1. IPsec Transport- und Tunnelmodus
2. http
3. HTTPs
4. SSL
5. VPN Arten Tunneling
6. SAN
7. DHCP
8. TCP/IP
9. Subnetting
10. SNMP und RMON
11. MIB
12. RAID Level – auch kombinierte
13. HexDump auswerten
14. Well know Ports
15. Virtualisierung von Betriessystemen
16. VoIP
17. PBX
18. ISDN D-/B1/B2-Kanal Primärmultip lex-Anschluss
19. Struktogramme
20. PAP
21. APIPA
22. IPv6
23. DNS
24. Firewall
25. DMZ
26. WLAN
27. RADIUS
28. AAA
29. DoS
30. DDoS
31. Malware
32. Statisches und dynamisches Routing
33. RIP
34. OSPF
35. Routingtabellen
36. Backup
37. Strukturierte Verkabelung
38. iSCSI-Frame
39. SAMBA-Server
40. VLAN
41. Spanning-Tree
42. USB
43. USB on-The-Go
44. Verschlüsselung
45. Digitale Signatur und sicherer Email-Versand
46. Green-IT
47. Layer-3-Switch
48. Hub

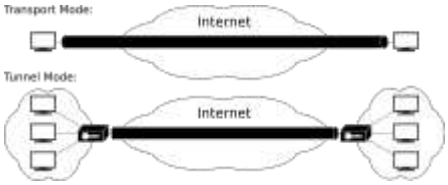
49. Layer-2-Switching-Verfahren: Cut-through store-and-forward
50. Round-Robin
51. ICMP
52. Intranet und Extranet
53. POP3
54. GSM
55. SDSL
56. ADSL
57. DSL Splitter
58. Masquerading
59. Unicast
60. Broadcast
61. Multicast
62. IGMP
63. TTL
64. ARP
65. MAC-Adresse
66. Verzeichnisdienste allgemein Windows AD
67. Speichermedien klassifizieren
68. IDS
69. SIP Verbindungsaufbau
70. Funktionsweise von USVs
71. LDAP
72. SLA (Service Level Agreement)
73. Arten und Eigenschaften von Glasfasern
74. SSD
75. Unterschiede im Datenzugriff bei NAS und SAN
76. NAS
77. Formate und Arten von Hashes (MD5 und SHA-1)
78. Netzwerk-Sicherheit
79. Unterschiede DDR/DDR-2/DDR-3/DDR-4
80. Cloud Computing
81. VDSL
82. Flashspeichern
83. Partitionieren
84. Workstation
85. Thin-Client

1. IPsec

(Kurzform für Internet Protocol Security) ist eine Protokoll-Suite, die eine gesicherte Kommunikation über potentiell unsichere IP-Netze wie das Internet ermöglichen soll.

IPsec arbeitet direkt auf der Internetschicht (Internet layer) des Protokollstapels, damit ist es für die Anwendung transparent.

Vergleich Transport- und Tunnelmodus

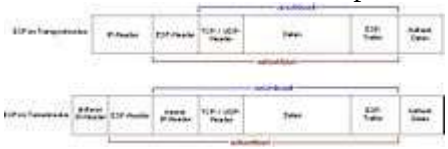


Im Transportmodus verbindet IPsec zwei Endpunkte direkt miteinander (Peer-to-Peer), zum Beispiel über eine auf den Peers installierte Software.

Im Tunnelmodus hingegen werden zwei IP-Netze miteinander verbunden. Die Endpunkte werden hier von zwei Routern bzw. VPN-Gateways gebildet, zwischen denen der Tunnel aufgebaut wird.

IPsec im Transportmodus

IPsec AH-Header im Transport- und Tunnelmodus



IPsec ESP-Header im Transport- und Tunnelmodus

Im Transportmodus wird der IPsec-Header zwischen dem IP-Header und den Nutzdaten eingefügt. Der IP-Header bleibt unverändert und dient weiterhin zum Routing des Pakets vom Sender zum Empfänger. Der Transportmodus wird verwendet, wenn die „kryptographischen Endpunkte“ auch die „Kommunikations-Endpunkte“ sind. Nach dem Empfang des IPsec-Paketes werden die ursprünglichen Nutzdaten (TCP/UDP-Pakete) ausgepackt und an die höherliegende Schicht weitergegeben. Der Transportmodus wird vor allem für Host-zu-Host- oder Host-zu-Router-Verbindungen verwendet, z. B. für die Netzwerkverwaltung.

IPsec im Tunnelmodus

Im Tunnelmodus wird das ursprüngliche Paket gekapselt und die Sicherheitsdienste von IPsec auf das gesamte Paket angewandt. Der neue (äußere) IP-Header dient dazu, die Tunnelenden (also die kryptografischen Endpunkte) zu adressieren, während die Adressen der eigentlichen

Kommunikationsendpunkte im inneren IP-Header stehen. Der ursprüngliche (innere) IP-Header stellt für Router usw. auf dem Weg zwischen den Tunnelenden nur Nutzlast (Payload) dar und wird erst wieder verwendet, wenn das empfangende Security-Gateway (das Tunnelende auf der Empfangsseite) die IP-Kapselung entfernt hat und das Paket dem eigentlichen Empfänger zustellt.

Im Tunnelmodus sind Gateway-zu-Gateway- oder auch Peer-zu-Gateway-Verbindungen möglich. Da an jeweils einer Seite Tunnelende und Kommunikationsendpunkt auf demselben Rechner zusammenfallen können, sind auch im Tunnelmodus Peer-zu-Peer-Verbindungen möglich. Ein Vorteil des Tunnelmodus ist, dass bei der Gateway-zu-Gateway-Verbindung nur in die Gateways (Tunnelenden) IPsec implementiert und konfiguriert werden muss. Angreifer können dadurch nur die Tunnelendpunkte des IPsec-Tunnels feststellen, nicht aber den gesamten Weg der Verbindung.

2. HTTP

Das Hypertext Transfer Protocol (HTTP, englisch für Hypertext-Übertragungsprotokoll) ist ein zustandsloses Protokoll zur Übertragung von Daten auf der Anwendungsschicht über ein Rechnernetz. Es wird hauptsächlich eingesetzt, um Webseiten (Hypertext-Dokumente) aus dem World Wide Web (WWW) in einen Webbrowser zu laden.

Eigenschaften

Nach etablierten Schichtenmodellen zur Einordnung von Netzwerkprotokollen nach ihren grundlegenderen oder abstrakteren Aufgaben wird HTTP der sogenannten Anwendungsschicht zugeordnet. Diese wird von den Anwendungsprogrammen angesprochen, im Fall von HTTP ist das meist ein Webbrowser. Im ISO/OSI-Schichtenmodell entspricht die Anwendungsschicht den Schichten 5 bis 7.

HTTP ist ein zustandsloses Protokoll. Informationen aus früheren Anforderungen gehen verloren. Ein zuverlässiges Mitführen von Sitzungsdaten kann erst auf der Anwendungsschicht durch eine Sitzung über einen Sitzungsbezeichner implementiert werden. Über Cookies in den Header-Informationen können aber Anwendungen realisiert werden, die Statusinformationen (Benutzereinträge, Warenkörbe) zuordnen können. Dadurch werden Anwendungen möglich, die Status- beziehungsweise Sitzungseigenschaften erfordern. Auch eine Benutzerauthentifizierung ist möglich. Normalerweise kann die Information, die über HTTP übertragen wird, auf allen Rechnern und Routern gelesen werden, die im Netzwerk durchlaufen werden. Über HTTPS kann die Übertragung aber verschlüsselt erfolgen.

Durch Erweiterung seiner Anfragemethoden, Header-Informationen und Statuscodes ist HTTP nicht auf Hypertext beschränkt, sondern wird zunehmend zum Austausch beliebiger Daten verwendet, außerdem ist es Grundlage des auf Dateiübertragung spezialisierten Protokolls WebDAV. Zur Kommunikation ist HTTP auf ein zuverlässiges Transportprotokoll angewiesen, wofür in nahezu allen Fällen TCP verwendet wird.

Derzeit werden zwei Protokollversionen, HTTP/1.0 und HTTP/1.1, verwendet. Neuere Versionen wichtiger Webbrowser wie Chromium, Opera, Firefox und Internet Explorer sind darüber hinaus bereits kompatibel zu SPDY, der Entwicklungsvorlage für Version 2 des HTTP (HTTP/2).

3. HTTPs

HyperText Transfer Protocol Secure (HTTPS, englisch für sicheres Hypertext-Übertragungsprotokoll) ist ein Kommunikationsprotokoll im World Wide Web, um Daten abhörsicher zu übertragen.

4. SSL

SSL ist ein Protokoll, das der Authentifizierung und Verschlüsselung von Internetverbindungen dient. SSL schiebt sich zwischen die Anwendungsprotokolle und den Transportprotokollen. Ein typisches Beispiel für den Einsatz von SSL ist der gesicherte Abruf von vertraulichen Daten über HTTP und die gesicherte Übermittlung von vertraulichen Daten an den HTTP-Server. In der Regel geht es darum, die Echtheit des kontaktierten Servers durch ein Zertifikat zu garantieren und die Verbindung zwischen Client und Server zu verschlüsseln.
SSL ist äußerst beliebt und das Standard-Protokoll bzw. die Erweiterung für Anwendungsprotokolle, die keine Verschlüsselung für sichere Verbindungen mitbringen.

5. VPN

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.

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 die Sicherheit der Daten, die darüber übertragen werden.

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-Typen

- End-to-Site-VPN (Host-to-Gateway-VPN / Remote-Access-VPN)
- Site-to-Site-VPN (LAN-to-LAN-VPN / Gateway-to-Gateway-VPN / Branch-Office-VPN)
- End-to-End-VPN (Host-to-Host-VPN / Remote-Desktop-VPN)

End-to-Site-VPN / Remote-Access-VPN

End-to-Site-VPN beschreibt ein VPN-Szenario, bei dem Heimarbeitsplätze oder mobile Benutzer (Außendienst) in ein Unternehmensnetzwerk eingebunden werden. Der externe Mitarbeiter soll so arbeiten, wie wenn er sich im Netzwerk des Unternehmens befindet. Man bezeichnet dieses VPN-Szenario auch als Remote Access.
Die VPN-Technik stellt eine logische Verbindung, den VPN-Tunnel, zum entfernten lokalen Netzwerk über ein öffentliches Netzwerk her. Hierbei muss ein VPN-Client auf dem Computer des externen Mitarbeiters installieren sein.
Im Vordergrund steht ein möglichst geringer, technischer und finanzieller Aufwand für einen sicheren Zugriff auf das entfernte Netzwerk.

Site-to-Site-VPN / LAN-to-LAN-VPN/ Branch-Office-VPN

Site-to-Site-VPN und LAN-to-LAN-VPN, oder auch Branch-Office-VPN genannt, sind VPN-Szenarien, um mehrere lokale Netzwerke von Außenstellen oder Niederlassungen (Filialen) zu einem virtuellen Netzwerk über ein öffentliches Netz zusammenzuschalten.
Netzwerke, die sich an verschiedenen Orten befinden lassen sich über eine angemietete Standleitung direkt verbinden. Diese Standleitung entspricht in der Regel einer physikalischen Festverbindung zwischen den beiden Standorten. Bei Festverbindungen, Frame Relay und ATM kommen je nach Anzahl, Entfernung, Bandbreite und Datenmenge sehr schnell hohe Kosten zusammen.
Da jedes Netzwerk in der Regel auch eine Verbindung zum Internet hat, bietet es sich an, diese Internet-Verbindung zur Zusammenschaltung von zwei oder mehr Netzwerken mit VPN-Technik (LAN-to-LAN-Kopplung) zu nutzen. Bei VPNs über das Internet entstehen nur die Kosten, die für den Internet Service Provider zu bezahlen sind.

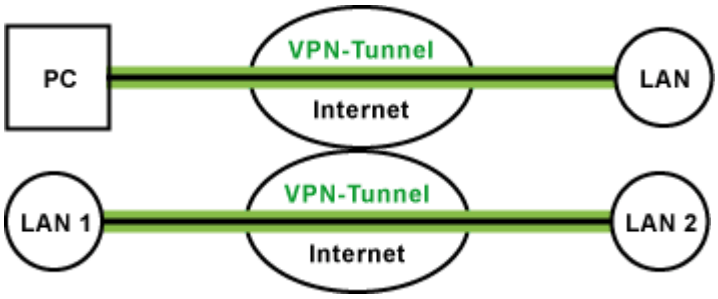
Virtuelle private Netze (VPN) werden immer öfter über das Internet aufgebaut. Das Internet wird so zur Konkurrenz zu den klassischen WAN-Diensten der Netzbetreiber. VPNs lassen sich über das Internet billiger und flexibler betreiben.

Eine Variante von Site-to-Site-VPN ist das Extranet-VPN. Während ein Branch-Office-VPN nur mehrere lokale Netzwerke einer Firma verbindet, ist ein Extranet-VPN ein virtuelles Netzwerk, das die Netzwerke unterschiedlicher Firmen miteinander verbindet. In der Regel geht es darum bestimmte Dienste fremder Unternehmen ins eigene Netzwerk zu integrieren oder Dienste für fremde Unternehmen anzubieten. Zum Beispiel für Geschäftspartnern, Lieferanten und Support-leistenden Unternehmen. Dabei gewährt man dem externen Unternehmen Zugriff auf Teilbereiche des eigenen Netzwerks. Die Zugriffsbeschränkung erfolgt mittels einer Firewall zwischen dem lokalen Netzwerk und dem Dienstenetzwerk. Extranet-VPNs ermöglichen eine sichere Kommunikation bzw. einen sicheren Datenaustausch zwischen den beteiligten Unternehmen.

End-to-End-VPN / Host-to-Host-VPN / Remote-Desktop-VPN

End-to-End-VPN beschreibt ein VPN-Szenario, bei dem ein Client auf einen anderen Client in einem entfernten Netzwerk zugreift. Hierbei deckt der VPN-Tunnel die gesamte Verbindung zwischen zwei Hosts ab. Auf beiden Seiten muss eine entsprechende VPN-Software installiert und konfiguriert sein. In der der Regel ist der Verbindungsaufbau nur durch die Unterstützung einer zwischengeschalteten Station möglich. Das bedeutet, eine direkter Verbindungsaufbau ist nicht möglich. Statt dessen bauen beide Seiten eine Verbindung zu einem Gateway auf, dass die beiden Verbindungen dann zusammenschaltet.
Typische Anwendung eines End-to-End-VPN ist Remote-Desktop über öffentliche Netze. Während RDP und VNC sich wegen der fehlenden Verschlüsselung nur für den Einsatz in lokalen Netzwerken eignet, gibt es für Remote-Desktop-VPNs meist nur propritäre und kommerzielle Lösungen. Zum Beispiel Teamviewer und GotoMyPC.

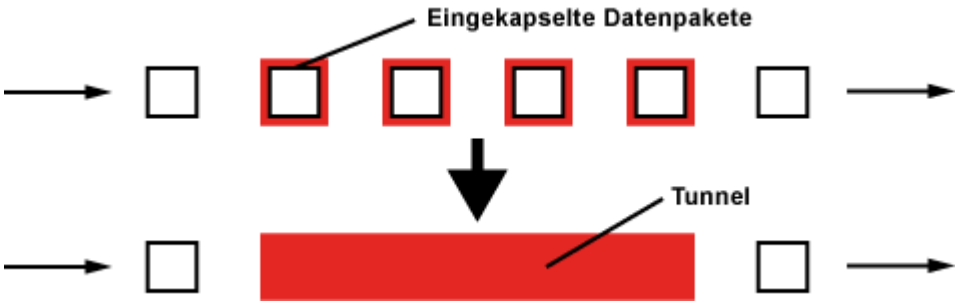
Tunneling / Tunnelmodus / Transportmodus



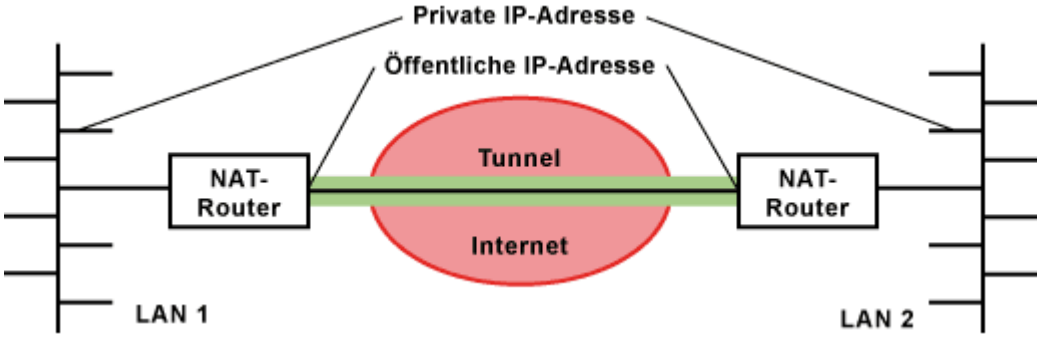
Um eine gesicherte Datenübertragung über das unsichere Internet zu gewährleisten, wird mit einem Tunneling-Protokoll eine verschlüsselte Verbindung, der VPN-Tunnel, aufgebaut. Der Tunnel ist eine logische Verbindungen zwischen beliebigen Endpunkten. Meist sind das VPN-Clients, VPN-Server und VPN-Gateways. Man nennt diese virtuellen Verbindungen Tunnel, weil der Inhalt der Daten für andere nicht sichtbar ist.
Einzelne Clients bindet man in der Regel per Tunnelmodus an. Für LAN-to-LAN-Kopplungen setzt man in der Regel den Transportmodus ein.

Tunneling-Protokolle (VPN)

Das Internet hat den Nachteil, dass die Infrastruktur im Detail nicht bekannt ist und der Weg zwischen zwei Kommunikationspartnern nicht nachvollziehbar, vorhersagbar und kontrollierbar ist. So kann an jedem Knoten ein Datenpaket gespeichert, verändert oder gelöscht werden. 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 Datenpakete 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.
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 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 bestimmtes Tunneling-Protokoll für die eine oder andere Anwendung besser oder schlechter.

	IPsec	**L2TP**	**PPTP**	**MPLS**
OSI-Schicht	Schicht 3	Schicht 2	Schicht 2	Schicht 2
Standard	Ja	Ja	Nein	Ja
Paketauthentisierung	Ja	Nein	Nein	Nein
Benutzerauthentisierung	Ja	Ja	Ja	Nein
Datenverschlüsselung	Ja	Nein	Ja	Nein
Schlüsselmanagement	Ja	Nein	Nein	Nein
Quality of Service	Ja	Nein	Nein	Ja
IP-Tunneling	Ja	Ja	Ja	Ja

IPX-Tunneling	Nein	Ja	Ja	Ja

6. SAN

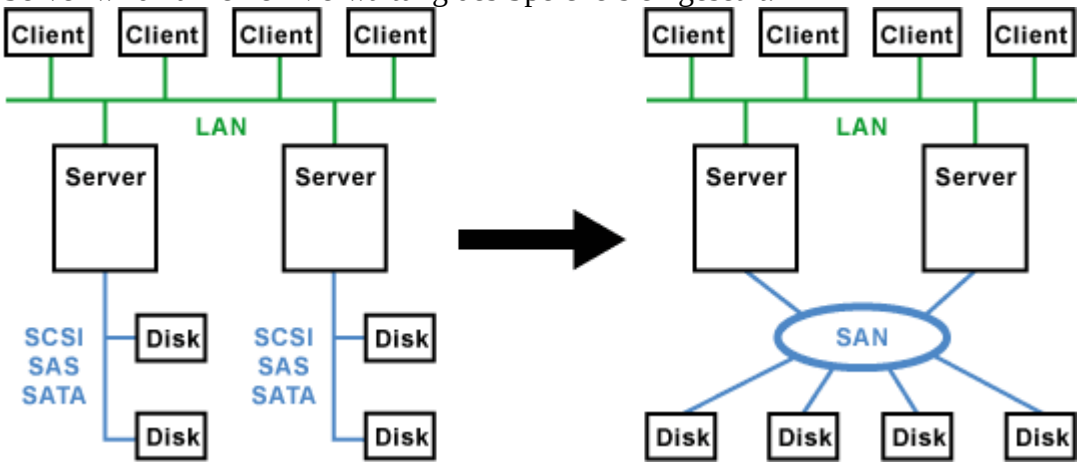
SAN - Storage Area Network

Ein Storage Area Network (SAN) ist ein Datenspeicher-Netzwerk in dem große Datenmengen gespeichert und bewegt werden. Im SAN wird der gesamte Speicher, unabhängig von Standort und Betriebssystem, zentral verwaltet und zu virtuellen Einheiten zusammengefasst. Der Zugriff auf den Speicher erfolgt über Server, die für die Verwaltung der Laufwerke zuständig sind. Die Laufwerke müssen dabei nicht am gleichen Ort sein, wie die Server.

Das Ziel von SAN ist auch die Zusammenfassung der einzelnen Festplatten der Servern, zu wenigen großen Speichergeräten, die von allen Servern über das Speichernetz gemeinsam genutzt werden. Das bedeutet, dass der gesamte Speicher als ein Block zur Verfügung steht und nicht auf verschiedenen Servern hier und da ein paar freie Gigabyte verstreut sind. In einem SAN lässt sich freier Speicherplatz flexibler den einzelnen Servern zuweisen. Das vereinfacht die Verwaltungsaufgabe.

SAN-Architektur

Speichernetze entkoppeln Server und Laufwerke. So kann man den Speicher besser skalieren. Der Server wird zur reinen Verwaltung des Speichers eingesetzt.



Das Storage Area Network ist so ausgelegt, dass es parallel zum LAN betrieben wird. Das SAN stellt sich dem LAN als ein gesamter Massenspeicher zur Verfügung, obwohl das SAN aus vielen kleinen Speichern bestehen kann. Das SAN ist für die schnelle Datenübertragung zwischen den einzelnen Speichern und Servern optimiert. So ist es möglich, die Datensicherung im SAN während des laufenden Betriebs zu erledigen, ohne dass es zu Überlastungen und Verzögerungen im LAN kommt. Die Server sehen das SAN als eine Art Datenpool, der in voneinander getrennten

logischen Einheiten aufgeteilt ist. Mehrere redundante Wege zwischen dem Anwender und den Daten schützen vor möglichen Ausfällen und Datenstaus.

Die Systemarchitektur eines SAN wirkt auf Außenstehende vergleichsweise komplex. In der Regel unterscheidet man zwischen Übertragungssystemen, Zugriffsprotokollen, Tunneling- und Transport-Protokollen. Die Unterschiede sind meist fließend, weil einige Techniken aufgabenübergreifende Funktionen haben.

Übertragungsmedien für SAN

Um Datensicherheit und Übertragungsleistung garantieren zu können, ist das SAN getrennt vom herkömmlichen Netzwerk (LAN) aufgebaut. Um Server und Laufwerke miteinander zu verbinden, gibt es verschiedene Schnittstellen.

- Fibre Channel (FC-0, FC-1, FC-2)
- iSCSI
- Ethernet / Fast-Ethernet / Gigabit-Ethernet
- Infiniband

Obwohl Fibre Channel (FC) sich als Übertragungsmedium für SAN durchgesetzt hat, kommen auch andere Techniken in Frage. Fibre Channel hat jedoch eine Nutzdatenauslastung von 90%, während z. B. Ethernet nur zwischen 20 und 60% der maximal möglichen Übertragungsrate mit Nutzlast belegen kann.

Zugriffsprotokolle für die Anwendungen

- SCSI
- Fibre Channel Protocol (FCP)
- Internet SCSI (iSCSI)
- Internet FCP (IFCP)

Gateway- und Tunneling-Protokolle

- IP over Fibre Channel (IPFC)
- Fibre Channel over IP (FCIP)

Transport-Protokolle

- Fibre Channel (FC-2, FC-3)
- TCP/IP
- UDP/IP

7. DHCP

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

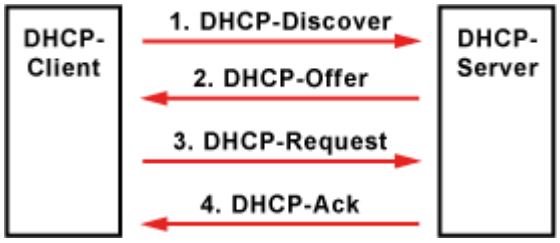
In den ersten IP-Netzen wurden IP-Adressen noch von Hand vergeben und fest in die Systeme eingetragen. Die dazu erforderliche Dokumentation war jedoch nicht immer fehlerfrei und schon gar nicht aktuell und vollständig. Der Ruf nach einer einfachen und automatischen Adressverwaltung wurde deshalb besonders bei Betreibern großer Netze laut. Hier war sehr viel Planungs- und Arbeitszeit notwendig. Deshalb wurde DHCP entwickelt.
Mit DHCP kann jede Host die Adresskonfiguration von einem DHCP-Server anfordern und sich selber automatisch konfigurieren. So müssen IP-Adressen nicht mehr manuell verwaltet und zugewiesen werden.

DHCPv6 / DHCP für IPv6

Bei IPv6 benötigt die IP-Konfiguration eigentlich keinen DHCP-Dienst. Dafür gibt es die Stateless Address Autoconfiguration (SLAAC). Doch nicht alle IPv6-Clients können den DNS-Server auf diese Weise entgegennehmen (RDNSS-Option). DHCPv6 ist im Prinzip das einzige Verfahren, welches diese und weitere Angaben innerhalb der Autokonfiguration ergänzen kann. Um wie bei IPv4 mit DHCPv4 die gleichen Funktionalitäten für IPv6 zu ermöglichen, wurde DHCPv6 definiert.

- DHCPv6 (Stateful Address Configuration)

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-Gateways es gibt. In der Regel ist der DHCP-Server ein Router.

Wird ein Host mit eine aktivierten DHCP-Client gestartet, wird ein funktional eingeschränkter Modus des TCP/IP-Stacks gefahren. Dieser hat keine gültige IP-Adresse, keine Subnetzmaske und kein Standard-Gateway. Das einzige, was der Client machen kann, ist IP-Broadcasts verschicken. 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.

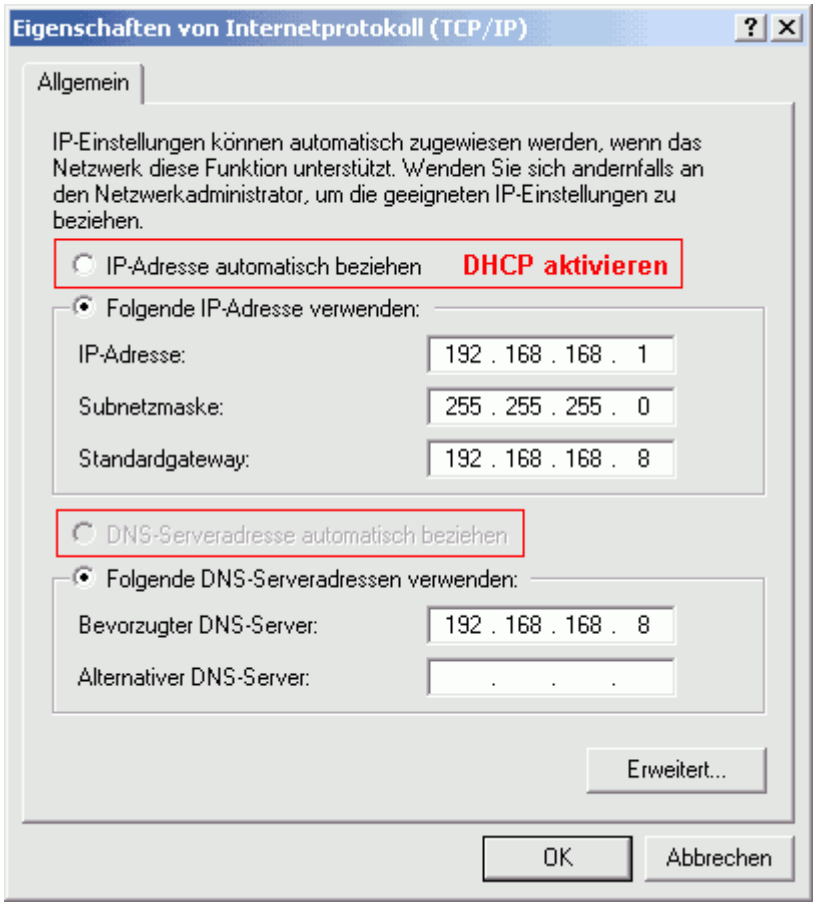
Mit DHCP werden nicht nur die IP-Adressen verteilt. Bei der Gelegenheit werden weitere Parameter übergeben, um die IP-Konfiguration im Client zu vervollständigen. Jeder angesprochene DHCP-Server schickt ein UDP-Paket mit folgenden Daten zurück:

- 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

Konfiguration des DHCP-Clients unter Windows 2000



Die Konfiguration des DHCP-Clients unter Windows ist in der Regel gar nicht notwendig. Meistens ist er bereits aktiviert. Sofern ein DHCP-Server installiert ist, holt sich das Betriebssystem die notwendigen Daten selber.
Wurden die TCP/IP-Konfiguration von DHCP vorgenommen können die Daten mit dem Befehl **ipconfig** auf der Kommandozeile bzw. MS-DOS-Eingabeaufforderung von Windows eingesehen werden.

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>ipconfig

Windows-IP-Konfiguration

Ethernetadapter LAN-Verbindung:

Verbindungsspezifisches DNS-Suffix: t-online.de
IP-Adresse. . . . . : 192.168.168.11
Subnetzmaske. . . . . : 255.255.255.0
Standardgateway . . . . . : 192.168.168.8

8. TCP/IP

TCP/IP ist eine Protokoll-Familie für die Vermittlung und den Transport von Datenpaketen in einem dezentralen Netzwerk. Die Abkürzung TCP/IP steht für die beiden Protokolle Transmission Control Protocol (TCP) und Internet Protocol (IP).
Der Erfolg des Internets ist zum großen Teil auch TCP/IP zu verdanken. TCP/IP ist ein weltweit Netzwerk-Standard im LAN (Local Area Network) und WAN (Wide Area Network).

Die wesentliche Funktion von TCP/IP ist dafür Sorgen zu tragen, dass Datenpakete innerhalb eines dezentralen Netzwerks beim Empfänger ankommen. Weil Datenpakete auf den unteren Übertragungsschichten verloren gehen können, fordert TCP/IP gegebenenfalls Datenpakete noch einmal an. Ebenso findet TCP/IP Stationen über Netze hinweg, auch wenn deren Standort nicht bekannt ist.

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

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

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.

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

- 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.

IP - Internet Protocol

Das Internet Protocol, kurz IP, 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. die IP-Adresse dient nicht nur zur Adressierung einzelner Stationen, sondern ganzer Netze. Beim IP-Routing geht es nicht darum, Datenpakete an bestimmte Stationen zu schicken, sondern die Pakete ins richtige Netzwerk zu leiten.
IP nimmt die Datenpakete von TCP entgegen, teilt sie entsprechend der Vorgaben des Übertragungsmediums noch einmal auf, versieht sie mit einer Adresse und übergibt sie an den Netzwerk-Adapter. Der Empfänger nimmt die Pakete entgegen und übergibt sie an TCP.

- IPv4 - Internet Protocol Version 4
- Subnetting
- IP-Routing
- DHCP - Dynamic Host Configuration Protocol
- NAT - Network Address Translation

- IPv6 - Internet Protocol Version 6
- IPv6-Adressen
- SLAAC - Stateless Address Autoconfiguration
- Übergangsverfahren von IPv4 auf IPv6

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, die Dateien oder den Datenstrom von den Anwendungen entgegen zu nehmen, aufzuteilen, mit einem Header zu versehen und an das Internet Protocol (IP) zu übergeben.
TCP sorgt auch dafür, dass diese Pakete der richtigen Anwendung zugeordnet werden können. Beim Empfänger werden die Datenpakete in die richtige Reihenfolge gebraucht, wieder zusammengesetzt und der Anwendung übergeben. Die Zuordnung erfolgt über eine Portnummer. Durch die Ports ist es möglich, dass mehrere Anwendungen gleichzeitig Verbindungen zu unterschiedlichen Kommunikationspartnern aufbauen können.
Der kleine Bruder von TCP ist UDP, dass ein abgespecktes Transport-Protokoll ist.

TCP - Transmission Control Protocol

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

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

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

Funktionen von TCP

- Sequenzierung
- Verbindungsmanagement
- Flusskontrolle
- Zeitüberwachung
- Fehlerbehandlung

Funktionsweise von Sequenzierung, Verbindungsmanagement und Fehlerbehandlung

Die Funktionsweise von TCP besteht darin, den Datenstrom verschiedener Anwendungen aufzuteilen (Sequenzierung). Die Pakete werden mit einem Header zu versehen, in dem Steuer- und Kontroll-Informationen enthalten sind. Danach wird das Paket an das Internet Protocol (IP) übergeben. Die Größe der Pakete wird an die physikalischen Eigenschaften des Übertragungsmediums angepasst (Maximum Transmission Unit). Beim Empfänger werden die Datenpakete in die richtige Reihenfolge gebracht und an die adressierte Anwendung übergeben.

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

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

TCP hat 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.
TCP nutzt freie Übertragungskapazität aus. Diese Steuerung findet in den Endgeräten statt. Ein Problem ist das dann, wenn Anwendungen einfach mehrere TCP-Verbindungen öffnen. Die Zuteilungsregeln von TCP können Übertragungsstrecken überlasten.

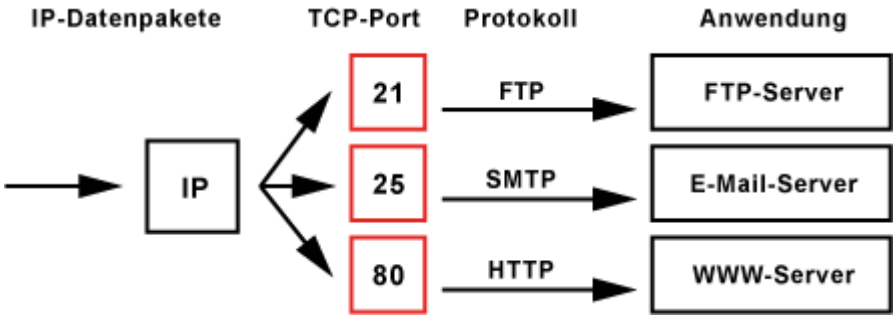
Windows-Size

TCP arbeitet mit einer Windows-Size von etwa 64 kByte/s. Doch die Datenpakete können nur mit einer bestimmten Maximalgeschwindigkeit transportiert werden. Nach jedem Paket wartet TCP beim Sender auf ein ACK (Bestätigung) vom Empfänger. In dieser Zeit ist die Verbindung ungenutzt. Im ungünstigsten Fall wartet TCP länger auf die Bestätigung als die Datenübertragung dauert.
Um das zu vermeiden, wird die Windows-Size so groß gewählt, dass die ungenutzte Zeit möglichst klein ist. Dabei steigt jedoch das Risiko, dass bei einem Datenverlust, ein Datenpaket noch mal übertragen werden muss.
Um die Wartezeiten zwischen Datenpaketen, Bestätigungen und nächsten Datenpaketen zu reduzieren, werden mehrere Datenpakete hintereinander verschickt (Sliding Window). Die Bestätigungen treffen dann mit Verzögerung ein. Weitere Datenpakete werden aber nur dann verschickt, wenn auch vorhergehenden Datenpakete bestätigt wurden.

Der kleine Bruder: UDP - User Datagram Protocol

Neben dem verbindungsorientierten TCP gibt es auch das verbindungslose und unsichere UDP. Das User Datagramm Protocol (UDP) ist ebenso auf der Schicht 4, der Transportschicht, des OSI-Schichtenmodells angeordnet. Es hat dieselbe Aufgabe wie TCP, nur das ihm nahezu alle Kontrollfunktionen fehlen und dadurch schlanker daher kommt und einfacher zu verarbeiten ist.

Zuordnung zwischen Datenpaket und Anwendung: Der TCP-Port



Datenpakete, die über IP ihr Ziel erreichen, werden von TCP zusammengesetzt an eine Anwendung übergeben. Da mehrere Anwendungen zugleich TCP-Verbindungen aufbauen können, muss eine Zuordnung zwischen Datenpaket und Anwendung erfolgen. Zu diesem Zweck wird eine Übergabekennung zwischen Daten und Anwendung definiert, die als Port bezeichnet wird. Es handelt sich dabei um eine fortlaufende Nummer zwischen 0 bis 65.535. TCP-Pakete sind mit diesen Port-Nummern (Sender- und Empfänger-Port) versehen, damit sie einer Anwendung zugeordnet werden können.

Die Port-Nummern, die für TCP und UDP gelten, werden von der IANA (Internet Assigned Numbers Authority) bzw. ICANN (Internet Corporation for Assigned Names and Numbers) verwaltet und vergeben.
Die Port-Nummern 0 bis 1.023 sind jeweils einer Anwendung, einem Dienst oder einem Anwendungs-Protokoll fest zugeordnet. Um Fehler und die damit einhergehende Fehlersuche zu vermeiden sollte diese Zuordnung nicht verändert werden.
Die Port-Nummern von 1.024 bis 49.151 sind zur Registrierung freigegeben. Im Prinzip kann sich jeder einen Port bei der IANA/ICANN für seine Anwendung reservieren, wenn er es begründen

kann.
Die darüberliegenden Port-Nummern, ab 49.152, können frei belegt werden, sofern sie gerade von keinem anderen Dienst belegt sind.

Wenn Anwendungen zu einem Server Kontakt aufnehmen wollen, dann vergibt TCP die festgelegte Nummer für den Empfänger-Port und vergibt einen freie Nummer für den Sender-Port. Wenn der Server die Daten erhalten hat und eine Antwort zurückschickt, dann werden die Port-Nummern vertauscht. Damit wird sichergestellt, dass die Daten nicht an eine falsche Anwendung übergeben werden.
Mit den Ports ist es möglich, dass mehrere Anwendungen gleichzeitig über das Netzwerk Verbindungen zu mehreren Kommunikationspartner aufbauen können.

TCP-Port-Übersicht

Well Known Ports	0 - 1.023	Diese Ports sind fest einer Anwendung oder einem Protokoll zugeordnet. Die feste Zuordnung ermöglicht eine einfachere Konfiguration durch den Benutzern. Er kommt so mit dem Protokoll TCP in Kontakt.
Registered Ports	1.024 - 49.151	Diese Ports sind für Dienste vorgesehen.
Dynamically Allocated Ports	49.152 - 65.535	Diese Ports werden dynamisch zugewiesen. Jeder Client kann diese Ports nutzen

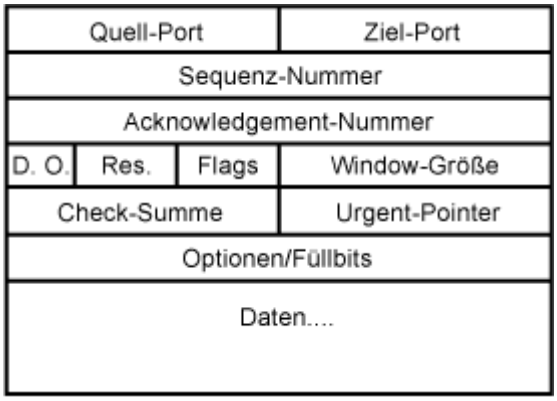
Beispiele für TCP-Ports

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

Was ist ein "offener Port"?

Was bedeutet es, wenn von einem "offenen Port" die Rede ist? Ein Port gilt dann als offen, wenn eine Anwendung an einem Port Datenpakete entgegennimmt, die an diesen Port geschickt werden, ohne dass die Anwendung dieses Datenpaket angefordert hat.
Ein Port wird dann "geöffnet", wenn eine Anwendung gestartet wird, die an diesem Port "lauscht".

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.

Bedeutung der Felder im TCP-Header

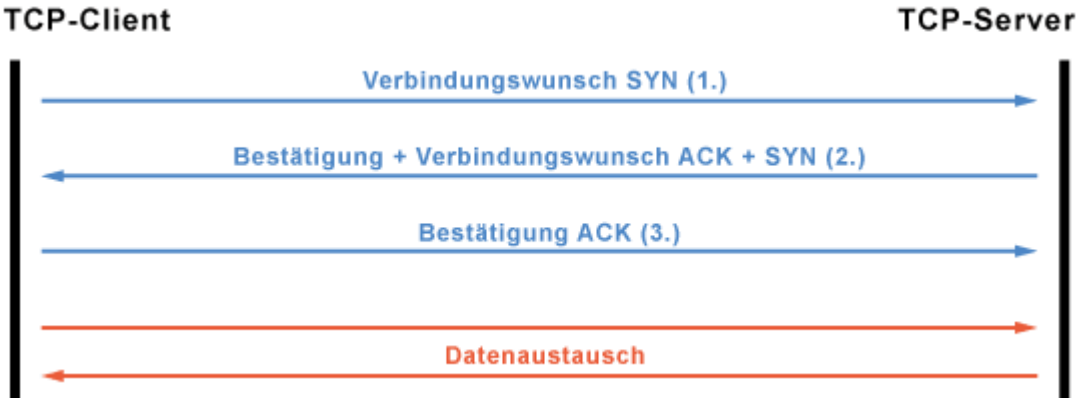
Feldinhalt	Bit	Beschreibung
Quell-Port (Source-Port)	16	Hier steht der Quell-Port, von der die Anwendung das TCP-Paket verschickt. Bei einer Stellenanzahl von 16 Bit beträgt der höchste Port 65.535.
Ziel-Port (Destination-Port)	16	Hier steht der Ziel-Port, über welchen das TCP-Paket der Anwendung zugestellt wird. Bei einer Stellenanzahl von 16 Bit beträgt der höchste Port 65.535.
Sequenz-Nummer	32	Bei jeder TCP-Verbindung werden Nummern zwischen den Kommunikationspartner ausgehandelt. Während der Verbindung werden diese Nummern verwendet um die TCP-Pakete eindeutig zu identifizieren.
Acknowledgement-Nummer	32	Alle Datenpakete werden bestätigt. Dazu dient das ACK-Flag und die Acknowledgement-Nummer, die sich aus der Sequenz-Nummer und der Anzahl von empfangenen Bytes errechnet. Damit kann der Sender feststellen, ob die Daten beim Empfänger vollständig angekommen sind.

Data Offset	4	Hier steht die Anzahl der 32-Bit-Blöcke des TCP-Headers. Die Mindestmenge beträgt 5.
Reserviert	6	Dieser Bereich ist auf 000000 gesetzt und für Erweiterungen des TCP-Headers gedacht.
Flags	6	Kennzeichnung bestimmter für die Kommunikation und Weiterverarbeitung der Daten wichtiger Zustände (URG, ACK, PSH, RST, SYN, FIN).
Window-Größe	16	Der Empfänger sendet dem Sender in diesem Feld die Anzahl an Daten, die der Sender senden darf. Dadurch wird das Überlaufen des Empfangspuffers beim Empfänger verhindert. Den Vorgang nennt man Windowing und dient der Datenflusssteuerung.
Check-Summe	16	Dieses Feld dient der Kontrolle von Header- und Datenbereich.
Urgent-Pointer	16	Zusammen mit der Sequenz-Nummer gibt dieser Wert die genaue Position der Daten im Datenstrom an. Der Wert ist nur gültig, wenn das URG-Flag gesetzt ist.
Optionen/Füllbits (Options/Padding), jeweils 32 Bit lang		Dieses Feld beinhaltet optionale Informationen. Um die 32-Bit-Grenze einzuhalten wird das Options-Feld mit Nullen aufgefüllt.

TCP-Flags zur Steuerung der Kommunikation

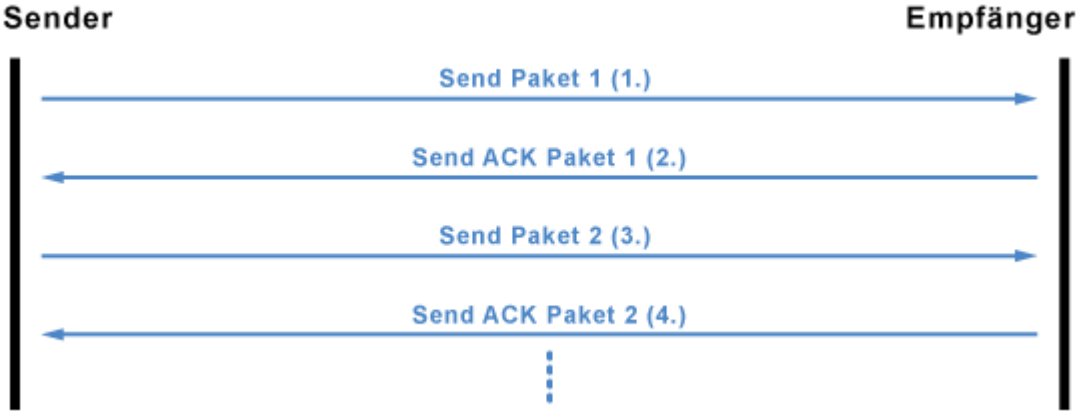
TCP-Flag	Beschreibung
Urgent-Pointer-Flag (URG-Flag)	Ist das URG-Flag gesetzt wird das Urgent-Pointer-Feld ausgewertet. Ein solches Datenpaket ist keiner Anwendung zugeordnet. Es hat eine besondere Priorität.
Acknowledgement-Flag (ACK-Flag)	Da sich die Acknowledgement-Nummer nicht bei jedem Datenpaket ändert, kennzeichnet ein gesetztes ACK-Flag die Gültigkeit der Acknowledgement-Nummer.
Push-Flag (PSH-Flag)	TCP puffert einzelne Datenpakete bis eine größere zusammenhängende Datenmenge vorhanden ist. Ist das PSH-Flag gesetzt, wird dieses Paket sofort an den TCP-Port weitergeleitet.
Reset-Flag (RST-Flag)	Ist ein Abbruch der TCP-Verbindung notwendig, wird das RST-Flag gesetzt. Es kommt auch zum Einsatz, wenn eine TCP-Verbindung abgewiesen wird.
Syncronization-Flag (SYN-Flag)	Das SYN-Flag wird gesetzt, wenn zwischen Sender und Empfänger eine Verbindung aufgebaut werden soll.
Final-Flag (FIN-Flag)	Sind zwischen zwei Stationen alle Daten übertragen, senden beide Stationen ein TCP-Paket mit gesetztem FIN-Flag. Danach gilt die TCP-Verbindung als beendet.

TCP-Verbindungsaufbau



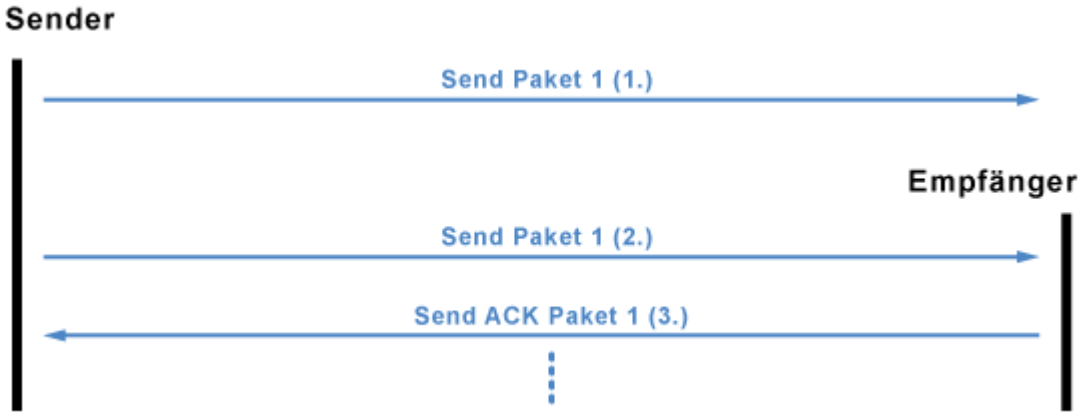
Der Verbindungsaufbau läuft nach dem Three-Way-Handshake ab. Zuerst schickt der Client an den Server einen Verbindungswunsch (SYN). Der Server bestätigt den Erhalt der Nachricht (ACK) und äußert ebenfalls seinen Verbindungswunsch (SYN). Der Client bestätigt den Erhalt der Nachricht (ACK). Danach erfolgt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

TCP-Datenaustasuch



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 der Datenaustausch 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 noch mal 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).

9. Subnetting

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 Host-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 Host-Anzahl in einem Subnetz adressierbar.

Hostanzahl	Subnetzmaske	32-Bit-Wert	Suffix
16.777.214	**255.0.0.0**	**1111 1111 0000 0000 0000 0000 0000 0000**	**/8**
8.388.606	255.128.0.0	1111 1111 1000 0000 0000 0000 0000 0000	/9
4.194.302	255.192.0.0	1111 1111 1100 0000 0000 0000 0000 0000	/10
2.097.150	255.224.0.0	1111 1111 1110 0000 0000 0000 0000 0000	/11
1.048.574	255.240.0.0	1111 1111 1111 0000 0000 0000 0000 0000	/12
524.286	255.248.0.0	1111 1111 1111 1000 0000 0000 0000 0000	/13
262.142	255.252.0.0	1111 1111 1111 1100 0000 0000 0000 0000	/14
131.070	255.254.0.0	1111 1111 1111 1110 0000 0000 0000 0000	/15
65.534	**255.255.0.0**	**1111 1111 1111 1111 0000 0000 0000 0000**	**/16**
32.766	255.255.128.0	1111 1111 1111 1111 1000 0000 0000 0000	/17
16.382	255.255.192.0	1111 1111 1111 1111 1100 0000 0000 0000	/18
8.190	255.255.224.0	1111 1111 1111 1111 1110 0000 0000 0000	/19
4.094	255.255.240.0	1111 1111 1111 1111 1111 0000 0000 0000	/20
2.046	255.255.248.0	1111 1111 1111 1111 1111 1000 0000 0000	/21
1.022	255.255.252.0	1111 1111 1111 1111 1111 1100 0000 0000	/22

510	255.255.254.0	1111 1111 1111 1111 1111 1110 0000 0000	/23
254	**255.255.255.0**	**1111 1111 1111 1111 1111 1111 0000 0000**	**/24**
126	255.255.255.128	1111 1111 1111 1111 1111 1111 1000 0000	/25
62	255.255.255.192	1111 1111 1111 1111 1111 1111 1100 0000	/26
30	255.255.255.224	1111 1111 1111 1111 1111 1111 1110 0000	/27
14	255.255.255.240	1111 1111 1111 1111 1111 1111 1111 0000	/28
6	255.255.255.248	1111 1111 1111 1111 1111 1111 1111 1000	/29
2	255.255.255.252	1111 1111 1111 1111 1111 1111 1111 1100	/30

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 an keinen Host 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 Host-Adresse.

	Dezimale Darstellung				**Binäre Darstellung (Bit)**			
IP-Adresse	192	.168	.0	.1	1100 0000	1010 1000	0000 0000	0000 0001
Subnetzmaske	255	.255	.255	.0	1111 1111	1111 1111	1111 1111	0000 0000
Netz-Adresse	192	.168	.0	.0	1100 0000	1010 1000	0000 0000	0000 0000
Host-Adresse	0	.0	.0	.1	0000 0000	0000 0000	0000 0000	0000 0001
Broadcast-Adresse	192	.168	.0	.255	1100 0000	1010 1000	0000 0000	1111 1111

Die Subnetzmaske wird also wie eine Schablone auf die IP-Adresse gelegt um die Netz-Adresse und Host-Adresse herauszufinden. Die Informationen über die Netz-Adresse ist wichtig bei der Zustellung eines IP-Datenpakets. Ist die Netz-Adresse bei der Quell- und Ziel-Adresse gleich, wird das Datenpaket innerhalb des gleichen Subnetzes zugestellt. Sind die Netz-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 / Subnetzmaske	192.168.0.1 / 255.255.255.0
IP-Adresse / Suffix	192.168.0.1 / 24

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

10. SNMP und RMON

SNMP - Simple Network Management Protocol

SNMP ist ein Protokoll zur Verwaltung und Steuerung von Netzwerken. Es ist für den Transport von Management-Informationen, Status- und Statistikdaten zwischen Netzwerkstationen und einem Management-System zuständig.

Bei der Einführung von TCP/IP wurde kurzfristig SNMP verwendet und sollte durch ein OSI-konformes Protokoll ersetzt werden. SNMP setzte sich jedoch innerhalb kürzester Zeit durch. Die Anpassung an die Anforderungen von OSI waren jedoch zu umfangreich. Deshalb wurden das neue Protokoll ausgesetzt. Stattdessen wurde kurzerhand SNMP, SMI und MIB zu den offiziellen Standards erklärt. Deshalb muss in allen verwaltbaren Netzwerk-Komponenten SNMP, SMI und MIB implementiert sein.

Netzwerk-Management

Mit zunehmender Tendenz werden immer mehr Anwendungen aus der Informations- und Kommunikationstechnik in betriebliche Arbeitsabläufe integriert. Dadurch entstehen immer größere und komplexere Netzwerke, an die immer mehr Anwendungen und Benutzer angeschlossen werden. Um Probleme und Störungen in einem Netzwerk frühzeitig erkennen und beseitigen zu können sind Elemente erforderlich, die ein Netzwerk verwalten und beobachten können. An dieser Stelle setzen Netzwerk-Management-Systeme an. Diese Systeme werden allgemein unter der Bezeichnung Netzwerk-Management-Technologie (NMT) zusammengefasst.

Architektur von SNMP

Die Architektur von SNMP trennt zwischen dem Manager, den Agenten, den Verwaltungsinformationen und dem Verwaltungsprotokoll. Der Manager ist eine Anwendung auf einem speziell dafür vorgesehenen Computer. Die Agenten sind die einzelnen Netzwerk-Komponenten. Sie führen die Management-Funktionen aus. Die Verwaltungsinformationen sind Informationen über das Netzwerk, der Konfiguration, dem Aufbau und den statistischen Daten. Das Verwaltungsprotokoll ist SNMP selber. Es tauscht die Verwaltungsinformationen und Daten zwischen dem Manager und den Agenten aus.
Der Ablauf zwischen Manager und Agenten ist immer der selbe. Der Manager schickt einen

Request an den Agenten. Dieser führt den Befehl aus und schickt einen Response zurück. Dieses Verfahren wird Polling genannt. Weiterhin existieren Trabs, die einen Agenten dazu veranlassen, unvorhergesehene Ereignisse an den Manager zu melden. Viele gleichzeitig versendete Traps können jedoch zur Überlastung des Managers führen. Deshalb sind Traps nur bei kritischen Ereignissen empfehlenswert. Um eine unnötige Netzwerkbelastung zu vermeiden, findet der Datenaustausch von SNMP über UDP statt.

SNMPv2

SNMPv1 hat nur IP, TCP und UDP unterstützt. Mit SNMPv2 kann SNMP auch auf anderen Protokollen, wie z. B. IPX, Appletalk und weitere OSI-Protokolle, eingesetzt werden. Neben den verbesserten Sicherheitsfunktionen und Werkzeugen zur Verwaltung verteilter Netze, ist es auch möglich mehrere Manager untereinander kommunizieren zu lassen.

11. MIB

MIB - Management Information Base

Die mit SNMP übertragenen Informationen und Daten müssen irgendwo abgelegt und gespeichert werden. Dazu dient die MIB. Die MIB ist mit einer Datenbank vergleichbar. In ihr werden hauptsächlich Daten gespeichert. Die Daten werden in Form von Objekten strukturiert in einer Art Baum abgelegt. Wegen den Bedürfnissen des Netzwerk-Managements wurde die Standard-MIB durch Erweiterungen angepasst. Daraus ergab sich die MIB II.
Wegen der steigenden Komplexität wurde SNMP und MIB durch die RMON-MIB (Remote Monitoring) erweitert.

12. RAID Level – auch kombinierte

RAID - Redundant Array of Independent Disk

RAID-Systeme sind Speicherkonzepte um Daten redundant zu speichern (RAID-Level 1) oder die Geschwindigkeit der Schreib- und Lesezugriffe zu steigern (RAID-Level 0). Dabei werden mehrere physikalische Festplatten zu einem logischen Laufwerk zusammen geschaltet. In der Regel geht es darum, sich vor dem Ausfall einer Festplatte zu schützen.
Bei einem RAID, kommt es auf die Verfügbarkeit von Daten an, in dem die Daten redundant gespeichert werden. Der Redundanz-Level drückt aus, wie viele Festplatten ausfallen dürfen, bis das ganze Array defekt ist.
Für spezielle Anforderungen, wo Datensicherheit und Geschwindigkeit gefragt sind, gibt es weitere RAID-Level, die aber nicht alle standardisiert sind.

Ein RAID kommt immer dann zum Einsatz, wenn folgende Ziele erreicht werden sollen:

- Datensicherheit erhöhen (Redundanz)
- Geschwindigkeit steigern
- oder beides zusammen

Drei Dinge die man über RAID wissen muss

1. Es gibt viele billige RAID-Varianten. Doch nur ein Hardware-RAID-Adapter schützt Daten ausreichend vor Hardware-Defekten.
2. Eine redundante Konfiguration macht nur dann Sinn, wenn es auf hohe Verfügbarkeit ankommt, die auch bei einem Plattendefekt erhalten bleiben muss. Mehr kann RAID nicht leisten. Die oft beworbenen Geschwindigkeitsvorteile sind in der Praxis meist nicht relevant.
3. RAID ersetzt kein Backup.

RAID-Prinzip

Ein RAID-Adapter oder ein Betriebssystem fassen mindestens zwei oder mehr Festplatten zu einem logischen Verbund zusammen. Für die Software sieht dieser Verbund wie ein einziges Laufwerk aus, das besondere Eigenschaften besitzt, die ein einzelnes Laufwerk nicht hat. Die Daten werden nach einem fest definierten Schema auf alle Festplatten verteilt. Dabei erfolgt die Arbeit des RAID unauffällig im Hintergrund.
Im Zusammenhang mit RAID und Speichersystemen (Storage) spricht man häufig von Arrays. Das ist die Bezeichnung von Festplatten, die zu einer logischen Einheit zusammen gefasst sind.

Was kann ein RAID nicht?

RAID hilft nur beim Ausfall einer Festplatte (nicht bei RAID 0). Wenn gleichzeitig eine zweite Festplatte ausfällt, dann hilft RAID nicht gegen Datenverlust (außer RAID 6). Deshalb gilt es bei einem Festplattenausfall schleunigst Ersatz zu beschaffen. Insbesondere dann, wenn man mehrere Festplatten aus der gleichen Produktion einsetzt. Wenn eines davon ausfällt, dann ist die Gefahr, dass ein anderes auch den Geist aufgibt relativ groß.
Auch schützt ein RAID nicht vor Viren, Würmern oder versehentlichem Löschen von Dateien. RAID erhöht die Ausfallsicherheit und damit die Verfügbarkeit des Speichersystems. Eine Datensicherung (Backup) kann kein RAID ersetzen.

RAID-Level

Mit RAID werden mehrere physikalische Festplatten zu einem großen logischen Laufwerk zusammen geschaltet. Die verschiedenen Möglichkeiten werden in RAID-Leveln definiert. Offiziell gibt es 8 RAID-Level, wobei nur die Level 0 bis 5 spezifiziert sind. Einige Hersteller haben weitere RAID-Level eingeführt, die in der Praxis aber nur in Ausnahmen eine Rolle spielen. So sind die RAID-Level 6 und 7 untereinander nur bedingt kompatibel. In der Praxis haben sich die RAID-Level 0, 1 und 5 durchgesetzt und reichen aus, um die meisten Anforderungen abzudecken. Die RAID-Level 2, 3 und 4 spielen in der Praxis keine Rolle.

RAID-Level	Lesegeschwindigkeit	Schreibgeschwindigkeit	Datensicherheit	Speicherkapazität
RAID 0	+ +	+ +	- -	+
RAID 1	+ +	+	+ +	- -
RAID 5	+	-	+	-

Bewertungen sind ein Vergleich zu einer einzelnen Platte (neutral oder Null).

- RAID 0: Nicht ausfallsicher, dafür schnelle Lese- und Schreibgeschwindigkeit
- RAID 1: Ausfallsicher, aber teuer
- RAID 5: Ausfallsicher, aber langsame Schreibgeschwindigkeit

RAID-Level im Vergleich

Betrieb	RAID 0	RAID 1	RAID 5	RAID 6
Redundanz	nein	ja	ja	ja
min. Datenträger	2	2	3	4
Rechenaufwand	sehr gering	sehr gering	mittel (XOR)	hoch
Datentransferrate	höher als Einzelplatte	beim Lesen höher als Einzelplatte	*abhängig vom Controller	*abhängig vom Controller
Kapazität bei 2 Platten	2	1	nicht möglich	nicht möglich
Kapazität bei 3 Platten	3	nicht möglich	2	nicht möglich
Kapazität bei 4 Platten	4	2	3	2
Kapazität bei 5 Platten	5	nicht möglich	4	3

* Je nach Implementierung bremst der Rechenaufwand für RAID 5 und 6 beim Schreiben. Das Lesen von mehreren Platten geht in der Regel schneller als von nur einer Platte.

Um die Datentransferrate von RAID 1, 5 und 6 zu steigern werden zwei RAID-Verbünde zu einem RAID 0 zusammengeschaltet. Dadurch entstehen ein RAID 10, 50 bzw. 60.

Einrichten von RAID

Der Einsatz eines RAIDs muss sorgfältig und durchdacht geplant werden. Es müssen zertifizierte RAID-Festplatten und zusätzlich eine kompatible Ersatzkarten für den Notfall beschafft werden. Und ganz wichtig, der Ernstfall muss vor dem Produktiveinsatz geprobt werden. Dazu muss das RAID mit Daten befüllt werden. Anschließend eine Festplatte entfernt und eine neue hinzugefügt werden. Danach sollte das RAID die neue Festplatte mit Daten bespielen (nicht bei RAID 0). Erst dann, wenn während dieser Aktion das RAID ohne Probleme weiterläuft, kann das System in den Produktiveinsatz gehen.
Beim Einsatz eines RAIDs macht man ganz automatisch neue Fehlerquellen auf. So ist die Wahrscheinlichkeit eines Bedienfehlers bei einem RAID höher, als bei einem einzelnen Laufwerk. Typische Fehler sind zum Beispiel, die falsche Festplatte zu tauschen oder falsche Software-

Optionen zu wählen. Manchmal fährt man besser, wenn man häufig Backups macht und ein Ersatzsystem bereitstellt.

Wenn es geplant ist, ein RAID zu einem späteren Zeitpunkt zu nutzen, dann sollte man sich vorher schon Gedanken darüber machen und mit den vorhandenen Komponenten beschäftigen. Unter Umständen muss ein bereits installiertes Betriebssystem noch mal neu aufgesetzt werden, weil sich die bestehende Festplatte nicht einfach so mit einer neuen Festplatte zu einem RAID-Verbund zusammenschließen lässt.
Zu beachten ist auch, ein richtig sicheres und schnelles RAID bekommt man nur mit Hardware-Unterstützung.

RAID-Festplatten

In einem RAID sollten grundsätzlich dauerbetriebstaugliche oder RAID-taugliche Festplatten (24x7) einsetzt werden. Solche Festplatten sind natürlich etwas teurer. Allerdings vibrieren sie weniger. Beim Betrieb mehrere Festplatten in einem Gehäuse können sich Festplatten sonst gegenseitig in Schwingung versetzen. Herkömmliche Festplatten sind wegen der hohen Spur- und Datendichte sehr empfindlich gegen Vibrationen. Höhere Latenzzeiten und im schlimmsten Fall Schreib- oder Lesefehler sind die Folge. In einem RAID führt das zu Fehlerkorrekturen, die das System verlangsamen können.
Grundsätzlich empfiehlt es sich Festplatten einzusetzen, die von der Geschwindigkeit und der Speicherkapazität gleichwertig sind. Man kann auch unterschiedliche Festplatten nehmen. Doch dann orientiert sich die Geschwindigkeit und Speicherkapazität an der kleinsten und langsamsten Festplatte. Sinnvollerweise nimmt man immer identische Festplatten.

Was, wenn eine Festplatte kaputt geht?

Wenn ein RAID 1 oder 5 nach langjähriger Betriebszeit einen Festplatten-Ausfall erleidet, dann sollte man das defekte Laufwerk nicht sofort tauschen. Tauscht man die defekte Platte aus, dann kommt es nicht selten vor, dass nach einem stressigen Rebuild weitere Platten ausfallen. Dann muss man das ganze Spiel wiederholen. Im schlimmsten Fall fällt eine andere Festplatte während des Rebuilds aus. Dann sind die Daten definitiv futsch. Deshalb gilt, RAID ersetzt kein Backup!
Wenn also bei einem RAID eine Festplatte ausfällt müssen zuerst die Daten auf den verbliebenen Festplatten gesichert und anschließend alle Festplatten des RAIDs ausgetauscht werden.
Bei einem RAID 6 kann man sich diese Vorgehensweise theoretisch sparen. RAID 6 kommt auch mit dem Ausfall einer zweiten Platte klar.

Hardware-RAID

Das klassische RAID ist das Hardware-RAID. Hier organisiert ein Mikroprozessor (RAID-Controller) auf dem RAID-Adapter die Datenverteilung auf die Festplatten. Der RAID-Controller ist so ausgelegt, dass er die Verteilung der Daten und die Berechnung der Prüfsummen selber ausführen kann und den Hauptprozessor nicht belasten muss.
Der RAID-Controller erscheint gegenüber dem Betriebssystem vollkommen transparent. Von der Zusammenschaltung der Festplatten bekommt das Betriebssystem nichts mit. Im Vergleich zum Zugriff auf eine einzelne Festplatte erkennt man auch als Anwender keinen Unterschied.
Bei der Konfiguration und im laufenden Betrieb bleiben beim Hardware-RAID keine Wünsche offen.

Software-RAID

Einige RAID-Level können auch mit Hilfe von Software realisiert werden. Für die Verteilung der Daten und der Berechnung der Prüfsummen ist dann der Hauptprozessor zuständig.
Die Betriebssysteme Linux, Windows (XP Pro, Vista, Server) und MacOS beherrschen einige RAID-Level. Linux erlaubt neben RAID 0, 1 und 5 auch noch RAID 4 und 6. MacOS beherrscht immerhin RAID 0 und 1. Windows Server beherrscht RAID 0, 1 und 5. Die Einzelplatz-Betriebssysteme von Microsoft nur RAID 0.

Host-RAID

Eine Zwischenstufe zwischen Hardware- und Software-RAID ist Host-RAID. Dazu zählen der RAID-Chipsatz, der sich auf manchen Motherboards befindet und auch einige günstige RAID-Adapter. Es gibt Motherboards, die sehr leistungsfähige RAID-Funktionen haben. Allerdings nicht immer so komfortabel, wie bei den RAID-Controllern (Hardware-RAID). Motherboards mit RAID-Funktion beherrschen meist nicht mehr als RAID 0, 1 und 5. Bei billigen Motherboards fehlt oft RAID 5.
Man spricht deshalb von Host-RAID, weil die RAID-Funktionen von der Firmware bzw. den Treibern erledigt werden. Aufwendige Berechnungen übernimmt der Hauptprozessor. Auffällig ist die hohe Belastung der CPU. Man bezeichnet diese Art von RAID auch als Fake-RAID.
Geht der RAID-Adapter kaputt, dann muss man einen kompatiblen, besser den gleich nachkaufen, um auf die Daten des RAID wieder zugreifen zu können.

Übersicht: RAID-Varianten

Bezeichnung	**Software-RAID**	**Host-RAID**	**USB-RAID**	**NAS mit RAID**
Controller-Chip	nein	ja	ja	ja
CPU-Berechnung	ja	ja	nein	nein
Performance	mittel	hoch	niedrig	niedrig
Alarmfunktion	nein	möglich	nein	ja
Kosten	integriert	gering	gering	hoch
Vorteile	Hardware-unabhängig	billig	billig	leicht erweiterbar
Nachteile	nur Windows	unzuverlässig	keine Warnfunktion	erschwerter Zugriff bei NAS-Defekt

Es gibt gute Gründe, warum häufig Hardware-Host-Adapter (nicht Host-RAID) eingesetzt werden. Nur ein Hardware-RAID schützt ausreichend vor Hardware-Defekten.

RAID im Desktop-Computer

In Anbetracht dessen, dass Festplatten eine immer größere Speicherkapazität haben und Systeme, die diese Speichermenge für ein Backup sichern können sehr teuer und aufwendig sind, ist ein RAID-System auch für Einzelplatzsysteme interessant. Vor allem im Privat-Bereich, wo Computer zum Speichern von wichtigen Schriftstücken, Fotos der Digitalkamera verwendet werden und manchmal mehrere Personen daran arbeiten, wird das regelmäßige Sichern der Daten auf CD, DVD oder externe Festplatten vernachlässigt. Eine fehlende Datensicherung von wichtigen Daten ist grob fahrlässig.
Ein RAID-System, z. B. RAID 1, schützt die Daten zumindest vor Verlust bei einem Festplattenausfall. Die wichtigsten Daten sollten zusätzlich auf einem externen Speichermedium, z. B. auf einer externen Festplatte, gesichert werden, um sie z. B. vor Viren oder versehentlichem Löschen eines unbedarften Anwenders zu schützen.
In Desktop-Computern hat sich RAID noch nicht durchgesetzt. Allerdings lassen sich viele Motherboards mit RAID onboard zu einem RAID-Speichersystem konfigurieren. Alternativ unterstützt fast jedes Betriebssystem Software-RAID.

Wenn es geplant ist, RAID zu einem späteren Zeitpunkt zu nutzen, dann sollte man sich vorher schon Gedanken darüber machen und mit den vorhandenen Komponenten beschäftigen. Unter Umständen muss ein bereits installiertes Betriebssystem noch mal neu aufgesetzt werden, weil sich die bestehende Festplatte nicht einfach so mit einer neuen Festplatte zu einem RAID-Verbund zusammenschließen lässt.

RAID-Level 0

Der RAID-Level 0 ist ein Festplatten-Verbund von zwei oder mehr Festplatten. Die Transferrate und Speicherkapazität der einzelnen Festplatten lassen sich einfach aufaddieren. Die 0 im RAID-Level steht für Null Daten-Redundanz. Die Daten werden nur abwechselnd auf zwei oder mehr Festplatten verteilt. Dadurch erhöht sich die Geschwindigkeit beim Lesen und Schreiben. Fällt jedoch eine Festplatte aus, sind alle Daten weg.

RAID-Level 1

Der RAID-Level 1 ist ein Festplatten-Verbund von zwei oder mehr Festplatten. Bei RAID 1 werden die Daten doppelt, also mindestens auf zwei Festplatten gespeichert. Man bezeichnet das als Datenspiegelung oder Mirroring. RAID 1 bietet so den bestmöglichen Schutz vor Datenverlust durch Festplattenausfall. Und beim Lesen von Daten hat man annähernd die doppelte Datentransferrate wie bei einem einzelnen Laufwerk.
Aber, die Kapazität eines RAID-Laufwerks beträgt die Hälfte der eingesetzten Laufwerke. Man muss also doppelt so viel Geld ausgeben oder man hat nur halb so viel Speicherkapazität, wie bei einem Laufwerk. Doppeltes Laufwerk bedeutet auch verdoppelter Stromverbrauch und verdoppelter Kühlaufwand.

RAID-Level 5

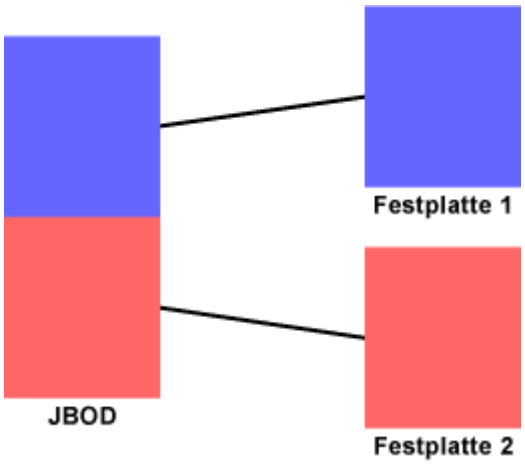
Der RAID-Level 5 ist ein Festplatten-Verbund von drei oder mehr Festplatten mit besonderen Eigenschaften, die eine einzelne Festplatte nicht hat.
Bei großen Datenmengen, die redundant gespeichert werden müssen, ist RAID 0 nicht akzeptabel und RAID 1 zu teuer, platzraubend und meistens überdimensioniert. Der RAID-Level 5 ist eine Weiterentwicklung aus den RAID-Leveln 3 und 4. Wie bei RAID 0 werden die Daten in Blöcke,

den Stripes, aufgeteilt und über die gesamte Festplatte verteilt.
Der RAID-Level 5 ist eine gute Kombination aus Datensicherheit und Speicherausnutzung. Bei 5 Festplatten beträgt die Speicherkapazität 80% von der Gesamtkapazität aller Festplatten.
Beim Ausfall einer Festplatte geht die Datentransferrate zurück, weil die Daten aus der Parität berechnet werden muss.

RAID-Level 6

Beim RAID-Level 6 wird wie bei RAID 5 auch mit Sector Striping gearbeitet. Zusätzlich wird ein Paritätslaufwerk verwendet, das über einen asynchronen Datenpfad und einen Cache verfügt. Bei RAID 6 speichert der Adapter gleich zwei Prüfsummen, sodass sich aus den Daten von verbliebenen Laufwerken die Daten rekonstruieren lassen.
Während RAID 5 nur den Ausfall eines Laufwerks verkraftet, verträgt RAID 6 den Ausfall von zwei bei mindestens 4 Laufwerken.

