

M117

Informatik- und Netzinfrastruktur für ein kleines Unternehmen realisieren

Autor: Schmid Tobias

Datum: 17.09.2020

Typ: Information

Version: 2.0

Inhaltsverzeichnis

INHALT	
1	Einleitung..... 4
2	Netzwerkarchitektur 4
2.1	PAN: Personal Area Network..... 5
2.2	LAN: Local Area Network oder WLAN: Wireless local Area Network..... 6
2.3	CAN: Campus Area Network..... 8
2.4	MAN: Metropolitan Area Network..... 9
2.5	WAN: Wide Area Network..... 11
2.6	GAN: Global Area Network..... 12
2.7	VPN: Virtual Private Network 13
2.8	SAN: Storage Area Network 14
2.9	LoRaWAN: Low Power Wide Area Network 15
3	Topologien..... 17
3.1	Begriffe 17
3.2	Bustopologie..... 18
3.3	Sterntopologie 19
3.4	Reine Ringtopologie 20
3.5	Ringtopologie mit Backbone 21
3.6	Baumtopologie 22
3.7	Maschentopologie (Mesh) 23
3.8	Zusammenfassung..... 24
3.9	Abschlussfragen..... 24
4	Betriebsarten von Netzwerken 25
5	Peer-to-Peer Netzwerk..... 26
5.1	Charakterisierung von Peer-to-Peer Netzwerken 27
5.2	Typen von Peer-to-Peer..... 27
5.3	Vor-/Nachteile von Peer-to-Peer..... 28
6	Client-Server Architektur 29
6.1	Definitionen 29
6.2	Client/Server Modell 30
6.3	Unterschiede zu Peer-to-Peer 31
6.4	Client-Server System 31
6.4.1	Beispiel eines Client-Server-Systems mit zentralem Datenbankserver 31
6.5	Grundsätzliche Funktionsweise 31
6.6	Vor-/Nachteile von Client/Server Modellen..... 32
6.7	Zusammenfassung..... 32
6.8	Abschlussfragen..... 33
7	Kabel- und Funktechnologie 34
7.1	Kabelbasierende Netzwerke..... 34
7.2	Kabeltypen..... 36
7.2.1	Twisted-Pair-Kabel..... 37
7.2.2	Glasfaserkabel 39
7.2.3	Vergleich Twisted-Pair/Glasfaserkabel..... 39
7.3	Funkbasierte Netzwerke..... 40
7.3.1	Betriebsarten 40
7.3.2	Gegenüberstellung LAN/WLAN 42
7.4	Standards im LAN Bereich 43
7.4.1	Datenpaket 43

8	Netzwerkgeräte	45
8.1	Switch	45
8.2	Router	45
8.3	Proxy	45
8.4	Firewall	46
8.5	Emulatoren	47
9	OSI Layer.....	48
9.1	Motivation	48
9.2	OSI kurz erklärt	48
9.2.1	Ein Schichtenmodell für Kommunikationsvorgänge im Internet - Kommunikation in Rechnernetzen	48
9.2.2	Nachrichtenübertragung im Schichtenmodell	49
9.2.3	Ein Stapel aus Protokollen	49
9.2.4	Datenanreicherung.....	50
9.3	Die sieben Schichten.....	51
9.3.1	Schicht 1 – Physikalische Schicht (Physical Layer)	53
9.3.2	Schicht 2 – Sicherungssicht (Data Link Layer).....	54
9.3.3	Schicht 3 – Vermittlungssicht (Network Layer)	55
9.3.4	Schicht 4 – Transportschicht (Transport Layer).....	56
9.3.5	Schicht 5 – Sitzungsschicht (Session Layer)	57
9.3.6	Schicht 6 – Darstellungssicht (Presentation Layer)	57
9.3.7	Schicht 7 – Anwendungssicht (Application Layer).....	57
9.4	Allgemeines	58

1 Einleitung

Das nachfolgende Dokument soll eine theoretische Grundlage für das Modul M117 darstellen. Sie finden in diesem Dokument sowohl Theorie wie auch Aufgabenstellungen.

2 Netzwerkarchitektur

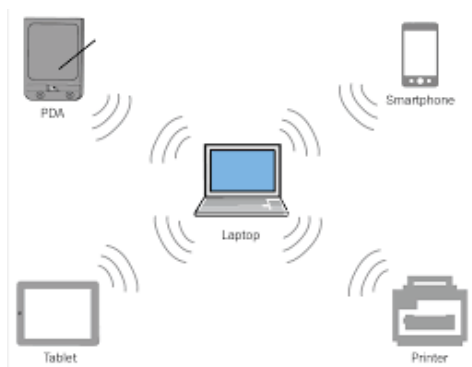
Unter einem Netzwerk versteht man eine beliebige Anzahl selbständiger Computersysteme, die so miteinander verbunden sind, dass ein **Datenaustausch** möglich wird. Dazu muss neben einer physischen Verbindung auch eine logische Verbindung der zu vernetzenden Systeme vorhanden sein. Letztere wird durch spezielle Netzwerkprotokolle wie TCP (Transmission Control Protocol) hergestellt. Bereits zwei miteinander verbundene Rechner können als Netzwerk betrachtet werden.

Netzwerke werden mit dem Ziel eingerichtet, Daten von einem System auf ein anderes zu übertragen oder gemeinsame Ressourcen wie Server, Datenbanken oder Drucker im Netzwerk zur Verfügung zu stellen. Je nach Größe und Reichweite des Rechnernetzes werden **verschiedene Netzwerkdimensionen** unterschieden. Zu den wichtigsten Netzwerktypen gehören:

Die physische Verbindung, die diesen Netzwerktypen zugrunde liegt, kann kabelgebunden oder auf Basis von Funktechnik realisiert werden. Oft stellen physische Kommunikationsnetze die Grundlage für mehrere logische Kommunikationsnetze, sogenannte **Virtual Private Networks (VPN)**. Diese nutzen bei der Datenübertragung zwar ein gemeinsames physisches Übertragungsmedium, beispielsweise ein Glasfaserkabel, werden mittels Tunneling-Software jedoch logisch unterschiedlichen virtuellen Netzen zugeordnet.

Jeder Netzwerktyp wurde für spezielle Anwendungsbereiche entwickelt, beruht auf jeweils eigenen Techniken und Standards und bringt somit unterschiedliche Vorteile und Beschränkungen mit sich.

2.1 PAN: Personal Area Network

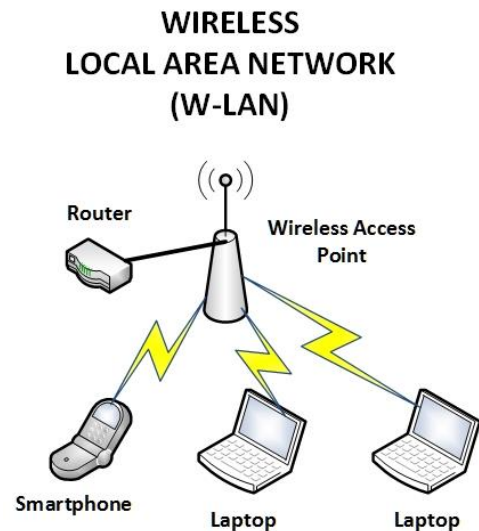
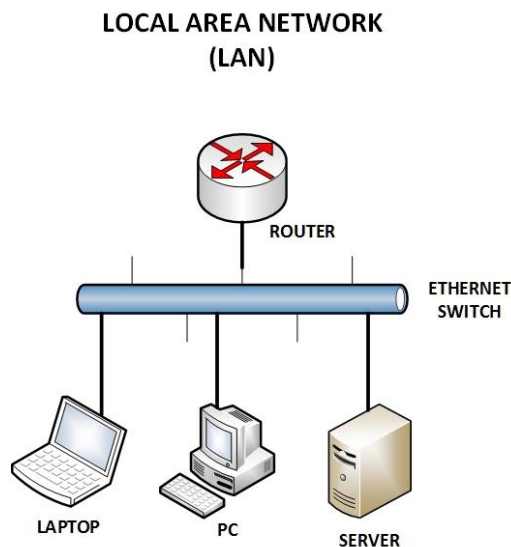


Standards/Anwendung	Ausdehnung

Um einen Datenaustausch zu ermöglichen, lassen sich moderne Endgeräte wie Smartphones, Tablets, Laptops oder Desktop-Computer ad hoc zu einem Netzwerk zusammenschließen. Dies kann kabelgebunden in Form eines Personal Area Networks (PAN) erfolgen. Übliche Übertragungstechniken sind **USB** oder **FireWire**. Die kabellose Variante **Wireless Personal Area Network (WPAN)** stützt sich auf Techniken wie Bluetooth, Wireless USB, Insteon, IrDA, ZigBee oder Z-Wave. Ein kabelloses Personal Area Network, das via Bluetooth zustande kommt, wird **Piconet** genannt. PANs und WPANs erstrecken sich in der Regel nur über wenige Meter und eignen sich somit nicht, Geräte in unterschiedlichen Räumen oder gar Gebäuden zu verbinden.

Neben der Kommunikation einzelner Endgeräte untereinander ermöglicht ein Personal Area Network zudem den Verbindungsaufbau zu anderen, in der Regel größeren Netzwerken. Man spricht in diesem Fall von einem **Uplink**. Aufgrund der begrenzten Reichweite und einer vergleichsweise niedrigen Datenübertragungsrate kommen PANs in erster Linie zum Einsatz, um Peripheriegeräte im Hobby- und Entertainment-Bereich zu verbinden. Typische Beispiele sind kabellose Kopfhörer, Spielekonsolen und Digitalkameras. Im Rahmen des **Internet of Things (IoT)** dienen WPANs der Kommunikation von Kontroll- und Monitoring-Anwendungen mit niedriger Datenrate. Protokolle wie Insteon, Z-Wave und ZigBee wurden speziell für Smart Homes und Heimautomation entworfen.

2.2 LAN: Local Area Network oder WLAN: Wireless local Area Network



Standards/Anwendung	Ausdehnung

Sollen mehrere Rechner zu einem Verbund zusammengeschlossen werden, erfolgt dies meist in Form eines Lokal Area Networks (LAN). Ein solches Ortsnetz kann zwei Rechner in einem privaten Haushalt umfassen oder mehrere tausend Geräte in einem Unternehmen. Auch Netzwerke in öffentlichen Einrichtungen wie Behörden, Schulen oder Universitäten werden als LAN realisiert. Ein weitverbreiteter Standard für kabelgebundene Local Area Networks ist **Ethernet**. Weniger gebräuchlich und weitgehend veraltet sind Vernetzungstechnologien wie ARCNET, FDDI und Token Ring. Die Datenübertragung erfolgt entweder elektronisch **auf Basis von Kupferkabeln** oder über einen **Lichtwellenleiter aus Glasfaser**.

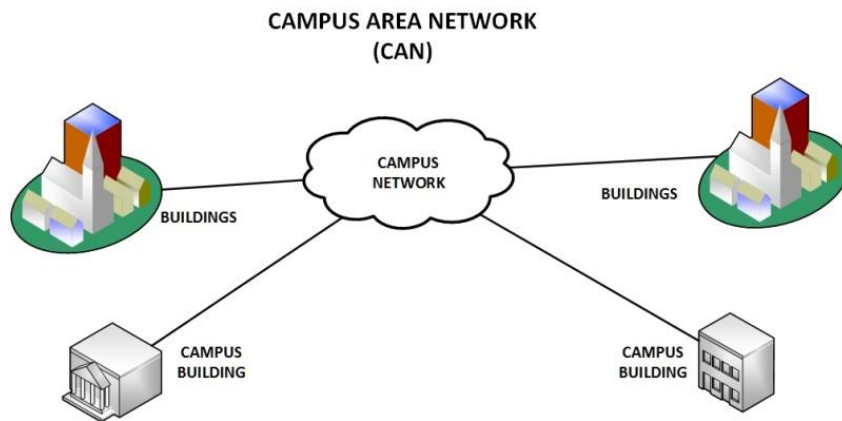
Werden mehr als zwei Rechner in einem LAN zusammengeschlossen, sind weitere Netzwerkkomponenten wie Hubs, Bridges und Switches erforderlich, die als Kopplungselemente und Verteilerknoten fungieren. Der Netzwerktyp LAN wurde entwickelt, um eine **schnelle Übertragung großer Datenmengen** zu ermöglichen. Abhängig vom Aufbau des Netzwerks und des verwendeten Übertragungsmediums ist ein Datendurchsatz von 10 bis 1.000 Mbit/s üblich. LANs erlauben einen komfortablen Informationsaustausch zwischen den verschiedenen im Netzwerk verbundenen Geräten. Im Unternehmenskontext ist es üblich, mehreren Arbeitscomputern gemeinsame Fileserver, Netzwerkdrucker oder Anwendungen über LAN zur Verfügung zu stellen.

Wird ein lokales Netzwerk über Funk realisiert, spricht man von einem **Wireless Local Area Network (WLAN)**. Die technischen Grundlagen des WLAN-Standards werden durch die Normenfamilie IEEE 802.11 definiert. Kabellose lokale Netzwerke bieten die Möglichkeit, Endgeräte bequem in ein Heim- oder Unternehmensnetz einzubinden,

und sind kompatibel zu kabelgebundenen Ethernet-LANs. Der Datendurchsatz ist jedoch geringer als bei einer Ethernet-Verbindung.

Die Reichweite eines LANs ist vom verwendeten Standard und dem Übertragungsmedium abhängig, lässt sich jedoch durch Signalverstärker, sogenannte Repeater, erhöhen. Bei Gigabit-Ethernet über Glasfaser ist eine Signalreichweite von mehreren Kilometern möglich. Local Area Networks erstrecken sich jedoch nur selten über mehr als einen Gebäudekomplex. Mehrere LANs in geografischer Nähe lassen sich zu einem übergeordneten Metropolitan Area Network (MAN) oder Wide Area Network (WAN) verbinden.

2.3 CAN: Campus Area Network

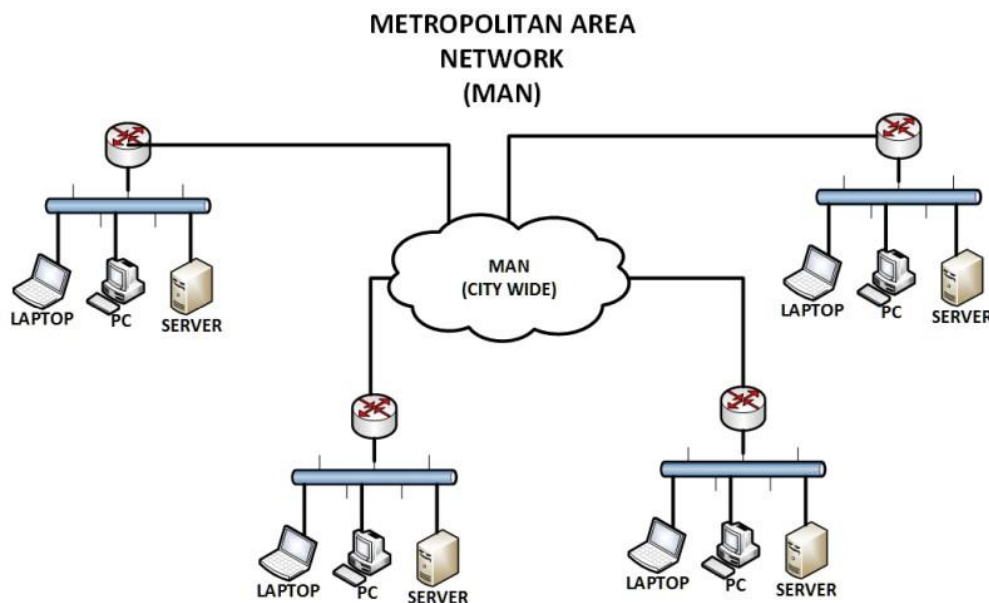


Standards/Anwendung	Ausdehnung

Mit Campus-Netzwerken (CAN) bezeichnet man Netzwerke, die sich auf einen bestimmten geografischen Bereich wie ein Gebäude, einen Unternehmens-, Universitäts-Campus oder einen Industriepark beziehen.

