Netzwerktechnik (vertieft)

Kenntnisse über den Aufbau einer Routingtabelle

Routingtabelle setzt sich zusammen aus:

- ein Ziel, bestehend aus Adresse und Subnetmaske.
- ein Gateway, die nächste Station zum Ziel.
- ein Interface, über welches das Paket versendet werden soll.
- die Metrik (wird verwendet, um Routen zu bevorzugen wenn es mehrere Routen für ein Ziel gibt).

Kenntnisse über statisches Routing, dynamisches Routing

Warum Routing?

- Es dient zur Verbindung verschiedener Netze.
- Unterschiedliche Topologien.
- Verbindung des LAN mit anderen Datennetzen (LAN, WAN) oder dem Internet.
- Verschiedene Subnetze.
- Routing (Wege Wahl) bezeichnet das Festlegen von Wegen für Nachrichtenströme über Rechnernetze.
- Routing beschreibt den Weg zum Ziel.
- Weg geht von Router zu Router (Hop by Hop).
- Weg ist tabellengesteuert (Routingtabelle).

Direkte Routen:

- Zieladresse ist im selben Netzwerk und vom Router direkt erreichbar.

Indirekte Routen:

- Zieladresse ist außerhalb des Netzwerks.
- Mindestens eine weitere Station (Hop) ist nötig, um das Ziel zu erreichen.

Default Route:

- Ziel ist nicht direkt erreichbar.
- Kein Eintrag in Routingtabelle vorhanden.
- Aufbau: Fiktive Netzwerkadresse (0.0.0.0./0) + Adresse des nächsten Hops.

Statisches Routing:

- Bei statischem Routing werden alle Einträge in der Routingtabelle manuell eingetragen.
- Fest vorgegebene Wege.
- Unflexibel bei Topologie Änderungen.
- Route muss auf allen Router richtig konfiguriert sein, da sonst das Paket verworfen wird.

Vorteil:

- Wege sind transparent und nachvollziehbar.
- Einfache Fehlersuche.
- Einfacher und schneller Konfigurationsaufwand.

Nachteil:

- Hoher Pflegeaufwand

- ist dessen Inflexibilität, da im Änderungsfall die statische Route manuell umkonfiguriert werden muss.
- Das gilt für Fehler, Netzwerkerweiterung, Umzüge von Endsystemen usw. Solange die Routenänderungen nicht manuell eingetragen sind, fließt kein Netzwerk-Traffic.

Dynamisches Routing:

- Router kommunizieren untereinander, teilen mit mit welchen Netzen sie verbunden sind.
- Kommunikation mittels Protokolle (RIP – kürzerer Weg, OSPF – schnellerer Weg, …).
- Routingtabelle wird anhand von Routing Protokollen (RIP, OSPF) ermittelt.
- Kein manuelles Eintragen der Routen nötig, wartungsfrei.

Vorteile:

- Dynamisches Routing ist skalierbarer und ausfallsicherer als statisches Routing.
- Außerdem verbessert sich damit nebenbei auch die Ausfallsicherheit Ihres Netzwerks.
- Die Hauptvorteile des dynamischen Routings gegenüber dem statischen Routing sind Skalierbarkeit und Anpassungsfähigkeit.

Nachteile:

- Höhere Prozessorlast als beim statischen Routing, da Routen von der CPU berechnet werden müssen.
- Höhere Netzauslastung, da Routeninformationen regelmäßig verschickt werden müssen.
- Höherer Aufwand für die Konfiguration und Wartung.

Fachbegriff Uplink-Port

- Ein Uplink ist die Verbindung eines Switches zum nächsten Switch (oder Hub) gemeint.
- Will man einen Switch mit einem anderen Switch über ein normales Netzwerkkabel (Patchkabel) verbinden, benötigt man den Uplink-Port.
- Dieser vertauscht das Sender- und Empfängerpaar der Ports, damit das Ganze funktioniert.
- Alternativ geht das auch ohne Uplink-Port. Dazu muss man allerdings ein Crossover-Cable nutzen, welches den gleichen Effekt hat.
- Letzteres ist heutzutage nicht mehr notwendig, dank der Auto Uplink-Technologie.
- Der Port erkennt, ob es sich um eine Verbindung zu einem Computer (Empfangen) oder eine Uplink-Verbindung zu einem Switch oder Router (Senden) handelt.

Fachbegriff VLAN

VLAN (Virtual Local Area Network):

- VLANs sind virtuelle lokale Netze.
- VLANs können verwendet werden, um physische Netze logisch voneinander zu trennen, hierzu wird dem Ethernet-Frame ein VLAN Tag mit der VLAN ID hinzugefügt. Paketgröße wächst dabei um 4 Byte von 1518 Byte auf 1522 Byte.
- Standard 802.1q
- Datenpakete werden nicht an andere VLANs weitergeleitet.
- Jedes VLAN ist eine eigene Broadcast-Domäne.
- Verbindung der VLANs über Routing.
- Arbeiten auf der Schicht 2 des OSI-Schichtenmodels.
- Werden mit Switches realisiert.
- VLANs Verbinden.

- Über Router
- Interne Router-Funktionalität im Switch (Layer 3).
- Physische (externe) Verbindung über VLAN-Port, Trunk-Port.

Dynamische VLANs:

- Anhand des Inhalts des Datenpakets wird Zuordnung getroffen.
- MAC / IP-Adresse (Mobile Geräte, Standgeräte, Server, …)
- Protokoll (TCP, UDP, …) bzw. deren Port-Nummer

Statische Portzuordnung (Portbasierendes VLAN):

- Trunk-Ports (Switch Ports, die zu allen VLANs gehören – dienen zur Verbindung von Switches)
- Andere Switch-Ports werden jeweils nur einem VLAN zugeordnet
- Paket wird an Ziel-Port weitergeleitet, denn dieser im gleichen VLAN wie der Quell-Port ist.

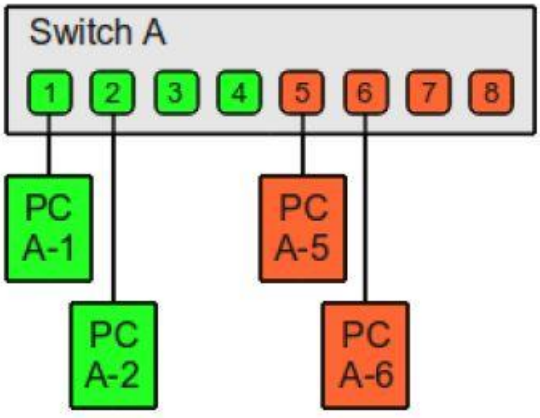
Grund:

- Flexibilität
- Änderung der logischen Struktur, ohne die physische ändern zu müssen.
- Performance
- Priorität für bestimmte Bereiche (VoIP, Abteilungen, …).
- Verkleinerung von Broadcast-Domänen, damit sich Broadcasts nicht über das gesamte Netz ausbreiten.
- Sicherheit
- Schutz vor Angriffsmöglichkeiten, wie MAC-Spofing oder MAC-Flooding.
- VLANs werden per Router verbunden.
- Gegen Layer 2 Attacken unempfindlich.
- Einsatz von Firewalls möglich.

