehört, verändert oder gelöscht wird. Die Daten werden also ungesichert über das Internet übertragen.



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. Tunneling ist die Basis eines jeden VPNs. Tunneling erlaubt es, Pakete eines Netzwerkprotokolls in die Pakete eines anderen Netzwerkprotokolls einzukapseln. Beim Tunneling werden die Pakete also durch die Einkapselung von anderen Paketen getrennt.
Das technische Prinzip einer VPN-Verbindung ist in der Regel immer gleich. Egal welches Protokoll. Am

Startpunkt des Tunnels werden die Pakete eingekapselt. Am Endpunkt werden die Pakete wieder entkapselt. Dabei wird jedes Datenpaket verschlüsselt. Der Inhalt des ursprünglichen Pakets können andere nicht mehr sehen.

Ein andere sinnvolle Anwendung, ist das Verstecken von privaten Netzwerkadressen, in dem man IP-Pakete in IP-Paketen tunnelt. Auf diese Weise werden Netzwerke über das Internet miteinander verbunden. Die IP-Pakete mit privaten Adressen werden in IP-Pakete mit der öffentlichen Adresse verpackt.

Tunneling im OSI-Schichtenmodell

Für das Tunneling gibt es zwei Ansätze. Im ersten Ansatz wird auf der Schicht 3 des OSI-Schichtenmodells das Tunneling aufgebaut. Dabei wird zur

Adressierung der Schicht bzw. des Datenpakets das Internet Protocol (IP) verwendet. Man spricht dann vom IP-in-IP-Tunneling. In der Regel wird IPsec für diese Lösung verwendet.

Ein anderer Ansatz greift direkt auf der Schicht 2 des OSI-Schichtenmodells ein. Hier wird das Datenpaket der Schicht 3 verschlüsselt und dann mit der physikalischen Adresse adressiert. In der Regel werden PPTP oder L2TP für diese Lösung verwendet.

Standardisierte Tunneling-Protokolle

PPTP - Point-to-Point Tunneling Protocol

L2F - Layer 2 Forwarding (Cisco)

PPTP und L2F sind keine echten Standards. Sie haben nur einen informellen Status.

L2TP - Layer-2-Tunneling-Protocol (Microsoft-Umgebungen)

IPsec (im Tunnelmodus)

MPLS - Multi-Protocol Label Switching

MPLS ist eigentlich kein Tunneling-Protokoll. Allerdings kann man damit Schicht-2-VPNs aufbauen

IPsec als Tunneling-Protokoll zu bezeichnen ist falsch. Es ist im allgemeinen Sinne ein Sicherheitsprotokoll, das auch Tunneling beherrscht und im Regelfall auch dafür eingesetzt wird.

Propritäre Tunneling-Protokolle

Altavista Tunnel

Bay Dail VPN Service (Bay-DVS)

Ascend Tunnel Management Protocol (ATMP)

L2F - Layer 2 Forwarding

L2F ist mit L2TP verwandt und wurde von Cisco als Software-Modul für RAC (Remote Access Concentrator) und

Router entwickelt. Es handelt sich dabei nicht um eine Client-Implementierung, wie zum Beispiel bei PPTP oder L2TP. Der Benutzer kommt mit L2F nicht in Berührung.

L2F bietet keine Verschlüsselung und auch keine starke Authentisierung. L2F kann lediglich verschiedene Netzwerkprotokolle tunneln. Zwei L2TP-Server dienen als Endpunkt für einen L2F-Tunnel.

Übersicht: Aktuelle Tunneling-Protokolle

Die Angabe Ja und Nein sind nicht als Wertungen, sondern Eigenschaften zu verstehen. In Abhängigkeit bestimmter Eigenschaften eignet sich ein Tunneling-Protokoll für die eine oder andere Anwendung.

IPsec

L2TP

Schicht Schicht

OSI-Schicht

3

2

Standard

Ja

Ja

Paketauthentifizierung

Ja

Nein

Benutzerauthentifizierung Ja

Ja

Datenverschlüsselung

Ja

Nein

Schlüsselmanagement

Ja

Nein

Quality of Service

Ja

Nein

IP-Tunneling

Ja

Ja

IPX-Tunneling

Nein

Ja

Hauptanwendung

End-

Provider

to-End

PPTP - Point-to-

Point Tunneling

Protocol

PPTP ist ein VPN-Tunneling-Verfahren für Remote-Access-Verbindungen. Es baut auf den Remote Access Server für Microsoft Windows NT inklusive der Authentisierung auf.

PPTP wurde 1996 von mehreren Unternehmen entwickelt, die sich zum PPTP-Forum zusammengeschlossen haben. Unter anderem war auch Microsoft an der Entwicklung von PPTP beteiligt. PPTP kommt hauptsächlich in

Microsoft-Betriebssystemen zum Einsatz. Daher auch die häufige Nennung im Zusammenhang mit Microsoft. Ein PPTP-Client ist nicht nur in Windows, sondern auch in Linux und MacOS integriert.

PPTP ist dadurch gekennzeichnet, dass es ausschließlich für den Transfer von IP, IPX und NetBEUI über IP geeignet ist. Außerdem gilt die Verschlüsselung von PPTP als nicht sicher genug. Aus diesen und weiteren Gründen hat sich Microsoft von PPTP verabschiedet. Seit Windows 2000 werden verschiedene Tunneling-Protokolle angeboten. Für eine sichere Installation wird L2TP over IPsec empfohlen. L2TP weist gewisse Ähnlichkeiten zu PPTP auf und transportiert Protokolle höherer Schichten. Allerdings bietet L2TP keine Verschlüsselung an. Zur Verschlüsselung der Daten muss deshalb auf IPsec

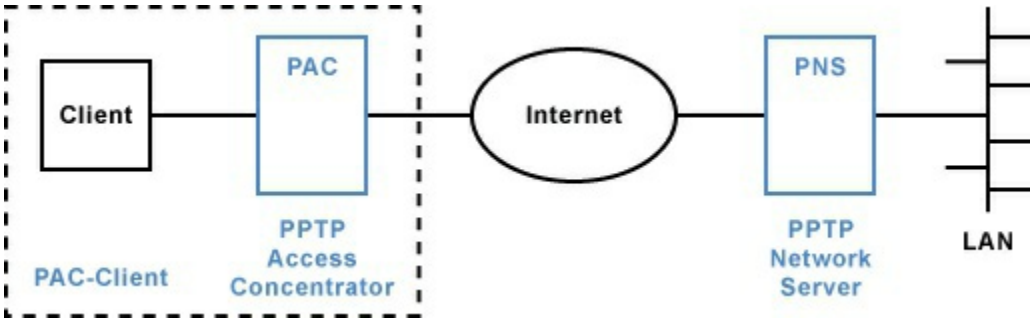
zurückgegriffen werden, das auch die Authentisierung übernimmt.

Trotz L2TP, IPsec und wegen der weiten Verbreitung von Windows-Betriebssystemen spielt PPTP beim Aufbau von VPNs in reinen Microsoft-Netzwerken immer noch eine Rolle.

PPTP kommt noch häufig als VPN-Technik zum Einsatz. Es ist auf fast allen Endgeräten verfügbar und einfach einzurichten. Es gilt als nicht besonders sicher. Das liegt weniger an PPTP, sondern am Anmeldevorgang mit MS-CHAPv2. Microsoft selber warnt vor VPN-Zugängen, die MS-CHAPv2 (insbesondere PPTP-Verbindungen) nutzen. Sie lassen sich mit vergleichsweise geringem Aufwand knacken. Eine Lösung wäre, die MS-CHAP-Authentifizierung in einen separat verschlüsselten Tunnel, zum Beispiel Protected Extensible Authentication

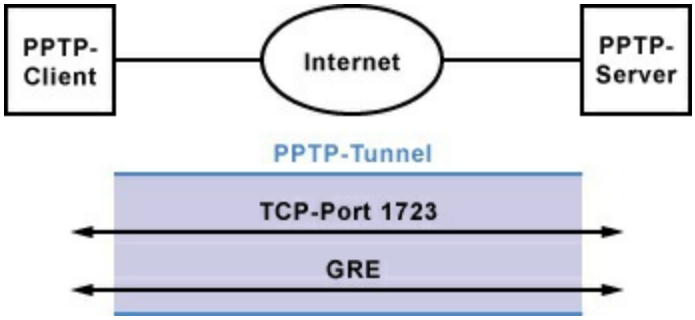
Protocol (PEAP), zu verpacken. Oder gleich auf eine sicherere VPN-Technik zu wechseln. Zum Beispiel L2TP/IPSec, IPSec mit IKEv2, SSTP oder das Open-Source-Protokoll OpenVPN.