Solche Netzwerke benutzen nicht den öffentlich-rechtlichen Fernmeldebereich und sind in ihrer Ausdehnung auf kürzere Entfernungen begrenzt. Campus-Netze können die lokalen Netze in Gebäuden oder Geschossen, von Forschungs- und Produktionseinrichtungen miteinander verbinden. Ein Campus-Netzwerk ist in den einschlägigen Normen mit einer maximalen Entfernung von 2 km angegeben. Es hat somit eine größere Ausdehnung als ein lokales Netz (LAN), ist allerdings kleiner als ein Stadtnetz (MAN). Die Verkabelungsstandards EIA/TIA 568 und ISO/IEC 11801 schreiben für Campus-Netzwerke die Geländeverkabelung vor.

2.4 MAN: Metropolitan Area Network



Standards/Anwendung	Ausdehnung

Metropolitan Area Network (MAN) wird ein breitbandiges Telekommunikationsnetz genannt, das mehrere LANs in geografischer Nähe verbindet. In der Regel handelt es sich dabei um einzelne Niederlassungen eines Unternehmens, die über **angemietete Standleitungen** zu einem MAN zusammengeschlossen werden. Dabei kommen leistungsstarke Router und Hochleistungsverbindungen auf Basis von Glasfaser zum Einsatz, die einen deutlich höheren Datendurchsatz ermöglichen als das Internet. Die Übertragungsgeschwindigkeit zwischen zwei entfernten Knotenpunkten ist mit der Kommunikation innerhalb eines LANs vergleichbar.

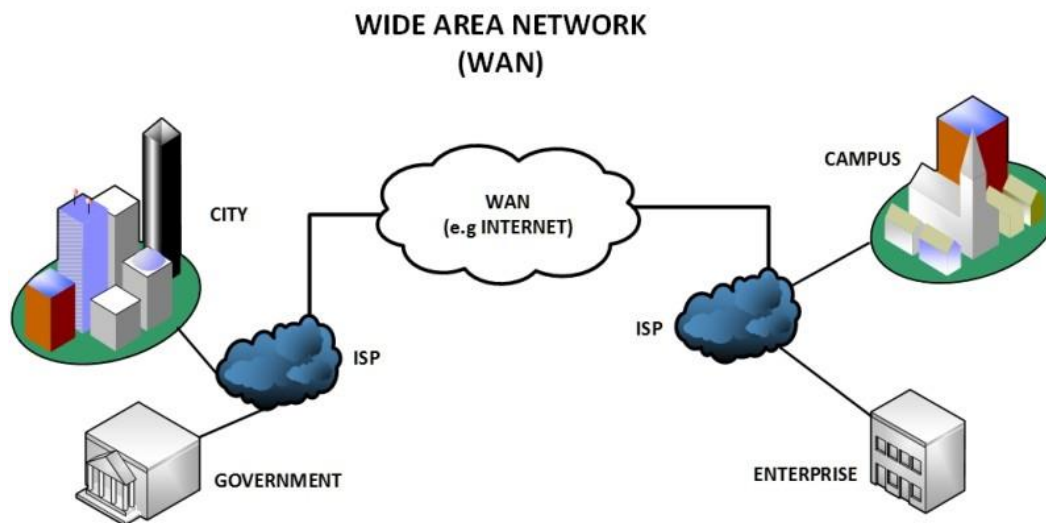
Die Infrastruktur für MANs wird von international agierenden Netzbetreibern zur Verfügung gestellt. Als Metropolitan Area Network verkabelte Städte lassen sich überregional in **Wide Area Networks (WAN)** und international in **Global Area Networks (GAN)** einbinden.

Mit **Metro-Ethernet** steht für MANs eine spezielle Übertragungstechnik zur Verfügung, mit der sich leistungsstarke **Metro-Ethernet-Netze (MEN)** auf Basis von Carrier-Ethernet (CE 1.0) oder Carrier-Ethernet 2.0 (CE 2.0) aufbauen lassen.

Ein Standard für größere regionale Funknetze, sogenannte Wireless Metropolitan Area Networks (WMAN) wurde mit IEEE 802.16 entwickelt. Die als WiMAX (Worldwide Interoperability for Microwave Access) bekannte Technologie ermöglicht es, sogenannte WLAN-Hotzones einzurichten. Dabei handelt es sich um mehrere im Verbund arbeitende WLAN-Zugriffspunkte an verschiedenen Standpunkten. In Deutschland kommen WMANs

zum Einsatz, um Endkunden in Regionen mit fehlender Infrastruktur eine leistungsstarke Anbindung an das Internet zu bieten. Der geläufige Übertragungsstandard DSL ist technisch bedingt nur da verfügbar, wo Kupferkabel verlegt wurden.

2.5 WAN: Wide Area Network



Standards/Anwendung	Ausdehnung

Während Metropolitan Area Networks nah beieinanderliegende Standpunkte in ländlichen Regionen oder Ballungsgebieten verbinden, erstrecken sich **Weitverkehrsnetze**, sogenannte Wide Area Network (WAN), über große geografische Bereiche wie Länder oder Kontinente. Die Anzahl der in einem WAN verbundenen lokalen Netzwerke oder Einzelrechner ist prinzipiell unbegrenzt.

Während LANs und MANs aufgrund der geografischen Nähe der zu verbindenden Rechner oder Netzwerke auf Basis von Ethernet realisiert werden können, kommen bei Weitverkehrsnetzen Techniken wie IP/MPLS (Multiprotocol Label Switching), PDH (Plesiochrone Digitale Hierarchie), SDH (Synchrone Digitale Hierarchie), SONET (Synchronous Optical Network), ATM (Asynchronous Transfer Mode) und selten noch das veraltete X.25 zum Einsatz.

Wide Area Networks sind meist im Besitz einer bestimmten Organisation oder eines Unternehmens und werden privat betrieben oder vermietet. Darüber hinaus nutzen Internet-Service-Provider WANs, um lokale Unternehmensnetzwerke und Endkunden an das Internet anzubinden.

2.6 GAN: Global Area Network



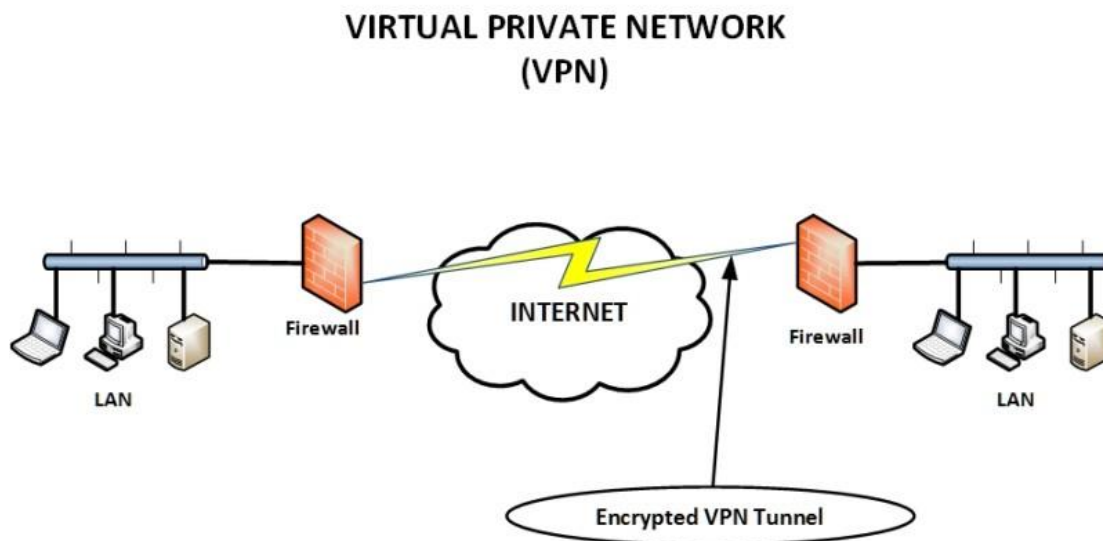
Standards/Anwendung	Ausdehnung

Ein **weltumspannendes Netzwerk** wie das Internet wird als Global Area Network (GAN) bezeichnet. Das Internet ist jedoch nicht der einzige Rechnerverbund dieser Art. Auch international tätige Unternehmen unterhalten abgeschottete Netzwerke, die mehrere WANs umfassen und so Firmenrechner weltweit verbinden. GANs nutzen die Glasfaserinfrastruktur von Weitverkehrsnetzen und schließen diese durch **internationale Seekabel** oder **Satellitenübertragung** zusammen.

Unter einem Global Area Network (GAN) versteht man ein Netz, das über unbegrenzte geographische Entfernungen mehrere Wide Area Networks verbinden kann. Dies kann zum Beispiel die Vernetzung weltweiter Standorte einer internationalen Firma sein. Oft wird bei einem GAN Satelliten- oder Glasfaserübertragung eingesetzt.

Der Begriff GAN wird im Vergleich zu Local Area Network (LAN) und Wide Area Network (WAN) eher selten verwendet. GAN ist nicht die direkte Bezeichnung für das Internet, da es theoretisch mehrere GANs abgeschottet und unabhängig geben kann, das Internet jedoch eine globale Vernetzung ohne (maßgebliche) Unterteilungen ist. So ist das Internet ein GAN, aber nicht jedes GAN wird Internet genannt.

2.7 VPN: Virtual Private Network

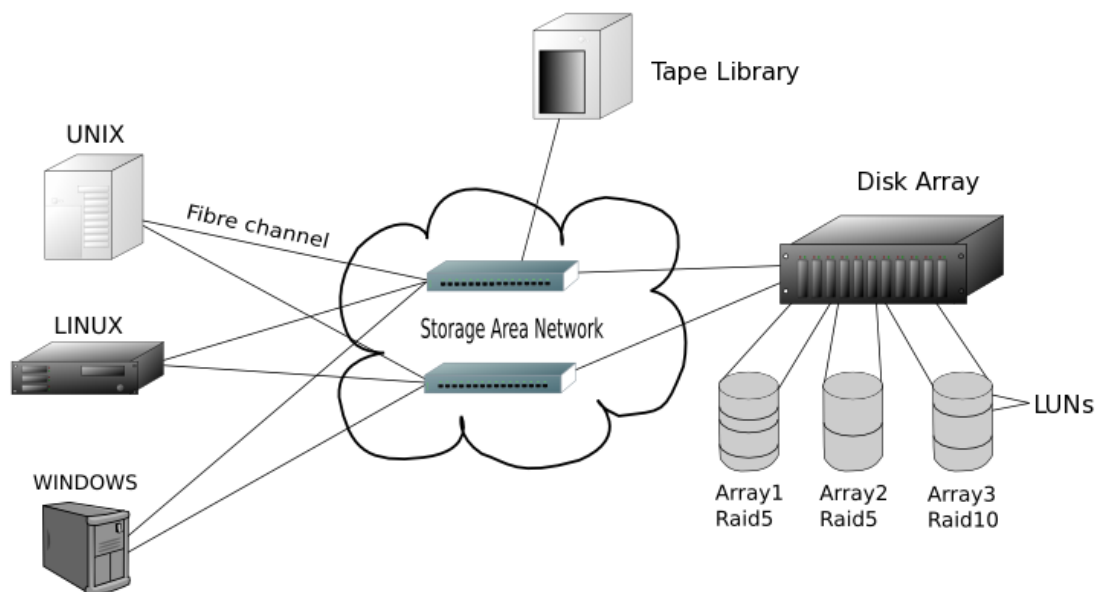


Standards/Anwendung	Ausdehnung

Ein Virtual Privat Network (VPN) ist ein **virtuelles Kommunikationsnetz**, das die Infrastruktur eines physischen Netzwerks nutzt, um Computersysteme logisch zu verbinden. Dabei kann es sich um jeden der oben dargestellten Netzwerktypen handeln. Am gängigsten ist jedoch das **Internet als Transportmedium**. Dieses verbindet nahezu alle Rechner weltweit und steht im Gegensatz zu privat betriebenen MANs oder WANs kostenlos zur Verfügung. Der Datentransfer erfolgt innerhalb eines virtuellen Tunnels, der zwischen einem VPN-Client und einem VPN-Server aufgebaut wird.

Kommt das öffentliche Netz als Transportmedium zum Einsatz, werden Virtual Private Networks in der Regel verschlüsselt, um die Vertraulichkeit der Daten sicherzustellen. VPNs kommen zum Einsatz, um LANs über das Internet zu vernetzen oder einen Fernzugriff auf ein Netzwerk oder einen Einzelrechner über die öffentliche Verbindung zu ermöglichen.

2.8 SAN: Storage Area Network



Standards/Anwendung	Ausdehnung

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.

2.9 LoRaWAN: Low Power Wide Area Network

LoRaWAN ist eine Low Power Wide Area Network (LPWAN oder auf dt. Niedrigenergieweitverkehrsnetzwerk) Spezifikation für drahtlose batteriebetriebene Systeme in einem regionalen, nationalen oder auch globalen Netzwerk. LoRaWAN zielt dabei auf die wichtigsten Anforderungen des IoT – Internet of things (Internet der Dinge) – wie sichere bidirektionale Kommunikation, Lokalisierung und Mobilität von Dienstleistungen. Die LoRaWAN-Spezifikation bietet eine nahtlose Zusammenarbeit von verschiedenen Systemen und Techniken unter Smart Things ohne die Notwendigkeit von starren, lokalen komplexen Installationen und gibt die Freiheit für den Benutzer, Entwickler und Unternehmen wieder zurück, die das Ausrollen im Internet der Dinge ermöglichen.

Die Netzwerkarchitektur des LoRaWAN ist typischerweise in einer Stern-der-Sterne-Topologie aufgebaut, bei der die Gateways als transparente Brücke fungieren, welche die Nachrichten zwischen einem zentralen Netzwerkserver, Endgeräten und im Backend weiterleiten. Die Gateways werden über eine Standard-IP-Verbindung mit dem entsprechenden Netzwerkserver verbunden, während die Endgeräte die Single-Hop Wireless-Kommunikation zu einem oder auch mehreren Gateways verwenden. Die Endpunkt-Kommunikation ist in der Regel bidirektional. Sie unterstützt auch den Betrieb von z. B. Multicast-Enabling Software-Upgrade über die Luft oder andere Möglichkeiten zur Massenverteilung von Nachrichten, um über die Luft-Kommunikation die Übermittlungsdauer zu reduzieren.

Die Kommunikation zwischen Gateways und Endgeräten verteilt sich auf unterschiedliche Datenraten und Frequenzkanäle. Die Auswahl der Datenrate ist ein Kompromiss zwischen Nachrichtendauer und Kommunikationsbereich. Durch die Spread-Spectrum-Technologie wird die Kommunikation mit verschiedenen Datenraten nicht gegenseitig gestört und schafft eine Reihe von „virtuellen“ Kanälen, welche die Kapazität der jeweiligen Gateways erhöhen. LoRaWAN-Datenraten reichen von 0,3 kbps bis hin zu 50 kbps. Zur Maximierung der Batterielebensdauer der gesamten Netzwerkkapazität und Endgeräte verwaltet der LoRaWAN-Netzwerkserver die HF-Ausgabe und die Datenrate für alle Endgeräte individuell unter Zuhilfenahme eines adaptiven Datenraten-Schemas.

Nationale Netzwerke, die auf das Internet der Dinge, wie kritischer Infrastruktur, persönlichen vertraulichen Daten oder sehr kritischen Funktionen für die Allgemeinheit abzielen, haben einen exklusiven Bedarf an sicherer Kommunikation.