JBOD - Just a Bunch of Disks

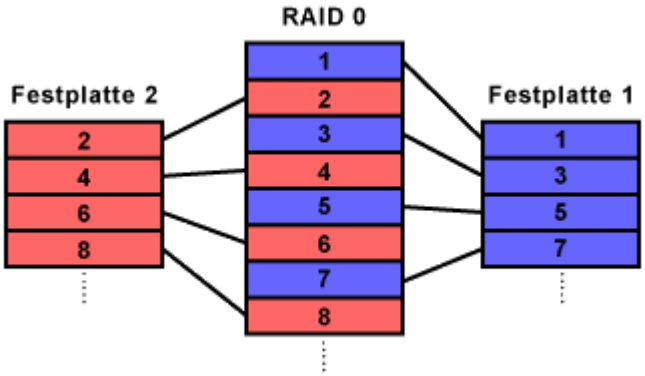


Die Bezeichnung JBOD, Linear Mode oder NRAID steht für Verschiedenes. Die einen bezeichnen damit mehrere einzeln ansprechbare Festplatten an einem Adapter. Die anderen bezeichnen damit eine Verkettung von Laufwerken. Das bedeutet, dass mehrere Festplatten zu einer großen zusammenhängenden Festplatte zusammengeschalten werden, in dem sie virtuell einfach hintereinander gehängt werden. Dieser Festplattenverbund sieht für das Betriebssystem wie ein einziges großes Laufwerk aus.
JBOD ermöglicht es ausschließlich mehrere Festplatten, auch unterschiedlicher Größe, zusammenzuschalten, um daraus ein einziges großes Laufwerk zu machen. Zum Beispiel um sehr große Dateien speichern zu können. Doch diese Zusammenschaltung hat mit RAID nichts zu tun. Fällt eine Festplatte aus, dann ist das gesamte Laufwerk aus Sicht des Betriebssystems defekt. Die Chance zur Rettung von Daten ist relativ gut, wenn auf den intakten Festplatten größere zusammenhängende Dateien liegen.

RAID-Level 0

Der RAID-Level 0 ist ein Festplatten-Verbund von zwei oder mehr Festplatten mit besonderen Eigenschaften, die eine einzelne Festplatte nicht hat. Die 0 im RAID-Level 0 steht für Null Daten-Redundanz. Weil die Daten abwechselnd auf zwei oder mehr Festplatten verteilt werden, bezeichnet man diesen RAID-Level auch als Striping.

Aufbau von RAID 0



Beim RAID-Level 0 werden zwei oder mehr Festplatten zu einem großen logischen Laufwerk zusammengeschaltet. Die Gesamtgröße des RAID richtet sich nach der kleinsten Festplatte mal der Anzahl der Festplatten. Deshalb empfiehlt es sich gleich große Festplatten zu verwenden.
Die Daten werden in Blöcken, typischerweise in der Größe von 64 oder 128 kByte, aufgeteilt (Stripe). Daher die Bezeichnung Striping. Ein Block von 128 kByte Daten wird in zwei 64 kByte Blöcke geteilt und wechselweise auf mindestens zwei Festplatten geschrieben.

Vorteile von RAID 0

Während eine Festplatte mit dem Speichern eines Datenblocks beschäftigt ist, wird durch den RAID-Controller bereits der nächsten Datenblock auf die nächste Festplatte geschrieben. Im Idealfall wird so der Zugriff auf das logische Laufwerk mit doppelter Geschwindigkeit erreicht. Auch beim Lesen der Daten von RAID 0 ist die Transferrate viel schneller als das Lesen von einer einzelnen Festplatte.
RAID 0 eignet sich also ausschließlich zur Geschwindigkeitssteigerung, allerdings gilt das nur bei sequenziellem Datentransfer. Beim sequenziellen Lesen und Schreiben von großen Dateien lassen sich alle Festplatten gleichzeitig nutzen. So addiert sich zumindest in der Theorie die Datentransferrate.

Nachteile von RAID 0

Man muss berücksichtigen, dass durch den Betrieb von zwei Festplatten die Gefahr für die Daten größer wird.
Fällt eine Platte aus, dann sind alle Daten weg, weil praktisch von jeder gespeicherten Datei nur noch die Hälfte lesbar ist. Wenn ein Teil einer Datei fehlt, kann der Rest der Datei nicht wiederhergestellt werden. Auch eine Datenrettung im klassischen Sinne ist in so einem Fall nicht mehr möglich.
Die Ausfallwahrscheinlichkeit liegt höher als bei einer einzelnen Festplatte. Sie steigt mit jeder zusätzlichen Festplatte im RAID-System.
Die Vorteile von RAID 0 (höhe Transferraten) wiegen die Nachteile (steigende Ausfallgefahr) nicht auf. Das Array ist defekt, wenn eine Festplatte kaputt geht oder der Controller oder das Betriebssystem beim Schreiben einen Fehler verursachen. Und auch im Fall eines Motherboard-Defekts lassen sich die Festplatten nicht ohne Weiteres in ein anderes System einbauen, um an die Daten zu kommen.

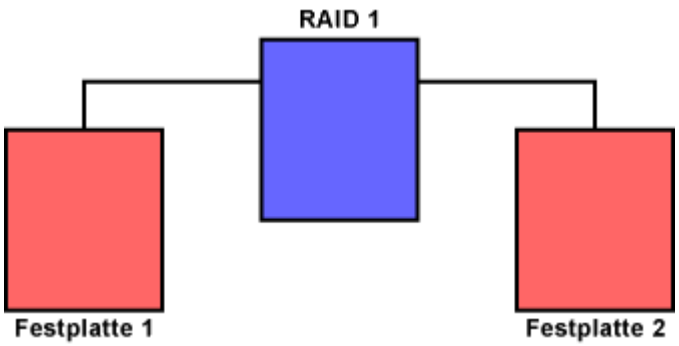
Anwendungen von RAID 0

Als Anwendung eignen sich Laufwerke mit temporären Daten, wie die Windows-Auslagerungsdatei oder die Swap-Partition von Linux. Auch große Datenmengen, die vor ihrer Weiterverarbeitung zwischengespeichert werden, lassen sich RAID 0 anvertrauen.
Im klassischen Server-Betrieb ist dieser RAID-Level ungeeignet. RAID 0 ist nur dann von Nutzen, wenn man höchste Schreib- und Lese-Geschwindigkeit braucht und gleichzeitig ein höheres Datenverlust-Risiko in Kauf nimmt.

RAID-Level 1

Der RAID-Level 1 ist ein Festplatten-Verbund von zwei oder mehr Festplatten mit besonderen Eigenschaften, die eine einzelne Festplatte nicht hat.
Bei RAID 1 werden die Daten doppelt, also mindestens auf zwei Festplatten gespeichert. Man bezeichnet das als Datenspiegelung oder Mirroring. RAID 1 bietet so den bestmöglichen Schutz vor Datenverlust durch Festplattenausfall.
Eine Variante davon ist RAID 1E. Es handelt sich dabei um Mirroring über 3 Festplatten.

Aufbau von RAID 1



Beim RAID-Level 1 werden zwei physikalische Festplatten zu einem logischen Laufwerk zusammengeschaltet. Der RAID-Controller legt alle Daten auf beiden Festplatten gleichzeitig ab, so dass beide Festplatten immer identische Werte haben. Bei RAID 1 müssen die Festplatten üblicherweise paarweise vorhanden sein. Die Kapazität des logischen Laufwerks wird durch die kleinste Festplatte vorgegeben. In der Regel verwendet man zwei identische Festplatten.
Eine Variante von RAID 1 ist das Duplexing, bei der jede Festplatte über einen eigenen Controller verfügt. Fällt ein Controller aus, kann das System mit dem zweiten Controller und der daran hängenden Festplatte weiterarbeiten.

Vorteile von RAID 1

Beim Schreiben ist das RAID nur so schnell, wie die langsamste Festplatte speichern kann. Beim Lesen ist RAID 1 zumindest schneller als eine einzelne Festplatte, da der Controller die Daten von der Festplatte ausgibt, die zuerst liefert. Wenn der RAID-Controller es schafft die Lesezugriffe intelligent auf beide Festplatten zu verteilen, dann kann sich dadurch theoretisch die Lesegeschwindigkeit verdoppeln. Fällt eine Festplatte aus, kann man mit der anderen ohne Daten- und einem geringen Geschwindigkeitsverlust weiter arbeiten.

Nachteile von RAID 1

Obwohl dieser RAID-Level 100% Redundanz ermöglicht, ist er auch der teuerste RAID-Level. Für den Speicherplatz ist praktisch immer der doppelte Preis zu zahlen. Oder man erhält für den gleichen Preis nur halb so viel Speicherplatz. Der Grund: Es steht nur die Hälfte der vorhandenen Speicherkapazität zur Verfügung. Zwei Festplatten mit jeweils 500 GByte wären zusammen 1.000 GByte. Weil RAID 1 die Daten spiegelt sind aber nur 500 GByte verfügbar.

Anwendungen von RAID 1

RAID 1 halbiert die zur Verfügung stehende Speicherkapazität. Dadurch ist es teuer. Im Gegenzug bietet es die größtmögliche Datensicherheit und -verfügbarkeit. Für kleine Server ist das praktikabel. Große Datenmengen speichert man besser mit höheren RAID-Leveln.

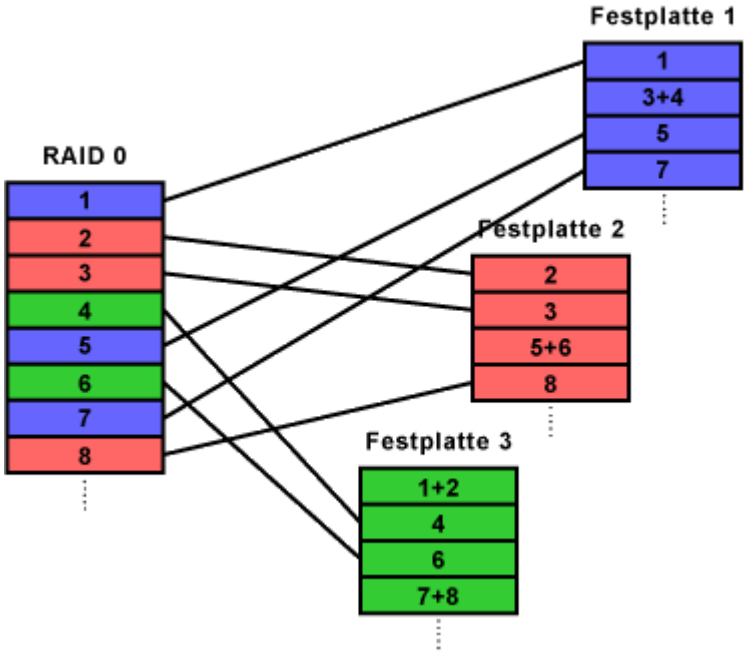
RAID-Level 10 / 0+1 - Mirrored Striping Array

RAID 10, das auch als RAID 0+1 bezeichnet wird, ist eine Kombination aus RAID 0 und RAID 1, also Striping und Mirroring. RAID 10 bietet die Vorteile von RAID 0 und RAID 1. Also gleichzeitig Datensicherheit und Geschwindigkeit. RAID 10 erfordert mindestens 4 Festplatten. Jeweils zwei der Festplatten werden zu einem RAID 1 zusammengeschaltet (gespiegelt), die dann zu einem RAID 0 zusammengefasst werden.
RAID 10 ist besonders geeignet um große Datenmengen redundant zu speichern. Doch auch hier braucht man die doppelte Anzahl von Festplatten, wie bei RAID 1.

RAID-Level 5 (2 / 3 / 4)

Der RAID-Level 5 ist ein Festplatten-Verbund von drei oder mehr Festplatten mit besonderen Eigenschaften, die eine einzelne Festplatte nicht hat.
Bei großen Datenmengen, die redundant gespeichert werden müssen, ist RAID 0 nicht akzeptabel und RAID 1 zu teuer, platzraubend und meistens überdimensioniert. Der RAID-Level 5 ist eine Weiterentwicklung aus den RAID-Leveln 3 und 4. Wie bei RAID 0 werden die Daten in Blöcke, den Stripes, aufgeteilt und über die gesamte Festplatte verteilt.
Der RAID-Level 5 ist eine gute Kombination aus Datensicherheit und Speicherausnutzung. Bei 5 Festplatten beträgt die Speicherkapazität 80% von der Gesamtkapazität aller Festplatten.

Aufbau von RAID 5: Block Striping mit verteilter Parität



Bei RAID 5 müssen mindestens 3 Festplatten vorhanden sein. Zur Steigerung der Gesamtkapazität des logischen Laufwerks können auch mehr Festplatten eingebunden werden.
Bei drei Festplatten wird ein Datenblock von 128 kByte in zwei Datenblöcke von 64 kByte geteilt. Aus den beiden Datenblöcken wird die Paritätsinformation gebildet, die einem dritten Block von 64 kByte entspricht. Die Parität ist das Ergebnis einer Exklusiv-Oder-Verknüpfung (XOR) der Datenblöcke eines Sektors. Die Parität wird aus Sicherheitsgründen nicht auf einem separaten Laufwerk gespeichert, sondern gleichmäßig auf alle Festplatten zwischen den Datenblöcken verteilt (Rotating Parity). Das Schreiben verzögert sich jedoch bei RAID 5. Vor dem Schreiben muss zuerst ein Lesezugriff erfolgen, damit die Paritätsinformation berechnet und danach wieder geschrieben werden kann.
Wenn eine Festplatte ausfällt, dann werden die fehlenden Datenblöcke aus den Paritätsblöcken vom Controller während der Laufzeit rekonstruiert. Wird die defekte Festplatte ausgetauscht, dann errechnet der Controller die fehlenden Daten aus der Parität und beschreibt damit die neue Festplatte. Dieser Vorgang kann einige Zeit dauern. Zusätzliche Schreib- und Lesezugriffe können die Rekonstruktion verlangsamen.

Vorteile von RAID 5

Die Daten sind vergleichsweise sicher gespeichert, solange bis eine Festplatte ausfällt. Dann müssen die Paritätsinformationen benötigt, um die fehlenden Daten zu rekonstruieren. Im Vergleich zu RAID 1 wird die Speicherkapazität besser ausgenutzt.

Nachteile von RAID 5

Der Hauptnachteil von RAID 5 ist die Notwendigkeit bei jedem Schreibzugriff den Paritäts-Sektor auszulesen, neu zu berechnen und wieder zu speichern. Daraus ergibt sich eine langsame Schreibgeschwindigkeit im Vergleich zu anderen RAID-Leveln. Doch Dank geschickter Paritätsberechnung und Puffern von Daten ist RAID 5 auch beim Schreiben vergleichsweise schnell.
Der zweite, aber weniger schwerwiegende Nachteil ist der Kapazitätsverlust durch die Speicherung

der Paritätsinformationen.
Wichtig zu wissen: Fällt im RAID 5 eine Festplatte aus, so sind die Daten in höchstem Maße gefährdet. Denn fällt noch eine Festplatte aus, so sind die Daten endgültig verloren. Ein RAID 5 verkraftet den Ausfall einer zweiten Festplatte nicht.

Lese- und Schreibgeschwindigkeit bei RAID 5

Zumindest in der Theorie kann ein RAID 5 aus drei Festplatten auch die Geschwindigkeit steigern. Es kann aber auch sein, dass der RAID-Verbund langsamer ist als eine einzelne Festplatte. Warum ist das so?
Ein RAID 5 aus drei Festplatten kann bei sequenziellen Transfers theoretisch doppelt so schnell arbeiten wie eine einzelne Festplatte. Doch nicht alle RAID-Controller beherrschen die Paritätsberechnung und das Verteilen oder Anfordern der Daten so schnell, dass sie Geschwindigkeit auch tatsächlich erreicht wird. Gerade günstige RAID-Controller sind bei RAID 5 und sequentiellen Transfers langsamer als eine einzelne Festplatte.
Auch bei verstreuten Zugriffen auf viele kleine Dateien bringt ein RAID 5 nicht mehr Geschwindigkeit. Die Positionierung der Schreib-/Lese-Köpfe der Festplatten verschlingt viel Zeit. Ein RAID 5 ist dann nicht schneller als eine einzelne Festplatte.

Anwendungen von RAID 5

Wegen der geringeren Schreibgeschwindigkeit eignet sich RAID 5 am ehesten bei großen Datenmengen mit kleinen Dateien. Mit nur drei Festplatten kann man sich sehr effizient gegen Ausfall einer Festplatte schützen. Mit dem Einsatz von mehr Festplatten lässt sich der nutzbare Anteil der Speicherkapazität gegenüber der Parität erhöhen.

RAID-Level 2

Beim RAID-Level 2 werden die Festplatten wie bei RAID 0 zu einem großen logischen Laufwerk zusammengeschaltet. Dort werden die Datenblöcke gespeichert. Zusätzlich werden aus den Datenblöcken mit dem Hamming-Code Prüfsummen errechnet. Der Hamming-Code erlaubt die Rekonstruktion fehlerhafter oder fehlender Bits.
Für ein 8-Bit-Datenwort werden 3-Bit zusätzlicher Speicherplatz benötigt. Dieser wird auf einem zusätzlichen Laufwerk bereitgestellt. Die Redundanz beträgt etwa 28%.
Die Schreibgeschwindigkeit wird durch die Prüfsummenbildung und deren Speicherung gebremst. Besonders bei kleinen Datenblöcken ist das System langsam.
RAID 2 ist nicht beliebig skalierbar. Zusätzliche Daten-Festplatten benötigen zusätzlichen Speicherplatz für die Prüfsummen.

RAID-Level 3

Beim RAID-Level 3 werden die Festplatten wie bei RAID 0 zu einem großen logischen Laufwerk zusammengeschaltet. Dort werden die Daten byteweise auf alle Festplatten verteilt. Zusätzlich werden aus den Datenblöcken Prüfsummen gebildet. Sektorweise werden die Datenblöcke mit einem logischen Exklusiv-Oder (XOR) verknüft. Die Prüfsumme wird dann auf einem separaten Laufwerk gespeichert. Fällt eine Festplatte aus, kann aus der Prüfsumme und den noch vorhandenen Daten die verlorenen Daten rekonstruiert werden. Aufgrund der einfachen Berechnung der Prüfsumme halten sich die Leistungsverluste bei einem Festplattenausfall in

Grenzen.
Bei einem RAID 3 mit 5 Festplatten ergibt sich eine nutzbare Kapazität von 80% der Gesamtkapazität aller Festplatten. RAID 3 ist für die Speicherung großer Dateien, wie sie z. B. bei CAD, Bild- und Videoverarbeitung anfallen geeignet. Der Vorteil gegenüber RAID 2 ist das simple Prüfsummenverfahren mit XOR. Die Schreibgeschwindigkeit ist allerdings durch die Geschwindigkeit des Prüfsummen-Laufwerks begrenzt.

RAID-Level 4 - Sector Striping

Beim RAID-Level 4 werden die Festplatten wie bei RAID 0 zu einem großen logischen Laufwerk zusammengeschaltet. Die Anzahl der Festplatten ist beliebig skalierbar und jederzeit erweiterbar. Die Dateien werden in ihrer ursprünglichen Größe auf die einzelnen Festplatten verteilt. Man bezeichnet das als Sector Striping. Auf einem zusätzlichen Laufwerk werden die XOR-Prüfsummen der Daten gespeichert.
Der Unterschied zum RAID 3 sind die unabhängig voneinander arbeitenden Festplatten und dass dadurch Zugriffe parallel voneinander abgearbeitet werden können. Beim Schreibvorgang werden die Daten nur auf zwei Festplatten gespeichert. Auf einer Daten-Festplatte und auf dem Prüfsummen-Laufwerk. Weil jeder Schreibvorgang das Prüfsummen-Laufwerk beansprucht, ist dieser nur so schnell, wie die Prüfsumme gespeichert wurde. Fehlende oder fehlerhafte Daten können aus der Prüfsumme rekonstruiert werden.
RAID 4 ist vor allem bei kleinen Dateigrößen interessant. Dort ist der Zugriff besonders schnell.

RAID-Level 1E0 - Striping, Mirroring und Skewed Parity

RAID 1E0 ist eine Erweiterung bzw. Kombination von RAID 1E und RAID 5. Entwickelt wurde es von IBM.
Konventionelles RAID 1E besteht aus mindestens 3 Festplatten, auf denen die Daten gespiegelt sind (Mirroring). Bei RAID 1E0 werden zwei oder mehr RAID-1E-Arrays zusammengeschaltet.

RAID 1E0					
1. RAID 1E			**2. RAID 1E**		
Festplatte 1	**Festplatte 2**	**Festplatte 3**	**Festplatte 4**	**Festplatte 5**	**Festplatte 6**
Block 1	Block 3	Block 5	Block 2	Block 4	Block 6
Mirror 5	Mirror 1	Mirror 3	Mirror 6	Mirror 2	Mirror 4
Block 7	Block 9	Block 11	Block 8	Block 10	Block 12
Mirror 11	Mirror 7	Mirror 9	Mirror 12	Mirror 8	Mirror 10

Ein RAID-Level 1E0 ist erst ab 6 Festplatten möglich. Das Beispiel oben besteht aus zwei 3-er Gruppen. Die Daten sind quer in jeder 3er Gruppe in den RAID 1E Arrays gespiegelt. Wenn nun eine Festplatte ausfällt, liegen deren Daten gespiegelt auf einer anderen Festplatte. Dies hat beim Lesezugriff einen Vorteil. Die Gschwindigkeit kann durch paralleles Lesen gesteigert werden.
RAID 1E0 Arrays können aus maximal 60 Festplatten bestehen. In dieser Ausbaustufe werden vier RAID 1E Arrays, bestehend aus 15 Festplatten, zu einem RAID 1E0 Array gruppiert.

RAID-Level 6 / 7

Beim RAID-Level 6 wird wie bei RAID 5 auch mit Sector Striping gearbeitet. Zusätzlich wird ein Paritätslaufwerk verwendet, das über einen asynchronen Datenpfad und einen Cache verfügt. Während RAID 5 nur den Ausfall eines Laufwerks verkraftet, verträgt RAID 6 den Ausfall von zwei Laufwerken. Bei RAID 6 speichert der Adapter gleich zwei Prüfsummen, sodass sich aus den Daten von verbliebenen Laufwerken die Daten rekonstruieren lassen.

Vorteile von RAID 6

Bei RAID 6 sind vor allem die Schreibzugriffe optimiert. Diese werden sofort quittiert und die Parität im Hintergrund aktualisiert. Der Geschwindigkeitszuwachs ist enorm. Außerdem verkraftet RAID 6 den Ausfall von zwei Laufwerken.

Nachteile von RAID 6

Die Nutzung des Caches macht allerdings Vorsichtsmaßnahmen notwendig. Ein Spannungsverlust vor der Aktualisierung der Parität aus dem Cache führt zu unterschiedlichen Datenbeständen zwischen Datenspeicher und Parität. Um das zu verhindern braucht das Paritätslaufwerk und der Cache mehrere redundante Netzteile und eine unterbrechungsfreie Stromversorgung (USV).

RAID-Level 7

RAID 7 ist eine Erweiterung von RAID 6. Hier geht man etwas weiter und übergibt alle eingehenden und ausgehenden Zugriffe einem zentralen Cache. Die Daten werden per Sector Striping auf mehrere Festplatten gespeichert. Mehrere Reserve-Festplatten übernehmen beim Ausfall einer Festplatte die gespeicherten Daten. Statt nur einer, können gleich mehrere Paritätslaufwerke definiert werden. Die Verarbeitungsgeschwindigkeit der Zugriffe ist hoch. Doch auch hier benötigt der zentrale Cache mehrere redundante Netzteile und eine unterbrechungsfreie Stromversorgung (USV).
RAID 7 ist besonders bei sehr großen Speichermengen ein flexibles System, da am laufenden System Festplatten getauscht und Erweiterungen vorgenommen werden können.

13. HexDump

Hexdump

Hexdump bezeichnet die Darstellung von Computerdaten im hexadezimalen Zahlensystem (in dem sich pro Ziffer vier Bit zusammenfassen lassen). Möchte man Daten (im RAM oder in Dateien) systemnah analysieren, so ist eine hexadezimale Darstellung oft unerlässlich.

Beispiel:

Unter DOS kann man mit dem DEBUG-Befehl Hexdumps erhalten.

Unix-Systeme stellen zur Erstellung eines Hexdumps Befehle wie „hexdump“, die oft zusätzliche Ausgabeoptionen (Dezimaldarstellung, Textdarstellung) enthalten. Mit „od -x“ (**o**ctal**d**ump) kann ebenfalls ein Dump erstellt werden.

Das folgende Beispiel zeigt den *Hexdump* einer Textdatei im ASCII-Code. Links ist eine (hexadezimale) Positionsangabe (Adresse) in der Datei, in der Mitte sind die Zeichen in ihrer Hexadezimaldarstellung (16 Zeichen, in zwei Gruppen von je 8 Zeichen) und rechts als Text angegeben, wobei Speicherinhalte, die kein darstellbares Zeichen repräsentieren, als „.“ gezeigt werden.

```
00000000  48 69 65 72 20 69 73 74  20 65 69 6e 20 42 65 69  |Hier ist ein Bei|
00000010  73 70 69 65 6c 74 65 78  74 2e 20 44 65 72 20 48  |spieltext. Der H|
00000020  65 78 64 75 6d 70 20 69  73 74 20 61 75 66 20 64  |exdump ist auf d|
00000030  65 72 20 6c 69 6e 6b 65  6e 20 53 65 69 74 65 20  |er linken Seite |
00000040  7a 75 20 73 65 68 65 6e  2e 0a 0a 4e 65 75 65 20  |zu sehen...Neue |
00000050  5a 65 69 6c 65 6e 20 6f  64 65 72 20 41 62 73 e4  |Zeilen oder Absä|
00000060  74 7a 65 20 73 69 6e 64  20 64 61 6e 6e 20 61 75  |tze sind dann au|
00000070  63 68 20 22 5a 65 69 63  68 65 6e 22 20 6d 69 74  |ch "Zeichen" mit|
00000080  20 65 69 6e 65 6d 20 62  65 73 74 69 6d 6d 74 65  | einem bestimmte|
00000090  6e 0a 43 6f 64 65 2e 28  30 61 29 2e 2e 2e 0a 0a  |n.Code.(0a).....|
```

Nach demselben Schema würde ein Speicherdump den Inhalt des Hauptspeichers, also zum Beispiel Programmbefehle im Maschinencode bzw. sich im Hauptspeicher befindliche Daten im jeweiligen Speicherformat zeigen.

14. Well know Ports

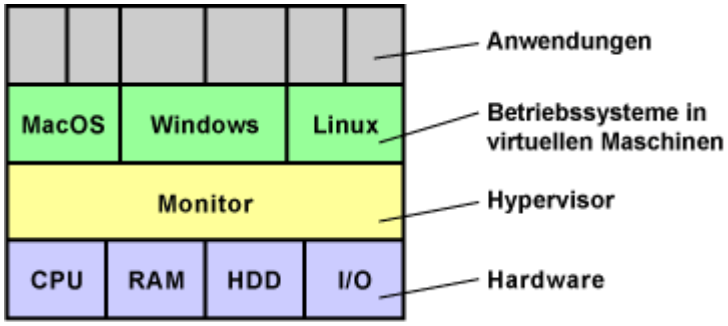
Port Number	Description
1	TCP Port Service Multiplexer (TCPMUX)
5	Remote Job Entry (RJE)
7	ECHO
18	Message Send Protocol (MSP)
20	FTP -- Data
21	FTP -- Control
22	SSH Remote Login Protocol
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
29	MSG ICP
37	Time
42	Host Name Server (Nameserv)
43	WhoIs
49	Login Host Protocol (Login)
53	Domain Name System (DNS)
69	Trivial File Transfer Protocol (TFTP)
70	Gopher Services
79	Finger

80	HTTP
103	X.400 Standard
108	SNA Gateway Access Server
109	POP2
110	POP3
115	Simple File Transfer Protocol (SFTP)
118	SQL Services
119	Newsgroup (NNTP)
137	NetBIOS Name Service
139	NetBIOS Datagram Service
143	Interim Mail Access Protocol (IMAP)
150	NetBIOS Session Service
156	SQL Server
161	SNMP
179	Border Gateway Protocol (BGP)
190	Gateway Access Control Protocol (GACP)
194	Internet Relay Chat (IRC)
197	Directory Location Service (DLS)
389	Lightweight Directory Access Protocol (LDAP)
396	Novell Netware over IP
443	HTTPS
444	Simple Network Paging Protocol (SNPP)
445	Microsoft-DS
458	Apple QuickTime
546	DHCP Client
547	DHCP Server
563	SNEWS
569	MSN
1080	Socks

15. Virtualisierung von Betriebssystemen

Virtualisierung

Der Begriff Virtualisierung ist mehrdeutig. In der Regel verwendet man den Begriff Virtualisierung in der Computertechnik. Typischerweise versteht man unter Virtualisierung die Prozessor-Virtualisierung. Neben der Prozessor-Virtualisierung gibt es auch noch andere Möglichkeiten. Dazu zählt zum Beispiel das Partitionieren von Festplatten oder die Netzwerk-Virtualisierung durch VLAN.



Virtualisierung ist eine Hardware-Unterstützung, die den Betrieb virtueller Computer auf einem echten Computer erleichtert oder beschleunigt. Mit der Virtualisierung kann man mehrere Software-Systeme auf einer Hardware laufen lassen. Das können zum Beispiel unterschiedliche Betriebssysteme sein. Virtualisierung macht dann Sinn, wenn ein Hardware-System nicht ausgelastet ist und die Ressourcen parallel für weitere Systeme genutzt werden sollen.

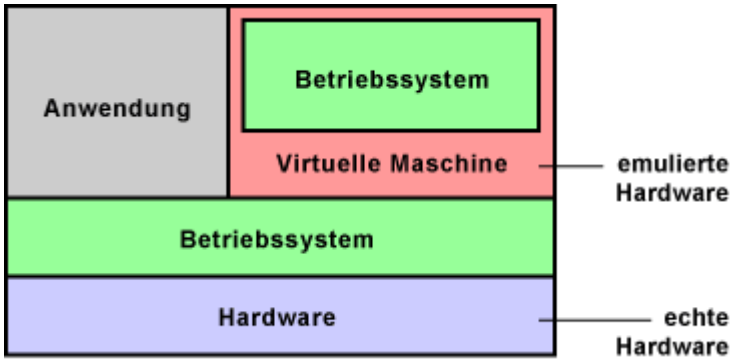
Da eine steigende Taktfrequenz bei Prozessoren so einfach nicht möglich ist, sind die Prozessorhersteller, insbesondere Intel und AMD, auf alternative leistungssteigernder Techniken für Prozessoren angewiesen. Neben Mehrkern-Prozessoren, Multimedia-Erweiterungen und 64-Bit gelten Virtualisierungs-Funktionen als die bahnbrechende Entwicklung.

Gründe für Virtualisierung

- Erhöhung der Ausfallsicherheit
- bessere Auslastung der IT-Systeme durch Konsolidierung der Hardware
- niedrigere IT-Kosten
- geringerer Stromverbrauch

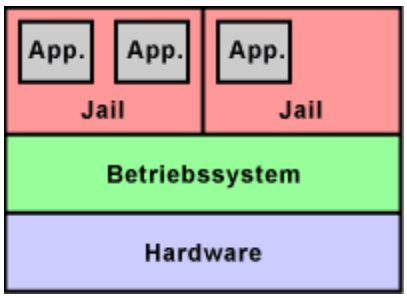
Wichtigstes Merkmal der Virtualisierung ist die Ausfallsicherheit. Wenn eine Applikation sich selbst oder sogar das gesamte Betriebssystem zum Absturz bringt, laufen die anderen virtuellen Maschinen weiter.
Der Betrieb unterschiedlicher Applikationen in mehreren Umgebungen ist die häufigste Anwendung. Zum Beispiel um Applikationen aus Sicherheitsgründen und des Datenschutzes getrennt zu halten. Um aber nicht für jede Applikation eine eigene Hardware bereitstellen zu müssen, werden virtuelle Maschinen geschaffen, auf denen dann die Applikationen getrennt voneinander arbeiten können.
Auf den ersten Blick scheint Virtualisierung nur etwas für Server zu sein. Doch auch normale Anwender können davon profitieren. Zum Beispiel zwei Umgebungen für das Arbeiten mit dem Computer. Die eine ganz normal und die andere bei Verbindung mit dem Internet. Hat sich das Internet-System Würmer oder Viren eingefangen, wird sie gelöscht und neu aufgesetzt. So etwas lässt sich zum Beispiel bei jedem Systemstart automatisieren. So hat man immer ein sauberes System. Das könnte auch soweit gehen, dass unsichere Programme in einer eigenen Umgebung laufen, damit das Betriebssystem von außen nicht angreifbar ist.

Virtuelle Maschine



Eine virtuelle Maschine ist ein Software-Container, der einem darin installierten Betriebssystem eine Scheinwelt vorgaukelt, in dem gängige Hardware-Komponenten emuliert werden. Üblicherweise verfügen Betriebssystem über Standard-Treiber mit denen sie die emulierte Hardware ansprechen können.
Virtuelle Maschinen verfügen nur über eine eingeschränkte Grafikleistung. 3D-Software und die Wiedergabe und Bearbeitung von Videos ist in einer virtuellen Maschine nicht ausreichend schnell machbar.
Mit virtuell ist die Hardware gemeint, die dem Betriebssystem in der virtuellen Maschine zur Verfügung steht. Denn CPU, Arbeitsspeicher, Grafikkarte, Laufwerke und Schnittstellen stehen den parallel arbeitenden Betriebssystemen nicht direkt zur Verfügung. Eine im Hintergrund laufende Virtualisierungssoftware überwacht die Zugriffe auf die Hardware. Sie organisiert und verwaltet die virtuellen Maschinen (VM).
Diese Aufgabe kann zum Beispiel ein Hypervisor übernehmen. Er benötigt einen kleinen Teil der Hardware-Leistung, insbesondere von Prozessor und Arbeitsspeicher, um seine Arbeit erledigen zu können.

Betriebssystem-Virtualisierung mit Container



Bei der Betriebssystem-Virtualisierung läuft nur ein Betriebssystem. Darauf werden mehrere virtuelle Laufzeitumgebungen erzeugt (Jails), die für die laufenden Programme als normale Betriebssysteme wirken. Die Applikationen sehen nur die Applikationen, mit denen sie ihre virtuelle Umgebung teilen. Die Laufzeitumgebungen sind schnell erzeugt, da sie nur Abbilder des Wirtssystems sind. Allerdings können einzelne Abbilder nicht verändert werden. Nur das Grundsystem kann verändert werden und dass verändert dann auch die Abbilder.
Beispiele sind FreeBSD Jails, Solaris Zone/Container, Linux VServer, Open VZ und Virtuozzo.

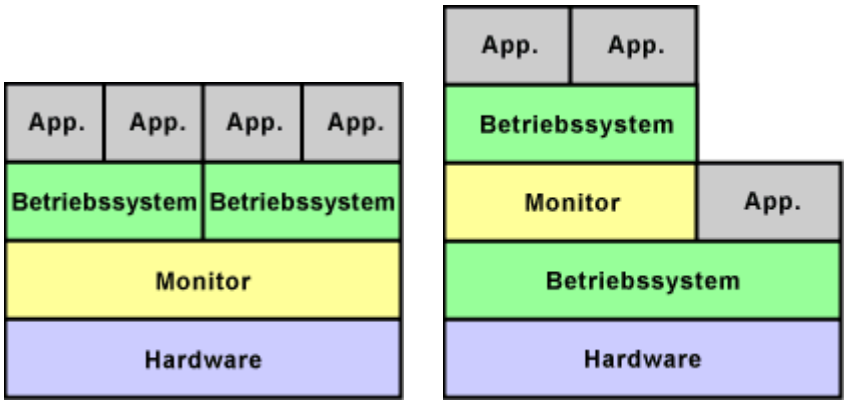
System-Virtualisierung mit Hypervisor

Bei der System-Virtualisierung wird ein oder mehrere vollständige Systeme nachgebildet, auf dem beliebige Betriebssysteme ausführbar sind. Die Systeme orientieren sich an echter Hardware. So

kann man verschiedene virtuelle Systeme nachbilden und mit unterschiedlicher Hardware ausstatten.
Beispiele sind VMWare Workstation, Virtual PC, Virtual Server und Parallels.

Hypervisor / Virtual Machine Monitor (VMM)

Der Hypervisor wird auch als Virtual Machine Monitor (VMM) bezeichnet. Er erstellt und verwaltet virtuelle Hardware. In der Regel stellt ein Hypervisor innerhalb der virtuellen Maschinen Standard-Schnittstellen zur Verfügung. Gleichzeitig stellt er eine Abstraktionsschicht zur Verfügung, die den Zugriff der Treiber auf die Hardware verhindert. Damit ist sichergestellt, dass sich verschiedene Betriebssysteme nicht gegenseitig in die Quere kommen.



Hypervisor Typ 1 **Hypervisor Typ 2**

Man unterscheidet zwischen zwei Arten. Typ 1 und Typ 2. Ein Typ-1-Hypervisor läuft als Betriebssystem direkt auf der Hardware (native). Das Gesamtsystem verbraucht so wenig Ressourcen. Aber der Hypervisor muss alle Treiber für die gesamte Hardware mitbringen.
Ein Typ-2-Hypervisor setzt auf einem vollwertigen Betriebssystem auf (hosted) und nutzt alle Ressourcen, die ihm in dieser Umgebung zur Verfügung stehen.

Der Hypervisor kann also ein vollwertiges Betriebssystem sein (Typ 1). Er ist dann ein Betriebssystem für ein Betriebssystem. Es bildet eine Virtualisierungsschicht, die es ermöglicht, mehrere Betriebssysteme gleichzeitig auf einem Computersystem zu betreiben. Der Hypervisor vermittelt den Betriebssystemen den Eindruck sie würden alleine auf dem System laufen und hätten die Hardware für sich alleine. Der Hypervisor stellt gleichzeitig sicher, dass ein Betriebssystem nicht die Daten eines andere Betriebssystems zerstört oder auch nur darauf Zugriff hat. Er verhindert, dass die Betriebssysteme miteinander in Konflikt geraten. Die Sicherheitsanforderungen an den Hypervisor sind entsprechend hoch.

Betriebssystem-Virtualisierung mit Container (Jail)

- Solaris/OpenSolaris
- Zoning
- BSD jails
- Mac-on-Linux

- OpenVZ
- Virtuozzo
- Linux-VServer
- UML - User Mode Linux
- Linux Container (LXC)

System-Virtualisierung mit Hypervisor (Typ 1)

- Hyper-V (Microsoft)
- vSphere Hypervisor, ehemals ESX/ESXi (VMware)
- XenServer (Citrix)
- Proxmox VE (Proxmox)
- KVM - Kernel-based Virtual Machine (Open Source)
- QEMU - Quick Emulator (Freie Software)

System-Virtualisierung mit Hypervisor (Typ 2)

- VMware Workstation/Player
- Windows Virtual PC
- VirtualBox (Oracle)
- Parallels Workstation

Hardware-Unterstützung

Ursprünglich war Virtualisierung reine Software-Sache. Doch für manche Funktionen braucht die Virtualisierungssoftware Hardware-Unterstützung. 64-Bit und Mehrkern-Prozessoren unterstützen die Virtualisierung. Erst mit einem großen Adressraum und viel Rechenleistung macht Virtualisierung Sinn. Mehrere parallel laufende virtuelle Computer sind darauf angewiesen. Sonst leidet der Bedienkomfort unter der schleichenden Ausführungsgeschwindigkeit der Anwendungen.

Bei der Hardware-Unterstützung geht es weniger um die Geschwindigkeitssteigerung, sondern um Zusatzfunktionen. Das sind bestimmte Funktionen im Prozessor und im Chipsatz.
Befehlserweiterungen in Prozessoren gibt es von AMD mit AMD-V (Pacifica) und von Intel mit VT-x. Ob AMD-V oder Intel VT-x, mit der Virtualisierungsunterstützung des Prozessors kann der Hypervisor die Virtualisierung deutlich schneller ausführen.
AMD-V von AMD und VT-x von Intel reichen für die Hardware-Virtualisierung nicht aus. Zusätzlich nötig ist auch Second-Level Address Translation (SLAT). Das ist ein Adressverwaltungsbeschleuniger, der in der CPU angesiedelt ist und sich in einer höheren Geschwindigkeit bemerkbar macht. Bei AMD heißt das Nested Page Tables (NPT) oder Rapid Virtualization Indexing (RVI). Bei Intel heißt es Extended Page Tables (EPT).

Im Regelfall ist Virtualisierung ein Aufgabenbereich des Prozessors. Doch auch bei der I/O-Virtualisierung ist die Unterstützung von CPU, BIOS und Chipsatz nötig. Dann kann man eine bestimmte PCIe-Komponente direkt an eine virtuelle Maschine durchreichen, sodass sich darin ein Treiber für dieses Gerät installieren lässt. Das ist vor allem bei Grafikkarten interessant.

Intel Vanderpool Technology (VT-x)

Vanderpool Technology, kurz VT-x, und Virtualization Technology for Directed I/O, kurz VT-d, bilden die Virtualisierungsunterstützung von Intel, die seit November 2005 in den beiden Prozessoren Pentium 4 662 und 672 eingebaut eingebaut wurde. Im Laufe des Jahres 2006 wurden auch die anderen Prozessor-Typen Centrino (Yonah), Pentium D (Presler), Pentium 4 und Celeron (Cedar Mill), die Xeon- und Itanium-Reihe mit VT ausgestattet.

AMD Pacifica (AMD-V)

Die Virtualisierungsunterstützung von AMD heißt AMD-V (Pacifica) oder Secure Virtual Machine (SVM), die seit 2006 in den AMD-Prozessoren eingebaut ist. Im Zusammenhang mit Pacifica wird auch immer die Sicherheitsfunktionen Presidio genannt. Beide Techniken hängen eng miteinander zusammen.

Was bringen VT-x (Intel) und AMD-V?

Hinweis: Die folgende Beschreibung ist stark vereinfacht und allgemein gehalten.

Ein Prozessor ist normalerweise darauf ausgelegt nur ein Betriebssystem auszuführen. Wenn ein Computersystem nun neben einem Host- auch ein Gast-Betriebssystem (virtuelle Maschine) beherbergt, dann ist es ohne Änderungen am Original-Code nicht möglich, bei der Befehlsausführung zwischen Host und Gast zu unterscheiden. Wenn bestimmte Instruktionen auf die gleiche Ressource zugreifen, dann kann es zu Abstürzen und Datenverlust kommen. Schon einfache Instruktionen, wie das Sichern und Schreiben von Statusregistern im Prozessor, können zu Problemen führen.
Um Probleme auszuschließen muss der Code vor der Ausführung auf problematische Instruktionen durchsucht und diese gegebenenfalls ersetzt werden. Für die Überprüfung ist der Hypervisor bzw. der Virtual Machine Monitor (VMM) zuständig. Weil jede einzelne Instruktion überprüft werden muss, geht dabei die Performance des gesamten Systems etwas in die Knie. Im Prinzip muss der VMM den virtuellen Maschinen vorgaukeln, dass sie den Prozessor für sich alleine haben.

Viel besser ist die Virtualisierungsunterstützung durch den Prozessor. Dadurch wird die Virtualisierung etwas schneller (Geschwindigkeitsvorteil). Das hilft vor allem "einfachen" Virtualisierungslösungen. Viel wichtiger ist, dass unter einem 32-Bit-Betriebssystem auch ein 64-Bit-Gastsysteme ausgeführt werden kann, wenn der Prozessor Virtualisierung unterstützt. Denn mit speziellen Virtualisierungsinstruktionen lassen sich die virtuellen Maschinen in eine Umgebung verschieben, wo das Durchsuchen auf problematische Instruktionen nicht mehr nötig ist.
Wenn die Virtualisierungsunterstützung trotzdem nicht sehr viel zur Geschwindigkeitssteigerung führt, dann liegt das daran, weil die meisten Instruktionen immer noch vom VMM abgefangen werden müssen. Das bedeutet, dass die Virtualisierungsunterstützung des Prozessors nicht besonders umfangreich ist. Der Prozessor kann nicht alle Instruktionen selber abhandeln.
Ob Instruktionen von der VMM oder vom Prozessor behandelt werden, hängt vom Umfang der Virtualisierungsunterstützung des Prozessors ab. Die Behandlung durch den Prozessor ist auf alle Fälle schneller. Aber prinzipiell ist immer ein VMM nötig, der sich um die Organisation und die aufwendigeren Instruktionen kümmert.

Anwendungen

Virtuelle Computer sind eher selten im Einsatz. Es werden aber schon konkrete Anwendungen diskutiert. Einiges davon ist jetzt schon möglich. Mit einem neuen Software-Zweig ist zu rechnen.

- Software-Entwickler nutzen virtuelle Computer, um ihre Produkte unter verschiedenen Betriebssystemen zu testen.
- Auf Arbeitsplatz-Rechnern könnte man verschiedene Arbeitsumgebungen schaffen. Eine normale Arbeitsoberfläche, eine Oberfläche für den Internet-Zugang und eine für spezielle Hardware-Ressourcen. So lassen sich die verschiedenen Oberflächen gegen Hardware- und Software-Fehler, Viren und Würmern schützen.
- Bestimmte Anwendungen für ältere Betriebssysteme können in einem virtuellen Computer ausgeführt werden. Parallel dazu kann ein aktuelles Betriebssystem mit vollem Leistungsumfang arbeiten.
- Wenn zwei Applikationen sich nicht vertragen, kann man sie unter eigenen virtuellen Umgebungen installieren und ausführen.

Virtualisierung in der Server-Umgebung

- bessere Systemauslastung erreichbar
- leichter managebar
- Energiekosten senken -> Umweltrichtlinien einhalten
- höhere Sicherheit und Stabilität
- schneller Anforderungen umsetzen

Virtualisierung in der Desktop-Umgebung

- höhere Sicherheit und Stabilität
- Abwärtskompatibilität

Virtualisierung im großen Maßstab

Ab 20 virtuellen Maschinen auf einem Rechner, tritt die Überwachung, das Update-Management und die Leistungsmessung in den Vordergrund. Es stellt sich unter anderem auch die Frage, wie man ein Update-Patch auf allen virtuellen Maschinen einspielt, ohne das jede einzelne virtuelle Maschine gestoppt und gestartet werden muss.
Ein Verteilungs- und Kontrollmechanismus muss in der Lage sein, die virtuellen Maschinen automatisch auf eine andere Hardware zu verteilen.

16. VoIP

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. Während die Festnetz-Telefonie aus möglichst wenigen Komponenten besteht, sind bei VoIP über das Internet sehr viele Komponenten im Spiel. Viele Faktoren spielen beim Verbindungsaufbau und auch danach eine große Rolle.

VoIP-Anwendungen	Call-Manager, Softphone, ...
VoIP-Protokolle	SIP, H.323, RTP, UDP, ...
VoIP unterstützende Dienste	DNS, NAT, QoS, AAA, ...
Betriebssysteme	Linux, Unix, Windows, ...
Hardware	Breitbandmodem, Router, Server, IP-Telefon, Smartphone, ...
Netze	LAN, WAN, DSL, TV-Kabel, ...

Sprachqualität bei Voice over IP

Die Sprachqualität ist von der Verbindung und vom Codec abhängig, mit dem die Sprache digitalisiert wird. Wird der Codec G.711 verwendet, dann hat man Festnetz-Sprachqualität. Voraussetzung ist eine stabile Verbindung ohne Laufzeitschwankungen (Jitter) und Paketverluste. Bei der Festnetz-Telefonie wird vom Vermittlungssystem eine leitungsvermittelte Verbindungsqualität garantiert. Im Internet durchlaufen die Sprachdaten unterschiedliche Netze und Stationen. Wie schnell die Pakete weitergeleitet werden liegt in der Hand deren 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, muss man unter Umständen mit Einschränkungen leben.

<table>
<tr><th>Call Control</th><th>Audio</th><th>Video</th></tr>
<tr><td rowspan="2">SIP
H.323</td><td>G.711
G.723
G.729</td><td>H.261
H.263</td></tr>
<tr><td colspan="2">RTP
RTCP</td></tr>
</table>

TCP	UDP
IP	
LAN	

Voice over IP im OSI-Schichtenmodell

Schicht		Protokoll
7.	**Anwendung**	**VoIP-Anwendung** Softphone / Call-Manager
6.	**Präsentation**	**Sprachcodecs** G.729 / G.723 / G.711
5.	**Session**	**Signalisierung** H.323 / SIP
4.	**Transport**	**Transport-Protokolle** RTP / UDP / RSVP
3.	**Netzwerk**	**Netzwerk-Protokoll** IP
2.	**Verbindung**	ATM / Ethernet
1.	**Physikalische Ebene**	DSL / Ethernet

Transport-Protokolle

Bei Voice over IP muss man zwischen den Datenpaketen zum Verbindungsauf- und -abbau (Signalisierung) und den eigentlichen Sprachpaketen (Datenstrom) unterscheiden. Die Signalisierungsdaten müssen dabei möglichst sicher übertragen werden. Sie steuern die Verbindung. Sie dürfen länger unterwegs sein und einen größeren Protokoll-Overhead haben. Hauptsache die Verbindung kommt zu Stande. Dagegen müssen die Sprachpakete schneller und verzögerungsfrei unterwegs sein. Dabei kann man sich eine unsichere Übertragung leisten. Wenn mal ein Datenpaket verloren geht, dann ist das nicht so schlimm.
In der Praxis sieht das so aus, dass die Sprachpakete zuerst in RTP-Pakete und dann in UDP-Pakete verpackt werden und zur Adressierung zusätzlich mit einem IP-Header versehen werden. Die Übertragungstechnik auf dem physikalischen Medium fügt dann noch einen Paketrahmen hinzu, der vom jeweiligen Medium und Übertragungssystem abhängig ist. Dabei entsteht ein Overhead von 54 Byte pro Paket. Durch Kompression kann der Protokoll-Kopf von 40 Byte auf nur zwei bis drei Byte komprimiert werden.

Sprach-Codec / Audio-Codec

Bevor die Sprache übertragen werden kann, muss sie zuerst digitalisiert werden. In der Regel werden die Sprachdaten auch gleich komprimiert. Bei zunehmender Komprimierung nimmt die Sprachqualität ab. Die Dekomprimierungszeit und die Rechenleistung nehmen zu.

Abhängigkeit der Sprachqualität von Laufzeit, Jitter und Paketverlusten

Voice over IP ist nur dann in einem Netzwerk nutzbar, wenn die wichtigen Kennwerte, wie Bandbreite, Laufzeit und Jitter bei einem voll ausgelasteten Netzwerk einschließlich der Netzübergänge ausreichend sind. Dadurch wird im Wesentlichen die Sprachqualität beeinflusst. Die Hauptprobleme entstehen durch eine zu geringe Bandbreite und zu lange Distanzen. Paketverluste, hoher Jitter und große Verzögerungen reduzieren die Sprachqualität.

Delay - Verzögerung - Laufzeit

Die Laufzeit der Sprachpakete ist ein wichtiges Kriterium für die Sprachqualität. Dabei interessiert man sich für die Gesamtverzögerung zwischen dem Sprechen des Senders und dem Hören des Empfängers (Ende-zu-Ende-Verzögerung).
Laufzeitverzögerungen, auch Delay genannt, entstehen bei der Umwandlung der Datenformate und durch das Routing. Gerade beim Transport entstehen die größten Verzögerungen. Besonders in den Zwischenstationen (Switch, Router, 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

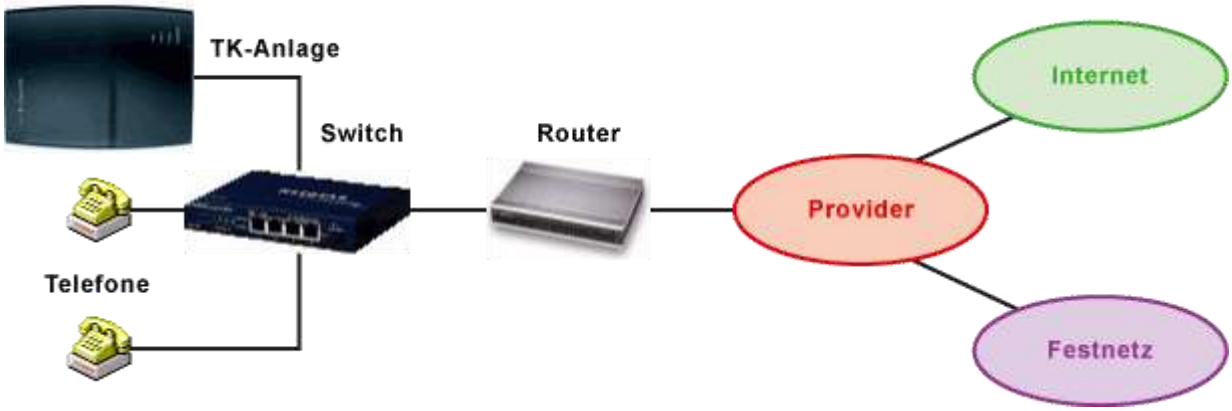
Sicherheits-Features für VoIP sind äußerst unpopulär. Als Grund wird der vergleichsweise hohe Aufwand für das Abhören oder Stören, im Vergleich zu ISDN oder analog, angeführt. Einen analogen Anschluss kann man abhören, in dem man ein Telefon oder Kopfhörer parallel zur Leitung schaltet. Bei VoIP ist das wesentlich komplizierter, weil die Daten auf mehreren Protokollschichten verteilt sind. Einen Datenverkehr mitzuschneiden ist sehr aufwendig und nur mit hochwertiger Hardware und Software möglich. Vorausgesetzt natürlich, man hat einen Punkt im Netz, an dem man Abhören kann.
Das Grundproblem bei VoIP ist die bidirektionale Datenverbindung. Die Datenpakete werden in beide Richtungen über die Firewall geschickt. Dafür werden Ports geöffnet, die wiederum als Angriffspunkt für Hacker dienen können. Solange die IP-Telefonie im lokalen Netzwerk und hinter einer Firewall arbeitet, ist das Risiko eines Angriffs von außen gering. Ist der Telefonie-Server über das öffentliche Netz zu erreichen, dann kann dessen Funktion beispielsweise durch Denial-of-Service-Attacken (DoS) gestört werden.

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

17. PBX

Hosted PBX



So schön IP-Centrex sein mag, es gibt auch Kunden deren Sicherheitsrichtlinien vorschreiben, dass der Betrieb des Systems im eigenen Netz erfolgen muss. Für solche Kunden gibt es Hosted PBX. Dabei wird dem Kunden vom Provider ein Server zur Verfügung gestellt. Bei Hosted PBX findet das Prinzip "dediziertes System" Anwendung. Die Hosted PBX wird aber weiterhin vom Provider betreut.

Umstieg von der klassischen TK-Anlage zu IP-Centrex oder Hosted PBX

Einen Spareffekt beim Umstieg von TK-Anlage zur IP-Centrex oder Hosted PBX gibt es nicht. Neue Systeme sind eher teurer als etablierte Techniken. So auch beim Umstieg von ISDN auf VoIP. Der Umstieg lohnt sich also nur, wenn man an andere Stelle profitiert.
Aber sparen lässt sich doch. Später wenn alles läuft, bei Umzügen innerhalb der Räumlichkeiten. Die Telefone sind viel schneller wieder verfügbar, weil das Telefon nur umgesteckt werden muss. Sparen lässt sich auch deshalb, weil Sprache und Daten auf einer einheitlichen Infrastruktur laufen und nicht zwei getrennte Kabelnetze vorhanden sein müssen.

18. ISDN

ISDN - Integrated Services Digital Network

ISDN ist ein digitales Telekommunikationsnetz (internationaler Standard). Die Abkürzung ISDN steht für Integrated Services Digital Network. Damit wird ein dienste integrierendes digitales Netzwerk bezeichnet. Die Telekommunikationsdienste Sprache, Daten, Text und Bilder werden zusammengefasst und über eine Anschlussleitung digital übertragen. So können verschiedenartige Endgeräte den gleichen ISDN-Anschluss parallel nutzen. Man braucht also für unterschiedliche Telekommunikationsdienste keine separaten Anschlüsse oder Übertragungssysteme. Durch die Digitalisierung werden die Dienste zeitlich verschachtelt (Zeitmultiplex) und sind so für den Anwender scheinbar gleichzeitig nutzbar.

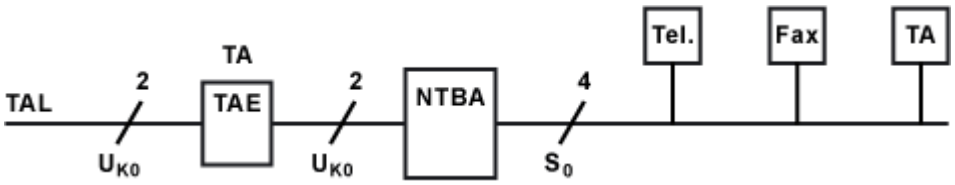
Im Jahr 1989 führte die damalige Deutsche Bundespost ISDN in Deutschland ein. Damit war Deutschland der Vorreiter für ISDN in Europa. Damals wurde damit begonnen, das gesamte Telefonnetz auf die digitale Technik umzustellen. 1997 war der Umbau abgeschlossen.

Herkömmliche ISDN-Anschlüsse sind langsam aber sicher auf dem Rückzug. Große Firmen setzen bei Neuinstallationen in der Regel auf VoIP-Lösungen. Bei kleinen Unternehmen sieht das noch etwas anders aus. Hier finden sich häufig noch EC-Kartenterminals, Frankiermaschinen oder

Alarmanlagen, die eine transparente ISDN-Verbindung mit 64 kBit/s benötigen. Denn VoIP-Verbindungen sind ausschließlich auf die Übertragung von Sprache ausgelegt.

ISDN-Anschluss

Prinzipiell unterscheidet man zwischen zwei ISDN-Anschlüssen. Einmal den Basisanschluss und den Primärmultiplexanschluss. Der Basisanschluss ist das was man typischerweise als ISDN-Anschluss bezeichnet.



Der ISDN-Anschluss (Basisanschluss) wird vom Netzbetreiber auf einer 2-adrigen Teilnehmeranschlussleitung (TAL) zum Kunden geschaltet. Der Übergabepunkt ist die TAE-Dose. Hier wird kein Endgerät angeschlossen, sondern ein Netzabschlussgerät. Der Network Termination for ISDN Basic Access (NTBA), auf Deutsch Netzwerkabschlusseinrichtung für den Basisanschluss. Der NTBA bildet den Endpunkt des ISDN-Netzes. Ab hier beginnt der ISDN-Anschluss und der Kunde selber verantwortlich. Der Kunde darf ab dem NTBA selber Endgeräte installieren oder die Installation an beliebige Unternehmen in Auftrag geben.

Der NTBA baut aus der zweiadrigen Kupferleitung von der Vermittlungsstelle einen internen vieradrigen Anschluss. Dieser Anschluss wird als S0 (S-Null) bezeichnet. Der daran angeschlossene Kabelstrang ist der S0-Bus (S-Null-Bus). Daran werden die ISDN-Endgeräte angeschlossen.
Die Stromversorgung für den NTBA erfolgt aus der Vermittlungsstelle. Zusätzlich kann der NTBA über sein integriertes Netzteil mit Strom versorgt werden. Wenn die angeschlossenen Endgeräte über keine eigene Stromversorgung verfügen, so reicht die Stromversorgung aus dem S0-Bus in der Regel aus. Man bezeichnet das dann als Notstrombetrieb, der eigentlich nur für den Fall eines lokalen Stromausfalls vorgesehen ist. Dieser Notstrombetrieb ist in der Praxis der Normalfall.
Am S0-Bus werden alle ISDN-Endgeräte an einem busförmigen Kabelstrang angeschlossen. Eine sternförmige Verkabelung ist nicht vorgesehen, auch wenn sie in einer bestimmten Konstellation möglich ist. Neben dem busförmigen Betrieb, gibt es auch einen Y-Betrieb. Dabei befindet sich der NTBA in der Mitte des Kabelstrangs. Die Enden des Kabelstrangs müssen mit Endwiderständen abgeschlossen sein.

Bei der Verkabelung für ISDN MUSS ein paarweise verseiltes Kabel verwendet werden. Unverseilte Kabel sind auch auf kurzen Strecken generell untauglich. Besser wären sogar höherwertige Kabel nach Kategorie 5 oder höher.

ISDN-Technik

Prinzipiell unterscheidet man zwischen zwei ISDN-Anschlüssen. Einmal der Basisanschluss und den Primärmultiplexanschluss.
Der Basisanschluss hat zwei Nutzkanäle (B-Kanäle) mit je 64 kBit/s und einen Steuerkanal (D-Kanal) mit 16 kBit/s.

Der Primärmultiplexanschluss, E1 oder S2M genannt, hat 30 Nutzkanäle (B-Kanäle) mit je 64 kBit/s und einen Steuerkanal und einen Synchronisationskanal mit je 64 kBit/s. Die 30 Nutzkanäle können einzeln oder bis 1.920 kBit/s gebündelt genutzt werden.

- ISDN-Basisanschluss (BRI, 2B1D)
  - Mehrgeräteanschluss für einzelne Endgeräte und TK-Anlagen für wenige Teilnehmeranschlüsse
  - Anlagenanschluss für TK-Anlagen bis 100 Teilnehmeranschlüssen
- ISDN-Primärmultiplexanschluss (PRI, 30B2D)
  - Anlagenanschluss für TK-Anlagen mit über 100 Teilnehmeranschlüssen

ISDN-Dienste

- ISDN-Telefonie (3,1 kHz)
- ISDN-Telefax (Gr. 4)
- ISDN-Bildschirmtext
- ISDN-Bildkommunikation
- ISDN-Datenübertragung mit 64 kBit/s
- ISDN-Teletex

ISDN-Endgeräte

- ISDN-Telefon
- ISDN-Karte
- ISDN-Faxgerät (Gr. 4)
- ISDN-TK-Anlage

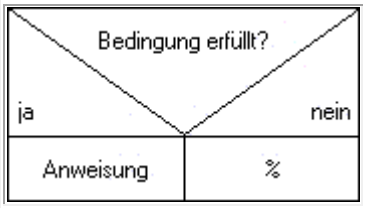
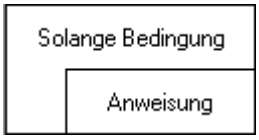
ISDN-Leistungsmerkmale für den Dienst Telefonie

- Anzeige der Rufnummer des Anrufers am eigenen Telefon (Rufnummernanzeige)
- Anklopfen
- Anrufweiterschaltung (Rufumleitung)
- Mehrfachrufnummer (mehrere Rufnummern an einem Anschluss)
- Rückruf
- Dreierkonferenz

19. Struktogramme

Struktogramme Grundlagen

Struktogramme ("Nassi-Shneiderman-Diagramm") stellen Programmstrukturen dar. Genormt nach DIN 66261.

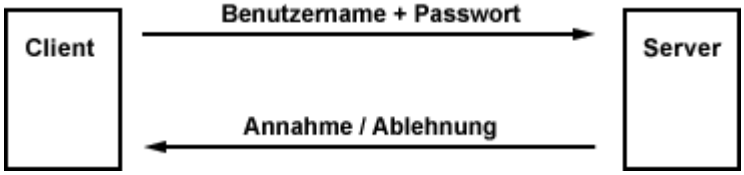
Struktogramm	Erklärung
	**Struktogramme** sind ineinander verschachtelte Rechtecke. Willst du ein Struktogramm verfeinern, so zeichnest du einfach in das Struktogramm ein weiteres hinein, das dann angibt, was du - b.z.w. dein Programm- tun soll(st). Links siehst du den einfachsten Typ: erst wird Anweisung 1 ausgeführt, dann Anweisung 2, u. s. w. **Aufgabe:** gib zum Struktogramm (irgend)ein JavaScript an.
	Das Struktogramm zur (einseitigen) **Verzweigung**, hier wird der if-Zweig ausgeführt, falls die Bedingung wahr ist. Sonst -siehe das %-Zeichen- passiert nichts! **Aufgabe (wie eben):** gib zum Struktogramm ein JavaScript an.
	Und dann war da noch die **Schleife** . Solange die Bedingung wahr ist, wird die Anweisung im Schleifenrumpf ausgeführt, wobei du für die Anweisung wieder ein beliebiges Struktogramm einsetzen darfst (klar?). Auch hier bitte ein JavaScript **(Aufgabe)**.

20. PAP

PAP - Password Authentication Protocol

Password Authentication Protocol, kurz PAP, ist ein Authentifizierungsverfahren über das Point-to-Point-Protocol (PPP). PAP wurde verwendet, um sich per PPP in eine Computernetzwerk einzuwählen und sich dort mit Benutzername und Passwort zu authentifizieren.

Ablauf der Authentifizierung mit PAP



PAP beschreibt einen 2-Wege-Handshake, wie er bei einer Einwahl mit einfacher Authentifizierung stattfindet. Dazu schickt der Client dem angerufenen Server die Benutzername-Passwort-Kombination. Nach Prüfung von Benutzername und Passwort nimmt der Server die Authentifizierung des Clients an oder lehnt sie ab. Bei einer Ablehnung wird die Verbindung getrennt.

Sicherheitsrisiken und Probleme von PAP

- Benutzername und Passwort werden unverschlüsselt übertragen. Wir die Datenübertragung abgehört, hat ein Angreifer die Daten zur Authentifizierung und kann sich selber einwählen und Schaden anrichten.
- Der Client kann beliebig viele Versuche zur Authentifizierung abschicken. Das Raten von Passwörtern oder testweise Ausprobieren von beliebigen Benutzernamen-Passwort-Kombinationen ist möglich und verschafft einem Angreifer zufälligen Zugang.

- Die Häufigkeit und Geschwindigkeit der Authentifizierung kann vom Client bestimmt werden. Ein Angreifer könnte ein Skript zur automatischen Einwahl und systematischer Passwort-Abfrage ausführen.
- Der Server kann durch mehrere parallele Aufrufe in seiner Arbeitsweise eingeschränkt werden. Im ungünstigsten Fall wird ein Totalausfall erzwungen.

Statt PAP nimmt man das sichere CHAP oder MS-CHAP.

21. APIPA

Automatic Private IP Adressing (APIPA) ermöglicht die automatische Konfiguartion von Netzwerkschnittstellen.

Ein Netzwerkinterface das APIPA unterstützt, gibt sich selbst eine zufällige IP-Adresse aus dem Bereich 169.254.1.0 bis 169.254.254.255. Der Host muss überprüfen, ob die gewählte Adresse im Netz bereits vorhanden ist. Dazu wird das Protokoll ARP genutzt.

Steht eine Schnittstelle unter Windows auf "IP-Adresse automatisch beziehen" und es antwortet kein DHCP-Server, greift APIPA. Apple hat die Technik unter dem Namen Bonjour (ehemals Rendezvous) implementiert.

22. IPv6

IPv6 - Internet Protocol Version 6

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

IPv6 ist der direkte Nachfolger von IPv4 und Teil der Protokollfamilie TCP/IP. Seit Dezember 1998 steht IPv6 bereit und wurde hauptsächlich wegen der Adressknappheit von IPv4 spezifiziert. Da weltweit immer mehr Menschen, Maschinen und Geräte an das Internet mit einer eindeutigen Adresse angeschlossen werden wollen, reichen 4 Milliarden IPv4-Adressen nicht aus. Doch IPv6 löst nicht nur die Adressknappheit, sondern bringt auch Erleichterungen bei der Konfiguration und im Betrieb mit. Die zustandslose Konfiguration und verbindungslokalen Adressen, die bereits nach dem Computerstart verfügbar sind, vereinfachen die Einrichtung eines lokalen Netzwerks.

IPv6 gilt als Wunderwaffe gegen so manche Probleme mit Netzwerkprotokollen und gleichzeitig wird es als Teufelszeug verdammt, das wieder neue unbekannte Probleme hervorruft. Eine Tatsache ist, dass Administratoren, Programmierer und Hersteller IPv6 neu lernen müssen. Viele Rezepte aus der IPv4-Welt taugen unter IPv6 nicht mehr. Erschwerend kommt hinzu, dass bei IPv6 es allen Beteiligten an Erfahrung fehlt. Wenn man vor einem großen Problem steht kann man nicht mal eben jemand Fragen.

Doch IPv4 hat keine Zukunft mehr und ein zügiger Wechsel zu IPv6 erscheint notwendig. Gleichzeitig muss nicht nur IPv6 eingeführt, sondern auch IPv4 parallel betrieben werden. Solange bis alle Rechner auf der Welt IPv6 beherrschen. Und das kann dauern. Es gibt viele Netzwerk-Komponenten, die kein IPv6 unterstützen und erst gegen IPv6-fähige Komponenten ausgetauscht werden müssen. Auf der anderen Seite ist der Markt für IPv6 noch nicht groß genug, dass sich die Entwicklung von IPv4-vergleichbaren Produkten mit IPv6 lohnt.

Internet Protocol Version 5?

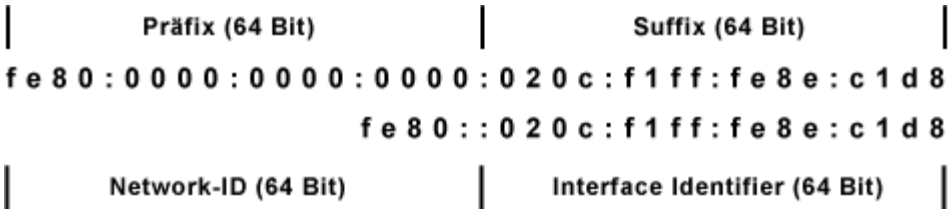
IPv5 hieß offiziell ST-2 (Internet Stream Protocol Version 2) und war ein experimentelles Protokoll für Echtzeit-Datenströme. ST-2 sollte ursprünglich Audio und Video per Multicast übertragen. Dadurch sollten die Bandbreitenreservierungsvorteile von ATM in die IP-Netze gelangen. Zur Serienreife hat es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

Vorteile von IPv6

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

- längere Adressen und dadurch ein größerer Adressraum
- Autokonfiguration der IPv6-Adresse
- Multicast durch spezielle Adressen
- schnelleres Routing
- Punkt-zu-Punkt-Verschlüsselung mit IPsec
- Quality of Service
- Datenpakete bis 4 GByte

IPv6-Adressen



Eine IPv6-Adresse besteht aus 128 Bit. Damit haben IPv6-Adressen genügend Raum, um möglichst viele Netzwerk-Topologien abbilden zu können. Gleichzeitig geht es darum, das Routing zu vereinfachen.
Die von IPv4 bekannte Netzwerkmaske bzw. Subnetzmaske fällt ersatzlos weg. Um den Adressbereich bzw. das Subnetz zu kennzeichnen wird ein Präfix verwendet, dass man durch ein "/" an die Adresse anhängt.
Häufig ist es so, dass die ersten 64 Bit einer IPv6-Adresse das Netz und die restlichen 64 Bit den Host adressieren.
Wegen der unhandlichen Länge werden die 128 Bit in 8 mal 16 Bit unterteilt. Je 4 Bit werden als eine hexadezimale Zahl dargestellt. Je 4 Hexzahlen werden gruppiert und durch einen Doppelpunkt

(":") getrennt.
Um die Schreibweise zu vereinfachen können führende Nullen in den Blöcken wegfallen. Eine Folge von Nullen kann man durch zwei Doppelpunkte ("::") ersetzen.

Hinweis: Im Gegensatz zu IPv4 sieht IPv6 vor, dass ein Computer in der Regel mehr als nur eine IPv6-Adresse hat. Konkret bedeutet das, dass wenn von IPv6-Adressen die Rede ist, dass immer klar sein muss welchen Gültigkeitsbereich diese IP-Adressen aufweisen. Grob unterscheidet man zwischen globalen und lokalen IPv6-Adressen.

IP-Autokonfiguration und Adressvergabe

Eine vollständige Autokonfiguration umfasst die Netzparameter IPv6-Adresse, Default-Route bzw. Gateway und einen DNS-Server. Hierbei muss man anmerken, dass ein IPv6-Host in der Regel mehrere IP-Adressen hat und diese auf unterschiedlichen Wegen bekommen kann. Man unterscheidet zwischen "stateless" und "stateful". Bei "stateless" erzeugt sich der IPv6-Host seine IP-Adresse selber. Bei "stateful" bekommt er sie zentral zugewiesen.

Standardmäßig ist es so, dass wenn ein IPv6-Client gestartet wird, dann weist er sich selber eine link-lokale IPv6-Adresse zu. Die ist nur im lokalen Netz gültig. Vergleichbar, aber nicht ganz identisch, mit einer privaten IPv4-Adresse. Verbindungen in andere Netze, zum Beispiel ins Internet, sind mit einer link-lokalen IPv6-Adresse nicht möglich.
Weil in IPv6 eine Autokonfiguration integriert ist, kann man sich die manuelle Konfiguration von IPv6-Adresse sparen. Mit der Autokonfiguration von IPv6 sollte in jedem Fall eine Kommunikation im lokalen Netz möglich sein.
Anders als bei IPv4 muss die IP-Konfiguration im lokalen Netzwerk nicht zentral vergeben werden. Unter IPv6 gibt es keine Netzwerkmaske und Broadcast-Adressen mehr. Die Einrichtung eines Netzwerks ist unter IPv6 viel einfacher.