PPTP-Architektur



Die PPTP-Architektur teilt sich in zwei logische Systeme. Den PPTP Access Concentrator (PAC) und den PPTP Network Server (PNS). Der PAC ist üblicherweise in den Client integriert, verwaltet die Verbindungen und stellt sie zum PNS her. Der PNS ist für das Routing und die Kontrolle der vom PNS empfangenen Pakete zuständig.

PPTP-Verbindungsaufbau



PPTP baut auf eine zweigeteilte Kommunikation. Zuerst eröffnet der Client die Kontrollverbindung zum Server über den TCP-Port 1723. Über diesen Port laufen alle Kontrolldaten der PPTP-Verbindung. Dieser Port muss bei der Nutzung von PPTP von innen geöffnet sein (z. B. mit PPTP-Passthrough oder Port-Forwarding), damit ein PPTP-Client die ausgehenden bzw. eingehenden Verbindungen nutzen

IP-Header	GRE-Header	PPP-Header	Nutzdaten (verschlüsselt)

kann. Als Quell-Port der Kontrollverbindung benutzt PPTP einen beliebig freien Port.

Der zweite Teil der Kommunikation ist die Verbindung mit GRE (Generic

Routing Encapsulation). Darüber werden die PPP-Pakete getunnelt. Das bedeutet, PPTP kapselt die PPP-Pakete mit GRE in IP-Pakete.

Die Benutzerauthentisierung erfolgt mit MS-CHAPv1 oder MS-CHAPv2. Die Authentisierung und Aushandlung der Schlüssel gilt als Schwachstelle von PPTP. Bei MSCHAPv1 wird die Authentisierung mit einem Passwort verschlüsselt, die sich mit einer Wörterbuch- oder Brute-Force-Attacke knacken lässt. Zwar bietet MSCHAPv2 Verbesserungen, die aber auch nur wenige Stunden standhalten.

Nach der Authentisierung wird dem Client eine IP-Adresse aus dem LAN zugewiesen. Danach erfolgt die Datenkommunikation.

Eine Verschlüsselung findet nicht statt. Die muss mit PPP ausgehandelt werden. Z. B. mit RC4, was Microsoft auch als

Microsoft Point-to-Point-Encryption (MPPE) bezeichnet.

Probleme mit NAT

Wie alle anderen VPN-Verfahren hat auch PPTP mit NAT zu kämpfen. NAT ordnet eingehende Datenpakete anhand der Portnummer einem Client zu. GRE ist ein IP-Protokoll, das keine Ports wie TCP oder UDP kennt. Dadurch ist die Zuordnung eines GRE-Pakets zu einem Client unmöglich. NAT-Router verwerfen GRE-Pakete. Ein Verbindungsaufbau ist nicht möglich.

Um die Probleme wegen NAT zu umgehen verwenden NAT-Router PPTP-Passthrough. NAT-Router, die PPTP-Passthrough bzw. PPTP mit NAT beherrschen, führen eine Liste mit den Clients und der von PPTP verwendeten Call-ID. Die Call-ID ist ein Art Tunnelnummer, die unverschlüsselt übertragen wird und der NAT-Router

auslesen kann. Er kann auf diese Weise eine Liste der von Clients verwendeten Call-IDs führen. So ist eine Zuordnung von GRE-Paket und Client doch möglich.

L2TP - Layer-2-Tunneling-Protocol

L2TP hat die Aufgabe, PPP-Verbindungen über ein IP-Netzwerk zwischen zwei Netzwerk-Stationen oder zwei eigenständigen Netzwerken herzustellen. Ein Szenario ist ein Außendienstmitarbeiter, der mit seinem Notebook über eine Wählverbindung Zugang zum Internet hat und darüber eine getunnelte Verbindung zum Netzwerk seiner Firma unterhält, die über eine Standleitung ebenfalls ans Internet angebunden ist.

Anstatt einer reellen Punkt-zu-Punkt-Verbindung besteht die

Übertragungsstrecke aus mehreren Routern, die miteinander verbunden sind. Für dieses Szenario gibt es zwei Protokolle:

L2F - Layer-2-Forwarding

PPTP - Point-to-Point Tunneling Protocol

L2TP ist eine Weiterentwicklung von PPTP und L2F. Die Struktur und Vorteile dieser beiden nichtstandardisierten Verfahren wurden in L2TP übernommen und standardisiert. Während PPTP nur IP, IPX und NetBEUI unterstützt, hat L2TP den Vorteil, dass es jedes beliebige Netzwerkprotokoll im PPP-Rahmen transportieren kann. Deshalb hat es auch einen großen Overhead und demzufolge eine geringe Netto-Datenrate. Im Gegensatz zu PPTP eignet sich L2TP sowohl für End-to-End-VPNs als auch Dialup-Verbindungen zu Service

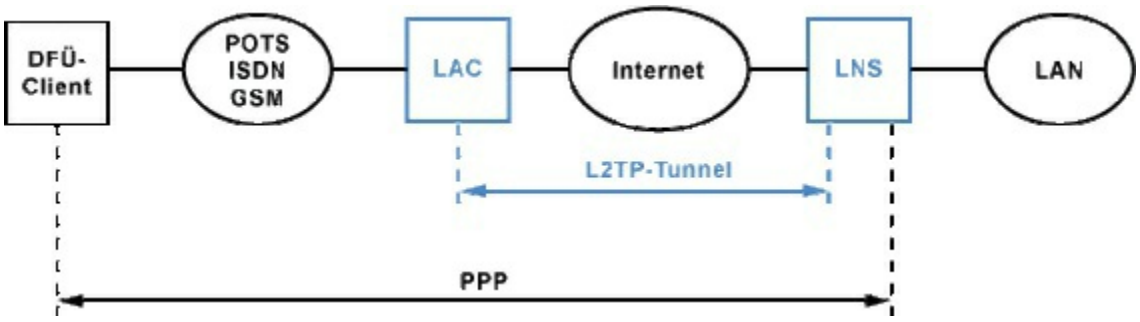
Providern.

L2TP bietet selbst keinen Authentifizierungs-, Integritäts- und Verschlüsselungsmechanismus. Dafür lässt es sich mit beliebigen Verschlüsselungsverfahren kombinieren. Der Schutz der getunnelten Daten muss z. B. mit IPsec erfolgen. Für VPN-Lösungen kommt meist eine Kombination aus L2TP und IPsec zum Einsatz. Unter Windows benötigt man für L2TP keinen separaten VPN-Client. Der ist in Windows bereits integriert.

L2TP-Architektur

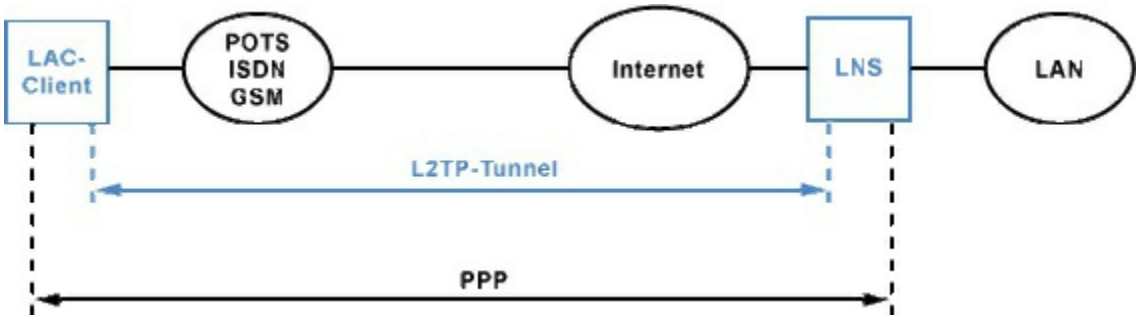
Die L2TP-Architektur teilt sich in zwei logische Systeme. Den L2TP Access Concentrator (LAC) und den L2TP Network Server (LNS). Der LAC verwaltet die Verbindungen und stellt diese zum LNS her. Der LNS ist für das Routing und die Kontrolle der vom LAC empfangenen Pakete zuständig. Das

L2TP definiert die Kontroll- und Datenpakete zur Kommunikation zwischen dem LAC und dem LNS. Das bedeutet, innerhalb des PPP-Tunnels existieren zwei verschiedene Kanäle. In einem befinden sich die Kontrollnachrichten, in dem anderen die eigentlichen Nutzdaten. Der Kontrollkanal ist eine gesicherte Verbindung, der Datenkanal ist eine ungesicherte Verbindung. Die Nutzdaten werden also ungesichert in Klartext übertragen, sofern das Transport-Protokoll (PPP) keine Verschlüsselung unterstützt oder nicht aktiviert wurde.
Die PPP-Verbindung wird durch den L2TP-Tunnel getunnelt.
Ein Network Access Server (NAS) stellt einen temporären Zugang für Remote-Systeme zur Verfügung. Der NAS kann im LAC oder im LNS implementiert



sein.