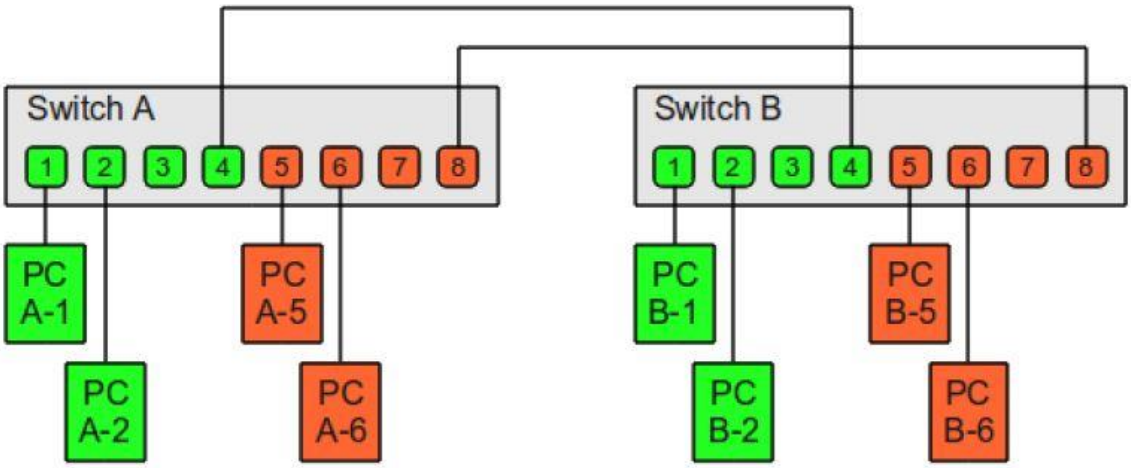
VLAN Typen:

Untagged VLAN (portbasiert):

- Bei portbasiert VLANS wird der physische Switch auf mehrere logischen Switche unterteilt.
- Durch Anlegen eines VLANs und zuweisen der entsprechenden Ports (untagged) können nur PCs vom gleichen VLAN miteinander kommunizieren.



Sollen z.B. zwei VLANs, die an unterschiedlichen Switches konfiguriert sind, verbunden werden, werden die beiden Switches mit einem Patchkabel verbunden. Und Zwar jeweils über einen freien Port der zum VLAN gehört.

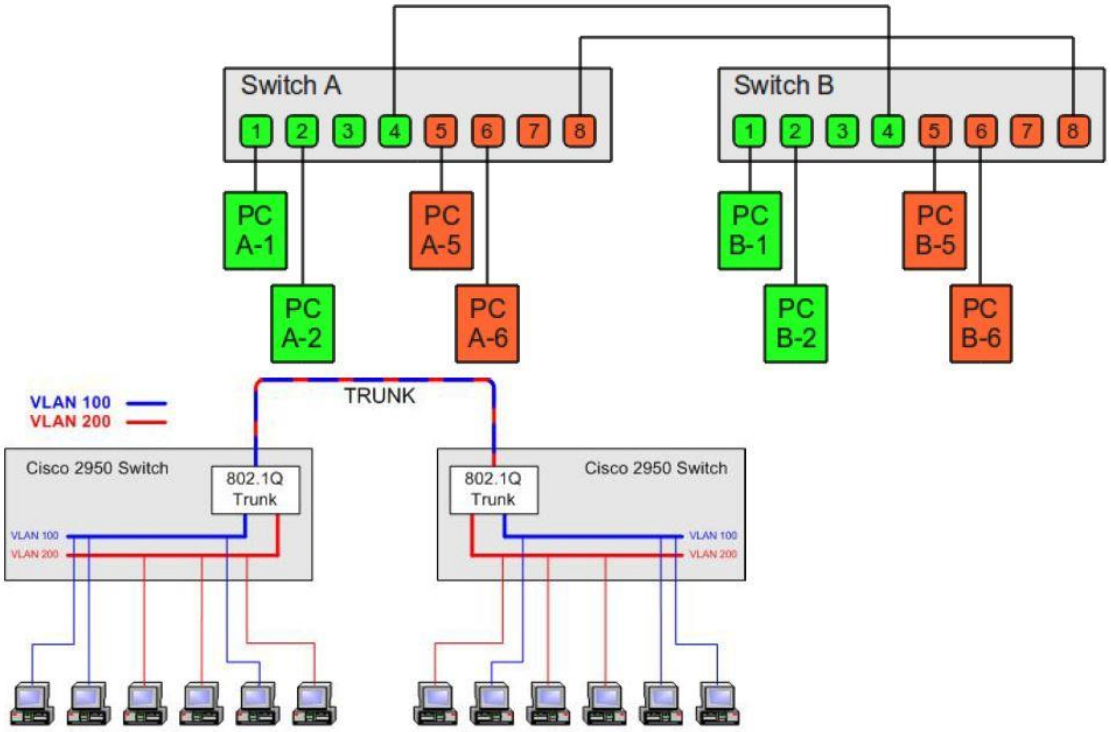


Tagged VLAN:

- Bei Tagged VLANs können mehrere VLANs von zwei Switches über einen einzelnen Switch-Port (Trunk Port) verbunden werden. Es wird nur ein Kabel zur Verbindung benötigt. (z.B. VLAN 1 und VLAN).
- Dabei wird vom ersten Switch im Ethernet Frame ein VLAN-TAG mit der jeweiligen VLAN-ID des Ziel VLANs hinzugefügt.
- Paket wird dem Switch-Port zugewiesen, wenn im selben VLAN.
- Falls das Ziel auf einem anderen Switch ist > Verbindung über Trunk-Port (getaggter Frame weitergeleitet)
- Dort wieder Zuweisung des Pakets an Switch-Port, wenn im gleichen VLAN wie im TAG des Pakets.

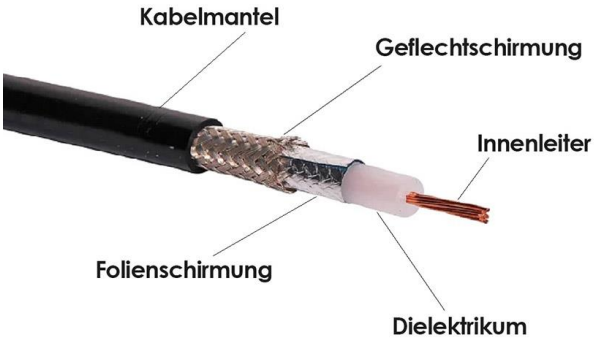
Beim letzten Switch wird der VLAN-TAG wieder entfernt:

- Wenn Endgerät angeschlossen ist.
- Wenn nicht-VLAN-fähiger Switch angeschlossen ist.
- Falls TAG nicht entfernt wird – wird der TAG als Typ Feld interpretiert und verworfen.



Aufbau eines Koaxialkabels, Twisted-Pair-Kabels

Koaxialkabel:



Innenleiter mit konzentrischen Außenleiter (Drahtgeflecht oder Folie).
Mantel und Trägerisolierung aus Kunststoff.