Die ersten 64 Bit einer link-lokalen IPv6-Adresse sind fest vorgegeben. Die ersten 16 Bit sind "fe80". Weitere 48 Bit werden mit Nullen aufgefüllt. Die restlichen 64 Bit entsprechen dem Interface Identifier für den die MAC-Adresse des Netzwerkadapters herangezogen und in das Nummerierungssystem EUI-64 des IEEE umgewandelt wird. Standardmäßig ist es jedoch so, dass ein zufälliger Interface Identifier erzeugt wird. Beispielsweise mit Privacy Extensions oder CGA.

Konnte der Client feststellen, dass seine link-lokale IPv6-Adresse im lokalen Netz einmalig ist, kann er die nächste Stufe der Autokonfiguration zünden. Mit der link-lokalen IP-Adresse besorgt sich der Client eine globale IPv6-Adresse, mit der er über das lokale Netz hinaus ins Internet Verbindungen aufbauen kann. Die globale IPv6-Adresse ist mit einer öffentlichen IPv4-Adresse vergleichbar, wobei ein IPv6-Host in der Regel immer eine link-lokale IP-Adresse hat und zusätzliche auch noch eine globale IP-Adresse.

IPv6 kennt drei Wege, wie ein Client an eine globale IPv6-Adresse kommen kann. Entweder wird sie manuell konfiguriert, per Autokonfiguration oder wie bei IPv4 per DHCP (DHCPv6) vergeben. Die manuelle Konfiguration der globalen IPv6-Adresse kann man sich sparen, weil die Autokonfiguration von IPv6 globale IPv6-Adressen zentral vergeben kann. Nur der DNS-Server und eventuell ein NTP-Server müssen manuell konfiguriert oder zusätzlich zentral verfügbar gemacht werden. Beispielsweise per DHCPv6.

Beide Verfahren haben jedoch den Nachteil, dass sie für sich alleine nicht gut funktionieren. Das liegt daran, weil in älteren Betriebssystemen IPv6 nur unzureichend integriert ist. Momentan (Stand Anfang 2014) gibt es drei Szenarien die für eine IPv6-Autokonfiguration sinnvoll erscheinen:

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

IPv6-Header und Extension Header

Jedes IPv6-Datenpaket besteht aus einem Header (Kopf) und dem Bereich, in dem sich die Nutzdaten befinden. Der Header ist den Nutzdaten vorangestellt. Der IPv6-Header enthält unter anderem die IP-Adresse von Sender und Empfänger und weitere Angaben, die für das IP-Routing wichtig sind und von den Routern auf dem Weg von Sender zu Empfänger ausgewertet werden. Der IPv6-Header weist eine feste Länge von 40 Byte auf. Optionale Informationen sind in den Extension-Header ausgelagert.

NDP und ICMPv6

Das Neighbor Discovery Protocol, kurz NDP, ist ein IPv6-Protokoll zum Austausch link-lokaler Nachrichten wie Router Discovery und Neighbor Discovery. NDP-Nachrichten sind Bestandteil von ICMPv6 und dürfen nicht in andere Netze gelangen. NDP vereint die Funktionen von ARP, RARP und IGMP bei IPv4, erfüllt aber noch mehr Aufgaben (z. B. Router Discovery und Router Renumbering).

Aufgaben von NDP

- Router- und Präfix-Ermittlung (Router Discovery und Prefix Discovery)
- Parameterermittlung (Parameter Discovery, z.B. MTU und Hop Limit)
- Adress-Autokonfiguration (Stateless Address Autoconfiguration, SLAAC)
- Adressauflösung (Address Resolution mit Neighbor Discovery)
- Bestimmung des nächsten Hops
- Erkennung der Nichterreichbarkeit des Nachbarn (Neighbor Unreachability Detection, NUD)
- Erkennung doppelter Adressen (Duplicate Address Detection, DAD)
- Umleitung (Redirect)

RD - Router Discovery

Bei Router Discovery handelt es sich um Verfahren, um die Hosts im Link-Local-Scope über die Anwesenheit eines Routers zu informieren.
Im Rahmen der Router Discovery mit Router Advertisement und Router Solicitation findet eine Prefix Discovery statt, die die Präfixe für die IPv6-Autokonfiguration ((Stateless Address Autoconfiguration, SLAAC) der link-lokalen und globalen IPv6-Adresse verteilt. Im Anschluss

findet eine Duplicate Address Detection (DAD) statt.
Ein Router kann die Hosts über ein Router Advertisement anweisen, IPv6-Adressen und andere Konfigurationsparameter über DHCPv6 zu beziehen.

Neighbor Discovery und Inverse Neighbor Discovery

Im Rahmen der Neighbor Discovery gibt es die Verfahren Duplicate Address Detection (DAD), Neighbor Unreachability Detection (NUD) und die Adressauflösung (Address Resolution).
Die Adressauflösung sorgt für die Zuordnung einer MAC- oder Hardware-Adresse zu einer IPv6-Adresse. Bei IPv4 findet die Zuordnung zwischen IP- und MAC-Adresse mittels ARP bzw. RARP statt. Bei IPv6 ist das Neighbour Discovery Protocol (NDP) für die Adressauflösung zuständig.
Im Rahmen der Neighbor Discovery dienen Neighbor Solicitation und Neighbor Advertisement dazu, um Netzwerk-Nachbarn und Router zu bestimmen und Adressen aufzulösen.

DAD - Duplicate Address Detection

Bei der Duplicate Address Detection, kurz DAD, fragt der Host per Neighbour Solicitation im LAN, ob andere Geräte bereits die gewählte Adresse nutzen. Bereits verwendete Adressen melden IPv6-Geräte per Neighbour Advertisement als belegt.

NUD - Neighbor Unreachability Detection

Bei der Neighbor Unreachability Detection, kurz NUD, geht es um die Erkennung der Nichterreichbarkeit der Nachbarn im Link-Local-Scope. Dabei werden einzelne IPv6-Adressen überprüft, ob sie on-link oder off-link sind.

Übergangsverfahren von IPv4 auf IPv6

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

Multicast-Adressen (Link-Local Scope Multicast Addresses)

IPv6 fasst Netzwerkknoten, Router, Zeit-Server und andere Dienste in Multicast-Gruppen zusammen. Jede Gruppe ist über eine eigene Adresse erreichbar. Link-lokale Multicast-Adressen beginnen immer mit "ff02" und enden mit einer Nummer, die einer Multicast-Gruppe zugeordnet ist. Im Folgenden ein Auszug aus der Liste der link-lokalen Multicast-Gruppen.

- ff02::1 : alle IPv6-Stationen
- ff02::2 : alle Router
- ff02::f : UPnP
- ff02::101 : alle Zeitserver (NTP)
- ff02::1:2 : DHCPv6-Server
- ...

Jede Multicast-Gruppe kann man auf der Kommandozeile oder Shell mit Ping ansprechen. Beispielsweise alle link-lokalen Geräte.

- Windows: ping -6 ff02::1
- Linux: ping6 -c 5 ff02::1

Sofern die Geräte mit dem LAN verbunden sind und keine Firewall oder eine andere Sicherheitsmaßnahme es verhindert, antworten alle IPv6-Stationen.

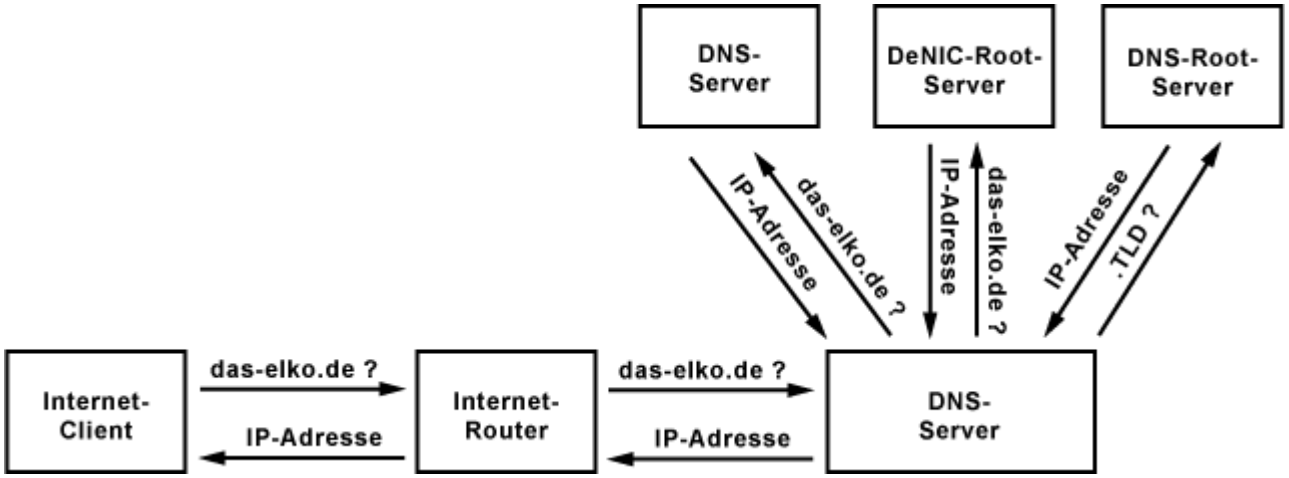
Lokales Netzwerk vs. Link-Local-Scope

Die Definition von Gültigkeitsbereichen (Scopes) ist einer der größten Unterschiede zwischen IPv4 und IPv6. Bezüglich der IPv6-Scopes gibt es in IPv4 nichts vergleichbares. Trotzdem gibt es manchmal den Vergleich zwischen den privaten IPv4-Adressen und den link-lokalen IPv6-Adressen. Doch das ist nicht das gleiche.
Wenn man vom Link-Local-Scope im Zusammenhang mit Neighbor Discovery oder Router Discovery spricht, darf man nicht vom lokalen Netzwerk sprechen. Denn in einem lokalen Netzwerk, im Sinne eines LAN, kann es auch mehrere Link-Local-Scopes geben. Beispielsweise wenn ein LAN durch IPv6-Router in mehrere Link-Local-Scopes geteilt ist.
In einem kleinen LAN, zum Beispiel in Privathaushalten, wo es nur einen Router gibt, da entspricht das lokale Netzwerk (LAN) dem Link-Local-Scope. In einem Unternehmensnetzwerk, bei dem das "LAN" aus mehreren lokalen Netzwerken besteht, kann es mehrere Link-Local-Scopes geben, die nur bis zur entsprechenden "link-lokalen" Netzgrenze reichen. Hier befindet sich ein Router, der Datenpakete mit link-lokalem Bezug nicht über die Netzgrenze hinweg weiterleitet.

23. 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 über Änderungen informieren.

DNS geht auf die Datei hosts zurück, deren Inhalt zur Namensauflösung im ARPANET diente und händisch gepflegt wurde. 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 URL (nicht die) ist eine "einheitliche Angabeform für Ressourcen" in Netzwerken. Die für DNS verwendete Struktur (URL) besteht aus drei oder mehr Teilen:

Computername (Host oder Dienst)	Second-Level-Domain (SLD)	Top-Level-Domain (TLD)
www.	elektronik-kompendium.	de
ftp.	elektronik-kompendium.	de

Manchmal befindet sich zwischen der Second-Level-Domain (SLD) und dem Computernamen eine Sub-Level-Domain (Subdomain).

Computername (Host oder Dienst)	Sub-Level-Domain (Subdomain)	Second-Level-Domain (SLD)	Top-Level-Domain (TLD)
www.	dse-faq.	elektronik-kompendium.	de

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 (Auszug)

Domain (gTLD)	Organisationsform
.aero	Lufttransportindustrie
.arpa	Alte Arpanet Domäne
.biz	Business, für große und kleinere Unternehmen
.com	Kommerzielle Domain
.coop	Kooperationen, Genossenschaften
.edu	Schulen, Universitäten, Bildungseinrichtungen
.gov	Regierungsstellen der Vereinigten Staaten von Amerika
.info	Informationsdienste
.int	International tätige Institutionen
.mil	Militär der Vereinigten Staaten von Amerika
.museum	Museen
.name	Privatpersonen
.net	Netzspezifische Dienste und Angebote
.org	Nichtkommerzielle Unternehmungen und Projekte
.pro	Professionals, spezielle Berufsgruppen
...	

Geografische Top-Level-Domains (Auszug)

Domain (ccTLD)	Land
.at	Österreich
.au	Australien
.cc	Kokos-Inseln
.ch	Schweiz
.de	Deutschland
.fr	Frankreich
.gb	Großbritannien
.ie	Irland
.it	Italien
.li	Lichtenstein
.nl	Niederlande
.no	Norwegen

.ru	Russland
.to	Tonga
.uk	Vereinigtes Königreich
...	

Nach der Top-Level-Domain (TLD) folgt die Second-Level-Domain (SLD), die einen beliebigen, aber unter der Top-Level-Domain einzigartigen Namen haben kann. Das jeweilige, für die Top-Level-Domain verantwortliche NIC verwaltet die Second-Level-Domains. Für .de (Deutschland) ist das die Denic. 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

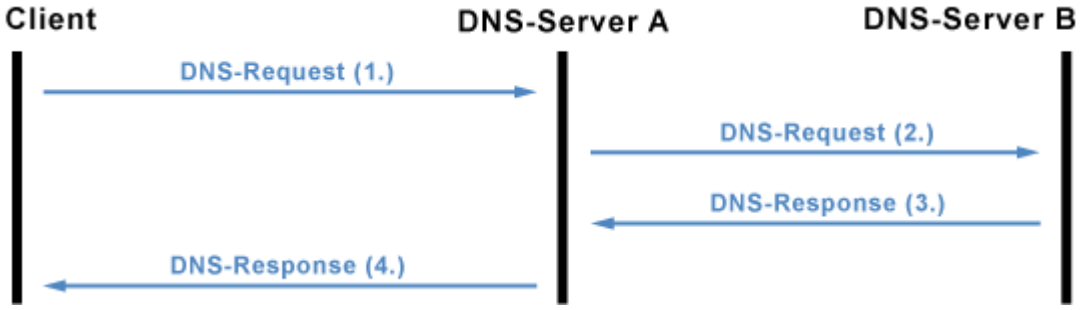
Grundsätzlich unterscheidet man zwischen der rekursiven und der iterativen Namensauflösung. Einer der beiden Abfragetypen wird zusammen mit dem Domain-Namen an den Resolver übermittelt.

- Rekursion / rekursive DNS-Abfrage

- Iteration / iterative DNS-Abfrage

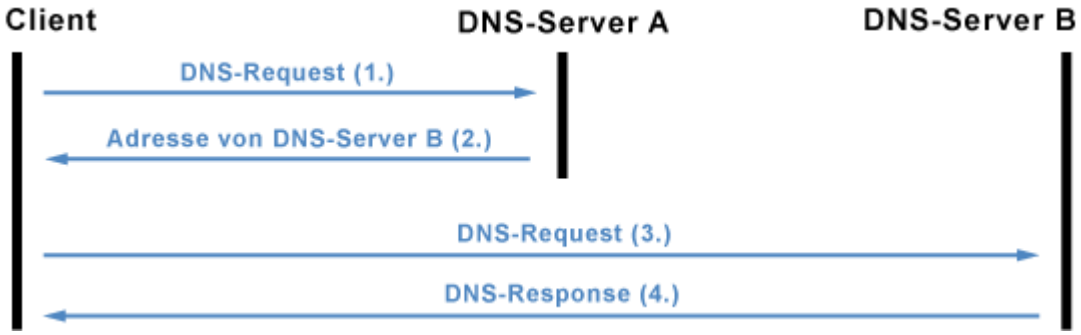
Damit ein beliebiger Server, über den nur der Domain-Name bekannt ist, kontaktiert werden kann, muss seine IP-Adresse bekannt sein. Dazu befragt der Resolver des TCP/IP-Clients den hinterlegten DNS-Server (1.).

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.).

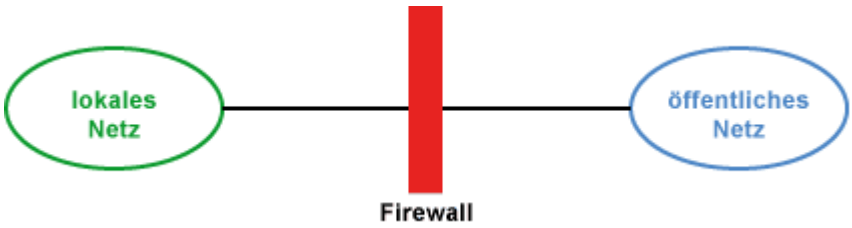
DNS-Protokoll

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).

24. 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.

Bestandteil einer Firewall

- Paketfilter mit Port- und Protokoll-Filter
- Network Adress Translation (NAT)
- Stateful Inspection

Firewall als Sicherheitsstrategie

Eine Firewall ist keine Blackbox, die Sicherheit für das lokale Netzwerk vor dem öffentlichen Netzwerk vorgaukelt. Eine Firewall ist eine technische Einrichtung, die eine Sicherheitsstrategie umsetzt, um unerwünschte, unsichere und schädigende Verbindungen zu verhindern. Ohne ständige Überwachung und Pflege bleibt nach einiger Zeit keine Schutzwirkung übrig.

Vor dem Einsatz einer Firewall ist die Akzeptanz und aktive Mitarbeit aller Beteiligten innerhalb eines lokalen Netzwerks zu gewährleisten, damit die Firewall effektiv funktionieren kann.
Am Anfang steht die Entscheidung zur Grundhaltung gegenüber Datenverbindungen. Die Firewall kann zunächst alle Verbindungen erlauben und nur bekannte und gefährliche Datenverbindungen unterbinden. Oder sie sperrt alles und alle erwünschten Datenverbindungen müssen explizit freigegeben werden.

Firewall-Strategie: Alles sperren

Alles ist gesperrt. Bekannte sichere und erwünschte Vorgänge werden freigegeben.

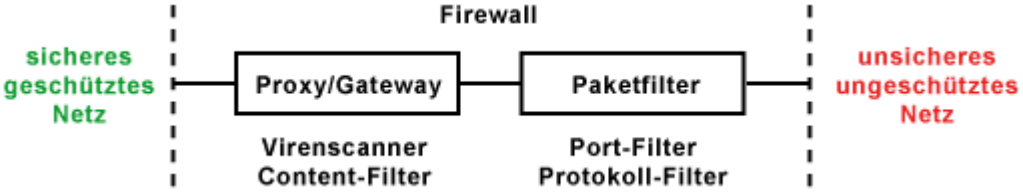
Diese Variante ist sehr sicher. Allerdings erfordert sie eine aufwendige Konfiguration der Firewall.

Firewall-Strategie: Alles freigeben

Alles ist freigegeben. Bekannte unsichere und unerwünschte Vorgänge werden gesperrt.

Diese Variante ist relativ komfortabel. Bei der Einführung ist mit keinerlei Problemen zu rechnen. Allerdings ist sie nur so sicher, wie Gefahren und Sicherheitslöcher bekannt sind und gesperrt werden.

Elemente einer Firewall



Grundsätzlich gibt es zwei verschiedene Ansätze für ein Firewall-Konzept:

- passiver Paketfilter
- 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!

Angriffsszenarien, die eine IPv6-Firewall abwehren muss

Eine Firewall für IPv4 filtert keinen IPv6-Verkehr. Und IPv6 ist nicht einfach nur ein IPv4 mit anderen Adressen. Die Erfahrungen aus der IPv4-Welt lassen sich nur bedingt auf IPv6 übertragen. Der Schutz eines LANs durch eine Firewall bedarf für IPv6 völlig neuer Regeln, die bei IPv4 bisher nicht notwendig waren.

- Umgehen der Filterregeln durch den kreativen Einsatz von Extension Header.
- IPv6-Datagramme mit vorgetäuschter Absender-Adresse aus dem internen Netz.
- Beliebige ICMPv6-Pakete
- Fluten der NDP-Table
- Überlasten der Firewall per TCP-Flooding

Es muss nicht immer zwangsläufig das Umgehen der Firewall sein. Einem Angreifer kann es schon genügen, wenn die Firewall überlastet wird und somit die Verbindung zum Internet gestört ist.

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 (bei IPv4). 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.

Next Generation Firewall

Die Bezeichnung "Next Generation Firewall" wurde von Gartner Research (Marktforschungsinstitut im Bereich IT) definiert. Diese Firewall der nächsten Generation kann im Datenstrom Anwendungen und Benutzer erkennen. Dazu gehört ein integriertes Intrusion Prevention System (IPS), die Identifikation von Anwendungen und Protokollen unabhängig vom genutzten Port und die Berücksichtigung externer Datenquellen, wie zum Beispiel Verzeichnisdienste mit Benutzerdaten.
Next Generation Firewalls gehen also über die üblichen Fähigkeiten einer Firewall, wie Paketfilter, Network Address Translation (NAT) und Stateful Inspection hinausgeht.

Insbesondere die Benutzer- und Anwendungserkennung ist für die zukünftige Sicherheit von Netzwerk extrem wichtig. Seit sich HTTP als Universalprotokoll entwickelt hat, müssen nicht mehr nur ein Browser und Webserver die Endpunkte einer HTTP-Verbindung sein. Grundsätzlich kann man mit HTTP alles transportieren. Aus Sicherheitsgründen darf man HTTP nach außen hin nicht mehr generell freigeben.

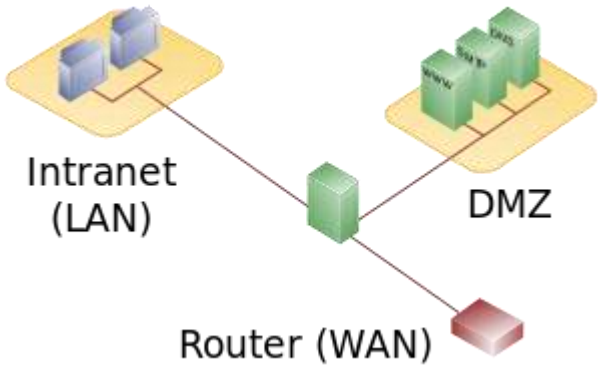
Hier setzt die Anwendungserkennung an, die versucht zu erkennen, was das System gerade überträgt. Die Anwendungserkennung übernimmt die Fähigkeiten eines Proxys bzw. Content-Filters. Aber sie muss weit mehr als das leisten. Um Anwendungen zu erkennen, bedarf es einen Abgleich mit Erkennungsmustern, ähnlich wie bei einem Virenscanner. Dabei ist es notwendig, dass diese Muster regelmäßig aktualisiert werden.

Typischerweise versucht man Google, Facebook, Youtube, Chats und Peer-to-Peer-Anwendungen zu erkennen. Wobei die meisten Anwendungen eher privater Nutzung zuzuordnen sind. Hierbei besteht der Irrweg darin, die Benutzer zu kontrollieren, anstatt Sicherheitslücken zu schließen. Sicherlich sinnvoll, wenn man bedenkt, dass der Mensch das größte Sicherheitsrisiko darstellt. Viel wichtiger wäre jedoch, dass die Firewall Anwendungen erkennt, vor denen das Unternehmensnetz tatsächlich geschützt werden muss.

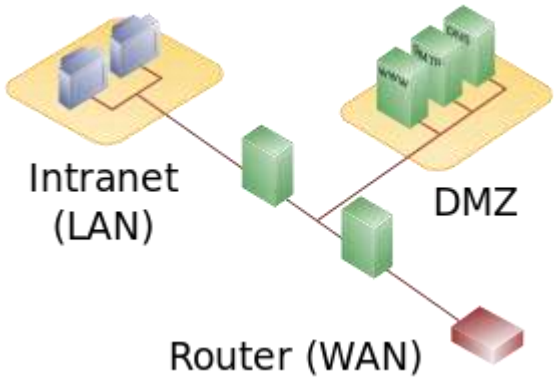
Eine Firewall sollte im Optimalfall auch der VPN-Endpunkt sein. Damit können die Firewall-Regeln auch für die VPN-Daten gelten.

25. DMZ

Demilitarized Zone



Aufbau mit einstufigem Firewall-Konzept



Aufbau mit zweistufigem Firewall-Konzept

Eine **Demilitarized Zone** (**DMZ**, auch *ent- oder demilitarisierte Zone*) bezeichnet ein Computernetz mit sicherheitstechnisch kontrollierten Zugriffsmöglichkeiten auf die daran angeschlossenen Server.

Die in der DMZ aufgestellten Systeme werden durch eine oder mehrere Firewalls gegen andere Netze (z. B. Internet, LAN) abgeschirmt. Durch diese Trennung kann der Zugriff auf öffentlich erreichbare Dienste (Bastion Hosts mit z. B. E-Mail, WWW o. ä.) gestattet und gleichzeitig das interne Netz (LAN) vor unberechtigten Zugriffen von außen geschützt werden.

Der Sinn besteht darin, auf möglichst sicherer Basis Dienste des Rechnerverbundes sowohl dem WAN (Internet) als auch dem LAN (Intranet) zur Verfügung zu stellen.

Ihre Schutzwirkung entfaltet eine DMZ durch die Isolation eines Systems gegenüber zwei oder mehr Netzen.

Exposed Host als „Pseudo-DMZ“

Einige Router für den Heimgebrauch bezeichnen die Konfiguration eines Exposed Host fälschlicherweise als „DMZ“. Dabei kann man die IP-Adresse eines Rechners im internen Netz angeben, an den alle Pakete aus dem Internet weitergeleitet werden, die nicht über die NAT-Tabelle einem anderen Empfänger zugeordnet werden können. Damit ist der Host (auch für potentielle Angreifer) aus dem Internet erreichbar. Eine Portweiterleitung der tatsächlich benutzten Ports ist dem - falls möglich - vorzuziehen.

Es hängt von der konkreten Konfiguration der Firewall ab, ob zunächst die Portweiterleitungen auf andere Rechner berücksichtigt werden und erst danach der Exposed Host, oder ob der Exposed Host die Portweiterleitungen auf andere Rechner unwirksam macht.

Dirty DMZ

Als dirty DMZ oder dirty net bezeichnet man im Allgemeinen das Netzsegment zwischen dem Perimeterrouter und der Firewall des (internen) LAN. Diese Zone hat von außen nur die eingeschränkte Sicherheit des Perimeterrouters. Diese Version der DMZ liefert einen Performancegewinn, da die eingehenden Daten nur einfach (Perimeterrouter) gefiltert werden müssen.

Protected DMZ

Mit protected DMZ bezeichnet man eine DMZ, die an einem eigenen LAN-Interface der Firewall hängt. Diese DMZ hat die individuelle Sicherheit der Firewall. Viele Firewalls haben mehrere LAN-Interfaces, um mehrere DMZs einzurichten.

26. WLAN

WLAN-Übertragungstechnik

4	**Transport-Schicht (TCP)**	**TCP**

3	**Netzwerk-Schicht (IP)**	**IP**
2	**Logical Link Control (LLC)**	**802.2**
	Medium Access Control (MAC)	**CSMA, VCD**
1	**Physical Layer Convergence Protocol (PLCP)**	**DSSS, FHSS, Infrarot**

Der Funknetz-Standard IEEE 802.11 definiert einen gemeinsamen MAC-Layer (Medium Access Control) für drei spezifische Physical Layer (PHY). Zwei davon sind den Funk-LANs, einer dem Infrarotnetz zugeordnet. Im Funknetz wird als Frequenzbereich das ISM-Band (2,4 GHz) von 2,400 bis 2,4835 GHz genutzt.
Die Infrarot-Variante ist so gut wie unbekannt. Sie nutzt die Frequenzen von 850 bis 950 Nanometer (Licht). Die verwendete diffuse IR-Übertragung erfordert keine exakte Ausrichtung von Sender und Empfänger. Die maximal 10 Meter weite Sichtlinie sollte trotzdem hindernisfrei sein, um unnötige Beeinträchtigungen bei der Datenübertragung auszuschließen.

Die Funktechnik sieht mehrere Modulationsverfahren vor, die mit dem Bandspreizverfahren arbeiten. Dabei wird das Funksignal über ein möglichst breites Frequenzspektrum aufgeteilt. Diese Methode verringert den Einfluss von schmalbandigen und breitbandigen Störungen.

WLAN-Frame nach IEEE 802.11

IEEE 802.11 hat Ethernet als Basistechnik und verfügt deshalb auch über dessen Frame-Typen und Zugriffsmethoden. IEEE 802.11 kennt drei verschiedene Frame-Typen. Darunter Control-, Management- und Daten-Frames. Normale WLAN-Adapter müssen nur einen Teil dieser Frames verstehen. Manches bleibt Access Points vorbehalten, die alle Dienste beherrschen müssen.

Präambel	802.11-Header	IV	SNAP	Ethernet-Frame	Prüfsumme
20 µs	24 bis 32 Byte	4 oder 8 Byte	8 Byte	maximal 2304 Byte	4 Byte

Im Prinzip wird ein Ethernet-Frame in einem WLAN-Frame eingebettet übertragen. Das Ethernet-Frame kann deutlich länger sein als bei Fast-Ethernet. Während ein normales Ethernet-Frame maximal 1518 Byte haben darf, darf das Ethernet-Frame über WLAN 2304 Byte betragen. Bei längeren Frames lassen sich die Anzahl der Header reduzieren und so die Übertragungsrate erhöhen.
Damit die Frames über WLAN übertragen werden können, werden bis zu 64 Byte an Header und Prüfsummen hinzugefügt und eine Präambel von 20 µs vorangestellt. Die Präambel dient zum Synchronisieren des Empfängers. Es folgt der 802.11-Header mit bis zu 32 Byte. Der Sequenzzähler (IV) wird bei verschlüsselten Paketen benötigt und beträgt 4 oder 8 Byte. Der LLC-SNAP-Header wird benötigt, um Ethernet-Pakete über Nicht-Ethernet-Medien zu transportieren. Er benötigt 8 Byte. Dann folgt das eigentliche Ethernet-Frame mit maximal 2304 Byte und die Prüfsumme mit 4 Byte.

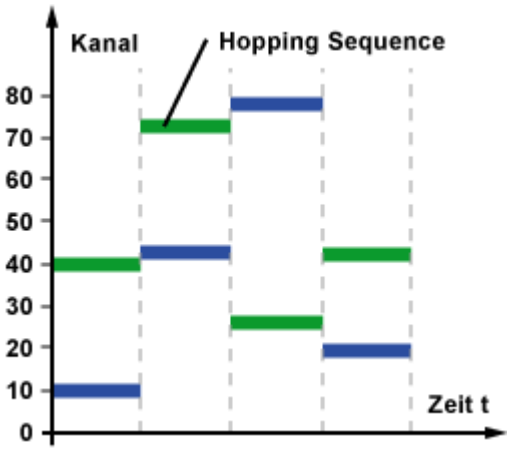
Strom-Spar-Funktionen / Power-Saving

WLAN kommt vor allem in mobilen und damit Akku-betriebenen Geräten vor. Zum Beispiel Smartphones, Tablets und Notebooks. Um die Akku-Laufzeit dieser Geräte zu verlängern gibt es spezielle Strom-Spar- und Power-Management-Funktionen.
Die Traffic-Indicator-MAP (TIM) ist eine Liste, die der Access Point erstellt, um dort alle Wireless-Stationen zu speichern. Um diese Liste aktuell zu halten, schickt der Access Point regelmäßig TIM-Signale (Beacons), die die Wireless-Stationen aufwecken.
Die Delivery-Traffic-Indicator-MAP (DTIM) ist auch eine Liste, die vom Access Point gepflegt wird. Der DTIM-Beacon ist ein Broadcast-Signal, das mit einem größeren zeitlichen Abstand gesendet wird, als der TIM-Beacon. Im Regelfall werden WLAN-Netzwerkkarten nur mit dem DTIM-Beacon aufgeweckt um die Laufzeit mobiler Geräte noch weiter zu erhöhen.
Für den TIM- bzw. DTIM-Beacon gibt es häufig Einstellungen im Access Point, wie häufig er gesendet werden soll. In der Regel lässt man von diesen Einstellungen die Finger.

IEEE 802.11d - World Mode - Global Harmonization

Der Standard IEEE 802.11d fällt unter dem Betriff "Global Harmonization" und wird auch als "World Mode" bezeichnet. Er regelt die technischen Unterschiede in unterschiedlichen Ländern und Regionen. Hierzu gehört auch die Definition der Anzahl und Auswahl der Kanäle, die in einem Land für die Nutzung von WLAN freigegeben sind.
Ebenso ist die Auswahl der Basistechnologie, also ob IEEE 802.11 a, h, b, g oder n verwendet werden darf, geregelt. Für den WLAN-Nutzer ist es dank IEEE 802.11d unerheblich, welcher Standard verwendet wird. Er muss lediglich seinen aktuellen Standort angeben. Der WLAN-Client arbeitet dann mit den jeweils zugelassenen Standards.
In der Praxis sieht das so aus, dass ein WLAN-Router oder WLAN-Client ein Länderprofil hinterlegt hat, anhand dessen er die notwendigen Einstellungen vornimmt.

FHSS - Frequency Hopping Spread Spectrum



FHSS ist Teil des Ursprungsstandards von IEEE 802.11. Es beschreibt, wie das Frequenzspektrum aufgeteilt wird. Sender und Empfänger nutzen für die Übertragung die 79 Kanäle im 2,4 GHz-Band und teilen die Datenpakete in kleine Häppchen auf. Durch die Vergabe einer bestimmten Hopping-Sequence werden die Kanäle nach einem Zufallsmuster gewechselt. Die vorgegebene Mindestsprungdistanz beträgt 6 Kanäle, also 6 MHz. Insgesamt lässt sich dieser Frequenzbereich mit 26 Teilnehmern betreiben, ohne dass sie sich die Übertragungsrate teilen müssen.
Diese Technik ist sehr anfällig gegen Störungen, vor allem dann, wenn gestörte Frequenzen aus dem Sprungmuster ausgelassen werden. Sollte auf einem Kanal dann doch mal zwei

Übertragungen miteinander kollidieren, werden diese Datenpakete einfach nochmal übertragen. Da die Kollisionen in einem Funknetz nicht erkannt werden können, kommt ein Verfahren zur Kollisionsvermeidung zum Einsatz (CSMA/CA).
FHSS ist relativ kostengünstig und stromsparend, was bei kleinen mobilen Geräten ein großer Vorteil ist. Der enorme Verwaltungsaufwand bei den Frequenzsprüngen drückt jedoch auf die Nutzdatenrate, verkompliziert das Roaming zwischen mehreren Access Points und hat nur eine begrenzte Reichweite.
Frequency Hopping hat einen entscheidenden Nachteil. Es lässt sich damit nur maximal 2 MBit/s erreichen. WLAN nach IEEE 802.11b verwendet daher DSSS als Modulationsverfahren und überbrückt damit größere Distanzen mit einer schnelleren Datenübertragungsrate.

Probleme durch IEEE 802.11

Obwohl IEEE 802.11 protokollunabhängig arbeitet, können sich Probleme in der Praxis mit einigen Protokollen und Anwendungen ergeben. Ausschlaggebende Faktoren sind die höhere Bitfehlerrate (Bit Error Rate, BER) und die größere Verzögerung bei der Übertragung von Daten. Es liegt in der Natur eines Wireless LAN, dass die zur Übertragung benötigte Zeit länger ist als im drahtgebundenen LAN. Ein einfacher Ping hat im drahtgebundenen LAN eine Round Trip Time von weniger als einer Millisekunde. Im Wireless LAN liegt die Zeit für ein Ping bei bis zu vier Millisekunden.
Anwendungen, die ein kurze Verzögerungszeit zwischen Senden und Empfangen (Delay) benötigen, haben mit einem Wireless LAN unter Umständen Schwierigkeiten.

WLAN-Sicherheit

In physikalischen Netzen, mit Leitungen und Kabel, setzt das Abhören der Kommunikation das physikalische Anzapfen der Leitung voraus. Da Netzwerkkabel in der Regel innerhalb gesicherter Gebäude und verdeckt verlaufen, ist das Abhören von Anfang an erschwert.
In einem Funknetz sieht das ganz anders aus. Hier dient der freie Raum als Übertragungsmedium. Sobald ein drahtloses Gerät seine Daten abstrahlt, benötigt ein Angreifer nur ein Empfangsgert, um sich zumindest Zugang zum Funksignal zu verschaffen. Aus diesem Grund sind Sicherheitsvorkehrungen zu treffen, die Funksignal für den Angreifer unbrauchbar machen.

Am Anfang der WLAN-Entwicklung war der IEEE-Standard 802.11 ein einziges Sicherheitsrisiko. Die Datenübertragung war nicht nur abhörbar, sondern auch unverschlüsselt. Bei der privaten Nutzung ist das ok. 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 einem 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 WLANs 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 oder unzureichend verschlüsselten 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 SSL, SSH und IPsec lässt sich die Kommunikation zwischen Anwendungen sicherer machen.
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. eigenes Admin-Passwort für den Access Point vergeben
2. WPA2-Verschlüsselung einschalten
3. undefinierbare SSID vergeben (sehr empfehlenswert)
4. MAC-Adressfilter einsetzen
5. SSID-Broadcast abstellen (nicht empfehlenswert)
6. WLANs von anderen Netzwerk-Segmenten logisch trennen
7. VPN einsetzen
8. Firewall zwischen WLAN und LAN installieren
9. IDS im WLAN aufstellen
10. regelmäßige Audits mit aktuellen Hacker-Tools

WLAN-Sicherheit: MAC-Adressfilter als Sicherheits-Tool?

Der MAC-Adressfilter schränkt die Nutzung des WLANs auf freigeschaltete MAC-Adressen ein, die einem bestimmten WLAN-Adapter zugeordnet ist. Doch 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. Der Angreifer kann die eigene MAC-Adressen mit einer freigegebenen überschrieben. Somit wäre der MAC-Adressfilter umgangen.

WLAN-Sicherheit: 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, in 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 können.
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 oder sogar Totalausfälle.
Auch 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. Wer einen WLAN-Router oder Access Point betreibt sollte darauf achten, dass die Verschlüsselung immer eingeschaltet ist.

WEP - Wired Equivalent Privacy

WEP ist ein Verschlüsselungsverfahren für WLANs, die dem Standard IEEE 802.11 entsprechen. Dazu wird in jedem WLAN-Endgerät Schlüssel (Passwort) hinterlegt, dem niemand bekannt ist und auch nicht nachvollziehbar sein sollte.
Trotz des offenen Übertragungsmediums Funk soll WEP ein Funknetzwerk genauso abhörsicher machen, wie es ein kabelgebundenes Netzwerk ist. Dazu stellt WEP Funktionen für die Paketverschlüsselung und zur Authentifizierung zur Verfügung.

Hinweis: WEP gilt als veraltet und sollte nicht mehr verwendet werden. Ein WLAN sollte immer mit WPA2 (IEEE 802.11i) abgesichert werden. WLAN-Geräte, die WPA2 nicht unterstützen, sollten dringend ausgetauscht und nicht mehr eingesetzt werden. Ab 2013 dürfen neue Access Points kein WEP mehr anbieten. Ab 2014 dürfen WLAN-Geräte, wie zum Beispiel Notebooks und WLAN-Sticks kein WEP mehr unterstützen.

Die folgende Beschreibung zu WEP, soll dokumentieren, warum WEP nicht mehr eingesetzt werden sollte.

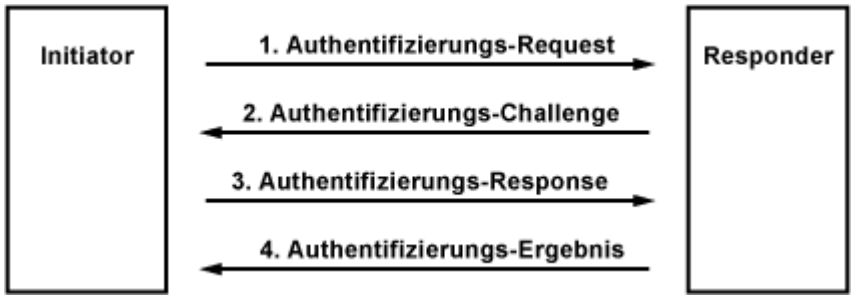
WEP-Konfiguration

Bei der Konfiguration von WEP gibt es in der Regel 3 Varianten zum Einstellen bzw. Konfigurieren.

1. **WEP ist deaktiviert.**
   Eine Verschlüsselung der Daten findet nicht statt. Zur Authentifizierung wird das Verfahren "Open System" verwendet.
2. **WEP ist aktiviert und wird zur Verschlüsselung verwendet.**
   Die mobilen Stationen und der Access Point verschlüsseln und entschlüsseln die Daten mit dem hinterlegten WEP-Code. Zur Authentifizierung wird das Verfahren "Open System" verwendet.
3. **WEP ist aktiviert und wird zur Verschlüsselung und Authentifizierung verwendet.**
   Die mobilen Stationen müssen sich über das Verfahren "Shared Key" vom Access Point authentifizieren lassen. Zusätzlich werden alle Daten verschlüsselt übertragen.

Authentifizierung

Die Authentifizierung unterscheidet zwei Verfahren. Das Open System Authentication ist die Standard-Authentifikation. Sie schaltet für ein WLAN alle Clients frei. Es findet praktisch keine Authentifizierung statt.
Shared Key Authentication ist die sichere Variante mittels einem Challenge-Response-Verfahren mit einem geheimen Schlüssel zur Authentifizierung. Das Challenge-Response-Verfahren basiert auf dem Austausch von 4 Nachrichten zwischen einem Initiator und einem Responder.



1. Die mobile Station schickt eine Authentifizierungsanforderung an den Access-Point.
2. Der Access-Point schickt einen Zufallstext (Challenge) an die mobile Station.
3. Die Station verschlüsselt den Text mit dem vorkonfigurierten 64- oder 128-Bit WEP-Code und sendet ihn an den Access-Point.

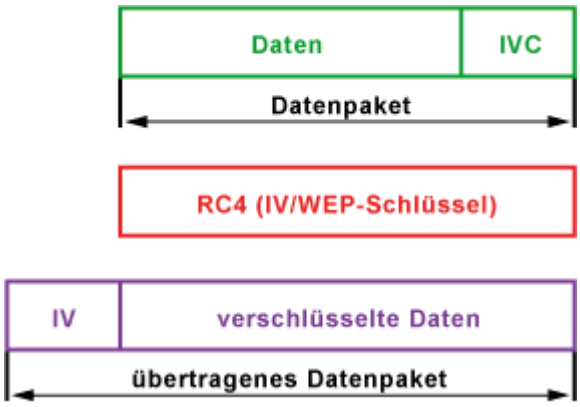
4. Der Access-Point entschlüsselt den Text mit dem eigenen bekannten WEP-Code. Wenn der verschickte Text mit dem erzeugten Zufallstext übereinstimmt, dann ist auch der WEP-Code identisch. Der Access-Point bestätigt die Identität der Station.
5. Die mobile Station stellt eine Verbindung zum Access-Point her.

Die 4 Nachrichten der WEP-Authentifikation sollen sicherstellen, dass der Initiator zugriffsberechtigt ist. In der Regel ist das WLAN-Endgerät der Initiator und der Access Point (AP) der Responder. Eine gegenseitige Authentifizierung lässt sich durch das Vertauschen der beiden Stationen und Wiederholen des Challenge-Response-Verfahrens erreichen.
Der Haken an WEP ist die manuelle Konfiguration des Schlüssels auf allen WLAN-Endgeräten. Dazu ist eine Person nötig, die sich um die Verwaltung der geheimen WEP-Schlüssel kümmert. Dynamische Sitzungsschlüssel oder Schlüsselzertifizierung ist in WEP nicht vorgesehen.

Verschlüsselung

Die Verschlüsselung erfolgt mit dem Verschlüsselungsverfahren RC4. Es handelt sich dabei um eine Datenstromchiffrierung von RSA Data Security.
Das mit WEP verschlüsselte WLAN-Datenpaket besteht aus mehreren Teilen:

- geheimer WEP-Schlüssel mit 40 (WEP40/WEP64) oder 104 (WEP104/WEP128) Bit
- 32-Bit-Prüfsumme der unverschlüsselten Daten (Integrity Check Value, ICV)
- 24-Bit Initialisierungsvektor (IV) der den WEP-Schlüssel zum Gesamtschlüssel mit 64 Bit oder 128 Bit macht und einmal pro Datenpaket inkrementiert (-1) wird



Das Datenpaket setzt sich aus den Daten und der 32-Bit-Prüfsumme der Daten zusammen. Dieses Datenpaket wird mit der IV-WEP-Schlüssel-Kombination verschlüsselt. Den verschlüsselten Daten wird der IV vorangestellt, damit der Empfänger den RC4-Schlüssel aus IV- und WEP-Schlüssel zusammensetzen und die verschlüsselten Daten entschlüsseln kann. Da der IV in Klartext übertragen wird, erfolgt die effektive Verschlüsselung nur mit 40 bzw. 104 Bit, obwohl gerne von 64 bzw. 128 Bit gesprochen wird.

Sicherheitsprobleme

WEP ist ein Verfahren um ein WLAN zu verschlüsseln. Trotzdem ist es möglich den Schlüssel zu knacken. Dazu muss die ablaufende WLAN-Kommunikation abgehört werden. Dazu ist nur eine handelsübliche Hardware nötig, die mit modifizierter Firmware oder auch nur mit entsprechenden Treibereinstellungen zu passiven Attacken geeignet ist.

Bis zum Herausfinden des WEP-Schlüssels reicht es, den in Klartext vorliegenden IV-Schlüssel mitzuprotokolieren. Insgesamt gibt es nur 16.777.216 (2^{24}) Schlüsselmöglichkeiten, die aufgrund der inkrementierenden Zählweise irgendwann wiederholt werden müssen. Ein durchschnittlich belasteter 11-MBit-Access-Point würde diesen Zahlenraum in ca. einer Stunde wiederholen.
Mit relativ einfachen Mitteln lässt sich dann der WEP-Schlüssel zurückberechnen. Die verschlüsselten Datenpakete können dann entschlüsselt werden.

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 2

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. Im Regelfall arbeitet die Verschlüsselung der üblichen WLAN-Komponenten mit WPA2 als Verschlüsselungsverfahren.

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

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.

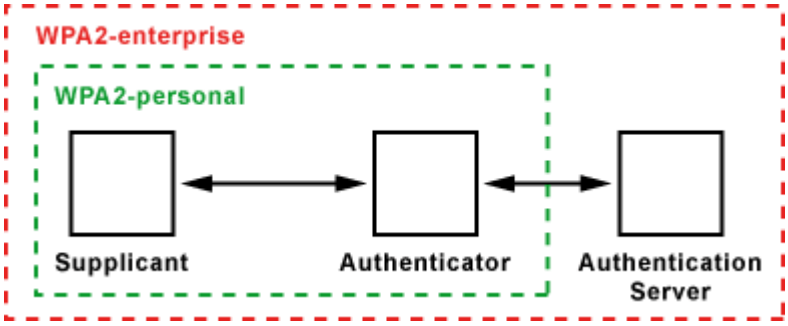
WPA2-enterprise

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, 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 bzw. WPA2 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 (86.400 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.

WPS - WiFi Protected Setup

WPS ist eine Konfigurationsautomatik und eine Spezifikation des Industriekonsortiums WiFi Alliance (WFA). WPS erleichtert die WLAN-Konfiguration von WLAN-Clients. Entweder per Knopfdruck (WPS-PBC) oder Zahleneingabe (WPS-PIN).

Die Hauptschwierigkeit bei der WLAN-Konfiguration eines WLAN-Clients ist die Vergabe des WLAN-Passworts (WPA2-Schlüssel), welches im Access Point hinterlegt ist. Die Verfahren von WPS sollen diese Umständlichkeit vereinfachen und automatisieren.

Konfiguration per Knopfdruck (WPS-PBC)

Bei der WPS-Push-Button-Methode zur WLAN-Client-Konfiguration benötigt der Access Point einen WPS-Button am Gehäuse. Nach dem Drücken wird die WPS-Anmeldephase gestartet. Für eine kurze Zeit bekommen neu angemeldete WLAN-Clients automatisch das WPA2-Passwort mitgeteilt.
WPS-PBC ist nur so lange sicher, wie man sicherstellt, dass kein fremder WLAN-Client während der Anmelde-Phase in der Nähe ist.

Konfiguration per Zahleneingabe (WPS-PIN)

Die Konfiguration der WLAN-Clients per Zahleneingabe sieht vor, dass der Schlüssel für WPA/WPA2 automatisch dem WLAN-Client mitgeteilt wird, wenn eine korrekte PIN eingegeben wurde. Dann übermittelt der Access Point dem Client ein Einrichtungspaket mit WPA2-Passwort. Die WPS-PIN besteht typischerweise aus acht Ziffern, wobei die letzte Ziffer die Prüfsumme ist. Es gibt aber auch eine WPS-PIN mit 4 Stellen, was einen weniger sicheren Schlüsseltausch bedeutet. Die WPS-PIN ist in der Regel auf der Rückseite des WLAN-Access-Points aufgedruckt. Es wird empfohlen WPS auszuschalten, nachdem die Clients mit WPS konfiguriert wurden.

Wie sicher ist WPS?

WPS ist einigermaßen sicher, da der Angreifer sich im Funkbereich des WLAN-Access-Points bzw. -Routers befinden muss. In der Regel kann man davon ausgehen, dass das Abgreifen der WPS-PIN in der Theorie möglich aber eher unrealistisch ist. Um in ein WLAN einzubrechen oder verschlüsselten Datenverkehr zu entschlüsseln gibt es andere Methoden.

Ein Angriffspunkt bei WPS-PIN ist, wenn der Access-Point die PIN erzeugt. Die Sicherheitslücke kann dadurch entstehen, wenn der Zufallsgenerator im Rahmen des Diffie-Hellman-Schlüsselaustauschs, der die PIN erzeugt, nicht ausreichend zufällige Zufallszahlen (Nonces) erzeugt. Weil der Umfang der möglichen PINs dadurch kleiner ist lässt sich die achtstellige WPS-PIN leichter errechnen. Wenn WPS-PIN eingeschaltet ist, dann könnte ein Angreifer rund um die Uhr versuchen, sich mit hochgezählten PINs anzumelden. Irgendwann wird er die richtige WPS-PIN erwischen.
Durch diese Sicherheitslücke kann sich ein Angreifer ohne Kenntnis des WLAN-Schlüssels auf das Funknetz unsicherer WLAN-Access-Points und -Router Zugriff verschaffen.

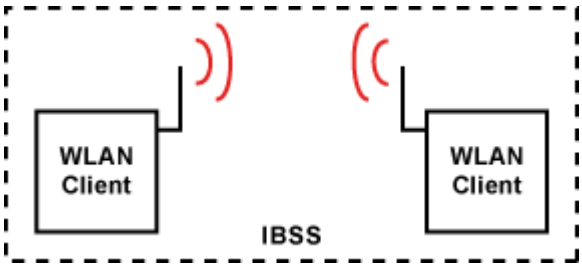
Einschränkend muss man sagen, dass dieses Problem nicht alle WLAN-Access-Points und -Router betrifft. Denn es ist kein generelles Problem von WPS, sondern steht im Zusammenhang mit einer schlechten Implementierung des Zufallszahlengenerators.
Das beschriebene Problem hat man nicht, wenn man WPS-PBC einsetzt. Bei dieser Methoden setzt man auf einen physischen Tastendruck am Gerät.
Bei anderen Implementierungen müssen die Nutzer eine WPS-PIN selbst vergeben. Und die Funktion ist ab Werk deaktiviert.
Generell kann man sagen, dass es eine gute Idee ist WPS im Router abzuschalten, wenn man es gerade nicht braucht.

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.

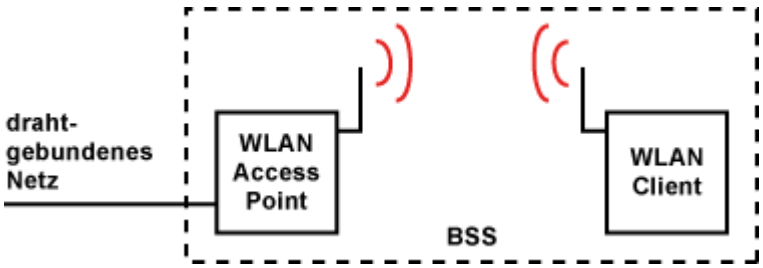
IBSS - Independent Basic Service Set



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.
Die Topologie dieses Ad-hoc-Netzwerks nennt sich Independent Basic Service Set (IBSS).
Solange sich die Stationen gegenseitig in Reichweite befinden, 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 Bluetooth schneller realisiert.

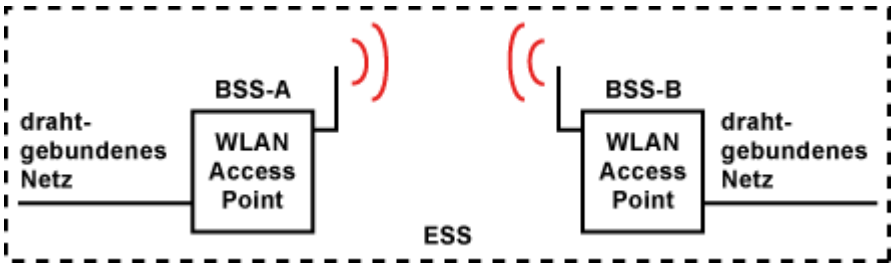
BSS - Basic Service Set



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

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

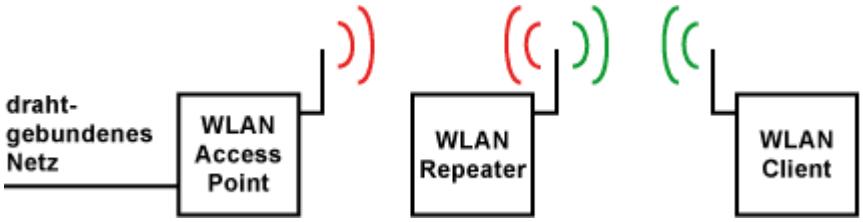
Mittels zweier Access Points lässt sich auch die Reichweite eines kabelgebundenen Netzwerkes erhöhen. Bei einer Infrastruktur auf Basis von 10Base-T/100Base-TX dürfen die einzelnen Kabelsegmente eine Maximallänge von 100 Metern haben. Mit Wireless LAN besteht die Möglichkeit, Bereiche zu verbinden, die 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 Extended 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.

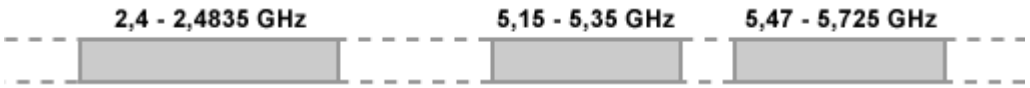
WDS - Wireless Distribution System (WLAN-Repeater)

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



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

WLAN-Frequenzen

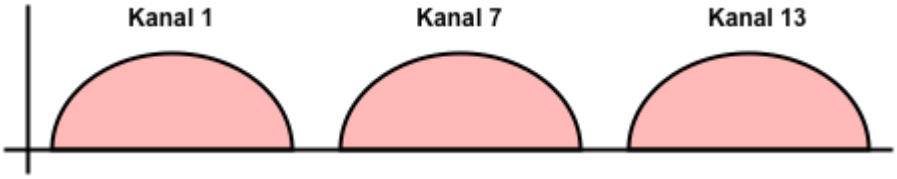


Für WLAN stehen zwei Frequenzbereiche zur Verfügung. Der eine Bereich liegt bei 2,4 GHz, der andere bei 5 GHz. Beide Frequenzbereiche sind weltweit Lizenz-frei nutzbar. Das bedeutet, dass auf privatem Grund und Boden für die Nutzung keine Gebühren bezahlt werden müssen. Das bedeutet aber auch, dass sich 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.

Aber, im Frequenzband 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.
Weniger im Gebrauch ist das Frequenzband um 5 GHz. Allerdings ist auch hier in Zukunft mit der Zunahme der Nutzung durch WLANs zu rechnen.

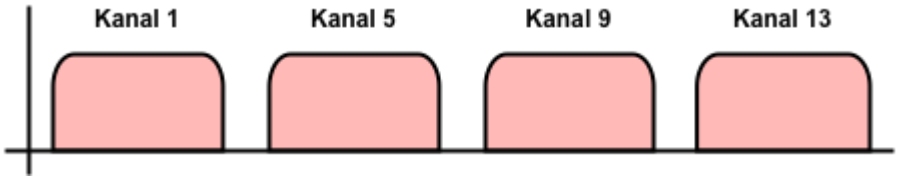
Im Folgenden wird beschrieben, wie die Frequenzbereiche um 2,4 und 5 GHz von den verschiedenen WLAN-Standards aufgeteilt werden, um das Frequenzspektrum möglichst optimal auszunutzen.

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



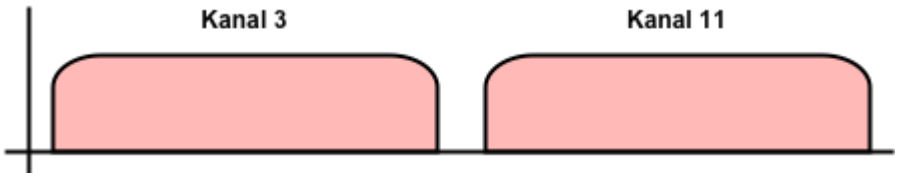
Bei einem WLAN mit IEEE 802.11b empfiehlt es sich, die Kanäle 1, 7 oder 13 einzustellen. Hierbei handelt es sich, bei einer Kanalbreite von 22 MHZ (DSSS), um die überlappungsfreien Kanäle, bei denen das Frequenzspektrum um 2,4 GHz optimal ausgenutzt wäre.

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.
Bei einer Kanalbreite von 20 MHz und 16,25 MHz pro Träger empfiehlt es sich die Kanäle 1, 5, 9 oder 13 einzustellen. Das ermöglicht die optimale Ausnutzung des Frequenzspektrums um 2,4 GHz.

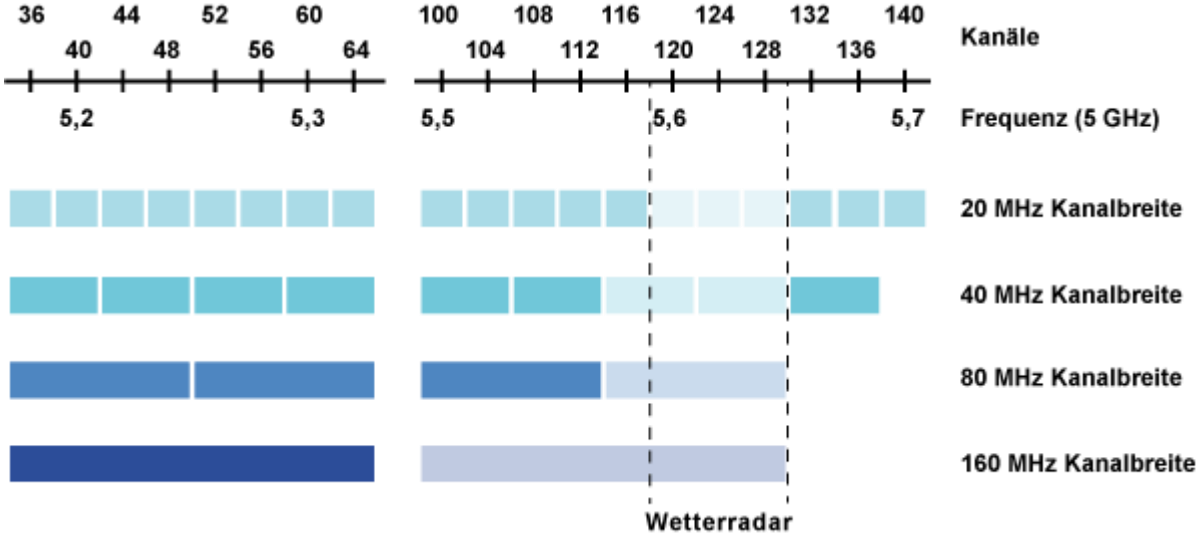
WLAN-Kanäle bei IEEE 802.11n (2,4 GHz, 40 MHz Kanalbreite)



Bei einem WLAN mit IEEE 802.11n mit einer Kanalbreite von 40 MHz (OFDM) und 33,75 MHz pro Träger empfiehlt es sich, die Kanäle 3 (1+5) oder 11 (9+13) einzustellen.

In der Praxis vermeidet man es, ein WLAN mit IEEE 802.11n bei 2,4 GHz mit einer Kanalbreite von 40 MHz einzurichten. Dabei wäre das Frequenzspektrum mit 2 WLANs voll belegt. Damit auch WLANs mit IEEE 802.11g parallel betrieben werden können, sollten WLANs mit IEEE 802.11n auch nur mit 20 MHz Kanalbreite eingerichtet sein.

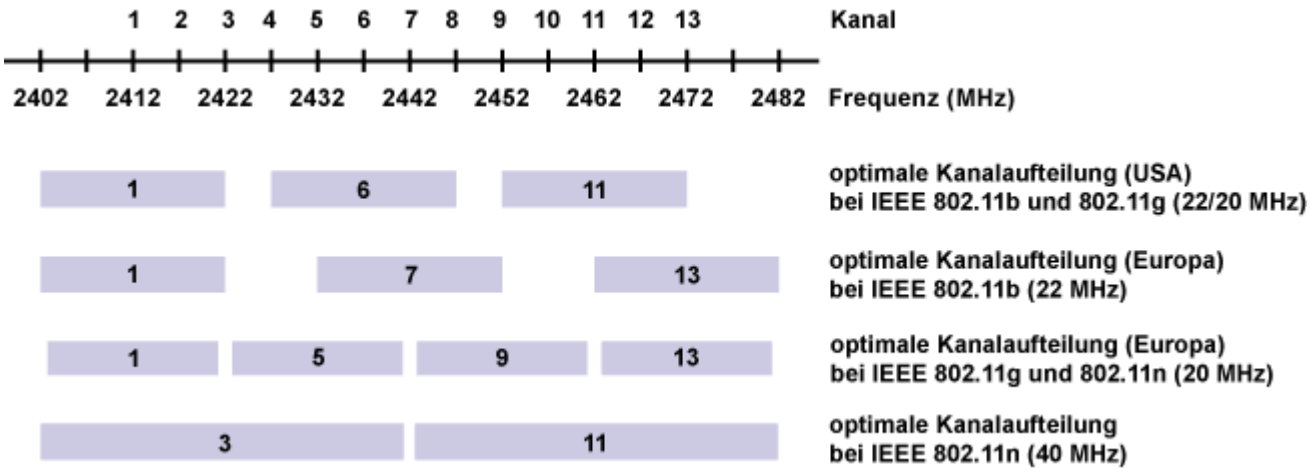
WLAN-Kanäle bei IEEE 802.11ac (5 GHz, 19 Kanäle, 40, 80 und 160 MHz Kanalbreite)



In der EU sind zwei Bereiche im 5-GHz-Frequenzband nutzbar. 5150 bis 5350 MHz (Kanal 36 bis 64) und 5470 bis 5725 MHz (Kanal 100 bis 140). In anderen Ländern liegen die Grenzen eventuell anders.
Zusammenfassend kann man sagen, dass es in der EU im 5-GHz-Frequenzband 19 je 20 MHz breite Kanäle gibt, wovon 3 vom Wetterradar genutzt werden. Damit WLAN-Basisstationen in der EU alle 19 Kanäle nutzen dürfen, müssen sie die Signale anderer Funksysteme erkennen und durch Kanalwechsel ausweichen können (DFS). Weiterhin gilt die Anordnung, dass nur mit DFS (Dynamic Frequency Selection) und TPC (Transmit Power Control) die Kanäle oberhalb von Kanal 48 genutzt werden dürfen. DFS ist notwendig, um bspw. den Betrieb des Wetterradars nicht zu stören.

Möchte man im 5-GHz-Frequenzband 40 MHz breite Kanäle nutzen, teilt sich das Frequenzband in 9 je 40 MHz breite Kanäle auf, wovon wegen dem Wetterradar nur 7 störungsfrei nutzbar sind.
Möchte man im 5-GHz-Frequenzband 80 MHz breite Kanäle nutzen, teilt sich das Frequenzband in 4 je 80 MHz breite Kanäle auf, wovon wegen dem Wetterradar nur 3 störungsfrei nutzbar sind.
Möchte man im 5-GHz-Frequenzband 160 MHz breite Kanäle nutzen, teilt sich das Frequenzband in 2 je 160 MHz breite Kanäle auf, wovon wegen dem Wetterradar nur eines störungsfrei nutzbar ist. Falls das Frequenzband nicht groß genug für einen 160 MHz breiten Kanal ist, kann IEEE 802.11ac auch 2 spektral getrennte 80-MHz-Kanälen zusammenfassen (Discontiguous Mode).

Welche Kanalverteilung um 2,4 GHz ist richtig? 1-6-11, 1-7-13 oder 1-5-9-13?



Um das Frequenzspektrum um 2,4 GHz optimal ausnutzen zu können ist eine bestimmte Kanalverteilung notwendig. Der Grund ist, dass die eigentlichen Kanäle im 2,4-GHz-Frequenzband für WLAN zu schmal sind und man deshalb einzelne Kanäle zusammenfasst bzw. einen breiteren Kanal nutzt, als ursprünglich vorgesehen. Das bedeutet aber auch, dass sich die Kanäle überlappen, wenn die Kanalverteilung willkürlich erfolgt. Deshalb gibt es die folgenden Empfehlungen: 1-6-11, 1-7-13 oder 1-5-9-13. Doch welche davon ist die richtige?

Es gibt hierbei nicht DIE richtige Antwort. Es kommt darauf an, welche Geräte eingesetzt werden, wie viele Basisstationen sich das Frequenzspektrum um 2,4 GHz teilen müssen und wer sich um die Kanalverteilung kümmert.

Das absolute Optimum würde man mit der Kanalverteilung 1-5-9-13 erreichen. Dann könnten man 4 WLAN-Basisstationen mit je 20 MHz Kanalbreite parallel betreiben. Leider lässt sich ein Funksignal nicht einfach auf 20 MHz begrenzen. Sondern es streut in die benachbarten Kanäle hinein und stört dort das Funksignal. Deshalb empfiehlt sich die Kanalverteilung 1-7-13. Hier kann man nur 3 WLAN-Basisstationen parallel betreiben. Im Gegenzug ist der Abstand zwischen den Kanälen größer und die gegenseitige Störung geringer.

Dummerweise sind in den USA die Kanäle 12 und 13 nicht für WLAN freigegeben. Dort wird deshalb die Kanalverteilung 1-6-11 verwendet, was uns in Deutschland bzw. EU egal sein könnte. Leider unterstützen die in Deutschland erhältlichen Geräte die Kanäle 12 und 13 nicht immer. Beispielsweise wenn die Geräte für die USA hergestellt wurden. Die Rede ist von ca. 30% der in Deutschland erhältlichen Geräte. In diesen Fällen ist die Hardware und Software nicht auf das Frequenzspektrum in Deutschland und die EU angepasst. Das bezieht sich sowohl auf WLAN-Clients in Notebooks, Smartphones und Tablets, als auch auf WLAN-Basisstationen. Manchmal hilft ein Firmware- oder Treiber-Update. Wenn nicht, dann muss der WLAN-Adapter oder eventuell das ganze Gerät getauscht werden. Im Zweifelsfall muss man mit einem kastrierten Gerät leben.

Um Beeinträchtigungen durch die fehlende Kanalunterstützung (12 und 13) zu vermeiden sollte man im Frequenzspektrum um 2,4 GHz konsequenterweise nur die Kanalverteilung 1-6-11 nutzen. Das Vernünftigste ist jedoch nicht die manuelle Kanalwahl, sondern die automatische Kanalwahl. Standardmäßig benutzen WLAN-Basisstationen 1-11 als Autokanal was dann häufig zu 1-6-11 führt.

Ein Problem ist, dass immer mehr WLAN-Router auf den Markt kommen bei denen Kanalbündelung (20 MHz + 20 MHz = 40 MHz) aktiviert ist. Hier werden die Kanäle 1 und 5 sowie 9 und 13 zu je 40 MHz zusammengefasst, um eine größere Übertragungsgeschwindigkeit zu erreichen. In der Praxis ist das in der Form meist unnötig. Geht man von einer normalen WLAN-Nutzung für den Internet-Zugang aus, dann ist die Übertragungskapazität mit einem 20-MHz-Kanal vollkommen ausreichend. Dummerweise sind die meisten WLAN-Router nicht in der Lage die Kanalbreite automatisch herunterzuschalten. Die Bestimmungen für 40 MHz breite Kanäle im 2,4-GHz-Band sind viel zu freigiebig.

Was bei der manuellen Kanalwahl zu beachten ist

1. Sofern möglich sollte in der WLAN-Basisstation immer die automatische Kanalwahl aktiviert sein.
2. Wenn das nicht möglich ist, orientiert man sich an der Kanalverteilung 1-6-11, 1-7-13 oder 1-5-9-13. Hierbei muss man jedoch berücksichtigen, welche WLANs in der Umgebung welchen Kanal benutzen und was die eigenen WLAN-Clients unterstützen. In der Regel wird man eine Kanalverteilung von 1-6-11 vorfinden. Manchmal auch 1-7-13. Oft auch ein Gemisch.
3. Man sollte es unbedingt vermeiden mehrere Kanalverteilungen miteinander zu vermischen.

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

27. RADIUS

IEEE 802.1x / RADIUS

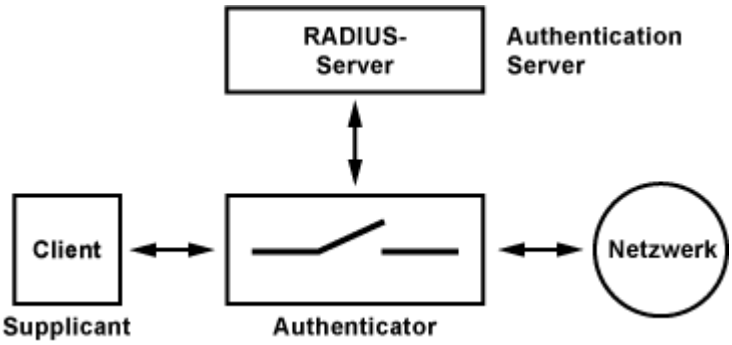
IEEE 802.1x ist ein sicheres Authentifizierungsverfahren für Zugangskontrollen in lokalen Netzwerken (LAN). Im Zusammenhang mit IEEE 802.1x werden auch häufig EAP und RADIUS genannt.
Das Protokoll EAP (Extensible Authentication Protocol), das ursprünglich als Erweiterung für PPP-Verbindungen entwickelt wurde, ist der Kern von IEEE 802.1x. IEEE 802.1x beschreibt die Einbettung von EAP-Datagrammen in Ethernet-Frames. Das ermöglicht den Austausch von Authentifizierungsnachrichten auf der Schicht 2 des OSI-Schichtenmodells.
EAP beschreibt ein einfaches Frage-Antwort-Verfahren, bei dem die Authentifizierungsdaten vom Benutzer zum Authentifizierunggs-Server und dessen Antworten ausgetauscht werden.
RADIUS kann bei der Anbindung einer zentralen Benutzerverwaltung eine wichtige Rolle spielen. Aber, IEEE 802.1x schreibt keinen RADIUS-Server vor. Doch in der Regel wird beim Einsatz einer Zugangskontrolle mit IEEE 802.1x auch ein RADIUS-Server eingesetzt.

Im Zusammenhang mit WLAN wird die Authentifizierungsmethode IEEE 802.1x auch als WPA2-Enterprise, WPA2-1x oder WPA2/802.1x bezeichnet.

Funktionen von IEEE 802.1x

- Zugangskontrolle
- Authentifizierung, Autorisierung und Accounting (AAA)
- Bandbreitenzuweisung (QoS)
- Single Sign-on (SSO)

Wie funktioniert IEEE 802.1x?



Bestandteil eines Authentifizierungsverfahrens wie IEEE 802.1x ist der Supplicant (Antragsteller), der Authenticator (Beglaubigter) und ein Authentication Server, der den Antrag des Supplicant überprüft und seine Entscheidung dem Authenticator mitteilt. Der Authenticator schaltet den Zugang zum Netzwerk für den Supplicant frei oder verweigert ihn.

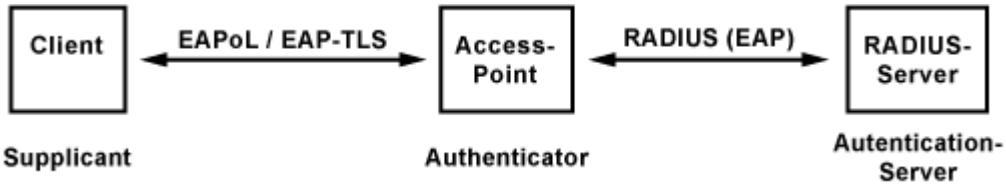
- Authenticator (Beglaubigter/Unterhändler): WLAN-Access-Point oder Switch mit IEEE 802.1x
- Authentication Server: RADIUS-Server, LDAP-Gateway/-Server, WLAN-Access-Point
- Supplicant (Antragsteller): WLAN-Client, LAN-Station

Anmeldungen vom Supplicant (Client) werden vom Authenticator zuerst an den Authentication Server weitergeleitet. Der entscheidet, ob der Supplicant Zugang bekommt. In Abhängigkeit einer erfolgreichen Authentifizierung wird der Zugang zum Netzwerk über einen bestimmten Port freigeschaltet. Wegen dem Bezug auf einen Port wird IEEE 802.1x auch als "Port-Based Network Access Control" bezeichnet.
Für IEEE 802.1x kann ein Port eine Buchse an einem Switch oder eine logische Assoziation sein. Denkbar ist hier die Zugangsmöglichkeit zum Netzwerk für einen WLAN-Client an einem WLAN-Access-Point. Mit IEEE 802.1x/EAP wird dem WLAN-Client zu Beginn einer Sitzung die dafür gültigen WPA2-Schlüssel mitgeteilt.