Es gibt insgesamt zwei Szenarien einen L2TP-Tunnel aufzubauen. Das erste Szenario sieht eine PPP-Verbindung zwischen dem Client und dem LAC vor. Z. B. über das Wählnetz (analog oder ISDN). Der LAC tunnelt die PPP-Daten zum LNS und bekommt von diesem eine IP-Adresse aus dem LAN zugeteilt.



Das zweite Szenario sieht eine direkte Unterstützung von L2TP auf dem Client vor. Der Client ist dann selber der LAC. Die Daten werden genauso mit PPP

übertragen. Die IP-Adresse aus dem LAN wird auch hier vom LNS zugeteilt. In beiden Fällen ist die Autorisierung und Authentifizierung von den Mechanismen im LAN abhängig. Das ist z. B. über den NAS möglich.
Mit L2TP wird ein Tunnel zwischen LAC und LNS aufgebaut. Der NAS identifiziert den Remote-User über einen Authentifizierungsserver. Ist die Authentifizierung erfolgreich wird der L2TP-Tunnel etabliert. Der LNS identifiziert sich ebenfalls beim Remote-User und bestätigt den L2TP-Tunnel. In diesem Tunnel wird für jede PPP-Verbindung eine Sitzung (Session) zwischen LAC und LNS aufgebaut. Mittels des Multiplex-Modus lassen sich in einem Tunnel mehrere Sitzungen aufbauen.

L2TP über eine Firewall

VPN über ein Firewall schließt sich

meistens aus. Ohne Probleme ist VPN über eine Firewall nur möglich, wenn die Firewall gleichzeitig als Endpunkt einer VPN-Verbindung arbeitet.
Eine Firewall erwartet die Datenpakete von dem Port kommend, von dem sie zuvor angefordert wurden. L2TP antwortet in der Regel von irgendeinem freien Port über 1024. Um L2TP doch über eine Firewall zu nutzen, verwendet man eine Funktion mit dem Namen Port-Triggering. Damit wird auf einem bestimmten Port mit ausgehendem Datenverkehr das Freischalten weiterer Ports für eingehenden Datenverkehr ermöglicht. Bei L2TP währe der Triggering-Port die 1701.
Dazu müssen die Ports 1024 bis 65535 freigeschaltet werden. Setzt die Firewall auf einen Portfilter wäre das eine riesige Lücke, was sie nahezu unbrauchbar macht.

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 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 keine Sicherheitsmechanismen hat, wurde IPsec für IPv4 nachträglich spezifiziert.

Bestandteile von IPsec-

VPNs

Interoperalitität

kyptografischer Schutz der übertragenen Daten

Zugangskontrolle

Datenintegrität

Authentifizierung des Absenders (Benutzerauthentifizierung)

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

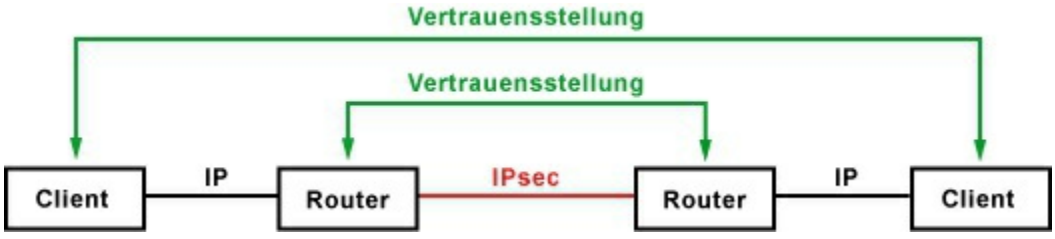
Gateway-zu-Gateway-VPN (LAN-to-LAN)

Host-zu-Gateway-VPN (Remote-Access)

Host-zu-Host-VPN (P2P oder Remote-Desktop)

Prinzipiell eignet sich IPsec für

Gateway-zu-Gateway-Szenarien. Also die Verbindung von Netzen über ein 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 fehlen. Deshalb macht es Sinn, zur Realisierung



eines VPNs außer IPsec auch L2TP (Layer 2 Tunneling Protocol), PPTP

(Point-to-Point Tunneling Protocol) oder SSL-VPN 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.

Pre-Shared Keys (PSK)

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. 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 Authentifizierung, Verschlüsselung und die Länge des Schlüssels festlegen.

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. Gängige Verfahren sind DES, Triple-DES (3DES) und SHA-1. Weil IPsec-Implementierungen kein bestimmtes Verfahren beherrschen müssen, 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 und erhöht die

Sicherheit.

IKEv2 ist allerdings nicht abwärtskompatibel zu IKE. Beide Protokolle werden aber über denselben UDP-Port betrieben.

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 neuen Adressen ausgetauscht werden. Entweder manuell oder per dynamische DNS-Einträge mit DynDNS.

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

1. Ein NAT-Router hat keinen Zugriff auf verschlüsselte IP-Pakete.
2. Hätte der NAT-Router Zugriff auf das verschlüsselte IP-Paket, dann wäre das per NAT veränderte Datenpakete ungültig.

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.

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

Gegenstellen die notwendigen Verfahren überhaupt beherrschen.

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 NAT-Router nicht aufgrund von Timeouts gelöscht werden.

4. Bei Bedarf, und das ist die Regel, wird NAT-Traversal aktiviert.

5. Danach beginnt die Aushandlung 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 Authentifizierungsverfahren 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 Authentifizierungsverfahren 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.

Alternativen zu IPsec: SSL-VPN und OpenVPN

Der Aufbau eines IPsec-VPNs ist vergleichsweise 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.

Eine einfache Alternative zu IPsec-VPN ist SSL-VPN. Dahinter steckt SSL bzw. TLS für die Verschlüsselung. Der wichtigste Vorteil von SSL-VPN ist ein quasi Client-loser Betrieb. Die Verbindung kann mit jedem Browser aufgebaut werden. Wenn jedoch andere Anwendungen diese Verbindung nutzen sollen, dann braucht man eine Art Gateway auf der Client-Seite. Zum Beispiel ein Java- oder ActiveX-Plugin.

Eine weitere Alternative ist OpenVPN,

welches IP-Pakete tunneln und

unabhängig von der Anwendung

übertragen kann.

AH -

Authentication

Header

Authentication Header (AH) sorgt

innerhalb von IPsec (VPN) für die

Authentizität der zu übertragenen Daten

und die Authentisierung des Senders.

Mit AH kann man "nur die Integrität und Echtheit" der Daten sicherstellen. Die

Nutzdaten werden nicht verschlüsselt

und sind damit für jeden lesbar.

AH wird selten verwendet, weil "nur

Integrität" meist nicht ausreicht. In der Regel möchte man die Daten noch

verschlüsseln, um sie vor fremdem

Zugriff zu schützen.

Neben Authentication Header (AH) gibt

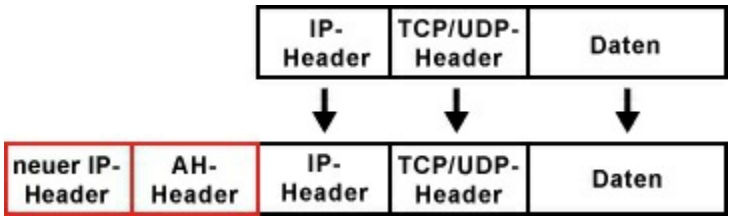
es auch noch Encapsulating Security

Payload (ESP). Beide können

gemeinsam oder alleine genutzt werden.

Im Unterschied zu Authentication Header verschlüsselt Encapsulating Security Payload die Daten.

Wie funktioniert Authentication Header im Tunnelmodus?

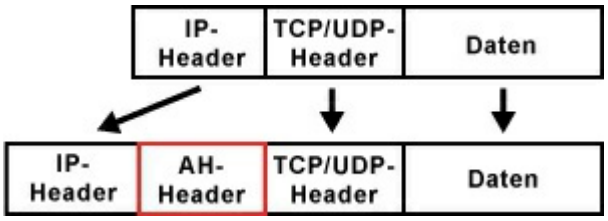


Der Tunnelmodus kann bei allen VPN-Anwendungen eingesetzt werden. Im Tunnelmodus wird das gesamte IP-Paket verschlüsselt in ein neues IP-Paket gepackt. Das bedeutet, die Original-IP-Adresse ist von außen nicht mehr sichtbar. Der Tunnelmode verschleiert die Original-Adresse des Absenders.
Im Tunnelmodus kapselt IPSec mit AH das ganze Paket inklusive IP-Header in ein neues Paket mit einem neuen IP-Header und bildet über das gesamte IP-Datenpaket eine Prüfsumme. Es wird

das gesamte IP-Paket, bis auf veränderbare Felder, in die "Authentication" einbezogen. Über die Prüfsumme ist beim Empfänger die Vollständigkeit und Korrektheit der Daten und die Identität des Absenders feststellbar.