Außenleiter:

- Cu Geflecht (Kupfer Cu)
- Oder Cu-Folie

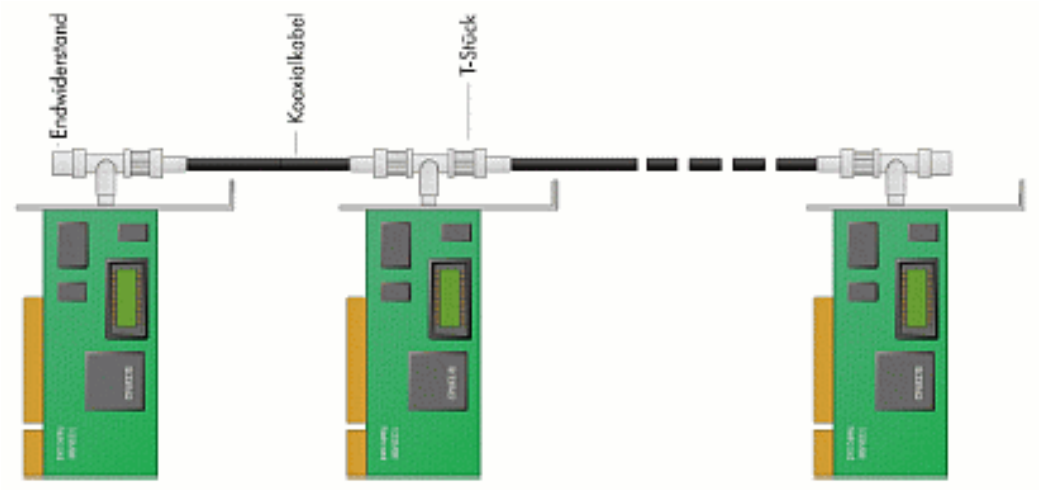
Innenleiter:

- Massiver Cu-Draht
- Cu-plattierter Stahldraht
- Cu-Litzenleiter

Eigenschaften:

- Einteilung nach elektrischen und mechanischen Eigenschaften
- Bezeichnung RGxx
- z.B. RG 5850 Ω Wellenwiderstand 4,6 mm Durchmesser

LAN-Verkabelung in Busstruktur:

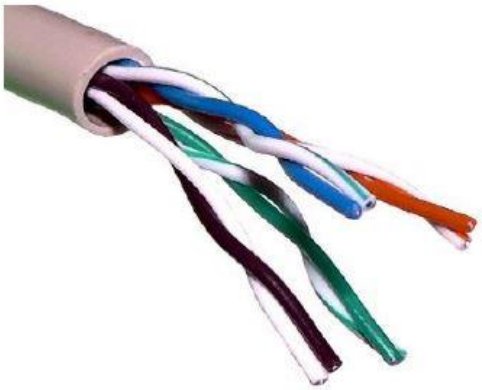


Spezifikation:

- Max. Segmentlänge: 185 m
- Max. Gesamtlänge: 925 m
- (5 Segmente, verbunden durch 4 Repeater).
- Min. Anschlussabstand: 0,5 m.
- Max. 3 Segmente dürfen mit PCs belegt sein.
- Max. 30 PCs / Segment.
- Geschwindigkeit: 10 Mbit/s

Twisted Pair Kabel:

- Unshielded Twisted Pair (UTP)

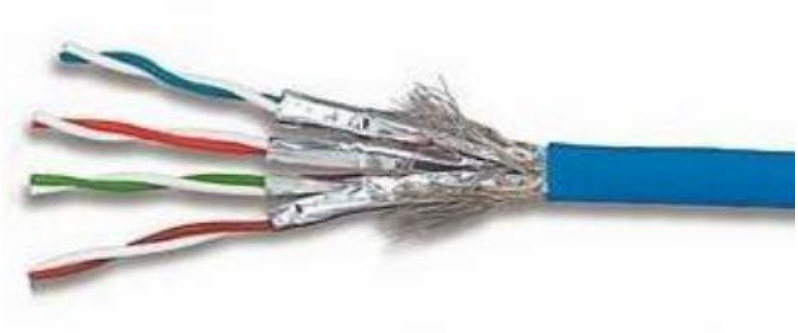


- Kunststoffmantel um Einzelader
- Verdrillte Adernpaare
- Kunststoffmantel um alle Adernpaare

Shielded Twisted Pair (STP) - Shielded UTP (S/UTP):

- Anders als bei UTP sind alle Adernpaare gesammelt von Kupfergeflecht zur Abschirmung umgeben.

Screened STP (S/STP):



Wie STP, nur sind alle Adernpaare nochmals einzeln von Aluminiumfolie umgeben.

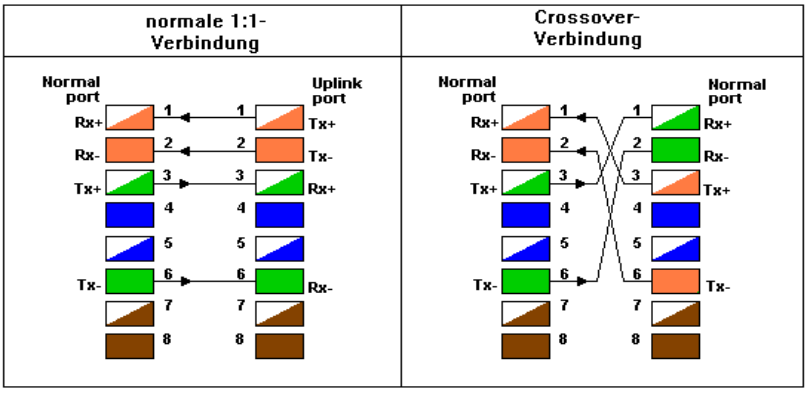
Eigenschaften:
Verdrillung bewirkt:

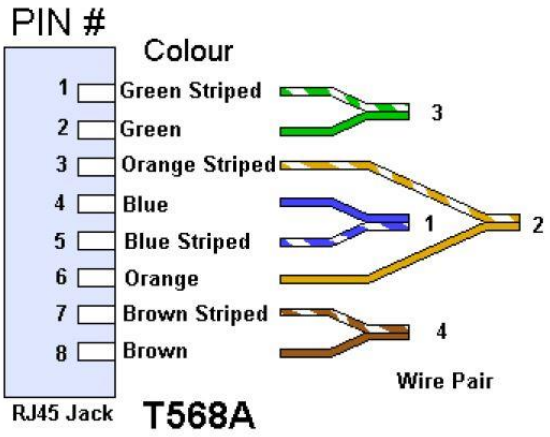
- Vermeidung von elektrischen Störungen.
- Keine Abstrahlung von Störungen.

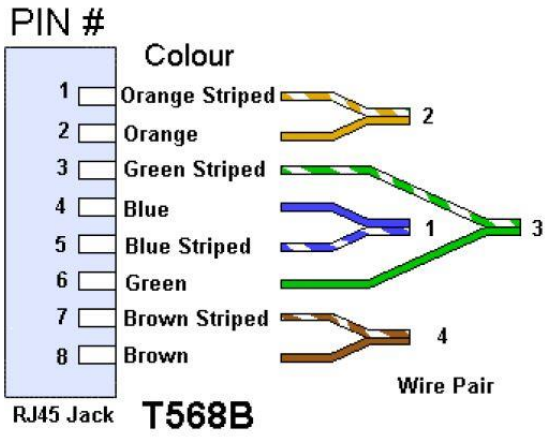
Gegeneinander verdrillte Paar bewirken:

- Unterdrückung von gegenseitiger Beeinflussung der Paare.
- da Störungseinflüsse beide gleich stark betrifft, je enger sie beisammen sind.