Wichtig bei WLAN, der WLAN-Access-Point muss auf WPA2-Enterprise eingestellt sein. Dabei hinterlegt man die IP-Adresse des RADIUS-Servers und ein Passwort, mit dem der RADIUS-Server und der WLAN-Access-Point ihre Kommunikation verschlüsseln und sichern.

Prinzipiell kann ein RADIUS-Server auch zur Verwaltung von Zugangsdaten dienen. Es gibt Architekturen bei denen der RADIUS-Server die Benutzer-Zugangsdaten nicht verwaltet, sondern zum Beispiel ein LDAP-Server (Verzeichnisdienst). In diesem Fall leitet der RADIUS-Server die Authentifizierung an den LDAP-Server weiter.

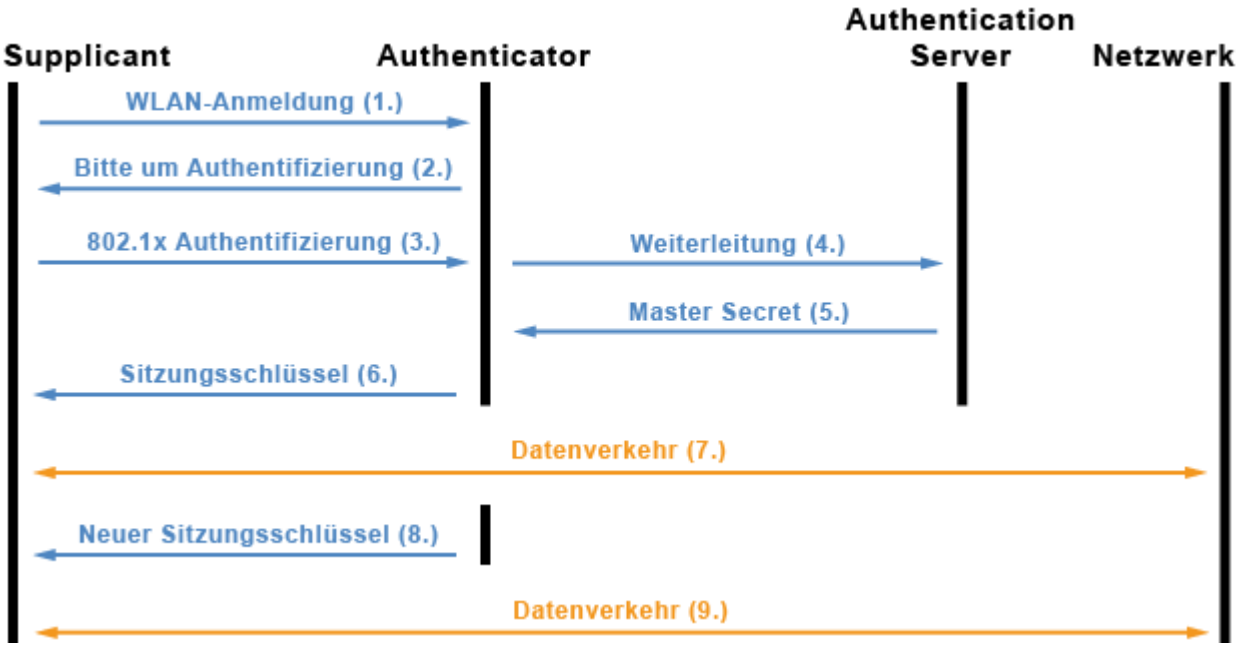
EAP - Extensible Authentication Protocol



Die Kommunikation zwischen Supplicant und Authenticator erfolgt über das Extensible Authentication Protocol over LAN (EAPoL). Die Kommunikation zwischen Authenticator und Authentication Server erfolgt über in RADIUS-Paketen gekapselte EAP-Pakete.

Beispiel für die Anwendung von IEEE 802.1x, EAP und RADIUS

Beim Zugriff auf ein lokales Netzwerk eines Unternehmens über WLAN reicht die einfache Authentifizierung über ein gemeinsames Passwort (WPA2-PSK) nicht aus. Wenn das Passwort die Runde macht, dann ist das WLAN praktisch offen.
Mit RADIUS werden serverseitig Passwörter zugeteilt, was dem Administrator Arbeit erspart und für die Nutzer vergleichsweise einfach ist. In dieser Konstellation kommt WPA2-Enterprise zum Einsatz, bei dem die WLAN-Basisstation die Zugriffe der WLAN-Clients über das Protokoll IEEE 802.1x mit einem RADIUS-Server aushandeln.
Ein RADIUS-Server ist nicht immer zwingend erforderlich. Manche WLAN-Router enthalten bereits einen RADIUS-Server, der für kleine Netzwerke eine Alternative ist.



1. Zuerst meldet sich der WLAN-Client (Supplicant) am WLAN-Access-Point (Authenticator) an. Beide Geräte sind entsprechend auf WPA2-Enterprise konfiguriert.
2. Der Access-Point (Authenticator) fordert den Client (Supplicant) zur Authentifizierung auf. In der Regel folgt hier die Eingabe von Benutzername und Passwort durch den Nutzer.
3. Der Client (Supplicant) authentisiert sich nach IEEE 802.1x.
4. Der Access-Point (Authenticator) leitet die Authentifizierung an den RADIUS-Server (Authentication Server) weiter.
5. Bei erfolgreicher Authentifizierung gibt der RADIUS-Server das Master Secret zurück.
6. Der Access-Point generiert den Sitzungsschlüssel und teilt diesen dem Client mit.

7. Durch den Sitzungsschlüssel bekommt der Client Zugriff auf das Netzwerk.
8. In regelmäßigen Abständen bekommt der Client einen neuen Sitzungsschlüssel mitgeteilt.
9. Damit ist weiterhin der Zugriff auf das Netzwerk durch den Client möglich.

RADIUS - Remote Authentication Dial In User Service

Innerhalb eines großen Netzwerks findet die Verwaltung und Speicherung von Benutzerdaten an einer zentralen Stelle statt. Diese Daten dienen auch zur Authentifizierung von Benutzern, die sich am Netzwerk anmelden.
Kommt es zu einem Zugriff von außen auf das Netzwerk wird eine RAS- oder VPN-Verbindung hergestellt. Über diese Verbindung muss der Benutzer authentifiziert werden, bevor er Zugriff auf das Netzwerk bekommt.
Das Bindeglied zwischen der zentralen Benutzerverwaltung und dem RAS ist der RADIUS. Obwohl IEEE 802.1x keinen RADIUS-Server vorschreibt, sind die meisten Authenticatoren in der Praxis RADIUS-Clients. Das RADIUS-Protokoll übernimmt die Authentifizierung und Verschlüsselung, sowie das Accounting. Vom RADIUS-Server wird der Anfang und das Ende der Benutzung einer Leistung protokolliert und kann zu Abrechnungszwecken herangezogen werden.

Radius kennt drei Pakettypen, deren Namen so lauten, wie ihre Funktion:

- Access-Request (Bitte um Freigabe des Zugriffs)
- Access-Accept (Annahme für die Freigabe des Zugriffs)
- Access-Reject (Ablehnung der Freigabe)

Die RADIUS-Nachrichten werden auf IP-Ebene mit UDP-Paketen versendet. Die Informationen stecken in Attribute-Value Pairs (AVP).

Konfiguration: Switch und Access Point

Beim Switch und Access Point beschränkt sich die Konfiguration auf den Eintrag der IP-Adresse des RADIUS-Servers, sowie ein gemeinsames Passwort (Key) mit dem Switch bzw. Access Point und Server die Kommunikation verschlüsseln. Anschließend müssen im Switch nur noch die betreffenden Ports gekennzeichnet werden, für die die Authentifizierung gilt.
Wenn ein Netzwerk auf diese Weise gesichert ist, muss man dafür sorgen, dass eventuell ungeschützte Ports unzugänglich gemacht sind. Zum Beispiel sollte der Netzwerkschrank oder Netzwerkraum abgeschlossen sein.

Hinweis: IEEE 802.1x geht von einem Host bzw. einem User pro Port aus. Es kann sich also immer nur ein User authentfizieren. Andere User bleiben ausgesperrt. Ausnahme, wenn Multi-802.1x konfigurierbar ist.

MAC-based Authentication

Wenn man eine IEEE-802.1x-Authentifizierung im Netzwerk betreibt hat man häufig das Problem, dass es Netzwerk-Geräte gibt, die keine IEEE-802.1x-Unterstützung mitbringen. Zum Beispiel Drucker, Webcams oder VoIP-Telefone. In so einem Fall benötigt man eine Alternative für IEEE 802.1x, um auch diese Hosts zu authentifizieren. Dazu nimmt der Switch die MAC-Adresse des Hosts als Benutzername und Passwort in hexadezimaler Schreibweise für die Authentifizierung mit

dem RADIUS-Server.
Aber, das hat einen schwerwiegenden Nachteil. Die MAC-Adresse kann ein Angreifer leicht übernehmen. Dazu muss der Angreifer nur die MAC-Adresse eines entsprechenden Druckers, Telefons oder eines anderen Geräts ausfindig machen. Häufig stehen die MAC-Adresse auf Typenschildern.
Ein solcher Angriff ist natürlich mit etwas Aufwand verbunden. MAC-based Authentication schützt also nur vor versehentlichen Verbindungsversuchen und unbedarften Personen.

Multi-802.1x

Normalerweise funktioniert eine Authentifizierung mit IEEE 802.1x nur einmal pro Port. Mit Multi-802.1x kann ein Switch an einem Port auch mehrere Hosts authentifizieren. Beispielsweise, wenn an einem Port ein weiterer Switch hängt, der kein IEEE 802.1x beherrscht.
Hinweis: Damit IEEE 802.1x über mehrere Switche hinweg funktioniert, muss jeder Switch EAPOL-Frames durchlassen. Dieses Leistungsmerkmal ist nicht selbstverständlich.

Troubleshooting

- Die meisten Probleme bei IEEE 802.1x entstehen durch Zertifikatsfehler. Ein typisches Beispiel sind selbstausgestellte Zertifikate für den RADIUS-Server, die nicht alle Clients, insbesondere Smartphones, annehmen. Hier muss man zuerst das passende Root-Zertifikat auf den Clients installieren.
- Bei einer Authentifizierung mit EAP-TLS muss sich nicht nur der RADIUS-Server mit einem Zertifikat ausweisen, sondern auch der Client. Hier muss zuerst das Nutzer-Zertifikat ausgestellt und auf dem Client installiert werden.

Wie sicher ist RADIUS?

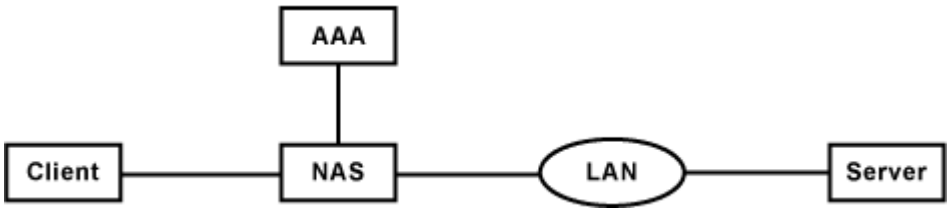
Die per RADIUS verwendeten Zugangsdaten (Benutzername und Passwort) sind normalerweise nicht sicherer als zum Beispiel ein WLAN-WPA2-Passwort. Eine höhere Sicherheit erreicht man nur durch den Einsatz zusätzlicher Zertifikate über EAP-TLS. Hierbei identifizieren sich RADIUS-Server und Client gegenseitig. Der dafür notwendige Einrichtungsaufwand sollte nicht unterschätzt werden. Selbst große Unternehmen betreiben diesen Aufwand nicht.

28. 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.

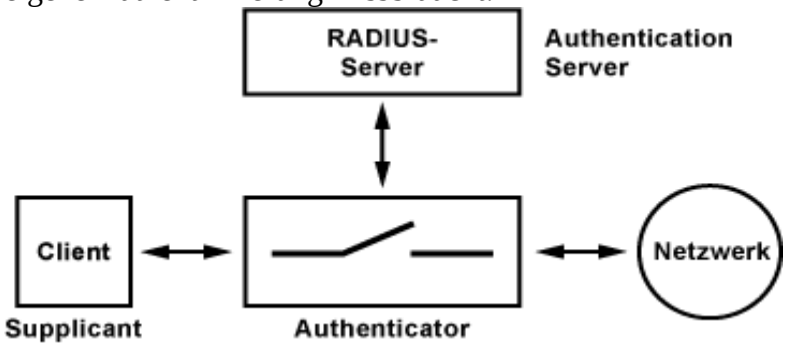
Vereinfachte Darstellung der Funktionsweise von AAA



Ein Nutzer (Client) möchte einen Dienst in Anspruch nehmen. Ein Network Access Server (NAS) bietet diesen Dienst oder den 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.

Authentifizierung / Authentication

Authentifizierung bedeutet, die Identität zu überprüfen. Zum Beispiel Benutzername und Passwort. Knackpunkt bei jeder Authentifizierung ist die Übertragung von Benutzername und Passwort. Erfolgt sie unverschlüsselt, dann ist es möglich, dass ein Angreifer beides ausspäht und für die eigene Authentifizierung missbraucht.



Die Bestandteile einer Authentifizierung 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 Authentifizierung akzeptiert. Erst 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 nutzen. Wenn hinter einer Authentifizierung mehrere Dienste angeboten werden, dann macht es Sinn 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 denkbar, die Nutzungsabläufe des Benutzers für Service-Fälle fest zu halten, 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 oder Identität beglaubigt bzw. dessen Echtheit bezeugt wird.
"Authentisieren" bzw. "Authentisierung" würde demnach bedeutet, dass der Nutzer oder Absender seine Identität glaubwürdig machen soll.
In der Praxis und im allgemeinen Sprachgebrauch wird zwischen beiden Formen jedoch nicht immer unterschieden. Im Allgemeinen spricht man auch dann von Authentifizierung, wenn die Authentisierung gemeint ist.

29. DoS

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.

30. DDoS

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.

31. Malware

Malware (zusammengesetzt aus dem engl. *malicious:* bösartig und *war*e von Software) bezeichnet ein schädliches Programm (Schadsoftware). Dies sind Computerprogramme, die entwickelt wurden, um vom Benutzer unerwünschte bzw. schädigende Funktionen auszuführen. Der Begriff bezeichnet keine schadhafte Software, obwohl auch diese Schaden anrichten kann.

Malware-Klassifizierungen

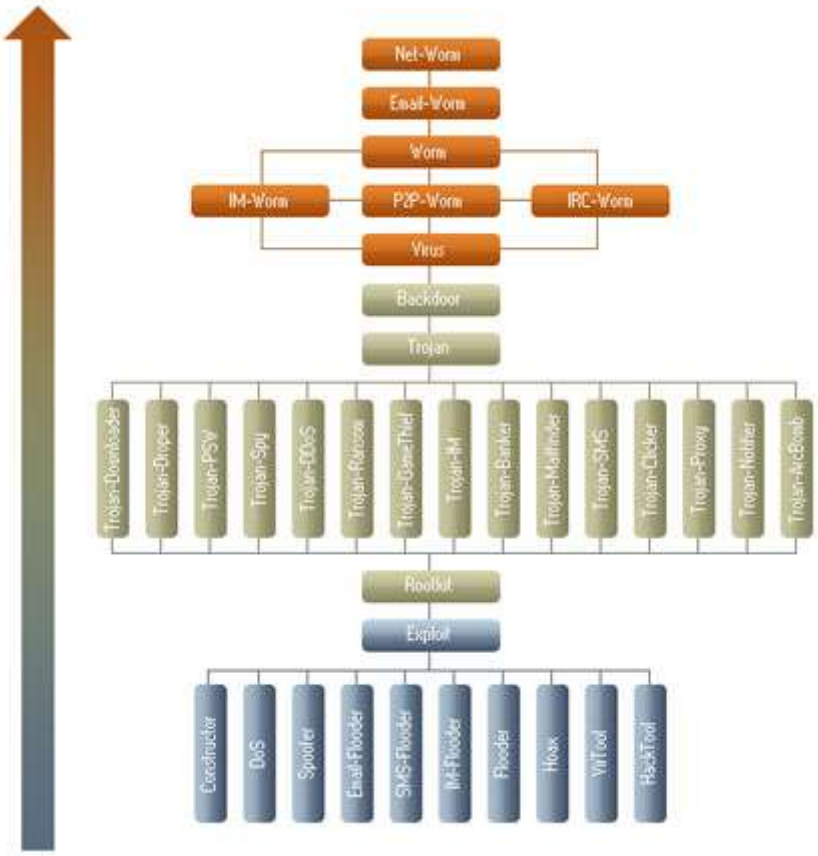
Bei so vielen unterschiedlichen Malware-Typen – und der großen Bandbreite von schädlichen Softwareprogrammen innerhalb der einzelnen Typen – ist es entscheidend, einzelne Malware-Objekte eindeutig klassifizieren und damit problemlos von anderen Schadprogrammen unterscheiden zu können.

Kaspersky Lab klassifiziert das gesamte Spektrum von schädlicher Software oder potenziell unerwünschten Elementen, die von unserer Antiviren-Engine erkannt werden, auf Grundlage der Aktivität, die auf den Computern von Benutzern ausgeführt wird. Das von Kaspersky Lab verwendete Klassifizierungsmodell wird auch von einer Reihe anderer Hersteller von Antiviren-Software als Grundlage für deren eigene Klassifizierungen herangezogen. .

Der Malware-„Klassifizierungsbaum“

Im Klassifizierungsmodell von Kaspersky Lab wird jedem erkannten Objekt eine eindeutige Beschreibung und ein Platz in dem unten abgebildeten „Klassifizierungsbaum“ zugeordnet. Innerhalb des „Klassifizierungsbaums“:

- Ist das Malware-Verhalten mit dem geringsten Bedrohungspotenzial im unteren Diagrammbereich angesiedelt.
- Ist das Malware-Verhalten mit dem größeren Bedrohungspotenzial im oberen Diagrammbereich angesiedelt.



*Malware-Typen mit mehreren Funktionen**

Malware-Programme besitzen nicht selten mehrere unterschiedliche Schadfunktionen und Verbreitungsarten, was ohne zusätzliche Klassifizierungsregeln zu begrifflicher Verwirrung führen könnte.

Beispielsweise könnte die Verbreitung eines Schadprogramms per E-Mail-Anhang, aber auch per Dateiaustausch in P2P-Netzwerken stattfinden. Außerdem könnte das Programm die Fähigkeit besitzen, die auf einem infizierten Computer vorhandenen E-Mail-Adressen ohne Wissen des Benutzers „abzuschöpfen“. Angesichts dieser funktionellen Vielfalt wäre eine Einstufung der Malware sowohl als E-Mail-Wurm, P2P-Wurm oder als Trojan-Mailfinder denkbar. Um diese begriffliche Verwirrung zu vermeiden, wurden bei Kaspersky Lab zusätzliche Regeln eingeführt, die eine eindeutige Kategorisierung von Schadprogrammen anhand ihres Verhaltens und unabhängig von den verfügbaren Funktionen erlauben:

- Wie aus dem Klassifizierungsbaum deutlich wird, wurde jedem Verhalten eine Bedrohungsstufe zugeordnet.
- Außerdem ist ersichtlich, dass Malware-Verhalten mit höherem Bedrohungspotenzial höherrangig sind als Verhalten, die ein geringeres Risiko darstellen.rs that pose a higher risk outrank those behaviours that represent a lower risk.
- In unserem Beispiel stellt also das Verhalten „E-Mail-Wurm“ eine höhere Bedrohung dar als „P2P-Wurm“ bzw. „Trojan-Mailfinder“, d. h. das zugehörige Schadprogramm würde als E-Mail-Wurm eingestuft.**

Mehrere Funktionen mit gleicher Bedrohungsstufe

- Wenn ein Schadprogramm mehrere Funktionen besitzt, die alle dieselbe Bedrohungsstufe aufweisen, z. B. Trojan-Ransom, Trojan-ArcBomb, Trojan-Clicker, Trojan-DDoS, Trojan-Downloader, Trojan-Dropper, Trojan-IM, Trojan-Notifier, Trojan-Proxy, Trojan-SMS, Trojan-Spy, Trojan-Mailfinder, Trojan-GameThief, Trojan-PSW oder Trojan-Banker, dann wird das Programm als Trojaner eingestuft.
- Wenn ein Schadprogramm mehrere Funktionen besitzt, die alle dieselbe Bedrohungsstufe aufweisen, z. B. IM-Worm, P2P-Worm oder IRC-Worm, wird das Programm als Wurm klassifiziert.

32. Statisches und dynamisches Routing

Statisches Routing ist ein fest vorgegebener Verbindungsweg zwischen Quelle und Ziel.
Man legt also fest wie Pakete den Weg durchs Netzwerk wählen sollen.

Beim Dynamischen Routing ist es anders, hier wird nur das Ziel festgelegt, auf welchem Weg das Paket dort ankommt, kann unterschiedlich sein, je nach dem welches dynamische System verwendet wird.

Beispiel:

Nehmen wir einmal an wir haben ein 5 Knoten Netzwerk, das wie folgt aufgebaut ist: (denk dir die Punkte weg)

```
1---------2
|...\...../...|
|....\..../....|
|......5......|
|..../.....\...|
|.../.......\..|
3---------4
```

1 möchte 4 Pakete schicken.
Mögliches Statisches Routing: 1 schickt über 5 an 4.
(natürlich gibts hier noch mehr Möglichkeiten ;-))
Aber angenommen das 5 und 3 momentan schon beschäftigt sind, dann müssten die Pakete von 1 warten bis 5 seine Übertragung beendet hat.
Ein mögliches Dynamisches Routing wäre hier, 1 "merkt" das 5 beschäftigt ist und schaut sich 2 an. Er schickt das Paket mit dem Ziel 4 also an 2 und 2 kann es nun weiter an 4 schicken.

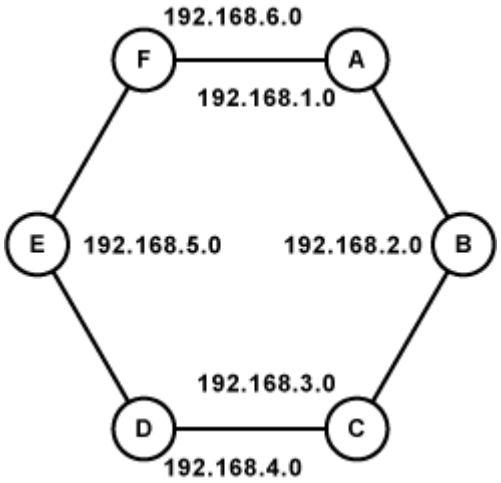
Vor und Nachteile haben beide Systeme, welches das bessere ist, hängt davon ab für was man das Netzwerk betreibt, oder ob bestimmte Knoten höhere Prioritäten haben.
Man kann dynamisches und statisches Routing auch mischen. In dieser Form ist das Internet aufgebaut.

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

33. RIP

Routing Information Protocol



Netzwerk		Hop-Anzahl
Von	**Nach**	
192.168.1.0	192.168.2.0	0 (Direktverbindung)
	192.168.3.0	1
	192.168.4.0	2
	192.168.5.0	1
	192.168.6.0	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.

34. OSPF

OSPF (open shortest path first)

OSPF-Protokoll

Open Shortest Path First (OSPF) ist ein Interior Routing Protocol (IRP) und beschreibt wie Router untereinander die Verfügbarkeit von Verbindungswegen zwischen Datennetzen propagieren. Es unterstützt hierarchische Netzstrukturen, zeichnet sich durch ein schnelles dynamisches Verhalten in Bezug auf die Änderungen in der Netztopologie aus, optimiert das Routing hinsichtlich der Übertragungskosten, hat eine dynamische Lastverteilung, einen geringen Overhead und kann die Dienstleistungsmerkmale (TOS) im Routing berücksichtigen.

Eine Kostenzuordnung für die einzelnen Nutzer kann anhand diverser Leitungsparameter wie Tarifierung, genutzte Bandbreite, Lastaufkommen u.a. vorgenommen werden. Diese Parameter können auch für die Metrik genutzt werden, wodurch die Routenerstellung flexibel und differenziert erfolgen kann.

OSPF arbeitet nach dem Link-State-Algorithmus (LSA) kann große Entfernungen mit mehr als 14 Zwischensystemen überbrücken und Subnetze in Gruppen zusammenfassen. Insgesamt kann OSPF Datenpakete über 65.000 Router leiten.

Datenrahmen des OSPF-Protokolls

Der dem OSPF-Protokoll zugrunde liegende Routing-Algorithmus ist der SPF-Algorithmus (Shortest Path First). Das Routing des OSPF-Protokolls nutzt zur Optimierung eine Datenbank, in der die angrenzende Topologie abgelegt ist. Aufbauend auf dieser Topologie generiert sich jeder Router eine hierarchische Baumtopologie, den Shortest-Path-Baum, in dem jedes Ziel mit der

kürzesten Route eingetragen ist. Die Baumstruktur ist in die Ebenen Netze, eine Gruppe von Netzen, die sogenannte Area, Backbones, die die Areas miteinander verbinden, und autonome Systeme, die eine Zusammenfassung aller über das Backbone verbundenen Netze darstellen, untergliedert.

Die Kommunikation zwischen den Routern erfolgt über einen Authentisierungs-Mechanismus, an dem nur autorisierte Router teilnehmen können. Routing-Informationen anderer Routing-Protokolle werden transparent weitergeleitet.

Das OSPF-Protokoll baut direkt auf dem IP-Protokoll auf und ist eine Weiterentwicklung einer frühen Version des Intermediate System to Intermediate System Protocol (IS-IS).

Aufbau des OSPF-Headers.

Der Header des OSPF-Protokolls kennt neben den Datenfeldern für die Version, den Typ und die Paketlänge, der Prüfsumme und der Quelladresse auch ein 4 Oktett langes Datenfeld für die ID der Area sowie mehrere Datenfelder für die Authentisierung, wobei der Authentisierungstyp festlegt, ob überhaupt eine Authentisierung stattfinden soll.

Neben dem klassischen OSPF gibt es zwei weitere Versionen: OSPFv2 für IPv4 und OSPFv3 für IPv6. OSPFv3 basiert auf der Vorgängerversion OSPFv2 und behält die meisten darin vorhandenen Routing-Mechanismen bei. Die erweiterten Funktionen betreffen die Adressierungssemantik, die von den OSPF-Datenpaketen und den Link-State-Algorithmen (LSA) entfernt und durch neue Link-State-Algorithmen für den Transport der IPv6-Adressen ersetzt wurden. Das klassische IP-basierte OSPF läuft unter OSPFv3 auf Link-Basis und nicht mehr auf IP-Basis. Die Authentifizierung wird nicht mehr vom OSPFv3-Protokoll vorgenommen, sondern durch den Authentication Header (AH) von IPv6.

Open Shortest Path First (OSPF) ist eine Spezifikation der Internet Engineering Task Force (IETF) und wird in diversen RFCs beschrieben. So in RFC 2328. Die Version 3, OSFPv3, ist in den RFC 2740 beschrieben.

35. Routingtabellen

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 möglicherweise folgende Angaben:

- alle bekannten Netzwerkadressen
- Verbindungsarten in andere Netzwerke
- Weginformationen zu anderen Routern
- Verbindungskosten

36. Backup

Komplett-/Vollsicherung

Die Komplett- oder Vollsicherung wird in Programmen auch als *„Normale Sicherung“* bezeichnet. Hierbei werden die jeweils zu sichernden Daten (ein komplettes Laufwerk, eine Partition, bestimmte Verzeichnisse und/oder bestimmte Dateien, bestimmte Dateiformate) komplett auf das Sicherungsmedium übertragen und als gesichert markiert.

Als Vorteil gilt, dass die Vollsicherung technisch sehr einfach ist - reines Kopieren der Daten reicht, und eigene Backup-Programme zu schreiben gestaltet sich leicht. Nachteilig ist der sehr hohe Speicherbedarf.

Speicherabbildsicherung

Bei der Speicherabbild-Sicherung (englisch *image backup*) kann der komplette Datenträger (meist die Festplatte, aber auch USB-Massenspeicher, optische Medien oder bei einigen Programmen auch Datenträger im Netzwerk) oder nur eine Partition durch ein 1-zu-1-Abbild gesichert werden. So können beispielsweise nicht nur die Nutzdaten, sondern das gesamte Dateisystem, inklusive Betriebssystem und Benutzereinstellungen, gespeichert werden. Der Vorteil dieser Sicherung besteht darin, dass bei einem Totalausfall des Rechners das Speicherabbild auf den Datenträger zurückgesichert und dadurch der Zustand der jeweiligen Datenträger zum Sicherungszeitpunkt vollständig wiederhergestellt werden kann. Bei einer derartigen Wiederherstellung wird entweder das gesamte Dateisystem in seiner Originalstruktur wiederhergestellt (in diesem Fall ist kein Dateisystemtreiber erforderlich, sondern lediglich ein Gerätetreiber für den Datenträgerzugriff), oder ein besonderer Treiber liest regulär das Dateisystem und extrahiert nur die gewünschten Verzeichnisse und Dateien aus der Sicherung, um diese als normale Verzeichnisse und Dateien in das aktuelle Dateisystem zu integrieren bzw. die aktuellen mit den älteren gesicherten zu überschreiben (siehe auch „Inkrementelle Sicherung“). Seit einigen Jahren sind auch Programme auf dem Markt, die solche Sicherungen ebenfalls inkrementell anlegen können.

Differenzielle Sicherung

Bei der sogenannten *differenziellen Sicherung* werden alle Daten, die seit der letzten Komplettsicherung geändert wurden oder neu hinzugekommen sind, gespeichert. Es wird also immer wieder auf der letzten Komplettsicherung aufgesetzt, wobei gegenüber einer neuen Vollsicherung Speicherplatz und Zeit gespart werden kann.

Vorteilig ist der deutlich reduzierte Speicherbedarf, und dass die derzeit aktuelle Datensicherung nur einen Schritt von der letzten Vollsicherung entfernt ist. Die Programmierung der Backup-Software kann relativ simpel sein. Ebenfalls von Vorteil ist, dass die verschiedenen Sicherungsstände unabhängig voneinander gelöscht werden können, während inkrementelle Sicherungen zwangsläufig miteinander verkettet sind.

Inkrementelle Sicherung

Bei der inkrementellen Sicherung werden immer nur die Dateien oder Teile von Dateien gespeichert, die seit der letzten inkrementellen Sicherung oder (bei der ersten inkrementellen Sicherung) seit der letzten Komplettsicherung geändert wurden oder neu hinzugekommen sind. Es wird also immer auf der letzten inkrementellen Sicherung aufgesetzt. Dieses Verfahren hat den Nachteil, dass bei einer Wiederherstellung die Daten in der Regel aus mehreren Sicherungen wieder zusammengesucht werden müssen. Mittels verschiedenen Techniken (Datumsstempel, Prüfsummen) muss gewährleistet sein, dass die vollständige Kette (Vollsicherung - inkrementelle Sicherungen 1, 2, 3, etc. - Originaldaten) fehlerfrei nachvollziehbar ist.

Zu beachten ist, dass die Inkremente auf zwei Weisen gespeichert werden können:

- Üblich sind die *forward deltas*. Dies entspricht dem oben beschriebenen Fall: Die (ältere) Vollsicherung dient als Fundament und wird nicht verändert, während darauf die Inkremente aufgebaut werden. Der *aktuelle* Datenbestand kann nur unter Berücksichtigung von Inkrementen wieder hergestellt werden. Beispiele: duplicity.
- Eine inkrementelle Sicherung mit *reverse deltas* kehrt dieses Prinzip auf den Kopf. Man stelle sich die Kante eines Daches vor, von denen Eiszapfen herunterwachsen. Die Vollsicherung verändert sich bei jedem Backup-Vorgang und stellt hier die Dachkante dar. Die anwachsenden Eiszapfen sind die Inkremente. Hat sich eine Datei gegenüber der letzten Vollsicherung verändert, wird die vorherige Dateiversion als Inkrement gespeichert - der Eiszapfen wächst nach unten - während die derzeit aktuelle Version in die Vollsicherung eingefügt wird. Auf die Vollsicherung kann jederzeit problemlos zugegriffen werden, während eine ältere Version einer Datei nur durch Berücksichtigung der Inkremente wieder hergestellt werden kann. Beispiele: rdiff-backup.

Vorteilig ist der sehr geringe Speicherbedarf, und eignet sich so für das Backup in Netzwerken oder das Backup in der Cloud. Jedoch ist das inkrementelle Backup rechnerisch ziemlich aufwändig. Prinzipiell bedingt sind alle Inkremente miteinander verkettet - es ist nur mit sehr grossem Rechenaufwand möglich, ein Inkrement zwischen zwei anderen Inkrementen zu entfernen, etwa um Speicherplatz zu sparen oder private Daten zu löschen.

37. 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

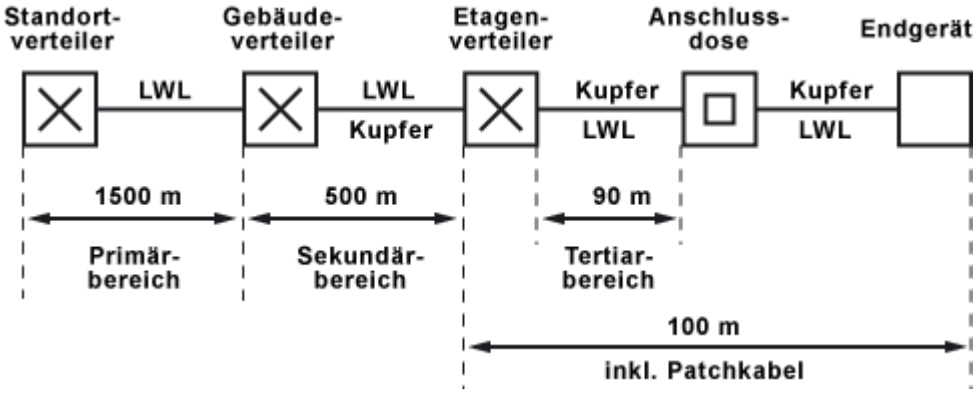
Normen für die strukturierte Verkabelung

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

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

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

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

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. Dasselbe 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

38. iSCSI-Frame

iSCSI ist ein Protokoll um in Rechenzentren Datenspeicher zu Storage Area Networks (SAN) zu verbinden und dabei die Daten über die bestehende Infrastruktur aus Ethernet und TCP/IP zu übertragen. In iSCSI werden die SCSI-Befehle zusammen mit den Daten in Protocol Data Units (PDUs) gebündelt und in serieller Form als iSCSI in TCP/IP eingebettet und dann über Ethernet übertragen. iSCSI ist somit eine Alternative zu Fibre Channel over Ethernet.

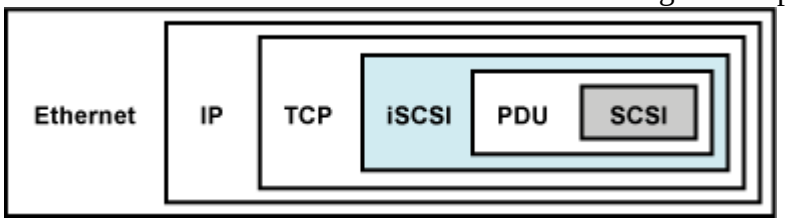
iSCSI ist ein Standard der Storage Networking Industry Association (SNIA). Die SNIA ist ein Zusammenschluss von mehr als 300 im Storage-Bereich aktiven Firmen.

Architektur

Der Server, der den Netzwerkspeicher anbietet, wird als Target bezeichnet. Der Computer, der die virtuelle Festplatte ins System einbindet, nennt sich Initiator.
iSCSI kennt ausschließlich Punkt-zu-Punkt-Verbindungen. Mechanismen, wie bei SMB oder NAS, um mehreren Anwendern Zugriff zu ermöglichen, kennt iSCSI nicht. iSCSI überträgt die Datenblöcke unabhängig vom Dateisystem und unterscheidet sich somit von Netzwerkfreigaben, wie zum Beispiel SMB. Auf diese Weise bleibt der Overhead gering. Das ermöglicht einen hohen Datendurchsatz.

Wie funktioniert iSCSI?

iSCSI ist ein Protokoll zum Verbinden von PCs mit großem Speicherplatzbedarf mit Netzwerk-Festplatten, so das sie sich wie lokale Laufwerke verwenden lassen. iSCSI verlängert praktisch das Kabel zur Festplatte über das lokale Netzwerk. Über iSCSI wird eine Festplatte direkt ins System eingebunden. Denkbar wäre es, einen Computer ohne eingebaute Festplatte zu betreiben.
Wenn man Festplatte per iSCSI anbindet, erscheint der Datenträger in der Systemsteuerung des PCs als zusätzliches Laufwerk. Auf dem ersten Blick scheint sich das Laufwerk von einem lokalen Laufwerk nicht zu unterscheiden. Es lässt sich wie gewohnt partitionieren und formatieren.



iSCSI hat die gleiche Funktion, wie FCP (Fibre Channel Protocol). Bei iSCSI geht es darum, das SCSI-Protokoll auf seriell betriebenen Netzen abzubilden. Der Datenverkehr wird über TCP/IP abgewickelt. Der iSCSI-Protokoll-Stack ist dann meistens eine Protokoll-Kombination aus SCSI, PDU, iSCSI, TCP/IP und Ethernet. Das hat den Vorteil, dass überall dort auf die Daten zugegriffen werden kann, wo ein Netzwerkanschluss vorhanden ist.

Anwendungen

iSCSI dient in Rechenzentren als Protokoll zum Verknüpfen von SANs.

39. SAMBA-Server

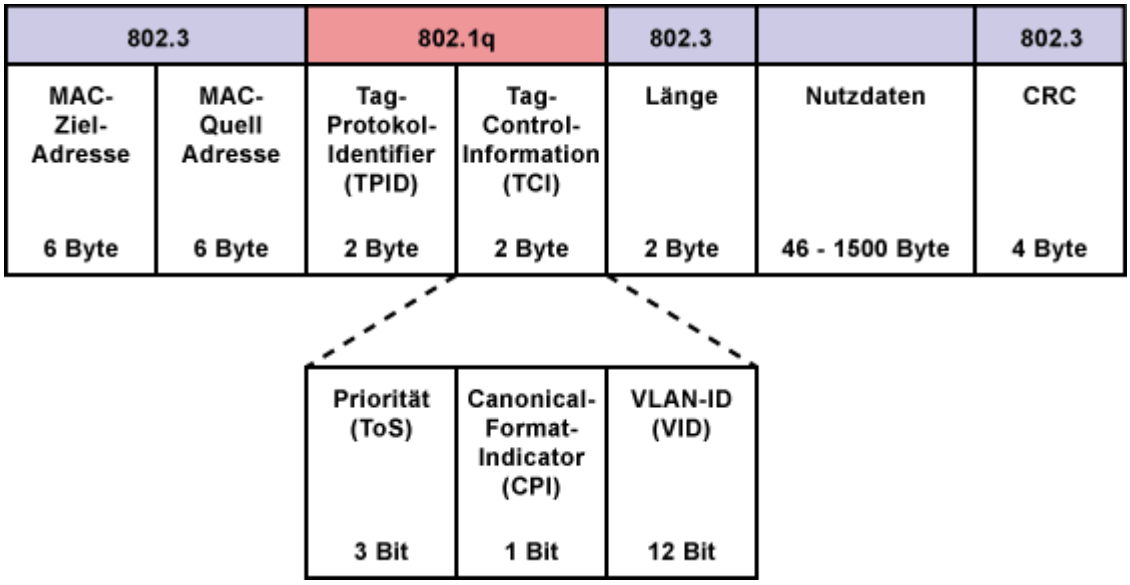
Ein **Samba-Server** unterstützt bei der Integration von **Windows- und Unix/Linux-Rechnern**. Es können gegenseitig zum Beispiel **Dateien** getauscht oder auch **Drucker** freigegeben werden. Der Name Samba hat seinen Ursprung beim SMB-Protokoll (***Server Message Block***), das unter Windows für den netzbasierten Datenaustausch eingesetzt wird. Aktuell wird an Stelle von SMB auch immer wieder vom "***Common Internet File System***" (CIFS) gesprochen. CIFS ist eine Weiterentwicklung von SMB und wurde ursprünglich von Microsoft entwickelt.

40. VLAN

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 Switche realisiert, die in gewisser Weise 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

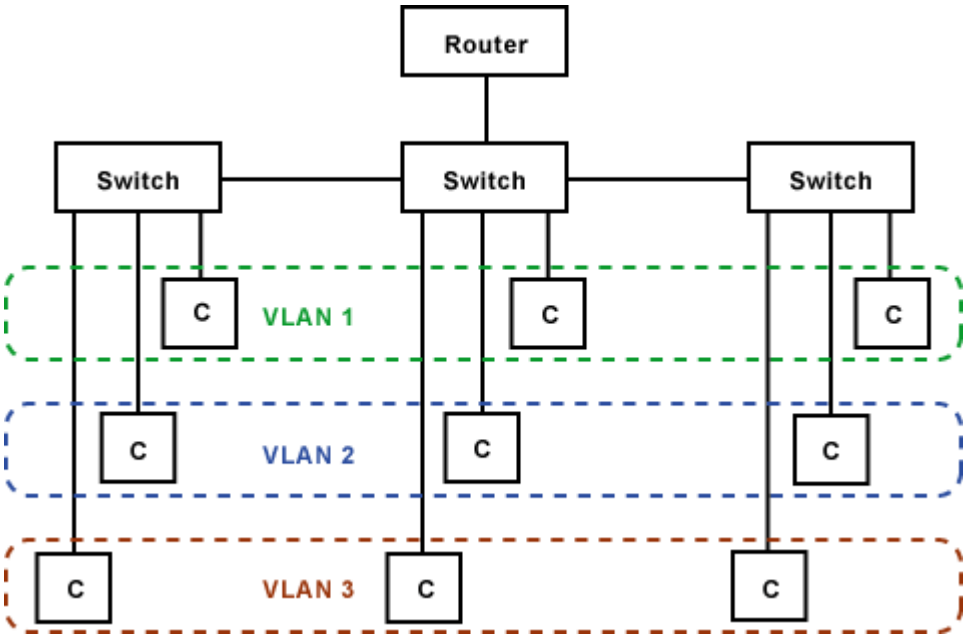


Um Daten verzögerungsfrei zu übertragen weist man den Datenpaketen Markierungen zu. Verfahren zur Markierung von Echtzeitdaten gibt es auf verschiedenen Ebenen des OSI-Schichtenmodells.
Auf der Schicht 2 kann der Standard IEEE 802.1q Ethernet-Frames mit so genannten Tags klassifizieren. Insgesamt wird das Ethernet-Frame um 4 Byte verlängert und zusätzliche Informationen in den Header gepackt, die den Datenaustausch innerhalb des VLANs regeln (Tagging). Im ToS-Feld des Ethernet-Headers können drei Bit für die Priorisierung verwendet werden (IP-Precedence). Mit drei Bit können 8 Prioritätsstufen abgebildet und Dienstklassen bzw. einem Class of Service (CoS) zugeordnet werden. Die Veränderung wird von den Treibern des Netzwerk-Adapters vorgenommen und von netzübergreifenden VLAN-Switches ausgewertet.

Damit dieses Verfahren funktioniert, müssen die Netzwerkkomponenten auf der gesamten Übertragungsstrecke in der Lage sein, die Datenpakete zu klassifizieren und zu priorisieren.

Mit diesem Verfahren ist trotzdem keine Garantie der Bandbreite und Verzögerungszeit möglich. Eine Garantie ist nur mit verbindungsorientierten Maßnahmen möglich.

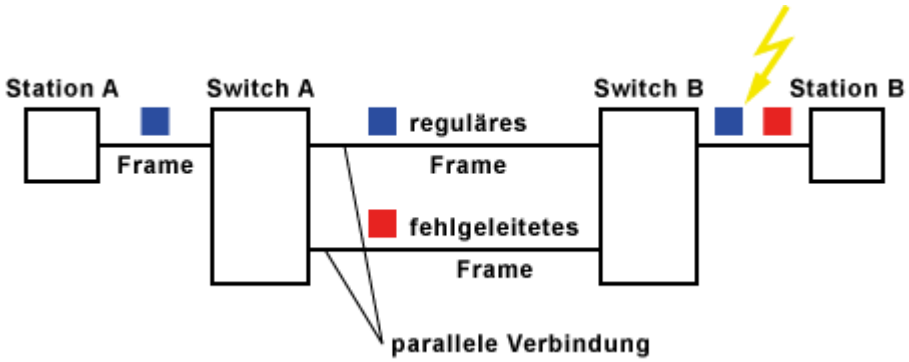
Beispiel-Architektur eines lokalen Netzwerkes mit VLANs



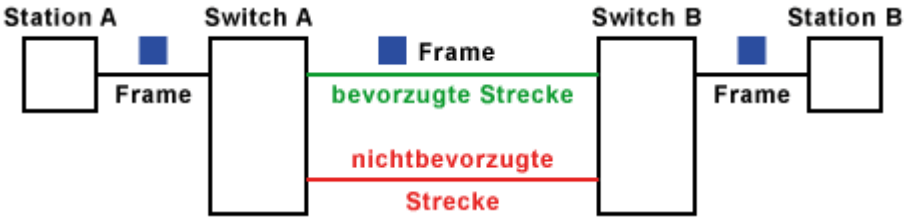
Obwohl die Clients der VLANs 1, 2 und 3 an unterschiedlichen Switche angeschlossen sind, sind sie für unterschiedliche Subnetze adressiert. Die Layer-3-Switche achten anhand der Subnetze auf die gezielte Weiterleitung von Broadcasts. Muss ein Datenpaket das Subnetz wechseln, wird es automatisch in ein anderes VLAN geroutet.

41. Spanning-Tree

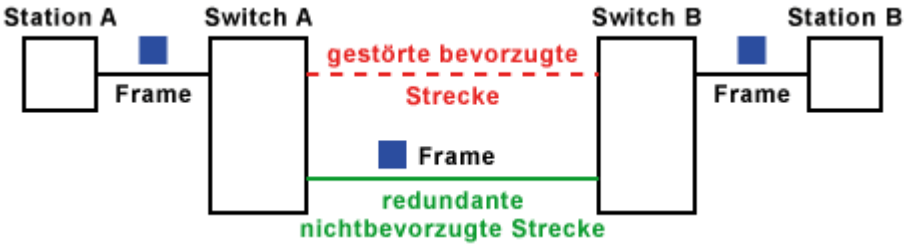
STP - Spanning Tree Protocol / IEEE 802.1d / 802.1w



Das Spanning-Tree-Verfahren ist im Standard IEEE 802.1d für die MAC-Schicht spezifiziert. Es soll das Auftreten von doppelten Frames in einem geswitchten Ethernet-Netzwerk verhindern. Die doppelten Frames entstehen durch zwei oder mehr parallele Verbindungen zwischen zwei Switches. Frames, die mehrfach beim Empfänger ankommen, können zu einem Fehlverhalten führen.



Spanning Tree spannt das physikalische Netzwerk zu einem logischen Baum auf, in dem zu jedem Ziel nur ein einziger Weg existiert. Die Switches bzw. Bridges kommunizieren in einem Netzwerk mit Hilfe von BPDUs (Bridge Protocol Data Unit). Diese Konfigurationspakete werden als Multicast-Frames an die MAC-Adresse 01-80-C2-00-00-10 geschickt. Diese Frames werden alle 2 Sekunden an die nächste, tiefer gelegene Station (Bridge oder Switch) übermittelt. Auf diese Weise werden parallele Strecken erkannt und die optimale Strecke ermittelt. Man spricht dann von Prioritäten bzw. Wegkosten, die die Datenrate und Entfernung berücksichtigt. Ports mit nichtbevorzugten Strecken werden dann deaktiviert.



Fällt die bevorzugte Strecke aus, bleibt auch das BPDU-Frame aus, was zu einer Reorganisation des Netzwerks führt. Bei komplizierten Verschachtelungen wird der Baum (Spanning Tree) neu berechnet, was zu einer Verzögerung von bis zu 30 Sekunden oder mehr führen kann. Erst danach kann auf der redundanten Strecke die Übertragung fortgesetzt werden.

IEEE 802.1w / RSTP - Rapid Spanning Tree Protocol

Die relativ lange dauernde Neuberechnung des logischen Netzwerks ist für einen potentielle Angreifer, der ein Netzwerk lahm legen will, ein gefundenes Fressen. Nur ein einziges gefälschtes Spanning-Tree-Frame ist in der Lage eine Reorganisation auszulösen und das gesamte Netzwerk für 30 Sekunden oder mehr lahm zulegen.
Um dieses Szenario zu vermeiden, wurde unter IEEE 802.1w das abwärtskompatible RSTP, auch Fast Spanning Tree genannt, entwickelt. Es sieht vor, dass bei einem Ausfall einer Verbindung mit der bestehenden Netzwerkstruktur weitergearbeitet wird, bis eine alternative Strecke berechnet ist. Anschließend wird ein neuer logischer Baum erstellt und erst dann, innerhalb einer Sekunde, umgestellt.

Loop Detection

Manche einfache Switches ohne Spanning Tree haben eine Loop-Detection-Funktion. Dazu sendet der Switch alle paar Minuten ein Frame an eine bestimmte Adresse. Empfängt der Switch ein solches Frame mit seiner eigenen Adresse, existiert eine Schleife, die über eine LED signalisiert wird.
Eine Schleife wird so nicht verhindert, aber der Netzwerk-Administrator kann sie zumindest optisch erkennen.

42. USB

USB - Universal Serial Bus

Der USB ist eine universelle externe Schnittstelle für alle möglichen Peripheriegeräte, die an einem Computer angeschlossen werden können. Egal ob Tastatur, Maus, Modem, Drucker, Mikrofon, Lautsprecher, Kamera oder Scanner. Der USB kennt nur einen Steckertyp für alle Geräte auf der Computerseite, so dass Verwechslungen von Schnittstellen ausgeschlossen sind. Mit USB werden die Anwender unabhängig von der Anzahl der verfügbaren Schnittstellen und Steckplätze für Erweiterungskarten. Die Identifikation der Geräte wird vom USB-Hostadapter im Rechner durchgeführt, der auch das Laden der Treiber und die Grundkonfiguration vornimmt. Zusätzlich reduziert Hot-Plugging, durch das Hinzufügen und Entfernen von Peripherie-Geräten im laufenden Betrieb, die Fehlerrate.

Warum wurde der USB eingeführt/entwickelt?

Der Kauf von externen Geräte scheiterte vor der Zeit von USB häufig daran, dass ein PC nicht genug freie Schnittstellen hatte. Und der Einbau von Erweiterungskarten war wegen begrenzter Ressourcen nicht immer möglich. Hinzu kam, dass die unterschiedlichen Geräte unterschiedliche Stecker und Schnittstellen hatten. Fast jeder Gerätetyp hatte seine eigene Schnittstelle. Zwar konnte ein Gerät leichter einem festen Steckplatz zugeordnet werden. Doch das war etwas für Experten und nicht für unbedarfte Anwender.

- Serielle Schnittstelle 1: Maus/Modem
- Serielle Schnittstelle 2: Modem
- Parallele Schnittstelle: Drucker/Scanner
- Game-Port: Joystick
- verschiedene Audio-Anschlüsse: Mikrofon, Lautsprecher
- SCSI (extern): Scanner, externe Laufwerke
- PS/2 1: Maus
- PS/2 2: Tastatur

Der USB sollte mit den unterschiedlichen Schnittstellen und Anschlussbegrenzungen Schluss machen. Gefordert wurde:

- eine einheitliche Schnittstelle für alle Peripherie-Geräte
- eine mechanisch stabile und trotzdem einfach steckbare Verbindung
- kleine platzsparende Stecker/Buchsen

Installation von USB-Geräten

Die Installation eines USB-Geräts ist vergleichsweise einfach. Die Installation ist ohne technisches Wissen und im laufenden Betrieb möglich. Bei den meisten Geräten reicht es aus, den Stecker einzustecken. Danach installiert das Betriebssystem die Treiber selbst. Nach einer kurzen Installationsphase ist das Gerät betriebsbereit. Manche USB-Geräte verfügen über einen internen Speicher in dem der Treiber gespeichert ist. Er wird automatisch beim erstmaligen Einstecken installiert. Bei den meisten USB-Geräten ist es jedoch so, dass nach dem Einstecken nach einer

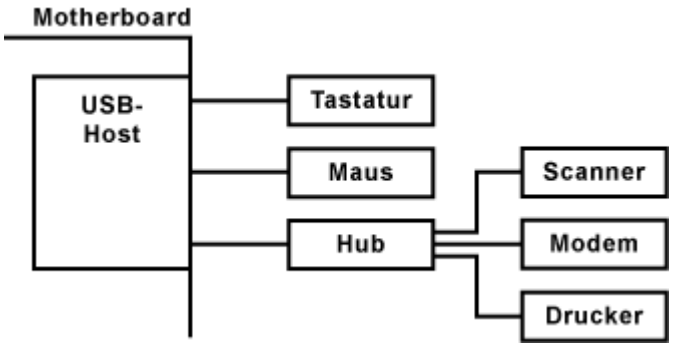
Treiber-CD gefragt wird. Der Treiber muss dann von CD installiert werden. Alternativ lässt sich auch der aktuelle Treiber von der Webseite des Herstellers herunterladen und installieren.
Bei manchen Geräten ist etwas mehr Aufwand nötig. Der Treiber muss zuerst von einer CD-ROM installiert werden, um nach einen Systemneustart das Gerät einstecken und in Betrieb nehmen zu können. Doch auch das erweist sich als einfach, da man in der Regel nur die CD oder DVD einlegen muss und danach der Treiber fast automatisch installiert wird. Alle weiteren Handgriffe seitens des Anwenders werden während des Installationsvorgangs erklärt, manchmal sogar in einer Kurzanleitung erläutert.

Warum der USB die serielle und parallele Schnittstelle nicht ersetzen kann!

Trotz ihrer langsamen Übertragungsgeschwindigkeit hielten sich die parallele und auch die serielle Schnittstelle sehr lange. Der Grund, sie lassen sich einfacher programmieren als der USB. Die serielle Schnittstelle lässt sich sehr einfach ansteuern. Jede Programmiersprache hat die dafür notwendigen Befehle und Bibliotheken integriert. So muss man nur den gewünschten Port öffnen (COM1, COM2, ...) und die Daten in den Port schreiben oder daraus lesen. Die gesamte Steuerung des Datenflusses übernimmt der Treiber des Betriebssystems.
Inzwischen gibt es keinen Grund mehr auf die alten Schnittstellen zurückzugreifen. Über programmierbare Schnittstellen (API) lassen sich alle elektronischen Geräte mit einem USB-Port ausstatten.
Trotzdem sind USB-Stecker im industriellen Umfeld weniger gern gesehen. Die Standard-USB-Stecker sind nicht industrietauglich. Sie lassen sich nicht gegen Herausziehen sichern. Außerdem sind sie nicht vibrationsfest. Die Auswahl industriekompatibler USB-Stecker ist gering und teuer. Der Stecker der seriellen und parallelen Schnittstelle lässt sich dagegen festschrauben. Wenn nötig kann man sich so einen Stecker auch selber an ein Kabel löten und so zum Beispiel ein paar Meter mehr überbrücken, als es mit dem USB-Kabel möglich ist.

Ein weiterer Nachteil des USB ist das fehlende Übertragungsprotokoll auf der Anwendungsebene. Das hat den Effekt, dass für die USB-Gerätetreiber entwickelt werden "müssen". Der einfache Wechsel von einer alten Schnittstelle zum USB ist nicht möglich, weil dazu ein neues Protokoll notwendig wäre. Für bestimmte USB-Geräte, wie zum Beispiel Maus, Tastatur und Massenspeicher haben sich Standard-Treiber vom Betriebssystem durchgesetzt. Für viele andere Anwendungen, die die serielle Schnittstelle unterstützen, wird ein VCP-Treiber (Virtual COM Port) installiert, der im Betriebssystem eine serielle Schnittstelle emuliert. Der Zugriff auf Anwendungsebene erfolgt dann wie auf eine physikalisch vorhandene serielle Schnittstelle. Das hat den Vorteil, dass für bestehende Anwendungen, die eine serielle Schnittstelle unterstützen kein neuer Treiber entwickelt werden muss.

Topologie und Verkabelung



Obwohl der USB von der Namensgebung her ein Bus sein müsste, handelt es sich dabei um eine mehrstufige Sterntopologie. Der Mittelpunkt des Sterns wird jeweils von einem Hub gebildet. Der Ausgangspunkt des USB ist der Host-Controller (Root Hub) auf dem Motherboard des Computers. Der Host-Controller steuert den gesamten Datenverkehr des USB. Am Host-Controller können bis zu 127 Geräte angeschlossen werden. Das können einzelne Geräte (Node) oder Hubs sein, an denen wiederum Geräte (Node) hängen.
Neben der Stromverteilung sorgen die Hubs auch dafür, dass immer nur ein USB-Gerät seine Daten zum Host-Controller schickt. Die Hubs können beliebig kaskadiert werden, wodurch ein pyramidenförmiger Aufbau entsteht. Wobei jedes Leitungssegment eine Punkt-zu-Punkt-Verbindung ist.

Ursprünglich ist eine direkte Kommunikation zwischen den USB-Geräten nicht vorgesehen. Eine Ergänzung (durch USB 2.0) ist USB-on-the-Go (OTG). Innerhalb eines USB-Baumes, der an einem PC hängt, kann ein Gerät ein anderes Gerät dadurch ansprechen.

USB-Geräte-Treiber

Für viele USB-Geräte gibt es Standard-Treiber in den Betriebssystemen. Dazu zählen Tastaturen, Mäuse, Digitalkameras, Scanner und Massenspeicher. Im Prinzip kann man jede Tastatur, Maus oder USB-Stick an jedem Computer ohne Probleme in Betrieb nehmen.
Die Treiber in Windows bestehen aus einer oder mehreren *.sys-Dateien (der eigentliche Treiber) sowie einer oder mehreren Windows-DLL-Dateien. Die DLL-Dateien enthalten die Softwareschnittstelle zum Treiber. Jedes Windows-Programm kann die DLL-Funktionen benutzen, um mit dem Geräte-Treiber zu kommunizieren.

HID-Treiber

Der HID-Treiber (human interface device, hid.dll) gehört zu Windows. Er ist für den Anschluss einfacher Geräte wie Tastatur oder Maus gedacht. Die Bezeichnung HID (human interface device) leitet sich aus der Anwendung für Bediengeräte für Menschen ab. Tastaturen und Mäuse, die sich an den HID-Standard halten, werden von den HID-Treibern von Windows unterstützt, so dass diese Geräte keine eigenen Treiber benötigen. Um den HID-Treiber nutzen zu können, muss sich das USB-Gerät als HID-Gerät in Windows anmelden.

CDC-Treiber

Der CDC-Treiber (communication device class, usbser.sys, MsPorts.dll) von Windows ermöglicht die RS232-Emulation über den USB. Beim Anschluss eines entsprechenden USB-Geräts wird in Windows ein virtueller COM-Port eingerichtet. Jedes Programm kann darauf zugreifen, wie wenn

es eine echte RS232-Schnittstelle wäre. Die erreichbare Transfergeschwindigkeit beträgt bis zu 1 MBit/s (125 kByte/s) und ist deutlich schneller als bei der echten RS232-Hardware mit nur 115.200 Bit/s.

Storage-Treiber

Für USB 2.0 gibt es das USB-Mass-Storage-Protocol, welches bei der Kommunikation mit USB-Massenspeicher, also externe Festplatten und USB-Sticks, zum Einsatz kommt. Die entsprechenden Treiber bringen alle Betriebssysteme mit (bei Windows usbstor.sys). Deshalb werden in der Regel alle USB-Speichersticks und USB-Festplatten ohne Probleme erkannt.
USB 3.0 bringt das USB Attached SCSI Protocol (UASP) mit, welches das USB-Mass-Storage-Protocol ablösen soll. Es bringt unter anderem die Unterstützung für NCQ (Native Command Queuing) mit. Das hat auch Vorteile für alte USB-2.0-Massenspeicher. Sie sind an einem USB-3.0-Port um bis zu 15% schneller.

Stromversorgung

Über die Kabelverbindungen versorgt der USB einfache Geräte, wie Maus und Tastatur, aber auch Scanner mit Strom. Unabhängig vom Stecker muss ein Host oder Hub die angeschlossenen Geräte mit mindestens 100 mA versorgen. Bis zu 500 mA (2,5 Watt) kann er dem Gerät auf Anforderung liefern.

Übertragungstechnik

Neben den beiden Leitungen für die Stromversorgung (+5V) gibt es zwei Datenleitungen. Die Datenübertragung erfolgt symmetrisch über zwei verdrillte Leitungen. Die eine Leitung überträgt das Datensignal, die andere das invertierte Datensignal. Man spricht von einer differenziellen Übertragung. Dabei ist der Spannungsunterschied bei der Signalspannung doppelt so groß, als wenn das Datensignal gegen Masse übertragen werden würde. Beim Empfänger wird die Differenz zwischen beiden Signalen gebildet, wobei Signalstörungen ausgeblendet werden. Das erhöht die Übertragungssicherheit, unterdrückt Gleichtaktstörungen und verbessert die elektromagnetische Verträglichkeit.

Übertragungsgeschwindigkeit

USB-Version	**USB 1.0/1.1**		**USB 2.0**	**USB 3.0**	**USB 3.1**
	Low-Speed	**Full-Speed**	**High-Speed**	**Super-Speed**	**Super-Speed+**
Symbolrate	1,875 MBi/ts	15 MBit/s	600 MBit/s	5 GBit/s	10 GBit/s
Datenrate (brutto)	1,5 MBit/s	12 MBit/s	480 MBit/s	4 GBit/s	-
Datenrate (theoretisch)	188 kByte/s	1,5 MByte/s	60 MByte/s	500 MByte/s	800 MByte/s
Datenrate (netto)	ca. 150 kByte/s	ca. 1 MByte/s	ca. 35 MByte/s	ca. 300 MByte/s	-

Interface	UHCI/OHCI	UHCI/OHCI	EHCI	xHCI	-
Leitungslänge	5 m	5m	5m	3 m	1 m
Anwendungen	Maus, Tastatur	Audio	Video, Speichermedien		

Um langsame Geräte wie Tastatur, Maus und auch schnelle Geräte wie Modems oder Videokameras über ein und den selben Bus zu führen, wurde die Übertragung in Kanäle unterteilt. Es gibt einen Low-Speed-Kanal bis 1,5 MBit/s (Maus, Tastatur) und einen Medium-Speed-Kanal mit 12 MBit/s (ISDN, Audio) die über dieselbe Schnittstelle geführt werden. Ein High-Speed-Kanal mit 480 MBit/s (Video, Speichermedien) ist auch vorgesehen (USB 2.0).

Neben der Geschwindigkeitskategorie gibt es auch unterschiedliche Prioritäten bei der Übertragung. Die höchste Priorität haben Geräte, die Daten in Echtzeit liefern und bei denen der Datenfluss nicht unterbrochen werden darf. Die mittlere Priorität ist für Interrupt-Übertragungen, wenn z. B. ein Gerät die Aufmerksamkeit des Prozessors erhalten will. Die niedrigste Priorität haben Massentransfer-Geräte. Die Übertragung dieser Daten ist meist nicht besonders dringend.

Mögliche USB-Geräte

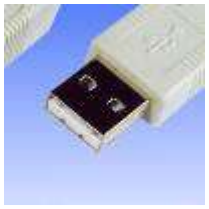
- Maus
- Tastatur
- Joystick
- ISDN-Adapter
- Digitalkamera
- Modem
- Drucker
- Scanner
- Dongle
- Lautsprecher (ohne Soundkarte nutzbar)
- USB-Speichersticks
- USB-Parallelport-Adapter
- USB-V.24-Adapter
- USB-EIDE-Adapter

Stecker und Kabel

Die Anschlusskabel dürfen maximal 5 Meter lang sein. Nach 5 Metern muss ein aktiver Hub oder ein aktives USB-Kabel als Verlängerung in die Kabelverbindung eingefügt werden. Trotzdem haben manche USB-Geräte ein Problem mit langen USB-Kabeln oder -Kabelstrecken. Meist melden sie sich nicht am System an. Es scheint, als ob sie nicht angeschlossen sind.

Unabhängig welcher Geschwindigkeitskategorie ein Gerät angehört, es wird immer der gleiche vierpolige Stecker verwendet. Unterschiede gibt es nur beim Anschlusskabel. High-Speed-Geräte benötigen ein geschirmtes und verdrilltes Kabel (USB 2.0). Für Low-speed-Gerät kann ein ungeschirmtes und unverdrilltes Kabel verwendet werden (USB 1.0/1.1).

Wegen der zunehmenden Miniaturisierung von Geräten, wie Digitalkameras, Handys und MP3-Player, war ein besonders kleiner Stecker gefragt. Der Micro-USB-Stecker ist eine noch kleinere Steckverbindung als der Mini-USB-Stecker.



USB-A-Stecker (Host)

USB-B-Stecker (Endgerät)

momentan kein Bild

Mini-A-Stecker (innen Weiß)

Mini-B-Stecker (innen Schwarz)

momentan kein Bild

Mini-AB-Stecker

Mini-B-Stecker von Hirose (z. B. für Digitalkameras)

Mini-B-Stecker von Mitsumi (z. B. für Digitalkameras)

Mini-B-Stecker von Fuji
(z. B. für Digitalkameras)

USB-Wendestecker oder USB-Flipper-Kabel

Die USB-Stecker haben den Nachteil, dass sie nur in einer Richtung in eine Buchse passen. Für den alten USB-2.0-Standard gibt es Typ-A-Stecker mit Wendestecker, was man auch als Flipper-Kabel bezeichnet. Der Typ-A-Stecker ist dabei so kontruiert, dass der innere Kunststoff-Isolator dünner ist und die Kontakte beidseitig im Stecker liegen. Das funktioniert aber nur bei USB-2.0-Anschlüssen. USB-3.0-Anschlüsse (blauer Innenteil) sind anders belegt.

USB-C-Stecker

Der USB-C-Stecker und die dazugehörigen Kabel sollen den Wildwuchs bei den USB-Steckern und -Kabeln beseitigen. Hier gibt es nicht nur A- und B-Stecker, sondern auch die ganzen Mini-Stecker und unterschiedliche Varianten für USB 2.0 und 3.0.
Der C-Stecker ist für USB 2.0, 3.0 und auch 3.1 gemacht. Die Kabel vertragen bei 5 V bis zu 5 A. Mit speziellen Kabeln für USB Power Delivery ist bei höherer Spannung bis zu 100 W zulässig. Damit sich der C-Stecker auch für mobile Geräte eignet hat er eine Abmessung von 8,25 x 2,4 mm. Die Buchse ist 8,34 x 2,56 mm groß. Das entspricht ungefähr einem USB-2.0-Micro-Anschluss, der bei Smartphones verwendet wird. Damit die korrekte Orientierung nicht mehr zur Qual wird, passt der C-Stecker auch in umgekehrter Steckposition.

Eine kurze Übersicht mit den wichtigsten Merkmalen des USB-C-Steckers:

- Der C-Stecker ist so konstruiert, dass es egal ist, wie herum er in die Buchse gesteckt wird. Man kann den C-Stecker nicht mehr falsch herum stecken.
- Der C-Stecker wird auf beiden Seiten eines Kabels verwendet. So kennt man es auch von anderen Steckverbindungen, wie HDMI, DisplayPort und RJ45.
- Der C-Stecker ist mit allen anderen USB-Steckverbindungen nicht kompatibel. Allerdings gibt es Adapter, die zu USB 2.0 abwärtskompatibel sind.
- Der C-Stecker hat in etwa die Größe eines Micro-USB-Steckers (USB 2.0).
- Der C-Stecker ist für 100 Watt Leistung ausgelegt. Die Kabel sollen sich mit Power Delivery (USB-PD) für das Laden von Notebooks eignen.

Wie sicher ist USB?

Prinzipiell ist jedes mit einem Speicher ausgestattete USB-Gerät ein potentielles Einfallstor für Schadsoftware.
Ursprünglich konnte ein USB-Massenspeicher über die AutoRun-Funktion von Windows XP ein beliebiges Programm starten. Diese Funktion wurde unter anderem dafür verwendet, um für ein USB-Gerät Treiber auf dem Computer installieren zu können, ohne dass ein Nutzereingriff notwendig war. Gleichzeitig konnte aber auch ein "böser" USB-Stick auf diese Weise Schadsoftware installieren.

Um diese Sicherheitslücke zu schließen, wurden unter Windows Vista die AutoRun-Programme erst nach einer Nachfrage gestartet, was aber kaum mehr Sicherheit brachte, weil der Nutzer das in der Regel einfach unbedacht weggeklickt hat. Bei einem mit Schadsoftware versehenen USB-Stick hat das dann zum Ausführen des Schadcodes geführt. In Windows 7 hat deshalb die AutoRun-Funktion nur noch bei optischen Laufwerken funktioniert. Doch ein entsprechend manipulierter USB-Stick ist in der Lage, sich als CD- oder DVD-Laufwerk auszugeben.
Eine weitere Gefahr geht von USB-Sticks aus, die sich beim Anschluss an den Rechner als Tastatur ausgeben, konfigurierte Aktionen ausführen und den Rechner auch übernehmen können. Böse ist das deshalb, weil eine "Tastatur" auf allen Systemen funktioniert. Zumindest bis zur nächsten Passwort-Abfrage.
Richtig böse ist es, wenn der Controller auf dem USB-Stick manipuliert ist oder wird. Die Kommunikation zwischen PC und USB-Stick verwendet das alte SCSI-Protokoll, dass in die Host- und Controller-Chips eingebaut ist und um zusätzliche Hersteller-spezifische Funktionen und Befehle erweitert ist. Beispielsweise um die Firmware eines solchen USB-Sticks auszulesen oder eine neue Firmware reinzuschreiben. Das Problem ist, dass eine Absicherung dieser Kommunikation praktisch nicht stattfindet.
Da in der Praxis die Controller von nur drei Herstellern verbreitet sind, am meisten die von Phison, wäre es denkbar, dass ein Angreifer die speziellen Kommunikationsbefehle durch Ausprobieren ermittelt und für die Firmware-Manipulation nutzt, um zum Beispiel mit Schadcode zu versehen, der sich bei jedem Einstecken in einen anderen PC dort einnistet. Bei jedem neuen USB-Stick würde der Schadcode auch diesen USB-Stick infizieren. Ein USB-Virus wäre geboren.

Um sich tatsächlich wirksam zu schützen, dürften keine USB-Geräte an einem PC angeschlossen werden. Auch keine USB-Tastaturen und -Mäuse. Als Alternative blieben nur noch PS/2-Tastaturen übrig und eine technologische Rückkehr zur seriellen und parallelen Schnittstelle. Gleichzeitig müssten USB-Ports mechanisch außer Betrieb gesetzt werden. Beispielsweise durch Verkleben mit Heißkleber.

43. USB - On the Go

USB-On-The-Go (OTG)

Normalerweise können USB-Geräte nur als Slave von einem Host-Rechner angesprochen werden. Mit USB-On-The-Go können zwei Endgeräte ihre Daten direkt miteinander austauschen. So kann zum Beispiel eine Digitalkamera Bilder ohne zwischengeschalteten Computer direkt an einen Drucker schicken. Allerdings sind die Host-Fähigkeiten der On-The-Go-Geräte im Punkt-zu-Punkt-Betrieb nur auf das notwendigste beschränkt. Nicht jedes USB-Gerät kann mit jedem anderen USB-Gerät kommunizieren.

44. Verschlüsselung

Verschlüsselung / Chiffrierung

Unter Verschlüsselung versteht man Verfahren und Algorithmen, die Daten mittels digitaler bzw. elektronischer Codes oder Schlüssel inhaltlich in eine nicht lesbare Form umwandeln. Diesen Vorgang bezeichnet man als Verschlüsseln. Gleichzeitig wird dafür gesorgt, dass nur mit dem Wissen eines Schlüssels die geheimen Daten wieder entschlüsselt werden können.
Anstatt von Verschlüsselung spricht man auch von Chiffrierung, was das gleiche meint.

Verschlüsselungsalgorithmus

Ein Verschlüsselungsalgorithmus ist eine mathematische Funktion, der man den Klartext und einen Schlüssel übergibt. Die Ausgabe ist ein Geheimtext, der keinen Rückschluss auf den Klartext erlaubt. Nur mit Kenntnis des Schlüssels kann man mit der selben mathematischen Funktion den Geheimtext wieder in den Klartext umwandeln.
Ein guter Verschlüsselungsalgorithmus macht aus, dass die Funktionsweise der mathematischen Funktion bekannt sein darf und die Daten nur mit Hilfe des Schlüssels entschlüsselt werden können. Und da das Verfahren bekannt ist, weiß man unter welchen Annahmen das Verfahren funktioniert und kann es überprüfen und auf Schwachstellen testen. Auf diese Weise kann man sicherstellen, dass ein Verschlüsselungsalgorithmus sicher ist.