Im Tunnelmodus kommen für den AH-Header 28 bis 32 Byte und für den zusätzlichen IP-Header 20 Byte hinzu.

Der Tunnelmodus bereitet Probleme im Zusammenhang mit einem NAT-Router. Denn die Absender-Adresse stimmt mit der Adresse im Original-Header nicht überein. Der NAT-Router manipuliert die IP-Adressen. Dadurch wird ein solches Datenpaket beim Empfänger als ungültig verworfen.



Wie funktioniert Authentication Header im

Transportmodus?

Es ist für IPsec nicht unbedingt erforderlich IP-Pakete vollständig neu zu encapsulieren (einzukapseln). Es ist von der Kommunikation abhängig. Beim Transportmodus wird der Original-IP-Header weiter benutzt und zusätzlich ein AH-Header eingefügt. Es kommen für den AH-Header 28 bis 32 Byte hinzu. Vorteil des Transportmodus ist der geringe Overhead gegenüber dem Tunnelmodus.
Der Transportmodus kann ausschließlich bei einer Host-to-Host-Verbindung verwendet werden.

ESP -

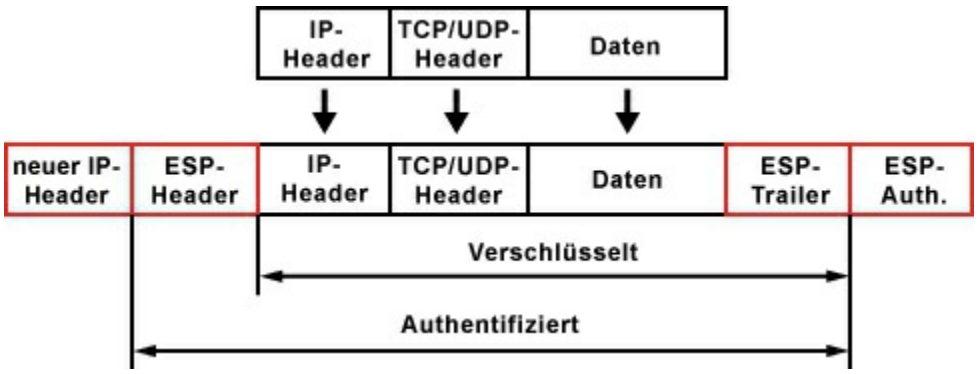
Encapsulating

Security Payload

Encapsulating Security Payload (ESP) sorgt innerhalb von IPsec (VPN) für die Authentisierung, Integrität und Vertraulichkeit der IP-Pakete. Im

Unterschied zu Authentication Header (AH) werden die Nutzdaten verschlüsselt übertragen.
Während AH "nur die Integrität und Echtheit" der Daten sicherstellen kann, erhöht ESP die Datensicherheit in Abhängigkeit des gewählten Verschlüsselungsalgorithmus. Deshalb wird in der Regel ESP und nicht AH verwendet.
ESP sorgt für die Vertraulichkeit der Kommunikation. Die Pakete werden verschlüsselt. Zusätzlich schützt eine Integritätssicherung vor Manipulation.
ESP beinhaltet zwei Betriebsmodi. Den Tunnelmodus und den Transportmodus.
Der Tunnelmodus kann bei allen VPN-Anwendungen eingesetzt werden. In der Hauptsache aber, wenn zwei Netzwerke über ein unsicheres Netzwerk miteinander verbunden werden sollen.
Will man nur zwei Rechner miteinander verbinden, dann verwendet man den

Transportmodus. Der Transportmodus



kann aber nur bei einer Host-to-Host-Verbindung verwendet werden.

Wie funktioniert

Encapsulating Security

Payload im Tunnelmodus?

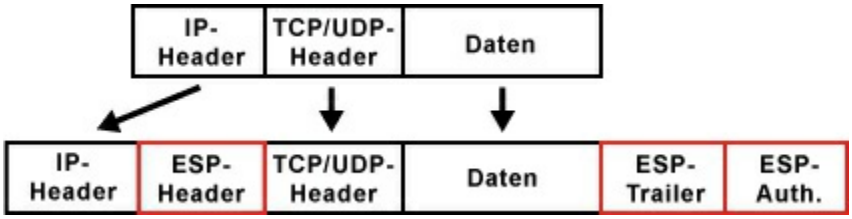
Im ESP-Tunnelmodus wird die Verschlüsselung über das gesamte Paket und dem ESP-Trailer und anschließend die Authentifizierung vom ESP-Header bis einschließlich ESP-Trailer vollzogen. Der Hash wird dann an den ESP-Trailer angehängt.

Im Tunnelmodus wird das gesamte IP-Paket verschlüsselt und in ein neues IP-Paket gepackt. Das bedeutet, die Original-IP-Adresse ist von außen nicht

mehr sichtbar. Der Tunnelmodus verschleiert die Original-Adresse des Absenders.

Im Tunnelmodus kommen für den ESP-Header 8 Byte, für den ESP-Trailer 16 bis 20 Byte und für den zusätzlichen IP-Header 20 Byte hinzu.

Wie funktioniert



Encapsulating Security Payload im Transportmodus?

Es ist für IPsec nicht unbedingt erforderlich IP-Pakete vollständig neu zu encapsulieren (einzukapseln). Es ist von der Kommunikation abhängig.

Beim Transportmodus wird der Original-IP-Header weiter benutzt und zusätzlich ein ESP-Header eingefügt. Es kommen für den ESP-Header 8 Byte und

für den ESP-Trailer 16 bis 20 Byte hinzu. Vorteil des Transportmodus ist der geringe Overhead gegenüber dem Tunnelmodus.

Im Transportmodus werden lediglich die Daten verschlüsselt und der alte IP-Header unverändert belassen. Die Daten sind so zwar geschützt, ein Angreifer kann jedoch zumindest eine bestehende VPN-Verbindung zwischen zwei Stationen feststellen.

Tunnelmodus vs. Transportmodus

Wenn Subnetze über unsichere Netze miteinander verbunden werden, dann kommt üblicherweise ESP im Tunnelmodus zum Einsatz.

Wenn zwei Computer in einem LAN miteinander verbunden werden sollen, dann wählt man üblicherweise den Transportmodus.

L2TP over IPsec

L2TP over IPsec ist eine Kombination aus dem Sicherheitsprotokoll IPsec und dem Tunneling-Protokoll L2TP. L2TP over IPsec setzt Microsoft für Punkt-zu-Punkt-Verbindungen zwischen zwei virtuellen Netzwerk-Schnittstellen ein. Dabei wird L2TP durch IPsec getunnelt. Durch die Kombination von L2TP und IPsec haben sich die Schwächen beider Protokolle gegenseitig auf. L2TP und IPsec miteinander zu kombinieren bedeutet, ein flexibles Tunneling-Protokoll mit höchster Sicherheit einsetzen zu können.

Nachteile von IPsec

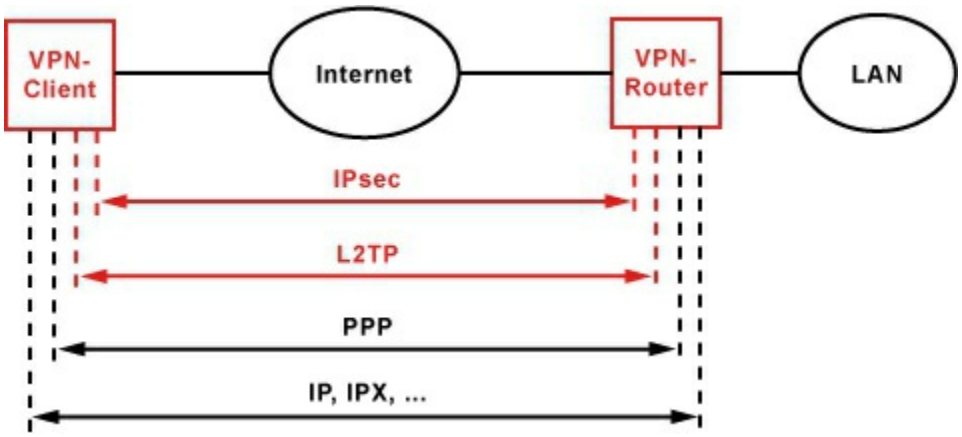
IPsec hat den Nachteil, dass es nur IP-Pakete tunneln kann. Außerdem ist es ohne zusätzliche Protokolle eher ungeeignet für Remote Access. Es fehlen die Funktionen zur Konfiguration von IP-Adresse, Subnetzmaske und DNS. In Kombination mit L2TP ist es möglich

über IPsec auch andere Protokolle als IP zu übertragen und gleichzeitig für Remote Access zu nutzen.