Dies wurde durch mehrere Schichten der Verschlüsselung gelöst:

- Sicherheit auf Netzwerkebene und eindeutiger Netzwerkschlüssel (EUI64)
- Ein einzigartiger Application Key (EUI64) sorgt für die Sicherheit auf der Applikationsebene
- Gerätespezifische Taste (EUI128)

LoRaWAN-Technologie verfügt über unterschiedliche Klassen von Endgeräten, die den unterschiedlichen Bedürfnissen der verschiedensten Anwendungen gerecht werden:

Bidirektionale Endgeräte (Klasse A):

Endgeräte der Klasse A gestatten bidirektionale Kommunikation, wobei die Uplink-Datenübertragung der Endgeräte von zwei kurzen Downlink-Übertragungsfenstern gefolgt wird.

Der vom Endgerät geplante Übertragungsfenster basiert auf seinen eigenen Kommunikationsbedürfnissen mit einer minimalen Anpassung basierend auf einer Zufallszeitbasis (der sogenannte ALOHA-Protokolltyp). Diese Klasse-A-Operation ist das niedrigste Leistungsgerät für Anwendungen, die nur eine Downlink-Kommunikation vom Server benötigen, kurz nachdem das Endgerät eine Uplink-Übertragung versendet hat. Downlink-Kommunikation von einem Server zu einem anderen Zeitpunkt müssen daher bis zum nachfolgend geplanten Uplink warten.

Bidirektionale Endgeräte mit vorhergesehenen Übertragungsfenster (Klasse B):

Ergänzend zu den zufälligen Übertragungsfenstern der Klasse A öffnen Class B-Geräte zu definierten Zeiten weitere zusätzliche Übertragungsfenster. Um das Endgerät sein Übertragungsfenster zum geplanten Zeitpunkt öffnen zu können, erhält es ein zeitlich synchronisiertes Beacon vom Gateway. Dadurch kann der empfangende Server wissen, wann das Endgerät hörbar ist.

Bidirektionale Endgeräte mit max. Übertragungsfenster (Klasse C):

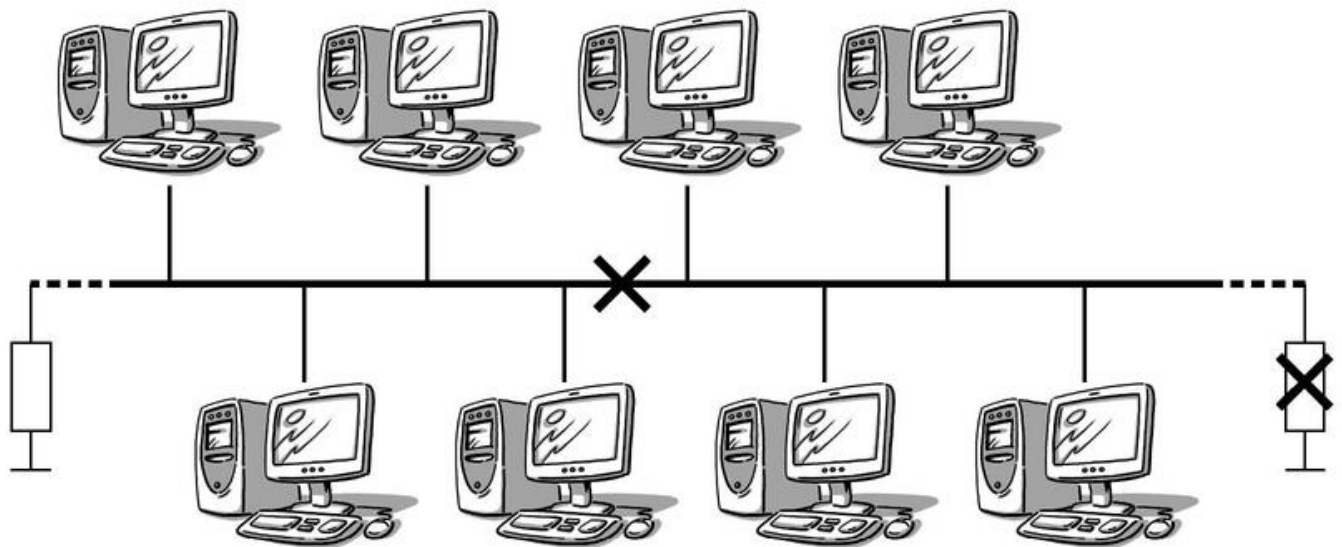
Endgeräte der Klasse C haben nahezu ständig offene Übertragungsfenster, welche nur beim Senden geschlossen sind.

3 Topologien

3.1 Begriffe

Begriff	Bedeutung/Erklärung
Latenzzeit	
Topologie	
SPOF	
Redundanz	
Backbone	

3.2 Bustopologie

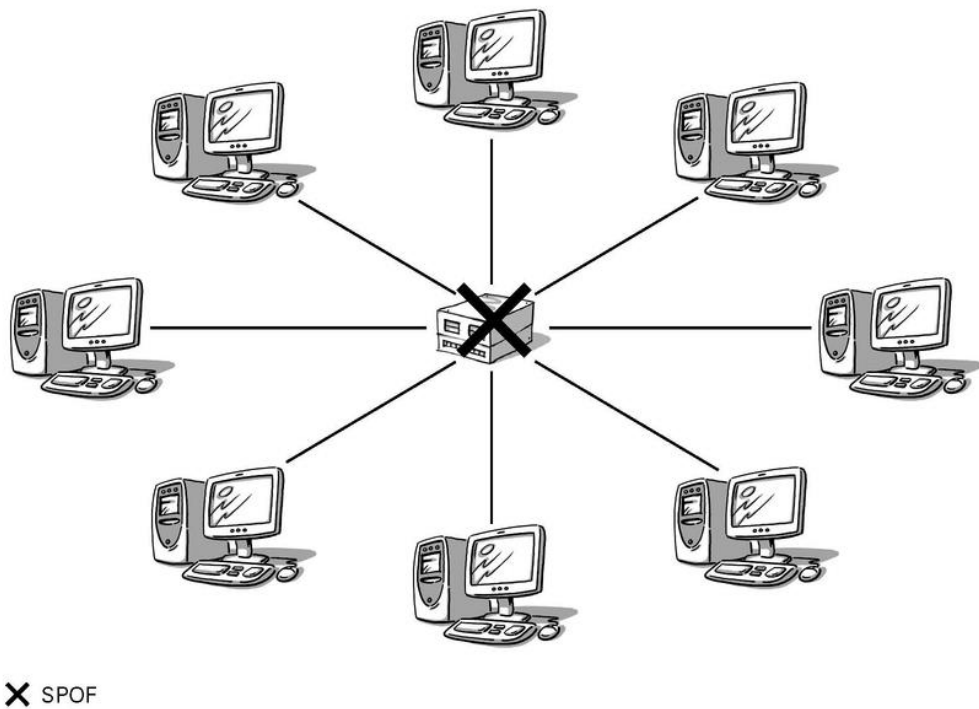


✗ SPOF

Beschreiben Sie nachfolgend kurz den Einsatz der Bustopologie und spezielle Merkmale der Bustopologie.

Bustopologie	
Vorteile	Nachteile

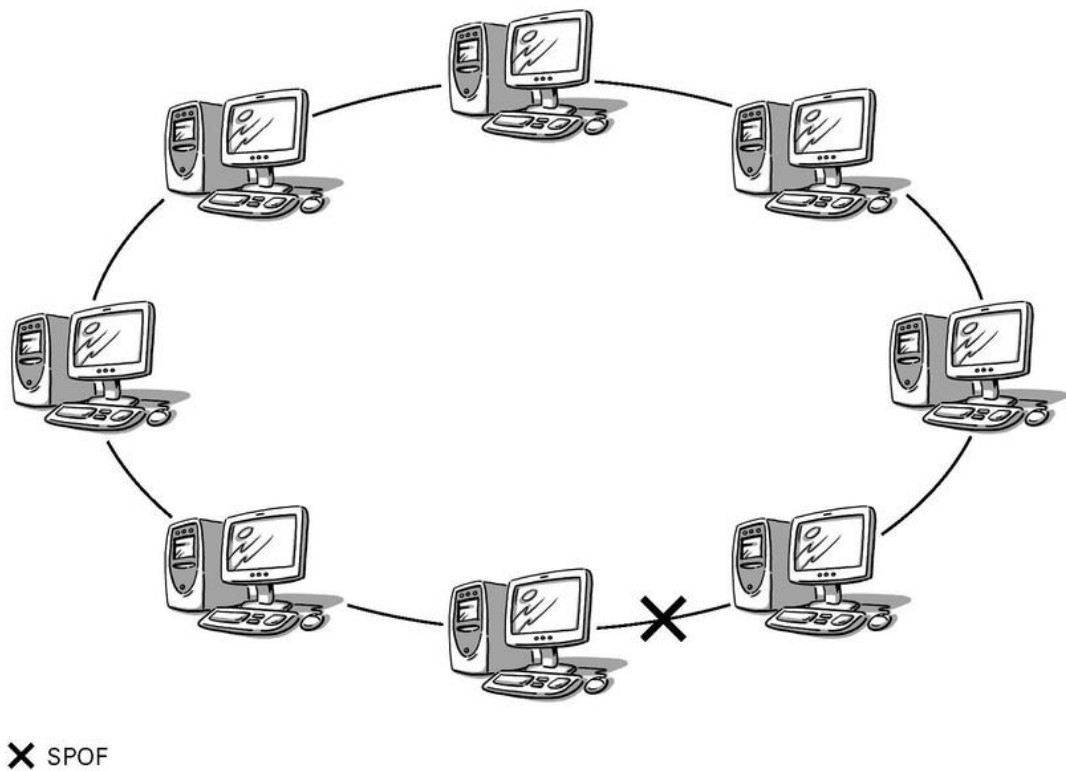
3.3 Sterntopologie



Beschreiben Sie nachfolgend kurz den Einsatz der Sterntopologie und spezielle Merkmale der Sterntopologie.

Sterntopologie	
Vorteile	Nachteile

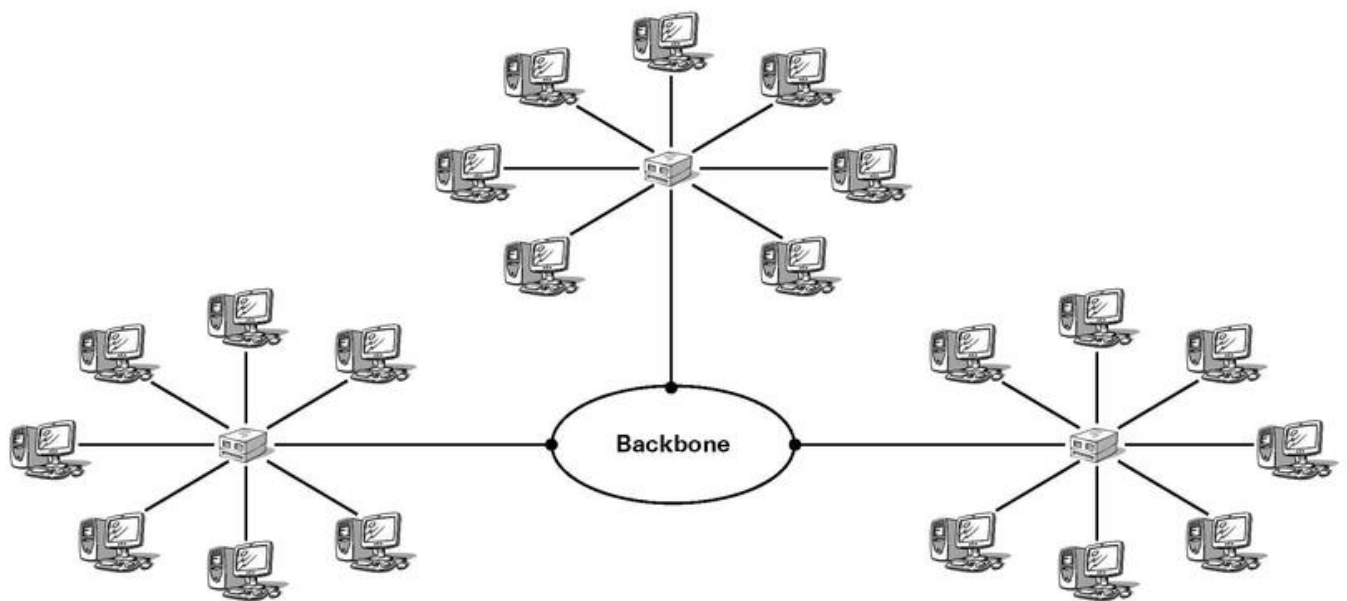
3.4 Reine Ringtopologie



Beschreiben Sie nachfolgend kurz den Einsatz der Ringtopologie und spezielle Merkmale der Ringtopologie.

Reine Ringtopologie	
Vorteile	Nachteile

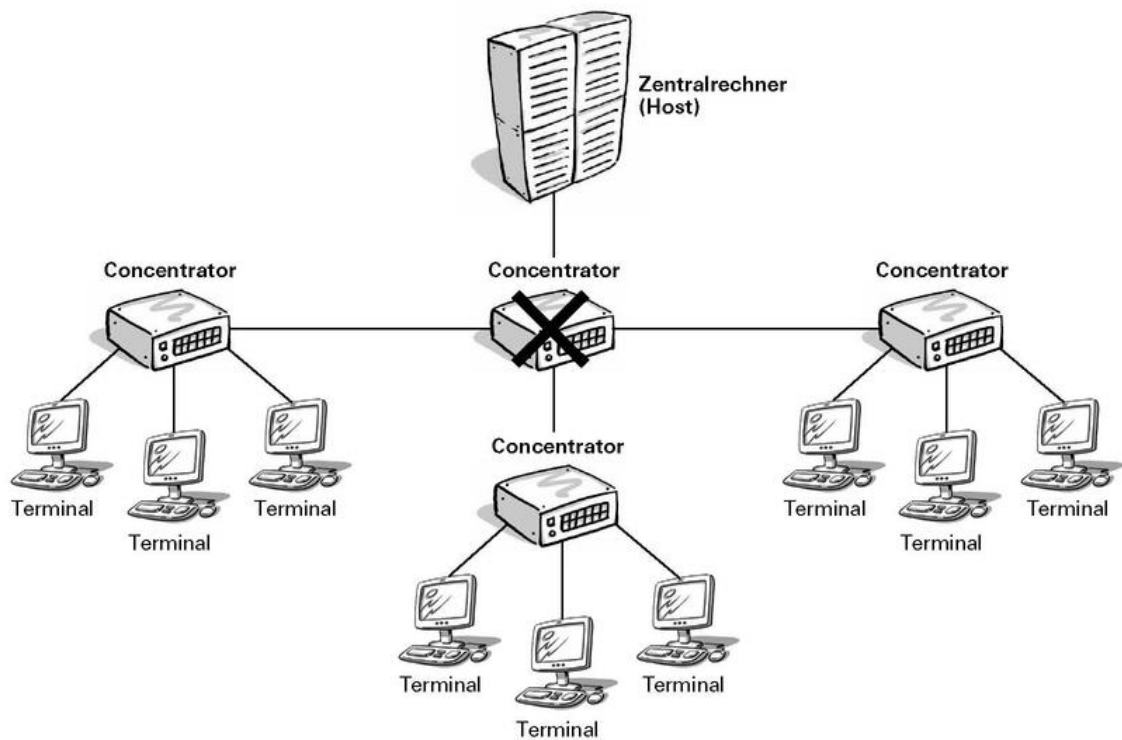
3.5 Ringtopologie mit Backbone



Beschreiben Sie nachfolgend kurz den Einsatz der Ringtopologie und spezielle Merkmale der Ringtopologie.