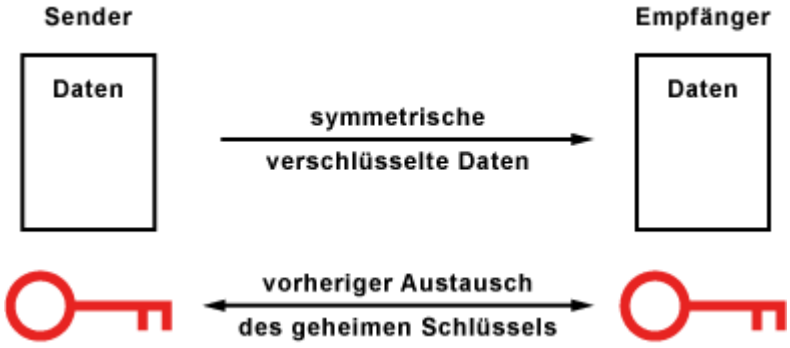
Verschlüsselungsverfahren

Ein Verschlüsselungsverfahren besteht aus einem Algorithmus zum Verschlüsseln und Entschlüsseln, sowie Verfahren zum Schlüsselaustausch, Prüfung der Authentizität und Integrität. Die bekannten Verschlüsselungsverfahren teilen sich in symmetrische, asymmetrische und hybride Verschlüsselungsverfahren auf. Bei den hybriden Verschlüsselungsverfahren wird ein symmetrisches und asymmetrisches Verschlüsselungsverfahren miteinander kombiniert.

Symmetrische Verschlüsselung

Die Verschlüsselungsverfahren, die mit einem geheimen Schlüssel arbeiten, der zum Ver- und Entschlüsseln dient, nennt man symmetrische Verfahren oder Secret-Key-Verfahren. Üblich sind auch die Bezeichnungen Secret-Key-Kryptografie und Secret-Key-Verschlüsselung.
Fast alle symmetrischen Verfahren sind auf ressourcenschonende Umgebungen optimiert. Sie zeichnen sich durch geringe Hardwareanforderungen, geringen Energieverbrauch und einfache Implementierung in Hardware aus.

Prinzip der symmetrischen Kryptografie (Secret-Key-Verfahren)



Die Verschlüsselungsverfahren der symmetrischen Kryptografie 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 Kommunikationspartnern. Vor der sicheren Datenübertragung mit Verschlüsselung müssen sich die Kommunikationspartner auf den Schlüssel einigen und austauschen. Wenn der Schlüssel den selben Kommunikationspfad nimmt,

wie die anschließend verschlüsselten Daten, dann besteht die Gefahr, dass ein Angreifer in Besitz des Schlüssels gelangt, wenn er die Kommunikation abhört. Wenn der Angreifer den Schlüssel hat, dann kann er nicht nur die Daten entschlüsseln, sondern auch selber Daten verschlüsseln, ohne das es die Kommunikationspartner bemerken. Knackpunkt ist der unsichere Schlüsselaustausch und die Authentifizierung.
Sicher ist die Schlüsselübergabe nur dann, wenn sich zwei Personen persönlich treffen und den Schlüssel austauschen oder der Schlüssel einen anderen Weg nimmt (Seitenkanal), wie es die Daten tun. Ein Möglichkeit wäre der postalische Weg (Brief, Einschreiben mit Rückschein). Allerdings nicht per E-Mail (Postkarten-Effekt).
Zur Unsicherheit trägt außerdem bei, wenn einer der Kommunikationspartner den Schlüssel nur ungenügend sicher aufbewahrt.

Der sichere Schlüsselaustausch ist eines der vielen Probleme der Kryptografie. Mit der asymmetrischen Kryptografie versucht man dieses Problem zu lösen. Weil die asymmetrische Kryptografie weit komplexere Verfahren umfasst, kombinieren die übliche kryptografischen Protokolle sowohl symmetrische als auch asymmetrische Verfahren.

Einfache Algorithmen für die Verschlüsselung mit symmetrischer Kryptografie

Jede symmetrische Verschlüsselung basiert auf einem bestimmten Algorithmus. Bei einem Verschlüsselungsalgorithmus bzw. Chiffre wird in den Klartext eine Geheiminformation, den Schlüssel, eingebracht und so der Geheimtext gebildet. Der Schlüssel kann ein Passwort, eine geheime Nummer oder auch nur eine zufällige Bitfolge sein.

- Monoalphabetische Substitutionschiffren
- Polyalphabetische Substitutionschiffren
- Permutationschiffren

Die einfachste Art der Verschlüsselung erreicht man, in dem man jeden Buchstaben ein festes Symbol zuordnen. Diese Verfahren sind monoalphabetisch. Sie sind bei genügend Verschlüsselungsmaterial leicht durch eine Häufigkeitsanalyse zu brechen. In jeder Schriftsprache kommen bestimmte Buchstaben häufiger vor. Man kann also mit einfachen statistischen Mitteln eine Kryptoanalyse machen. Mit Computer-Unterstützung geht es automatisch und noch schneller. Wesentlich schwieriger sind polyalphabetische Geheimtexte. Hier kann ein Buchstabe mehreren Symbole entsprechen. Statistische Verfahren funktionieren hier nicht mehr so einfach.

Alle gängigen symmetrische Verfahren arbeiten ausschließlich mit Bit-weisen Operationen. Hier werden Schlüssel, Klartext und Geheimtext in Form von Bitfolgen verarbeitet. In dem die Funktionen nahezu beliebig miteinander kombiniert werden, lassen sich neu symmetrische Verfahren in nahezu beliebiger Zahl entwickeln und mit bekannten Angriffen auf Schwächen testen.
In der Regel kombinieren symmetrische Verschlüsselungsalgorithmen Substitutionschiffren und Permutationschiffren miteinander und wiederholen den Vorgang mehrmals (Runden), wobei eine härtere Verschlüsselung entsteht. Typische Bestandteile von symmetrischen Verschlüsselungsalgorithmen sind:

- Exklusiv-oder-Verknüpfung
- Permutation: Reihenfolge einer Bit-Folge wird verändert.

- Substitution: Eine Bit-Folge wird durch eine andere ersetzt.

Erfahrungsgemäß sind für eine wirkungsvolle Verschlüsselung keine aufwendigen Funktionen notwendig. Insbesondere beim Hardware-nahen Programmieren oder der Implementierung in Hardware ist das von Vorteil, weil sich so eine hohe Geschwindigkeit erreichen lässt.
Beim praktischen Einsatz von Verschlüsselungsalgorithmen stellt sich auch immer die Frage, wie groß die Rechenleistung für die Verschlüsselung ist. Generell gilt, je schneller ein Verschlüsselungsverfahren arbeitet, desto niedriger sind die Hardwarekosten.

Angriffe auf symmetrische Verschlüsselungsverfahren

Angriffe auf symmetrische Verschlüsselungsverfahren zielen darauf ab, an den Schlüssel zu kommen, um den Geheimtext entschlüsseln zu können, um dann an den Klartext zu kommen.

- Ciphertext-Only-Angriff: Der Angreifer kennt den Klartext nicht. Er versucht den Schlüssel durch ausprobieren zu erraten, was der übliche Angriff auf eine Verschlüsselung ist.
- Known-Plaintext-Angriff: Im ersten Moment ungewöhnlich, aber denkbar, dass der Angreifer den Klartext oder auch nur Teile davon kennt.
- Chosen-Plaintext-Angriff: Der Angreifer hat die Möglichkeit den Klartext zu wählen und den Geheimtext zu bekommen. Anschließend versucht er, aus Geheim- und Klartext den Schlüssel zu berechnen.

Bekannte symmetrische Verschlüsselungsverfahren

Es gibt eine Unmenge an symmetrischen Verschlüsselungsverfahren. Die meisten sind allerdings wenig bekannt und weniger gut dokumentiert. Deshalb ist diese Liste als unvollständig anzusehen.

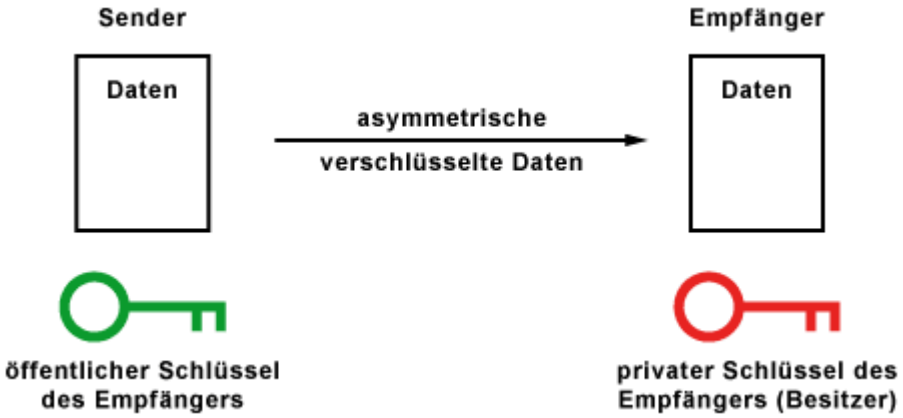
- DES - Data Encryption Standard
- 3DES - Triple DES
- IDEA - International Data Encryption Algorithm
- RC4 (Rivest-Cipher 4)
- Blowfish (Bruce Schneier)
- RC5, RC5a, RC6 (Rivest-Cipher 5 bzw. 5a bzw. 6)
- A5 (GSM)
- AES - Advanced Encryption Standard
- Serpent
- Twofish (Bruce Schneier)
- MARS
- SAFER/SAFER+
- CAST (Carlisle Adams und Stafford Tavares)
- MAGENTA
- MISTY1
- KASUMI (UMTS)
- Camellia

Asymmetrische Verschlüsselung

In der asymmetrischen Kryptografie arbeitet man nicht mit einem einzigen Schlüssel, sondern mit einem Schlüsselpaar. Bestehend aus einem öffentlichen und einem privaten Schlüssel. Man bezeichnet diese Verfahren als asymmetrische Verfahren oder Public-Key-Verfahren. Üblich sind auch die Bezeichnungen Public-Key-Kryptografie und Public-Key-Verschlüsselung.

Ein fundamentales Problem der Kryptografie ist, dass sich die Kommunikationspartner auf einen gemeinsamen Schlüssel verständigen müssen. Man bezeichnet das als Schlüsselaustauschproblem. Während ein manueller Schlüsselaustausch durch ein persönliches Treffen oder per Telefon bei einer handvoll Kommunikationspartner sicherlich kein Problem wäre. Wird es bei vielen Schlüsseln oder vielen Kommunikationspartnern schnell unübersichtlich und aufwendig. Hier kommt das Thema Schlüsselverwaltung und -verteilung zum Tragen. Alternativ bestünde die Möglichkeit einen Authentifizierungsserver einzusetzen. Beispielsweise Kerberos. Oder eben die asymmetrische Kryptografie.

Prinzip der asymmetrischen Kryptografie (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 werden, können nur mit dem privaten Schlüssel entschlüsselt werden. Deshalb muss der private Schlüssel vom Besitzer des Schlüsselpaares geheim gehalten 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 (Einwegfunktion). 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 wird. Kommt eine fremde Person an den privaten Schlüssel muss sich der Schlüsselbesitzer ein neues Schlüsselpaar besorgen.

Das Problem bei der asymmetrischen Kryptografie ist die Verteilung der öffentlichen Schlüssel. Typischerweise erfolgt die Übergabe des öffentlichen Schlüssels beim Erstkontakt. Doch hierbei stellt sich die Frage, ob dieser Schlüssel tatsächlich der echte Schlüssel des Kommunikationspartner ist.

Hinweis: Asymmetrische Verfahren benötigen viel mehr Rechenleistung als symmetrische Verfahren. Wenn man RSA und AES miteinander vergleicht, dann ist RSA ungefähr um den Faktor 1.000 langsamer als AES.

Einwegfunktion und Falltürfunktion

Bei der asymmetrischen Verschlüsselung geht es darum, eine Funktion zu wählen, die sehr einfach zu rechnen ist, aber deren Umkehrung dagegen sehr aufwendig. Realisiert wird das mit Modulo-Rechenarten. Einige davon sind tatsächlich sehr einfach zu rechnen, während die Umkehrung sehr aufwendig ist. Sie entsprechen also einer Einwegfunktion. Es gibt allerdings auch Funktionen, bei denen sich mit einer zusätzlichen Information die Umkehrung abkürzen lässt. In so einem Fall spricht man von einer Falltürfunktion.

Der diskrete Logarithmus fällt hier als Einwegfunktion besonders auf, weil man diesen sehr leicht berechnen kann. Umgekehrt ist es schlichtweg nicht möglich eine große Zahl in praktikabler Zeit zurückzurechnen. Man bezeichnet das als Diskreter-Logarithmus-Problem. Viele asymmetrische Verfahren basieren darauf. Allerdings bedeutet das nicht, dass nicht doch irgendwann ein Weg gefunden wird, den diskreten Logarithmus zu lösen.

Eine weitere Einwegfunktion ist das Multiplizieren von Primzahlen. Während die Multiplikation für einen Computer kein Problem darstellt, ist der umgekehrte Weg, beim dem das Primzahlprodukt in seine Faktoren zerlegt werden soll, nicht in akzeptabler Zeit machbar. Man spricht von Faktorisierung und in dem Zusammenhang vom Faktorisierungsproblem.
Ein Beispiel: Wenn man 17 x 19 berechnet (beides Primzahlen), dann kommt 323 heraus. Und jetzt soll man die beiden unbekannten Faktoren (17 und 19) daraus zurückberechnen. Es gibt im Prinzip nur einen Weg. Man muss alle Möglichkeiten durchprobieren. Bei hinreichend großen Primzahlen dauert das ewig. Damit ist das Faktorisierungsproblem gemeint.

Alle gängigen asymmetrische Verfahren basieren auf komplexen mathematischen Berechnungen, die gemeinsam haben, dass es für sie noch keine Vereinfachung gibt. Schlüssel, Klartext und Geheimtext stellen große Zahlen bzw. Zahlenpaare dar. Die Verfahren sind aber nur so lange sicher sind, bis jemand eine Vereinfachung gefunden hat.
Weil es nur begrenzt geeignete mathematische Berechnungen mit Einwegfunktion gibt, lassen sich nicht beliebig viele asymmetrische Verfahren entwickeln.

Angriffe auf asymmetrische Verschlüsselungsverfahren

- Public-Key-Only-Angriff: Mit Wissen des öffentlichen Schlüssels kann der Angreifer beliebigen Klartext verschlüsseln und beispielsweise mit bereits verschlüsselten Klartext vergleichen.
- Chosen-Cipertext-Angriff: Bei diesem Angriff schickt der Angreifer einen beliebigen Geheimtext an sein Ziel, um diesen entschlüsseln zu lassen.

Überblick: Asymmetrische kryptografische Verfahren

Im Vergleich zu den symmetrischen Verfahren gibt es nicht so viele asymmetrische Verfahren. Hier sind hauptsächlich RSA und Diffie-Hellman bekannt. Seltener hat man es mit MQV bzw. LMQSV zu tun.

- Diffie-Hellman-Merkle-Schlüsselaustausch
- RSA - Rivest, Shamir und Adleman
- MQV - Menezes, Qu und Vanstone (LMQSV)
- PGP - Pretty Good Privacy (OpenPGP)

Wie sicher ist asymmetrische Kryptografie?

Alle sicheren asymmetrischen Verfahren der letzten Jahrzehnte beruhen auf der Faktorisierung von Primzahlen oder dem diskreten Logarithmus. Nur so lange, wie niemand auf einen Trick kommt, wie man in realistischer Zeit faktorisieren oder das Diskreter-Algorithmus-Problem lösen kann, bleiben Verfahren wie RSA und Diffie-Hellman sicher.
Schon die Entdeckung einer praktikablen Faktorisierungsmethode würde bedeuten, dass die momentan üblichen asymmetrischen Verfahren unsicher sind. Das wäre eine Katastrophe für die moderne Kryptografie. Die Sicherheit weiter Teile der Telekommunikation, Computersysteme und Netzwerke würde wie ein Kartenhaus in sich zusammenfallen.

Asymmetrische Verfahren sind im Vergleich zu symmetrischen Verfahren langsam und komplex und deshalb sehr anfällig gegenüber Implementierungsfehlern. Komplizierte mathematische Verfahren, wie sie bei asymmetrischen Verfahren angewendet werden, bieten mehr Angriffsfläche und damit mehr Ansätze für die Kryptoanalyse. Dummerweise entstehen die meisten Sicherheitslücken durch fehlerhafte Implementierungen von kryptografischen Protokollen und bei der Prüfung der Authentizität der Kommunikationspartner. Im Vergleich dazu sind die gängigen symmetrischen Verfahren mit ihren einfachen Bit-Operationen bei geringerer Schlüssellänge sicherer.

Aus gutem Grund werden Klartexte niemals direkt mit asymmetrischen Verfahren verschlüsselt. Die Gefahr einer erfolgreichen Kryptoanalyse ist einfach zu hoch. In der Praxis werden asymmetrische Verfahren bevorzugt zum verschlüsselten Übertragen von Sitzungsschlüsseln oder Hashes verwendet.
In der Praxis kombinieren die übliche kryptografischen Protokolle sowohl symmetrische als auch asymmetrische Verfahren. Wobei der Schlüssel über ein asymmetrisches Verfahren ausgetauscht wird und anschließend mit einem symmetrischen Verfahren verschlüsselt wird.

Digitaler bzw. elektronischer Schlüssel

Man spricht von digitalen oder elektronischen Schlüsseln, wobei damit das selbe gemeint ist. Der digitale Schlüssel ist eine Bitfolge, deren Länge in Bit angegeben ist. Alle Verschlüsselungsverfahren benötigen den digitalen Schlüssel als individuellen Bestandteil der Verschlüsselung.
Von einem guten Verschlüsselungsverfahren erwartet man, dass ein Angreifer ohne Schlüssel keine Chance hat, an den Klartext zu kommen. Gleichzeitig möchte man, dass der Sender mit Hilfe des Schlüssels schnell verschlüsseln und der Empfänger schnell entschlüsseln kann.

Ein Kriterium für die Sicherheit einer Verschlüsselung ist die Anzahl möglicher Schlüssel und eine möglichst überschaubare Anzahl schwacher Schlüssel. Ein Schlüssel mit einer Länge von 1.024 Bit, also eine Folge von 1.024 Nullen und Einsen, ist sicherer als ein Schlüssel mit nur 64 Bit. Selbst wenn man weiß, wie die Verschlüsselung arbeitet, müsste man alle möglichen Schlüssel durchprobieren, um irgendwann den richtigen Schlüssel zu bekommen. Selbst bei einem relativ

unsicheren Schlüssel kann bei ausreichender Länge der Sicherheitspuffer groß genug sein. In der Regel gilt, je länger ein Schlüssel ist, desto schwieriger ist es an eine verschlüsselte Information ohne Schlüssel zukommen.

Stromchiffren und Blockchiffren

Bei Stromchiffren bzw. Stream-Cipher werden die Daten am Stück verschlüsselt. Diese Art und Weise der Verschlüsselung kommt aber nicht so häufig vor. Viel häufiger werden Blockchiffren bei der Verschlüsselung verwendet.
Bei Blockchiffren bzw. Block-Cipher werden die Daten blockweise zu einer festgelegten Größe einzeln und hintereinander verschlüsselt.

Kryptografische Protokolle / Verschlüsselungsverfahren

Um wirkungsvoll verschlüsseln zu können reicht es nicht aus, einen wirkungsvollen Verschlüsselungsalgorithmus zu haben, sondern man muss auch die verschiedenen Probleme bei der Übertragung von Daten und der Kommunikation lösen. Zu diesem Zweck fasst man verschiedene kryptografische Verfahren zusammen. Daraus entstehen dann standardisierte Verschlüsselungsverfahren bzw. kryptografische Protokolle.

Wie sicher ist Verschlüsselung?

Die Geschichte der Kryptografie lehrt uns, dass man neuen Verfahren grundsätzlich nicht trauen darf. Die meisten neuen Algorithmen werden nach kurzer Zeit oder auch etwas später geknackt, das heißt Vereinfachungsmechanismen gefunden. Nur ein paar Algorithmen bleiben übrig, bei denen auch nach Jahren alle Angriffe erfolglos blieben.
Trotzdem bleibt es schwierig Aussagen zu treffen, welche Verfahren wirklich sicher sind. Irgendwann wird jedes Verfahren gebrochen, die Schlüssel müssen länger gemacht oder die Verfahren verändert werden.

Verschlüsselung ist immer ein Spagat zwischen Sicherheit und Komfort. Absolute Sicherheit gibt es nicht. Man kann nur den Aufwand erhöhen. Mit Verschlüsselung erkauft man sich also nur Zeit, bis jemand einen Weg findet, an den Klartext der verschlüsselten Daten zu kommen.
Im Gegensatz zu oft verlautbarten Mitteilungen sind Geheimdienste, wie die NSA (USA), nicht in der Lage jede Verschlüsselung zu knacken. Eine starke Verschlüsselung ist sicher. Voraussetzung ist natürlich, dass die Schlüssel lang genug sind, das zum privaten, geheimen Schlüssel zugehörige Passwort stark genug und der geheime Schlüssel auch geheim ist und bleibt.
Generell kann man sagen, das bestätigen Krypto-Experten, dass eine gut und sauber implementierte Verschlüsselung sicher ist.
Das gilt natürlich nur unter der Voraussetzung, dass die eingesetzten Implementierungen keine Hintertüren aufweisen und in naher Zukunft kein Durchbruch bei Quantencomputern erfolgt. Spätestens dann ist jede aktuelle Verschlüsselung hinfällig.

Oft wird behauptet, dass quelloffene Software sicherer sei, als proprietärer Code. Und prinzipiell ist das auch richtig. Quellcode, der von jedem eingesehen werden kann, ist eine gute Sache. Dieser Code kann dann von jedem, insbesondere von Experten, geprüft werden. Allerdings stellt sich in der Praxis häufig heraus, dass viele diese Software einsetzen, aber doch eher selten geprüft wird. Das bedeutet, offener Code bringt nichts, wenn nur die Entwickler in den Code schauen.

Proprietärer Code, der einem unabhängigen Audit unterzogen wurde ist einem offenen Code unter Umständen vorzuziehen.
Egal ob offen oder nicht, im Endeffekt läuft es immer darauf hinaus, dass man den Entwicklern und dem Hersteller vertrauen muss.

45. Digitale Signatur

Digitale Schlüssel (Verschlüsselung)

Digitale Schlüssel sind zufällige Zeichenketten, die zusammen mit einem Algorithmus Daten im Klartext in einen Geheimtext umwandeln. Man spricht hierbei auch von Verschlüsseln. Wobei das Verschlüsselungsverfahren dafür sorgt, dass derjenige, der den Schlüssel hat aus dem Geheimtext wieder den Klartext bekommen kann. Der digitale Schlüssel ist also ein geheimer Wert, der idealerweise nur derjenige weiß, der die Daten Ver- und Entschlüsseln darf.
Dem Schlüssel kommt eine besondere Bedeutung zu, weil es neben starken und schwachen Verschlüsselungsverfahren auch starke und schwache Schlüssel gibt. Die Art und Weise, wie ein Schlüssel erzeugt wird und dessen Komplexität und Länge, spielen bei der Beurteilung eines Schlüssels eine Rolle. Aber auch, wie sicher der Schlüssel aufbewahrt wird. Denn in der Regel ist es so, dass der Schlüssel eine Länge und Komplexität aufweist, weshalb die Zeichenkette, die den Schlüssel repräsentiert, sich kein normaler Menschen merken kann. Weshalb der Schlüssel zur einfacheren Verarbeitung innerhalb eines Computersystems zum Ver- und Entschlüsseln gespeichert wird. Damit ein Angreifer nicht einfach so auf den Schlüssel zugreifen kann, sind Berechtigungen notwendig und zusätzlich die Sicherung durch ein Passwort mit einer entsprechenden Verschlüsselung.

Vom Passwort zum Schlüssel

Ein gutes Verschlüsselungsverfahren wird niemals das Passwort des Nutzers zum Verschlüsseln verwenden. Der Grund dafür ist, dass ein typisches Passwort als Schlüssel zu kurz und viel zu leicht zu erraten ist. Deshalb muss ein digitaler Schlüssel wesentlich länger sein.
Bevor ein Programm oder ein Verfahren ein Passwort zum Verschlüsseln verwenden kann, muss es aus dem Passwort einen Schlüssel generieren. Je länger der Schlüssel, desto sicherer ist die Verschlüsselung.
Bei AES-256 ist der Schlüssel zum Beispiel 256 Bit lang. Zum Vergleich hat ein Passwort mit 8 Zeichen gerade mal 64 Bit, wenn jedes Zeichen mit 8 Bit codiert ist (Unicode). Bei einem 64 Bit langen Schlüssel gäbe es immerhin $2^{64} = 1{,}8 \times 10^{16}$ Schlüssel (eine 18 mit 15 Nullen). Für einen sicheren Schlüssel sind 64 Bit allerdings viel zu kurz.

Um von einem relativ kurzen Passwort zu einem langen Schlüssel zu kommen, löst man in der Kryptografie mit einer kryptografischen Hash-Funktion. Da ein Passwort nur eine Folge von Nullen und Einsen ist, wird daraus einfach eine neue Folge von Nullen und Einsen mit fester Länge berechnet. Beispielsweise mit einer Länge von 256 Bit oder mehr.
Das hat folgenden Vorteil: Wenn ein Angreifer alle möglichen Passwörter durchprobieren will, dann dauert das sehr lange. Entweder, weil er alle möglichen Folgen von Nullen und Einsen durchprobieren muss, oder weil er alle denkbaren Passwörter mit der kryptografischen Hash-Funktion umrechnen muss. Ein normaler Computer ist damit viele Jahre beschäftigt.

Um den Aufwand beim Schlüsselknacken zu erhöhen und damit die Rechenzeit zu verlängern, wird die Hash-Funktion mehrere tausend Mal angewendet. Man bezeichnet das als Key Stretching oder Key Derivation Function. PBKDF2 (Password Based Key Derivation Function 2) gilt hier als das Maß aller Dinge. Das führt dazu, dass die Verschlüsselung mit ausreichend langen und komplexen Passwörtern kaum zu knacken ist.

Hinweis: Nicht in jedem Fall geht das Passwort oder die Passphrase in die Berechnung eines Schlüssels mit ein. Bei asymmetrischen Verschlüsselungsverfahren, wie es bei PGP zum Einsatz kommt, wird das Schlüsselpaar rein zufällig erzeugt. Hierbei hängt die Qualität des Schlüssels vom Zufall ab (Entropie), der zum Zeitpunkt der Schlüsselerzeugung auf dem System vorhanden ist. Um mehr Zufall zu erzeugen wird man bei der Schlüsselerzeugung dazu aufgefordert die Maus unsystematisch zu bewegen oder irgendwelche Tasten zu drücken. In so einem Fall ist ein Passwort nur eine Hülle, um den unberechtigten Zugriff auf den Schlüssel zu verhindern.

Erzeugung der Schlüssel / Schlüsselerzeugung

Es gibt grundsätzlich drei Faktoren, die bei der Schlüsselerzeugung wichtig sind. Zum einen woraus der Schlüssel entsteht (Schlüsselmaterial), wie der Schlüssel entsteht (Verfahren) und wo er erzeugt wird (Hardware/System). Wobei das "Wo" auch darüber entscheidet, wie und woraus der Schlüssel entsteht.

- Schlüsselmaterial (Was): Damit ein Schlüssel nicht erraten werden kann, muss das Schlüsselmaterial umfangreich und zufällig sein. Also einer zufälligen Folge von Nullen und Einsen entsprechen. Das Problem ist, dass echte Zufallsbitfolgen auf Digitalrechnern nicht realisierbar sind. Es werden nur Pseudozufallszahlenfolgen produziert, was die Sicherheit der Schlüssel reduziert. Man kann sie nachträglich berechnen. Zumindest theoretisch.
- Funktion (Wie): Die Schlüsselerzeugung erfolgt meist durch kryptografische Hash-Funktionen. Wobei nicht alle für das Erzeugen von Schlüsseln geeignet sind. Hash-Funktionen generieren aus beliebig langen Datensätzen eine Zeichenkette mit einer üblicherweise festen Länge (Angabe in Bit).
- Hardware/System (Wo): Um zu verhindern, dass ein Angreifer den Schlüssel bei der Schlüsselübertragung abgreifen kann, sollte die Schlüsselerzeugung auf dem Rechner erfolgen, auf dem der Schlüssel eingesetzt wird. Er ist zwingend geheim zu halten, weil sonst jeder der in Besitz des Schlüssel kommt, die Daten entschlüsseln kann.

Schlüssellänge

Ein Verschlüsselungsverfahren gilt dann als sicher, wenn über mehrere Jahre und intensive Untersuchungen keine Schwachstelle gefunden wurde, die in der Praxis für Angriffe nutzbar ist. Theoretische Angriffe kann es natürlich trotzdem geben. Doch die sehen bestimmte Konstellationen vor, die man in der Praxis erfolgreich vereitelt.
In der Praxis darf es also keinen besseren Angriff geben als die Suche nach dem vollständigen Schlüssel. In der Regel ist es so, dass für die verwendeten Verschlüsselungsverfahren der vollständige Schlüssel nur mit viel Rechenleistung zu ermitteln ist. Also das Durchprobieren aller denkbaren Schlüssel. In so einem Fall ist die Sicherheit des Verfahrens nur noch von der Länge des Schlüssels abhängig. Der Schlüssel sollte deshalb möglichst lang sein.

Um ein Gefühl zu bekommen, wie lang ein Schlüssel sein muss, nehmen wir einen Schlüssel, der 128 Bit lang ist (für ein symmetrisches Verfahren). Das entspräche eine Menge von 2^{128} bzw. 3,4 x 10^{38} Schlüssel. Mit jedem Bit verdoppelt sich der Aufwand für den Angreifer, den er zum Knacken benötigt.
Nehmen wir weiter an, dass ein Angreifer einen Rechner hat, mit dem er 100 Milliarden Schlüssel pro Sekunden durchprobieren kann. Das Durchprobieren aller Schlüssel würde 3,4 x 10^{27} Sekunden dauern. Hätte der Angreifer 10 solcher Rechner, dann würde er 3,4 x 10^{26} Sekunden brauchen. Gehen wir mal davon aus, dass der Angreifer 100 solcher Rechner hat, dann würde er 3,4 x 10^{25} Sekunden brauchen. Hat der Angreifer großes Glück, und er hätte schon nach 1 Prozent der möglichen Schlüssel, den richtigen gefunden, dann hätte er 3,4 x 10^{23} Sekunden dafür gebraucht. Um ein Verständnis für diesen Zeitraum zu bekommen: Das sind 10^{16} Jahre. Das Alter unseres Universums wird auf 10^{10} Jahre geschätzt.
Wir stellen also fest, ein Schlüssel mit einer Länge von 128 Bit lässt sich praktisch nicht per Brute-Force (vollständige Schlüsselsuche) herausbekommen.

Eine Schlüssellänge von 128 Bit ist also durchaus ausreichend. In der Praxis ist es jedoch so, dass man längere Schlüssel verwendet. Beispielsweise 192 oder sogar 256 Bit. Das rührt daher, weil man davon ausgehen muss, dass irgendwann einmal mit Quantencomputer Kryptoanalysen möglich sind. Schon jetzt halbiert der Grover-Algorithmus mit den quantenmechanischen Gesetzen auf einem Quantencomputer die Schritte bei einer Schlüsselsuche um die Hälfte.
Außerdem gibt es in der Kryptografie Angriffe, die zur Halbierung der effektiven Schlüssellänge führt. Aus diesem Grund empfiehlt sich eine Schlüssellänge von 256 Bit, um die Sicherheit von 128 Bit zu haben. Schlüssellängen von 512 Bit oder mehr werden jedoch nicht empfohlen, weil man sonst an Software- und Hardware-Grenzen stößt. Beispielsweise beim Speicherplatzbedarf.

Hinweis: Längere Schlüssel bedeuten nicht zwangsläufig mehr Sicherheit. Ein langer Schlüssel bedeutet in der Regel auch, dass die vollständige Schlüsselsuche nicht mehr der beste Angriff ist. Wenn einem Angreifer der Schlüssel zu lang ist und er keine Möglichkeit hat, den Schlüssel mit einer vollständigen Schlüsselsuche herauszubekommen, muss er andere Wege finden. Unter Umständen tritt dann eine Schwäche des Verschlüsselungsalgorithmus oder eine Implementierung in den Vordergrund, die vorher in der Praxis keine Rolle gespielt hat.

Wie lang sollte ein Schlüssel sein?

Es gibt auf die Frage, wie lang ein Schlüssel sein muss, keine richtige Antwort. Im Prinzip sollte er immer so lang wie möglich sein. Aber irgendwie muss man die Länge definieren. Da die Sicherheit eines Schlüssels von seiner Länge abhängig ist, muss zuerst definiert werden, wie lange Daten sicher gespeicherte sein müssen. Danach legt man sich auf die Länge der Schlüssel fest. Klar muss jedoch sein, dass mit steigender Rechenleistung auch die Länge der Schlüssel zunehmen muss.
Grundsätzlich muss man zwischen asymmetrischen Schlüsseln für die Authentisierung, wie sie bspw. in Zertifikaten enthalten sind und symmetrischen Schlüsseln, die einfache Hash-Werte sind, unterscheiden. Die asymmetrischen Schlüssel in Zertifikaten sind immer länger (1.024 bis 4.096 Bit), während Hash-Werte kürzer sind (128 bis 512 Bit).
Bei symmetrischen Verfahren ist die Schlüssellänge immer vorgegeben oder man kann zumindest aus mehreren Vorgaben wählen. Bei asymmetrischen Verfahren ist die Schlüssellänge variabel, weil die als Schlüssel verwendete Zahl eine beliebige Größe annehmen kann.

Die folgenden Empfehlungen kommen von der European Union Agency for Network and Information Security, kurz ENISA, die einen Bericht zu Algorithmen und Schlüssellängen veröffentlicht hat (Stand Oktober 2013). Diese Empfehlungen sind mit Sicherheit besser, als von der NSA unterwanderte US-amerikanische Organisationen. So unterscheiden sich die ENISA-Empfehlungen deutlich von denen des National Institute of Standards and Technology (NIST).

Die ENISA unterscheidet zwischen kurzfristig, mittel- und langfristig gespeicherten Daten. Kurzfristig gespeicherte Daten sind schutzbedürftige Transaktionsdaten. Hier werden für **symmetrische Schlüssel** eine Länge von 80 Bit empfohlen. Für die mittelfristig gespeicherten Daten sollen es schon 128 Bit und für langfristig gespeicherte Daten 256 Bit sein.

Für **Blockchiffren (Block Cipher)** in Kombination mit AES werden 128 Bit und langfristig 256 Bit empfohlen. Als **Hash-Funktion** empfiehlt sich SHA-256 und für den langfristigen Einsatz SHA-512 zu benutzen. Alternativen sind Camellia, SHA-3 und Whirlpool. Gute **Stromchiffren (Stream Cipher)** sind Rabbit und Snow 3G. Auf RC4 ist zu verzichten.

Für die Public-Key-Verschlüsselung wird der Einsatz von Elliptic Curve Cryptography (ECC) empfohlen. Für Transaktionen sind Kurven mit 160 Bit, für mittelfristige Speicherung 256 Bit und langfristig 512 Bit ausreichend.
Die Vertrauenswürdigkeit der spezifizierten Kurven wird allerdings wegen der Mitwirkung der NSA und Standardisierung durch das NIST angezweifelt. Ob der Einsatz elliptischer Kurven mehr Sicherheit bringt, wird sich erst in der Zukunft herausstellen.
Für **asymmetrische Schlüssel** empfiehlt es sich für neue Schlüssel mindestens eine Länge von 3.072 Bit zu wählen. Für die längerfristige Sicherheit sollte die Schlüssel sogar 15.360 Bit haben. Das entspricht einer Sicherheit von 256-Bit-Schlüsseln bei symmetrischen Verfahren.

Leider sind in der Praxis nicht immer die Funktionen zur Erzeugung der empfohlenen Schlüssellängen verfügbar. Deshalb kann man sich an Schlüssellängen von 4.096 Bit und Hash-Werten mit 512 Bit orientieren. Mit diesen Werten hat man Schlüssel, die ausreichend sicher sind. Kürzere Schlüssel sind weniger sicher. Sind die Schlüssel wesentlich kürzer, dann sind die Schlüssel für die Zukunft als unsicher anzusehen und auszutauschen.

46. Green-IT

Green-IT ist ein Schlagwort in der IT-Branche, mit der umweltverträgliche und energieeffiziente Produkte und Prozesse beschrieben werden. Dazu gehört die Schonung der natürlichen Ressourcen, der sparsame Materialeinsatz, Recycling und langsame Nutzungszyklen, die Vermeidung von Schadstoffen und technische Maßnahmen zur Verlängerung der Batterielaufzeit in mobilen Geräten. Doch die Gerätehersteller geraten sehr schnell mit Green-IT in einen Interessenskonflikt. Sie wollen vor allem ihre Geräte verkaufen. Und die Kunden schauen vor allem auf den Preis.

Den Weg für Green-IT haben Richtlinien und Gesetze vor allem auf der europäischen Ebene geebnet. Dazu gehören die RoHS- und WEEE-Richtlinien, die beispielsweise zu bleifreien Lötprozessen geführt haben. Und die EuP-Richtlinie (Energy using Products), die Regelungen für das Öko-Design enthält. Zwar gelten diese Richtlinien hauptsächlich in Europa. Doch der Trend geht zu Systemen, die auf der ganzen Welt geeignet sind. Die Produkte unterscheiden sich nur noch anhand programmierbarer Hardware und Software. Bei der Produktion müssen die

europäischen Richtlinien berücksichtigt werden. Das bedeutet, dass umweltverträgliche und energieeffiziente Produkte auf der ganzen Welt zum Einsatz kommen.

Kann IT grün sein?

Kritiker sprechen von einer "Fehlinterpretationen" im Zusammenhang mit der Nutzung des Begriffs "Green IT". Sie behaupten IT kann gar nicht "grün" sein. Die ITK-Branche ist für 2 Prozent der CO^2-Emissionen weltweit verantwortlich und auch noch für die weltweit enorme Zunahme des Energieverbrauchs. Über den Energieverbrauch hinaus müsste die bei der Produktion eingesetzten Materialien und der anfallende Elektroschrott berücksichtigt werden. Bei der Herstellung von IT-Hardware kommen toxische Substanzen wie Blei, Quecksilber, Cadmium oder Brom zum Einsatz, was eine spätere Wiederverwertung erschwert und zu weiteren Umweltbelastungen führt.

Sowohl in der Politik und der IT-Branche sind Themen, wie Ökologie und Energieeffizienz keine echte Herzensangelegenheit. In wirtschaftlich schwierigen Zeiten sind nur Wenige bereit nachhaltige Strategien und Konzepte umzusetzen. Wenn dann auch noch die Energiepreise fallen, dann wird es schwieriger die Vorteile ressourcen- und energiesparender Technik zu demonstrieren.

Blauer Engel

Den Blauen Engel gibt es schon seit 1978. Weltweit ist es die erste und älteste Kennzeichnung für umweltschonende Produkte und Dienstleistungen. Der Blaue Engel legt verschiedene gerätespezifische Kriterien und strenge Richtlinien für PCs, Notebooks, Bildschirme, Drucker, Kopierer und Tastaturen fest.

TCO certified

TCO ist die Abkürzung für Tjänstemännens Centralorganisation. Es handelt sich dabei um den Dachverband der schwedischen Angestelltengewerkschaft. Gewerkschaften agieren bekanntlich für die Interessen ihrer Mitglieder. Die TCO gibt Richtlinien für Geräte heraus, die üblicherweise an Büroarbeitsplätzen zum Einsatz kommen. In den letzten Jahren berücksichtigte die TCO auch Geräte für den mobilen Einsatz.
Die TCO legt in ihren Richtlinien fest, dass bei der Herstellung keine giftigen Stoffe verwendet werden dürfen. Dazu zählen Schwermetalle oder bromierte oder chlorierte Flammschutzmittel. Außerdem legt die TCO Richtwerte für die Emission magnetischer und elektrischer Felder, den

Stromverbrauch im Standby-Modus und im ausgeschalteten Zustand von Geräten und Grenzwerte für die Staub- und Ozonemission bei Druckern fest.

- TCO'92: Monitore
- TCO'95: Monitore und Tastaturen
- TCO'99: Drucker und Tastaturen
- TCO'01: Mobiltelefone
- TCO'03: Monitore
- TCO'05: PCs und Notebooks
- TCO'06: Monitore
- TCO'07: Headsets

Energy-Star

Mit dem Energy Star werden Computer, Drucker, Scanner und Monitore ausgezeichnet, die den Stromsparkriterien der amerikanischen Umweltschutzbehörde (EPA, Environmental Protection Agency) entsprechen. Das bedeutet aber auch, dass die Energy-Star-Richtlinien nicht verpflichtend gültig sind. Deren Einhaltung fordern nur Großfirmen und Behörden bei Ausschreibungen. In der Regel ist es so, dass gewerblich genutzte Computer diese Vorgaben eher einhalten, als Heim-Computer.

80Plus

Bei 80Plus handelt es sich um eine nordamerikanische Initiative für energieeffiziente Netzteile, die aber in weltweit eingesetzten Netzteilen Früchte trägt. Die 80Plus-Richtlinie legt fest, dass Netzteile bei den Lastzuständen 20, 50 und 80 Prozent, mindestens einen Wirkungsgrad von 80% haben müssen.

RoHS

RoHS ist das Kürzel für die EU-Richtlinie 2002/95/EG. In Deutschland entspricht RoHS dem ElektroG (Gesetz). Mit dieser Richtlinie wird die Herstellung und Verarbeitung von gefährlichen

Substanzen, wie Blei, Cadmium und Quecksilber in elektronischen Geräten verboten. Konkret bedeutet das, dass bleifrei gelötet werden muss und bei der Herstellung von Kabeln keine giftigen Flammenhemmer benutzt werden dürfen.

Eco-Blume

Die Eco-Blume ist ein europäisches Umweltzeichen für PCs, Notebooks und Fernseher. Die Eco-Blume kennzeichnet Geräte, die im Betrieb und Standby einen geringen Stromverbrauch haben, aus langlebigen und wiederverwertbaren Materialien bestehen und nur wenige umweltschädliche Substanzen enthalten.
Für Fernsehgeräte gibt es eine kostenfreie Rücknahme von Altgeräten. PCs und Notebooks sind zerlegbar, wiederaufbereitbar und nachrüstbar. Speziell Notebook enthalten weniger umweltschädliche Batterien.

Steigende Energie-Preise

Im Zuge von Green-IT und Umweltschutz dreht sich der Leistungsverbrauch von PCs aufgrund der stark steigenden Energiepreise in die andere Richtung. Das bedeutet, bei der Ausstattung wird mehr auf stromsparende Komponenten, insbesondere des Prozessors, geachtet. Dabei geht der Stromverbrauch von PCs wieder zurück. PC-Netzteile mit weniger Watt (unter 450 Watt) sind wieder stärker gefragt.

EuP-Richtlinie: 1-Watt-PC

Die Öko-Design-Richtlinie (EuP-Richtlinie) der EU ist seit Anfang 2009 in Deutschland gültig. Die Richtlinie legt fest, dass ab 2010 der Energieverbrauch von PCs im Soft-Off-Modus (ACPI S5) 1 W betragen darf. Wichtig ist, der 1-W-Betriebsmodus muss werksseitig voreingestellt sein. Ab 2014 sogar nur höchstens 0,5 W.
Technischer Hintergrund: Die Leistungsaufnahme im S5-Modus bezieht sich auf Motherboard und Netzteil. Die Erzeugung der Standby-Versorgungsspannung von 5 Volt hat einen Wirkungsgrad von 50%. Das bedeutet, bei 1 W Energieverbrauch darf das Motherboard nicht mehr als 0,5 Watt Leistung aufnehmen, was für die meisten Motherboards kein Problem sein sollte. Im Soft-Off-Modus muss eigentlich auch nur der Super-I/O-Chip laufen, in dem die Ein- und Ausschaltlogik des PCs steckt.

Batterie-Richtlinie der EU seit September 2008

Schon im März 1991 hat die Europäische Union eine Batterie-Richtlinie (91/157/EEC) verabschiedet. Darin wurde die Verwendung von Quecksilber in Batterien beschränkt und die Sammlung und Wiederverwertung unterstützt. Allerdings war es immer noch so, dass die meisten Gerätebatterien im Restmüll landeten.
Deshalb hat die EU eine neue Batterie-Richtlinie (2006/66/EC) verabschiedet, die am 26. September 2008 in Kraft getreten ist und die bestehende Richtlinie von 1991 ersetzt hat.
Da ein völliger Verzicht auf Batterien und Akkus als unrealistisch gilt strebt die EU durch diese Batterie-Richtlinie die Verwendung weniger gefährlicher Stoffe bei der Herstellung von Batterien und Akkus an. Die Richtlinie untersagt die Ausstattung von Geräten mit Batterien (nicht wiederaufladbar) und Akkumulatoren (wiederaufladbar), die bestimmte gefährliche Metalle enthalten. Außerdem ist vorgesehen, dass alle Industrie- und Gerätebatterien nach Ablauf ihrer Lebensdauer gesammelt und wiederverwertet werden müssen. Dies liegt in der Verantwortung der Produzenten und muss in deren Kostenrechnung und Prozesse berücksichtigt werden. Die Mehrkosten für die Entsorgung von Akkus und Batterien werden so beim Produktpreis aufgeschlagen. Damit werden die Entsorgungskosten schon im Anschaffungspreis berücksichtigt.

47. 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-Switche gegenüber reinen Routern bevorzugt. Zumindest in großen Netzen. Layer-3-Switche lassen sich als Router, Switch oder als Mischform betreiben. Im Vergleich zu Routern haben Layer-3-Switche eine geringere Verzögerungszeit und einen höheren Datendurchsatz.
Funktionell ist es so, dass das erste Datenpaket einer Verbindung wie bei einem Router behandelt wird. 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

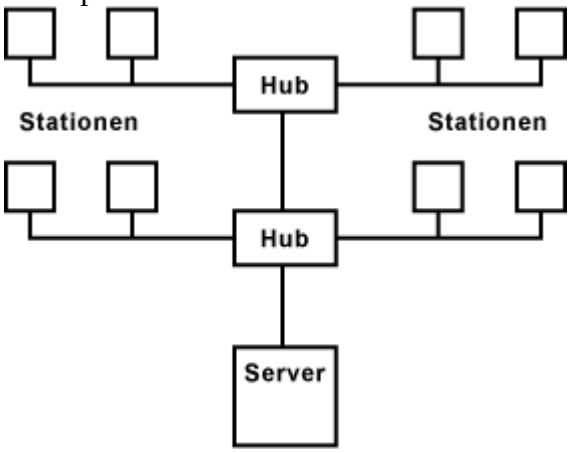
Nachteile Layer-3-Switch (gegenüber Router)

- weniger Features

Auf IP-Ebene lassen sich durch Routing-Funktionen deutlich mehr Möglichkeiten zur Steuerung von Netzwerkverkehr realisieren.

48. 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.
Das Versenden 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 können.

49. Layer-2-Switching-Verfahren: Cut-Though, store and forward

Switching ist ein Mechanismus in paketorientierten Netzwerken, um für eingehende Datenpakete den richtigen Ausgang zu ermitteln. Dabei geht es darum auf Basis von Sender- und Empfänger-Adressen eine Verbindung zwischen einem Eingangs-Port und einem Ausgangs-Port zu schalten.

Dafür gibt es verschiedene Switching-Verfahren, die in der folgende Beschreibung Ethernet als Grundlagen haben.

Switching-Verfahren

Beim Switching wird das eingehende Ethernet-Frame (Datenpaket) 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, wodurch der Tabelleneintrag veralten würde, werden die Einträge in der MAC-Tabelle regelmäßig gelöscht (Ageing-Mechanismus).

- Cut-Through
- Store-and-Forward
- Adaptive-Cut-Through
- FragmentFree-Cut-Through

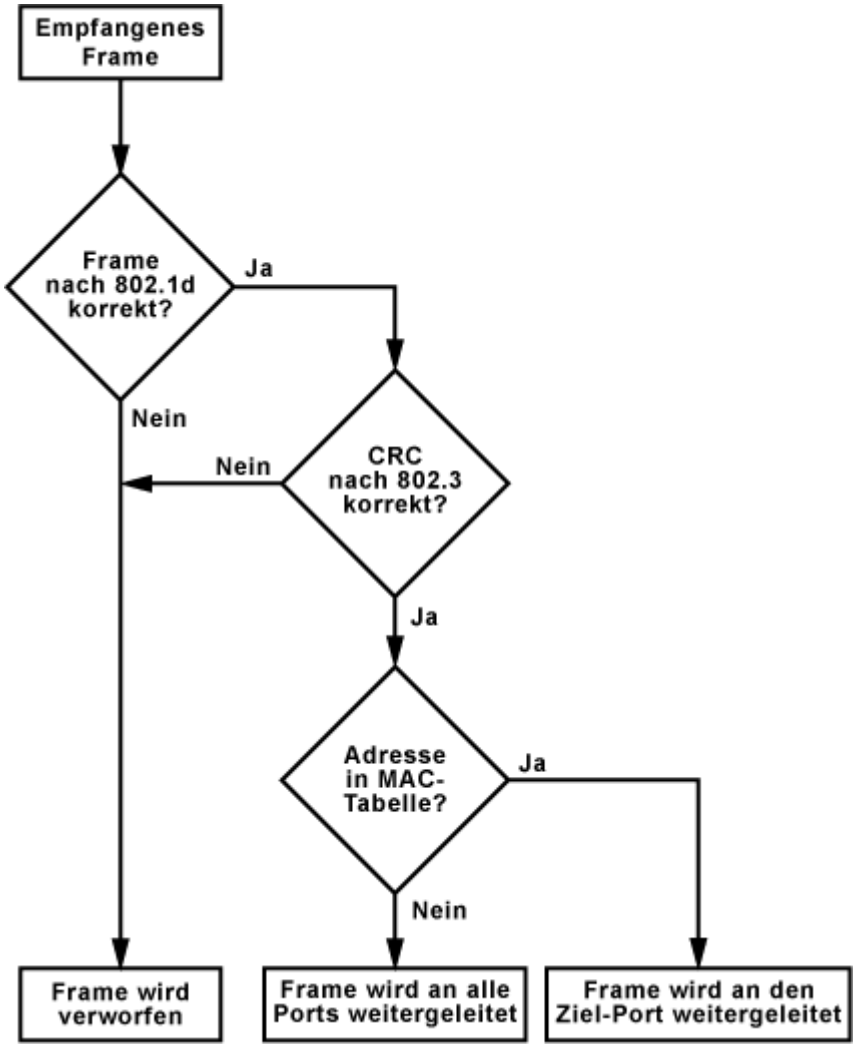
Cut-Through

Der Switch analysiert die Ethernet-Frames, bevor sie vollständig eingetroffen sind. Hat er die Ziel-Adresse identifiziert, wird das Frame sofort an den 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. 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 alle 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.

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.

Ermittlung der Latenz von Switching-Verfahren

Die Verzögerung, die beim Verarbeiten und Weiterleiten von Ethernet-Frames entsteht, wird Latenz genannt. Die Dauer hängt vom verwendeten Switching-Verfahren ab. Bei Store-and-Forward ist die Latenz die Zeit, die zwischen dem Empfang des letzten Bit und der Ausgabe des ersten Bit eines Ethernet-Frames verflossen ist. Die genaue Bezeichnung lautet Last In First Out (LIFO) Latency.
Bei Cut-Through wird die Latenz zwischen dem ersten eingegangenen Bit und dem ersten ausgegebenen Bit eines Ethernet-Frames gemessen. Die genaue Bezeichnung lautet First In First Out (FIFO) Latency.
Wegen der unterschiedlichen Messverfahren ist ein direkter Vergleich anhand der Latenz zwischen Cut-Through und Store-and-Forward nicht möglich.

Switching-Verfahren	Messverfahren	Latenz
Cut-Through	First In First Out (FIFO)	~ 35 µs
Store-and-Forward	Last In First Out (LIFO)	~ 18 µs

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.

Beim Vergleich von Switching-Verfahren interessiert hauptsächlich die Verzögerung, die der Switch im Vergleich zur Weiterleitung auf der blanken Leitung zusätzlich verursacht. Diese Verzögerung ist bei Cut-Through die angegebene Latenz. Sie ist unabhängig von der Frame-Länge und damit konstant. Bei Store-and-Forward ist die Verzögerung gleich der Latenz, zuzüglich der Frame-Dauer und damit abhängig von der Art des Datenverkehrs. Konkret bedeutet das, je länger ein Frame, desto größer die Verzögerung.

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. Diese Maßnahmen gehen zu Lasten der Übertragungsgeschwindigkeit. Denn kleinere Pakete bedeuten einen größeren Anteil von Steuerungsdaten (Header) gegenüber den 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.

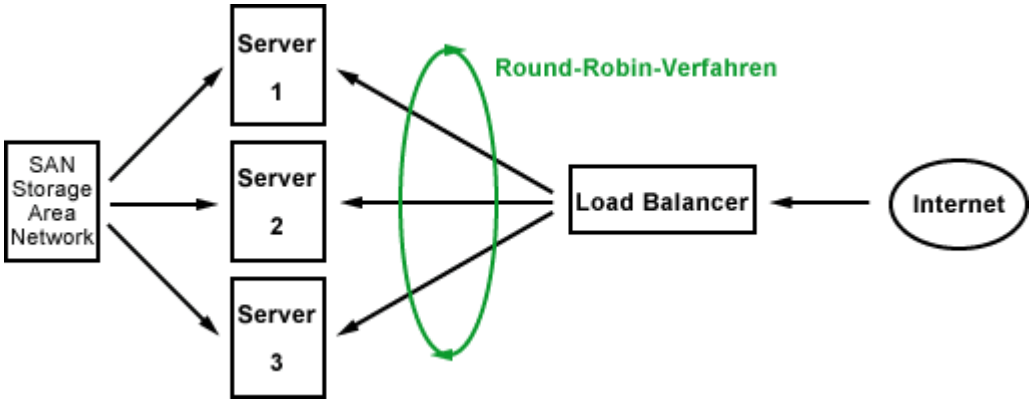
Back-Pressure

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 Flow-Control. Bei Fast-Ethernet-Komponenten ist das nicht immer der Fall. Ob diese Funktion genutzt werden kann, wird während dem Link-Aufbau (nach dem Herstellen der Steckverbindung) mit 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.

50. Round-Robin-Verfahren



Das Round-Robin-Verfahren kommt mit einer einzigen IP-Adresse aus. Anstatt des DNS-Servers übernimmt ein NAT-Proxy die Lastverteilung. Anstatt einer Liste mit den verfügbaren Servern leitet der Proxy alle Anfragen an die ihm bekannten Zielsysteme weiter. Dabei merkt er sich welche IP-Adresse mit welchem Server eine Verbindung hatte und leitet eine erneute Anfrage an diesen Server weiter.
Der Vorteil ist, dass nur eine IP-Adresse zum Internet hin benötigt wird und diese Variante nur einen geringen Administrationsaufwand erfordert. Unter anderem muss keine Liste mit Servern gepflegt werden. Allerdings handelt es sich hierbei ebenfalls um keine richtige Lastverteilung. Der Zustand einzelner Server wird nicht berücksichtigt.

51. ICMP

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.

ICMPv6 - Internet Control Message Protocol Version 6

Das Internet Control Message Protocol Version 6 (ICMPv6) ist Bestandteil des Internet Protocols Version 6 (IPv6). 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.

ICMPv6 wird verwendet, um NDP-Nachrichten, wie Router Discovery und Neighbor Discovery zu verschicken. NDP umfasst die Funktionen von ARP, RARP und IGMP als Teil von IPv4. Für IPv6 sind das in NDP Neighbor Discovery, Inverse Neighbor Discovery und Multicast Listener Discovery (MLD).
ICMPv6 spielt eine wichtige Rolle für die Funktionsweise von IPv6-Verbindungen. Im Vergleich zu IPv4 dürfen ICMPv6-Datenpakete nicht einfach so blockiert werden.

Aufbau des ICMPv6-Headers

Der ICMPv6-Header besteht aus mindestens drei Feldern:

- 8 Bit für den Typ der NDP-Nachricht
- 8 Bit für den Code der NDP-Nachricht
- 16 Bit für die Prüfsumme des ICMPv6-Datenpakets

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.

ICMPv6-Nachrichten-Typen

- Router Advertisement (ICMPv6-Typ 134)
- Router Solicitation (ICMPv6-Typ 133)
- Neighbor Advertisement (ICMPv6-Typ 136)
- Neighbor Solicitation (ICMPv6-Typ 135)
- Redirect (ICMPv6-Typ 137)

RA - Router Advertisement

Router Advertisements (RA) sind ICMPv6-Nachrichten vom Typ 134, mit denen sich Router im Netz bekanntgeben, Routing-Informationen verbreiten und Informationen für die IP-Autokonfiguration (Stateless Address Autoconfiguration, SLAAC) verteilen.
Dazu sendet ein Router in regelmäßigen Abständen ein sogenanntes Router Advertisement an die Multicast-Adresse "ff02::1". Davon fühlen sich alle Hosts im Link-Local-Scope angesprochen, die gegebenenfalls ihre IPv6-Konfiguration aktualisieren. Auf diese Weise erfahren alle Hosts die Adresse des Default-Routers und die link-lokalen und globalen Präfixe.
Router Advertisements lassen sich auch per Router Solicitation durch einzelne Hosts erzwingen.

RS - Router Solicitation

Router Solicitations (SA) sind ICMPv6-Nachrichten vom Typ 135, mit denen ein Host um einen Router Advertisement bittet.
Zwar sendet der Router periodisch Router-Advertisement-Nachrichten. Doch muss ein Host nicht darauf warten, sondern kann ein Router Advertisement erzwingen in dem er ein Router Solicitation senden. Der Router kann darauf mit einer Multicast-Nachricht an alle oder mit einer Unicast-Nachricht an den anfragenden Host antworten.

Neighbor Advertisement und Neighbor Solicitation (Neighbor Discovery)

Neighbor Advertisements sind ICMPv6-Nachrichten vom Typ 136, bei denen es sich um Antworten auf Neighbor Solicitations handelt. Neighbor Solicitation sind ICMPv6-Nachrichten vom Typ 137, bei denen es sich um Nachrichten mit der Bitte um Antwort handelt. Neighbor Advertisement und Neighbor Solicitation werden im Rahmen der Duplicate Address Detection (DAD), Neighbor Unreachability Detection (NUD) und Adressauflösung ausgetauscht.

Neighbor-Cache

Im Rahmen der Neighbor Discovery mit Neighbor Solicitation und Neighbor Advertisement entsteht der Neighbor-Cache. Das ist eine Liste von Netzwerkbekanntschaften aller Netzwerkschnittstellen, die ein Betriebssystem anlegt. Hier sind alle Rechner verzeichnet zu denen in letzter Zeit eine Verbindung bestand.
Der Neighbor-Cache entspricht dem ARP-Cache unter IPv4.

Mit den folgenden Befehlen kann man sich den Neighbor-Cache des eigenen Rechners anschauen:

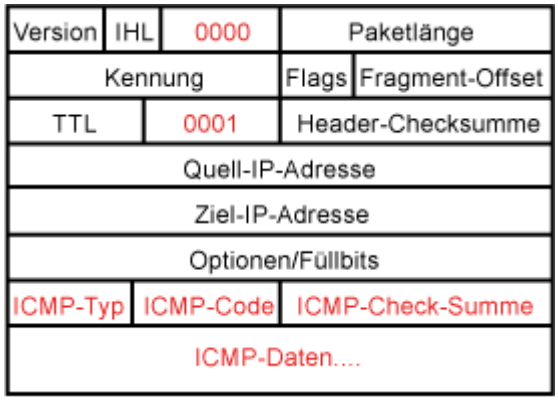
- Windows: netsh interface ipv6 show neighbors
- Linux: ip -6 neighbor show

Auf einem neu gestarteten Rechner ist diese Liste sehr kurz und enthält in der Regel nur die Adresse des nächsten IPv6-Routers im Link-Local-Scope.
Dank der Multicast-Adresse "ff02::1" kann man mit einem "ping" alle im Link-Local-Scope laufenden IPv6-Geräte herausfinden (Neighbor Solicitation).

- Windows: ping -6 ff02::1
- Linux: ping6 -c 5 ff02::1

Alle Systeme am Link-Local-Scope versenden dann Antwortpakete (Neighbor Advertisement), sofern die Geräte die Neighbor Solicitation erhalten haben. Dazu müssen sie mit dem LAN verbunden sein. Und eine Firewall oder eine andere Sicherheitsmaßnahme darf ICMPv6-Pakete nicht blockieren.
Anschließend finden sich alle Systeme, die geantwortet haben, im Neighbor Cache wieder. Diese Liste kann für weitere Untersuchungen im Link-Local-Scope nützlich sein.

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.

Anwendung von ICMP

Die meisten Internet- und Netzwerk-Benutzer kommen mit ICMP selten 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.

52. Intranet und Extranet

Intranet und Extranet sind Rechnernetze, die auf den gleichen Techniken wie das Internet basieren, aber im Gegensatz zum Internet nicht für jedermann zugänglich sind. Beide dienen in erster Linie der Bereitstellung und dem Austausch von Informationen.

Intranet: Austausch innerhalb der Organisation

Jedes Intranet besteht aus mehreren Internet-Diensten innerhalb eines lokalen Netzwerkes. Es ist in der Regel auch nur über die Arbeitsplätze des lokalen Netzwerks zugänglich. Die Nutzer eines Intranets müssen sich häufig mit einem Benutzernamen und Passwort anmelden, da dadurch die Vergabe der Zugriffsrechte einzelner Teilnehmer geregelt wird. Das Intranet nutzt die Client-Server-Standards des Internets, basiert also auch auf TCP/IP Protokollen. Durch die Verwendung von Webbrowsern- und Servern wird somit für eine Organisation oder ein Unternehmen ein internes Informationssystem erzeugt.

Extranet: Austausch außerhalb der Organisation

Das Extranet funktioniert in den Grundzügen genauso wie das Intranet. Der wesentliche Unterschied ist jedoch, dass auch ein Benutzerkreis von außen auf das Netzwerk zugreifen kann. Somit ist das Extranet eine Erweiterung des Intranets. Ein Extranet ermöglicht es beispielsweise einem Unternehmen oder einer Organisation, nicht nur internen Nutzern wie beispielsweise Mitarbeitern, sondern auch externen Nutzern, wie etwa Kunden oder Partnern, Informationen zugänglich zu machen.

Nutzen und Vorteile von Intranet und Extranet

Durch den Einsatz eines Intranets oder Extranets kann ohne großen Aufwand ein umfassendes Informationssystem erzeugt werden. Intranet und Extranet ermöglichen es, Dokumente jeder Art auszutauschen und sie einer bestimmten Personengruppe zur Verfügung zu stellen. Außerdem

können sie auch die Funktion einer Groupware erfüllen, also kooperative Arbeit ermöglichen. Daneben können weitere Funktionen integriert werden wie beispielsweise eine Suchmaschine, ein Personalverzeichnis, eine Projektverwaltung, ein Messenger-Dienst, etc.
Somit kann das Intranet bzw. Extranet als eine Informationsschnittstelle, je nach dem intern oder extern, bezeichnet werden. Die beiden Netzwerke ermöglichen einen vereinfachten Zugriff auf Informationen, stellen eine hohe Aktualität sicher (da die Inhalte sehr einfach gepflegt werden können) und sorgen damit auch für eine erhöhte Transparenz in der jeweiligen Organisation.

Voraussetzungen und Bedingungen

Damit der Einsatz eines Intranets oder Extranets zum Erfolg führt, sollten bestimmte Punkte beachtete werden: Neben eine sachgerechte Implementierung und den entsprechenden Investitionen in das System selbst, ist in erster Linie das Thema Datenschutz ein Knackpunkt. Die Daten des Intranets sind nur für den internen Gebrauch bestimmt und dürfen unter keinen Umständen nach außen dringen. Durch entsprechende Maßnahmen, wie den Einsatz von Firewalls und Proxy Server, kann jedoch ein sehr hoher Sicherheitsstandard realisiert werden - wobei es in Zeiten von zunehmenden Cyber-Angriffen nie einen hundertprozentigen Schutz vor einem digitalen Einbruch mehr geben kann.

53. POP3

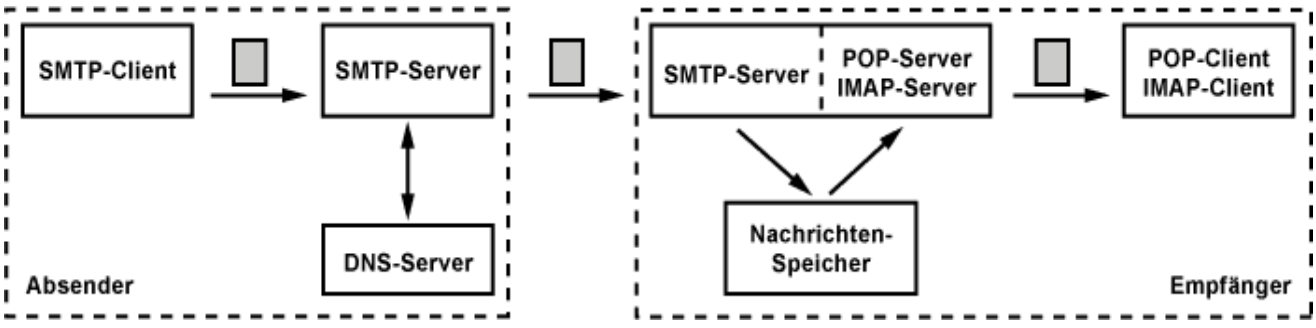
POP3 sieht das Prinzip der Offline-Verarbeitung von E-Mails vor. Online werden die E-Mails vom Posteingangsserver vom E-Mail-Client heruntergeladen. Die Bearbeitung der eingegangenen E-Mails erfolgt anschließend auf dem lokalen Computer des Benutzers ohne Verbindung (offline) zum SMTP-Server.

Die Verbindung zwischen POP3-Server und E-Mail-Client erfolgt über TCP auf Port 110.

POP - Post Office Protocol

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, und deshalb manchmal auch als POP3 bezeichnet wird.

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.

POP-Befehle

Ist eine Verbindung zwischen POP-Server und E-Mail-Client zustande gekommen, werden zur weiteren Kommunikation Kommandos ausgetauscht. Die POP-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). Die folgenden Befehle stellen die Minimal-Implementierung des POP-Protokolls dar.

POP-Kommando	Beschreibung
USER	Dieser Befehl identifiziert die Mailbox.
PASS	Nach der Anmeldung muss der Benutzer mit einem Passwort authentifiziert werden.
QUIT	Mit diesem Befehl wird die Verbindung zum POP3-Server beendet. Alle gespeicherten Änderungen werden dann ausgeführt. Zum Beispiel der Befehl DELE.
STAT	Dieser Befehl fordert vom Server die Anzahl der gespeicherten E-Mails an. Außerdem wird die Größe der Mailbox in Oktetts zurückgeliefert.
LIST	Dieser Befehl fordert vom Server die Nummer und Größe (in Oktetts) aller E-Mails an. Es kann auch die Größe einzelner E-Mails abgefragt werden.
RETR	Dieser Befehl veranlasst den Server die angeforderte E-Mail zu liefern.
DELE	Dieser Befehl veranlasst den Server die angeforderte E-Mail zu löschen. Dieser wird aber erst nach dem Beenden der Verbindung wirklich ausgeführt.
NOOP	Dieser Befehl dient zur Aufrechterhaltung der Verbindung. Ein Timeout würde sonst die Verbindung trennen. Als Antwort liefert der Server +OK.
RSET	Dieser Befehl setzt die aktive Verbindung zurück. Noch nicht ausgeführte Änderungen werden verworfen. Zum Beispiel der Befehl DELE.

POP-Sitzungen

Eine POP-Verbindung umfasst mehrere Sitzungsstufen. Nach dem der POP-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.

Beispiel für den Ablauf einer POP-Verbindung

```
 1: > USER ******
 2: < +OK
 3: > PASS ******
 4: < +OK
 5: > CAPA
 6: < +OK
 7: < EXPIRE 240
 8: < LOGIN-DELAY 720
 9: < TOP
10: < UIDL
11: < PIPELINE
12: < USER
13: < .
14: > LIST
15: < +OK
16: < MsgID Größe in Byte
17: < .
18: > STAT
19: < +OK MsgID Größe in Byte
20: > RETR MsgID
21: < +OK message follows
22: < E-MAIL
23: < .
24: > DELE MsgID
25: < +OK message MsgID deleted
26: > RSET
27: < +OK
28: > QUIT
29: < +OK
```

Analyse der POP-Verbindung

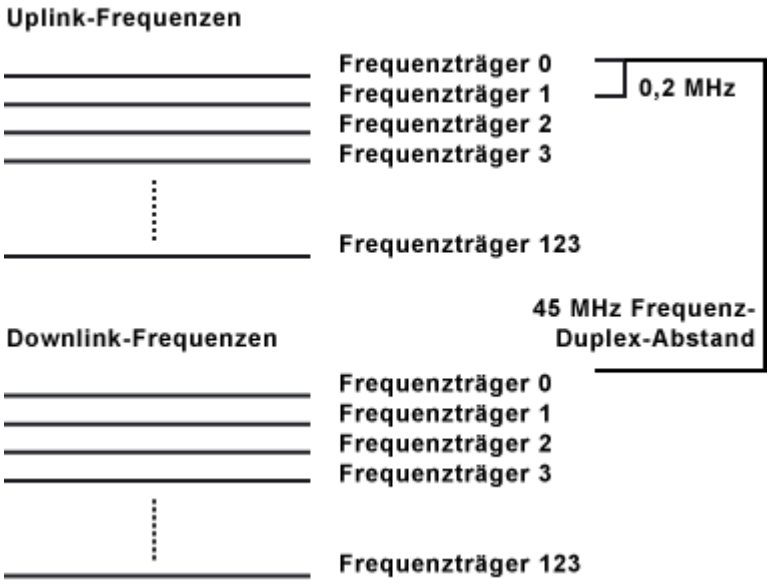
1. Nach dem Verbinungsaufbau meldet sich der E-Mail-Client mit dem Benutzername an. Meistens ist das die E-Mail-Adresse.
2. Der Server liefert eine positive Antwort und erwartet das Passwort.
3. Das Passwort wird vom E-Mail-Client in Klartext an den Server übermittelt.

4. Der Server liefert eine positive Antwort zurück. Der Benutzer ist nun korrekt angemeldet.
5. Der Client fragt die Fähigkeiten des POP-Servers ab.
6. Der Server liefert eine positive Antwort zurück.
7. Anschließend liefert der POP-Server hintereinander alle Fähigkeiten.
8.
9.
10.
11.
12.
13. Die Liste der Fähigkeiten wird vom Server mit einem . (Punkt) abgeschlossen.
14. Mit LIST fordert der E-Mail-Client eine Liste aller vorliegenden E-Mails an.
15. Der Server gibt eine positive Antwort zurück.
16. Anschließend liefert er einzeln alle E-Mails mit Message-ID und Größe in Byte zurück.
17. Die E-Mail-Liste wird vom Server mit einem . (Punkt) abgeschlossen.
18. Mit STAT fordert der E-Mail-Client eine Liste aller ungelesenen E-Mails an.
19. Der Server gibt eine positive Antwort und die E-Mail mit Message-ID und Größe in Byte zurück.
20. Mit RETR fordert der E-Mail-Client diese E-Mail an. Er kennzeichnet die Forderung mit der Message-ID.
21. Der Server gibt eine positive Antwort zurück.
22. Anschließend liefert er die ausgewählte E-Mail.
23. Der Server schließt mit einem Punkt das Ende der E-Mail ab.
24. Der E-Mail-Client löscht die E-Mail.
25. Der Server gibt eine positive Antwort zurück.
26. Der E-Mail-Client setzt mit RSET die Verbindung zurück. Damit wurde auch der vorhergehende Befehl DELE verworfen.
27. Der Server gibt eine positive Antwort zurück.
28. Mit QUIT beendet der E-Mail-Client die Verbindung zum Server
29. Der Server gibt eine positive Antwort zurück. Die Verbindung wird beendet.

54. GSM

GSM-Übertragungstechnik

Funkschnittstelle

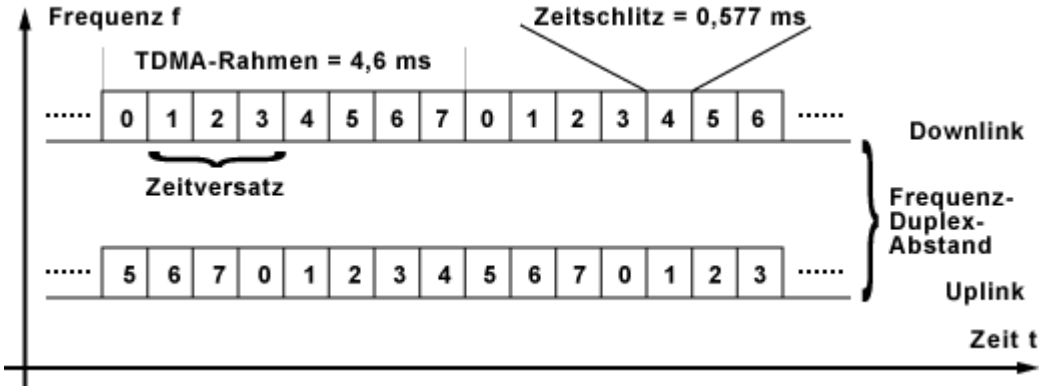


Die Funkschnittstelle von GSM wird in den technischen Unterlagen als U_m-Schnittstelle oder RadioPath bezeichnet. Innerhalb der Funkschnittstelle werden zwei Richtungen unterschieden. Einmal der Funkweg von Handy zur Basisstation. Man spricht von Uplink. Und die umgekehrte Richtung von Basisstation zum Handy. Man spricht von Downlink. Da für die Sprachverbindung zwei Kanäle benötigt werden (Up- und Downlink), werden die Kanalpaare mit dem Frequenzduplex-Verfahren (FDM, Frequency Division Multiplex) mit Zeitversatz gebildet. Jede Mobilfunkverbindung besteht aus einem Uplink- und Downlink-Kanal, die einen festen Frequenzabstand von 45 MHz hat. Dieser wird als Frequenz-Duplex-Abstand bezeichnet.