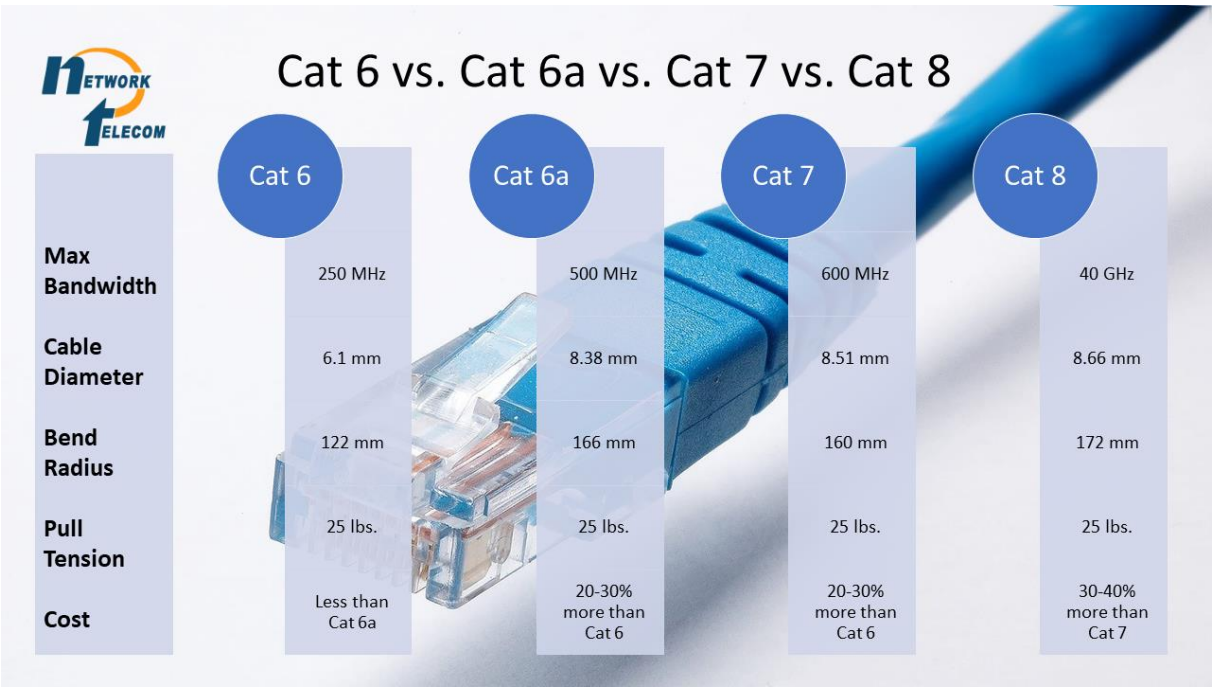
Cross-Over-Kabel / Gekreuztes Patchkabel:







Kenntnis der CAT6/6a/7-Spezifikationen



CAT-6:

- Kabel erreichen Betriebsfrequenzen von bis zu 250 MHz. Ihre Übertragungsgeschwindigkeit nimmt aber ab, je länger das Kabel ist.
- Die Kabel der CAT-6-Kategorie werden in der gesamten Netzwerkinfrastruktur des öffentlichen Lebens eingesetzt.

CAT-6a:

- ist ein Standard, der aus dem erhöhten Bandbreitenbedarf von 10-Gigabit-Ethernet (10GBASE-T) resultiert, für Übertragungsfrequenzen bis 500 MHz und Strecken bis 100 m ausgelegt sowie abwärtskompatibel zu bestehenden Kategorien ist.

CAT-7:

- der Standard ist der schnellste und am besten abgeschirmte Standard unter den Netzwerkkabeln.
- Kabel erreichen eine Betriebsfrequenz von bis zu 600 MHz.
- Die Unterkategorie CAT-7a schafft sogar bis zu 1.000 MHz.

- Alle Kabel der CAT-7-Kategorie haben 4 separat abgeschirmte Aderpaare in einer gesamten Abschirmung. Dadurch kommen so gut wie keine Nebensignale an das Kabel heran.

CAT-8:

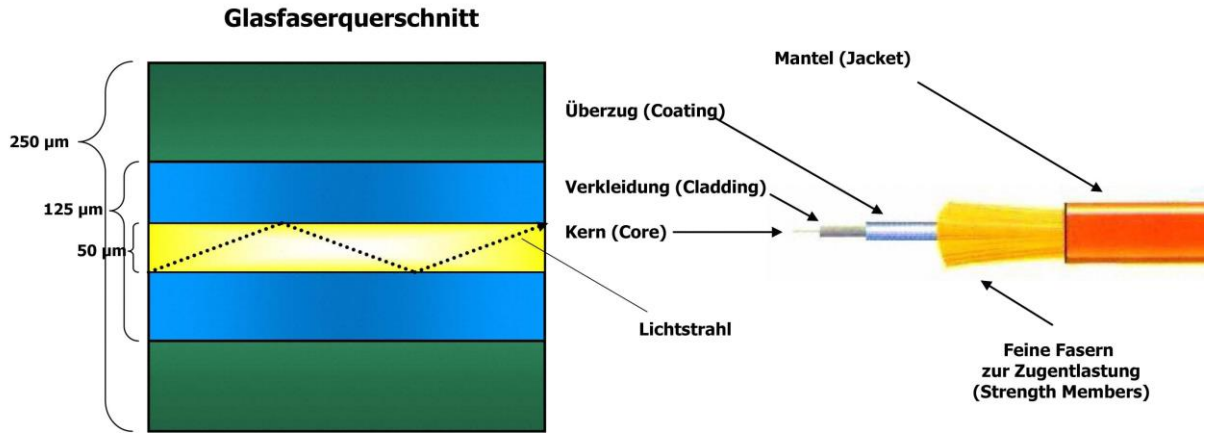
- erreicht doppelt so hohe Betriebsfrequenzen wie CAT 7.
- Dafür können die Kabel aber auch nur auf kurzen Distanzen eingesetzt werden.
- Bei dem Standard handelt es sich um Twisted-Pair-Kabel, die komplett abgeschirmt sind, Störungen haben hier keine Chance.
- Bei CAT-8-Kabeln gibt es zwei Unterkategorien, nämlich 8.1 und 8.2. CAT 8.1 ist kompatibel mit den normalen Ethernet-Steckern.
- CAT 8.2 verwendet einen speziell für den professionellen Bereich entworfenen Stecker.

Um dem Standard gerecht zu werden, muss das Kabel besonders vor äußeren Einflüssen wie Nebensignalen oder Rauschen geschützt sein.
Die Normen legen außerdem Grenzwerte für NEXT, ACR -N, ACR-F (PSNEXT, PSACR) fest die bei der Zertifizierung nicht überschritten werden dürfen

- CAT6: Schlechtere Übertragungsgeschwindigkeit bei längeren Kabeln.
- Cat7: Größerer Abstand der Adernpaare im Stecker

Aufbau eines LWL-Kabels

LWL Kabel bestehen aus einem Kernglas durch das sich die Lichtwelle/n (Single bzw. Multimode) bewegen, und einem Mantelglas. Moden bei LWL Kabeln beschreiben die Wege, die das Licht gehen kann, Multi – viel, Single- eine. Das Mantelglas ist für die Brechung der Wellen zuständig, hier unterscheidet man Gradienten Profil (Brechung Parabelförmig) und Stufen Profil (harte Brechung)
Um das Mantelglas ist eine Beschichtung aufgetragen, die das Austreten von Wellen verhindert. Der dicke Mantel aus Plastik schützt und macht das Kabel flexibel.