Ringtopologie mit Backbone	
Vorteile	Nachteile

3.6 Baumtopologie

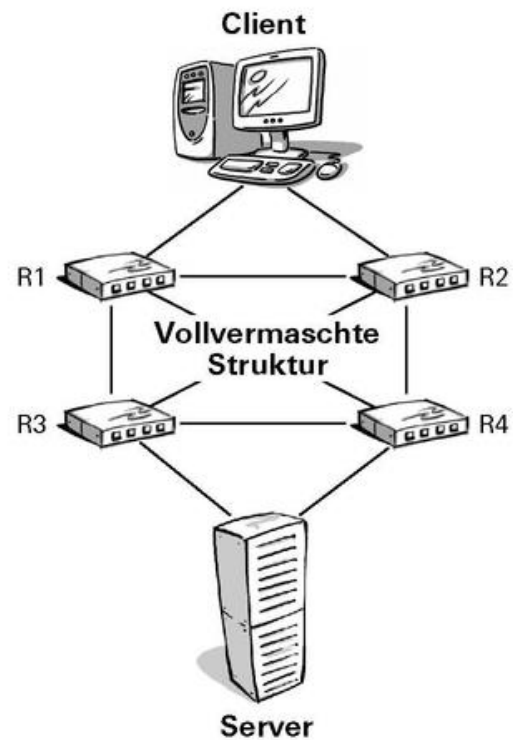
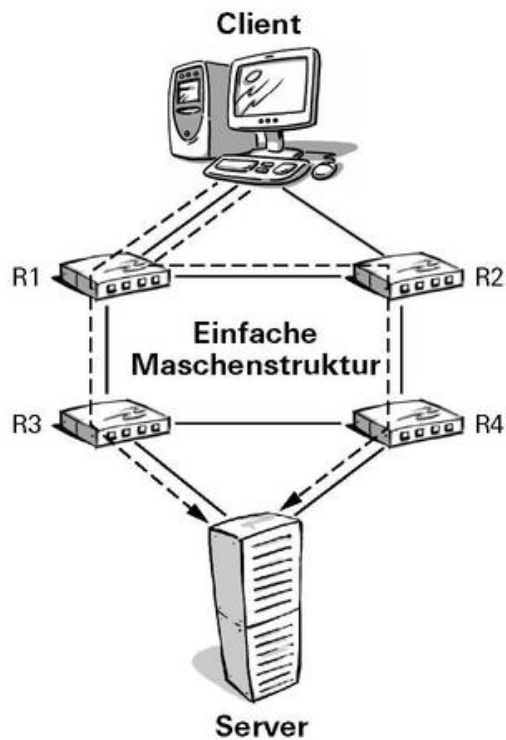


X SPOF

Beschreiben Sie nachfolgend kurz den Einsatz der Baumtopologie und spezielle Merkmale der Baumtopologie.

Baumtopologie	
Vorteile	Nachteile

3.7 Maschentopologie (Mesh)



R = Router

Beschreiben Sie nachfolgend kurz den Einsatz der Maschentopologie und spezielle Merkmale der Maschentopologie.

Maschentopologie (Mesh)	
Vorteile	Nachteile

3.8 Zusammenfassung

Netzwerke werden zur besseren Einordnung bzw. Abgrenzung gemäss ihrer Ausdehnung einer bestimmten Kategorie zugeteilt. Diese Einteilung kann hilfreich sein, sich ein Bild von einem Netzwerk zu machen. Problematisch an dieser Zuweisung kann sein, dass diese Kategorien nicht verbindlich standardisiert sind und deshalb die Grenzen zwischen den einzelnen Kategorien etwas unscharf sein können.

Bei einer bestimmten Topologie ist es wichtig, zu erkennen, wo sich der sog. SPOF befindet. Sobald diese zentrale Schwachstelle identifiziert ist, gilt es Massnahmen zu treffen, damit bei einem Ausfall an diesem Ort nicht das ganze Netzwerk in Mitleidenschaft gezogen wird. Nur die Maschentopologie weist keinen SPOF auf. Mittels redundanter oder fehlertoleranter Massnahmen lassen sich SPOFs gezielt entschärfen.

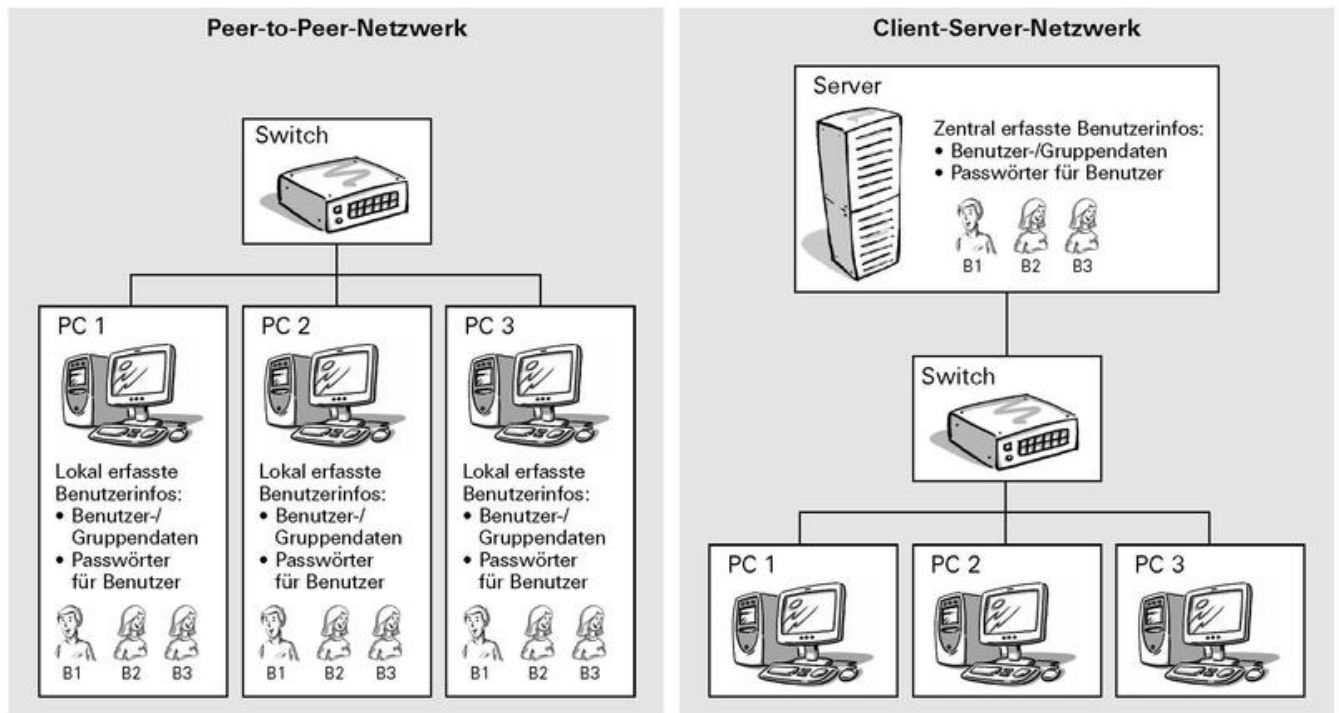
3.9 Abschlussfragen

Erklären Sie, weshalb eine Maschentopologie keinen SPOF besitzt.

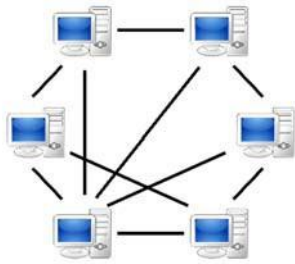
Zählen Sie zwei grundsätzliche Unterschiede zwischen einem CAN und einem WAN auf.

Welcher Umstand kann bei einer Satellitenverbindung zu Problemen führen?

4 Betriebsarten von Netzwerken



5 Peer-to-Peer Netzwerk



Wenn alle Computer im Netzwerk gleichberechtigt sind und ihre Ressourcen wie Daten, Drucker und weitere Peripherie frei zur Verfügung stellen können, spricht man von einem Peer-to-Peer (jeder mit jedem) Netzwerk.

Peer-to-Peer (P2P) Connection (von englisch peer ‚Gleichgestellter‘, ‚Ebenbürtiger‘) und Rechner-Rechner-Verbindung sind synonyme Bezeichnungen für eine Kommunikation unter Gleichen, hier bezogen auf ein Rechnernetz. In einigen Kontexten spricht man auch von Querkommunikation.

Die Koordination erfolgt durch alle Teilnehmer, die vollen Zugriff auf ihre Ressourcen und Geräte haben. Das erfordert einen entsprechenden Aufwand, der bis zu ca. zehn Clients sinnvoll geleistet werden kann. Im Microsoftumfeld spricht man von sogenannten Arbeitsgruppen (engl. Workgroup, Heimnetz ab Windows 7). Peer-to-Peer findet man deshalb im Allgemeinen nur bei kleineren Netzwerken oder wenn bewusst auf zentrale Dienste verzichtet werden soll.

In einem reinen Peer-to-Peer-Netz sind alle Computer gleichberechtigt und können sowohl Dienste in Anspruch nehmen, als auch zur Verfügung stellen. In modernen P2P-Netzwerken werden die Netzwerkteilnehmer jedoch häufig abhängig von ihrer Qualifikation in verschiedene Gruppen eingeteilt, die spezifische Aufgaben übernehmen. Kernkomponente aller modernen Peer-to-Peer-Architekturen, die meist bereits als Overlay-Netzwerk auf dem Internet realisiert werden, ist daher ein zweites internes Overlay-Netzwerk, welches normalerweise aus den besten Computern des Netzwerks besteht und die Organisation der anderen Computer sowie die Bereitstellung der Such-Funktion übernimmt.

Mit der Lookup-Operation können Peers im Netzwerk diejenigen Peers identifizieren, die für eine bestimmte Objektkennung (Object-ID) zuständig sind. In diesem Fall ist die Verantwortlichkeit für jedes einzelne Objekt mindestens einem Peer fest zugeteilt, man spricht daher von strukturierten Overlays. Mittels der Such-Operation können die Peers nach Objekten im Netzwerk suchen, die gewisse Kriterien erfüllen (z. B. Datei- oder Buddynamen-Übereinstimmung). In diesem Fall gibt es für die Objekte im P2P-System keine Zuordnungsstruktur, man spricht also von unstrukturierten Overlays.

Sobald die Peers, die die gesuchten Objekte halten, in dem P2P-System identifiziert wurden, wird die Datei (in Dateitauschbörsen) direkt, d. h. von Peer zu Peer, übertragen. Es existieren verschiedene Verteilungsstrategien, welche Teile der Datei von welchem Peer heruntergeladen werden soll, z. B. BitTorrent.

Der Gegensatz zum Peer-to-Peer-Modell ist das Client-Server-Modell. Bei diesem bietet ein Server einen Dienst an und ein Client nutzt diesen Dienst. In Peer-to-Peer-Netzen ist diese Rollenverteilung aufgehoben. Jeder Teilnehmer ist ein peer, denn er kann einen Dienst gleichermaßen nutzen und selbst anbieten.

5.1 Charakterisierung von Peer-to-Peer Netzwerken

Typische, aber nicht notwendige Charakteristika von Peer-to-Peer-Systemen sind:

- Peers weisen eine hohe Heterogenität bezüglich der Bandbreite, Rechenkraft, Online-Zeit, ... auf.
- Die Verfügbarkeit/Verbindungsqualität der Peers kann nicht vorausgesetzt werden („Churn“).
- Peers bieten Dienste und Ressourcen an und nehmen Dienste anderer Peers in Anspruch (Client- Server-Funktionalität).
- Dienste und Ressourcen können zwischen allen teilnehmenden Peers ausgetauscht werden.
- Peers bilden ein Overlay-Netzwerk und stellen damit zusätzliche Such/Lookup-Funktionen zur Verfügung.
- Peers haben eine signifikante Autonomie (über die Ressourcenbereitstellung).
- Das P2P-System ist selbstorganisierend.
- Alle übrigen Systeme bleiben konstant intakt und nicht skaliert.

5.2 Typen von Peer-to-Peer


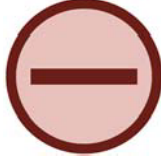
P2P-Systeme lassen sich in unstrukturierte und strukturierte P2P-Systeme unterteilen.

Unstrukturierte P2P-Systeme unterteilen sich nochmals nach der Art ihres Aufbaus. Man unterscheidet:

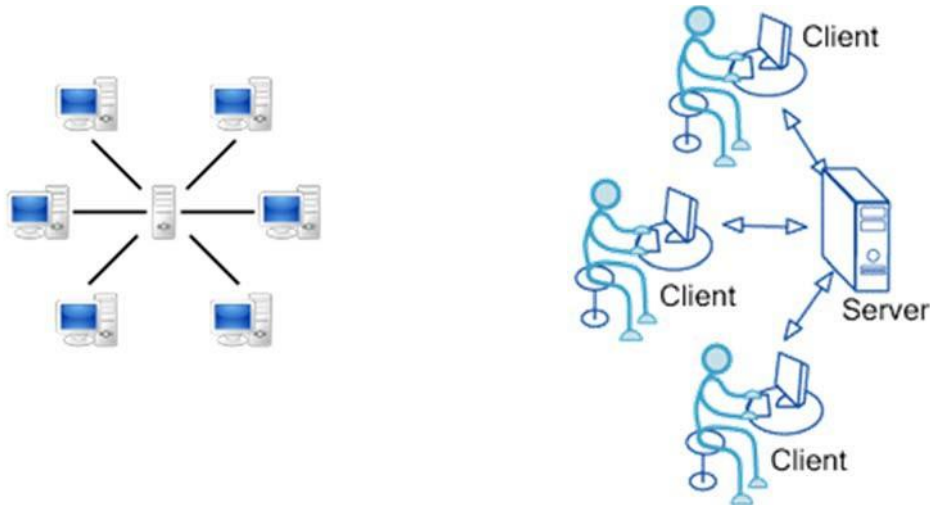
- Zentralisierte P2P-Systeme (Beispiel: Napster), welche einen zentralen Server zur Verwaltung benötigen, um zu funktionieren
- Reine P2P-Systeme ohne zentrale Instanz (Beispiele: Gnutella 0.4, Freenet) Eine spezielle Art eines reinen, dezentralen Netzwerkes bildet das friend-to-friend- oder Web-of-Trust-Netzwerk, bei dem keinerlei Verbindungen zu unbekannten IP-Adressen unterhalten werden, sondern ausschließlich Verbindungen zu Freunden (trusted friends) etabliert werden.
- Hybride bzw. Hierarchische P2P-Systeme, welche dynamisch mehrere zentrale Server („Superknoten“) zur Verwaltung bestimmen (Beispiele: Gnutella 0.6, Gnutella2 (G2), JXTA)
- Zentralisierte und reine P2P-Systeme bezeichnet man als Systeme erster Generation während dezentrale Systeme als Systeme zweiter Generation bezeichnet werden. Systeme, die Dateien über nicht-direkte Verbindungen weiterreichen, sind Systeme dritter Generation. Siehe dazu auch ausführlich den Begriff Filesharing.

5.3 Vor-/Nachteile von Peer-to-Peer

Überlegen Sie sich, welche Vorteile sprechen für ein Peer-to-Peer Netzwerk, welche Nachteile können entstehen?

6 Client-Server Architektur



6.1 Definitionen

Server (deutsch: Bediener, Anbieter, Dienstleister, Bereitsteller, englisch: to serve)

Ein Server ist ein Programm (Prozess), das mit einem anderen Programm (Prozess), dem Client (deutsch: Kunde), kommuniziert, um ihm Zugang zu einem Dienst zu verschaffen. Hierbei muss abgrenzend beachtet werden, dass es sich bei "Server" um eine Rolle handelt, nicht um einen Computer an sich. Ein Computer kann nämlich ein Server und Client zugleich sein, siehe: Peer-to-Peer.

Client (deutsch: Kunde, Dienstinutzer)

Ein Client kann einen Dienst bei dem Server anfordern, welcher diesen Dienst bereitstellt.

Dienst (englisch: Service)

Vereinbarung einer festgelegten Aufgabe, die der Server anbietet und der Client nutzen kann.

Request (deutsch: Anforderung, Anfrage)

Anforderung eines Clients an den Server, dessen Dienst er benötigt.