Modulationsverfahren

Im GSM-Standard ist als Phasenmodulation die GMSK-Modulation vorgesehen. Sie verwendet Trägerfrequenzen, die das GSM-Frequenzband aufteilt. Diese Unterteilung nennt man Frequenz-Multiplex (FDM, Frequency Division Multiplex). Der Uplink- und Downlink-Frequenzbereich unterteilen sich jeweils in 124 Trägerfrequenzen auch Funkkanäle genannt, die zueinander einen Abstand von 0,2 MHz oder 200 kHz haben. Jeder Frequenzträger ist wiederum in einem Zeitmultiplex-Verfahren (TDMA) in 8 Zeitschlitze (time slots) aufgeteilt. So lässt sich in jedem Frequenzträger 8 physikalische Verbindungen unterbringen. Diese 8 Verbindungen sind in einem TDMA-Rahmen mit einer Dauer von 4,615 ms verpackt. Jeder Zeitschlitz beträgt 0,577 ms, der sich immer wieder im folgenden TDMA-Rahmen wiederholt. Der Zeitintervall wird als Burst bezeichnet. Er beträgt 156,25 Bit. Wobei 1 Bit 3,692 µs entsprechen. Es gibt 5 Arten von Bursts. Der normale Burst ist für den eigentlichen Transport der Nutzdaten einer Verbindung gedacht. Er überträgt 114 Bit von echter Daten. Der Rest von 42,25 bit geht für den Verwaltung-Overhead

drauf.



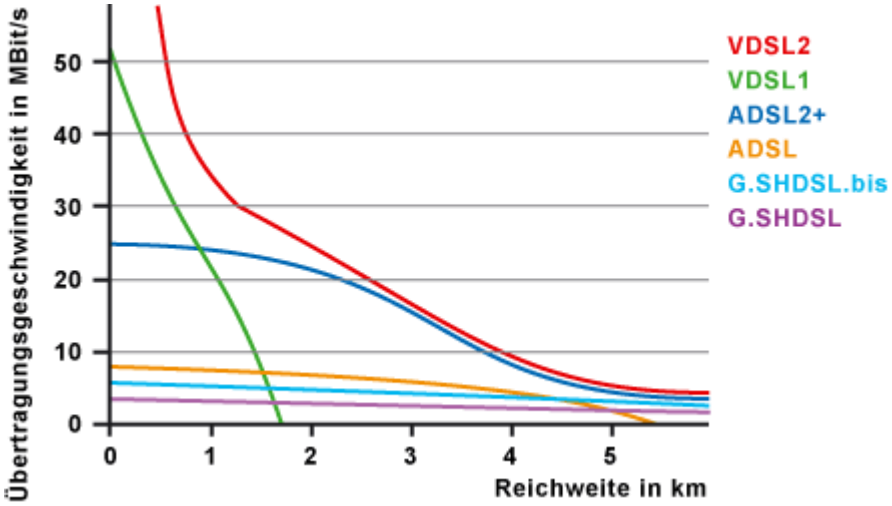
Die 0,577 ms bzw. 114 Bit reichen allerdings nicht aus, um Sprache zu übertragen. Deshalb stehen auch nicht 124 Träger mit je 8 Sprachverbindungen zu Verfügung. Statt dessen gibt es ein Verfahren, das aus 124 Trägerfrequenzen 11 echte Verbindungen macht. Auf das Zusammenspiel zwischen den physikalischen und logischen Kanälen wird hier nicht weiter eingegangen. Nur noch absolute GSM-Spezialisten, z. B. Systemhersteller kennen sich damit aus.
Verbleibt man bei 11 logischen Kanälen teilen diese sich in den Traffic Channel (TCH) und spezielle Steuerkanäle. Die Traffic Channel stellen die Bandbreite für ein Telefongespräche oder eine Datenübertragung zur Verfügung.

55. SDSL

SDSL - Symmetric Digital Subscriber Line

SDSL wurde entwickelt, um die gleiche Übertragungsgeschwindigkeit von HDSL auf nur einer Doppelader zu ermöglichen. Das ursprüngliche SDSL war eine propritäre Weiterentwicklung von HDSL.
Für die Abkürzung SDSL gibt es verschiedene Definitionen. Zum Beispiel "Symmetric Digital Subscriber Line" oder "Single Pair Digital Subscriber Line". Plausibel klingt "Symmetric Digital Subscriber Line", da SDSL ein symmetrisches Übertragungsverfahren ist. Doch auch HDSL ist ein symmetrisches Übertragungsverfahren. Viel eher passt "Single Pair DSL", weil sich SDSL dadurch kennzeichnet, dass es gegenüber HDSL nur eine Doppelader benötigt.
Heute steht die Bezeichnung SDSL für eine ganze Familie von symmetrischen Übertragungstechniken. Dazu zählen vor allem die Standards SHDSL, G.SHDSL und ESHDSL. Beide werden unter dem Begriff SDSL geführt. Ihnen liegt eine symmetrische Übertragungstechnik zu Grunde.

Übertragungsgeschwindigkeit



Die Übertragungsgeschwindigkeit von SDSL wird je nach Standard oder Produkt unterschiedlich angegeben. Einfach nur von 2 MBit/s zu sprechen ist nicht ganz richtig. G.SHDSL erreicht zum Beispiel eine Übertragungsgeschwindigkeit mit ganzzahligen Vielfachen von 64 kBit/s ab 192 kBit/s bis 2,304 MBit/s. Mit einer Kupferdoppelader mit 0,6 mm Durchmesser ist eine Reichweite von 6 km möglich. Bei zwei Doppeladern erreicht man eine Verdoppelung der Übertragungsrate. Oder die Reichweite ist kürzer, dann ist eine höhere Übertragungsgeschwindigkeit möglich. Prinzipiell gilt, je länger eine Leitung ist, desto eher eignet sie sich SDSL. SDSL hat eine Reichweite von 8 Kilometer. Bei ADSL ist schon bei 5 Kilometern definitiv Schluss. SDSL nutzt auch das untere Frequenzspektrum, das normalerweise von analogen Telefonanschlüsse oder ISDN belegt sind.

SHDSL - Symmetric High Data Rate DSL

Im Gegensatz zu propritären SDSL ist SHDSL im ITU-T G.991.2 standardisiert und somit Hersteller-unabhängig. Es ist die aktuelle Technik, um eine symmetrische Datenübertragung mit Bandbreiten zwischen 192 und 2320 kBit/s auf einer Kupferdoppelader zu ermöglichen. Die Reichweite ist bis zu 20% höher als bei den älteren HDSL- und SDSL-Verfahren.

G.SHDSL

G.SHDSL ist die Kurzbezeichnung für "Global Standard for Single-Pair of Highspeed DSL" und ist ebenfalls im ITU-T G.991.2 standardisiert. Es ist eine Erweiterung von SHDSL um größere Entfernungen zu überbrücken.
Dieser Standard ist nicht so leistungsfähig wie SHDSL. Dafür stellt er den kleinsten gemeinsamen Nenner dar, der in jedem Leitungsnetz auf der ganzen Welt funktioniert. Es geht auch darum, den Herstellern der Vermittlungsstellen und Modems die Möglichkeit zu geben eine möglichst große Anzahl an Kunden und Ihre Anforderungen bedienen zu können. Welcher Standard letztendlich in den nationalen Märkten zum Einsatz kommt, dass entscheiden die Netzbetreiber.
Durch den Standard G.991.2 (SHDSL und G.SHDSL) sind viele SDSL-Router zu anderen SDSL- und HDSL-Standards kompatibel.

Übertragungstechnik

SDSL baut auf den Leitungscode Trellis Coded Pulse Amplitude Modulation (TC-PAM). Hieran erkennt man auch die Verwandschaft zu ISDN. Der PAM-Leitungscode (16 PAM - 4B1Q) hat eine

geringe Durchlaufzeit, eine gute Reichweite und ist abwärtskompatibel zu 2B1Q, wie es bei HDSL eingesetzt wird. Eine maximale Verträglichkeit zu anderen Diensten, wird durch das Power-cut-back-Verfahren erreicht. Störungen für andere Dienste sind dadurch sehr gering.

Anwendungen

Schaut man sich die Preise von SDSL an, dann könnte einem schlecht werden. Ein SDSL-Anschluss kostet rund das fünf- bis fünfzehnfache eines ADSL-Anschlusses und bietet maximal 2 MBit/s in beide Richtungen an. SDSL ist nicht nur langsamer, sondern auch sehr teuer. Dafür ist die Reichweite höher als bei ADSL.
Der hohe Preis von SDSL rechtfertigt sich mit zusätzlichen Serviceleistungen. So zum Beispiel zugesicherte Reaktionszeiten im Störungsfall und feste IP-Adressen. Alles das bekommt man als ADSL-Kunde nicht. Somit kommen SDSL-Anschlüsse nur für Unternehmen in Frage.
Typische Anwendungsfälle sind:

- Netzwerkkopplung
- Vernetzung von TK-Anlagen
- Internet-Zugang für Firmen (die eine hohe Upload-Geschwindigkeit brauchen)
- Überbrücken großer Entfernungen

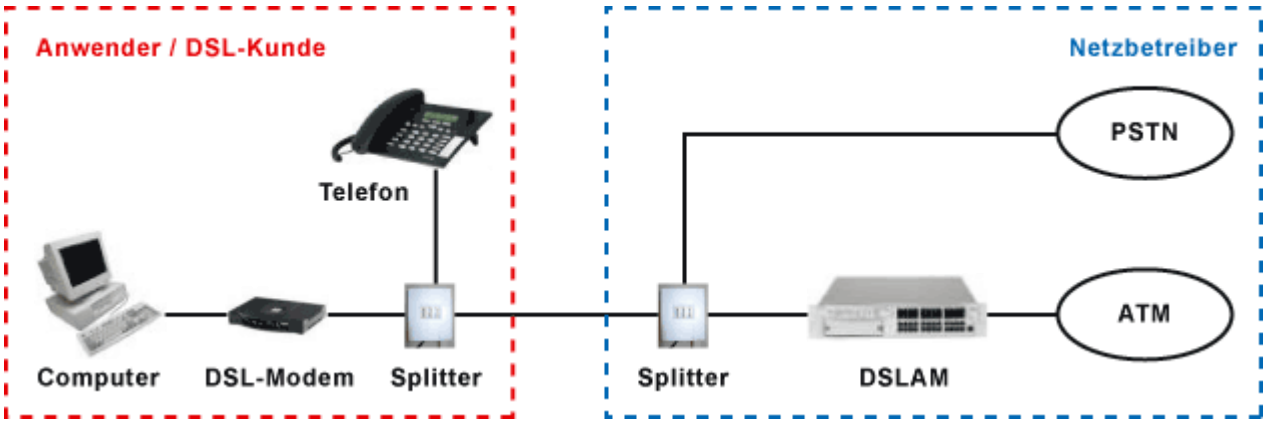
56. ADSL

ADSL - Asymmetric Digital Subscriber Line

Um die Ansprüche nach mehr Bandbreite für Datendienste zu erfüllen, wurde zwischen 1991 und 1995 die ADSL-Technik entwickelt. ADSL wurde von der ITU-T (International Telecommunications Union) in G.992.1 und vom ANSI (American National Standardisation Institute) in T1.413-1995 standardisiert.
Bei ADSL handelt es sich um ein Übertragungsverfahren für einen Breitband-Internet-Anschluss über eine normale Telefonleitung. Der wichtigste Vorteil von ADSL ist, dass die vorhandenen Kabelnetze für Telefonanschlüsse weiterverwendet werden können.

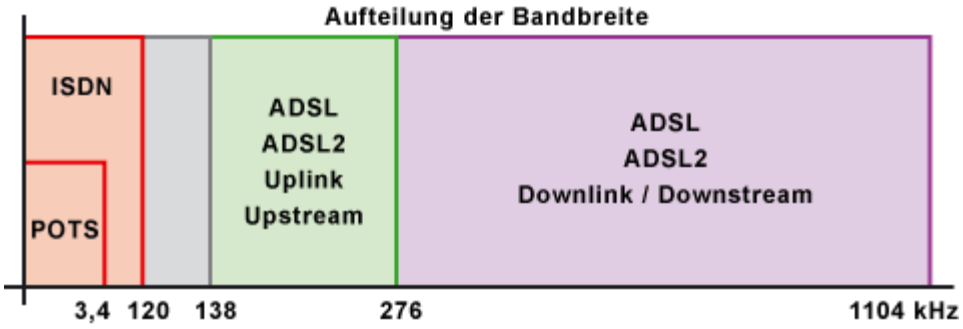
In Deutschland wird der Begriff "ADSL" nur unter Fachleuten verwendet. Die ADSL-Breitband-Anschlüsse werden in Deutschland als DSL-Anschlüsse bezeichnet. Je nach Netzbetreiber oder Provider haben sich unterschiedliche Markennamen herausgebildet. Bekannt sind T-DSL von der Deutschen Telekom, Q-DSL von QSC und diverse Bezeichnungen, wie DSL2+ oder DSL3+. Hinter den verschiedenen Bezeichnungen steckt im Prinzip immer die gleiche Technik.

Das zentrale Problem von ADSL ist die begrenzte Reichweite. Im Laufe der Zeit wurde die ADSL-Technik immer wieder erweitert und verbessert, so dass die Reichweite oder die Übertragungsrate immer wieder gesteigert werden konnte. Trotzdem ist eine vollständige Netzabdeckung in Deutschland bis heute praktisch nicht möglich.



Bei einer ADSL-Verbindung handelt es sich im Prinzip um zwei Modems an einer herkömmlichen Telefonleitung (Kupferdoppelader). Wobei das eine Modem beim Endanwender steht und das andere beim Netzbetreiber in der Vermittlungsstelle.
Das ADSL-Modem wird über eine Netzwerkkarte oder USB-Schnittstelle an einen Computer oder ein Netzwerk angeschlossen. So entsteht eine feste Anbindung. Das Anwählen, wie bei einer Telefonverbindung, entfällt. Stattdessen ist der Computer mit dem Internet wie mit einer "Standleitung" fest verbunden. Wobei die Standleitung als DSL-Anschluss bezeichnet wird.

Asymmetrische Übertragung

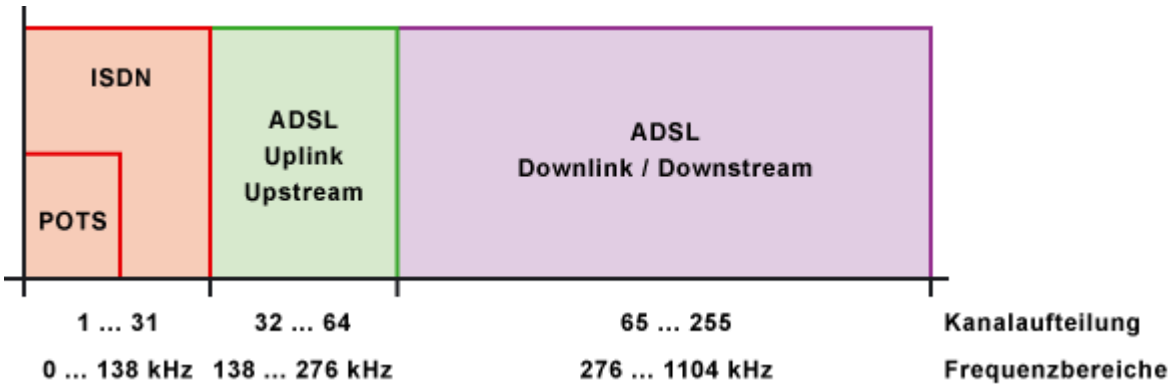


Das Grundprinzip von ADSL beruht auf einem asymmetrischen Übertragungsverfahren. Damit ist gemeint, dass der Übertragungsweg vom Netzbetreiber zum Kunden (Downlink) und der Übertragungsweg vom Kunden zum Netzbetreiber (Uplink) unterschiedliche Bandbreiten aufweisen.
Werden viele symmetrische Signale (z. B. bei HDSL und SDSL) gleichzeitig über mehrere parallel liegende Leitungen übertragen, so wird durch Signalkopplung die Übertragungsgeschwindigkeit und die Signalreichweite deutlich begrenzt. Bei der asymmetrischen Übertragung, wie bei ADSL, lässt sich die Signalkopplung deutlich reduzieren, womit sich höhere Datenraten erreichen lassen.
Das Verhältnis der Bandbreite von Downlink und Uplink ist der Anforderung eines typischen Internet-Nutzers nachempfunden. Er lädt typischerweise mehr Daten aus dem Internet herunter, als er ins Internet überträgt. Deshalb ist die Bandbreite beim Downlinks größer als beim Uplink.
Um Telefonie (POTS) und ADSL gleichzeitig nutzen zu können, sind sogenannte Splitter notwendig, die die genutzten Frequenzbereiche trennen bzw. zusammenführen und in das richtige Netzwerk einspeisen.
Die Trennung des nutzbaren Frequenzspektrums in drei Segmente erfolgt mit Frequency Division

Multiplexing (FDM). FDM erzeugt über dem schmalbandigen Frequenzbereich von POTS (mit Schutzabstand bis 25,875 kHz) bzw. ISDN (bis 138 kHz) den Upstream-Frequenzbereich, an den sich der breitbandige Downstream-Frequenzbereich anschließt. Eigentlich reicht ISDN nur bis 120 kHz. Doch zwischen 120 und 138 kHz ist ein Schutzabstand berücksichtigt, weil der Splitter, der die Frequenzbereiche voneinander trennen soll, passiv arbeitet und nicht exakt bei 138 kHz scharf genug trennen kann.

DMT - Discrete Multiton Modulation

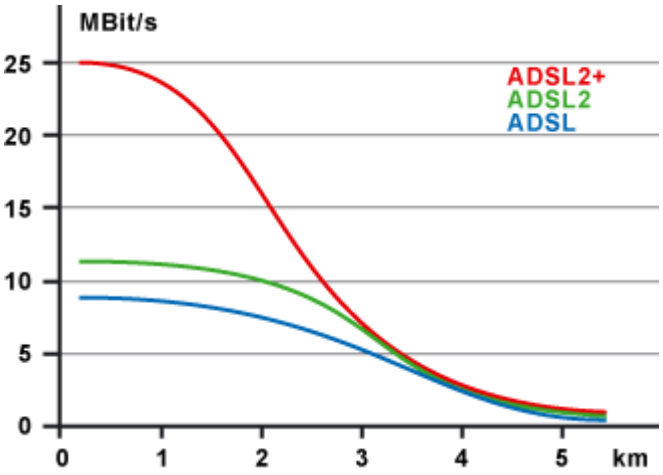
Der Frequenzbereich oberhalb von POTS oder ISDN muss mit einem Modulationsverfahren nutzbar gemacht werden, weil dieser Frequenzbereich verlustbehaftet ist. Das Modulationsverfahren DMT eignet sich am besten dafür. DMT wurde vom ANSI als ADSL-Standard (T1.413) festgelegt. Die Vorteile sind hohe Leistung und Flexibilität bei vertretbarem technischem Aufwand, sowie Stabilität auch bei Zustandsänderungen auf der Leitung.



Das Modulationsverfahren DMT ist ein Mehrträger-Bandpass-Übertragungsverfahren (Multi-Carrier). Für ADSL teilt DMT den Frequenzbereich bis 1,1 MHz in 256 einzelne Träger (Kanäle) mit je 4,3125 kHz Bandbreite auf. Die Träger 1 bis 31 sind in Deutschland für ISDN bzw. POTS (bis 0 bis 138 kHz) reserviert (ADSL Annex B). Die Träger 32 bis 64 werden für den Uplink (von 138 bis 276 kHz), die Träger 65 bis 256 für den Downlink (von 276 bis 1104 kHz) genutzt. In Uplink-Richtung stehen also 32 und in Downlink-Richtung 190 Kanäle zur Verfügung. Der Kanal 65, der sich zwischen Uplink und Downlink befindet, wird für den Pilotton verwendet (bei ADSL2 Kanal 96). Darüber können das ADSL-Modem (beim Kunden) und das DSLAM (in der Vermittlungsstelle) feststellen, ob sie miteinander verbunden sind.
Diese Form der Kanalaufteilung wird als Annex B bezeichnet und wird in Deutschland von allen Netzbetreibern für ADSL-Anschlüsse verwendet.
Je höher sich ein Kanal im Frequenzspektrum befindet, desto mehr machen sich die schlechten Übertragungseigenschaften der Kupferkabel bemerkbar. Je nach Störung, Dämpfung und Übersprechen wird ein Kanal mit einer unterschiedlichen Anzahl von Bits pro Übertragungsschritt genutzt. Die Anzahl der Bits reicht dabei von 2 bis zu 15 Bit. Je schlechter die Übertragungseigenschaften des Kanals, desto weniger Bit werden übertragen. DMT sorgt für die dynamische Optimierung jedes einzelnen Kanals, indem in jedem Kanal die Anzahl der zu übertragenen Bits zwischen 2 und 15 individuell angepasst werden. Kanäle, die mit Interferenzen und Rauschen behaftet sind, werden ausgeblendet oder nur mit einer niedrigen Datenrate genutzt. Auf einem ungestörten Kanal werden die Daten mit der maximal möglichen Datenrate übertragen.

Um eine möglichst hohe Datenrate aus einem Kanal herauszuholen wird die Quadratur Amplituden Modulation (QAM) verwendet.

Übertragungsgeschwindigkeit



Geht man von ADSL-over-ISDN (Annex B) mit 4 kHz Takt, 190 Kanälen und jeweils 15 Bit aus, dann wäre ein Downlink von 11,4 MBit/s möglich. Aber, nur bei einer sehr guten Leitungsqualität. Durch eine Fehlerkorrektur mit der Reed-Solomon-Codierung reduziert sich die Geschwindigkeit auf 8 MBit/s (Downlink) unter idealen Bedingungen. In Downlink-Richtung ist das fast so schnell wie ein Ethernet-Netzwerk (10Base-T). In Uplink-Richtung stehen effektiv nur 1 MBit/s zur Verfügung. Die Übertragungsgeschwindigkeit ist jedoch durch äußere Einflüsse und die Leitungslänge begrenzt. So haben ohmsche, kapazitive und induktive Effekte Einfluss auf die Dämpfung des Signals und somit auch auf die Reichweite dieses Übertragungsverfahrens. Für die Reichweite gilt, je höher die Frequenz, desto geringer ist die Reichweite.

Generell gilt, die Netzbetreiber definieren eine maximale Leitungslänge oder Leitungsqualität und bestimmen danach, welche Übertragungsgeschwindigkeit sie ihren Kunden anbieten können.

Synchronisation/Handshake

Bevor Daten übertragen werden können, müssen die Übertragungseigenschaften vom ADSL-Modem und DSLAM ermittelt werden. Dazu werden beim erstmaligen Verbindungsaufbau über ein Handshake-Verfahren die Übertragungseigenschaften ermittelt und die notwendigen Parameter über Leitungsbeschaffenheit, Datenrate und Latenzpfad (Fast/Interleaved) ausgetauscht. Die Parameter bleiben bis zum Verlust der Synchronisation, zum Beispiel durch Verbindungstrennung oder Stromausfall, bestehen. Kommt es nach der Synchronisation zu einer Störung oder Veränderung der Übertragungseigenschaften, muss die Synchronisation und somit der Handshake erneut durchgeführt werden.

Datenpriorisierung

Unterschiedliche Daten lassen sich über Permanent Virtual Connections (PVC) priorisieren. Dafür stehen die Parameter VPI (Virtual Path Identifier) und VCI (Virtual Channel Identifier) bereit.

Manche Provider nutzen diese Optionen, um zwei getrennte PPPoE-Verbindungen mit unterschiedlichen IP-Adressen aufzubauen. Das wird gemacht, um Sprach- und Datenverbindungen unterschiedlich priorisieren zu können.

Traffic Shaping

Um eine größere Downlink-Datenrate zu erreichen, hat ein ADSL-Anschluss eine kleinere Uplink-Datenrate. Bei normalem Surfverhalten merkt man von dem kleineren Uplink kaum etwas. Die Datenmenge, die heruntergeladen wird ist in der Regel größer, als die Datenmenge, die man verschickt. Allerdings sorgt ein vollgestopfter Uplink dafür, dass der Downlink gebremst wird. Mit Traffic Shaping wird dafür gesorgt, dass die ACK-Pakete zur Bestätigung empfangender Pakete bevorzugt durchgeleitet werden.
Traffic Shaping ist keine Besonderheit von ADSL, sondern ist ein Verfahren, dass auch andere Übertragungsverfahren kennen. Überall da, wo der Empfang von Datenpaketen bestätigt werden muss, kann Traffic Shaping sinnvoll eingesetzt werden.

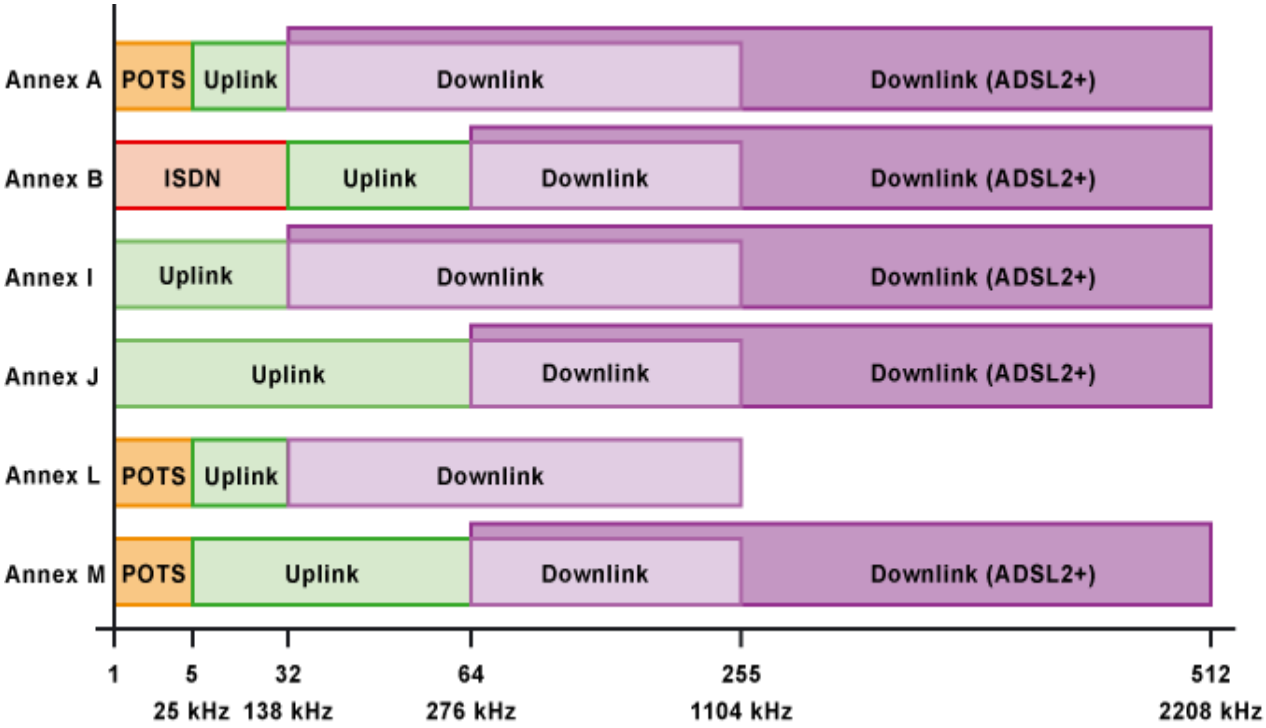
RAM - Rate Adaptive Mode

RAM ist ein Verfahren zur Bestimmung der ADSL-Bandbreite. Beim ratenadaptiven Betriebsmodus wird vor jedem Verbindungsaufbau die Leitungsqualität geprüft und die maximal mögliche Übertragungsrate ermittelt (Synchronisation). Der Kunde erhält keine Bandbreitengarantie, sondern nur die maximal mögliche Bandbreite, die an seinem Standort möglich ist.

Anwendungen

Einsetzbar ist ADSL bei allen Anwendungen, wo die Datenmenge zum Client größer ist als zum Server. Typische Einsatzgebiete wären demnach Internet- und Intranet-Zugänge. Durch eine flexible Bandbreitenverteilung im Up- und Downlink kann für jede Anwendung ein geeigneter Datendurchsatz gewählt werden.
ADSL hat wie jedes andere schnelle Übertragungsverfahren einen kleinen Haken. Hohe Übertragungsraten lassen sich nur dann erreichen, wenn die Infrastruktur hinter dem Endgerät, beim Netzbetreiber, dazu ausgelegt ist eine hohe Menge an Daten zu übertragen. Generell führen Überlastungen im Netz zur einer langsameren Übertragung der Daten. Dann kommt man auch nicht in den Genuss der schnellen Übertragungsrate von ADSL.
Für professionelle Anwendungen ist ADSL als Internet-Zugang weniger geeignet. Unternehmen, die eigene Datendienste anbieten wollen reicht die niedrige Uplink-Datenrate meist nicht aus. Hier muss man auf andere DSL-Varianten zurückgreifen.

ADSL-Varianten und ADSL-Standards



Mit der Zeit wurden einige ADSL-Varianten entwickelt. Im wesentlichen wurde dadurch versucht, die Technik an die Marktgegebenheiten und die weltweit unterschiedlichen Anforderungen anzupassen.
Bei den verschiedenen ADSL-Varianten geht es häufig darum, welchen Frequenzbereich ein ADSL-Anschluss nutzen darf. In Deutschland wurd der untere Frequenzbereich häufig von analoger Telefonie oder ISDN belegt. Das bedeutet, ein ADSL-Anschluss muss sich die Leitung mit einem Telefonanschluss teilen (Annex B). Entsprechend steht der unter Frequenzbereich bis 138 kHz für den ADSL-Anschluss nicht zur Verfügung. Doch gerade der untere Frequenzbereich hat eine geringere Streckendämpfung und ist für hochfrequente Signale für ADSL viel besser geeignet, als die höher liegenden Frequenzbereiche. Die unteren Frequenzbereiche haben auch eine größere Reichweite und sind gegenüber Störungen weniger empfindlich.
Da sich in Deutschland immer mehr entbündelte ADSL-Anschlüsse durchsetzen kann auch der untere Frequenzbereich für den ADSL-Anschluss genutzt werden (Annex J).

Standard	Bezeichnung	Annex	Downstream	Upstream
G.992.1	**ADSL**	Annex A/B	12 MBit/s	1,3 MBit/s
G.992.2		Annex A/B	4 MBit/s	0,5 MBit/s
		Annex I/J		
G.992.3	**ADSL2**	Annex A/B	12 MBit/s	1,0 MBit/s
		Annex L	5 MBit/s	0,8 MBit/s
		Annex M	12 MBit/s	2,5 MBit/s
G.992.4		Annex A/B	12 MBit/s	1,0 MBit/s

G.992.5	**ADSL2+**	Annex A/B	25 MBit/s	1,0 MBit/s
		Annex L	25 MBit/s	1,0 MBit/s
		Annex M	25 MBit/s	3,5 MBit/s

Annex A (ADSL-over-POTS) und Annex B (ADSL-over-ISDN)

Annex A ist eine ADSL-Variante, die den Frequenzbereich unterhalb von 25 kHz für analoge Telefone (POTS) frei hält.
Annex B ist eine ADSL-Variante, die den Frequenzbereich unterhalb von 138 kHz für den ISDN-Basisanschluss reserviert. Alle ADSL-Netzbetreiber in Deutschland verwenden Annex B. ADSL-over-ISDN (Annex B) nutzt 4,3125 kHz breite Subträger mit einer Symbolrate von 4 kBaud.
ADSL-over-POTS (Annex A) und ADSL-over-ISDN (Annex B) unterscheiden sich nur in der Signalisierung und der verwendeten Frequenzbereiche. In Deutschland kommt generell nur ADSL-over-ISDN (Annex B) zum Einsatz. Das vereinfacht den Wechsel zwischen Analog-Anschluss und ISDN-Anschluss, sowie beim Umzug von einem DSL-Anbieter zu einem anderen.

Annex C (ADSL-over-TCM-ISDN)

In Japan gibt es ein spezielles ISDN, das TCM-ISDN (Time-Code-Multiplexed).

Annex I und Annex J

Annex I und J sind Ergänzungen zur ADSL-Spezifikation G.992. Der Unterschied zwischen I und J liegt in der unterschiedlichen Größe des Uplinks. Der ist bei Annex J größer.
Annex I und Annex J haben kein Basisband. Demzufolge haben sie keinen Frequenzbereich, der für Analog- oder ISDN-Anschlüsse genutzt werden kann. Die Anschlussleitung und somit der komplette Frequenzbereich steht für ADSL zur Verfügung.
Bei Annex J ist der Uplink bis 260 kHz nutzbar. Der Schutzabstand bis zum Downlink reicht bis 276 kHz. Die Handshake-Töne liegen wie bei Annex B bei 159,5625 kHz, 194,0625 kHz und 228,5625 kHz.
DSL-Anschlüsse nach Annex J bezeichnet man in Deutschland auch als "entbündelter Zugang" oder "naked DSL". Diese DSL-Anschlüsse brauchen keinen Splitter und haben eine höhere Reichweite, die mit einer schnelleren Übertragungsgeschwindigkeit verbunden ist.

Annex L / RE-ADSL2 - Reach Enhanced ADSL2

Annex L ist eine Erweiterung von Annex A. Es wird durch gezieltes Ausblenden von benachbarten Trägern eine Maximierung der Reichweite bei Verringerung der möglichen Bitrate erreicht. Annex L wird auch als Reach Extended Mode bezeichnet (RE-ADSL/RE-ADSL2).

Annex M

Annex M ist eine Erweiterung von Annex A. Der Uplink ist zu Lasten des Downlinks vergrößert. Annex M wurde in Deutschland nicht eingeführt, weil die Handshake-Töne die ISDN-Anschlüsse im gleichen Kabelbündel stören. Aus diesem Grund wird in Deutschland Annex J verwendet, wenn

die Leitung vollständig für den DSL-Anschluss genutzt wird.
Die Handshake-Töne liegen bei Annex M bei 38,8125 kHz, 73,8125 kHz und 107,8125 kHz.

57. DSL Splitter

Der Splitter hat die Aufgabe, das auf der Telefonleitung ankommende Signal anhand ihrer Frequenz aufzutrennen und an zwei verschiedenen Ausgängen herauszuführen. Der Splitter entspricht einer Frequenzweiche mit einem integrierten Hoch- und Tiefpassfilter. So wird sicher gestellt, dass die Endgeräte nur das Signal bekommen dass für sie gedacht ist und nicht von dem anderen Signal gestört werden können.
Beim Betrieb eines Telefons an einem Telefonanschluss mit DSL, aber ohne Splitter, hört man ein Rauschen. In guten Telefonen ist eine Frequenz-Weiche enthalten, so dass es in der Regel zu keinen Störungen des Telefons kommt. Jedoch bedeuten Telefonsignale für das DSL-Modem eine Erhöhung der Fehlerrate und eine Reduzierung der Datenrate. Auf keinen Fall sollte man Telefone und DSL-Modems einfach so parallel zueinander anschließen. Dabei kommt es zu Impedanzverschiebungen und Kurzschlüssen.

Ein Splitter hat durchaus Einfluss auf die Übertragungsgeschwindigkeit des DSL-Anschlusses. Prinzipiell funktioniert ein alter Splitter auch an neuen ADSL2- oder ADSL2+-Anschlüssen. Doch ein Splitter aus der Anfangszeit von DSL kann ein ADSL2+-Modem ausbremsen. Mit einem neuen Splitter könnte die Übertragungsgeschwindigkeit höher sein.
Ein Splitter besteht aus Spulen und Kondensatoren, die als Tiefpass- und Hochpassfilter zusammengeschaltet sind. Spulen und Kondensatoren sind allerdings alles andere als ideale Filter. Es gibt Qualitätsunterschiede, die auf die Datenrate Einfluss nehmen können. Kondensatoren mit geringer Güte haben eine höhere amplitudenabhängige Kapazität und verzerren und verschmieren das Signal stärker als Kondensatoren mit hoher Qualität. Und auch Spulen können Verzerrungen verursachen.
Spulen und Kondensatoren leiden unter Exemplarstreuung was dazu führt, dass der Filter ungenau ist. Von der Qualität und Genauigkeit der einzelnen Bauteile hängt die Qualität des Filters ab. Um Probleme auszuschließen, befindet sich zwischen der Telefon-Frequenz und dem ADSL-genutzten Frequenzspektrum ein Schutzabstand von ca. 18 kHz.

58. Masquerading

Beim Masqerading gibt es einen Rechner, der einen Zugang zum Internet hat und eine gültige IP-Nummer für das Internet besitzt. Ob dies eine dauerhafte Nummer ist oder eine dynamisch vom Provider zugeteilte, ist belanglos. Der Masqeradingrechner nimmt nun alle Pakete in Richtung Internet in Empfang, steckt sie in die Hülle seiner eigenen Pakete mit gültiger Absendernummer und sendet sie an das Internet. Die zurückkehrenden Pakete packt er wieder aus und sendet es an den Auftraggeber.

Ein Netz braucht nur ein IP-Nummer
Dies vermindert bei kleinen Firmen die Kosten für einen Komplettzugang zum Internet, da mehrere gültige Internetnummern zu haben inzwischen Luxus ist. Ferner bleiben die Rechner des lokalen Netzes für das Internet unerreichbar. Da auf diese Weise die Anzahl benötigter Adressen gering bleibt, sorgt diese Technik dafür, dass ein Wachstum des Internets möglich ist, auch wenn nicht sofort auf IPv6 umgestiegen wird.

Masquerading und Firewall

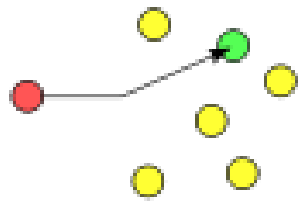
Man kann sich leicht vorstellen, dass das Umsetzen der IP-Nummern am besten an der Stelle geschieht, wo sowieso jedes Paket betrachtet und überprüft wird. Darum wird das Masquerading normalerweise durch die Firewallsoftware mit erledigt. Im folgenden eine Regel unter ipchains, die die Pakete des lokalen Netzwerkes 192.168.109.0 weiterleiten.

```
ipchains -A forward -i ppp0 -s 192.168.109.0/24 \
                    -d ! 192.168.109.0/24 -j MASQ
```

Mit ipfwadm lauten die Befehle:[1])

```
ipfwadm -F -p deny
ipfwadm -F -a m -S 192.168.109.0 -D 0.0.0.0/0
```

59. Unicast



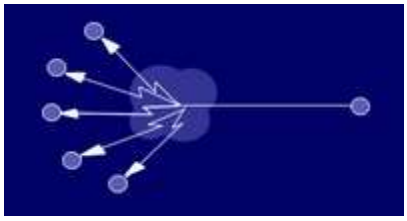
In der Telekommunikation bezeichnet **Unicast** die Übertragung von Nachrichten zwischen einem Sender und einem einzigen Empfänger. Die dazu in der Vermittlungsschicht (OSI-Modell) verwendete Adresse, die das Ziel eindeutig identifiziert, wird als Unicast-Adresse bezeichnet. Der Begriff ist vor allem bei Computernetzwerken gebräuchlich, findet jedoch ebenso allgemeine Verwendung. So kann im übertragenem Sinne, das Senden eines Briefes an einen Empfänger als Unicast bezeichnet werden. Bei einer Direktverbindung zwischen zwei Netzwerkteilnehmern spricht man hingegen von Punkt-zu-Punkt-Verbindungen.

Unicast-Nachrichten werden für alle Netzwerk-Prozesse verwendet, vor allem bei denen vertrauliche oder einzigartige Ressourcen angefordert werden. Bestimmte Internet-Anwendungen nutzen Unicast-Verbindungen wie beispielsweise Streaming Media in vielen Varianten.

Bei IPv6 werden bestimmte Bereiche für Unicast-Adressen reserviert, welche durch die ICANN spezifiziert sind.

60. Broadcast

Eine Broadcast-Übertragung entspricht einem Rundruf, es ist die gleichzeitige Übertragung von einem Punkt aus zu allen Teilnehmern. Klassische Broadcast-Anwendungen sind Rundfunk und Fernsehen. Bei Broadcast werden die Informationen immer nur vom Sender zu den Empfängern und nicht in gegengesetzter Richtung übertragen. Außerdem kann der Empfänger nur aus den Informationen auswählen, die ihm angeboten werden. Zwischen Sender und Empfänger besteht keine Interaktivität, bzw. nur über spezielle Rückkanäle.



Broadcast-Prinzip: einer an alle

Beim Broadcast unterscheidet man daher zwischen Enhanced Broadcast und Interactive Broadcast. Enhanced Broadcast hat keinen Rückkanal und kann interaktiv nur mit lokalen Diensten wie beispielsweise Electronic Program Guide (EPG) arbeiten. Dagegen hat Interactive Broadcast einen Rückkanal, der über das Internet oder das Telefonnetz geschaltet wird. Beim Interactive Broadcast besteht somit eine Nutzerinteraktion beispielsweise für das Televoting.

Um in einem lokalen Netz bestimmte Klassen von Empfängern oder alle angeschlossenen Stationen gleichzeitig anzusprechen, bestehen die Möglichkeiten des Multicast oder des Broadcast.

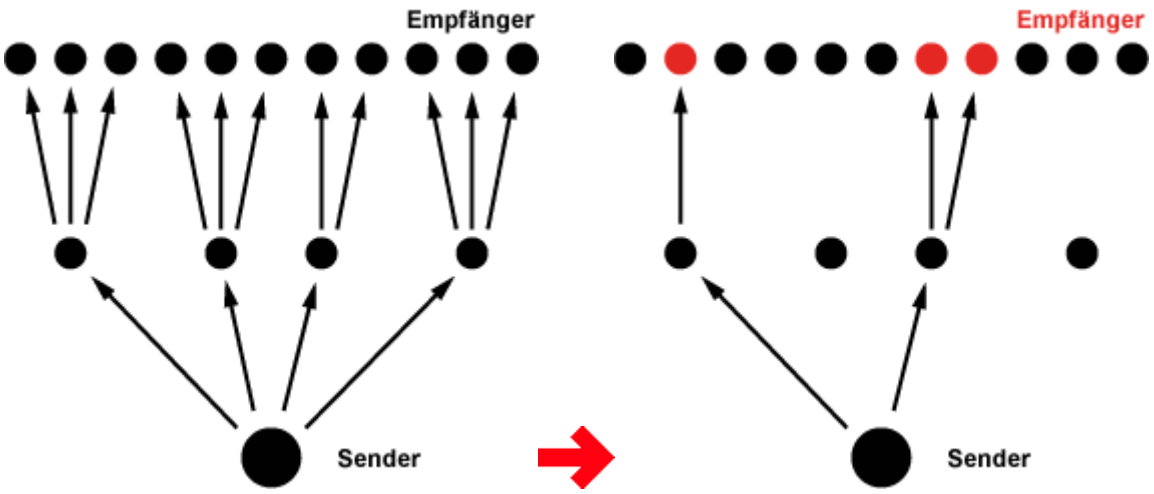
In lokalen Netzen ist ein Broadcast eine Nachricht, die an alle Geräte in allen Netzen verschickt wird. Sie wird von jedem Router an alle angeschlossenen Netzwerke weitergeleitet. Sollen alle Endgeräte eines bestimmten Netzes angesprochen werden, spricht man von Multicast oder Netzwerk-Broadcast, im Falle von IP-Netzen von IP-Multicast.

IP-Broadcasts können durch die IP-Adressen direkt ausgeführt werden. So ginge beispielsweise die Klasse-A-Adresse 1.0.0.0 an alle Knoten im Netzwerk 1 und die Klasse-C-Adresse 192.7.4.0 an alle Knoten im Netzwerk 192.7.4.

61. Multicast

Multicast / Multicasting

Multicasting ist eine Methode, um einen IP-Datenstrom an viele Teilnehmer gleichzeitig auszuliefern. Es entspricht dem Broadcasting bzw. Rundfunkverfahren, bei dem es einen Sender und viele Empfänger gibt. Ein typischer Anwendungsfall wäre das Streaming von TV- oder Video-Daten. Bei IP (Internet Protocol) ist das ein Problem, weil der Sender für jeden Empfänger eigene Datenpakete verschicken müsste, was bei vielen Empfängern zu einer Überlastung führen könnte.



Beim Multicasting wird nicht jeder Empfänger mit einem eigenen Datenstrom beliefert. Der Datenstrom wird vom Absender im Prinzip nur einmal gesendet. Er vervielfältigt sich nur in den Verzweigungspunkten, an dem die Multicast-Empfänger liegen. Auf diese Weise wird die parallele Übertragung gleicher Pakete vermieden. Beim Sender nimmt die Last also nicht mit der Zahl der Empfänger zu. Die verfügbare Routing- und Transportkapazität wird besser genutzt.

In der Praxis ist es mit der Umsetzung von Multicasting schwierig. Multicasting setzt auf dem gesamten Übertragungsweg eine Multicast-fähige Infrastruktur voraus. Das Multicast-Verfahren muss in allen Routern aktiviert sein. Insbesondere dort wo es vom Kernnetz ins Zugangsnetz geht. Doch die Zugangsnetzbetreiber sind wenig daran interessiert. Ihnen bringt es nichts, wenn Multicasting aktiviert ist. Deshalb ist Multicasting in der Regel nur in privat kontrollierten Subnetzen zu finden.

Multicasting und Broadcasting bei IPv6

Broadcasting gibt es bei IPv6 nicht mehr. Hier wird ausschließlich auf Multicast gesetzt. Die Nutzung von Multicasts, statt Broadcasts, reduziert die Netzlast erheblich. Multicasts lassen sich mit IPv6 über Subnetzgrenzen hinweg routen. Außerdem stehen endlich genug Adressen zur Verfügung.
Mit Multicasts werden Anwendungen von der Netztopologie unabhängig. Und die Netzlast an den angeschlossenen Nodes wird auch reduziert.

62. IGMP

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)

<table>
<tr><td>Version</td><td>IHL</td><td>0000</td><td colspan="2">Paketlänge</td></tr>
<tr><td colspan="3">Kennung</td><td>Flags</td><td>Fragment-Offset</td></tr>
<tr><td>0001</td><td colspan="2">0002</td><td colspan="2">Header-Checksumme</td></tr>
<tr><td colspan="5">Quell-IP-Adresse</td></tr>
<tr><td colspan="5">Ziel-IP-Adresse</td></tr>
<tr><td>10010100</td><td>00000100</td><td colspan="3">0</td></tr>
<tr><td colspan="5">Weitere Optionen/Füllbits</td></tr>
<tr><td>IGMP-Typ</td><td>max.Antwortzeit</td><td colspan="3">IGMP-Check-Summe</td></tr>
<tr><td colspan="5">Gruppenadresse</td></tr>
</table>

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 bei IP nur mit IGMP möglich.

63. TTL

Time-to-Live-Feld

Das TTL-Feld (Time to Live) ist ein 1 Byte langes Zählerfeld im IP-Header zur Begrenzung der Lebensdauer von Datagrammen. Der Zähler befindet sich im IP-Header und wird von jedem Netzknoten um den Wert "1" dekrementiert, beginnend bei 255 (8 Bit).

Hat das IP-Paket 255 Netzknoten durchlaufen, ist der Wert "0" erreicht und das Datagramm wird verworfen. Dies wird gemacht, um das Netz nicht unnötig mit im Netz kreisenden Datagrammen zu belasten. Mit der Dekrementierung wird auch die Prüfsumme geändert.

TTL-Feld im IP-Header

Da das Datagramm auch für längere Zeit in einem Router verweilen kann, wird der TTL-Wert sowohl durch den Hop, als auch durch die Zeit verringert. Als Zeiteinheit ist die Sekunde definiert. Befindet sich das Datagramm beispielsweise für 5 Sekunden in einem Netzknoten, wird der TTL-Wert um 5 reduziert. Die relative Lebensdauer eines Datagramms beträgt somit maximal 255 Sekunden oder sie entspricht der Zeit, die das Datagramm für das Durchlaufen von 255 Routern benötigt.

64. ARP

ARP - Address Resolution Protocol

Das Address Resolution Protocol (ARP) arbeitet auf der Schicht 2, der Sicherungsschicht, des OSI-Schichtenmodells und setzt IP-Adressen in Hardware- und MAC-Adressen um. Alle Netzwerktypen und -topologien benutzen Hardware-Adressen um die Datenpakete zu adressieren. Damit ein IP-Paket innerhalb eines lokalen Netzwerks zugestellt werden kann, muss die Hardware-Adresse des Ziels bekannt sein.
Jede 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 sendet eine Station einen ARP-Request mit der MAC-Adresse "FF-FF-FF-FF-FF-FF". Das ist ein MAC-Broadcast an alle Systeme im Netzwerk. Diese Meldung wird von jedem Netzwerkinterface entgegengenommen und ausgewertet. Das Ethernet-Frame enthält die IP-Adresse der gesuchten Station. Fühlt sich eine Station mit dieser IP-Adresse angesprochen, schickt sie ein ARP-Reply an den Sender zurück. Die gemeldete MAC-Adresse wird dann im lokalen ARP-Cache des Senders gespeichert. Dieser Cache dient zur schnelleren ARP-Adressauflösung. Eine Variante von ARP ist das RARP-Protokoll. Das wird verwendet, wenn die MAC-Adresse bekannt ist und die IP-Adresse gesucht wird.

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

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

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.