LWL- Kabel gängige Stecker:

LC:
- Lucent Connector

SC:
- Subscriber Connector

MTP:
- Multi-fiber Termination Push-on

ST:
- Straight Tip

FC:
- Fibre Connector

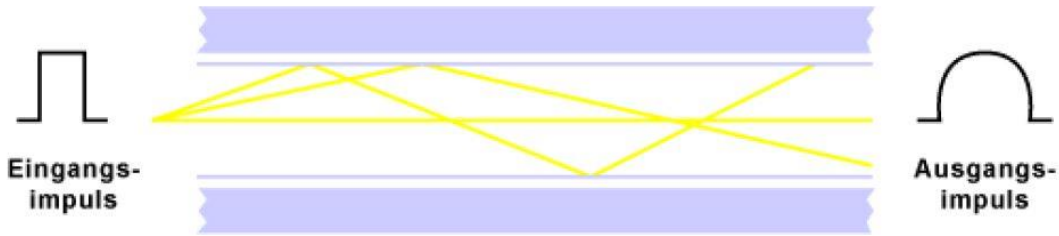
Physikalische Grundlagen:
- Licht wird beim Übergang von Medien mit unterschiedlicher optischer Dichte gebrochen bzw. reflektiert.
- Der Reflexionsgrad hängt vom Unterschied der beiden optischen Dichten und vom Einfallswinkel ab.
- Erreicht der Einfallswinkel einen kritischen Wert, gelangt überhaupt kein Licht am Ende aus dem Medium mit der höheren Brechzahl heraus.
- Auf dieser Totalreflexion beruht das Prinzip des Lichtwellenleiters.

Vorteile:
- große Übertragungsbandbreite
- niedrige Signaldämpfung
- unempfindlich gegenüber elektromagnetischen Störungen
- nahezu abhörsicher

Nachteile:
- aufwendige Verlegearbeiten (Biegeradius)
- hohe Kosten

Typen von Lichtwellenleiter:
- Multimode: mehrere Wellenlängen sind ausbreitungsfähig
- Singlemode: nur eine Wellenlänge ist ausbreitungsfähig

Multimode mit „Stufenprofil“:
- Wellen werden durch Totalreflexion innerhalb der Faser geführt
- Durch unterschiedliche Ausbreitungswinkel entstehen Laufzeitunterschiede – Impuls wird verzerrt (=Dispersion).



Multimodefaser mit Stufenindex-Profil

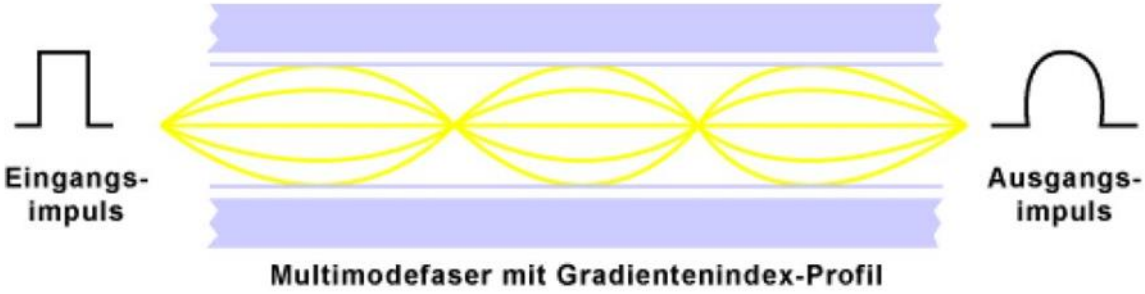
Unterscheidung der Fachbegriffe Monomode und Multimode

Singlemode-Monomodefaser:

- Nur eine Welle ist ausbreitungsfähig
- Bessere Bandbreite
- Geringer Durchmesser (1/10 von Multimode).
- Höhere Reichweite, aber teurer als Multimode.

Multimode mit Gradienten Profil:

- Kontinuierlicher Verlauf der Brechzahl
- Wellen werden mit wachsendem Abstand zur Kernachse stärker gebrochen > - Verminderung der Laufzeitunterschiede



	Kernglas	Mantelgals	Wellenlänge
Multimode	50 µm	125 µm	850, 1300nm
Singlemode	3,5-10,4 µm	125 µm	1310,1550nm

Schutzmaßnahmen:

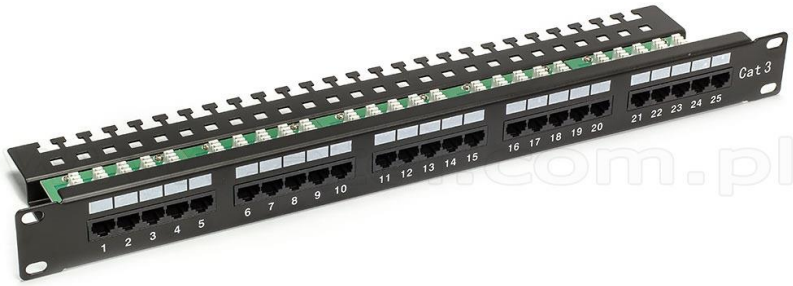
- Schaue niemals in den Strahl einer Lichtwellenleitung > Erblindung droht!
- Lichtwellenleiter immer mit Schutzkappen abdecken.

Fachbegriff Patch-Panel

Patch Panel = Rangierfeld:

- Auf einem Patchpanel werden alle Leitungen aufgelegt und mit der dazugehörigen Dose verbunden, es dient zum leichten und modularem verkabeln zum Switch.
- Dient zum Aufbau von komplexen Kabelstrukturen in Gebäuden.
- Dient zur strukturierten Verkabelung.

- Dient zur 1 zu 1 Verbindung, um aus mehreren Kabeln eine durchgehende Verbindung zwischen zwei Punkten zu schaffen.
- Dient zum Verbinden von Anschlüssen eines Patchpanels mit Ports eines anderen Patchfeldes.
- Dienst zum Verbinden von Anschlüssen eines Patchfeldes mit einem Netzwerkverteilergerät (z.B.: Switch, Hub, Router).
- Meist in einem 19 Zoll Schrank verbaut. Pro Stockwerk ein Schrank.



Fachbegriff Netzwerkdose

An eine Universal Anschluss Einheit – kurz UAE oder auch Netzwerkdose genannt, lassen sich Computer und andere Netzwerkgeräte in Gebäuden geordnet anschließen.
Die Dose ermöglicht eine störungsfreie Verbindung und zuverlässigen Datenaustausch zwischen den Geräten. Damit die UAE funktionstüchtig ist, muss sie mit dem Netzwerk verbunden sein, also richtig verkabelt und angeschlossen.
Dabei hilft die Farbkodierung von Dose und Kabel, sodass die Verkabelung funktioniert.

- Netzwerkdose die über die sekundäre Verkabelung mit dem Patchpanel im Netzwerkverteiler verbunden ist, Teil der Gebäudeverkabelung.
- Dient zum Anschluss von Endgeräten.