Response (deutsch: Antwort)

Antwort eines Servers auf eine Anforderung eines Clients

6.2 Client/Server Modell

Das Client-Server-Modell ist das Standardkonzept für die Verteilung von Aufgaben innerhalb eines Netzwerks. Aufgaben werden mittels Server auf verschiedene Rechner verteilt und können bei Bedarf von mehreren Clients zur Lösung ihrer eigenen Aufgaben oder Teilen davon angefordert werden. Bei den Aufgaben kann es sich um Standardaufgaben (E-Mail-Versand, E-Mail-Empfang, Web-Zugriff, etc.) oder um spezifische Aufgaben einer Software oder eines Programms handeln. Eine Aufgabe wird im Client- Server-Modell als Dienst bezeichnet.

Ein Server ist ein Programm, das einen Dienst (Service) anbietet. Im Rahmen des Client-Server-Konzepts kann ein anderes Programm, der Client, diesen Dienst nutzen. Die Kommunikation zwischen Client und Server ist abhängig vom Dienst, d. h. der Dienst bestimmt, welche Daten zwischen beiden ausgetauscht werden. Der Server ist in Bereitschaft, um jederzeit auf die Kontaktaufnahme eines Clients reagieren zu können. Im Unterschied zum Client, der aktiv einen Dienst anfordert, verhält sich der Server passiv und wartet auf Anforderungen. Die Regeln der Kommunikation für einen Dienst (Format, Aufruf des Servers,

und die Bedeutung der zwischen Server und Client ausgetauschten Daten), werden durch ein für den jeweiligen Dienst spezifisches Protokoll festgelegt.

Clients und Server können als Programme auf verschiedenen Rechnern oder auf demselben Rechner ablaufen. Allgemein kann das Konzept ausgebaut werden zu einer Gruppe von Servern (Software), die eine Gruppe von Diensten anbietet. Beispiele: Mail-Server, (erweiterter) Web-Server, Anwendungsserver, Datenbank-Server.

Da in der Praxis diese Server meist gesammelt auf bestimmten Rechnern laufen, hat es sich eingebürgert, diese Rechner selbst als Server zu bezeichnen. Die gleichen Beispiele: Mail-Server, Web-Server, Anwendungsserver, ...Datenbank-Server.

6.3 Unterschiede zu Peer-to-Peer

Im Unterschied zum Peer-to-Peer-Modell, bei dem ein beteiligtes Programm innerhalb des Netzwerkes gleichzeitig Client und Server darstellt, sind beim Client-Server-Modell die Komponenten Client und Server getrennt und auf verschiedene Programme verteilt.

6.4 Client-Server System

Ein Client-Server-System ist eine Software (Anwendungssystem), welche für ihre Aufgaben und Funktionen vom Client-Server-Modell Gebrauch macht. Anders ausgedrückt wurde die Software so entwickelt, dass sie das Client-Server-Modell nutzen kann. Das System besteht daher mindestens aus zwei Teilen, einer Server- und einer Client-Komponente, die in der Regel auf verschiedenen Rechnern ablaufen.

6.4.1 Beispiel eines Client-Server-Systems mit zentralem Datenbankserver

Das Client-Server-System bildet eine Netzwerkstruktur, bestehend aus dem zentralen Datenbankserver als Server-Komponente und mehreren Benutzer-Clients als Client-Komponente. Den Client bildet das Anwendungsprogramm, über dessen Benutzerschnittstelle der Benutzer über das Netzwerk auf Ressourcen des Datenbankservers zugreift. Er liest und pflegt die Daten in der Datenbank durch „Abschicken“ von SQL-Befehlen. Jeden SQL-Befehl sendet der Client als Anforderung an den Server um diesen ausführen zu lassen. Das Ergebnis (Daten oder Fehlermeldung) liefert der Server als Antwort an den Client zurück.


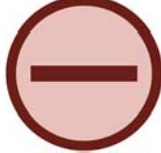
6.5 Grundsätzliche Funktionsweise

Der Client stellt eine Anfrage an den Server. Der Server reagiert darauf mit einer Antwort.

Bei Client/Server Netzwerken werden die Aufgaben den speziell dazu bestimmten Netzwerkteilnehmern zugeordnet. In Client/Server Netzwerken gibt es zwei Arten von Netzwerkteilnehmern: Arbeitsstationen (engl. Workstation oder Desktop), an denen die Benutzer arbeiten und mindestens einen Server, der die verlangten Serverdienste zur Verfügung stellt.

6.6 Vor-/Nachteile von Client/Server Modellen

Überlegen Sie sich, welche Vorteile sprechen für ein Client/Server Modell, welche Nachteile können entstehen?

6.7 Zusammenfassung

Im Grunde spricht nichts gegen den Einsatz von Peer-to-Peer Netzwerken. Der Betrieb eines LANs als reines P2P Netz scheint sogar auf den ersten Blick recht einfach und unproblematisch zu sein. Dennoch muss die Wahl dieser Betriebsart gut überlegt sein, da man sich möglicherweise Probleme einhandelt, die auf den ersten Blick nicht erkennbar waren, aber später umso aufwendiger zu beheben sind. Ein Peer-to-Peer Netz eignet sich erfahrungsgemäss nur für Umgebungen mit sehr wenigen Benutzern.

Client-Server Netzwerke hingegen eignen sich auch für Umgebungen mit wenigen Benutzern, aber auch für Netze mit mehreren Tausend Benutzern. So oder so muss vor der Wahl der optimalen Betriebsart eine gründliche Analyse der Anforderungen an das Netzwerk erfolgen.

6.8 Abschlussfragen

Bis zu welcher Anzahl von Rechnern kann ein Peer-to-Peer Netzwerk vernünftig betrieben werden (im geschäftlichen Sinn, nicht Torrent Netzwerke)?

Nennen Sie zwei Unterschiede zwischen Peer-to-Peer und Client/Server Netzwerken.

Bei welchem Typ von Netzwerken erfolgt die Administration zentral?

Wie viele Computer sind im Minimum für ein Client/Server-Netzwerk nötig?

Welchen Netzwerktyp setzen Sie bei sich zu Hause ein? Zeichnen Sie einen möglichen Netzplan auf.

7 Kabel- und Funktechnologie

Beim Bau eines Netzwerks wird man zwangsläufig mit den unterschiedlichen Kabel- und Funktechnologien konfrontiert. Bei der Verwendung einer bestimmten Technologie sollte unbedingt darauf geachtet werden, dass diese auf einem international anerkannten und offenen Standard basiert. Bei Netzwerklösungen, die auf proprietären Standards basieren, besteht die Gefahr, dass Produkte (Komponenten) verschiedener Hersteller untereinander nicht funktionieren, sprich diese zueinander inkompatibel.

7.1 Kabelbasierende Netzwerke

Für die Übertragung der Daten in einem Netzwerk wird sog. Übertragungsmedium benötigt. Bei einem Netzwerk, das auf Kabeln basiert, spricht man in diesem Fall von einer «gebundenen» Übertragung. Die Datenübertragung wird mittels elektrischem Strom oder optischer Signale vorgenommen. Diese Signale sind auf das jeweilige Übertragungsmedium gebunden. Für die Realisation eines Netzwerks stehen verschiedene Kabeltypen zur Auswahl. Jeder Kabeltyp besitzt unterschiedliche spezifische Eigenschaften. Jede Übertragung im Kabel wird durch bestimmte Faktoren beeinflusst. Diese Faktoren müssen besonders beachtet werden:

Elektromagnetische Störungen (Magnetfelder)

.....

.....

.....

.....

.....

Der Widerstand eines Übertragungsmediums (Dämpfung)

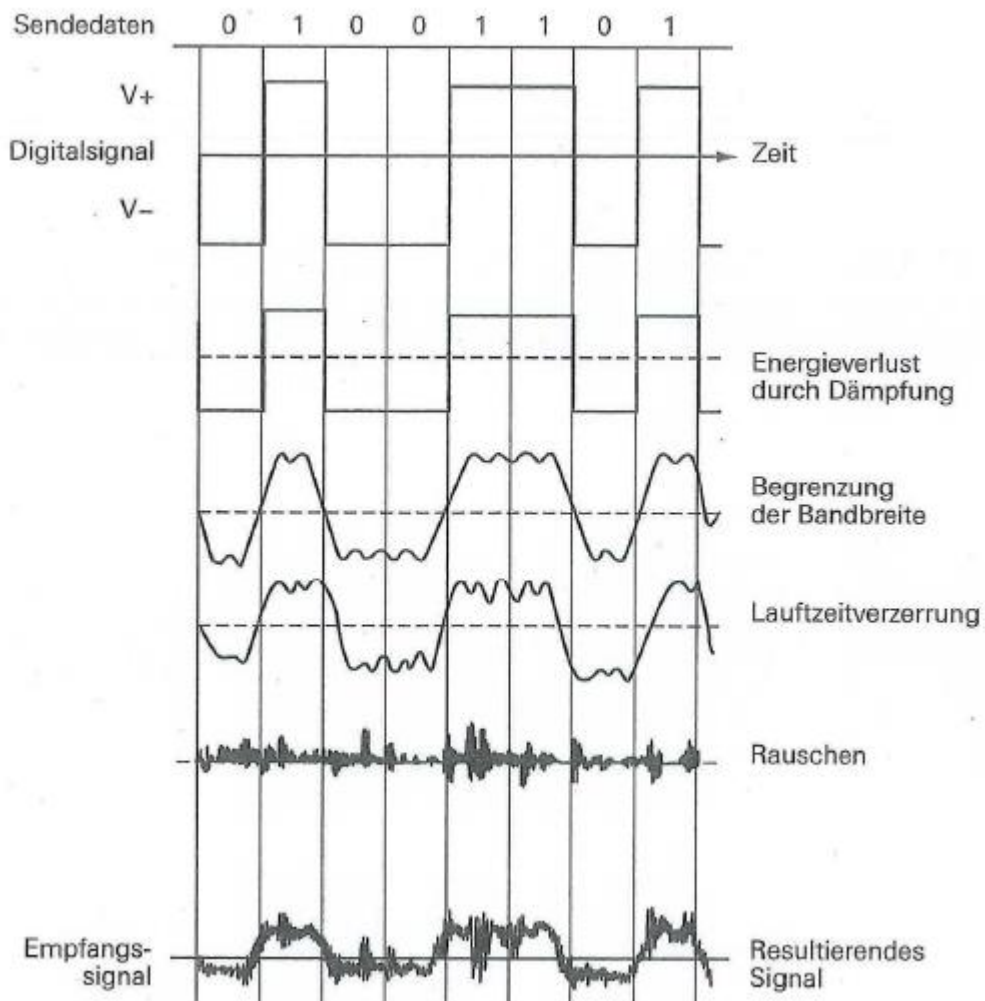
.....

.....

.....

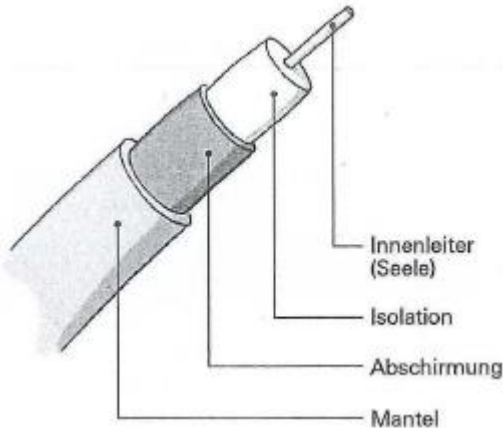
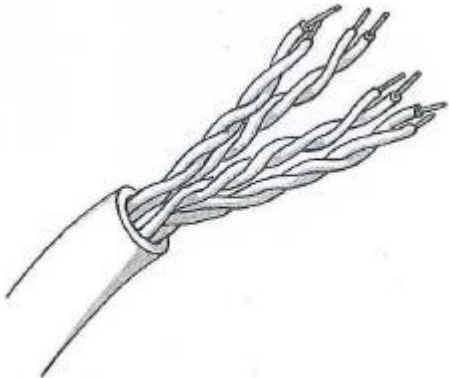
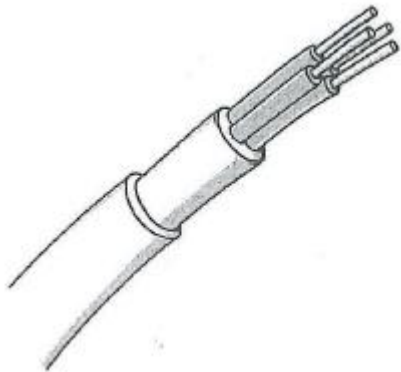
.....

.....

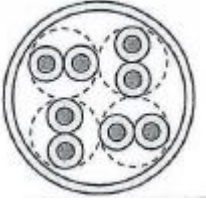
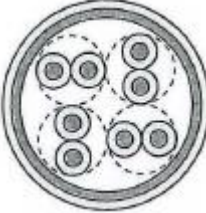
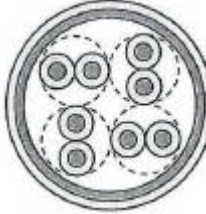
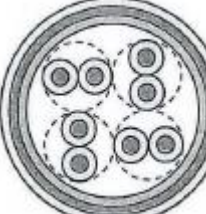
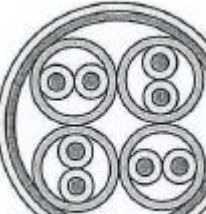


Massnahmen gegen elektromagnetische Störungen:

7.2 Kabeltypen

IEEE	Kabelbezeichnung	Topologie	Bandbreite	Max. Länge	Bemerkung
					
					
					

7.2.1 Twisted-Pair-Kabel

Bezeichnung	Querschnitt	Beschreibung	Vor-/Nachteile
U/UTP Kabel		Bestehen aus je zwei Kupferadern, die ohne Abschirmung paarweise verdreht sind. Das Kabel verfügt über keinerlei Abschirmung	
STP Kabel		Besitzen einen Gesamtschirm aus einem Drahtgeflecht	
FTP Kabel		Besitzen einen Gesamtschirm aus meist alukaschierten Kunststoffolie	
S/FTP Kabel		Besitzen einen Gesamtschirm aus meist alukaschierten Polyesterfolie und darüber liegendem Kupfergeflecht	
S/STP Kabel		Besitzen eine Abschirmung für jedes Kabelpaar sowie eine Gesamtabschirmung. Auch PIMF genannt, Pair in Metal Foil	

Kategorie	Typ	Bandbreite	Anwendung	Bemerkungen
Cat3	UTP	16 MHz	10BASE-T	Wird nicht mehr eingesetzt.
Cat4	UTP	20 MHz	IEEE 802.5	Wird nicht mehr eingesetzt.
Cat5	UTP	100 MHz	10 / 100BASE-TX (2 Pairs) 100BASE-T4 (4 Pairs)	Absolutes Minimum im Netzbereich, 4 Pairs wurde kaum eingesetzt.
Cat5e	UTP/STP	125 MHz	10 / 100 / 1000BASE-T	Verbesserte Eigenschaften gegen Crosstalk und magnetische Abstrahlung.
Cat6a	STP	500 MHz	Bis 10GBASE-T	Bei Verwendung von UTP ist die max. Segmentlänge < 50 m.
Cat7	S/FTP	600 MHz	Bis 10GBASE-T	10G Ethernet befindet sich auf dem Vormarsch.