C:\>arp -a

Schnittstelle: 192.168.168.11 --- 0x2
  Internetadresse      Physikal. Adresse     Typ
  192.168.168.8        00-30-ab-0e-d3-6a     dynamisch
```

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.

65. MAC-Adresse

Jede Station in einem Ethernet-Netzwerk hat eine eigene Adresse. Diese Adresse soll die 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.

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

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).

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)

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

MAC-Multicast- und MAC-Broadcast-Adressen

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

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

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

66. Verzeichnisdienste allgemein Windows AD

Microsoft Active Directory

Active Directory (AD) ist der Verzeichnisdienst für Windows 2000 Server und Windows 2003 Server von Microsoft. Ab Windows Server 2008 wird es als Active Directory Domain Services (ADDS) bezeichnet.

Mit Active Directory kann man ein Netzwerk der Struktur einer Organisation oder seiner räumlichen Verteilung nachbilden. Dazu speichert und verwaltet Active Directory Informationen über Netzwerk-Objekte und -Ressourcen. Ein oder mehrere Administratoren können Verzeichnisdaten und Verzeichnisstruktur des gesamten Netzwerks verwalten und Netzwerk-Benutzern die benötigten Netzwerk-Ressourcen freischalten oder sperren. Als Netzwerk-Ressourcen zählen Zugriffsberechtigungen, Nutzungsrechte für Anwendungen, Speicherplatz, Netzwerkdienste und Netzwerk-Peripherie, wie z. B. Drucker.

Vorteile von Active Directory

- Informationssicherheit
- Richtlinienbasierte Verwaltung
- Erweiterungsfähigkeit
- Skalierbarkeit
- Replikation von Informationen
- DNS-Integration
- Zusammenarbeit mit anderen Verzeichnisdiensten

Das Active Directory ist ein objektorientierte Datenbank bestehend aus Klassen, Schemata und Objekten, die hierarchisch angeordnet sind.

Domäne

Um die Organisationsstruktur in einem Unternehmen nachbilden zu können, werden in Active Directory Domänen eingesetzt. Eine Domäne ist immer eine Organisationseinheit. Ihr unterliegen Sicherheitsrichtlinien und -einstellungen, die nicht auf eine andere Domäne übertragen werden kann. In jeder Domäne werden nur Informationen der betreffenden Domäne gespeichert.
Eine Domäne hat einen eindeutigen Namen und bietet Zugriff auf die Benutzer- und Gruppenkonten, die vom Domänenadministrator verwaltet werden.

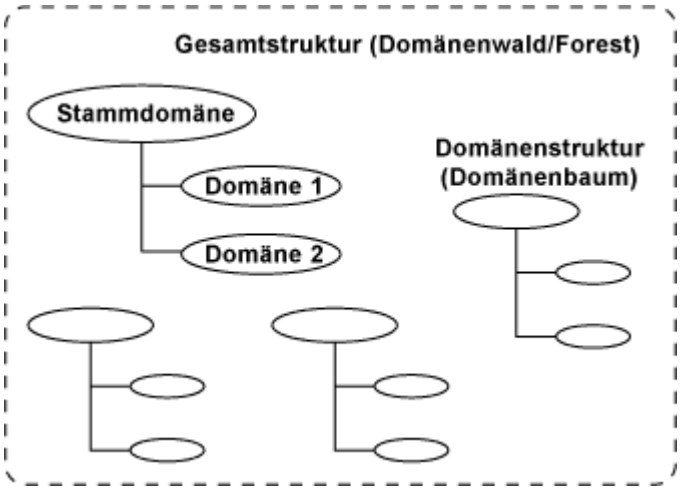
Domänenstruktur

- das-elko.de (Stammdomäne)
  - technik.das-elko.de (untergeordnete Domäne von das-elko.de)
  - verwaltung.das-elko.de (untergeordnete Domäne von das-elko.de)
    - finanzen.verwaltung.das-elko.de (untergeordnete Domäne von verwaltung.das-elko.de)
    - personal.verwaltung.das-elko.de (untergeordnete Domäne von verwaltung.das-elko.de)

Die Domänenstruktur von Active Directory basiert auf den Namenskonventionen des DNS. Jede Domäne wird durch einen DNS-Namen identifiziert. Eine Domänenstruktur wird als Domänenbaum bezeichnet. Die erste Domäne einer Domänenstruktur wird als Stammdomäne bezeichnet. Alle weiteren Domänen in derselben Domänenstruktur sind untergeordnete Domänen. Alle Domänen in derselben Domänenstruktur bilden einen fortlaufenden Namen. Das bedeutet, dass eine untergeordnete Domäne immer auch den Namen der übergeordneten Domäne enthält. In der Liste oben ist verwaltung.das-elko.de eine untergeordnete Domäne von das-elko.de und finanzen.verwaltung.das-elko.de eine untergeordnete Domäne von verwaltung.das-elko.de.
Die physische Struktur (Architektur) eines Netzwerkes ist an die Standortaufteilung gebunden. Die Domänenstruktur ist in der Regel (nicht zwingend) an die logische Struktur des Unternehmens gebunden. Die logische Struktur und physische Struktur sind voneinander unabhängig:

- An einem Standort können mehrere Domänen sein.
- In einer Domäne können mehrere Standorte sein.
- Zwischen Standort und Namensgebung besteht kein Zusammenhang.

Gesamtstruktur



Die Gesamtstruktur besteht aus mehreren Domänenstrukturen, den Domänenbäumen. Die Namensgebung zwischen den Domänenstrukturen haben keinen zusammenhängenden Namensraum. Untergeordnete Domänen-Bezeichnungen können in allen Domänenstrukturen vorkommen, haben aber nichts miteinander zu tun.
Die Gesamtstruktur wird auch als Domänenwald bezeichnet (mehrere Domänenbäume).

Wichtig: Die erste eingerichtete Domäne in einer Gesamtstruktur wird als Stammdomäne der Gesamtstruktur bezeichnet. Diese Domäne wird bei der Installation des ersten Domänencontrollers erstellt. Durch die Installation mehrerer Domänencontroller für eine Domäne kann die Fehlertoleranz und eine hohe Verfügbarkeit des Verzeichnisdienstes gewährleistet werden.

Benutzer- und Computerkonten

Benutzer- und Computerkonten im Active Directory sind einer physisch vorhandenen Person oder einem Computer zugeordnet. Diese Konten werden als Sicherheitsprincipals bezeichnet, denen eine Sicherheitskennung zugewiesen ist. Objekte mit Sicherheitskennung können sich am Netzwerk anmelden und auf Domänenressourcen zugreifen. Benutzer- und Computerkonten haben folgende Aufgaben:

- Authentifizierung des Benutzers oder des Computers
- Zugriffskontrolle auf Domänenressourcen
- Verwaltung anderer Sicherheitsprincipals
- Überwachungsaufgaben

67. Speichermedien klassifizieren

Physikalisches Speichermedium	Speichermedium
Mechanisch	Papier, Karton: Lochstreifen, Lochkarte
Elektromechanisch	Relais
Elektrisch	Memristor
Magnetisch	Ferrite: Kernspeicher, Blasenspeicher, Oxid-Kristalle, Eisenoxid, Chromdioxid: Magnetband, Magnetkarte, Magnetplatte, Diskette, Festplatte
Elektronisch	Halbleiter: RAM, ROM in allen Versionen, Flashspeicher, Speicherkarte
Optisch	Laser-basiert: CD, DVD, HD-DVD, Blu-Ray-Disc, Bildplatte, Holografisch: HVD-Disc

68. IDS

Intrusion Detection System (IDS) sind autarke Systeme, die Eindringlinge erkennen und Attacken auf IT-Systeme und Netze vermeiden. Diese IDS-Überwachungssysteme sollten nicht bekannt sein, keine Dienste anbieten, Angriffe protokollieren, Eindringlinge erkennen und nach Möglichkeit Gegenmaßnahmen einleiten. Alles was im Netzwerk anormal ist, sollte von dem IDS-System erkannt und protokolliert werden.

Dazu benutzen IDS-Verfahren Sensoren resp. Sniffer, die anormalen Datenverkehr aufspüren und mit vorgegebenen Mustern vergleichen. Dabei unterscheidet man zwischen dem Erkennen von Missbrauch, dem Misuse Detection, und dem Aufspüren von Anomalien, dem Anomaly Detection.

Das Misuse Detection basiert auf dem Vergleich von Mustern oder Signaturen. Dazu werden die erfassten Muster mit anderen Mustern aus einer Datenbank verglichen, die vorwiegend von den Eindringlingen benutzt werden. Bei dieser Methode, dem sogenannten Pattern Matching, werden nur bereits bekannte Angriffsmuster erkannt. Neue Angriffe, von denen noch kein Muster vorliegt, bleiben unerkannt.

Beim Anomaly Detection wird hingegen jedes Verhaltensmuster, das sich außerhalb des normalen Datenverkehrs bewegt, als Angriff gewertet. Dadurch werden auch Abweichungen von bisherigen Angriffen erkannt. Eine Pflege der Angriffsmuster in einer Datenbank entfällt. Allerdings muss beim Anomaly Detection definiert werden, welches Muster zum normalen Datenverkehr gehört, wodurch sich die Schwelle für Fehlalarme erhöhen kann.

Die beiden Verfahren verdeutlichen die Entwicklung vom IDS-System hin zu Intrusion Prevention Systems (IPS), die bestimmte Datenpakete erst gar nicht passieren lassen.

Für die IDS-Technologie gibt es auch netzwerkbasierte Lösungen, Network-based Intrusion Detection (NIDS) und hostbasierte, Host-based Intrusion Detection (HIDS).

69. SIP Verbindungsaufbau

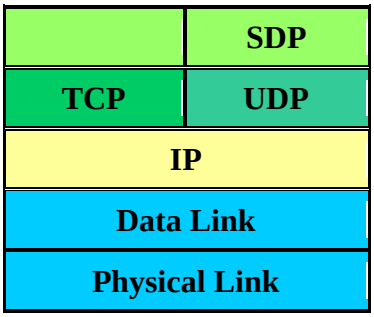
SIP - Session Initiation Protocol

Das SIP wurde entwickelt, um Teilnehmer zu Mehrpunktkonferenzen zusammen zu schalten. Schnell erkannte man die Eignung für die Punkt-zu-Punkt-Telefonie (Voice over IP). Genauso wie H.323 eignet sich SIP für den Aufbau, Betrieb und Abbau von Sprach- und Video-Verbindungen. Sowohl Punkt-zu-Punkt- als auch Multicast-Verbindungen lassen damit steuern.
SIP wurde 1996 von einer Arbeitsgruppe der IETF (Internet Engineering Task Force) entwickelt, 1999 veröffentlicht und genormt. Obwohl H.323 zuerst da war, war das Interesse an SIP gleich von Anfang an sehr groß. Schon 1999 war es beliebter als H.323.

SIP hat einem starken Bezug zu anderen Internet-Protokollen. Die Kommunikation ist von den TK-üblichen Mechanismen entlastet und auf das wesentliche beschränkt. Aufgrund seiner Einfachheit ist SIP leichter zu verstehen und der Aufwand für die Implementierung geringer. Die Vermittlung der Datenpakete folgt der Logik von IP-Anwendungen. SIP ist stark am HTTP (Hypertext Transfer Protocol) angelehnt. Somit lässt sich die SIP-Telefonie in Browser-Umgebungen, Webservices, Anwendungen und Geräte leicht integrieren.
Die Einfachheit von SIP stellt aber ein großes Sicherheitsproblem dar. Vor allem, weil die Informationen im Klartext übertragen werden. So einfach und flexibel es aufgebaut ist, so leicht lässt es sich manipulieren. Deshalb empfiehlt es sich, die verschlüsselte Variante SIPS zu verwenden.

SIP-Protokolle

<table>
<tr><th colspan="2">Teilnehmer</th></tr>
<tr><th colspan="2">G.711 / G.729 / G.723 / ...</th></tr>
<tr><th>SIP</th><th>SAP</th></tr>
</table>



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-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.

SIP-Requests (Anforderung)

SIP kennt folgende 6 Anforderung (Request).

Anforderung	Beschreibung

(Request)	
Invite	Die Gegenstelle wird zu einer Sitzung eingeladen. Dieser Vorgang entspricht der Signalisierung beim Angerufenen, dessen Telefon klingelt. Invite ist der wichtigste Request. Mit ihm wird die Verbindung gestartet.
Ack (nowledge)	Mit diesem Request wird die Verbindung bestätigt.
Bye	Dieser Request wird ausgeführt, wenn einer der beiden Gesprächspartner die Verbindung beendet.
Cancel	Dieser Request wird ausgeführt, wenn die Verbindung nach einer gewissen Zeit abgebrochen wird.
Options	Mit diesem Request werden Zusatzinformationen des Anwenders übermittelt.
Register	Mit diesem Request werden die Standort-Informationen des Client an den Server übergeben, damit dieser den Client bei einem Anruf finden kann.

Beispiel für ein INVITE-Request

INVITE sip:my@sip.server.com SIP/2.0

VIA:SIP/2.0/UDP 192.168.0.1
Call-ID:300f0gd090fgsa0f9da0gf0g@sip.server.com
From:<sip:my@sip.server.com>
To: Name <name@sip.server.com>
Call-ID:300f0gd090fgsa0f9da0gf0g@sip.server.com
CSeq:1 INVITE

SIP-Responses (Rückmeldungen)

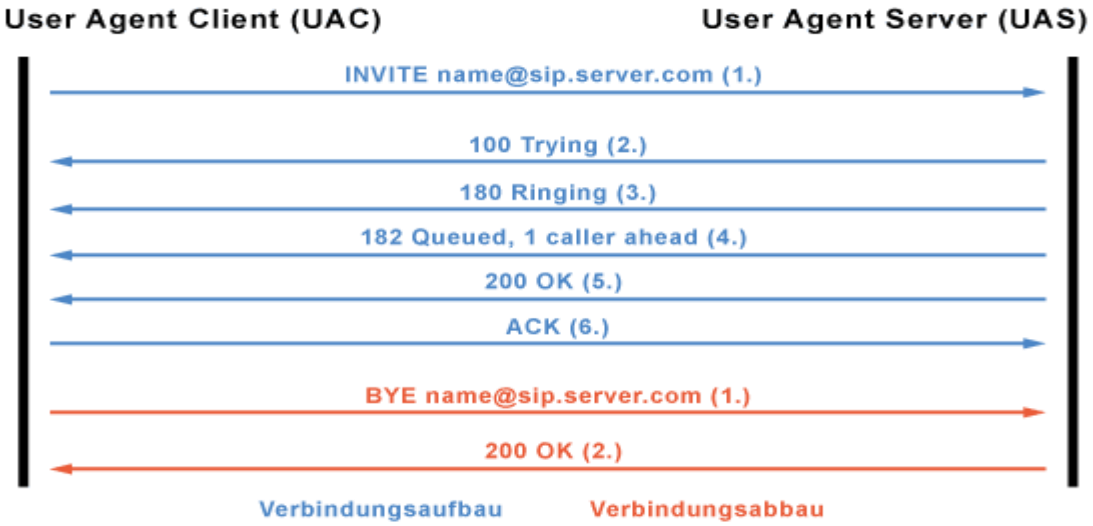
Kennung	Bedeutung
1	Anruf erfolgt
100	Verbindung wird hergestellt
180	Verbindung etabliert, warten auf Gegenseite
181	Der Anruf wird zu einem anderen Bestimmungsort umgeleitet.
182	Die Gegenstelle ist zur zeit nicht verfügbar, weist den Anrufer aber nicht zurück, sondern stellt ihn in eine Warteschleife.
200	OK
300	Die Rufnummer führt zu mehreren Zielen. Es folgt eine Auswahlmöglichkeit.
305	Das Anrufziel ist nur über einen Proxy-Server zu erreichen.

400	SIP-Syntaxfehler bei der Verbindungsaufnahme.
404	Die Gegenstell teilt mit, das2 das Anrufziel nicht existiert.
485	Das Anrufziel ist vieldeutig. Der SIP-Server kann mögliche Alternativen nennen.
500	Interner Server-Fehler, die Bearbeitung wurde abgebrochen.
501	Das SIP-Gateway unterstützt die angeforderte Aktion nicht.
504	Timeout beim Warten auf einen anderen Server überschritten.
600	Besetzt.
603	Die Gegenstelle weist den Anruf ab.
604	Die Gegenstelle existiert nicht im angegebenen SIP-Netz.
605	Der Session-Aufbau wurde ohne weitere Begründung nicht akzeptiert.

Prinzip des Verbindungsaufbaus

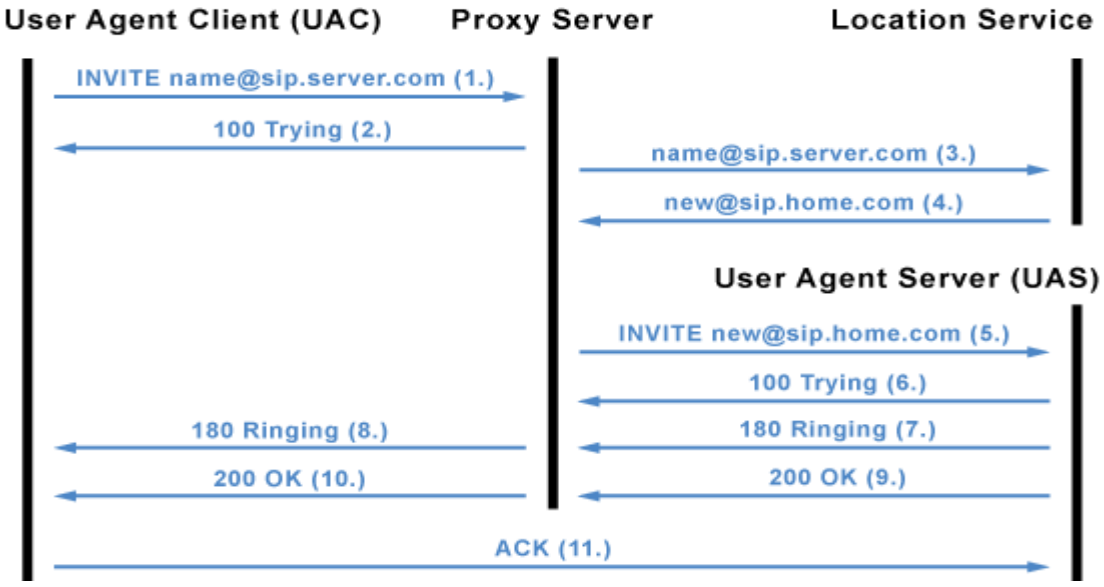
In einer SIP-Verbindung wird der Anrufer als User Agent Client (UAC) und der Angerufene als User Agent Server (UAS) bezeichnet.
Die Sitzungsabläufe können direkt zwischen den User Agents ablaufen. Allerdings ist nicht immer gewährleistet, dass ein User Agent erreichbar ist und immer dieselbe IP-Adresse 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



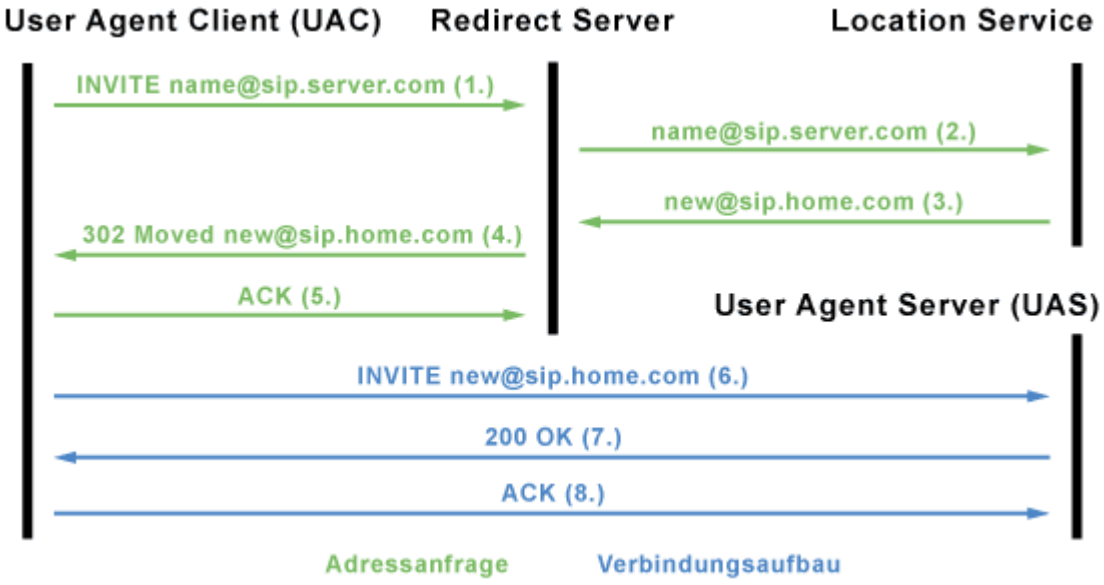
Der UAC leitet den Verbindungswunsch durch ein INVITE ein. Der UAS bestätigt dem UAC den Verbindungswunsch mit einem "Trying". Mit "Ringing" wird dem UAC bestätigt, dass dem Angerufenen der Verbindungswunsch signalisiert wird. Ist der Gesprächspartner belegt, dann schickt der UAS dem UAC ein "Busy here".
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.

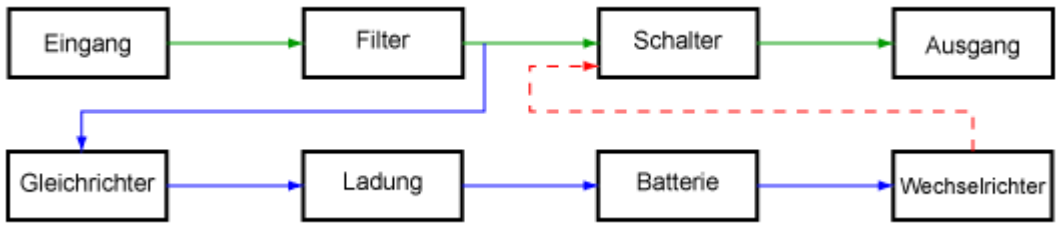
70. Funktionsweise von USVs

USV - Unterbrechungsfreie Stromversorgung

Viele Geräte und Maschinen müssen nahezu 100% ihrer Laufzeit zu Verfügung stehen. Hierzu gehören Server und Router, die z. B. das Internet am Laufen halten. Neben Hardware- und Software-Problemen zählt auch die Stromversorgung zur Achillesferse eines jeden Gerätes aus der Kommunikations- und Informationstechnik. Deshalb werden wichtige Geräte mit einer USV, unterbrechungsfreie Stromversorgung, ausgestattet. Doch nicht nur ein Stromausfall, sondern auch kurzzeitige Unter- und Überspannungen sollen durch die USV abgefangen werden.
Aufgrund der unterschiedlichen Bedürfnisse der einzelnen Geräte haben sich drei Klassen im USV-Bereich etabliert, die das International Engineering Consortium (IEC) unter der Produktnorm IEC 62040-3 und die Europäische Union unter EN 50091-3 festgelegt haben.

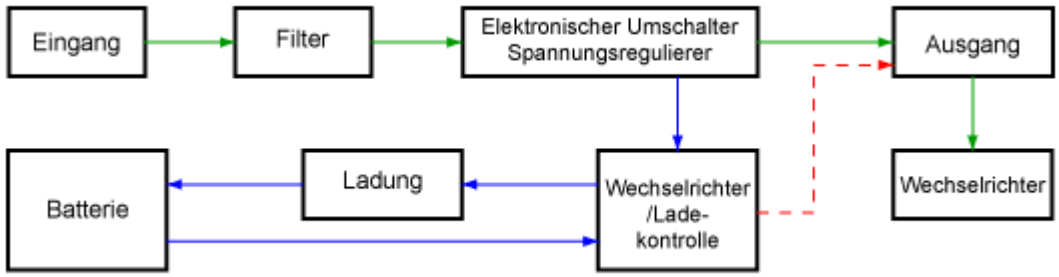
- Standby- oder Offline-USV
- Line-Interactive-, Netzinteraktiv-, Delta-Conversion- oder Single-Conversion-USV
- Online-Double-Conversion- oder Dauerwandler-USV

Standby- oder Offline-USV



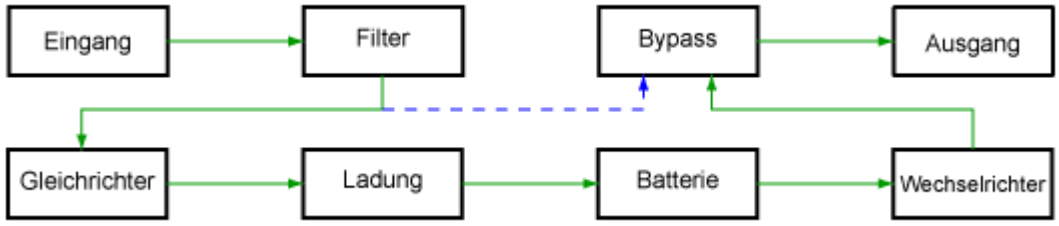
Die einfachsten und billigsten USVs (nach IEC 62040-3.2.20 der USV-Klasse 3) sind Standby- bzw. Offline-USVs. Sie schützen nur gegen Netzausfälle und kurzzeitigen Spannungsschwankungen und -spitzen. Unter- und Überspannungen werden nicht ausgeglichen. Wegen der Umschaltdauer zwischen Netzbetrieb auf Batteriebetrieb von 4 bis 10 Millisekunden (ms) werden Störspannungen, Spannungseinbrüche und Spannungsspitzen unterhalb dieser Zeit nicht erkannt.
Offline-USVs schalten automatisch bei Über- oder Unterspannung auf Batterie-Betrieb um. Viele USVs liefern dann am Ausgang eine Rechteck-ähnliche Spannung. Geräte mit induktiver Last, z. B. Laserdrucker, sind für diese USVs ungeeignet. Empfehlenswert und zweckmäßig sind robuste Verbraucher, wie kleine TK-Anlagen und einzelne Computer mit Peripherie, die mit primär getakteten Netzteilen mit Überspannungsschutz und Spannungsfilter ausgestattet sind. Der Wirkungsgrad der Offline-USVs liegt bei 95%.

Netzinteraktive USV



Netzinteraktive USVs (nach IEC 62040-3.2.18 der Klasse 2) funktionieren ähnlich wie Standby-USVs. Sie schützen vor Netzausfall, kurzzeitige Spannungsspitzen und können durch Filter Spannungsschwankungen ständig regeln. Die Umschaltzeit von Netzbetrieb auf Batteriebetrieb dauert 2 bis 4 Millisekunden (ms). Umgekehrt wird verzögerungsfrei geschaltet. Netzinteraktive USVs liefern in der Regel ein stufenförmiges Ausgangssignal. Der Wirkungsgrad liegt zwischen 95 und 98%. Dieser sinkt, wenn der Ausgangswandler aktiv wird.
Netzinteraktive USVs eignen sich in Gegenden, wo viele Spannungsschwankungen vorkommen. Einzelne Computer, größere TK-Anlagen und Netzwerke lassen sich absichern. Auf den Schutz hochsensibler Systeme sollte verzichtet werden.

Online-USV



Die bisher beschriebenen USV-Techniken haben alle einen gravierenden Nachteil: Die Last wird erst bei Netzausfall aus der Batterie gespeist. Die Umschaltzeit bereitet aber hochsensiblen Systemen Probleme.
Die Dauerwandler- bzw. Online-USVs (nach IEC 62040-3.2.16 der Klasse 1) gelten als echte Stromgeneratoren, die ständig eine eigene Netzspannung erzeugen. Damit werden angeschlossene Verbraucher dauerhaft ohne Einschränkungen mit Netzspannung versorgt. Zeitgleich wird die Batterie aufgeladen. Dabei kann die Eingangsspannung zwischen 160 und 290 V schwanken. Die Ausgangsspannung entspricht nahzu einer Sinuskurve. Sie verfügt aber über bessere Eigenschaften, als der Strom aus der Steckdose. Ganz ohne Störspannungen, elektromagnetischen Einflüssen, Frequenzstörungen und Spannungsverzerrungen. Verfügt die USV über eine galvanische Trennung oder einen Trenntransformator (Trenntrafo) werden sogar Störungen über den Null- bzw. Erdleiter gefiltert.
Dauerwandler-USVs sind mit einem statischen Bypass ausgestattet, auf den die Verbraucher umgeschaltet werden. Da im laufenden Betrieb ständig die Spannung gewandelt wird, entstehen elektrische Verluste und Wärme. Der Wirkungsgrad liegt deshalb nur bei 90%. Die Lebensdauer

der Akkus beträgt wegen der Dauerbelastung nur 3 bis 4 Jahre.
Dauerwandler-USVs kommen in hochsensiblen Bereichen in der Computer- und Kommunikationstechnik zum Einsatz. Für diesen umfassenden Schutz muss entsprechend Geld angelegt werden.

Eigenschaften im Überblick

USV-Klasse	Klasse 1	Klasse 2	Klasse 3
Leistung	ab 500 VA	bis 5 kVA	bis 1 kVA
Wirkungsgrad	90%	95-98%	95%
Preis	hoch	mittel	niedrig
Anwendung	Server und Datenkommunikation	einzelne Computer, TK-Anlagen und Netzwerke	Kleinst-Verbraucher, einzelne Computer
Schutz vor	umfassender Schutz durch ständige Erzeugung einer Sinusspannung	Netzausfall, filtern von Spannungsschwankungen und -spitzen	Netzausfall, kurzzeitige Spannungsschwankungen
Umschaltdauer		2 bis 4 ms	4 bis 10 ms

Kaufberatung

Welche USV-Klasse? Geschäftskritische Anwendungen benötigen Dauerwandler-USVs (Klasse 1). Computer und Server kommen mit Klasse-2-USVs aus. Für billige Geräte, ohne teure Bauteile, reichen Offline-USVs (Klasse 3) aus.
Geräte mit ungleichmäßigem Stromverbrauch sind für USVs generell ungeeignet.

Shutdown-Zeit? Sollte es zu Stromausfällen kommen oder ständige Spannungsschwankungen auftreten, müssen alle Geräte ordnungsgemäß heruntergefahren werden, um Hardware-Schäden und Datenverluste zu vermeiden. Entsprechend lange muss die Leistung der USV ausgelegt sein.

Mindestleistung? Ausschlaggebend ist der Stromverbrauch der per USV versorgten Geräte. Diesen Wert mulipliziert man mit 230 V und addiert 30% als Sicherheit dazu. Ist der Stromverbrauch unbekannt, dann dividiert man die Wirkleistung durch 0,6. Damit erhält man annähernd die Scheinleistung in VA.
Damit bei bei Neuanschaffungen die USV nicht auch noch aufgerüstet werden muss, empfiehlt sich eine Leistungsreserve von 15 bis 25% einzuplanen.

Bauart? USVs gibt es in den unterschiedlichsten Bauweisen. Neben den normalen Standgeräten gibt es auch Rackmodule für 19". Wichtig ist, dass man den

Standort vorher wählt und dann die Bauweise bestimmt. Besonders große USVs sind schwer und mit viel Mühe zu installieren und zu warten. Wenn die Batterien ausgetauscht werden müssen, dann sind schwer zugängliche USVs immer ein Ärgernis.

71. LDAP

LDAP - Lightweight Directory Access Protocol

LDAP ist ein Protokoll, das für die Kommunikation zwischen Client und X.500-Verzeichnisdienst gedacht ist. Obwohl LDAP im Zusammenhang mit Verzeichnisdiensten genannt wird, ist es kein Verzeichnisdienst, sondern nur ein Protokoll. LDAP ist auch kein offizieller Standard, sondern nur als RFC veröffentlicht.

Die X.500-Spezifikation (Verzeichnisdienst nach OSI) sieht die komplette Implementierung des OSI-Schichtenmodells vor. Die Nutzung vorhandener Protokolle ist dabei nicht vorgesehen. Die Kommunikation zwischen Directory User Agent (DUA) und Directory System Agent (DSA) muss mit viel Aufwand realisiert werden. Deshalb wurde 1993 mit LDAP ein komplettes Protokoll definiert, mit dem ein TCP/IP-Client auf ein X.500-Verzeichnis zugreifen kann.

Wie funktioniert LDAP?

Der LDAP-Client greift über TCP/IP auf den LDAP-Server zu. Der LDAP-Server ist Teil eines LDAP-Gateways, in dem sich ein X.500-Client befindet, der über den OSI-Protokoll-Stack auf den X.500-Server zugreift.

Stand-alone-LDAP-Server

Anstatt eines LDAP-Gateways und der Umweg über einen X.500-Server kann der LDAP-Server auch direkt auf das Verzeichnis zugreifen. Man bezeichnet diese Konstellation auch als Stand-alone-LDAP-Server.
Für den LDAP-Client spielt es keine Rolle, ob der LDAP-Server direkt auf das Verzeichnis zugreift oder als LDAP-Gateway fungiert.

Greift der LDAP-Server direkt auf das Verzeichnis zu, kann man von einem LDAP-Verzeichnisdienst sprechen. Die Architektur ist ein Client-Server-Modell das im Vergleich zu X.500 einfacher zu realisieren ist.
Bei einem LDAP-Verzeichnisdienst stehen die X.500-Funktionen nicht mehr zur Verfügung. Es gilt nur ein eingeschränkter Funktionsumfang.

72. SLA (Service Level Agreement)

Dienstgütevereinbarung

Ein Service Level Agreement (SLA) ist eine bilaterale, juristische Übereinkunft zwischen Netzwerk-Provider und Kunde, in der die vertraglichen Vereinbarungen zur Qualität der Leistungen spezifiziert sind. Zu den wesentlichen Aspekten einer solchen Qualitätsvereinbarung, in denen die Netz- und Service-Parameter festgelegt sind, gehören die Bandbreite, die Verfügbarkeit, die Netzkapazität und die Netzqualität. Neben den genannten technischen Parametern spielen die Güte der Dienstleistung, die Technik und Messtechnik, mit der die Dienstleistungen erbracht werden, die Verfügbarkeit, die Ausfall-, Reaktions- und Reparaturzeiten, die Servicequalität beeinflussende Faktoren, eine Rolle.

Eine Dienstgütevereinbarung umfasst alle Dienste, Netze, Komponenten und Verbindungen: Sprach-, Daten- und Internetdienste, Basisdienste und Value Added Services (VAS), Fest- und Mobilfunknetze, Lokale Netze, Stadtnetze und Weitverkehrsnetze sowie Fest-, Richtfunk- und Ende-zu-Ende-Verbindungen. Da es keine Standards für die SLAs gibt, kann jeder Service Provider beliebige Angebote und Leistungen mit dem SLA-Label versehen.

Ein SLA-Vertrag sollte den Gegenstand der Dienstleistung definieren, die Laufzeit und die Kündigungsmodalitäten enthalten, die technische Leistung beschreiben, die Behandlung von Störungen, Vertragsstrafen und das Änderungsmanagement umfassen.

Neuere Ansätze gehen weit über die IT-spezifischen Vereinbarungen hinaus und stellen in den SLAs auch Anforderungen an die Geschäftsprozesse des Unternehmens. So beispielsweise an die Anzahl der abgewickelten Transaktionen, den Druck-Output oder die Menge an archivierten Dokumenten. In diese Ansätze können weitere administrative, personelle, entwicklungs- und produktionstechnische, marketing- und vertriebstechnische Größen aufgenommen werden.

73. Arten und Eigenschaften von Glasfasern

Lichtwellenleiter (LWL / Glasfaser)

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

Durch Lichtwellenleiter können optische Signale ohne Verstärker große Entfernungen überbrücken. Trotz weiter Strecken ist eine hohe Bandbreite möglich. Die Bandbreite auf einer einzigen Glasfaser beträgt rund 60 THz. Das macht Lichtwellenleiter zum Übertragungsmedium der Gegenwart und Zukunft. Da reicht kein Kupferkabel oder Funksystem heran.

Glasfaser und Lichtwellenleiter

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

Prinzip eines Übertragungssystems auf Basis eines Lichtwellenleiters

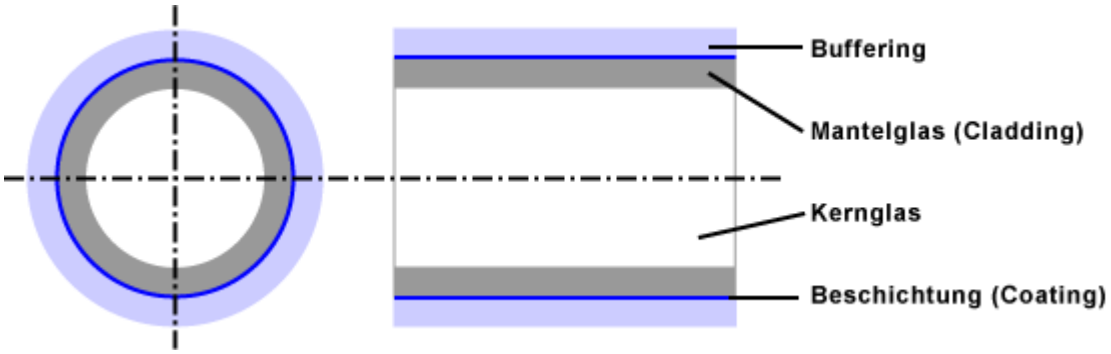
Sender oder Quelle	Analog-Digital-Wandler	Treiber-Stufe	Leucht-diode	Licht-wellen-leiter	Foto-Trs.	Digital-Analog-Wandler	Treiber-Stufe	Empfänger

Abhängig von der Datenform, findet zuerst eine Analog-Digital-Wandlung statt. In der Regel liegen die Daten als elektrische Signale vor, die dann noch durch eine Treiberstufe verstärkt werden. Vor der Übertragung müssen die elektrischen Signale in optische Signale umgewandelt werden. Dazu dienen spezielle Leuchtdioden (LEDs) oder Laserdioden als Lichterzeuger. Das Licht wird direkt in den Lichtwellenleiter eingespeist. Am 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. Sie sind äußerst flexibel und empfindlich.
Der Faserkern (Kernglas) ist der zentrale Bereich eines Lichtwellenleiters, der zur Wellenführung des Lichts dient. Der Kern besteht aus einem Material mit einem höheren Brechungsindex als der darrüberliegende Mantel. An den Wänden im Innern des Lichtwellenleiters findet eine Reflexion statt, so dass der Lichtstrahl nahezu verlustfrei um jede Ecke geleitet wird. Das Mantelglas ist das optisch transparente Material eines Lichtwellenleiters an dem die Reflexion stattfindet. Das Mantelglas oder auch Cladding genannt ist ein dielektrisches Material mit einem niedrigeren Brechungsindex als der Kern. Das dielektrische Material ist nichtmetallisch und nichtleitend. Es enthält also keine metallischen Anteile.
Das Coating ist die Kunststoffbeschichtung, die als mechanischen Schutz auf der Oberfläche des Mantelglases aufgebracht ist.
Buffering nennt man das Schutzmaterial, das auf dem Coating aufextrudiert ist. Es schützt das Kabel vor Umwelteinflüssen. Buffering gibt es auch als Röhrchen, dass die Faser vor Stress im Kabel isoliert, wenn das Kabel bewegt wird.

Vorteile der Lichtwellenleiter gegenüber Kupferkabel

- Lichtwellenleiter können beliebig mit anderen Versorgungsleitungen parallel verlegt werden. Es 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 somit 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.

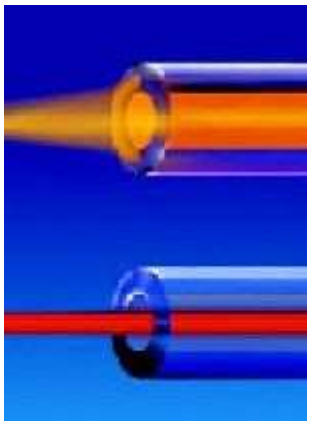
Einfügedämpfung

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

Dispersion

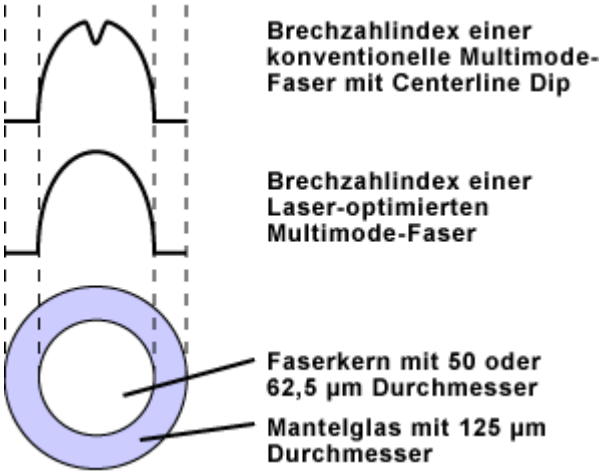
Dispersion beschreibt den Effekt, dass der eingespeiste Impuls über den Ausbreitungsweg zeitlich ausgeweitet wird. Der Impuls wird breiter. Dadurch kann es zu Überlappungen mit den vorangegangenen und nachfolgenden Impulsen kommen. Bei hohen Geschwindigkeiten kann es zu Übertragungsfehlern kommen.
Um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

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. Speziell für Lichtwellenleiter wurden VCSELs (Vertical Cavity Surface Emitting Lasers) entwickelt und 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 Laser-Lichteinkopplung sind zwingend Laser-optimierte Lichtleiter zu verwenden.

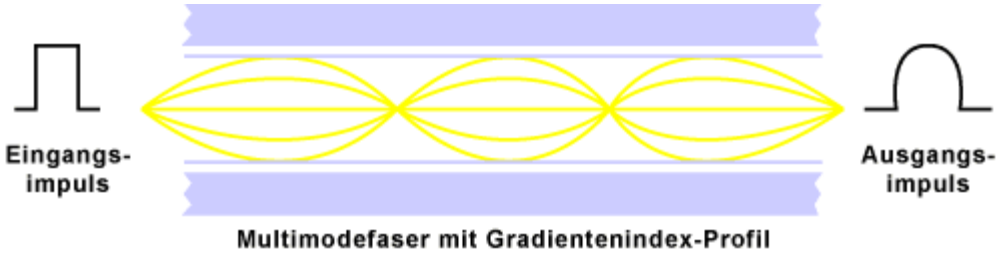
Übersicht: Lichtwellenleiter

Kabeltyp	Durchmesser (Kern / Gesamt)	Bandbreite (1 km)	Anwendung
Multimode mit Stufenprofil	100 bis 400 µm / 200 bis 500 µm	100 MHz	Entfernungen unter 1 km
Multimode mit Gradientenprofil	50 µm / 125 µm	1 GHz	LAN, Backbone, ATM (655 MHz) in Europa
	62,5 µm / 125 µm	1 GHz	LAN, Backbone, ATM (655 MHz) in den USA
Monomode (Singlemode) mit Stufenprofil	9 µm / 125 µm	100 GHz	Netzbetreiber

Multimodefaser mit Stufenindexprofil

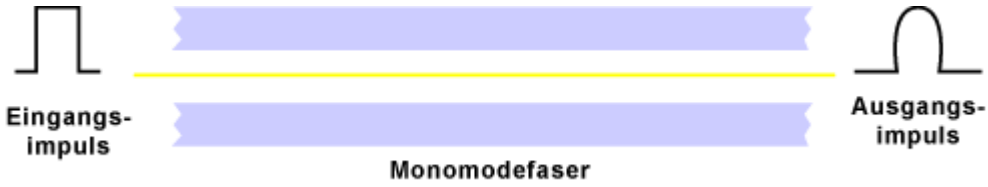
Multimodefasern mit Stufenprofil haben einen Gesamtdurchmesser von 200 bis 500 µm. Durch sie werden mehrere Lichtwellen gleichzeitig geschickt. An den Wänden der Faser wird das Signal hart reflektiert. Die Brechzahl fällt zwischen Kern und Mantel scharf ab. Das Ausgangssignal wird dadurch schlechter. Sie werden z. B. als Verbindungskabel im Patchschrank verwendet.

Multimodefaser mit Gradientenindexprofil



Multimodefasern mit Gradientenprofil haben einen Gesamtdurchmesser von 125 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 Gesamtdurchmesser von 125 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

Laser-optimierte Multimodefasern

Fasertypen	Fast Ethernet	Gigabit Ethernet	10 Gigabit Ethernet	40 Gigabit Ethernet	100 Gigabit Ethernet
OM1 Faser (62,5/125 µm)	2.000 m (FX)	275 m (SX)	33 m (SR)	nicht spezifiziert	nicht spezifiziert
OM2 Faser (50/125 µm)	2.000 m (FX)	550 m (SX)	82 m (SR)	nicht spezifiziert	nicht spezifiziert
OM3 Faser (50/125 µm)	2.000 m (FX)	550 m (SX)	300 m (SR)	100 m (SR4)	100 m (SR10)
OM4 Faser (50/125 µm)	2.000 m (FX)	1.000 m (SX)	550 m (SR)	150 m (SR4)	150 m (SR10)

Glasfaser-Netzarchitektur

In der zukünftigen Breitband-Infrastruktur spielen Glasfaserkabel eine große Rolle. Um eine hohe Bandbreite bei den Teilnehmeranschlüssen zu erreichen, sind die Netzbetreiber gezwungen, die "letzte Meile" im Festnetz von der reinen Kupferverkabelung auf Glasfaserverkabelung umzubauen. Die "letzte Meile" bezeichnet die Strecke der Leitung von der Vermittlungsstelle bis zum Teilnehmeranschluss beim Kunden.

Auf dem Weg zur vollständigen "Verglasung" gibt es mehrere Zwischenschritte, die eine Kombination aus Kupferkabel und Glasfaserkabel vorsehen. Im folgenden Text werden Netzarchitekturen beschrieben, die Glasfaserkabel auf der "letzten Meile" zum Kunden verwenden.

- FTTC - Fibre-to-the-Curb
- FTTB - Fibre-to-the-Building
- FTTH - Fibre-to-the-Home
- FTTD - Fibre-to-the-Desk

Für die verschiedenen Glasfaser-Netzarchitekturen gibt es unterschiedliche Übertragungstechniken und -systeme, die die Entfernung zwischen Vermittlungsstelle und Teilnehmeranschluss mit einer entsprechenden Kombination aus Glasfaser- und Kupferkabel überbrücken.

Klassisches Festnetz (zum Vergleich)

Typischerweise besteht das klassische Festnetz aus einer durchgängigen Kupferverkabelung. Ausnahme ist die Vermittlungsstellte (VSt). Die wird seit der Digitalisierung des Telefonnetzes mit Glasfaser angebunden. Der Rest der Strecke vom Teilnehmerendgerät (TE) zum Teilnehmeranschluss (TA), APL (Anschlusspunkt Linientechnik), zum Kabelverzweiger (KvZ) am Straßenrand bis zur Vermittlungsstelle (VSt) besteht ausschließlich aus Kupferkabel.

Kurz zu Erläuterung: Das Teilnehmerendgerät (TE) ist zum Beispiel ein Telefon, ein PC oder ein Router, der den Übergang in ein lokales Netzwerk darstellt. Der Teilnehmeranschluss (TA) ist die Anschlussdose ab der der Endkunde seine eigenen Endgeräte anschließen darf. Im Festnetz ist das die TAE-Dose. Der APL ist ein Übergabepunkt innerhalb eines Gebäudes in dem verschiedene Teilnehmeranschlüsse zusammenlaufen. In der Regel ist das ein einfacher Verteiler, der sich im Keller befindet. Der Kabelverzweiger (KvZ) ist ein grauer Verteilerkasten am Straßenrand, der mehrere Gebäude oder Straßenzüge mit einem Hauptkabel von der Vermittlungsstelle (VSt) verbindet.

FTTC - Fibre-to-the-Curb

Fibre-to-the-Curb (FTTC) oder Fibre-to-the-Cabinet (FTTC) bedeutet "Glasfaser bis zum Bordstein/Straßenrand". Die VDSL2-Infrastruktur der Deutschen Telekom in den Großstädten Deutschlands ist eine typische FTTC-Installation.
In der FTTC-Architektur endet das Glasfaserkabel in einem grauen Kasten, im Kabelverzweiger (KvZ), der am Straßenrand steht. Von diesem Anschlussverteiler aus werden die vorhandenen Kupferkabel bis zum Kunde weiter verwendet. Im Kabelverzweiger ist dafür ein aktive Komponente installiert, die die Signale von Glasfaser auf Kupferkabel bzw. umgekehrt umsetzt. Dazu unterscheidet sich auf beiden Seiten die Übertragungstechnik. Die Umsetzung ist recht aufwendig und erfordert aktive Komponenten.
Weil die Hauptkabel im städtischen Bereich in Rohren verlegt sind, lassen sich hier Glasfaserkabel kostengünstig einziehen. Dazu werden Kanaldeckel geöffnet und in einem freien Rohr ein Glasfaserkabel bis zum nächsten Kanaldeckel eingezogen.
Problematisch ist die Verkabelung zwischen Vermittlungsstelle (VSt) und Kabelverzweiger in ländlichen Gebieten. Dort ist das Kupferkabel meist direkt im Erdreich vergraben. Der Austausch durch ein Glasfaserkabel ist nicht so einfach möglich. Für die Verlegung eines Glasfaserkabels muss in der Regel das Erdreich aufgegraben werden. Die Kosten für einen Kilometer liegen bei 50.000 bis 100.000 Euro.

FTTB - Fibre-to-the-Building / Fibre-to-the-Basement

Fibre-to-the-Building (FTTB) bedeutet "Glasfaser bis zum Gebäude". Die FTTB-Architektur sieht vor, dass das Glasfaserkabel innerhalb des Gebäudes endet, in dem der Kunde seinen Anschluss hat. Genauer gesagt endet das Glasfaserkabel am APL (Abschlusspunkt Linientechnik) bzw. HÜP (Hausübergabepunkt) oder in der Nähe davon. Der APL befindet sich meistens im Keller des Gebäudes. Innerhalb des Gebäudes wird die vorhandene Kupferverkabelung verwendet, um bis in die Wohnungen zum Teilnehmeranschluss (TA) zu kommen. Dort wird ein IAD (Integrated Access Device) angebracht, an dem die Endgeräte angeschlossen werden.
Die FTTB-Architektur kommt vorwiegend im städtischen Bereich zum Einsatz. Denkbar ist die Anbindung von Hochhäusern, Mehrfamilienhäusern oder Wohnanlagen, die aus vielen einzelnen Wohneinheiten bestehen. Meist steht der Kabelverzweiger oder die Vermittlungsstelle direkt vor dem Haus. Da bietet es sich an, von dort aus, ein Glasfaserkabel bis ins Gebäude zu verlegen. Innerhalb des Gebäudes werden die einzelnen Wohneinheiten über die bestehende hausinterne Kupferverkabelung mit Internet versorgt.

FTTH - Fibre-to-the-Home

Fibre-to-the-Home (FTTH) bedeutet "Glasfaser bis in die Wohnung". Die FTTH-Architektur sieht vor, dass das Glasfaserkabel in den Wohnungen des Kunden am Teilnehmeranschluss (TA) endet. In der Regel ist das eine Anschlussdose in der Wand, die sich an einer zentralen Stelle in der Wohnung befindet.
Eine Variante davon ist FTTB (Fibre-to-the-Building oder Fibre-to-the-Basement). Hier endet das Glasfaserkabel hinter der Hauseinführung. Üblicherweise gibt es bei Einfamilienhäusern keinen Unterschied zwischen FTTB und FTTH. Hier endet das Glasfaserkabel in der Regel immer hinter der Hauseinführung. Hier ist der APL (Abschlusspunkt Linientechnik) bzw. HÜP (Hausübergabepunkt) angebracht. Dahinter sitzt das ASG (anwendungsspezifische Gerät). Es handelt sich dabei um ein ONT, CPE, NTFA oder Fibre Node, die den Netzabschluss darstellen. Der ASG wird häufig mit dem IAD (Integrated Access Device) kombiniert. Der IAD ist ein Multifunktionsgerät, dass vom Netzbetreiber oder Provider bereitgestellt wird. Im IAD sind die Zugangsdaten des Kunden gespeichert. Vom IAD werden Telefonanschlüsse über TAE und der Internetzugang über RJ-45 oder WLAN bereitgestellt.
Für die Heimvernetzung braucht es ein Glasfaserkabel das die optischen Eigenschaften von Glasfaserkabel und die Biegsamkeit von Kupferkabel hat. In den Anwendungsbereichen von FTTH kommen wesentlich kleinere Biegeradien vor, als bei üblichen Glasfaser-Installationen. Das Kabel muss dem Standard ITU-T-G.657B entsprechen.

FTTH bedeutet nicht, dass von der Vermittlungsstelle bis zu jedem Kunden ein Glasfaserkabel verlegt wird. Von der FTTC-Architektur ausgehend, werden die Kupferkabel vom Kabelverzweiger bis zum Teilnehmeranschluss des Kunden durch ein Glasfaserkabel ersetzt. Im

Kabelverzweiger wird durch einen optischen Splitter das Lichtsignal für alle ausgehenden Glasfaserkabel dupliziert.

Auf der untersten Ebene der Glasfaserverkabelung konkurrieren zwei System. Zum einen PON (PtMP) und PtP. PON ist eine Punkt-zu-Mehrpunkt-Topologie in Gruppen zu je 32 oder 64 Teilnehmern. Hier teilen sich die Teilnehmer eine gemeinsame Glasfaser-Zuführung. Dagegen steht PtP-Ethernet, bei der jeder Teilnehmer seine eigene Glasfaser vom nächsten Netzknoten (VSt) bekommt.

FTTD - Fibre-to-the-Desk

Fibre-to-the-Desk (FTTD) bedeutet "Glasfaser bis zum Schreibtisch". Es handelt sich dabei um eine sogenannte "Vollverglasung", bei der die gesamte Übertragungsstrecke von der Vermittlungsstelle bis zum Schreibtisch aus Glasfaser besteht. Das bedeutet, auch von der Anschlussdose (TA) bis zum Endgerät (TE) wird ein Glasfaserkabel verwendet.

74. SSD

SSD - Solid State Drive

Ein Solid State Drive, kurz SSD, ist ein Massenspeicher, vergleichbar mit einer Festplatte. Im Gegensatz zur Festplatte hat eine SSD keine beweglichen Teile. Bei der SSD ist das Speichermedium ein Flash-Speicher (z. B. NAND-Flash).
Flash-Speicher wird hauptsächlich in mobilen Endgeräten, wie Handys, Digitalkameras und MP3-Player, eingesetzt. Flash-Speicher arbeitet vollkommen geräuschlos, hat kurze Zugriffszeiten und schont den Akku, weil keine mechanischen Teile durch Motoren bewegt werden müssen.
Die SSD wird wie eine herkömmliche Festplatte angesprochen. Um einen bestimmten Sektor zu lesen, muss eine Festplatte die Köpfe auf die richtige Spur bewegen. Diese Bewegung unterliegt einer gewissen mechanische Trägheit, die überwunden werden muss. Dann vergeht noch eine geringe Latenzzeit, bis der gewünschte Sektor am Lesekopf vorbeidreht. Dieser Zeitverlust fällt bei der SSD weg. SSDs zeichnen sich also durch eine sehr hohe Lese- und Schreibgeschwindigkeit, sowie einen geringeren Energieverbrauch aus.

SSD in der Form einer herkömmlichen Festplatte

SSD als mSATA-Steckkarte

SSD in der m.2-Bauform (NFF)

Vorteile von SSD (Solid State Drive)

- hohe Transferraten
- kurze Zugriffszeiten, vor allem beim Lesen
- niedrige Leistungsaufnahme
- geräuschloser Betrieb

Lesen und Schreiben

Beim Lesen holt der Flash-Controller immer 2 bis 4 kByte aus den Flash-Zellen und schreibt sie in einen Pufferspeicher. Da beim Lesen keine Lese-/Schreibköpfe mechanisch positioniert werden müssen ergeben sich äußerst geringe Zugriffszeiten.

Während das Lesen sehr schnell geht, gestaltet sich das Schreiben von Daten etwas aufwändiger. Flash-Speicher ist blockweise organisiert. Typischerweise hat ein Speicherblock 128 bis 512 kByte. Auch dann, wenn es nur ein paar Bit sind, muss der betreffende Block vollständig neu geschrieben werden. Vor dem Beschreiben einer Speicherzelle, muss sie gelöscht werden. Dazu wird eine hohe Löschspannung angelegt. Dabei verlieren alle Zellen dieses Blocks ihren Inhalt. Erst dann werden die Daten geändert und dann wieder zurück geschrieben. Dieser Vorgang führt dazu, dass schnelle Festplatten beim Schreiben schneller sein können.

Um die niedrige Schreibgeschwindigkeit zu beschleunigen wird der Flash-Speicher um einen Puffer ergänzt. Davon profitiert vor allem NCQ. NCQ fängt die Schreibzugriffe ab und sortiert sie um, damit sie möglichst intelligent auf die einzelnen Speicherblöcke verteilt werden. Obwohl dieses Verfahren mit dem Namen NCQ (Native Command Queuing) für herkömmliche Festplatten eingeführt wurde, ermöglicht es auch SSDs einen Geschwindigkeitsgewinn.
Bei normalem Nutzungsverhalten machen sich die hohen Zugriffszeiten beim Schreiben nicht negativ bemerkbar. Die meisten Daten werden immer noch aus dem Speicher gelesen. Schreibzugriffe treten wesentlich seltener auf.

SLC-, MLC- und TLC-Flash

SSDs mit SLC-Flash sind sehr zuverlässig und dafür teuer. SSDs mit MLC-Flash haben eine langsamere Schreibgeschwindigkeit und weisen eine geringere Haltbarkeit gegenüber SLCs auf. Dafür sind MLCs günstig, aber eben weniger zuverlässig. Mit Wear Leveling versucht man diese Nachteile zu kompensieren. Die langsamere Schreibgeschwindigkeit ist nicht so das Problem. Bei der typischen PC-Nutzung werden sehr viel mehr Daten gelesen als geschrieben.

Speicherkapazität

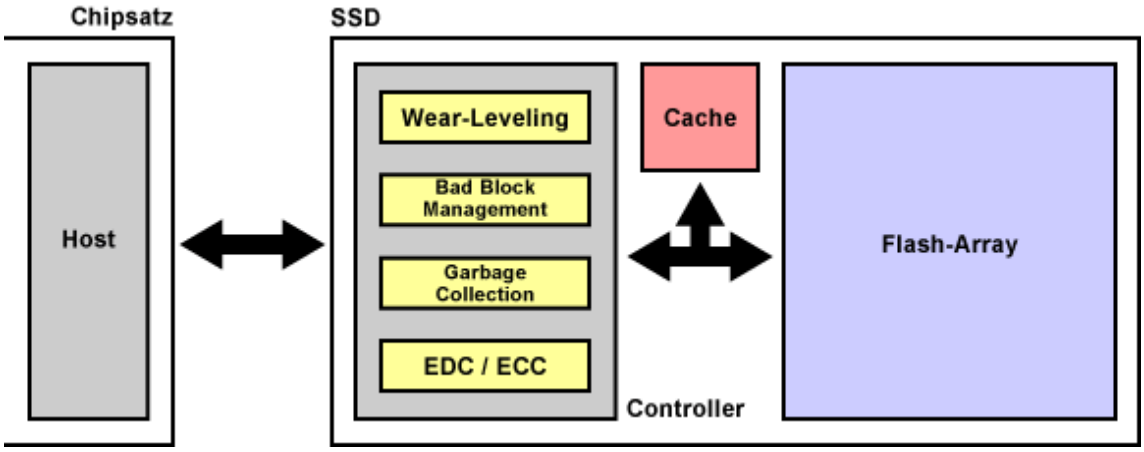
Ein Nachteil von SSDs ist der relativ große Platzbedarf. Prinzipiell kann man mit feineren Halbleiterstrukturen mehr Speicherkapazität bei gleicher Chipgröße bekommen. Bei Flash-Speicher lässt sich die Datendichte aber nicht einfach erhöhen, ohne dabei Nachteile in Kauf zu nehmen. Mit jeder weiteren Verkleinerung der Chipstrukturen wird das Floating Gate jeder Speicherzelle immer empfindlicher und auch der Stromverbrauch höher. Im Floating Gate werden die Ladungen gespeichert. Jedes Ändern des Ladezustandes, das so genannte Schreiben, belastet das Floating Gate und die umgebenden Sperrschichten.

Empfindlichkeit und Stromverbrauch stehen dem Wunsch nach größerer Speicherkapazität gegenüber. Deshalb versucht man die Speicherdichte pro Speicherzelle zu erhöhen, in dem man mehrere Zustände in eine Zelle packt. Also nicht nur 1 Bit, sondern 2 oder mehr Bit pro Speicherzelle. Zum Beispiel mit MLC und TLC. Bei 3 Bit umfasst eine Speicherzelle 8 verschiedene Zustände, die in Form einer Ladung abgebildet wird. Diese Ladung muss entsprechend exakt in die Speicherzelle geschrieben werden. Entsprechend exakt muss auch der Lesevorgang sein, bei dem die Ladung der Speicherzelle gemessen wird.

Erschwerend kommt hinzu, dass die Zellen auch noch feinere Halbleiterstrukturen aufweisen. Dann reduziert sich die Anzahl der Schreibvorgänge, die eine einzelne Speicherzelle aushält. Kleinere Strukturbreiten haben zur Folge, dass jede Speicherzelle immer weniger Elektronen aufnehmen, deren Ladung eine bestimmte Zelleninhalt darstellt. Je geringer die Anzahl von Elektronen, desto höher die Wahrscheinlichkeit von Bitfehlern. Fehlerkorrekturmaßnahmen im Chip und im Controller senken die Fehlerwahrscheinlichkeit. Zusätzlich geht die Zahl der Schreibzyklen zurück, die jede einzelne Zelle übersteht.

Mit zunehmender Anzahl an Zuständen (oder Bit pro Speicherzelle) steigt die Dauer, bis der Controller den Zelleninhalt ausgelesen hat. Bei 4 Bit pro Zelle könnte Schluss sein. Hier müssen 16 Zustände sauber voneinander getrennt werden. Dafür braucht es ausreichend Ladungsträger im Floating-Gate. Eine weitere Miniaturisierung wäre möglich, hat aber ihre Grenze. Die ist dann erreicht, wenn in das Floating-Gate nicht mehr Elektronen passen als es für eine saubere Unterscheidung der Ladung notwendig wäre.
Nur bei SLC-Flash sind sehr kleine Strukturen möglich. Hier ist die Gesamtkapazität bei 4 TByte erreicht. Eine Alternative sind Flash-Speicherchips mit 3D-Strukturen.

Aufbau einer SSD



Wear-Leveling

Ein Hauptproblem von Flash-Speicher und damit auch bei SSDs ist die begrenzte Lebensdauer. Je nach Flash-Typ geht eine Speicherzelle nach rund 1.000 bis 100.000 Speichervorgängen kaputt. Zwar wird nicht der gesamte Speicher zerstört. Doch es machen sich Verschleißerscheinungen bemerkbar, die auch zu Datenverlust führen können. Deshalb ist eine ständig auf den Speicher schreibende Anwendung für Flash-Speicher eher ungeeignet.

Wear-Leveling sind eine Kombination aus Verfahren und Mechanismen, die die Lebensdauer von Flash-Speicher insbesondere in SSDs verlängern. Beispielsweise verteilt der Flash-Controller die Schreibzugriffe gleichmäßig über alle Speicherzellen. So müssen einzelne Speicherblöcke nicht durch ständige Speicherzugriffe leiden.
Über die exakte Arbeitsweise der Wear-Leveling-Algorithmen ist wenig bekannt. Die SSD-Controller-Hersteller halten sie verständlicherweise unter Verschluss. Doch soviel ist bekannt, man unterscheidet zwischen dynamischen und statischen Wear-Leveling.

Beim dynamischen Wear-Leveling verteilt der Flash-Controller die Schreibzugriffe gleichmäßig über die freien oder frei werdenden Blöcke. Dabei nutzen sich Bereiche, die häufiger geändert werden stark ab und fallen irgendwann aus. Deshalb verschiebt man beim statischen Wear-Leveling immer mal wieder Daten in stark abgenutzte Bereiche, die sich nicht oder selten ändern. Auf dieses Weise wird der Ausfallzeitpunkt einzelner Zellen hinausgezögert. Das erhöht die Lebensdauer des Flash-Speichers. Die zusätzlichen Lese- und Schreibzugriffe kosten jedoch Performance.

Beim statischen Wear-Leveling macht sich jedoch ein Mechanismus des Betriebssystems negativ bemerkbar. Denn beim Löschen von Dateien bekommt der Flash-Controller nichts mit. Lediglich ein paar Bit im Dateinamen und der Dateistruktur ändern sich. So merkt sich das Betriebssystem, dass der Platz anderweitig genutzt werden kann. So kann es passieren, dass der Flash-Controller beim statischen Wear-Leveling mit viel Aufwand Daten verschiebt, die bereits vom Anwender gelöscht wurden. Genau aus diesem Grund ist ein vom Betriebssystem frisch formatierter Speicher aus Sicht des Flash-Controllers nahezu voll. Deshalb gibt es das Trim-Kommando mit dem das Betriebssystem dem Flash-Controller mitteilt, welche Speicherbereiche es nicht mehr braucht.

Als Anwender kann man der Belastung der Speicherzellen dadurch entgegenwirken, dass man das Speichermedium im Vergleich zur schreibenden Datenmenge sehr groß wählt. Dadurch kommt jede einzelne Zelle seltener an die Reihe. Mit der Größe der Speicherkapazität steigert also indirekt auch die Lebensdauer.
Wenn also eine SSD nur wenig befüllt ist, hat der Controller keine Schwierigkeiten die Daten auf dem Speicher zu verteilen. Erst bei zunehmender Speicherbelegung gehen dem Controller die unbelegten Speicherblöcke aus und er muss die Daten auf verschiedene Blöcke verteilen. Wenn dann nur noch teilweise beschriebene Blöcke vorhanden sind, dann muss der Controller diese Blöcke lesen, modifizieren und wieder zurückschreiben. Das kostet Zeit und macht sich mit größeren Verzögerungszeiten und geringen Transferraten bemerkbar. Aus diesem Grund werden SSDs im Lauf der Zeit beim Schreiben immer langsamer.

Um diesen Effekt möglichst lange hinauszuzögern, ist es empfehlenswert Defragmentierung, Dateiindexierung und Prefetching des Betriebssystems abzuschalten. SSDs brauchen diese Optimierungsmechanismen aufgrund ihrer geringen Lesezugriffszeit überhaupt nicht. Im Gegenteil. Sie schaden, weil unnötigerweise sehr viele zusätzliche Schreibzugriffe anfallen. Dadurch brauchen normale Schreibzugriffe länger und die Lebensdauer des Flash-Speichers reduziert sich.

Bad Block Management / Defect Management

Das Bad Block Management bzw. Defect Management überwacht die Flash-Speicherzellen auf Abnutzung. Wird eine Speicherzelle zu stark abgenutzt und steht kurz vor einem Ausfall, wird ein ganzer Zellenblock als fehlerhaft markiert und als Ersatz ein Zellenblock aus der Reserve ersetzt. Bei SLC-SSDs ist die Gefahr der Abnutzung nicht so groß. Hier steht in der Regel eine Reserve von 2% der Gesamtspeicherkapazität zur Verfügung. Bei MLC-SSDs ist die Abnutzung größer. Hier steht in der Regel eine Reserve von 7% zur Verfügung.
Durch das Bad Block Management verliert eine SSD auch nach Jahren und großer Beanspruchung keine Speicherzellen. Die Lebensdauer, Zuverlässigkeit und Speicherkapazität einer SSD bleiben so längerfristig erhalten.

Error Correction Code / Error Detection Code

Bei ECC und EDC geht es um das Erkennen und die Korrektur von Bitfehlern. Die Anzahl der Bitfehler nimmt zu, wenn eine Flashzelle in die Nähe ihrer maximalen Schreib-/Löschzyklen kommt. In dem Fall schlägt das Bad Block Management zu. Doch schon vorher kann es zu einem Bitfehler kommen. Die Folgen könnten zum Beispiel Datenverlust oder inkonsistente Daten sein. Bei MLC-SSDs kommen 24 Bit für die Fehlerkorrektur auf 1 kByte. Bei SLC-SSDs kommen nur 8 Bit für die Fehlerkorrektur auf 512 Byte. Die Gefahr durch Bitfehler ist bei SLC-SSDs geringer.

Garbage Collection

Hinter Garbage Collection steckt ein Hintergrundprozess, der vom Betriebssystem mit dem TRIM-Befehl angestoßen wird.
Da beim Löschen einer Datei nur der Name im Dateisystem gelöscht wird und die eigentliche Informationen in den Speicherzellen erhalten bleiben kann das Betriebssystem nicht geleerte Speicherzellen prüfen und leeren lassen. Dadurch steigt die Schreibgeschwindigkeit bei gelöschten Zellen

Haltbarkeit und Zuverlässigkeit von SSDs

Es wurde bereits die begrenzte Lebensdauer von Flash-Speicher und damit von SSDs angesprochen. Hierzu gibt es folgende Erkenntnisse:
Die Anzahl der möglichen Schreib- bzw. Löschzyklen lässt keine direkten Rückschlüsse auf die Haltbarkeit oder die Zuverlässigkeit zu. Anders als bei Festplatten besteht zwischen den Speicherzellen und den Sektoren des Dateisystems keine direkte Zuordnung. Generell verteilt der Flash-Controller die Schreibzugriffe gleichmäßig über alle Zellen. Die Daten in Zellen, die mit selten veränderten Daten, wie Betriebssystem und Programmen belegt sind, werden ab und zu umgeschichtet, um so wieder weniger stark abgenutzte Zellen zu bekommen.
Generell kann man davon ausgehen, dass SSDs im alltäglichen Desktop-Betrieb länger halten, als von den Herstellern angegeben. 3.000 bis 100.000 Speicher- bzw. Löschzyklen sind für die meisten Anwendungen vollkommen ausreichend. Außerdem wird mit zusätzlichem technischen Aufwand die Anzahl der Zugriffe auf die Speicherzellen verringert.

Prinzipiell darf man sich von den Angaben zur Lebensdauer von Flash-Speicher nicht irritieren lassen. Alle SSD-Controller verteilen die Schreibzugriffe mit Wear-Leveling-Algorithmen gleichmäßig über alle Speicherzellen. Zusätzlich korrigieren ECC-Verfahren eventuelle Fehler.
Die Webseite "The Tech Report" hat hierzu einige SSDs einem Langzeittest unterzogen. Hierbei kam heraus, dass die Datenmenge, die auf eine SSD geschrieben werden muss, um sie zu zerstören, zwischen 700 TByte und 1 PByte liegt. Das ist 10 mal mehr als die Hersteller garantieren. Beispielsweise beträgt die Garantie bei einer SSD von Sandisk bei 80 TByte geschriebenen Daten in 10 Jahren. Hierbei der Hinweis, dass das für Server-SSDs zu wenig ist. Bei einem gewöhnlichen PC oder einem Notebook mit typischer Nutzung müsste man schon mehr als 20 GByte pro Tag auf die SSD schreiben, um die SSD ins Nirvana zu schicken. Das ist dann doch eher unwahrscheinlich. Das Schreiben kommt in typischen Client-Systemen sehr viel seltener vor als Lesen.
Diese Tests sind schon etwas älter und damit nicht auf aktuelle SSDs und Flash-Controller übertragbar. Allerdings ist ersichtlich, dass die Gefahr eines Ausfalls einer SSD bei angemessener Nutzung eher unwahrscheinlich ist. Angemessen bedeutet, dass die richtige SSD für den jeweiligen Einsatzzweck anhand ihrer Parameter und Leistungsangaben ausgewählt wurde.

Wenn bei einer SSD irgendwann mal die Verschleißgrenze erreicht ist, dann stellt sie ihren Betrieb unter Umständen in einer äußerst unangenehmen Form ein. Sie lässt sich überhaupt nicht mehr ansprechen und das ohne Vorwarnung. Aber das ist bei herkömmlichen Festplatten nicht anders.

Preis und Speicherkapazität

SSDs sind im Vergleich zu herkömmlichen, magnetischen Festplatten relativ teuer. Während Festplatten pro Gigabyte billiger werden, ist das bei SSDs nicht immer der Fall. Je nach Flächendichte, Performance und Technik ergeben sich unterschiedliche Preise.
Außerdem ist die Speicherkapazität noch begrenzt. Während man bei herkömmlichen Festplatten schon weit im TByte bereich ist, liegt man bei SSDs noch weit darunter (Stand Mitte 2014).

Übersicht: SSD-Schnittstellen

Wegen immer schnellerer Flash-Speicher und -Controller nimmt die Geschwindigkeit von SSDs unaufhörlich zu. Da SSDs als Festplatten-Ersatz dienen, ist die SATA- bzw. SAS-Schnittstelle als Massenspeicher-Schnittstelle hier maßgeblich im Einsatz. Im Vergleich zur Weiterentwicklung

von SSDs bleibt die Weiterentwicklung von SATA leider zurück. Während es schon SSDs gibt, die Daten mit 2 GByte/s schaufeln können, hängt SATA 6G bei 600 MByte/s bzw. SAS bei 1,2 GByte/s fest. In der Praxis können SATA-6G-Desktop-Festplatten Daten linear mit ca. 180 MByte/s lesen. Sehr schnelle Server-Festplatten erreichen ca. 250 MByte/s. Mit der bisherigen Übertragungstechnik und den dazugehörigen Steckverbindern ist es leider nicht möglich, die Datenrate von SATA zu steigern.

- SSD in Form einer 2,5-Zoll-Festplatte mit SATA 6G (aktuell)
- SSD in Form einer Speicherkarte mit m.2-Anschluss (aktuell)
- SSD in Form einer 2,5-Zoll-Festplatte mit SATAe (zukünftige Form)

Vermeintliche PCIe-SSD-Steckkarten für Server und Worksstations benutzen einen integrierten SATA- oder SAS-Hostadapter für die Anbindung des Flash-Speicher. Das bedeutet, trotz PCIe-Anbindung wird intern bei den meisten SSDs mit SATA 6G gearbeitet. Es ist jedoch davon auszugehen, dass sich PCIe mit m.2 oder SATAe in Workstations und Servern durchsetzen wird. Sicher ist auch, dass sich bei SSDs der PCIe als Standardschnittstelle durchsetzen wird. Was noch nicht sicher ist, welche Steckverbindung und Bauform das sein wird. Während m.2-Steckplätze bei allen Motherboard-Herstellern zumindest auf den teuren Motherboards aufgelötet sind, ist die Resonanz für SATA Express durchwachsen.

In Zukunft soll der PCI Express (PCIe) als Basis für Massenspeicher-Schnittstellen dienen. PCI Express erreicht pro Lane 500 MByte/s (Version 2.0) oder 1.000 MByte/s (Version 3.0). Bündelt man mehrere Lanes kann man in Zukunft sehr schnelle SSDs möglich machen.

SSD vs. Festplatte

Obwohl die SSD in den letzten Jahren sich immer mehr durchgesetzt hat, hat die klassische Festplatte immer noch ihre Daseinsberechtigung. Trotz der typischen Vorteile, wie hohe Geschwindigkeit bei nicht-sequenziellen Zugriffen und niedrigen Energieverbrauch ist eine SSD nicht zwangsläufig der bessere Datenspeicher. Mit einem Blick auf Speicherkapazität, Preis und Zuverlässigkeit spricht mehr für die herkömmliche Festplatte.

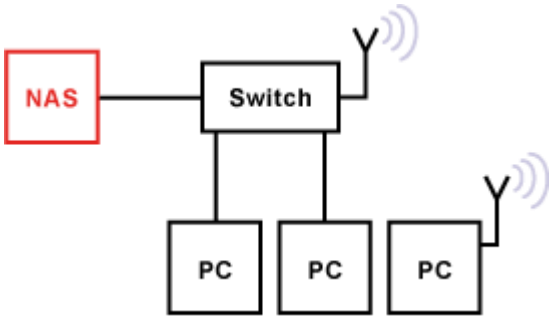
Hohe Performance erreichen SSDs bisher nur mit rechenstarken Controllern, die ausgefeilte Wear-Leveling-Algorithmen beherrschen, viele Flash-Chips parallel anbinden und SDRAM-Cache nutzen. Eine Zwischenlösung zwischen Festplatten und SSDs sind Hybrid-Festplatten (SSHD, Solid-State Hybrid Drives), die neben dem Plattenspeicher auch einen Chip-Speicher haben, der das Booten des Betriebssystems und den Start von Anwendungen beschleunigen kann.

75. Unterschiede im Datenzugriff bei NAS und SAN

Der Unterschied liegt im Zugriffsprotokoll. Während sich die virtuellen Teile eines SAN als blockorientierte Laufwerke in den Server einklinken, tritt das NAS als eigenständiger Fileserver in Erscheinung. Hier kann man über Protokolle wie NFS, CIFS, HTTP, FTP oder SMB zugreifen. Während Speichernetze (SAN) die Server mit virtuellen Speichern verbinden, arbeiten NAS-Server auf Dateiebene. In Form eines Gateways kann der NAS-Server aber auch als Kopf eines Speichernetzwerks dienen.

76. NAS

NAS - Network Attached Storage



Ein NAS ist ein konfigurierbarer Datenspeicher, um in einem Netzwerk Speicherplatz zur Verfügung zu stellen. Beim NAS sind die Festplatten an keinen Server gebunden, sondern in Summe als eine 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 bezeichnet man als NAS. Der Zugriff wird nicht zentral, sondern im NAS geregelt. Entweder steht der Speicherplatz allen Netzwerkteilnehmern zur Verfügung oder wird benutzerabhängig aufgeteilt. In der Regel ist die Benutzer-, Gruppen- und Passwort-Verwaltung sind nur in einfacher Form integriert. Betreibt man mehrere NAS muss man jedes neu konfigurieren.

Typische Leistungsmerkmale

- 24h-Stunden-Betrieb
- Datensicherheit durch RAID und Datenspiegelung
- Hot-Plug der Laufwerke möglich
- Protokolle: SMB, CIFS, AFP, NFS
- Active Directory Integration
- UPnP-Medien-Server
- USB-Schnittstelle zur Erweiterung oder für Printserver (Netzwerkdrucker)

Manche Hersteller integrieren eigene Schnittstellen, Protokolle und Dateisysteme, anstatt sich an Standards zu halten. Manchmal ist man auf eine Client-Software angewiesen, die man installieren muss.

Anwendungen

- Speicherlösung im SOHO-Bereich
- Wenn es darum geht, schnell und unkompliziert Speicher bereitstellen, dann ist ein NAS die optimale Lösung.

Server oder NAS?

Beim Betrieb eines File-Servers oder eines NAS scheint es auf den ersten Blick kaum einen Unterschied zu geben.
Im Prinzip spielt die Verfügbarkeit der Daten beim Betrieb eines Servers oder NAS eine große Rolle. So sind die Daten auf einem NAS mit RAID mindestens genauso sicher wie auf einem

Server mit RAID. Wenn es aber darum geht Backups und Archive anzulegen, dann ist ein Server mit einem vollwertigen Betriebssystem und frei installierbaren Anwendungen flexibler. Ein NAS ist eben nur ein Netzwerkspeicher. Die meisten NAS-Systeme haben zwar zusätzliche Funktionen. Ob die das können, was man braucht, muss erst überprüft und getestet werden.

Außerdem ist der Betrieb eines NAS kritisch zu betrachten. Wenn von NAS die Rede ist, dann sind damit meist Geräte einfacher Bauart gemeint, die nur als Netzwerk-Festplatten zu gebrauchen sind. Dabei spielt es keine Rolle, ob das NAS RAID-fähig ist oder nicht. In der Regel wird das RAID über ein Linux-Betriebssytem mit dem mdadm-Tool erzeugt. Die Festplatten werden dabei zu einem Software-RAID zusammengeschaltet. Es handelt sich dabei um kein echtes RAID. Bei einem Hardware-Ausfall kommt man nur mit erhöhtem Aufwand an die Daten ran.
Wegen der systembedingten Nachteile behaupten böse Zungen, dass die Abkürzung NAS "Nur aus Spaß" bedeutet.

77. Formate und Arten von Hashes (MD5 und SHA-1)

Kryptografische Hash-Funktionen

Kryptografische Hash-Funktionen sind ein wichtiges kryptografisches Instrument und bilden einen eigenen Bereich in der Kryptografie. Kryptografische Hash-Funktionen generieren aus beliebig langen Datensätzen eine Zeichenkette mit einer festen Länge (Angabe in Bit). Ein Datensatz kann ein Wort, ein Satz, ein längerer Text oder auch eine ganze Datei sein.
Die erzeugte Zeichenkette wird als digitaler Fingerabdruck (Fingerprint), kryptografische Prüfsumme, Message Digest (MD) oder Message Authentication Code (MAC) bezeichnet. Gemeint ist damit in der Regel immer der sogenannte Hash-Wert oder auch nur Hash.

Das Bilden eines Hash-Werts hat erst einmal nichts mit Kryptografie zu tun. Denn nicht alle Hash-Funktionen sind nach den Gesichtspunkten der Kryptografie eine kryptografische Hash-Funktion. Für "echte" kryptografische Hash-Funktionen gibt es die unterschiedlichsten Begriffe und zusätzlich auch noch Produktbezeichnungen oder Leistungsmerkmale, die allerdings nichts darüber aussagen, ob sie kryptografischen Anforderungen entsprechen.

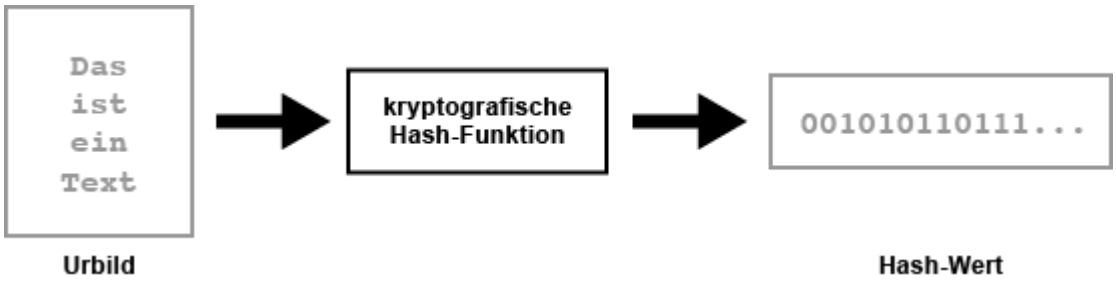
- Footprint-Funktion
- sichere Hash-Funktion
- Manipulation Detection Code (MDC)
- Message Integrity Code (MIC)
- Prüfsummenverfahren

Anforderungen an kryptografische Hash-Funktionen

- Eindeutigkeit: Eine identische Zeichenfolge muss zum selben Hash-Wert führen.
- Reversibilität: Der Hash-Wert darf nicht in die ursprüngliche Zeichenfolge zurückberechnet werden können.
- Kollisionsresistenz: Zwei unterschiedliche Zeichenfolgen dürfen nicht den gleichen Hash-Wert ergeben.

Nicht alle Hash-Funktionen erfüllen alle diese Anforderungen. Deshalb eignen sich nicht alle Hash-Funktionen für kryptografische Anwendungen, wie Authentisierung und Verschlüsselung.

Funktionsweise einer kryptografischen Hash-Funktion



Im Prinzip erzeugt eine Hash-Funktion aus einem Datensatz, das als Urbild oder im Englischen Preimage bezeichnet wird, eine duale Zahl, die meist in hexadezimaler Schreibweise dargestellt und als Hash-Wert bezeichnet wird.
Die Funktionsweise einer kryptografischen Hash-Funktion basiert auf einer Einwegfunktion, die sich sehr einfach rechnen lässt, aber deren Umkehrung dagegen sehr aufwendig bis unmöglich ist. Die Umkehrung vom Hash-Wert auf das Urbild zu schließen ist das was man verhindern möchte.

Reversibilität

Grundsätzlich sollte es nicht möglich sein aus einem Hash-Wert die ursprünglichen Daten zurückzuberechnen. Weil mit der Zeit doch Möglichkeiten gefunden werden und die Rechenleistung steigt, gibt es immer bessere Verfahren aus einem Hash-Wert die ursprünglichen Daten zurück zu berechnen. Deshalb stellt sich mit der Zeit immer wieder heraus, dass Hash-Funktionen reversibel sind.

Kollisionsresistenz

Prinzipiell ist es so, dass ein Urbild beliebig viele Stellen und beliebig viele Werte einnehmen kann. Ein Hash-Wert ist allerdings auf eine bestimmte Länge begrenzt. So kann es vorkommen, dass ein beliebiger Hash-Wert unterschiedlichen Urbildern entspricht. Man spricht dann von einer Kollision. Bei einer guten Hash-Funktion sollte eine Kollision so wenige wie möglich vorkommen. Nehmen wir als Beispiel die Quersummenbildung. Hier kann es vorkommen, dass die Quersumme mehreren Zahlenwerten entsprechen kann. Aus Sicht der Kryptografie ist eine Quersumme also keine kryptografische Hash-Funktion.
Die Kryptografie stellt an Hash-Funktionen und ihre Anwendungen höhere Anforderungen. Es sollte für einen Angreifer unmöglich sein Kollisionen zu erzeugen.

- Statistisch gesehen sollte jeder Hash-Wert etwa gleich oft vorkommen.
- Der Hash-Wert sollte auch bei kleinen Änderungen des Urbilds anders sein.

Um die Wahrscheinlichkeit von Kollisionen zu vermeiden, verwendet man immer bessere Verfahren, die meist längere Hash-Werte erzeugen.
Beispielsweise sind die bekannten und beliebten Hash-Funktionen MD5 und SHA1 für Kollisions-Attacken verwundbar. Damit ist gemeint, dass ein anderer Datensatz den gleichen Hash-Wert erzeugen kann. Das heißt, dass ein MD5- oder SHA1-Hash nicht einzigartig ist. Besser ist es, SHA256 oder gleich SHA512 zu verwenden.

Angriffe auf kryptografische Hash-Funktionen