Nachteile von L2TP

L2TP kann alle Protokolle tunneln, sofern sie in PPP eingekapselt werden können. Das heißt, wenn es für ein Netzwerk-Protokoll einen NCP für PPP gibt, dann kann es durch L2TP getunnelt werden. Allerdings bietet L2TP keine besonderen Sicherheitsfunktionen. IPsec kümmert sich um die in L2TP nicht vorhandene Verschlüsselung.

L2TP/IPsec-Architektur



Zuerst wird die IPsec-Verbindung aufgebaut. Danach folgt durch die

sichere Verbindung der L2TP-Tunnel,
durch den die privaten Netzwerk-Pakete
in PPP-Paketen transportiert werden.

L2TP/IPsec-Protokoll-Stack

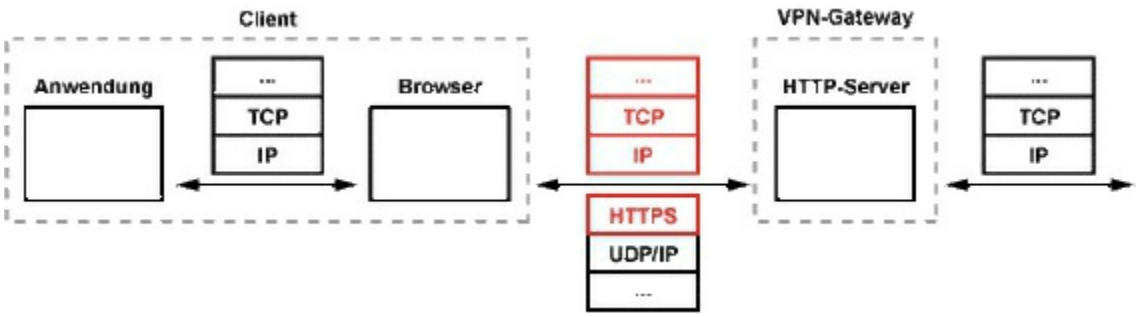
Die IP-Pakte werden in PPP-Frames
eingekapselt. Die werden in L2TP-
Pakete eingekapselt. Dann folgt der
UDP-Paket. Und dann wird noch ein
IPsec-Header und -Trailer drumherum
gebaut. Die Daten sind somit
verschlüsselt. Danach werden die
Pakete noch von einem Schicht-2-
Protokoll (L2), zum Beispiel PPP,
PPPoE oder Ethernet, nochmals
eingekapselt und vom VPN-Router
weitergeleitet.
Die Verarbeitung ist recht aufwändig
und der Paket-Overhead im Vergleich zu
den Nutzdaten groß. Allerdings ist das
die einzige Möglichkeit Nicht-IP-Pakete
mit höchstmöglichster Sicherheit zu

übertragen.

SSL-VPN

SSL-VPN ist eine Art Remote-Access-VPN, das eine Alternative zu IPsec, PPTP und L2TP 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



und 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.

Vergleich: IPsec und SSL-VPN

IPsec und SSL kann man nicht direkt miteinander vergleichen. Dafür sind ihre Ausrichtungen und der 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 und hat im laufenden Betrieb 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.

Sicherheitsbedenken gegen SSL-VPN?

Gegen SSL kann man grundsätzlich

nichts aussetzen. In SSL kommen viele Verschlüsselungs-, Schlüsselerzeugungs- und Hash-Verfahren zu Einsatz, die auch im IPsec- und IKE-Protokoll Anwendung finden.

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. Probleme können insbesondere veraltete Browser mit Sicherheitslücken machen.

Warum kommt SSL-VPN trotzdem nicht bei allen VPN-Anwendungen zum Einsatz?

Der erste Punkt, SSL verschlüsselt nur die Daten, aber nicht die gesamte Kommunikation. Zweitens, SSL-VPN funktioniert von fast jedem Computer, der Internet-Zugang hat. Und das auch, bei einem unsicheren Rechner.

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. Doch für manche Anwendungen ist das nicht sicher genug. SSL unterstützt keine Tunnel, was aber für ein VPN eigentlich eine Voraussetzung ist.

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 ablösen zu wollen ist in den seltensten Fällen eine gute Idee. SSL-VPN ergänzt IPsec auf Applikationsebene mit vergleichbaren Sicherheitsfunktionen.

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.
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.
OpenVPN nutzt SSL bzw. TLS zur Verschlüsselung. OpenVPN schiebt sich zwischen die nicht TLS-fähigen Anwendungen und dem TCP/IP-Protokollstack. Dafür muss der OpenVPN-Client auf der einen und auf der anderen Seite ein OpenVPN-Server installiert sein. Der OpenVPN-Server kann nicht auf einem normalen Router laufen.
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 eine Datenflusskontrolle. NAT-Router stellen für OpenVPN-Verbindungen kein Problem dar, weil OpenVPN weder die IP-Adresse noch die Portnummern des Pakets authentisiert.

Betriebsarten: Routing oder 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.

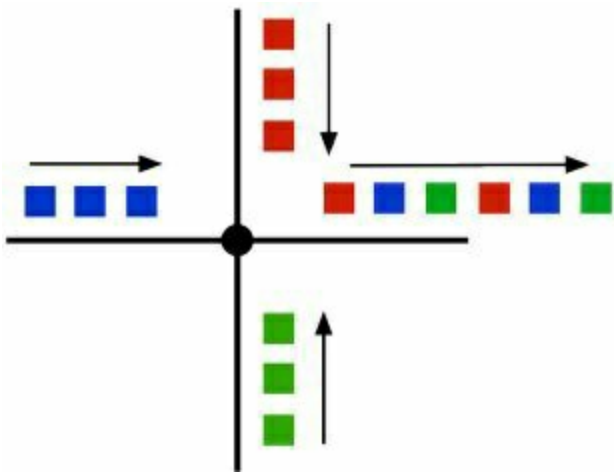
OpenVPN oder IPsec

Bei beiden VPN-Techniken muss man grundsätzlich unterscheiden. Während es sich bei IPsec um einen Standard handelt, der im Internet-Protokoll und damit im Betriebssystem verankert ist, nutzt OpenVPN unterschiedliche Standards und läuft als Software innerhalb eines Betriebssystems wie jede andere Software auch. Beide Szenarien haben Vor- und Nachteile. Während IPsec zwingend die Unterstützung durch die Netzwerk-Hardware (z. B. Router) braucht, ist das bei OpenVPN nicht erforderlich. Während IPsec ein Standard und damit vergleichsweise komplex ist, ist OpenVPN nur Open-Source, weist aber eine große Flexibilität auf und ist vergleichsweise einfach einzurichten.

Aber auch nur dann, wenn man einfach Sachen machen will. Sobald Routing oder komplexere Spielchen dazukommen, fährt man mit IPsec besser. Letzten Endes ist es eine Frage der Anwendung und deren Reichweite. Große Firmen werden IPsec-Lösungen mit Support und Dienstleistungsverträgen bevorzugen. Kleinere Firmen fahren mit OpenVPN unter Umständen besser.

Layer-2-VPN

Bei einem Layer-2-VPN wird das VPN von einem Netzbetreiber bereitgestellt. Der Netzbetreiber überträgt die Daten über sein nicht-öffentliches Netz und dessen Verbindungen. Früher waren das üblicherweise Frame Relay, X.25 und ATM. Heute ist das MPLS.



MPLS bildet eine Brücke zwischen verbindungsorientierten Übertragungstechniken und verbindungslosen, paketbasierten Verfahren. Mit MPLS ist es möglich, verschiedene Arten von Daten, wie zum Beispiel Telefonie oder Internet-Verkehr, über die gleiche Infrastruktur zu transportieren. Obwohl im Hintergrund paketorientierte Übertragungstechniken arbeiten, sieht das Netz für den Kunden wie eine Standleitung aus. Auf diese Weise kann der Kunde verschiedene Arten von Paketen durch das MPLS-Netz schicken. Manchmal weiß der Kunde gar nicht,

dass es sich um ein MPLS-Netz handelt. Er mietet schlicht und einfach eine Standleitung zur Übertragung von Ethernet-, ATM-, Frame-Relay-, oder IP-Paketen.