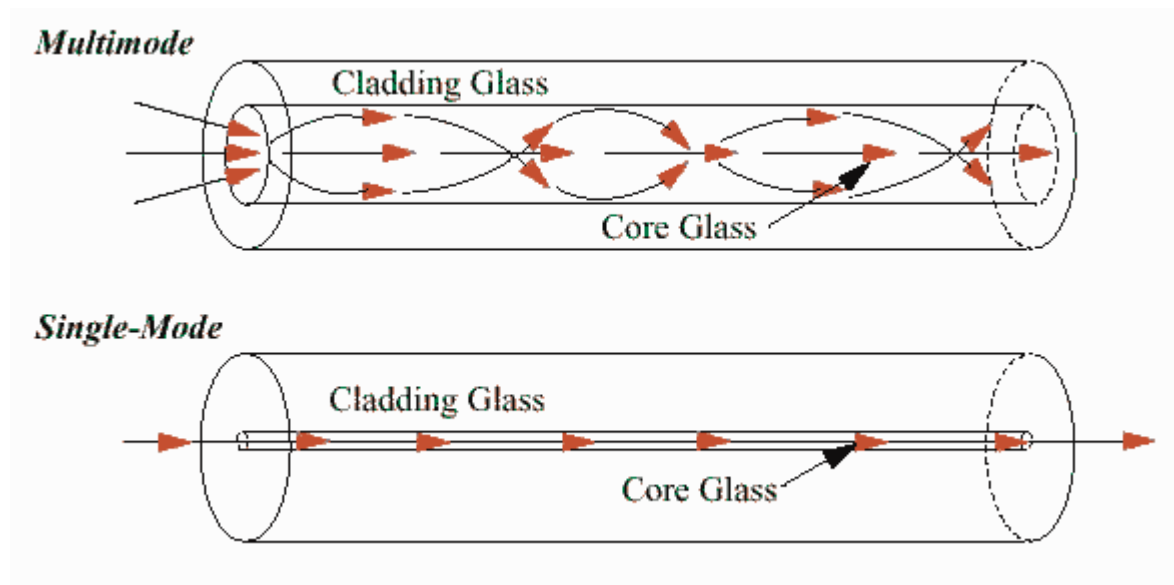
Hinweis:

.....

.....

7.2.2 Glasfaserkabel

Umwandlung und Übertragung des optischen Signals im Glasfaserkabel



7.2.3 Vergleich Twisted-Pair/Glasfaserkabel

Eigenschaft	TP	LWL	Bemerkungen
Anfälligkeit gegen äussere Störeinflüsse	Hoch	Sehr gering	LWL ist immun gegen Magnetfelder.
Max. Übertragungskapazität	Hoch	Extrem hoch	TP max. Ü-Kapazität ≈ 100 Gbit/s.
Max. Übertragungsdistanz	Gering	Sehr hoch	TP kann mittels einer Verstärkung weiter als 100 m übertragen, max. 500 m.
Anschaffungskosten (Ü-Medium)	Tief	Hoch	TP Cat6a STP \approx CHF 0.75 p. M. LWL multim. $62.5 \mu\text{m}$ \approx CHF 1.80 p. M.
Konfektionierungskosten ^[1]	Tief	Hoch	LWL benötigt sehr spezielle und teure optische Messgeräte sowie spezielles Know-how und spezielle Fertigkeiten.
Kosten für Kabelverlegung	Mittel	Hoch	LWL empfindlich gegen mechanische Einwirkungen, keine enge Radien möglich.
Abhörsicherheit	Gering	Sehr hoch	Auch ein LWL kann von aussen abgehört werden, der technische Aufwand dazu ist aber enorm hoch.

7.3 Funkbasierte Netzwerke

Funknetzwerke übertragen Daten mithilfe elektrischer Impulse (Signale). Diese Impulse auch elektromagnetische Wellen genannt, sind nicht zwingend auf ein bestimmtes Übertragungsmedium gebunden. Daher spricht man bei Funknetzen auch von einer ungebundenen Übertragung. Funkwellen können im Grunde alle Medien verwenden, in denen sich elektromagnetische Wellen übertragen lassen. Elektromagnetische Wellen können sich auch im freien Raum (Äther) ausbreiten und brauchen somit nicht einmal ein spezifisches Übertragungsmedium.

Ähnlich wie bei Kabelnetzwerken werden auch Funknetzwerke von bestimmten Faktoren beeinflusst. Folgende Faktoren sind bei Funknetzwerken zu beachten:

Andere benachbarte Funknetze: Elektromagnetische Wellen (Funkwellen) können sich gegenseitig «überlagern» und somit eine Übertragung verunmöglichen. Man spricht in diesem Fall von Interferenzen. Dies passiert v. a. dann, wenn die Funkwellen im gleichen Frequenzbereich arbeiten. Aus diesem Grund benutzen Funknetzwerke die sog. ISM-Frequenzbänder. Diese Frequenzbänder sind international normiert und stehen jedermann frei zur Verfügung. Für WLANs wurden bestimmte Frequenzen im 2.4-GHz- und im 5-GHz-Band reserviert. Das 2.4-GHz-Band ist mittlerweile international einheitlich geregelt. Die Aufteilung des 5-GHz-Bands hingegen kann von Land zu Land stark variieren.

7.3.1 Betriebsarten

Adhoc Mode

Infrastructure Mode

IEEE 802.3 – LAN-Standards			
Standard	Topologie	Segmentlänge	Bemerkungen
802.3u (10BASE-T)	Stern	100 m, mit UTP	Abwärtskompatibel zu 10BASE-T
802.3C26 (10BASE-SX)	Stern	550 m, mit LWL	Abwärtskompatibel zu 10BASE-FL
802.3ab (1GBASE-T)	Stern	100 m, mit UTP	
802.3z (1GBASE-L/SX)	Stern	5 km, mit LWL	
802.3ae (10GBASE-L/SX)	Stern	10 km, mit LWL	

IEEE 802.11– WLAN-Standards			
Standard	F-Band	Datenrate	Bemerkungen
802.11a	5 GHz	54 Mbit/s	
802.11b	2.4 GHz	11 Mbit/s	Nur noch aus Kompatibilitätsgründen
802.11g	2.4 GHz	54 Mbit/s	
802.11h	5 GHz	54 Mbit/s	
802.11n	2.4 GHz	~ 300 Mbit/s	Benötigt MIMO-Technologie (Antennen)
802.11n	5 GHz	600 Mbit/s	Benötigt MIMO-Technologie (Antennen)
802.11ac	5 GHz	6 933 Mbit/s	Direkte Weiterentwicklung von 802.11n mit 8-fach-MIMO-Technologie

Power over Ethernet IEEE 802.3af: Stromversorgung via Netzkabel

Immer mehr Geräte verfügen über eine RJ45-Netzwerkschnittstelle. Dies sind Geräte (Devices) wie z. B. Webkameras, Telefonapparate, Miniswitches, Print Server etc. Aus diesem Grund wurde mit Power over Ethernet (PoE) die Möglichkeit geschaffen, die elektrische Energie für das Netzwerkgerät direkt mit dem Netzkabel zur Verfügung zu stellen. Das Ganze funktioniert über Twisted-Pair-Kabel (UTP Cat. 5 oder besser). Die maximale Energieleistung via Netzkabel beträgt 25.5 Watt. Und sollte mal ein nicht PoE-taugliches Netzwerkgerät in einen Port mit aktiver PoE-Funktion eingesteckt werden, so passiert dennoch nichts. Eine integrierte Schutzschaltung von PoE verhindert, dass ein PoE-untaugliches Gerät Schaden nehmen kann.

7.3.2 Gegenüberstellung LAN/WLAN

Eigenschaft	LAN	WLAN	Bemerkung
Anfälligkeit gegenüber äusseren Störeinflüssen			
Übertragungskapazität (Bandbreite)			
Übertragungsdistanzen			
Anschaffungskosten (Ü-Medium)			
Konfektionierungskosten			
Kosten für Kabelverlegung (Installation)			
Aufwand für die Realisierung			
Abhörsicherheit			

7.4 Standards im LAN Bereich

<http://standards.ieee.org/about/get/>

- IEEE 802.3 – Netzwerke basierend auf Ethernet (CSMA/CD)
- IEEE 802.11 – Wireless Local Area Network (WLAN)

7.4.1 Datenpaket

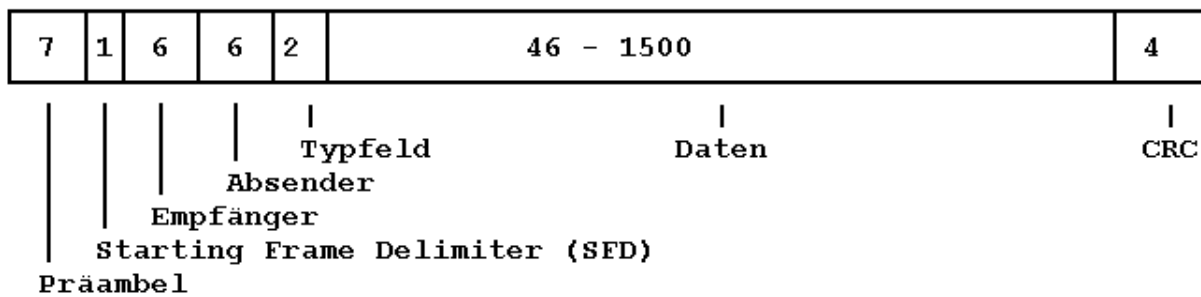
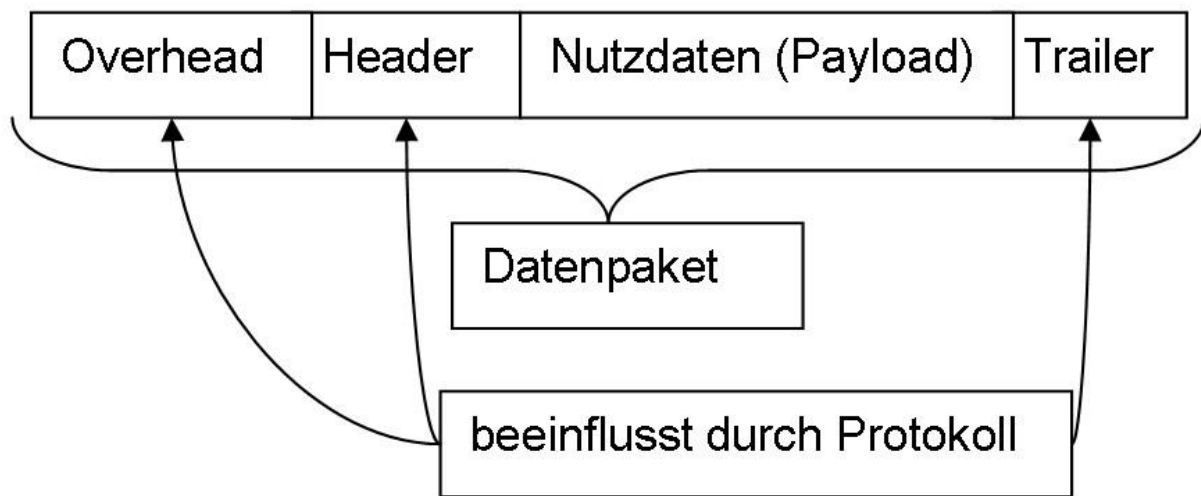
Ein Datenpaket ist in der Datenverarbeitung ganz allgemein eine der Bezeichnungen für in sich geschlossene Dateneinheiten, die ein Sender (z. B. ein digitaler Messfühler) oder auch ein sendender Prozess einem Empfänger (z. B. einer Messstation über eine RS232-Kabelverbindung) sendet (vergl.: Rahmen (Nachrichtentechnik)). Ein solches Datenpaket – im Unterschied zu einem Datenstrom – hat eine wohldefinierte Länge und Form, es kann daher auf Vollständigkeit und Brauchbarkeit geprüft werden. Das OSI-Schichtenmodell ist für solche Pakete kaum sinnvoll, da 4 von 7 OSI-Schichten (Darstellungsschicht, Sitzungsschicht, Transportschicht und Vermittlungsschicht) hier belanglos sind und nicht implementiert werden.

Auch in Computernetzen wird dieser Ausdruck gebraucht, ein Datenpaket ist dort eine der Bezeichnungen für die Dateneinheiten, die in einem Computernetz oder Telekommunikationsnetz versendet werden. Dazu zählen in erster Linie die Dateneinheiten auf Schicht 3 des OSI-Modells, der Begriff wird aber auch häufig nicht ganz korrekt für die Protocol Data Units der anderen Schichten verwendet.

Der größte Teil von Datenpaketen besteht aus den zu verschickenden Informationen. Außerdem enthält es wichtige Adressierungs- und Verwaltungsinformationen - in IP-basierten Netzwerken zum Beispiel die Quell- und Ziel-IP-Adressen, um das Paket an den richtigen Computer zu liefern. Solche Informationen sind oft im sogenannten Header eingetragen. Eine Netzwerkverbindung überträgt gewöhnlich mehrere Datenpakete, die nicht unbedingt über denselben Weg desselben physikalischen Netzes geroutet werden.

Normalerweise wird der Begriff Datagramm synonym mit Datenpaket verwendet. Gelegentlich werden sie aber auch voneinander unterschieden. So wird ein Datagramm oft als Datenpaket betrachtet, dessen Zusatzinformation unter anderem Sender- und Empfängeradresse, aber auch Ordnungsnummer und Fehlerkorrekturschlüssel enthält, während ein Datenpaket allgemein als jede Dateneinheit betrachtet wird, die über Netze übertragen wird, die auf Paketvermittlung basieren. Im Gegensatz zu Protocol Data Unit und Service Data Unit ist der Begriff Datenpaket nicht genau definiert.

Speziell bei serieller Übertragung wird statt von einem Datenpaket auch von einem Telegramm gesprochen.