Ein Angriff auf eine kryptografische Hash-Funktion sieht vor, das Urbild zu erhalten. Es sind mehrere Möglichkeiten bekannt.

- Substitutionsangriff
- Geburtstagsangriff
- Wörterbuchangriff
- Regenbogentabelle

Gegen die ersten beiden Angriffe kann man sich nur durch ausreichend lange Hash-Werte schützen. Diese sollten länger sein, als die empfohlene Schlüssellänge für symmetrische Verfahren. 160 Bit gelten als das absolute Minimum.

Der mit Abstand häufigste Angriff ist der Wörterbuchangriff. Er ist am erfolgreichsten. Er funktioniert dann am besten, wenn das Urbild aus einem Wort besteht. Vielleicht sogar ein Begriff, der sich in einem Wörterbuch befindet.
Wörterbuchangriffe werden besonders auf Passwörter angewendet, die als Hash-Wert in einer Benutzerdatenbank abgelegt sind.
Erschweren kann man es dem Angreifer, wenn man vom erzeugten Hash-Wert mehrmals einen Hash-Wert erzeugt. Auch bei mehreren hundert Durchläufen sollte sich selten ein Performance-Problem einstellen. Ein Angreifer muss allerdings genauso viele Durchläufe machen, um auf den richtigen Hash-Wert zu kommen. Und das für sein ganzes Wörterbuch.

Schlüsselabhängige Hash-Funktionen

Typischerweise arbeiten kryptografische Hash-Funktionen ohne einen Schlüssel. In der Regel ist es egal, wenn der Angreifer weiß, um welche Hash-Funktion angewendet wird. Bei den meisten Anwendungen geht es darum, eine Art Prüfsumme zu bilden oder Datenspeicherung oder-übertragung im Klartext zu vermeiden.

Es gibt allerdings auch Anwendungen, wo für die Berechnung eines Hash-Werts ein geheimer Schlüssel von Vorteil wäre, den der Angreifer nicht kennt. Beispielsweise dann, wenn zwei Kommunikationsteilnehmer bereits einen geheimen Sitzungsschlüssel ausgetauscht haben. In so einem Fall spricht man von einer schlüsselabhängigen Hash-Funktion. Wobei häufig von einem Message Authenticaton Code (MAC) gesprochen wird.

Die Frage ist jetzt, warum braucht man eine schlüsselabhängige Hash-Funktion, wenn es Signaturverfahren gibt. Denn ein Signaturverfahren wäre genau das. Allerdings braucht eine schlüsselabhängige Hash-Funktion wesentlich weniger Rechenzeit und kommt mit kürzeren Schlüsseln aus. Die digitale Signatur ist deshalb aber nicht überflüssig. Im Gegenteil. Wenn es um Verbindlichkeit geht, dann kommt man ohne die digitale Signatur nicht aus. Denn die digitale Signatur kann nur derjenige anfertigen, der den privaten Schlüssel des Schlüsselpaares hat. Würden Sender und Empfänger dagegen nur einen Schlüssel vereinbaren und eine schlüsselabhängige Hash-Funktion anwenden, könnte der Empfänger dem Sender nichts beweisen. Weil den geheimen Schlüssel hätte ja jeder haben können.

Der Unterschied zwischen schlüsselabhängiger Hash-Funktion und einer normalen Hash-Funktion liegt im unterschiedlichen Sicherheitsziel. Der bevorzugte Angriff bei der schlüsselabhängigen Hash-Funktion liegt im Herausbekommen des Schlüssels. Bei der normalen Hash-Funktion will der Angreifer Kollisionen finden.
Bei einer schlüsselabhängigen Hash-Funktion ähneln die Angriffe denen bei einer symmetrischen Verschlüsselung. Beispielsweise ein Known-Preimage- oder Chosen-Preimage-Angriff.

Anwendungen von kryptografischen Hash-Funktionen

- Pseudozufallsgenerator
- Mischer für Zufallsquellen
- Sitzungsschlüssel aus Masterschlüssel ableiten
- Generator für Einmal-Passwörter
- Verfahren für die Authentifizierung (Digitale Signatur)
- Speichern von Passwörtern
- Bilden kryptografischer Prüfsummen
- Integritätsprüfung

SHA - Secure Hash Algorithm (SHA-1 / SHA-2 / SHA-3)

Der Secure Hash Algorithm, kurz SHA, und alle seine Versionen, sind kryptografische Hash-Funktionen. Entwickelt wurde SHA vom US-Geheimdienst NSA im Auftrag der US-Standardisierungsbehöre NIST.
SHA wurde zusammen mit dem Signaturverfahren DSA im Jahr 1991 der Öffentlichkeit vorgestellt. Obwohl Entwicklungen der NSA immer mit Misstrauen gesehen werden, stellte sich SHA als gute kryptografische Hash-Funktion heraus.

SHA kommt in allen gängigen Webanwendungen und Netzwerk-Protokollen zum Einsatz. PGP, SSL, IPsec und S/MIME. Und natürlich bei verschiedenen Signaturverfahren. Zum Beispiel zum Signieren von Zertifikaten.

Das ursprüngliche SHA wird als SHA-1 bezeichnet, um es von seinen Nachfolgern SHA-2 und SHA-3 unterscheiden zu können. SHA-3 soll SHA-2 nicht ersetzen, sondern ist eine Alternative. Sollte SHA-2 irgendwann einmal gebrochen werden, kann man zu SHA-3 übergehen.

MD4 - Message Digest 4

MD4 wurde von RSA-Miterfinder Ron Rivest entwickelt. Die meisten kryptografischen Hash-Funktionen sind Weiterentwicklungen von MD4. Es hat einige Schwächen, weshalb es nicht allzu sicher ist und für kryptografische Anwendungen nicht mehr verwendet werden sollte.

MD5 - Message Digest 5

Aufgrund der Schwächen von MD4 hat Ron Rivest eine überarbeitete Version mit der Bezeichnung MD5 im Jahr 1991 veröffentlicht, wodurch es vorübergehend zur meistverwendeten kryptografischen Hash-Funktion wurde. Allerdings sollte man MD5 nicht mehr verwenden, weil es auch mit einem normalen PC möglich ist, Kollisionen innerhalb weniger Stunden zu berechnen. Aber, für nicht-kryptografische Anwendungen ist MD5 immer noch akzeptabel.

SHA-1 - Secure Hash Algorithm Version 1

SHA-1 ist eine Weiterentwicklung von MD4 und war in den 1990er Jahren die wichtigste kryptografische Hash-Funktion. Aus diesem Grund ist sie heute immer noch weit verbreitet. Obwohl SHA-1 seit 2004 nicht mehr als sicher gilt, ist es bei vielen verschlüsselten Verbindungen und Zertifikaten immer noch im Einsatz.
SHA-1 ist anfällig für Kollisionsangriffe. Das haben chinesische Kryptografen herausgefunden. Praktikabel sind diese Angriffe seit 2009, wenn auch sehr aufwendig und damit teuer, dass eigentlich nur staatlich finanzierte Angriffe durch Geheimdienste zu befürchten sind. Trotzdem oder gerade deshalb sollte man SHA-1 in Neuentwicklungen vermeiden.

Der Grund, warum die meisten Webseiten immer noch SHA-1 für die Signatur von SSL/TLS-Zertifikaten verwenden, liegt daran, dass die Webseiten-Betreiber ihre Zertifikaten nicht selbst erstellen, sondern von Zertifizierungsstellen, sogenannten Certificate Authorities (CAs), beziehen müssen. Nur deren Zertifikate sind in den gängigen Web-Browsern vorinstalliert und werden als vertrauenswürdig akzeptiert. Leider stellen diese CAs zum Großteil ihre Zertifikate immer noch mit Hilfe von SHA-1 aus.
Ein Webseiten-Betreiber könnte sich auch ein eigenes Zertifikat ausstellen, dass mit Hilfe einer anderen kryptografischen Hash-Funktion signiert wurde. Nur dann löst dieses Zertifikat eine Warnung im Browser der Besucher aus, das er vom kontaktierten Server geliefert bekommt. Um das zu vermeiden nutzen Webseiten-Betreiber Zertifikate von CAs, die mit Hilfe einer unsicheren kryptografischen Funktion signiert und dafür auch noch als vertrauenswürdig akzeptiert werden.

SHA-1 ist bei SSL-Zertifikaten besonders kritisch. Ein Angreifer könnte theoretisch falsche Serverzertifikate erstellen, die von den Browsern als gültig angesehen werden. Das erfordert aktuell zwar noch einen erheblichen Rechenaufwand, den bestenfalls Geheimdienste leisten können. Es ist allerdings nicht auszuschließen, dass nicht irgendwann auch Kriminelle diese Fähigkeit erlangen können.
Der Wechsel auf ein moderneres Hash-Verfahren wie SHA-2 und SHA-3 ist angebracht.

SHA-2 - Secure Hash Algorithm Version 2

Schon vor Bekanntwerden der Schwächen von SHA-1 hat die NIST im Jahr 2000 vier neue SHA-Versionen standardisiert: SHA-224, SHA-256, SHA-384 und SHA-512. Wobei die Zahl im Namen die Länge des Hash-Werts ausdrückt.
Die neuen Hash-Funktionen unterscheiden sich jedoch nicht nur in ihrer Länge von SHA-1, sondern auch durch eine Reihe funktionaler Unterschiede.
Die Algorithmen des SHA-2-Standards werden auf allen gängigen Betriebssystemen unterstützt und können deshalb SHA-1 ablösen.
Oftmals ist nur von SHA-256 und SHA-512 die Rede. Es gibt aber auch noch SHA-224 und SHA-384. Das liegt daran, weil es sich bei SHA-224 um den selben Ablauf, wie bei SHA-256 handelt, bei dessen Ausgabe am Ende 32 Bit abgeschnitten werden. Genauso bei SHA-384. Hierbei handelt es sich funktional um SHA-512, bei dessen Ausgabe am Ende 128 Bit abgeschnitten werden.

SHA-3 - Secure Hash Algorithm Version 3

SHA-3 basiert auf dem Hashing-Algorithmus Keccak und wurde von der NIST im Jahr 2012 als Nachfolger von SHA-2 bekanntgegeben. Allerdings hatten Krypto-Experten der NIST

vorgeworfen, den Algorithmus im Rahmen von Performance-Optimierungen absichtlich geschwächt zu haben.
SHA-3 gibt es mit 224, 256, 384 und 512 Bit.
SHA-3 soll SHA-2 nicht ersetzen, sondern ist eine Alternative. Sollte SHA-2 irgendwann einmal gebrochen werden, kann man zu SHA-3 übergehen.

78. Netzwerksicherheit

Die globale, wie auch lokale, weltweite Vernetzung hat zu einer großen Bedeutung für die Computer- und Netzwerksicherheit geführt. Wo früher vereinzelt kleine Netze ohne Verbindungen nach außen für sich alleine standen, ist heute jedes noch so kleine Netzwerk mit dem Internet verbunden. So ist es möglich, dass aus allen Teilen der Welt unbekannte Personen, ob mit guter oder böser Absicht, eine Verbindung zu jedem Netzwerk herstellen können.

Die paketorientierte Protokoll-Familie TCP/IP ist speziell dafür ausgelegt, dass eine Ende-zu-Ende-Verbindung für alle am Netzwerk hängenden Stationen möglich ist. Die dabei vorherrschende dezentrale Struktur des Internets erlaubt jedoch kaum eine Kontrolle über den Weg den Datenpakete nehmen. Diese an sich vorteilhafte Eigenschaft, z. B. bei Ausfällen oder Überlastungen von Übertragungsstrecken, macht sich bei der Übertragung von sicherheitsrelevanten Daten und Anwendungen negativ bemerkbar.
Grundsätzlich kann man sagen, dass alle persönlichen und kritischen Daten, die über das unsichere Internet übertragen werden, immer mit einem sicheren Übertragungsprotokoll geschützt sein sollten.

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 dafür die Auseinandersetzung mit völlig neuen Sicherheitsfragen.
Dabei stellt sich die Frage, welche Geräte werden mit welcher Applikation wo innerhalb und außerhalb des Unternehmens und wie und wann eingesetzt? Ein zentrales Problem ist dabei, dass viele mobilen Geräte ursprünglich für den Privatgebrauch und nicht für Unternehmenszwecke entwickelt wurden.

Seit den ersten Veröffentlichungen um die Geheimdienstaktivitäten der NSA und Co. müssen zahlreiche IT-Themen völlig neu bewertet werden.

Die 3 Pfeiler der Netzwerk-Sicherheit

- Integrität
- Vertraulichkeit
- Authentizität

Integrität // Vertraulichkeit // Authentizität

Netzwerksicherheit umfasst drei wesentliche Merkmale. Das eine ist die Integrität. Dazu zählen Mechanismen und Verfahren, die die Echtheit von Daten prüfen und sicherstellen können und somit auch 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 dritte 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

Im echten Leben weisen wir uns durch Unterschriften, Pässe und Karten aus. Im Internet fällt dies durch die räumliche Trennung weg. Auf Sicherheit zu achten bedeutet auch, niemals die Authentifizierung und Autorisierung zu vernachlässigen. Authentifizierung ist der Vorgang, bei dem eine Person oder Maschine auf ihre Identität geprüft wird. Autorisierung ist der Vorgang, bei dem ermittelt wird, was die Person oder Maschine machen darf (Berechtigung).

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	**Application Layer Anwendungsschicht**	**HTTPS S-MIME SSL SSH OpenVPN**
6		
5		

4 3	**Network Layer Netzwerkschicht**	**IPsec (AH/ESP)**
2 1	**Data Link Layer Übertragungsschicht**	**PPTP L2TP PAP/CHAP**

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.

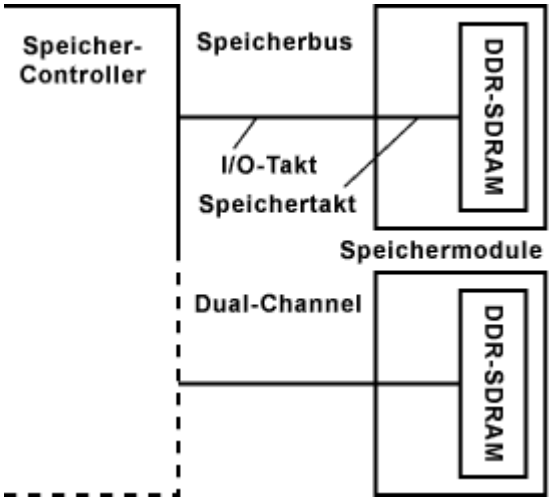
79. Untershiede DDR/DDR-2/DDR-3/DDR-4

DDR-SDRAM entspricht dem normalen SDRAM, jedoch mit einer kleinen Modifikation: Bei der Übertragung der Daten wird nicht nur die ansteigende Flanke, sondern auch die abfallende Flanke des Taktsignals genutzt. In der Praxis entspricht das einer Taktverdopplung. Rein rechnerisch entsteht so eine Verdopplung der Übertragungsrate.

Um eine Verwechslung mit DDR-SDRAM (Double Data Rate) zu vermeiden, wird normales SDRAM als SDR-SDRAM (Single Data Rate) bezeichnet. Fälschlicherweise wird "DDR-SDRAM" auch als "DDR-RAM" oder "DDR-DRAM" bezeichnet. Um Verwechslungen und Missverständnisse zu vermeiden, sollte man die einzig richtige Bezeichnung "DDR-SDRAM" verwenden.

DDR-SDRAM ist die gängigste Speichertechnik. Sie wird nicht nur in Computern, sondern auch in Kraftfahrzeugen, Netzwerken, Kommunikationstechnik, medizinischen Apparaten und in der Unterhaltungselektronik eingesetzt.

Vom Mythos der Verdopplung der Übertragungsrate



Pro Übertragungszyklus werden theoretisch zweimal Daten übertragen. Einmal bei der steigenden und einmal bei der fallenden Taktflanke. Doch Vorsicht, man unterscheidet zwischen internem Speicher-Takt und externem Bus-Takt! Das bedeutet, wenn der Bustakt mit 100 MHz arbeitet und durch DDR rechnerisch mit 200 MHz arbeitet, bedeutet das nicht, dass diese 200 MHz sich in der Praxis als Taktverdopplung auswirken. Denn intern arbeitet der Speicher nur mit 100 MHz. Auf die Speicherchips bezieht sich Double Data Rate (DDR) nicht.
Konkret bedeutet das, die Verdopplung der externen Datentransferrate erreicht man nur durch Prefetching innerhalb des Speichers. Dazu werden einfach zwei (DDR) oder mehr (DDR2, DDR3) Datenbits auf einmal ausgelesen. Die Zugriffsbeschleunigung durch Prefetching funktioniert aber nur dann, wenn der Speichercontroller hintereinander liegende Adressbereiche aus der gleichen Speicherfeldzeile anfordert oder wenn die angeforderten Daten auf unterschiedlichen Speicherbänken liegen. Das bedeutet, die Adresszugriffe müssen optimal auf die internen Speicherbänke verteilt werden, um die Taktverdopplung für eine Verdopplung der Übertragungsrate nutzen zu können.
DDR ist also erst mal nichts weiter als eine Verdopplung der Speicherbusgeschwindigkeit. Erst mit verschiedenen Tricks werden mehr Daten aus dem Speicher gelesen. Beim Prefetching erfolgt das Auslesen der Speicherzellen in Zweier (DDR-SDRAM)- oder Vierergruppen (DDR2-SDRAM).

Um die Speicherbandbreite zu erhöhen kann man die Daten auch gleich aus zwei Speichermodulen anfordern. Man bezeichnete das als Dual-Channel. Dual-Channel bezieht sich nicht auf das Speichermodul, sondern auf den Speicher-Controller. Manche Speicher-Controller können auch mehr als 2 Speichermodule gleichzeitig auslesen.

Bezeichnung

Mit DDR-SDRAM wurde eine neue Speicher-Bezeichnung eingeführt, um die Leistungsfähigkeit der Speichermodule leichter unterscheiden zu können. Die Bezeichnung wurde von der JEDEC offiziell festgelegt. Sie gibt nicht wie ursprünglich die Taktrate an (zum Beispiel PC66, PC100, PC133), sondern die Speicherbandbreite (zum Beispiel PC1600, PC2100). Doch Vorsicht, die Angabe ist nach oben gerundet. PC1600 steht für rund 1,6 GByte/s. Wobei DDR200-Speicherchips verwendet werden. Die physikalische Taktrate beträgt nur 100 MHz. Durch DDR beträgt die rechnerische Taktrate 200 MHz. PC2100 steht für eine Speicherbandbreite von rund 2,1 GByte/s. Wobei DDR266-Speicherchips verwendet werden. Die physikalische Taktrate beträgt 133 MHz. Durch DDR beträgt die rechnerische Taktrate 266 MHz.

Die genaue Erläuterung zur Bezeichnung von Speicherchips und Speichermodulen ist unter PC/PC2/PC3-Spezifikation zu finden.

SDR-SDRAM und DDR-SDRAM im Vergleich

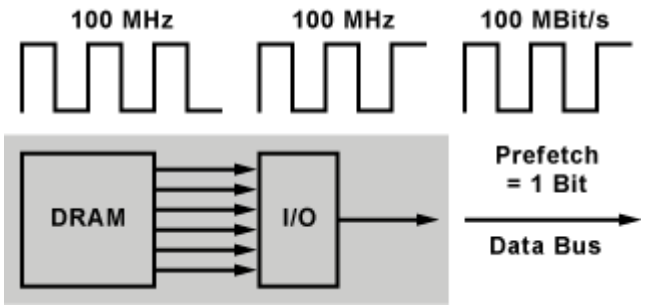
Speichermodul	Speicher-Typ	physikalische Taktfrequenz	genutzte Flanken	rechnerische Taktrate	Interface	Speicher-Bandbreite
PC66	SDR-SDRAM	66 MHz	1	66 MHz	64 Bit	0,50 GByte/s
PC100	SDR-	100 MHz	1	100 MHz	64 Bit	0,75

	SDRAM					GByte/s
PC133	SDR-SDRAM	133 MHz	1	133 MHz	64 Bit	0,99 GByte/s
PC150	SDR-SDRAM	150 MHz	1	150 MHz	64 Bit	1,12 GByte/s
PC166	SDR-SDRAM	166 MHz	1	166 MHz	64 Bit	1,24 GByte/s
PC1600 (PC200)	DDR-SDRAM	100 MHz	2	200 MHz (DDR200)	64 Bit	1,49 GByte/s
PC2100 (PC266)	DDR-SDRAM	133 MHz	2	266 MHz (DDR266)	64 Bit	1,98 GByte/s
PC2700 (PC333)	DDR-SDRAM	166 MHz	2	333 MHz (DDR333)	64 Bit	~ 2,7 GByte/s
PC3200	DDR-SDRAM	200 MHz	2	400 MHz (DDR400)	64 Bit	~ 3,2 GByte/s

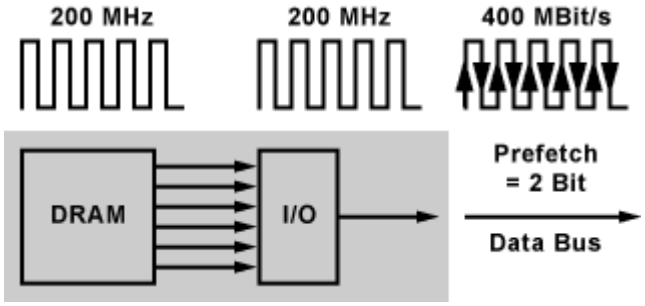
DDR2-SDRAM - Double Data Rate 2 SDRAM

DDR2-SDRAM bietet verschiedene Vorteile gegenüber dem normalen DDR-SDRAM. DDR- und DDR2-Speichermodule (DIMM) arbeiten mit unterschiedlichen Spannungen und unterscheiden sich auch mechanisch voneinander.
DDR2-SDRAM wurde entwickelt, um den Energiebedarf zu reduzieren und die Signalqualität und damit die Systemstabilität zu verbessern. Beides wird durch die Senkung der Frequenz, beispielsweise von 200 MHz auf 100 MHz, und der Spannung, von 2,4 V auf 1,8 V, erreicht.
In der Regel haben DDR2-Speichermodule eine Betriebsspannung von 1,8 oder 1,9V. Liegt sie darüber eignen sich die Speichermodule zum Übertakten.
Die Senkung der Taktfrequenz wurde wegen der schlechten Signalqualität und dem zunehmenden Rauschen notwendig. Der Zeitraum, in dem ein Datensignal als 1 oder 0 erkannt werden kann, reduziert sich bei hoher Frequenz deutlich. Das Signal ist kürzer und deshalb die Erkennung anfälliger für Fehler. Eine weitere Maßnahme ist die Verkürzung der Leitungswege zum Speichercontroller. Zum Beispiel durch On-Die-Terminatoren (ODT). Die ODT-Technik verhindert Reflektionen auf den Signalleitungen und erhöht somit die Systemstabilität. Dabei werden die Abschlusswiderstände vom Speicher-Controller in den Speicherchip implementiert. Das verkürzt die Leitungswege und vermindert das Rauschen durch Reflektionen am Leitungsende.

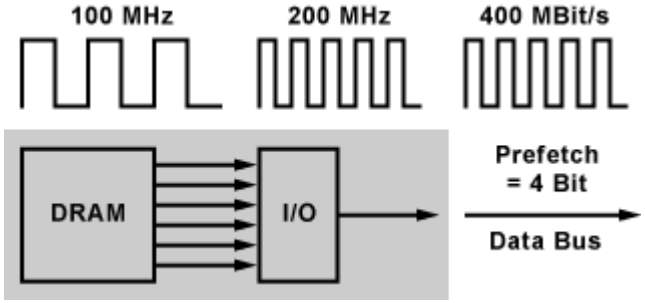
SDR-SDRAM (Beispiel: PC100)



DDR1-SDRAM (Beispiel: DDR1-400)



DDR2-SDRAM (Beispiel: DDR2-400)



DDR2 überträgt die Daten genauso wie DDR1 mit steigender und fallender Taktflanke. Die DDR2-Technik nennt sich QDR und überträgt vier Datenworte pro Takt. Durch ein 4-Bit-Prefetching liefert der interne Speicher vier, anstatt zwei Bit pro Taktschritt an ein Ein-/Ausgabe-Puffer. Somit bleibt die maximale Bandbreite von DDR400 und DDR2-400 mit 3,2 GBit/s gleich. Zur Wiederholung: DDR400 arbeitet intern mit einer Taktfrequenz von 200 MHz, während DDR2-400 nur mit 100 MHz arbeitet. Der externe Speicherbus wird bei beiden Speichertypen mit 200 MHz getaktet.
Bedeutet das, dass DDR2 gegenüber normalem DDR keinen Vorteil hat? Doch, hinsichtlich des Energieverbrauchs und der Systemstabilität schon. Im Lauf der Zeit wurde die interne Speichertaktrate von 100 auf bis zu 266 MHz gesteigert, um parallel dazu auch die

Speicherbandbreite zu erhöhen.
Neben DDR2-400 gibt es auch Speichermodule mit 533er, 667er, 800er und 1066er Speicherchips.

Speichermodul	Speicherchip	Spannung	interner Speichertakt	externer Bustakt	Bandbreite
PC2-3200	**DDR2-400**	1,8 V	100 MHz	200 MHz DDR	3,2 GByte/s (2,98 GByte/s)
PC2-4200	**DDR2-553**	1,8 V	133 MHz	266 MHz DDR	4,2 GByte/s (3,97 GByte/s)
PC2-5300	**DDR2-667**	1,8/2,0 V	166 MHz	333 MHz DDR	5,3 GByte/s (4,97 GByte/s)
PC2-6400	**DDR2-800**	1,8/2,1 V	200 MHz	400 MHz DDR	6,4 GByte/s
PC2-8500	**DDR2-1066**	1,8 V	266 MHz	533 MHz DDR	8,5 GByte/s

DDR3-SDRAM - Double Data Rate 3 SDRAM

Die Nachfrage nach einem schnellen Speicher, der wenig Strom verbraucht, hat zum DDR3-SDRAM geführt. Die Speicherchips werden mit einer Spannung von 1,5V betrieben. Dadurch wird Verlustleistung gespart. Und die Speicherchips eignen sich noch besser für höhere Taktraten.
Die Latenzzeiten der Zugriffe sind bei DDR3 bei gleichem Takt etwas höher als bei DDR2. Höhere Latenzen ermöglichen höhere Taktraten. Durch einen höheren Takt werden die höheren Latenzen wieder ausgeglichen.
Unterscheiden muss man auch bei DDR3 die Taktfrequenz des Speicher-Interfaces und die Speicher-interne Taktrate. Im Speicher beträgt die Taktfrequenz nur ein Viertel des nominellen Takts. Um die Daten trotzdem für die hohe Bandbreite aus den Speicherzellen lesen zu können, sind die Speicherzellen von DDR3-SDRAM gegenüber DDR1-SDRAM mit einem vierfach so breiten Interface angebunden. Nur ein Bruchteil eines einzelnen Speicherchips wird als Speicher verwendet. Der Großteil sind I/O-Einheiten.
DDR3 stellt nichts anderes dar, als die konsequente Fortsetzung des mit DDR2 eingeschlagenen Wegs.

Die DDR3L-Version mit 1,35 V ist eine Stromspar-Variante für Notebooks und Mini-PCs. Die Stromverbrauchsersparnis ist allerdings minimal und lohnt sich wirklich nur für Server mit einem sehr großen Arbeitsspeicher oder für Akku-betriebene Geräte.

Speichermodul	Speicherchip	Spannung	interner Speichertakt	externer Bustakt	Bandbreite
PC3-6400	**DDR3-800**	1,5 V	100 MHz	400 MHz DDR	6,400 GByte/s
PC3-8500	**DDR3-1066**	1,5 V	133 MHz	533 MHZ	8,528 GByte/s

				DDR	
PC3-10600	**DDR3-1333**	1,5 V	166 MHz	667 MHz DDR	10,667 GByte/s
PC3-12800	**DDR3-1600**	1,5 V	200 MHz	800 MHz DDR	12,800 GByte/s
PC3-14900	**DDR3-1866**	1,5 V	233 MHz	933 MHz DDR	14,933 GByte/s
PC3-17000	**DDR3-2133**	1,5 V	266 MHz	1.066 MHz DDR	17,066 GByte/s

Noch ein kurzer Hinweis auf die Geschwindigkeitsklassifizierung der Speicherchips: PC3-8500-Speichermodule haben DDR3-1066-Speicherchips. Die werden nicht mit 1066 MHz, sondern nur mit 533 MHz angesteuert. Die Datenübertragung erfolgt dann mit DDR (Double Data Rate), also sowohl bei steigender als auch bei fallender Taktflanke, wodurch sich rein rechnerisch 1066 MHz ergeben würde.

DDR4-SDRAM - Double Data Rate 4 SDRAM

Seit Mitte 2014 gibt es DDR4-SDRAM-Speichermodule. Es gibt verschiedene Verbesserungen gegenüber DDR3-SDRAM. Dazu zählen höhere Taktfrequenzen,verbesserte DRAM-Chips und Speicher-Controller. Die Taktfrequenzen sind auf 800, 933, 1066 und 1200 MHz festgelegt. Das bedeutet, es gibt DDR4-1600, -1866, -2133 und -2400-Chips. Die Latenzparameter reichen von 10-10-10 bis 18-18-18. Höhere Datentransferraten und eine niedrigere Leistungsaufnahme sind das Ziel. Die Speichermodule (DIMM) laufen mit 1,2 Volt und haben 288 (Desktop und Server) bzw. 256 (Notebooks) Pins. Die Angabe, dass ein DDR4-DIMM 284 Pins hat ist veraltet und damit falsch.

Um höhere Taktfrequenzen zu erreichen bringt DDR4 ein paar technische Neuerungen.Zu den Neuerungen gehört das Übertragungsverfahren POD12 (Pseudo Open-Drain Interface mit 1,2 Volt Nominalspannung). Die Referenzspannungen zur Unterscheidung von High- und Low-Pegeln ist nicht mehr festgelegt, sondern die handeln die Chips untereinander aus. Damit kompensieren sie äußere Einflüsse durch wechselnde Temperaturen, unterschiedlich lange Busleitungen und unterschiedliche SDRAM-Chips.
Bisher wurde der Speicherbus bei jedem neuen DDR-SDRAM beschleunigt, wobei sich das nur auf die externen Anschlüsse der Chips bezog. Doch die Daten müssen natürlich auch schneller in die Speicherzellen geschrieben und ausgelesen werden. Die Zellen lassen sich aber nicht so einfach hochtakten. Bei den vielen Tausend Transistor-Kondensator-Reihen ist es schwierig, die Geschwindigkeit zu halten, wenn auch immer wieder die Strukturen verkleinert werden. Feinere Leiterbahnen haben einen größeren Widerstand und kleinere Kondensatoren nehmen weniger Elektronen (Ladungsträger) auf, was zu schwächeren Signalen führt und damit auch zu empfindlicheren Sense Amplifiern, die den Speicherzellenzustand sicher erkennen müssen. Mehr Geschwindigkeit in den Chips ist da Gift. Deshalb laufen die Speicherchips intern schon seit Jahren nur mit 200 MHz. Damit pro Taktzyklus mehr Daten geliefert werden können greift der DDR-Speicher intern parallel auf mehrere Speicherzellen zu. Diese Parallelisierung des Speicherzellen-Zugriffs wird als Prefetching bezeichnet.

Die erste DDR-Generation arbeitete mit zweifachem Prefetching, DDR2 mit vierfachem und DDR3 mit achtfachem Prefetching. Bei DDR4 wollte man das Prefetching nicht noch mal steigern. Das hätte nur Nachteile gebracht. Denn nur wenn der Inhalt aufeinanderfolgender Speicherzellen auch in unmittelbarer aufeinanderfolgenden Taktzyklen übertragen wird, dann arbeitet Prefetching effizient. Bei DDR3 sind das 64 Byte, was exakt zur Cache Line Length aktueller Prozessoren passt.
Bei DDR4 bleiben das Prefetching mit 64 Byte erhalten und statt dessen die Zugriffe auf die internen Speicherbänke geschickter verteilt. Im Prinzip ist das auch Prefetching, aber eben auf einer anderen Ebene.

Speichermodul	Speicherchip	Spannung	interner Speichertakt	externer Bustakt	Bandbreite
PC4-1600	**DDR4-1600**	1,2 V	100 MHz	800 MHz DDR	12,8 GByte/s
PC4-1866	**DDR4-1866**	1,2 V	133 MHz	933 MHz DDR	14,9 GByte/s
PC4-2133	**DDR4-2133**	1,2 V	166 MHz	1.066 MHz DDR	17,0 GByte/s
PC4-2400	**DDR4-2400**	1,2 V	200 MHz	1.200 MHz DDR	19,2 GByte/s
PC4-3200	**DDR4-3200**	1,2 V		1.600 MHz DDR	25,6 GByte/s

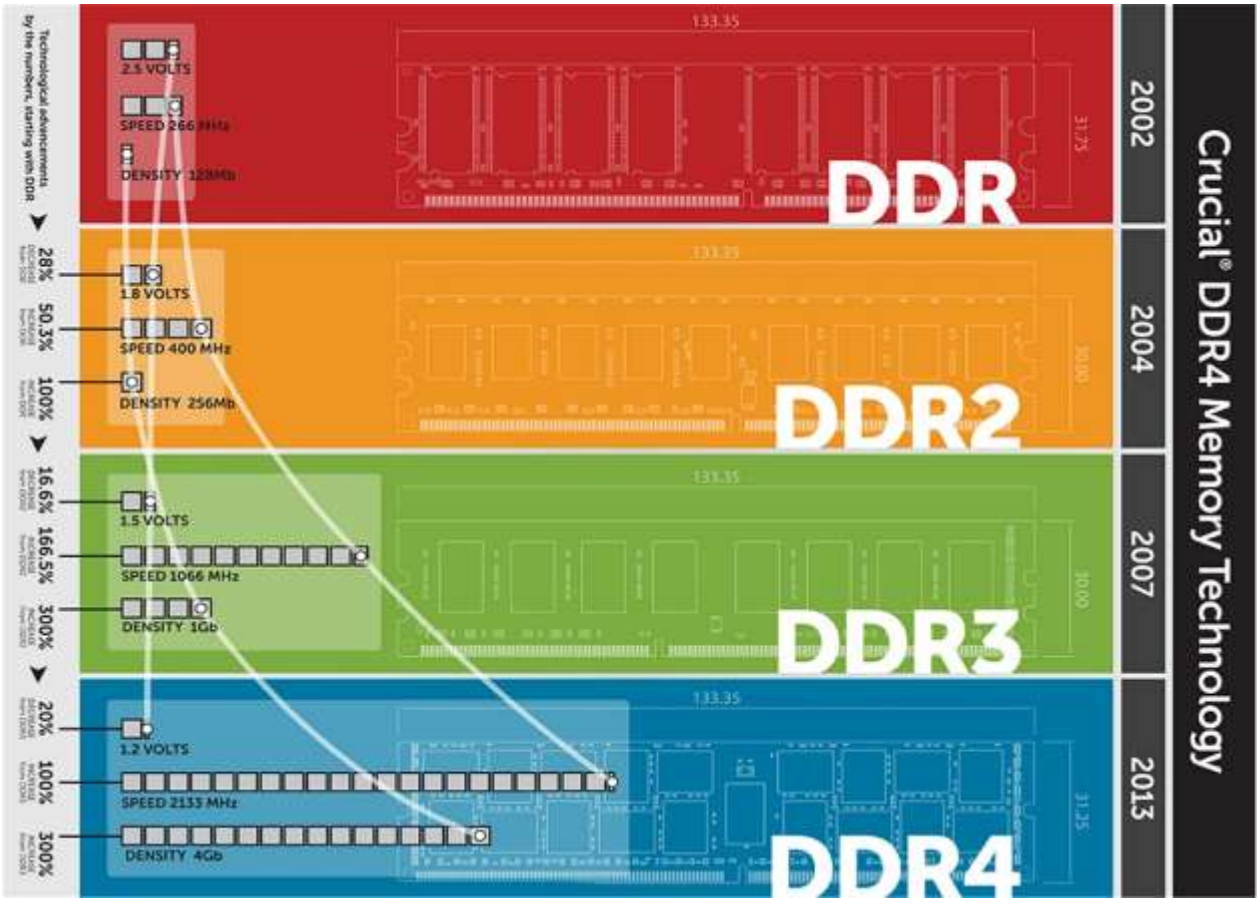
Geändert hat sich mit DDR4 auch die Schreibweise der Bezeichnungen. Ein DIMM-Speichermodul mit DDR3-1600-Chips wird mit PC3-12800 bezeichnet. Im Vergleich dazu wird ein DIMM-Speichermodul mit DDR4-2400-Chips mit PC4-2400 bezeichnet. Während sich bei DDR3, die Bezeichnung der Chips indirekt auf die Taktfrequenz beziehen, hat man das bei DDR4 auf dem Speichermodul übernommen. Ein DDR3-1600-Chip arbeitet mit einer Taktfrequenz von 800 MHz und erreicht mit Double-Data-Rate 1.600 Megatransfers pro Sekunde (MT/s). Das ist aber nicht die eigentliche Datentransferrate. Die ist von der Anzahl der Datenleitungen abhängig. Bei 64 Datenleitungen und 8 Byte pro Transfer ergibt das bei 1.600 MT/s rechnerisch 12,8 GByte/s.
Bei DDR4 kann man nun auf die Taktfrequenz schließen, aber eben nicht mehr so einfach auf die Übertragungsrate des Speicherkanals. Bei PC4-2400 wäre es 19,2 GByte/s. Bei PC4-3200 wäre es 25,6 GByte/s.

DDR1, DDR2, DDR3 und DDR4 im Vergleich

	DDR1	DDR2	DDR3	DDR4
offizielle Taktfrequenzen	100 - 200 MHz (DDR200 - DDR400)	200 - 400 MHz (DDR2/400 - DDR2/1066)	400 - 1066 MHz (DDR3/800 - DDR3/2133)	800 - 1200 MHz (DDR4/1600 - DDR4/2400)

Takt-Verhältnis I/O-Einheiten zu Speicherzellen	1:1	1:2	1:4	1:8
Takt der Speicherzellen	200 MHz bei DDR400	200 MHz bei DDR2/800	200 MHz bei DDR3/1600	200 MHz bei DDR4/2400
nominelle Speicherspannung	2,5 V (± 0,2 V)	1,8 V (± 0,1 V)	1,5 V (± 0,075 V)	1,2 V

DIMM-Speichermodule von DDR1, DDR2 und DDR3 im Vergleich



80. Cloud Computing

Cloud Computing oder Cloud IT umfasst Anwendungen, Daten, Speicherplatz und Rechenleistung aus einem virtuellen Rechenzentrum, das auch Cloud (= Wolke) genannt wird. Die Bezeichnung Cloud wird deshalb verwendet, weil das virtuelle Rechenzentrum aus zusammengeschalteten Computern (Grid) besteht und die Ressource von keinem spezifischen Computer bereitgestellt wird. Die Ressource befindet sich irgendwo in dieser Wolke aus vielen Computern. Eine Anwendung ist keinem Server mehr fest zugeordnet. Die Ressourcen sind dynamisch und bedarfsweise abrufbar.

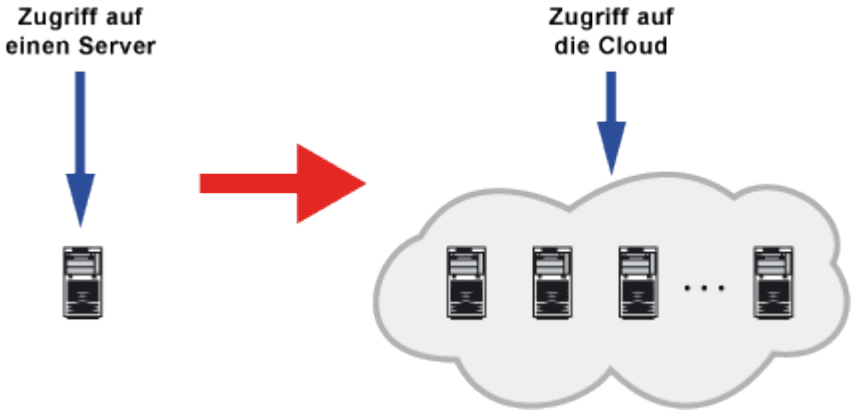
Die meisten Angebote und Leistungen, die unter dem Begriff "Cloud Computing" angeboten werden, sind nicht unbedingt neu. Das Wort Cloud gibt es zwar erst seit 2009, davor gab es dafür verschiedene Produktbezeichnungen. Amazon war der Vorreiter, wurde allerdings nicht ernst genommen. Inzwischen ist das Thema Cloud Computing im IT-Bereich normal. Die Cloud setzt sich vor allem dort durch, wo eine hohe Flexibilität und Skalierbarkeit erforderlich ist. Die Cloud krempelt nicht nur die IT um, sondern auch das Geschäftsmodell der Anbieter. Insbesondere Unternehmen aus der IT-Branche, die bisher Software, Hardware und Serviceleistungen angeboten haben, müssen ich mit den neuen Cloud-Angeboten umstellen.

Die Zukunft der IT liegt in der Cloud. Die Vorteile sind vielfältig. Doch es gibt auch einige Gründe, die dagegen sprechen. Insbesondere das Thema Datenschutz ist ein wichtiges Thema.

Definition von Cloud Computing

So viele Lösungen es gibt, so viele Definitionen zu Cloud Computing gibt es. Eine allgemein gültige Definition von Cloud Computing hat sich noch nicht durchgesetzt. Trotzdem kann man zusammenfassend sagen, dass Cloud Computing eine virtuelle und skalierbare IT-Infrastruktur bereitstellt. Bestandteil von Cloud Computing kann Speicher, Rechenzeit oder komplexe Dienste sein, die über festgelegte Schnittstellen angefordert werden können. Dabei spielt es keine Rolle, auf welcher Hardware diese ausgeführt werden.

Wie funktioniert Cloud Computing?



Bei Cloud Computing verschiebt sich der Ort der Bereitstellung von Speicher, Rechenleistung und Anwendungen von einem einzelnen Server auf mehrere virtuelle Server, die in großen Serverfarmen organisiert werden.
Mit Cloud Computing wird IT zu einem Gebrauchsgut, wie Wasser oder Strom. Die Entwicklung, die IT dabei durchläuft lässt sich mit der industriellen Revolution im frühen 19. Jahrhundert vergleichen. Erst haben Industriebetriebe ihren eigenen Strom produziert, um dann auf ein Versorgermodell zu wechseln, dass den Strom direkt ins Haus lieferte. Damals wie heute setzt das eine Infrastruktur voraus, die heute mit dem Internet und den breitbandigen Anschlüssen faktisch vorhanden ist.
Cloud Computing baut auf Techniken, die für sich alleine ausgereift und praxiserprobt sind. Dazu gehört Virtualisierung, Grid Computing und Provisioning-Software. Ebenso wichtig ist eine hohe verfügbare Bandbreite, die den Zugang zur "Cloud" erst möglich macht.
Wirklich neu an Cloud-Computing ist das Abrechnungsmodell, bei dem der Anwender auch nur das bezahlen muss, was er tatsächlich benötigt.

Formen von Cloud Computing

Dienstebene	Beschreibung	Anbieter	Zielgruppe
Software as a Service (SaaS)	Die Anwendung ist auf dem Server des Anbieters installiert, vorkonfiguriert und wird meist über einen Browser bedient. Auch die Daten, die erstellt und bearbeitet werden, werden dort gespeichert. **Consumer-Cloud-Services, wie Google Docs, Apple iCloud, Strato HiDrive oder die Windows Live Services, sind typiche Software as a Servces.**	Google Apps for Business, Microsoft Online Services, Salesforce.com	Anwender in Unternehmen
Platform as a Service (PaaS)	Im Prinzip handelt es sich hier um ein Betriebssystem, ein technisches Framework oder eine Entwicklungsumgebung, auf der einfache Applikationen entwickelt und betrieben werden können.	Google App Engine, Microsoft Azure Services	IT-Entwickler
Infrastructure as a Service (IaaS)	IaaS bietet Zugriff auf virtualisierte Computer-Ressourcen, beispielsweise Server-Umgebungen, Rechenleistung oder Festplattenspeicher, die nach Bedarf erweitert werden. Bezahlt wird das, was man nutzt bzw. verbraucht. IaaS ist das Cloud-Computing-Modell, auf dem die anderen Modelle aufbauen. IaaS ist das Modell bei dem im großen Maßstab Geld verdient werden kann.	Amazon EC2, Amazon Web Services, IBM Blue Cloud, Microsoft Windows Azure Plattform, VMware vCloud Hybrid Service	IT-Abteilungen IT-Dienstleister Cloud-Services

Cloud-Management-Plattform

Eine Cloud-Management-Plattform verwaltet CPUs, Arbeitsspeicher, Festplatten und virtuelle Maschinen. Die Hardware wird von einer übergeordneten Plattform gesteuert und sorgt dafür, dass die Gesamtheit der Hardware-Ressourcen besser skalieren können. Grob gesehen besteht die Management-Plattform aus einem Scheduler, Storage, Image-Service und einem Interface von dem alles aus bedient wird.

Der Scheduler entscheidet je nach Auslastung der Rechner, auf welchem Rechner eine virtuelle Maschine gestartet wird. Der Image-Service ist für die Zuordnung der Images zu den virtuellen

Maschinen zuständig. Es kümmert sich um die Speicherung und die Auslieferung der Images. Die Storage-Komponente dient zur verteilten und redundanten Speicherung von Daten aller Art. Die Daten werden in Containern und Objekten gespeichert. Container sind so eine Art Verzeichnis, die Objekte enthalten. Objekte können einzelne Dateien sein oder Festplatten-Images virtueller Maschinen.

- OpenStack
- Eucalyptus
- OpenNebula

Warum Cloud Computing?

- Sofern man auf die Cloud eines Dienstleisters zurück greift, hat man die Möglichkeit immer die neuste Technologien einzusetzen.
- Vorausgesetzt, die Ansprüche an die Leistungsfähigkeit und Flexibilität ist nicht zu hoch, besteht die Möglichkeit Kosten zu senken.
- Insgesamt steigt die Flexibilität, wenn mehr Leistungsmerkmale zur Verfügung stehen.
- Outsourcing, gerade im IT-Bereich wird gerne dazu verwendet, Verantwortung zu verschieben. Zum Beispiel an einen Dienstleister, der für die Verfügbarkeit seiner Dienste geradestehen muss.
- Wenn es um die Zusammenarbeit von Mitarbeitern, Kunden, Lieferanten und Partnern geht, sind Anwendungen aus der Cloud meist besser geeignet, als wenn man Zugänge für Fremde ins eigene Netzwerk schaffen muss.
- Der mobile Zugriff auf Unternehmensdaten und Anwendungen für Mitarbeiter, die unterwegs sind, kann über Cloud-Anwendungen einfacher gestaltet werden.

Vorteile und Nutzen durch Cloud Computing

- schnelle Bereitstellungszeit
- zentrale Datenhaltung
- verbrauchsabhängige Abrechnungsmodelle
- skalierbar und flexibel anpassbar

Durch den Verzicht auf langfristige Verträge wäre eine verbrauchsabhängige Abrechnung nach CPU-Stunden oder Speichervolumen denkbar.
Vorstellbar ist, dass Firmen künftig ihre eigene IT-Infrastruktur dynamisch mit zusätzlichen Ressourcen aus der "Cloud" erweitern, die Einführungszeit neuer Anwendungen verkürzen und die Umgebungen an die jeweiligen Anforderungen anpassen.

Nachteile durch Cloud Computing

Die Verfügbarkeit von Daten und Diensten ist ein wesentlicher Knackpunkt. Wenn die Daten außerhalb des eigenen Netzes liegen, dann hat man wenig Einfluss auf das entfernte System. Man ist hier vom jeweiligen Anbieter abhängig. In der Regel ist das kein Problem, wenn man auf die Big Player baut. Ausfälle halten sich hier in Grenzen.
Der Datenschutz ist der zweite Knackpunkt. Hier muss man dem Anbieter vertrauen. Allerdings kann man in Deutschland juristische Probleme bekommen, wenn sensible Daten auf Servern im Ausland liegen oder wenn die Datenverarbeitung im Ausland statt findet.

Private Cloud

Software und Hardware ist immer öfter mit Private-Cloud-Funktionalitäten zu bekommen. Meistens geht es darum, Daten auf unterschiedlichen Geräten miteinander zu synchronisieren oder verfügbar zu machen. Die Cloud ist hierbei der zentrale Datenspeicher. Die Geräte oder Clients bilden den Datenbestand lokal ab und ermöglichen den Zugriff darauf. Durch die Private-Cloud-Angebote lassen sich viele Anwendungen und Dienste bequemer nutzen.

- Google Drive (Google)
- SkyDrive (Microsoft)
- iCloud (Apple)
- Kindle (Amazon)

Im Business-Bereich sind die Geschäftsprozesse meist komplexer, weshalb die Private-Cloud-Angebote in der Regel nur eingeschränkt nutzbar sind. Höchstens noch zur Synchronisation von Kontakten, Terminen und einigen Dokumenten. Doch bereits hier stellt sich die Frage, ob aus Datenschutzgründen auch diese Private-Cloud eher ungeeignet ist.

Wie sicher ist Cloud Computing?

Im Prinzip kommt man angesichts der Veröffentlichungen im Rahmen der NSA-Geheimdiensttätigkeit zu der Erkenntnis, dass man Cloud Computing guten Gewissens nicht empfehlen kann. Allerdings kommt es darauf an, welche Daten in der Cloud gespeichert und welche Daten von Cloud-Anwendungen übertragen werden.

Grundsätzlich sollte man nur die Daten in die Cloud geben, die nicht so sicherheitsrelevant sind. Hier ist dann zur der folgenden Vorgehensweise zu raten: Daten, die vom lokalen Rechner in die Cloud gespeichert werden und von dort auch wieder heruntergeladen werden müssen verschlüsselt übertragen und gespeichert werden. Wenn nicht, kann jede Station auf dem Weg zwischen lokalem Rechner und der Cloud die Daten abgreifen und hat direkten Zugriff darauf.
Meistens werden Cloud-Dienste mit Verschlüsselung angeboten. Sowohl für die Übertragung als auch die Speicherung. Aber, eine Verschlüsselung, die vom Anbieter implementiert ist, ist als nicht wirksam anzusehen, da der private Schlüssel sich im Besitz des Anbieters befindet. Den muss er im Zweifelsfall an Geheimdienste und Behörden ausliefern.
Wer die Cloud als Datenspeicher und Dateiablage verwendet, der sollte die Dateien dort verschlüsselt speichern und verschlüsselt übertragen. Um die Verschlüsselung muss sich der Benutzer selber kümmern und darf sich nicht auf den Cloud-Anbieter verlassen. Andernfalls kann er von der Sicherheit der Daten nicht ausgehen.

81. VDSL

VDSL - Very High Speed Digital Subscriber Line

VDSL ist eine asymmetrische Übertragungstechnik, um im Festnetz einen breitbandigen Internet-Zugang mit hohen Übertragungsraten zu erreichen. In Deutschland wird ein VDSL-Zugang mit Übertragungsraten von 50 bis 100 MBit/s im Downlink (asymmetrisch) angestrebt.
VDSL basiert auf ADSL, ADSL2 und ADSL2+, was man allgemein als DSL bezeichnet. Allerdings wird die Geschwindigkeit von VDSL nur auf einer kurzen Distanz und nur in einem

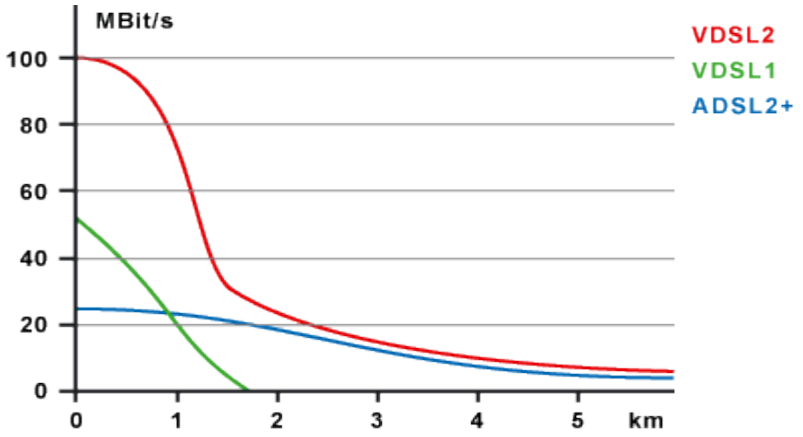
Hybridnetz erreicht. Das ist ein Leitungsweg aus der Kombination von Glasfaser- und Kupferkabel.

Für VDSL gibt es verschiedene Bezeichnungen. Beispielsweise "Very High Data Rate DSL" oder "Very High Bitrate DSL". Doch "Very High Speed Digital Subscriber Line" ist die einzig richtige Bezeichnung. Sie ist im VDSL-Standard der ITU definiert.
Man unterscheidet prinzipiell zwischen zwei verschiedenen VDSL-Standards. Die wurden von der ITU (Internationale Fernmeldeunion) festgelegt:

ITU-Standard	VDSL1 ITU-T G.993.1	VDSL2 ITU-T G.993.2
Spektrale Bandbreite	12 MHz	30 MHz
Reichweite	bis 1 km	bis 3 km
Echokompensation	nein	ja
ADSL-Kompatibilität	nein	ja
Downstream-Sendeleistung	14,5 dBm	max. 20 dBm
Quality of Service	nein	ja
Diagnostik-Modus	nein	ja

Der erste VDSL-Standard (G.993.1) hat sich in Deutschland nicht durchgesetzt. Statt dessen kommt in Deutschland der zweite VDSL-Standard (G.993.2) zum Einsatz. Prinzipiell gibt es einige Gemeinsamkeiten. Doch beide Verfahren sind nicht kompatibel zueinander.
Weil es in Deutschland kein VDSL1 gab, wird VDSL2 in in der Öffentlichkeit in der Regel als VDSL bezeichnet. Fachleute unterscheiden bei VDSL sehr wohl zwischen VDSL1 und VDSL2.
Wenn wir von VDSL sprechen, dann meinen wir eigentlich VDSL2 (G.993.2).

VDSL1 / ITU-T G.993.1

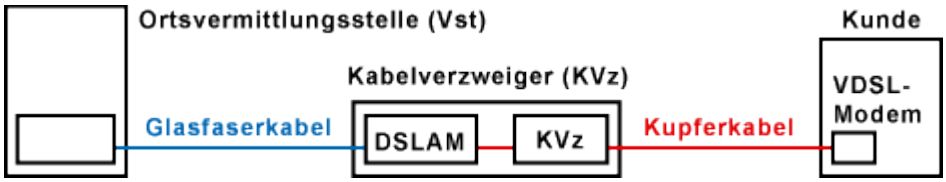


VDSL1 ist eine breitbandige asymmetrische Übertragungstechnik, die sich in Deutschland nicht durchgesetzt hat. Das lag vor allem daran, weil die Reichweite zu kurz war.

VDSL2 / ITU-T G.993.2

Ein besonderes Merkmal von VDSL2 ist die Abwärtskompatibilität zu ADSL, ADSL2 und ADSL2+. Es bietet sogar einen Fallback-Modus nach ADSL/ADSL2/ADSL2+. Das macht VDSL2 so interessant für die Netzbetreiber, die bereits ADSL2 und ADSL2+ einsetzen. VDSL2 gilt technisch als der direkte Nachfolger von ADSL2+.
In VDSL2 wurde die Unterstützung paralleler virtueller Verbindungen über eine physikalische Verbindung implementiert. So ist es möglich bestimmte Datenverbindungen zu priorisieren. Zum Beispiel für Telefonie oder TV. VDSL2 bietet Funktionen für Quality of Service, was für Triple Play (Internet, Telefonie, TV) wichtig ist.
Nachdem VDSL1 weltweit nur auf wenig Interesse gestoßen ist, gewann VDSL2 immer mehr an Bedeutung und wird allgemein als VDSL bezeichnet. Eine Unterscheidung zwischen VDSL1 und VDSL2 ist eigentlich nicht mehr notwendig.

VDSL-Netzarchitektur



Wird VDSL in einem Telefonnetz eingesetzt, dann ist die Voraussetzung ein Hybrid-Netz, bestehend aus Glasfaser- und Kupferleitungen. Die Glasfaserleitungen müssen möglichst nahe an den Teilnehmeranschluss herangeführt werden, um auf den letzten hundert Metern über die Kupferleitung eine sehr hohe Übertragungsrate zu erreichen.

VDSL-Übertragungstechnik

Die VDSL-Übertragungstechnik basiert auf ADSL und DSM. Die Höhe der tatsächlich möglichen Übertragungsrate hängt in der Praxis sehr stark von der Länge und Qualität des Kupferkabels zwischen Kabelverzweiger und Teilnehmeranschluss (DSL-Modem) ab.

VDSL-Vectoring / ITU-T G.993.5

Bei VDSL-Vectoring handelt es sich um eine Erweiterung von VDSL, um auf der Teilnehmeranschlussleitung (TAL) eine höhere Datenübertragungsgeschwindigkeit zu erreichen. Mit VDSL-Vectoring verdoppelt ein Netzbetreiber die Übertragungsgeschwindigkeit der VDSL-Anschlüsse beispielsweise von 50 auf 100 MBit/s.

VDSL in der Praxis

Nachdem VDSL1 weltweit nur wenig Interessenten gefunden hat, gewinnt VDSL(2) immer mehr an internationaler Bedeutung. Auch in anderen Ländern setzt man auf die Kombination aus Glasfaserkabel und Kupferleitungen. Zum Beispiel Belgacom, KPN, AT&T, Telenor, Swisscom und France Telecom.
In Deutschland wird VDSL hauptsächlich von der Deutschen Telekom bereitgestellt. Mit der Einführung von VDSL-Vectoring kommen auch andere Netzbetreiber zum Zug, weil seit 2015 jeder Netzbetreiber jeden Kabelverzweiger mit VDSL ausbauen darf.

VDSL vs. TV-Kabel

VDSL konkurriert in Deutschland hauptsächlich mit der TV-Kabelmodemtechnik. Hier erreicht das TV-Kabelnetz bereits bis zu 200 MBit/s. Das TV-Kabel ist hinsichtlich des geringeren Upstreams leicht im Nachteil. Hier ist die Geschwindigkeit auf 12 MBit/s festgefahren. Das liegt am Frequenzbereich unterhalb von 87,5 MHz, der sich nicht ohne großen Aufwand erweitern lässt. Die Aufteilung in Sende- und Empfangsrichtung erfolgt mit Frequenzweichen, die festgelegt sind. Weitere Geschwindigkeitssteigerungen im TV-Kabelnetz sind nur mit umfangreichen Arbeiten in den Kopfstationen verbunden.

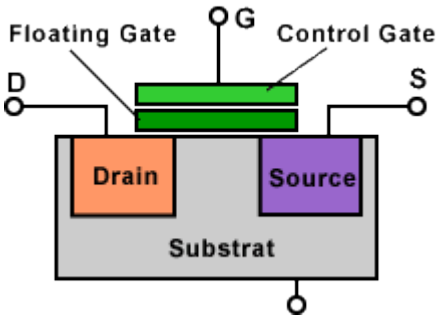
82. Flashspeichern

Flash-Speicher / Flash-Memory

Flash-Speicher bzw. Flash-Memory kombiniert die Vorteile von Halbleiterspeicher und Festplatten. Wie jeder andere Halbleiterspeicher kommt Flash-Speicher ohne bewegliche Teile aus. Und die Daten bleiben wie bei einer Festplatte auch nach dem Abschalten der Energieversorgung erhalten.
Der Flash-Speicher hat sich aus dem EEPROM (Electrical Erasable and Programmable Read-Only Memory) entwickelt. Je nach Literatur gibt es auch die Bezeichnungen Flash-EPROM und Flash-ROM.
Beim Flash-Speicher ist die Speicherung von Daten funktionell identisch wie beim EEPROM. Die Daten werden allerdings blockweise in Datenblöcken zu 64, 128, 256, 1024, ... Byte zugleich gelesen, geschrieben und gelöscht.

Computer, deren Speicher rein auf Flash-Speicher basieren, sind der Traum eines jeden Software-Entwicklers und Anwenders. Der Computer müsste nie mehr minutenlang beim Starten booten, sondern wäre innerhalb weniger Sekunden sofort betriebsbereit. Genauso schnell wäre er auch ausgeschaltet. Und beim nächsten Start wären die gleichen Programme und Dateien geladen, wie vor dem Ausschalten.

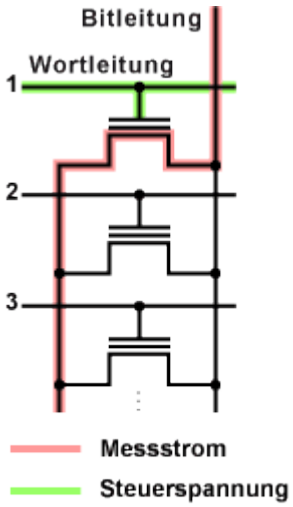
Flash-Speicherzelle



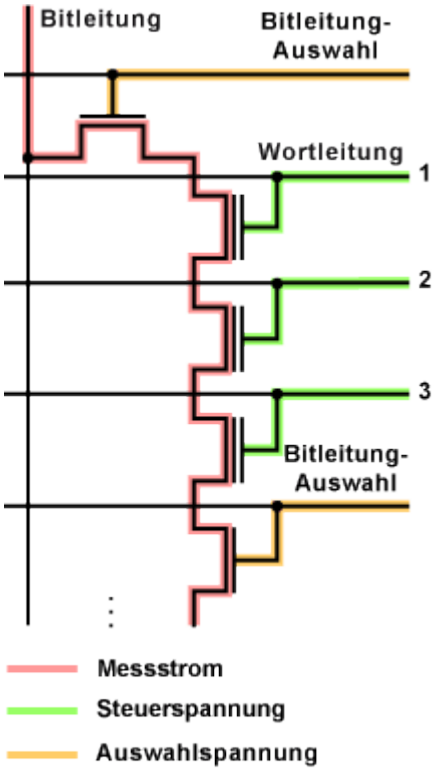
Die Speicherzelle eines Flash-Speichers ist dem Feldeffekttransistor (FET) sehr ähnlich. Im Gate ist jedoch eine Ladungsfalle enthalten, die Floating Gate genannt wird. Es handelt sich um eine elektrisch isolierte Halbleiterschicht. Das Floating Gate speichert die Ladung wie ein Kondensator. Es ist gegen die Anschlüsse Drain, Source und Control Gate mit einer Oxidschicht isoliert. Die Oxidschicht verhindert das Abfließen der Ladung. Im spannungslosen Zustand bleibt die Ladung über viele Jahre erhalten.
Beim Löschvorgang springt die Ladung in einem Blitz (Flash) auf das Floating Gate über. Es wird aufgeladen. Der Stromfluss zwischen Source und Drain wird abgeschnürt. Der Transistor befindet sich dann im Null-Zustand.
Zum Lesen der Speicherzelle wird Spannung an den Transistor gelegt und der Strom, der zwischen Drain und Source fließt, gemessen. Ist das Floating Gate entladen, dann fließt ein Strom zwischen Source und Drain. Der Zustand des Transistors ist dann 1.

Unterschied NAND- und NOR-Flash

Die NAND- und NOR-Architekturen unterscheiden sich in der Speicherdichte und der Zugriffsgeschwindigkeit.



Bei NOR-Flash sind die Speicherzellen parallel verschaltet. Der Zugriff auf die Speicherzellen erfolgt wahlfrei und direkt. Entsprechend kurz sind die Zugriffszeiten. Die Parallelschaltung garantiert einen geringeren Widerstand zwischen Stromquelle und Auswerteschaltung. So wird für den Programmspeicher von Mikrocontrollern NOR-Flash verwendet.



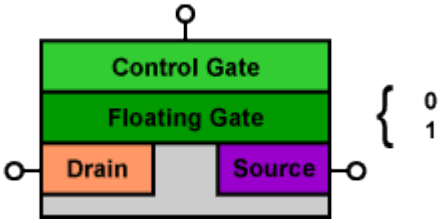
Bei NAND-Flash ist wegen der internen seriellen Verschaltung das Lesen und Schreiben nur in Blöcken möglich. Durch die geringe Anzahl an Datenleitungen benötigt NAND-Flash weniger Platz. Da Daten auf Festplatten ebenfalls Blockweise gelesen und geschrieben werden, eignet sich NAND-Flash hervorragend als Speicher für Speicherkarten, USB-Sticks und SSDs.
Im Vergleich zu anderen nichtflüchtigen Speicherarten erlaubt NAND-Flash höhere Speicherdichten zu geringen Kosten und arbeitet mit wesentlich schnellerer Schreibgeschwindigkeit und geringem Stromverbrauch. Bei gleichen Speicherbausteinen liegen Geschwindigkeitsunterschiede bei den Controllern.

SLC-, MLC- und TLC-Flash

	SLC (Single Level Cell)	**MLC (Multi Level Cell)**	**TLC (Triple Level Cell)**
Bit pro Zelle	1 Bit	2 Bit	3 Bit
Speicherbare Zustände	2 (2^1)	4 (2^2)	8 (2^3)
Lebensdauer	100.000 Schreibvorgänge	3.000 Schreibvorgänge	ca. 1.000 Schreibvorgänge
Fehlerrate	sehr niedrig	mittel	hoch
Geschwindigkeit	sehr hoch	niedrig	niedrig
Stromverbrauch	sehr niedrig	hoch	hoch

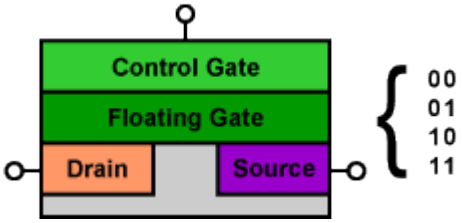
Preis	> 10 Euro pro GByte	2 bis 4 Euro pro GByte	?

SLC-Flash (Single Level Cell)



SLC-Flash speichert nur ein Bit pro Speicherzelle. Er ist mit rund 100.000 Schreibzyklen ein zuverlässiger Flash-Speicher für SSDs und aber auch sehr teuer.

MLC-Flash (Multi Level Cell)

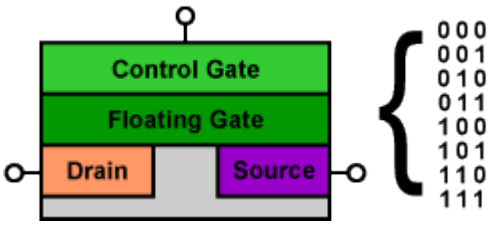


MLC-Flash speichert zwei Bit pro Speicherzelle (x2-MLC). Er hat dadurch eine höhere Speicherdichte im Vergleich zu SLC-Flash, bei gleichen Siliziumkosten. MLC-Flash lässt sich deshalb günstiger fertigen und eignet sich besonders in Produkten für den Massenmarkt. Allerdings lassen sich die MLC-Speicherzellen nicht ganz so schnell beschreiben, wie SLC-Speicherzellen. Bei 2 Bit muss eine Speicherzelle mehrere Spannungsniveaus vertragen (00, 01, 10, 11). Es treten häufig Lesefehler auf. Vor allem dann, je öfter eine Zelle beschrieben wurde. Deshalb benötigen MLCs mehr Fehlerkorrekturmechanismen. Dementsprechend dauert das Lesen länger. Auch der Lesevorgang hat eine physikalische Beanspruchung der Zellen zur Folge. Insgesamt eignen sich MLCs besonders gut für Systeme, die mehr Lese- als Schreibvorgänge haben.

Anfangs war noch von 10.000 Schreibvorgängen pro MLC-Zelle die Rede. Wegen feineren Halbleiterstrukturen ist die Anzahl auf 5.000 gesunken und ist inzwischen bei 3.000 angekommen (Stand: Oktober 2013). Wegen den Ladungsunterschieden für mehrere Bit sind die Speicherzellen mit rund 3.000 Schreibzyklen pro Zelle (bei 19-nm-Herstellungsprozess) defektanfälliger, als bei SLC. Nur durch Wear-Leveling und Reserve-Speicherzellen lässt sich die Gesamtlebensdauer des Flash-Speichers verlängern, was aber auch die Herstellungskosten erhöht.

MLC-Flash wird wegen der begrenzten Schreibzyklen hauptsächlich für USB-Sticks und Speicherkarten verwendet. MLC-Flash findet man auch manchmal in billigen SSDs.

TLC-Flash (Triple Level Cell)



TLC-Flash speichert drei Bit pro Speicherzelle (x3-MLC). Wegen der höheren Speicherdichte im Vergleich zu MLC-Flash könnte man auf einen noch günstigeren Flash-Speicher schließen. Allerdings müssen die Speicherzellen eine hohe Qualität aufweisen, um die unterschiedlichen Ladungszustände für drei Bit stabil halten zu können, was die Herstellung wieder verteuert.
Weil dieser Flash-Speicher möglichst billig sein soll kommen einzelne TLC-Zellen auf höchstens 1.000 Schreibvorgänge. Damit ist die Lebensdauer von TLC-Flash gerade noch akzeptabel, um es in USB-Sticks und Speicherkarten einzusetzen. Beim Einsatz als SSD in normalen PCs und Notebooks muss man technische Klimmzüge machen, was den Speicher wieder verteuert. Für Server, wo häufiger geschrieben wird, ist TLC-Flash unbrauchbar.
TLC-Flash wird wegen der begrenzten Schreibzyklen hauptsächlich für USB-Sticks und Speicherkarten verwendet. TLC-Flash findet man auch manchmal in der extrem billigen SSDs.

Vorteile von Flash-Speicher

- Die gespeicherten Daten bleiben auch bei fehlender Versorgungsspannung erhalten. Auf eine Erhaltungsladung kann verzichtet werden. Somit ist auch der Energieverbrauch und die Wärmeentwicklung geringer.
- Wegen fehlender beweglicher Teile ist Flash geräuschlos, unempfindlich gegen Erschütterungen und magnetische Felder.
- Im Vergleich zu Festplatten haben Flash-Speicher eine sehr kurze Zugriffszeit. Lese- und Schreibgeschwindigkeit sind über den gesamten Speicherbereich weitestgehend konstant.
- Die erreichbare Speichergröße ist durch die einfache und platzsparende Anordnung der Speicherzellen nach oben offen.

Nachteile von Flash-Speicher

- begrenzte Schreib- bzw. Löschvorgänge
- begrenzte Speicherkapazität
- hoher Preis

Der gravierendste Nachteil von Flash-Speicher ist die begrenzte Zahl von Schreib- bzw. Löschvorgängen, die eine Speicherzelle vertragen kann. Typischerweise gehen die Speicherzellen nach 100.000 Zyklen bei Single-Level-Cells (SLC), 3.000 Zyklen bei Multi-Level-Cells (MLC) und schon nach 1.000 Zyklen bei Triple-Level-Cells (TLC) kaputt.

Die Zuverlässigkeit von Flash-Speicher leidet auch darunter, weil mit der Zeit die Speicherzellen ihre Ladung verlieren. Je höher die Temperatur und die Ladungsmenge pro Zelle, desto schneller. Bei einem Lesevorgang kann der Zelleninhalt schon gekippt sein. Je feiner die Strukturen werden, desto größer ist die Gefahr. SLC-Flash ist hier die einzige Flash-Technik, die Sicherheit bietet.

Endurance

Mit Endurance bezeichnet man die maximal zulässige Anzahl an Lösch- bzw. Speicherzyklen, die ein nichtflüchtiger Datenspeicher (NVRAM) pro Speicherzelle verträgt, bis es zu spürbaren Fehlern bei Speicheroperationen kommt.
Dass die Anzahl überhaupt beschränkt ist, liegt bei heutigen Flash-Speichern (die gängige Technologie zur Umsetzung des NVRAM-Prinzips) daran, dass die Speicherzellen für die Programmier- und Löschoperationen hohen Spannungen (10 bis 18 V) ausgesetzt werden, wodurch Schädigungen in der Struktur der Zelle auftreten. Die Schädigungen werden umso geringer, je geringer die Spannungen für Programmieren und Löschen gewählt werden können. Diese Minimierungsanforderung führt dazu, dass man eine zentrale Isolationsstruktur in der Speicherzelle möglichst dünn ausführen muss. Das wiederum hat allerdings negative Auswirkungen auf die Dauer der Datenhaltung (Retention).

Warum geht eine Flash-Speicherzelle kaputt?

Das Floating Gate wird mit einer Spannung von 10 bis 13 Volt geladen (Schreibzugriff). Das ist notwendig, um die Oxidschicht (Isolation) zu überwinden. Dabei nimmt die Oxidschicht Schaden. Bei jedem Schreibzugriff etwas mehr. Irgendwann isoliert sie nicht mehr und die Speicherzelle wird unbrauchbar.
Da ein Schreibvorgang Speicherblöcke zwischen 16 und 128 kByte gleichzeitig beschreibt, werden auch Speicherzellen beansprucht, die gar keiner Veränderung bedürfen. Das bedeutet, schon bei geringen Änderungen des Speicherinhalts werden viele Speicherzellen neu geschrieben.

Haltbarkeit und Zuverlässigkeit von Flash-Memory

Zur Haltbarkeit und Zuverlässigkeit von Flash-Memory gibt es folgende Erkenntnisse: Die Anzahl der möglichen Schreib- bzw. Löschzyklen lässt keine direkten Rückschlüsse auf die Haltbarkeit oder die Zuverlässigkeit zu. Anders als bei herkömmlichen Festplatten besteht zwischen den Speicherzellen und den Sektoren des Dateisystems keine direkte Zuordnung. Generell verteilt der Flash-Controller die Schreibzugriffe gleichmäßig über alle Flash-Speicherzellen. Die Daten in den Zellen, die mit selten veränderten Daten, wie Betriebssystem und Programmen belegt sind, werden ab und zu umgeschichtet, um so wieder an weniger stark abgenutzte Zellen zu kommen. Gleichzeitig werden alle Speicherzellen regelmäßig aufgefrischt, damit sich mit der Zeit kein Datenverlust durch den Verlust der Ladung in den Speicherzellen einschleicht.
Alle Verfahren und Mechanismen, die die Lebensdauer der Speicherzellen verlängern fallen unter den Begriff "Wear-Leveling".

Generell kann man davon ausgehen, dass SSDs im alltäglichen Desktop-Betrieb länger halten, als von den Herstellern angegeben. 3.000 bis 100.000 Speicher- bzw. Löschzyklen sind für die meisten Anwendungen vollkommen ausreichend. Vor allem wenn mit Wear-Leveling alle Speicherzellen gleichmäßig belastet und so die Lebensdauer verlängert wird.

Weiterentwicklung von Flash-Speicher

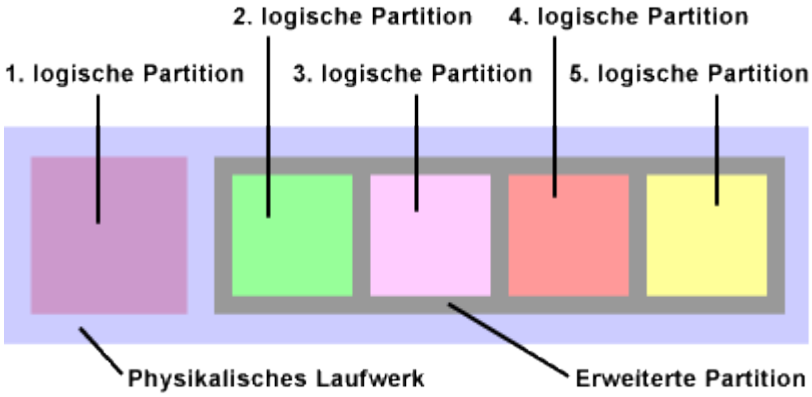
Die Entwicklung bei Flash-Speichermedien geht in Richtung lange Haltbarkeit, kleine Zugriffszeit und hohe Geschwindigkeit. Dabei strebt man an, die Anzahl der Schreib- und Lesefehler auf ein Niveau zu drücken, so dass die Haltbarkeit von günstigem MLC-Flash in den Bereich von SLC-

Flash rückt.
Mögliche Lösungen sind 3D-V-NAND, iSLC oder eMLC, bei denen mehrere MLC-Speicherzellen in mehreren Lagen übereinander geschichtet sind. Statt der typischen planaren Architektur setzt man auf eine vertikale Anordnung. Bei monolithischen 3D-V-NAND-Chips liegen über 20 Lagen übereinander. Das Stapeln spart Siliziumfläche, weshalb die einzelnen Zellen größer sein dürfen. Auf diese Weise erhöht man die Speicherkapazität, Lebensdauer, Geschwindigkeit und verlängert die Datenhaltung der einzelnen Speicherzellen.

Es gibt allerdings auch andere Anforderungen an Flash-Speicher. Der soll möglichst groß und billig sein und bei Leerlauf ausgeschaltet bleiben, bis eine konkrete Anfrage eingeht. Auch die Zuverlässigkeit und Geschwindigkeit steht an zweiter Stelle. Interessant sind solche Flash-Speicher bei Datenarchiven, wo der Anwender bei seinen Zugriffen ein wenig länger warten kann.

83. Partitionen / Partitionieren / Dateisysteme

Partitionen / Partitionieren / Dateisysteme



Eine Partition ist ein logischer Teil einer Festplatte, der wie eine physikalische Festplatte angesprochen wird. Unterschieden wird zwischen logischer, primärer und erweiteter Partition.
Das Partitionieren ist das Aufteilen eines physikalischen Laufwerks oder einer erweiterten Partition in mehrere kleinere logische Partitionen um sie als eigenständige Laufwerke ansprechen zu können.

Physikalische Laufwerke

Die Festplatte, aus Metall und Kunststoff bestehend, wird als physikalisches Laufwerk bezeichnet. Den physikalischen Laufwerken sind Gerätenummern zugeordnet (0, 1, 2, 3,...).

Logische Partition

Die logische Partition ist ein Bestandteil einer oder mehreren Festplatten, die sich über eine Laufwerksbezeichnung ansprechen lässt.
Unter einem Windows-Betriebssystem werden logische Partitionen wie physikalische Festplatten durch einen Buchstabe zwischen **C** und **Z** gekennzeichnet.
Unter Linux wird jede physikalische Festplatte, jede logische, primäre und erweiterte Partition

einzeln gekennzeichnet. Die physikalischen Festplatten werden mit **hda**, **hdb, hdc** und fortlaufend gekennzeichnet. Wobei **hda** die erste Festplatte am primären Controller, **hdb** die zweite Festplatte am primären Controller, **hdc** die erste Festplatte am sekundären Controller uns so weiter wären.
Die Partitionen werden mit **hda1, hda2, hda3** usw. gekennzeichnet. Wobei **hda1 bis hda4** ausschließlich die primären Partitionen sind. **hda5** ist die erweiterte Partition und **hda6, hda...** die logischen Partitionen.

Primäre Partition

Die primäre Partition ist der Teil einer Festplatte, von der ein Betriebssystem gebootet werden kann. Pro Festplatte ist es möglich 4 primäre Partitionen einzurichten, ohne den Bootsektor der Festplatte anzupassen.

Erweiterte Partition

Muss eine Festplatte in mehr als 4 Partitionen unterteilt werden, dann kann eine zusätzliche erweiterte Partition pro physikalisches Laufwerk eingerichtet werden. Die erweiterte Partition ist nicht bootfähig. Sie kann allerdings in kleinere logische Partitionen unterteilt werden.

Warum wird partitioniert?

Der Grund liegt in der Art und Weise, wie Dateien auf der physikalischen Festplattenstruktur abgelegt werden. Man spricht von Dateisystemen, die irgendwann entwickelt wurden, um Dateien und Ordner auf der Festplatte zu speichern.
Ein Problem waren die Festplatten-Controller, die nicht in der Lage waren, einen größeren Adressbereich anzusprechen. Und, der technische Fortschritt und die höheren Kapazitäten von Festplatten wurden schneller eingeführt als neue und bessere Dateisysteme. Vor allem unter Windows-Betriebssystemen war das FAT-Dateisystem (File Allocation Table) lange führend. FAT ermöglichte durch die Zusammenführung mehrerer Blöcke zu einer logischen Ansprecheinheit (Cluster), um die Adressierungsbeschränkung zu umgehen. Es hatte den Nachteil, dass es Festplatten nur bis zu einer bestimmten Kapazität verwalten und die Dateien nicht besonders platzsparend speichern konnte.

Bei FAT16 ist die Partitionsgröße auf 2 GByte beschränkt. Der Nachfolger von FAT16 war FAT32. Damit wurde der Adressierungsbereich auf 32 Bit vergrößert. Allerdings blieb FAT32 aus Kompatibilitätsgründen auf eine gewisse Größe beschränkt. Bei FAT32 ist die Partitionsgröße auf 2 TByte begrenzt. Über 32 GByte verwendet man üblicherweise das Dateisystem NTFS.
Um die überschüssige Festplatten-Kapazität trotzdem nutzen zu können, teilte man die Festplatten mindestens in zwei Partitionen auf. Man umging somit die Adressierungsbeschränkung der Festplatten-Controller und die Kapazitätsbeschränkung von FAT.

Der andere Nachteil bestand in der logischen Aufteilung (Cluster) der physikalischen Festplatte. Je nach Festplatte oder Partitionsgröße waren die Cluster unterschiedlich groß. Je größer die Partition, desto größer waren die Cluster. Jede gespeicherte Datei belegte mindestens einen Cluster. War die Datei zu groß für den Cluster wurde die Datei so oft geteilt, bis die Datei in mehrere Cluster passte. War die Datei kleiner als ein Cluster, wurde sie im Cluster gespeichert. Der freie Speicherplatz im Cluster war dann verloren. Er konnte nicht belegt werden. Besonders kleine Dateien mit wenigen Byte konnten so genauso viel Speicher belegen, wie mehrere große Dateien. Um den Speicherplatz

nicht unnötig zu verschwenden, teilte man eine physikalische Festplatte in mehrere kleinere Partitionen mit einer gerade noch akzeptablen Clustergröße auf.

Da es heute für alle Betriebssysteme bessere Dateisysteme gibt, partitioniert man aus den genannten Gründen nicht mehr. Im Prinzip gibt es keinen wirklichen Grund mehr zu Partitionieren. Es sei denn, man möchte irgendwelche Speziallösungen umsetzen:

- Installation mehrerer Betriebssysteme
- Einrichten verschiedener Dateisysteme
- Reservierung für eine Windows- oder Linux-Auslagerungsdatei (SWAP-Partition)
- Installationsdateien
- sehr großen Speicher verwalten
- Trennung von Programmen und Daten

84. Workstation

Eine Workstation ähnelt einem Personal Computer und ist im Prinzip ein Arbeitsplatz-PC. Die Workstation dient meistens nur einer bestimmten Aufgabe, bei denen es auf viel Grafik-Performance, Rechenleistung oder einen großen Speicherausbau ankommt. Zum Beispiel bei der Bildbearbeitung. Die Hardware und Software ist speziell für diesen Anwendungsfall ausgelegt.
Da Personal Computer immer leistungsfähiger werden, verschwimmt der Unterschied zwischen Workstation und Personal Computer. Eine klare Trennung findet immer seltener statt. Meistens bezeichnet man einen leistungsfähigen PC als Workstation, wenn er eine Workstation-typische Aufgabe hat.

85. Thin-Client

Ein Thin-Client ist ein Mini-Computer, dessen Hardware auf ein Minimum reduziert ist. Sogar der Speicherplatz für Software wurde eingespart. Stattdessen lädt der Thin-Client sein Betriebssystem und seine Anwendungen aus dem Netzwerk von einem Server. Die Daten werden ebenfalls auf einem Server gespeichert.
Thin-Clients gibt es in Miniaturausführung in der Größe eines Buchs. Nach außen wird nur ein DVI- oder VGA-Anschluss für den Monitor, mehrere USB-Anschlüsse für Tastatur, Drucker und Maus herausgeführt. Strom bekommt das System von einem Steckernetzteil.
Inzwischen ermöglicht die hochintegrierte Bauweise, die den Thin-Client in eine Unterputz-Steckdose verschwinden lässt. In diesem Fall wird für den Netzwerk-Anschluss das Netzwerkkabel direkt Unterputz aufgeklemmt.