Obwohl man bei einem VPN Daten verschlüsselt, ist das bei einem Layer-2-VPN nicht der Fall. Der Netzbetreiber verschlüsselt keine Daten. Das ist auch nicht nötig. Fremde haben keinen Zugriff auf die Infrastruktur des Netzbetreibers. Und die Nutzer (Kunden des Netzbetreibers) kommen mit den unverschlüsselten Daten anderer Nutzer nicht in Berührung. Denn die Übertragungstechniken des Netzbetreibers halten die verschiedenen Datenströme getrennt. Das Risiko vor unberechtigtem Zugriff ist relativ gering.

MPLS ist nur bei der Kopplung großer Netze sinnvoll. Und auch nur dann, wenn man die Netze nicht übers öffentliche

Internet, sondern über das private Netz eines Netzbetreibers verbinden will. Zum Beispiel, weil einem der Betrieb eines eigenen VPN zu unsicher ist oder eine bestimmte Bandbreite gefordert wird.

Hinweis: Die Nutzung eines Netzbetreiber-VPN setzt voraus, dass die VPN-Endpunkte am Netz des Netzbetreibers angeschlossen sind. Die VPN-Endpunkte müssen zwingend am gleichen Zugangsnetz hängen.

Authentisierung im Netzwerk

Authentisierung 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 Authentisierung durch die räumliche Trennung erschwert. Hier greift man auf symmetrische Schlüssel,

Zertifikate und andere

Authentisierungsmechanismen zurück.

Im Zusammenhang mit der

"Authentisierung" tauchen auch häufig die Begriffe "Autorisierung" und

"Authentifizierung" auf. "Autorisierung"

ist der Vorgang, bei dem ermittelt wird,

welche Berechtigung die Person oder

Maschine hat und was sie machen darf.

"Authentifizierung" bedeutet, dass eine elektronische Unterschrift beglaubigt

bzw. dessen Echtheit bezeugt wird.

Die Authentisierung, nicht

Authentifizierung oder Autorisierung,

erfolgt zum Beispiel mit Benutzername

und Passwort. Knackpunkt bei jeder

Authentisierung 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 Authentisierung möglich. Um Sicherheit in einem Netzwerk herzustellen sollte man niemals die Authentisierung vernachlässigen.

Übersicht: Authentisierung

Pre-Shared-Keys

Zertifikate

Kerbero

SecurI

Pre-Shared-Keys

Pre-Shared-Keys sind symmetrische Schlüssel (Passwort), die vor einer Verbindungsaufnahme ausgetauscht werden müssen. 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.

Zertifikate

Bei der Authentisierung mit Zertifikat kommt ein asymmetrischer, zertifizierter Schlüssel zum Einsatz. Nach der erfolgreichen Authentisierung 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 Authentisierung, sondern auch bei der gesicherten Übertragung von E-Mails, dem Webseiten-Abruf (SSL/TLS) oder dem Code-Signing verwendet.

Software für die Verwaltung von Zertifikaten

Windows Server

OpenCA

TinyCA

Easy-RA (OpenVPN)

Protokolle für die Authentisierung

PAP - Password Authentication Protocol

CHAP - Challenge Handshake

Authentication Protocol

MS-CHAP - Microsoft CHAP

EAP - Extensible Authentication

Protocol

Authentisierungsverfahren

IEEE 802.1x / RADIUS

AAA -

Authentication

Authorization

Accounting

AAA steht für ein Sicherheitskonzept

unter dem Authentication, Authorization

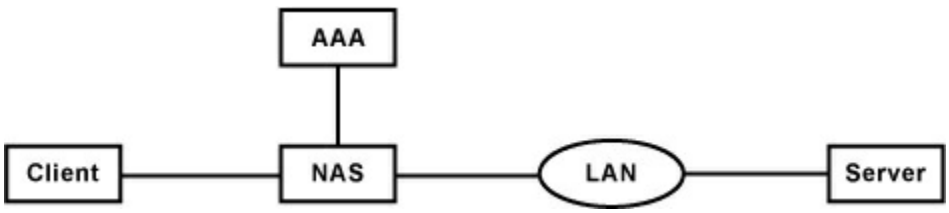
und Accounting zusammengefasst sind.

Es handelt sich dabei um die drei

Hauptaufgaben von AAA.

Vereinfachte Darstellung

der Funktionsweise von



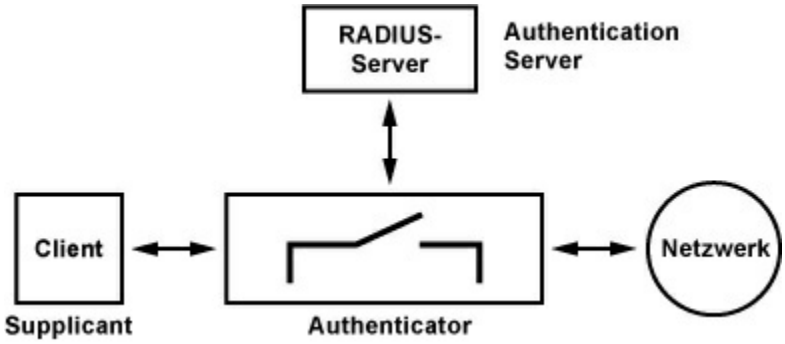
AAA

Ein Nutzer (Client) möchte einen Dienst in Anspruch nehmen. Ein Network Access Server (NAS) bietet diesen Dienst oder Zugang zum Dienst (Server im LAN) an. Der Client greift auf den NAS zu. Der NAS befragt seinen AAA-Server, der Informationen über die Berechtigung zur Nutzung von Diensten bereitstellt und alles aufzeichnet. Der AAA-Server bestätigt die Freigabe oder lehnt sie ab. Aufgrund der Berechtigung gibt der NAS dem Client den Zugang frei oder lehnt ihn ab.

Authentisierung / Authentication

Authentisierung bedeutet, die Identität zu überprüfen. Zum Beispiel mit Benutzername und Passwort. Knackpunkt bei jeder Authentisierung ist die Übertragung von Benutzername und Passwort. Erfolgt sie unverschlüsselt, dann ist es möglich, dass ein Angreifer

beides ausspäht und für die eigene Authentisierung missbraucht.



Die Bestandteile eines Authentisierungssystems sind der Supplicant (Antragsteller), der Authenticator (Beglaubigter) und ein Authentication Server, der den Antrag des Supplicant überprüft und seine Entscheidung dem Authenticator mitteilt.
Der Supplicant ist eine Client-seitige Komponente, die für alle gängigen Betriebssysteme existiert und in der die Verfahren für Schlüsselaustausch und Authentifizierung implementiert sind.
Der Authenticator regelt den Zugang zum Netz. Solange ein Client nicht authentisiert ist, werden nur Pakete zur

Authentisierung akzeptiert. Im Erfolgsfall wird jeglicher Verkehr zugelassen.

Der Authentication Server bekommt vom Authenticator Anfragen weitergeleitet. Er ist die Instanz, die den Zugang zum Netzwerk erlaubt oder verweigert. Der Authentication Server wird in der Regel durch einen RADIUS-Server implementiert.

Autorisierung / Authorization

Bei der Autorisierung stellt man fest, ob ein bestimmter Benutzer einen bestimmten Dienst nutzen darf. Nur weil sich der Benutzer authentisiert hat bedeutet das nicht, dass er auch berechtigt ist einen bestimmten Dienst zu benutzen. Wenn hinter einer Authentisierung mehrere Dienste angeboten werden, dann auch die Berechtigungen zu prüfen, wenn nicht

alles pauschal freigegeben sein soll.

Accounting

Beim Accounting geht es darum, die Nutzung eines Dienstes durch einen Benutzer festzuhalten und zu dokumentieren. Später kann die Nutzung zum Beispiel abgerechnet werden. Es ist aber auch möglich, für Service-Fälle festzustellen, was der Benutzer gemacht hat, um Fehler aufzuspüren.

Anmerkung zum Schluss

In der Deutschen Sprache gibt es einen Unterschied zwischen "authentifizieren" und "authentisieren". Im Duden steht dazu folgende Erläuterung:

au|then|ti|fi|zie|ren: die Echtheit bezeugen oder beglaubigen

au|then|ti|sie|ren: glaubwürdig oder rechtsgültig machen

"Authentifizieren" bzw. "Authentifizierung" würde demnach bedeuten, dass eine elektronische Unterschrift beglaubigt bzw. dessen

Echtheit bezeugt wird.
"Authentisieren" bzw. "Authentisierung" würde demnach bedeutet, dass der Absender seine Identität glaubwürdig machen soll. Demnach wären die typischen Benutzername-Passwort-Abfragen eine Authentisierung.
In der Praxis und im allgemeinen Sprachgebrauch wird zwischen beiden Formen jedoch nicht immer unterschieden. Wenn von Authentifizierung die Rede ist, dann ist damit in der Regel die Authentisierung gemeint.