Ethernet II-Frame

8 Netzwerkgeräte

8.1 Switch



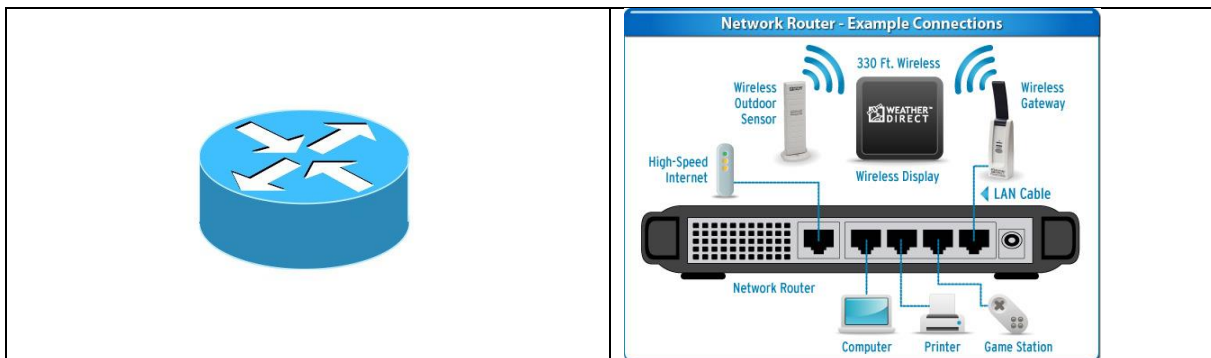
Mögliche Nachschaumöglichkeiten

HP - <https://www.hpe.com/ch/de/networking/switches.html>

Aruba - <https://www.arubanetworks.com/products/networking/switches/>

Cisco - https://www.cisco.com/c/de_ch/products/switches/index.html#~stickynav=1

8.2 Router



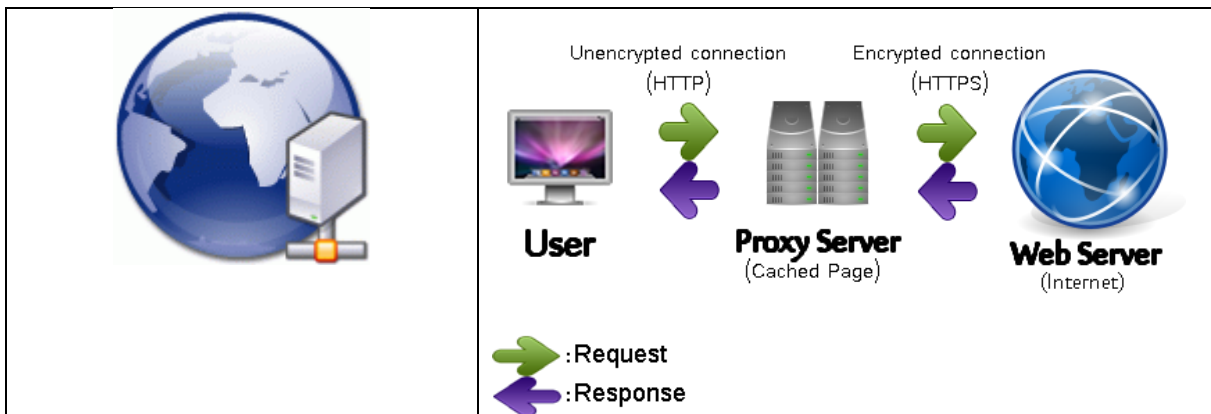
Mögliche Nachschaumöglichkeiten

Cisco - <https://www.cisco.com/c/en/us/products/routers/index.html>

HP - <https://buy.hpe.com/ch/de/networking/routers/c/4172265>

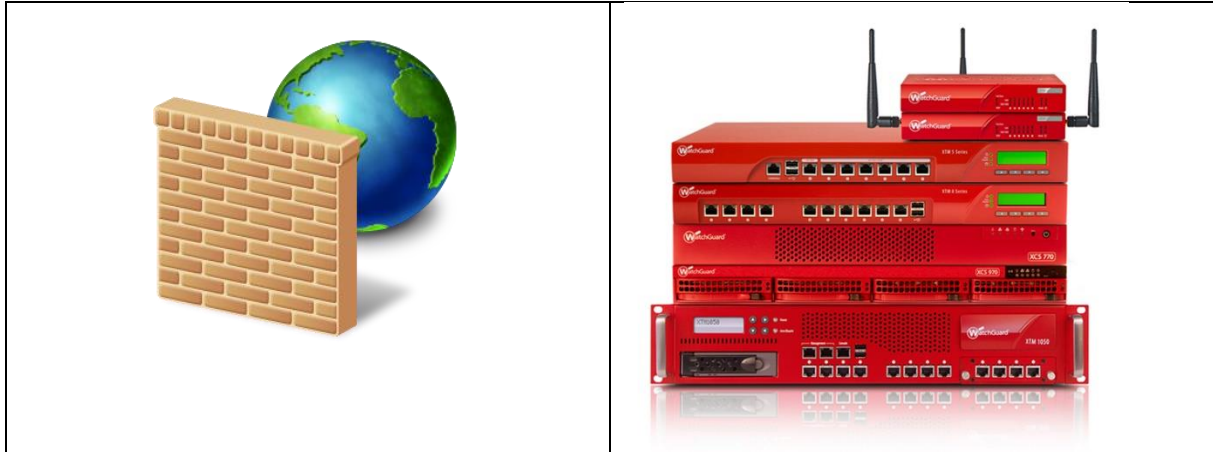
Netgear - <https://www.netgear.de/home/products/networking/>

8.3 Proxy



[https://de.wikipedia.org/wiki/Proxy_\(Rechnernetz\)](https://de.wikipedia.org/wiki/Proxy_(Rechnernetz))

8.4 Firewall



Watchguard

<http://www.boll.ch/watchguard/firewalls.html>

Fortigate

<http://www.boll.ch/fortinet/fortigate.html>

IpFire

<http://www.ipfire.org/>

8.5 Emulatoren

TP-Link Sortiment

<http://www.tp-link.com/en/emulators.html>

Netgear

Benutzername	admin
Passwort	password

<http://www.voiproblem.com/emulators/Netgear/>

Draytek

Benutzername	admin
Passwort	password

<http://www.draytek.com/index.php?lang=en&Itemid=302>

Linksys (Cisco)

<http://www.voiproblem.com/emulators/Linksys/>

DLink

<http://www.voiproblem.com/emulators/DLink/>

http://support.dlink.com/emulators/dir825/113NA/Device_Info.html

HP Comware Simulater 7

<http://h20565.www2.hpe.com/hpsc/swd/public/readIndex?sp4ts.oid=7107838&swLangOid=8&swEnvOid=4132>

Fortigate

<http://www.avfirewalls.com/Online-Demos.asp>

Cisco

https://www.cisco.com/assets/sol/sb/RV180W_Emulators/RV180W_Emulator_v1.0.3.14/home.htm

9 OSI Layer

Das OSI-Modell (englisch Open Systems Interconnection Model) ist ein Referenzmodell für Netzwerkprotokolle als Schichtenarchitektur. Es wird seit 1983 von der International Telecommunication Union (ITU) und seit 1984 auch von der International Organization for Standardization (ISO) als Standard veröffentlicht. Seine Entwicklung begann im Jahr 1977.

Zweck des OSI-Modells ist, Kommunikation über unterschiedlichste technische Systeme hinweg zu ermöglichen und die Weiterentwicklung zu begünstigen. Dazu definiert dieses Modell sieben aufeinander folgende Schichten (engl. layers) mit jeweils eng begrenzten Aufgaben. In der gleichen Schicht mit klaren Schnittstellen definierte Netzwerkprotokolle sind einfach untereinander austauschbar, selbst wenn sie wie das Internet Protocol eine zentrale Funktion haben.

9.1 Motivation

In einem Computernetz werden den verschiedenen Hosts Dienste unterschiedlichster Art bereitgestellt, und zwar von den anderen Teilnehmern im Netz (siehe auch Client-Server-Modell). Die dazu erforderliche Kommunikation ist nicht so trivial, wie es auf den ersten Blick scheint, denn es müssen eine Vielzahl von Aufgaben bewältigt und Anforderungen bezüglich Zuverlässigkeit, Sicherheit, Effizienz usw. erfüllt werden. Die zu lösenden Probleme reichen von Fragen der elektronischen Übertragung der Signale über eine geregelte Reihenfolge in der Kommunikation bis hin zu abstrakteren Aufgaben, die sich innerhalb der kommunizierenden Anwendungen ergeben.

Wegen der Vielzahl von Problemen und Aufgaben hat man sich entschieden, diese in verschiedene Ebenen (Schichten) aufzuteilen. Beim OSI-Modell sind es sieben Schichten mit festgelegten Anforderungen. Auf jeder einzelnen Schicht setzt jeweils eine Instanz die Anforderungen um.

Die Instanzen auf Sender- und Empfängerseite müssen nach festgelegten Regeln arbeiten, damit sie sich einig sind, wie die Daten zu verarbeiten sind. Die Festlegung dieser Regeln wird in einem Protokoll beschrieben und bildet eine logische, horizontale Verbindung zwischen zwei Instanzen derselben Schicht.

Jede Instanz stellt Dienste zur Verfügung, die eine direkt darüberliegende Instanz nutzen kann. Zur Erbringung der Dienstleistung bedient sich eine Instanz selbst der Dienste der unmittelbar darunterliegenden Instanz. Der reale Datenfluss erfolgt daher vertikal. Die Instanzen einer Schicht sind genau dann austauschbar, wenn sie sowohl beim Sender als auch beim Empfänger ausgetauscht werden können.

9.2 OSI kurz erklärt

9.2.1 Ein Schichtenmodell für Kommunikationsvorgänge im Internet - Kommunikation in Rechnernetzen

Schichtenmodelle spielen auch bei der Beschreibung und Entwicklung von Kommunikationsvorgängen in komplexen Rechnernetzen wie dem Internet eine zentrale Rolle. Erst durch eine klare Zuordnung der Kommunikationsvorgänge in Aufgabenbereiche und eine hierarchische Anordnung dieser Aufgabenbereiche wird es möglich, komplexe Systeme flexibel und beherrschbar zu entwickeln.

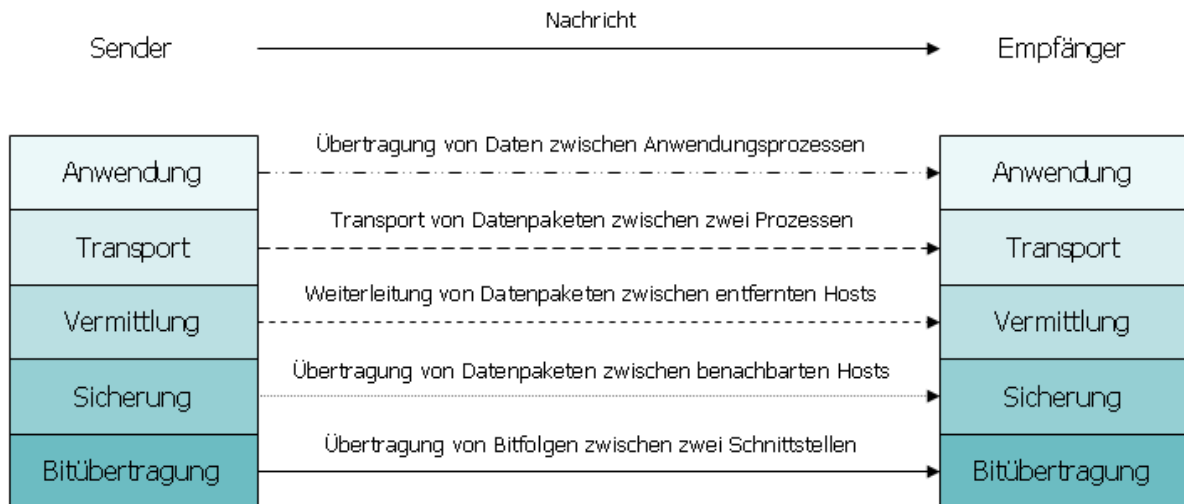
9.2.2 Nachrichtenübertragung im Schichtenmodell

Wenn eine Nachricht von einem Sender zu einem Empfänger übertragen wird, dann werden letztendlich physikalisch repräsentierte Bitfolgen über ein Transportmedium übertragen.

Die Übertragung von Bitfolgen bildet die unterste Schicht im Schichtenmodell.

Aufbauend auf Dienste der darunterliegenden Schicht kann man jetzt Übertragungsprozesse schrittweise abstrahierend beschreiben. So setzt eine Weiterleitung von Datenpaketen zwischen entfernten Hosts voraus, dass eine Übertragung zwischen benachbarten Host geregelt ist.

Für die Beschreibung von Kommunikationsvorgängen im Internet benutzen wir hier das folgende Schichtenmodell.



9.2.3 Ein Stapel aus Protokollen

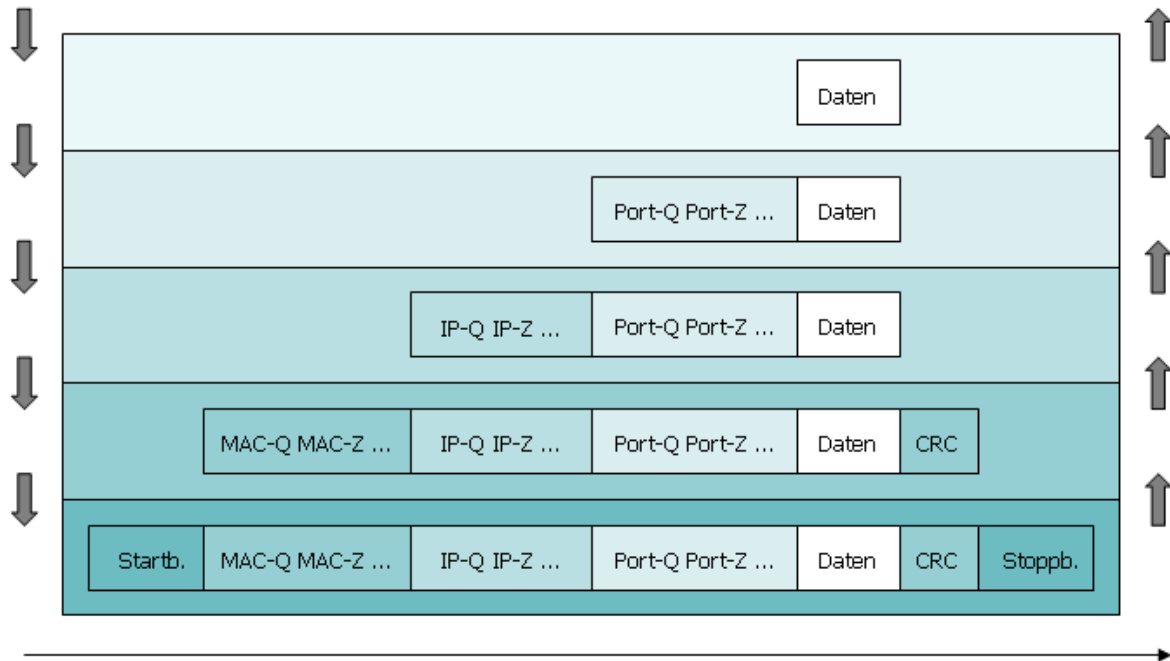
Die Vorgänge in den einzelnen Schichten werden durch Protokolle geregelt. Beachte, dass diese hierarchisch angeordnet sind. Protokolle benutzen in der Regel Dienste, die eine darunterliegende Schicht (geregelt durch ihre Protokolle) bereitstellt.



Die Pfeile in der Abbildung sollen andeuten, dass eine Nachricht - durch Protokolle geregelt - schrittweise verarbeitet wird, bevor sie auf der Bitebene dann tatsächlich übertragen wird.

9.2.4 Datenanreicherung

Die Protokolle der verschiedenen Schichten sehen vor, dass die zu übertragenden Daten schrittweise um Zusatzdaten angereichert werden. So müssen Schicht um Schicht den Daten bestimmte Adressinformationen hinzugefügt werden. Die Abbildung deutet eine solche Datenanreicherung für einen bestimmten Protokollstapel an.










9.3 Die sieben Schichten

Der Abstraktionsgrad der Funktionalität nimmt von Schicht 7 bis zur Schicht 1 ab.

Das OSI-Modell im Überblick (siehe im Vergleich dazu das TCP/IP-Referenzmodell):

OSI-Schicht	Einordnung	DoD-Schicht	Einordnung	Protokollbeispiel	Einheiten	Kopplungselemente	
7 Anwendungen (Application)	Anwendungs-orientiert	Anwendung	Ende zu Ende (Multihop)	HTTP FTP HTTPS SMTP LDAP NCP	Daten	Gateway, Content-Switch, Proxy, Layer-4-7-Switch	
6 Darstellung (Presentation)							
5 Sitzung (Session)							
4 Transport (Transport)	Transport-orientiert	Transport	Punkt zu Punkt	TCP UDP SCTP SPX	TCP = Segmente UDP = Datagramme		
3 Vermittlung (Network)		Internet		ICMP IGMP IP IPsec IPX	Pakete		Router, Layer-3-Switch
2 Sicherung (Data Link)		Netzzugriff			Ethernet Token Ring FDDI	Rahmen (Frames)	Bridge, Switch
1 Bitübertragung (Physical)					MAC ARCNET	Bits, Symbole, Pakete	Netzwerkkabel, Repeater, Hub

OSI Layer

		Device	PDU	Layers	Layer No	Implementaion & Protocols	Application Examples	
<div> <div>Encapsulation</div> <div> <div>↑</div> <div>↓</div> </div> </div>	Host Layer	Firewall	data	Application 	7	DHCP, DNS, FTP, HTTP, IMAP4, NNTP, POP3, SMTP, SNMP, SSH, TELNET & NTP	End User Layer Program that opens what was sent or creates what is to be sent • Resource sharing • Remote file access • Remote Printer Access • Diretory Services • Network Management	Upper Layer
		Firewall	data	Presentation 	6	SSL, WEP, WPA, Kerberos, MIME & XDR	Syntax layer encrypt & decrypt (if required) • Character Code translation • Data conversion • Data Compression • Data encryption • Character set Translation	
		Firewall	data	Session 	5	Dialog control Named pipe NetBIOS SAP PPTP RTP SOCKS SPDY TLS/SSL	Synch & send to ports (Interhost communication) • Session establishment, maintainence and termination • Session support - perform security, name recognition, logging, etc	
	Media Layer	Gateway	segements	Transport 	4	TCP, UDP, SCTP, DCCP & SPX	TCP Host to Host, Flow control (logical ports) • Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	Lower Layer
		Router IP/IPX/ICMP	packet	Network 	3	IPv4, IPV6, IPX, Apple Talk, OSPF, ICMP,IGMP, and ARPMP	Packets ("letter", contains IP address) • Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting	
		Switch,Bridge & WAP PPP/SLIP	frame	Data link 	2	802.11 (WLAN), Wi-Fi, WiMAX, ATM, Ethernet, Token Ring, Frame Relay, PPTP, L2TP and ISDN-ore	Frames ("envelops" contain MAC address) [NIC card -----Switch----- NIC card] end to end • Establishment & terminates the logical link between nodes • Frame traffic control • Frame Sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media aces control	
		Hubs, Repeaters	bits	Physical 	1	Hubs, Repeaters, Cables, Optical Fiber, SONET/SDN,Coaxial Cable, Twisted Pair Cable and Connectors	Physical structure Cables, hubs, etc • Data encoding • Physical medium attactment • Trasmission technique • Baseband vs Broadband • Physical medium tansmission Bits & Volts	

Source : davidprasad.blogspot.in

9.3.1 Schicht 1 – Physikalische Schicht (Physical Layer)

Die Bitübertragungsschicht (engl. Physical Layer) ist die unterste Schicht. Diese Schicht stellt mechanische, elektrische und weitere funktionale Hilfsmittel zur Verfügung, um physische Verbindungen zu aktivieren bzw. zu deaktivieren, sie aufrechtzuerhalten und Bits darüber zu übertragen. Das können zum Beispiel elektrische Signale, optische Signale (Lichtleiter, Laser), elektromagnetische Wellen (drahtlose Netze) oder Schall sein. Die dabei verwendeten Verfahren bezeichnet man als Übertragungstechnische Verfahren. Geräte und Netzkomponenten, die der Bitübertragungsschicht zugeordnet werden, sind zum Beispiel die Antenne und der Verstärker, Stecker und Buchse für das Netzkabel, der Repeater, der Hub, der Transceiver, das T-Stück und der Abschlusswiderstand (Terminator).