Fachbegriff RJ45-Stecker

- RJ-45 (Registered Jack) ist der Standard-Konfektionsstecker für Cat Kabel.
- Er führt alle 8 Adern einseitig parallel zueinander auf, und hat auf der anderen Seite einen Halteclip.
- RJ Stecker sind typisch in der Telekommunikation RJ-11 Telefon/Fax bspw.

Fachbegriff PoE

PoE (Power over Ethernet):
- Bezeichnet die Stromversorgung (Gleichstrom) über ein Netzwerkkabel.
- Die Einspeisung erfolgt durch den Switch, so können Niedervoltige Geräte ohne einen separaten Netzteil betrieben werden. z.B. Telefone, Webcams, WLAN-Access Points.
- Spezifiziert im IEEE 802.3at-2009.
- Die Spannung liegt in der Regel bei 48V und einer Leistung von 15,4W bei POE+ bei bis zu 25,5W.
- Aufgrund des geringen Querschnitts von TP Kabeln und der Länge von bis zu 100m entsteht ein teilweise erheblicher Widerstand, sodass der Wirkungsgrad bei grade mal 70-86% liegt.

Fachbegriff Ethernet

- Meist verbreitete LAN-Technologie.
- Ist eine Hardware und Software-Technologie zum Datenaustausch in Form von Frames in einem LAN.
- Ethernet wurde als Konzept für lokale Netzwerks und die damit verbundene gemeinsame Nutzung eines Datenmediums entwickelt.
- Basiert auf dem Standard IEEE 802.3 (Institute of Electrical and Electronics Engineers).
- Ursprünglich wurde eine Bustopologie (Thick Ethernet) mit CSMA/CD-Verfahren genutzt (10Mbit/s).
- Ständige Weiterentwicklung > 10 Mbit/s, 100 MBit/s, 1 GBit/s, 10 GBit/s, 40 GBit/s, 100GBit/s
- Definiert auf OSI Schicht 2 die Adressierung und Zugriffskontrolle auf unterschiedlichen Übertragungsmedien.
- Zugriff auf das Medium mit dem CSMA/CD-Verfahren (Carrier Sense Multiple Access and Collision Detection).

- Zentrale Komponenten:
- Ethernet Frame
- CSMA/CD Verfahren
- Ethernet-Standards

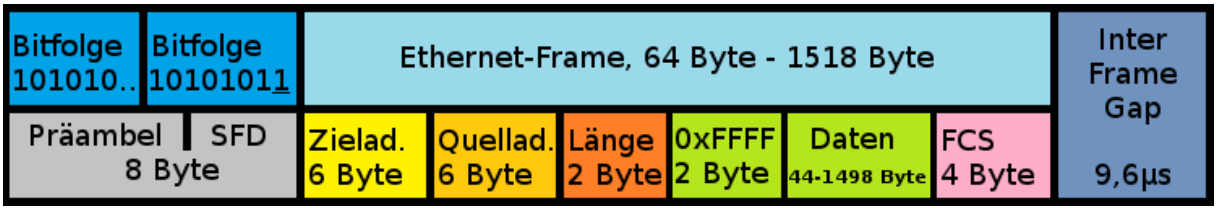
- Ethernet transportiert Daten paketweise. Als sogenannte FRAMES.
- Ethernet überträgt die Daten ohne Garantie das diese innerhalb einer bestimmten Zeit den Empfänger erreichen.
- Deswegen verwerfen Ethernet Komponenten Datenpakete, wenn nicht genügend Bandbreite verfügbar ist. Wegen der unzuverlässigen Übertragungstechnik ist Ethernet auf die Intelligenz höherer Protokolle angewiesen.

Fast Ethernet:
Beibehaltung aller „alten" Spezifikationen (802.3)

Erweiterungen:
- ermöglicht den Geräten die bestmöglichen Übertragungseigenschaften automatisch zu erkennen und zu konfigurieren.
- (10 oder 100 Mbit/s, Halb- oder Vollduplex).
- Überprüfung auf Optimum.

CSMA/CD- Carrier Sense Multiple Access / Collission Detection:
- ist ein System entwickelt um bei gemeinsamer Nutzung eines Übertragungsmediums (Kabel).
- Informationsverlust durch Listen-before-talking vermeidet und durch Collission Detection ggf. Pakete erneut sendet.

Aufbau eines Ethernet-Paketes



- Min. Länge: 64 Byte (Präambel & SFD werden nicht mitgezählt)
- Max. Länge: 1518 Byte (Präambel & SFD werden nicht mitgezählt)
- SFD = Start Frame Delimiter
- FCS = Frame Check Summe
- CRC = Verfahren

Type Feld:

- 0x0800 IP Internet Protocol (IPv4)
- 0x0806 Address Resolution Protocol (ARP)
- 0x8035 Reverse Address Resolution Protocol (RARP)
- 0x809B Appletalk (Ethertalk)
- 0x80F3 Appletalk Address Resolution Protocol (AARP)
- 0x8100 VLAN Tag (VLAN)
- 0x8137 Novell IPX (alt) 0x8138 Novell
- 0x86DD Internet Protocol, Version 6 (IPv6)

0x bedeutet, dass es sich um Hexadezimal handelt.

- Standard Ethernet Frame = ARPA, DIX, TIPII auch genannt.
- IEEE 8023 Frame: benutzt anstatt den TYPE Feld ein LENGTH Feld.
- LENGTH: 0x0000 – 0x05DC (0 - 1500 Byte).

Fachbegriffe 100BaseTx, 1000Base-T, 10GBASE-T

Base steht für Ethernet over Twisted Pair.

Bezeichnung	Geschwindigkeit	Standart	Ausnutzung
100BaseTx	100Mbit	802.3u	2 oder 4 Paare des TP Kabels
1000Base-T	1000Mbit	802.3ab	4 Paare des TP Kabels min Cat5e
10GBase-T	10Gbit	802.3an	Min. Cat6a

100Base-TX / Fast Ethernet / IEEE 802.3u:

- Übertragungsgeschwindigkeit: 100 MBit/s
- Physikalische Struktur: Stern-Topologie
- Maximale Kabellänge: 100 m
- Netzwerkkabel: Twisted-Pair-Kabel der Kategorie 5
- Weiterentwicklung von 10Base-T
- X bedeutet das es sich um ein UTP-Straight-Through-Kabel (Durchgangskabel) der Kategorie CAT5 handelt.

1000Base-T / IEEE 802.3ab:

- Übertragungsgeschwindigkeit: Gigabit Ethernet mit 1000 MBit/s
- Physikalische Struktur: Stern-Topologie
- Maximale Kabellänge: 100 m
- Netzwerkkabel: Twisted-Pair-Kabel
- Nutzt alle 4 Adern Paare des Kabels für die Übertragung.

10GBase-T / IEEE 802.3an:

- Übertragungsgeschwindigkeit: Gigabit Ethernet mit 10 GBit/s
- Physikalische Struktur: Stern-Topologie

- Maximale Kabellänge: 100 m
- Netzwerkkabel: Twisted-Pair-Kabel
- Nutzt alle 4 Adern Paare des Kabels für die Übertragung.
- 10GBASE-T ist eingeschränkt auch über Cat 5e Kabel möglich.