MS-CHAP -
Microsoft CHAP

Das Microsoft Challenge Handshake Authentication Protocol, kurz MS-CHAP, ist ein Authentisierungsverfahren. MS-CHAP wurde von Microsoft speziell für Windows NT, Windows 2000,

Windows 95 und höher entwickelt.
Dabei muss man zwischen der Version 1 und 2 unterscheiden. Sie wurden für unterschiedliche Zwecke entwickelt und sind deshalb zueinander inkompatibel.
MS-CHAPv1 ist für die Authentifizierung von DFÜ-Verbindungen gedacht und entspricht in weiten Teilen dem standardmäßigen CHAP. MS-CHAPv2 ist ein Authentisierungsverfahren für virtuelle private Netzwerkverbindungen (VPN).

MS-CHAPv2

Für das Tunneling-Protokoll PPTP hat Microsoft mit MS-CHAPv2 ein eigenes Authentisierungsverfahren entwickelt. Seine Besonderheit ist die gegenseitige Authentisierung durch Client und Server. Der Kryptografieschlüssel besteht aus dem Passwort und einem echten zufälligen Wert (Challenge String). Je ein Kryptografieschlüssel wir für

Sende- und Empfangsrichtung verwendet. Dadurch ist die Sicherheit für RAS-Verbindungen deutlich höher. MS-CHAPv2 unterstützt nur VPN-Verbindungen. Bei normalen DFÜ-Verbindungen kann MS-CHAPv2 nicht verwendet werden.

Ablauf der Authentifizierung bei MS-CHAPv2

MS-CHAP arbeitet wie ein 3-Wege-Handshake mit wechselseitiger Authentisierung. Also muss sich nicht nur der Client gegenüber dem Server ausweisen, sondern auch der Server muss dem Client beweisen, dass er auch wirklich über dessen Benutzerdaten verfügt.

Der Schlüssel zur Verschlüsselung wird vom Passwort und vom Challenge String abgeleitet. Auf diese Weise kommt bei jeder Verbindung ein anderer Schlüssel

zum Einsatz. Und es wird in beide Richtungen unterschiedliche Schlüssel verwendet.

1. Der Server fordert den Client zur Authentisierung auf (Challenge).
Die Aufforderung besteht aus einer Sitzungs-ID (Session Identifier) und einem zufälligen Wert, dem Peer Challenge String.

2. Der Client bildet aus dem Peer Challenge String, der Sitzungs-ID und seinem Passwort einen Hashwert (z. B. mit SHA-1). Dann schickt er Benutzername, einen eigenen zufälligen Wert und den gebildeten Hashwert an den Server zurück.

3. Der Server prüft die Antwort und sendet eine Annahmebestätigung oder die Ablehnung. Die Annahme enthält die authentisierte Antwort der gesendeten Challenge, den Peer

Challenge String, die
verschlüsselte Antwort des Clients
und das MD4-gehashte Passwort.
4. Der Client prüft die Antwort. Ist
die Antwort fehlerfrei wird die
Verbindung genutzt. Wenn nicht,
dann bricht der Client die
Verbindung ab.

IEEE 802.1x /
RADIUS

IEEE 802.1x ist ein sicheres
Authentisierungsverfahren 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 Authentisierungsnachrichten auf der Schicht 2 des OSI-Schichtenmodells.
EAP beschreibt ein einfaches Frage-Antwort-Verfahren, bei dem die Authentisierungsdaten vom Benutzer zum Authentisierungs-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 Authentisierungsmethode IEEE 802.1x auch als WPA2 Enterprise, WPA2-1x oder WPA2/802.1x bezeichnet.

Funktionen von IEEE

802.1x

Zugangskontrolle

Authentisierung, Autorisierung und

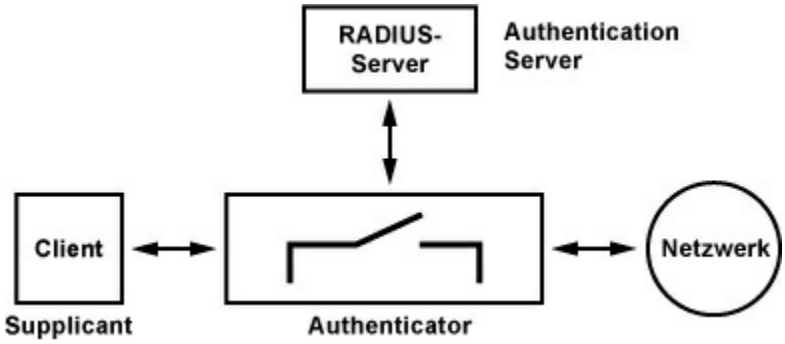
Accounting (AAA)

Bandbreitenzuweisung (QoS)

Single Sign-on (SSO)

Wie funktioniert IEEE

802.1x?



Bestandteil eines

Authentisierungsverfahrens 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

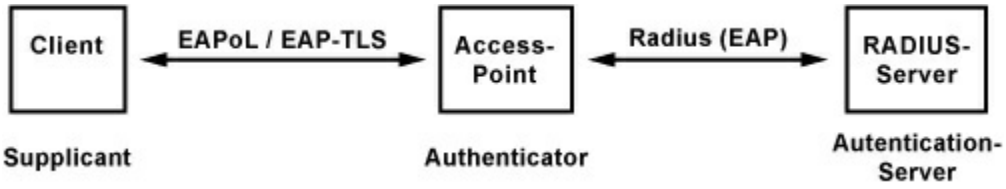
Anmeldungen vom Supplicant (Client)
werden vom Authenticator zuerst an den
Authentication Server weitergeleitet.
Der entscheidet, ob der Supplicant
Zugang bekommt. In Abhängigkeit einer
erfolgreichen Authentisierung wird der
Zugang zum Netzwerk über einen
bestimmten Port freigeschaltet. Wegen
dem Bezug 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 aber 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 Authentisierung 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.

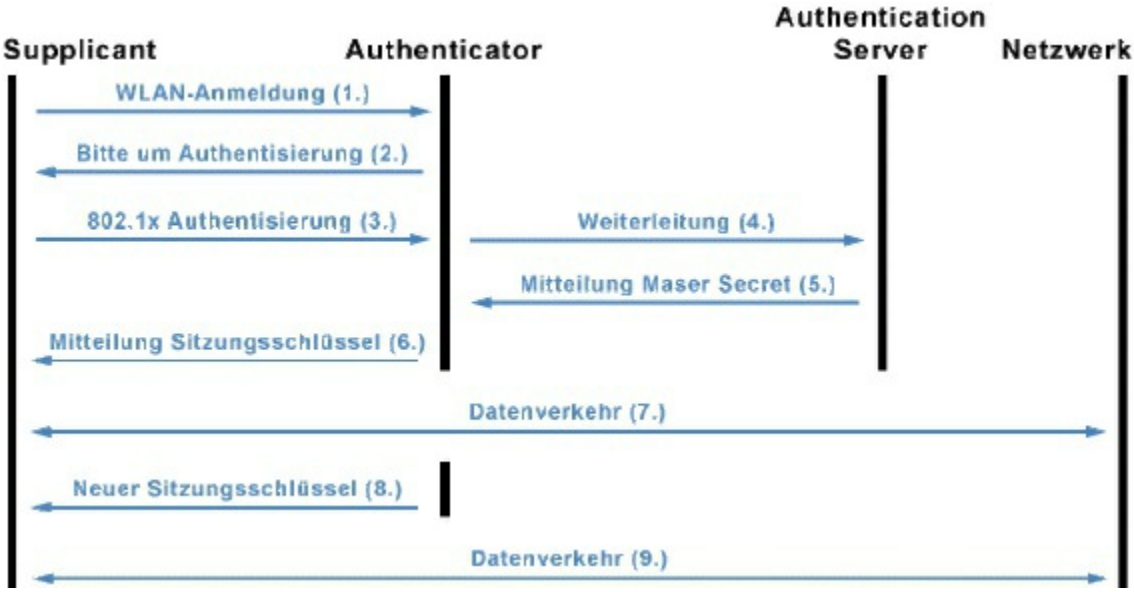
Beispiel für die Anwendung von IEEE 802.1x, EAP und RADIUS

Beim Zugriff auf ein lokales Netzwerk eines Unternehmens über WLAN reicht die einfache Authentisierung 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 Authentisierung auf.

3. Der Client (Supplicant) authentisiert sich nach IEEE 802.1x. In der Regel ging dem die Eingabe von Benutzername und Passwort durch den Nutzer voraus.