Auf der Bitübertragungsschicht wird die digitale Bitübertragung auf einer leitungsgebundenen oder leitungslosen Übertragungsstrecke bewerkstelligt. Die gemeinsame Nutzung eines Übertragungsmediums kann auf dieser Schicht durch statisches Multiplexen oder dynamisches Multiplexen erfolgen. Dies erfordert neben den Spezifikationen bestimmter Übertragungsmedien (zum Beispiel Kupferkabel, Lichtwellenleiter, Stromnetz) und der Definition von Steckverbindungen noch weitere Elemente. Darüber hinaus muss auf dieser Ebene gelöst werden, auf welche Art und Weise ein einzelnes Bit übertragen werden soll.

Damit ist folgendes gemeint: In Rechnernetzen werden heute Informationen zumeist in Form von Bit- oder Symbolfolgen übertragen. Im Kupferkabel und bei Funkübertragung dagegen sind modulierte hochfrequente elektromagnetische Wellen die Informationsträger, im Lichtwellenleiter Lichtwellen von bestimmter oder unterschiedlicher Wellenlänge. Die Informationsträger kennen keine Bitfolgen, sondern können weitaus mehr unterschiedliche Zustände annehmen als nur 0 oder 1. Für jede Übertragungsart muss daher eine Codierung festgelegt werden. Das geschieht mit Hilfe der Spezifikation der Bitübertragungsschicht eines Netzes.

Hardware auf dieser Schicht: Repeater, Hubs, Leitungen, Stecker, u. a.

Protokolle und Normen: V.24, V.28, X.21, RS 232, RS 422, RS 423, RS 499

9.3.2 Schicht 2 – Sicherungssicht (Data Link Layer)

Aufgabe der Sicherungsschicht (engl. Data Link Layer; auch Abschnittssicherungsschicht, Datensicherungsschicht, Verbindungssicherungsschicht, Verbindungsebene, Prozedurebene) ist es, eine zuverlässige, das heißt weitgehend fehlerfreie Übertragung zu gewährleisten und den Zugriff auf das Übertragungsmedium zu regeln. Dazu dient das Aufteilen des Bitdatenstromes in Blöcke – auch als Frames oder Rahmen bezeichnet – und das Hinzufügen von Prüfsummen im Rahmen der Kanalkodierung. So können fehlerhafte Blöcke vom Empfänger erkannt und entweder verworfen oder sogar korrigiert werden; ein erneutes Anfordern verworfener Blöcke sieht diese Schicht aber nicht vor.

Eine „Datenflusskontrolle“ ermöglicht es, dass ein Empfänger dynamisch steuert, mit welcher Geschwindigkeit die Gegenseite Blöcke senden darf. Die internationale Ingenieursorganisation IEEE sah die Notwendigkeit, für lokale Netze auch den konkurrierenden Zugriff auf ein Übertragungsmedium zu regeln, was im OSI-Modell nicht vorgesehen ist.

Nach IEEE ist Schicht 2 in zwei Unter-Schichten (sub layers) unterteilt: LLC (Logical Link Control, Schicht 2b) und MAC (Media Access Control, Schicht 2a).

Hardware auf dieser Schicht: Bridge, Switch (Multiport-Bridge)

Das Ethernet-Protokoll beschreibt sowohl Schicht 1 als auch Schicht 2, wobei auf dieser als Zugriffskontrolle CSMA/CD zum Einsatz kommt.

Protokolle und Normen, die auf anderen Schicht-2-Protokollen und -Normen aufsetzen: HDLC, SDLC, DDCMP, IEEE 802.2 (LLC), ARP, RARP, STP, Shortest Path Bridging

Protokolle und Normen, die direkt auf Schicht 1 aufsetzen: IEEE 802.11 (WLAN), IEEE 802.4 (Token Bus), IEEE 802.5 (Token Ring), FDDI

9.3.3 Schicht 3 – Vermittlungssicht (Network Layer)

Die Vermittlungsschicht (engl. Network Layer; auch Paketebene oder Netzwerkschicht) sorgt bei leitungsorientierten Diensten für das Schalten von Verbindungen und bei paketorientierten Diensten für die Weitervermittlung von Datenpaketen. Die Datenübertragung geht in beiden Fällen jeweils über das gesamte Kommunikationsnetz hinweg und schließt die Wegesuche (Routing) zwischen den Netzwerknoten ein. Da nicht immer eine direkte Kommunikation zwischen Absender und Ziel möglich ist, müssen Pakete von Knoten, die auf dem Weg liegen, weitergeleitet werden. Weitervermittelte Pakete gelangen nicht in die höheren Schichten, sondern werden mit einem neuen Zwischenziel versehen und an den nächsten Knoten gesendet.

Zu den wichtigsten Aufgaben der Vermittlungsschicht zählt das Bereitstellen netzwerkübergreifender Adressen, das Routing bzw. der Aufbau und die Aktualisierung von Routingtabellen und die Fragmentierung von Datenpaketen. Aber auch die Aushandlung und Sicherstellung einer gewissen Dienstgüte fällt in den Aufgabenbereich der Vermittlungsschicht.

Neben dem Internet Protocol zählen auch die NSAP-Adressen zu dieser Schicht. Da ein Kommunikationsnetz aus mehreren Teilnetzen unterschiedlicher Übertragungsmedien und -protokolle bestehen kann, sind in dieser Schicht auch die Umsetzungsfunktionen angesiedelt, die für eine Weiterleitung zwischen den Teilnetzen notwendig sind.

Hardware auf dieser Schicht: Router, Layer-3-Switch (BRouter)

Protokolle und Normen: X.25, ISO 8208, ISO 8473 (CLNP), ISO 9542 (ESIS), IP, IPsec, ICMP

9.3.4 Schicht 4 – Transportschicht (Transport Layer)

Zu den Aufgaben der Transportschicht (engl. Transport Layer; auch Ende-zu-Ende-Kontrolle, Transport-Kontrolle) zählen die Segmentierung des Datenstroms und die Stauvermeidung (engl. congestion avoidance).

Ein Datensegment ist dabei eine Service Data Unit, die zur Datenkapselung auf der vierten Schicht (Transportschicht) verwendet wird. Es besteht aus Protokollelementen, die Schicht-4-Steuerungsinformationen enthalten. Als Adressierung wird dem Datensegment eine Schicht-4-Adresse vergeben, also ein Port. Das Datensegment wird in der Schicht 3 in ein Datenpaket gekapselt.

Die Transportschicht bietet den anwendungsorientierten Schichten 5 bis 7 einen einheitlichen Zugriff, so dass diese die Eigenschaften des Kommunikationsnetzes nicht zu berücksichtigen brauchen.

Fünf verschiedene Dienstklassen unterschiedlicher Güte sind in Schicht 4 definiert und können von den oberen Schichten benutzt werden, vom einfachsten bis zum komfortabelsten Dienst mit Multiplexmechanismen, Fehlersicherungs- und Fehlerbehebungsverfahren.

Protokolle und Normen: ISO 8073/X.224, ISO 8602, TCP, UDP, SCTP.

9.3.5 Schicht 5 – Sitzungsschicht (Session Layer)

Die Schicht 5 (Steuerung logischer Verbindungen; engl. Session Layer; auch Sitzungsschicht[3]) sorgt für die Prozesskommunikation zwischen zwei Systemen. Hier findet sich unter anderem das Protokoll RPC (Remote Procedure Call). Um Zusammenbrüche der Sitzung und ähnliche Probleme zu beheben, stellt die Sitzungsschicht Dienste für einen organisierten und synchronisierten Datenaustausch zur Verfügung. Zu diesem Zweck werden Wiederaufsetzpunkte, so genannte Fixpunkte (Check Points) eingeführt, an denen die Sitzung nach einem Ausfall einer Transportverbindung wieder synchronisiert werden kann, ohne dass die Übertragung wieder von vorne beginnen muss.

Protokolle und Normen: ISO 8326 / X.215 (Session Service), ISO 8327 / X.225 (Connection-Oriented Session Protocol), ISO 9548 (Connectionless Session Protocol)

9.3.6 Schicht 6 – Darstellungssicht (Presentation Layer)

Die Darstellungsschicht (engl. Presentation Layer; auch Datendarstellungsschicht, Datenbereitstellungsebene) setzt die systemabhängige Darstellung der Daten (zum Beispiel ASCII, EBCDIC) in eine unabhängige Form um und ermöglicht somit den syntaktisch korrekten Datenaustausch zwischen unterschiedlichen Systemen. Auch Aufgaben wie die Datenkompression und die Verschlüsselung gehören zur Schicht 6. Die Darstellungsschicht gewährleistet, dass Daten, die von der Anwendungsschicht eines Systems gesendet werden, von der Anwendungsschicht eines anderen Systems gelesen werden können. Falls erforderlich, agiert die Darstellungsschicht als Übersetzer zwischen verschiedenen Datenformaten, indem sie ein für beide Systeme verständliches Datenformat, die ASN.1 (Abstract Syntax Notation One), verwendet.

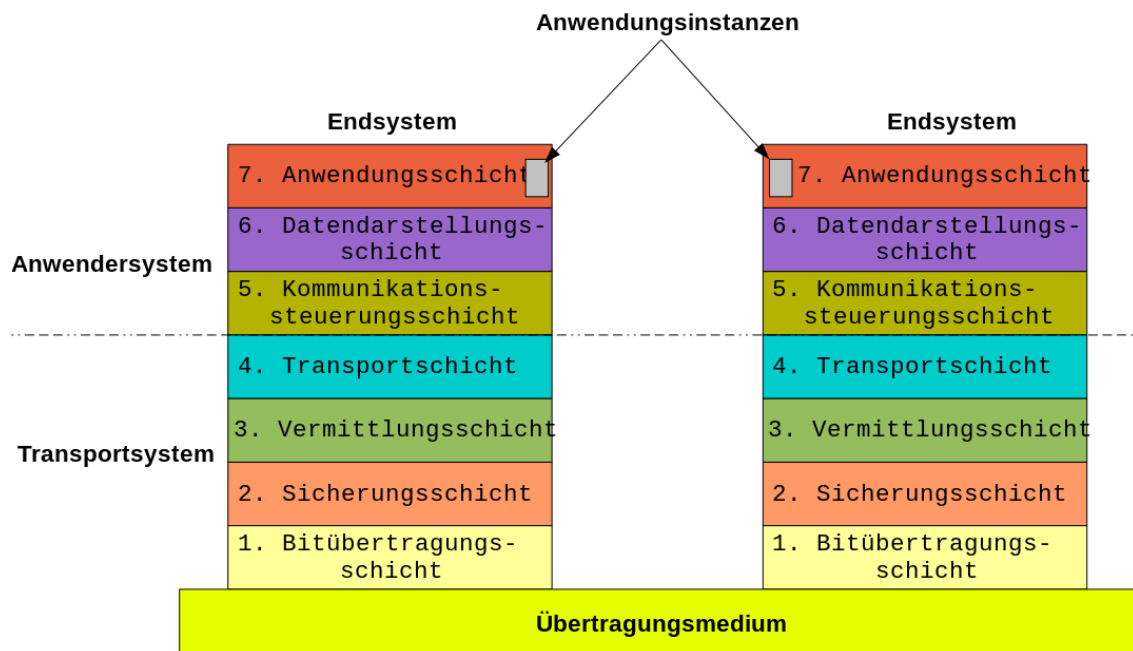
Protokolle und Normen: ISO 8822 / X.216 (Presentation Service), ISO 8823 / X.226 (Connection-Oriented Presentation Protocol), ISO 9576 (Connectionless Presentation Protocol)

9.3.7 Schicht 7 – Anwendungssicht (Application Layer)

Dienste, Anwendungen und Netzmanagement. Die Anwendungsschicht stellt Funktionen für die Anwendungen zur Verfügung. Diese Schicht stellt die Verbindung zu den unteren Schichten her. Auf dieser Ebene findet auch die Dateneingabe und -ausgabe statt.

Anwendungen: Webbrowser, E-Mail-Programm

9.4 Allgemeines



Das OSI-Referenzmodell wird oft herangezogen, wenn es um das Design von Netzprotokollen und das Verständnis ihrer Funktionen geht. Auf der Basis dieses Modells sind auch Netzprotokolle entwickelt worden, die jedoch fast nur in der öffentlichen Kommunikationstechnik verwendet werden, also von großen Netzbetreibern wie der Deutschen Telekom. Im privaten und kommerziellen Bereich wird hauptsächlich die TCP/IP-Protokoll-Familie eingesetzt. Das TCP/IP-Referenzmodell ist sehr speziell auf den Zusammenschluss von Netzen (internetworking) zugeschnitten.

Die nach dem OSI-Referenzmodell entwickelten Netzprotokolle haben mit der TCP/IP-Protokollfamilie gemeinsam, dass es sich um hierarchische Modelle handelt. Es gibt aber wesentliche konzeptionelle Unterschiede: OSI legt die Dienste genau fest, die jede Schicht für die nächsthöhere zu erbringen hat. TCP/IP hat kein derartig strenges Schichtenkonzept wie OSI. Weder sind die Funktionen der Schichten genau festgelegt noch die Dienste. Es ist erlaubt, dass eine untere Schicht unter Umgehung zwischenliegender Schichten direkt von einer höheren Schicht benutzt wird. TCP/IP ist damit erheblich effizienter als die OSI-Protokolle. Nachteil bei TCP/IP ist, dass es für viele kleine und kleinste Dienste jeweils ein eigenes Netzprotokoll gibt. OSI hat dagegen für seine Protokolle jeweils einen großen Leistungsumfang festgelegt, der sehr viele Optionen hat. Nicht jede kommerziell erhältliche OSI-Software hat den vollen Leistungsumfang implementiert. Daher wurden OSI-Profile definiert, die jeweils nur einen bestimmten Satz von Optionen beinhalten. OSI-Software unterschiedlicher Hersteller arbeitet zusammen, wenn dieselben Profile implementiert sind.

Zur Einordnung von Kommunikationsprotokollen in das OSI-Modell siehe auch:

AppleTalk
IPX Internetwork Packet Exchange