T = Twisted-Pair
S = 850 nm, bis 65 m, Multimode
L = 1310 nm
E = 1550 nm, bis 40 km, Singlemode
R = 64b/66b, LAN
X = 8b/10b, LAN
W = 64b/66b, WAN, SONET/SDH Framing
4 = WWDM mit 4 Wellenlängen

Fachbegriffe Gbit-Ethernet, 10Gbit-Ethernet

Geben jeweils die Geschwindigkeit an, auf die Geräte bzw. die Infrastruktur maximal operieren kann.

- Gbit- 1Gbit/s, 10Gbit -> 10Gbit/s, 40Gbit -> 40Gbit/s.

Gbit-Ethernet:

- Wird vorwiegend im LAN eingesetzt. Aber auch in großen Netzwerken.
- Ist für Glasfaserkabel und Twisted-Pair-Kabel spezifiziert.
- Ist für CAT5 Kabel geeignet (bis 10m Kabellänge, ab 10m sollte man CAT5e verwenden).
- Erlaubt Datenübertragungsraten mit 1 GBit/s.
- Ist 100 Mbit/s und 10 Mbit/s abwärts kompatibel.
- Es werden alle 4 Adern Paare des Twisted-Pair-Kabels zur Übertragung genutzt.
- Gbit-Ethernet ist ein Minimum, wenn man Server und Speichergeräte in einem Netzwerk einbinden will, und viele Nutzer darauf zugreifen sollen.
- Ein Upgrade auf ein Gbit-Ethernet ist noch leicht, da keine neue Verkabelung notwendig ist (bei CAT5e) um die Datenübertragungsrate zu erreichen.
- bei 10Gbit braucht man alles neu.

10Gbit-Ethernet:

- Wird im WAN (Wide Area Network) eingesetzt.
- Wird aber auch in MAN und LAN eingesetzt.
- Wurde für die Verbindung von großen Netzwerken, also WAN, mit Glasfaserkabel aber auch Twisted-Pair-Kabel entwickelt.
- Ist für Glasfaserkabel und Twisted-Pair-Kabel spezifiziert.
- Erlaubt Datenübertragungsraten mit 10 GBit/s.
- Jumbo-Frames mit 9014 Byte Größe kommen zum Einsatz.
- Es werden alle 4 Adern Paare des Twisted-Pair-Kabels zur Übertragung genutzt.

Der Standard für die Glasfaserübertragung heißt IEEE 802.3ae.
Die Standards für Kupfer sind IEEE 802.3ak und IEEE 802.3an.

Fachbegriff Traffic-Shaping

Traffic Shaping (auch als „Packet Shaping" bezeichnet) ist eine Technik zur Bandbreitenverwaltung, die den Datenfluss bestimmter Arten von Netzwerkpaketen verzögert, um die Netzwerkleistung für Anwendungen mit höherer Priorität sicherzustellen.

Beispiel:
Wenn z.B. ein Download stattfindet, und gleichzeitig eine E-Mail verschickt wird, kommen die TCP-Quittierungspakete für den Server, die für den Fortgang des Downloads notwendig sind, nur verzögert an.

- Denn der Uplink ist durch den Mail-Versand blockiert.
- Dadurch sinkt die Download-Geschwindigkeit.
- Beim Traffic-Shaping zieht der Router die Quittierungspakte beim Versand anderen Paketen vor.
- Dadurch sinkt die Download-Geschwindigkeit nicht mehr.

Fachbegriff Subnetmask

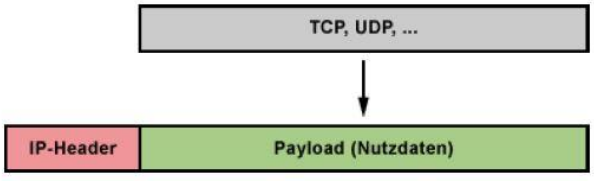
Die Subnetzmaske (auch Netzwerkmaske genannt) ist eine mehrstellige Binärzahl (Bitmaske), die in einem Netzwerk eine IP-Adresse in eine Netzadresse und eine Geräteadresse trennt.
Die Geräteadressen werden auch als Hostadressen bezeichnet.
Der Vorteil von Subnetzmasken besteht darin, dass man einen zur Verfügung stehenden Adressraum in verschiedene Subnetze unterteilen kann.

Das kann verschiedene Gründe haben:
- Einzelne Abteilungen eines Unternehmens können logisch voneinander getrennt werden, z.B. aus Sicherheitsgründen.
- Sie haben nur einen bestimmten Adressraum zur Verfügung, den Sie nicht voll ausnutzen.
- Durch die Aufteilung schaffen Sie zwei oder mehrere autarke Netze.
- Routingentscheidungen können schneller getroffen werden.

Aufbau einer Subnetzmaske:
Die Subnetzmaske sieht auf den ersten Blick der IP-Adresse sehr ähnlich. Sie hat immer die gleiche Länge wie die IP-Adresse. So ist ein aus 32 Bit bestehender Zahlencode bei der IP-Version 4 in 4 mal 8 Bit unterteilt.

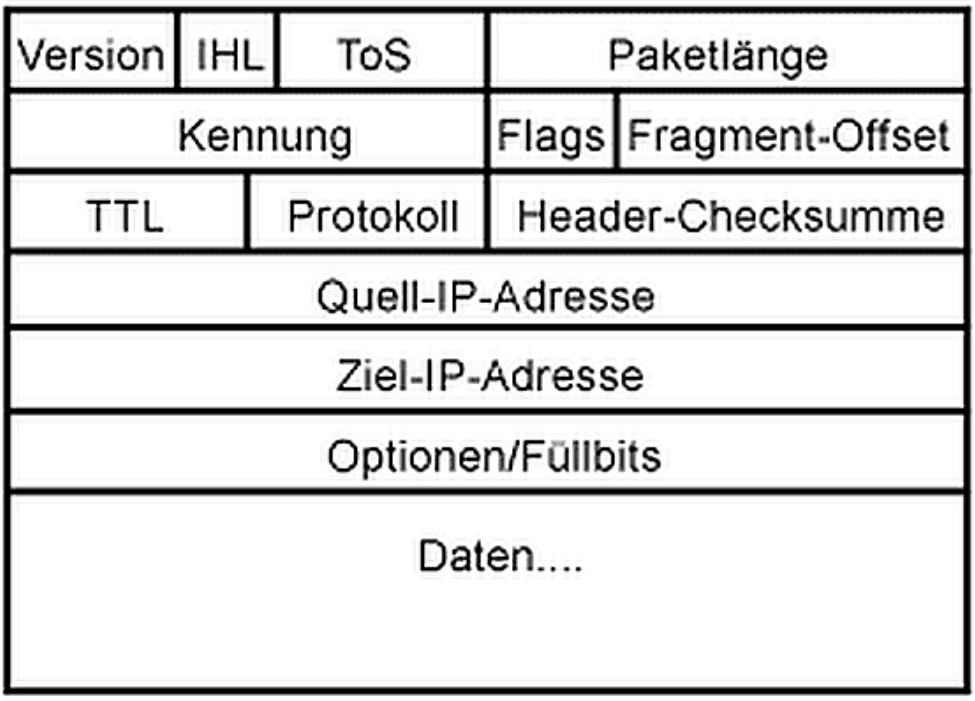
- Subnetting bedeutet die Aufteilung eines zusammenhängenden Adressraums von IP-Adressen in mehrere kleinere Adressräume.
- Ein Subnetz bzw. Teilnetz ist ein physikalisches Segment eines Netzwerks, in dem IP-Adressen mit der gleichen Netzwerkadresse benutzt werden. Diese Teilnetze können über Router miteinander verbunden werden.
- Jede IP-Adresse besteht aus einem Netzwerkteil und Hostteil.
- Die Subnetzmaske bestimmt, wo sich die IP-Adresse teilt.
- Gibt an wie viel Bits am Anfang der IP-Adresse der Netzwerkteil ist.
- Der Netzwerkteil muss bei allen Geräten des jeweiligen Netzes gleich sein.
- 32 Bit Länge (bei IPv4 in 4 x 8 Bit unterteilt).
- Binäre Darstellung ist wichtig, um den Aufbau und die Berechnung zu verstehen.
- Im Netzwerkteil sind lauter 1, im Hostteil lauter 0.