4. Der Access-Point (Authenticator)

leitet die Authentisierung an den RADIUS-Server (Authentication Server) weiter.

5. Bei erfolgreicher Authentisierung gibt der RADIUS-Server das Master Secret zurück.

6. Der Access-Point generiert den Sitzungsschlüssel und teilt das 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 ein weiterer Zugriff auf das Netzwerk 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 Authentisierung 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 authentisiert 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 Authentisierung 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).

TACACS - Terminal Access Controller Access Control Server

TACACS ist in gewissen Bereichen dem RADIUS ähnlich. So stellt ein Client eine Authentisierungsanfrage an einen NAS (Network Access Server), der diese Anfrage an den zentralen TACACS-Server weiterleitet.

EAP - Extensible

Authentication

Protocol

Das Extensible Authentication Protocol, kurz EAP, ist eine Erweiterung von PPP und wird innerhalb von IEEE 802.1x verwendet. Die Aufgabe von EAP ist sicherzustellen, dass eine Verbindung mit PPP oder der Zugang zu einem Netzwerk erst nach erfolgreich abgeschlossener Authentisierung möglich ist.

Im Gegensatz zu PPP ist EAP nicht auf Internet-Zugänge über Analogmodem- und ISDN-Verbindungen oder Festverbindungen beschränkt. Es findet zum Beispiel auch Anwendung im LAN und WLAN. Außerdem bietet EAP sicherere Verschlüsselungsverfahren an, als sie von PPP unterstützt werden. Geschickterweise ist EAP ein Framework, dass sich jederzeit um

weitere Verfahren erweitern lässt.

EAP ist ein einfaches Protokoll. Es kennt nur Authentisierungs-Requests und -Replies. Es arbeitet üblicherweise auf der Schicht 2 des OSI-Schichtenmodells. Allerdings ist es nicht an diese Schicht gebunden. Je nach dem, auf welcher Schicht EAP arbeitet, überträgt es die Authentisierungsdaten im Klartext. Das macht den Authentisierungsprozess nicht besonders sicher. Allerdings gibt es EAP-Varianten, die eine verschlüsselte und gesicherte EAP-Kommunikation vorsehen.

EAP implementiert verschiedene Verfahren zur Nutzer-Authentifizierung:

Nutzerkennung/Passwort

Challenge/Response-Verfahren

Signaturkarten-Systeme

(Authentisierung des Netzes gegenüber dem Client möglich)

EAP-Varianten

Das ursprüngliche EAP gilt als nicht besonders sicher. Daher wurden sicherere Varianten entwickelt. EAP unterstützt verschiedene kryptografisch gesicherte Methoden. So kann im LAN oder WLAN, zum Beispiel EAP over LAN (EAPoL) oder EAP-TLS verwendet werden.

LEAP - Lightweight EAP (von Cisco)

EAP-TLS - EAP mit TLS (Kryptoschutz)

EAP-TTLS - EAP mit Tunnelled TLS (Variante von EAP-TLS)

PEAP - Protected EAP (geschütztes EAP)

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/

http://www.facebook.com/ElektronikKompendium
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/

http://www.facebook.com/ElektronikKompendium 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/

http://www.facebook.com/ElektronikKompendium ElektronikQuest

ElektronikQuest ist ein Lernsystem auf
Basis von Fragen mit vorgegebenen,
klickbaren Antworten und eignet sich für
Schüler, Azubis und Studenten mit einer
technischen Ausbildung.

Bessere Noten

Kein Bock mehr auf schlechte Noten? Willst Du endlich mal wieder gute Noten haben? Dann bist Du hier genau richtig.

Stressfrei lernen

Hast Du Stress beim Lernen? Einfach und stressfrei mit weniger Aufwand für die Klassenarbeit, Klausur oder Prüfung lernen.

Wie gut bist Du?

Wie gut kennst Du Dich in Elektronik, Computertechnik und Netzwerktechnik aus? Zeig mal was Du drauf hast. Kostenlos anmelden und testen.

http://www.elektronik-quest.de/

Document Outline

- Ethernet-Frame
- MAC-Adresse
- Ethernet-Standards
- Fast-Ethernet / IEEE 802.3u
- Gigabit-Ethernet / 1GBase-T / 1000Base-T / IEEE 802.3z / IEEE 802.3ab
- 10-Gigabit-Ethernet / 10GBase-T / IEEE 802.3ae / IEEE 802.3an
- 40- und 100-Gigabit-Ethernet / IEEE 802.3ba
- Power-over-Ethernet
- VLAN - Virtual Local Area Network / IEEE 802.1q
- IEEE 802.11 / WLAN-Grundlagen
- WLAN-Frequenzen
- CSMA/CA - Carrier Sense Multible Access/Collision Avoidance
- WLAN-Topologie
- WDS - Wireless Distribution System
- IEEE 802.11s / Wireless Mesh Network
- IEEE 802.11b / WLAN mit 11 MBit
- IEEE 802.11g / WLAN mit 54 MBit
- IEEE 802.11a / IEEE 802.11h / IEEE 802.11j
- IEEE 802.11n / WLAN mit 100 MBit/s
- IEEE 802.11ac / Gigabit-WLAN
- MIMO - Multiple Input Multiple Output
- WLAN-Sicherheit
- IEEE 802.11i - WPA/WPA2 - WiFi Protected Access
- WLAN-Authentifizierung
- HomePlug-Powerline
- MPLS - Multi-Protocol Label Switching
- TCP/IP
- TCP/IP
- IPv4 - Internet Protocol Version 4
- IPv6 - Internet Protocol Version 6
- Privacy Extensions
- Subnetting
- IP-Routing
- NAT - Network Address Translation
- DHCP - Dynamic Host Configuration Protocol
- ARP - Address Resolution Protocol
- ICMP - Internet Control Message Protocol
- IGMP - Internet Group Management Protocol
- TCP - Transmission Control Protocol

- UDP - User Datagram Protocol
- RTP - Realtime Transport Protocol
- Ping - Paket Internet Groper / pathping
- Trace Route
- ipconfig / winipcfg
- Anwendungen und Dienste
- Internet
- URI - Uniform Resource Identifiers
- URL - Uniform Resource Locator
- WWW - World Wide Web
- E-Mail
- IM - Instant Messaging
- Internet-Telefonie
- P2P - Peer-to-Peer
- Namensauflösung
- DNS - Domain Name System
- WINS - Windows Internet Name Service
- Bonjour / Zeroconf
- DynDNS
- HTTP - Hypertext Transfer Protocol
- WebDAV - Web-based Distributed Authoring and Versioning
- FTP - File Transfer Protocol
- TFTP - Triviale File Transfer Protocol
- SMTP - Simple Mail Transfer Protocol
- POP3 - Post Office Protocol Version 3
- IMAP 4 - Internet Mail Access Protocol Version 4
- MIME-Types - Multipurpose Internet Mail Extensions
- Telnet
- Verzeichnisdienste
- Storage
- VoIP - Voice over IP
- H.323
- H.323-Systemarchitektur
- H.323-Kommunikation
- SIP - Session Initiation Protocol
- SIP-Systemarchitektur
- SIP-Kommunikation
- SIPS - Session Initiation Protocol Security
- H.323 und SIP im Vergleich
- STUN - Simple Traversal of UDP through NAT

- Audio-Codecs zur Sprachdigitalisierung
- FoIP - Fax over IP
- QoS - Quality of Service
- Netzwerk-Sicherheit
- Grundlagen der Netzwerk-Sicherheit
- Verschlüsselung
- SSL - Secure Socket Layer
- TLS - Transport Layer Security
- SSH - Secure Shell
- Firewall
- DMZ - Demilitarisierte Zone
- DoS - Denial of Service
- Man-in-the-Middle
- IP-Spoofing
- Drive-by-Angriffe
- Botnetze
- VPN - Virtual Private Network
- RAS - Remote Access Service
- PPP - Point-to-Point Protocol
- Tunneling-Protokolle
- PPTP - Point-to-Point Tunneling Protocol
- L2TP - Layer-2-Tunneling-Protocol
- IPsec - Security Architecture for IP
- AH - Authentication Header
- ESP - Encapsulating Security Payload
- L2TP over IPsec
- SSL-VPN
- OpenVPN
- Layer-2-VPN
- Authentisierung im Netzwerk
- AAA - Authentication Authorization Accounting
- MS-CHAP - Microsoft CHAP
- IEEE 802.1x / RADIUS
- EAP - Extensible Authentication Protocol
- Elektronik-Fibel
- Kommunikationstechnik-Fibel
- Computertechnik-Fibel
- ElektronikQuest