Aufbau eines IP-Paketes



Aufbau eines IP-Headers:

- Ein IP-Paket muss min. 20 Byte Header und 8 Byte Nutzdaten enthalten.
- IP-Header ist in jeweils 32-Bit Blöcke unterteilt
- Max. Länge 65.535 Byte



Version:

- Kennzeichnet die IP-Protokoll-Version (IPv4 oder IPv6).

IHL (Internet Header Lenght):

- Länge des IP-Headers in 32-Bit Worten.

ToS (Typ of Service):

- Beinhaltet Steuerinformationen für die Übertragung.

Total Length (Paketlänge):

- Gesamtlänge des IP-Pakets in Byte.

Identification:

- Eindeutige Kennung des IP-Pakets.

Flags:

- Die niederwertigen Bits haben folgende Bedeutung:
- Don't Fragment: Für Hosts, die keine Fragmentierung unterstützen.
- More Fragmentes: zum Erkennen ob alle Fragmente eines Datagramms empfangen wurden.

Fragment-Offset:

- Die Daten-Bytes werden nummeriert und auf die Fragmente verteilt
- Das erste Fragment hat Offset 0, für jedes weitere erhöht sich der Wert um die Länge des Datenfeldes eines Fragments.
- Dient zum Erkennen ob Fragmente fehlen.

TTL (Time to Live):

- Ist die Lebensdauer des Datagramms, ein Hop Count. Beginnt bei 128 und zählt bei jedem Erreichen eines Hops (Router) um 1 herunter. Bei 0 wird das Paket verworfen.

Protocoll:

Übergeordnetes Protokoll:

- 1: ICMP (Internet Control Message Protocol)
- 3: GGP (Gateway to Gateway Protocol)
- 6: TCP (Transmission Control Protocol)

- 8: EGP (Exterior Gateway Protocol)
- 17: UDP (User Datagram Protocol)

Header Checksum:
- Checksumme über den IP-Header

Source Address:
- Quell-IP-Adresse

Destination Address:
- Ziel-IP-Adresse

Options:
- Optionales Feld für weitere Information.
- Dienen der Netzsteuerung, Fehlersuche, Messungen.

Padding:
- Füllbits

Fachbegriffe Multicasting, Unicasting

Multicasting:
- Multicasting bezeichnet das Adressieren von mehreren Empfängern oder eine Gruppe von Empfänger.
- Das Datenpaket wird an mehrere Empfänger verschickt.

Unicasting:
- Unicasting bezeichnet das Adressieren von einem einzigen Empfänger.
- Das Datenpaket wird nur an einen Empfänger verschickt.

Broadcasting:
- Bei Broadcasting werden alle Teilnehmer im gleichen Netz adressiert.
- Das Datenpaket wird an alle Teilnehmer im gleichen Netz verschickt.

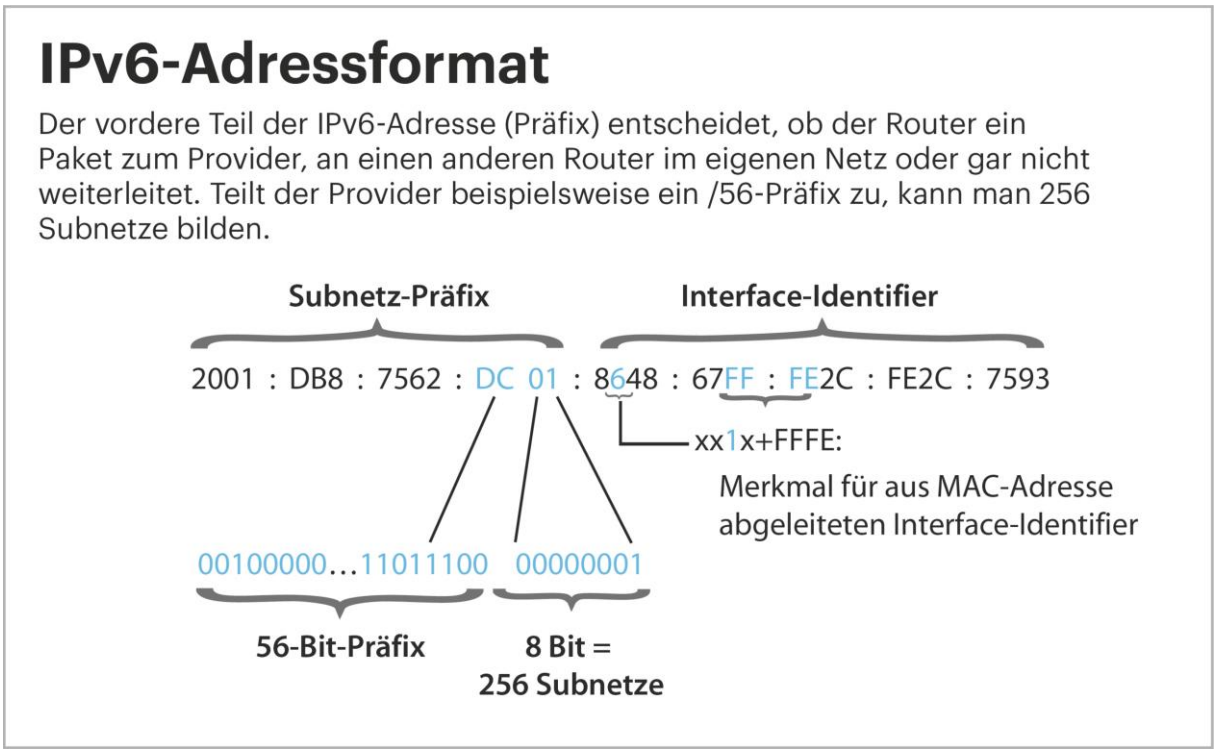
Fachbegriffe Präfix und Interface Identifier in Zusammenhang mit IPv6

IPv6-Adressen sind 128 Bit lang (IPv4: 32 Bit). Die ersten 64 Bit bilden das sogenannte Präfix, die letzten 64 Bit bilden bis auf Sonderfälle einen für die Netzwerkschnittstelle (englisch network interface) eindeutigen Interface-Identifier.

Präfix:
Das Präfix kennzeichnet das Netz/Subnetz/Adressbereich - den Netzteil.
- Zur Kennzeichnung wird ein „/" an die Adresse angehängt. In der Regel immer „/64"

Das Präfix gibt ähnlich wie bei IPv4 die Art der IPv6 Adresse an.
- 2002::/16 6to4 Adresse
- 2001::/32 Tredo Adresse CDIR
- 200::/3 Global Unicast Adresse
- FE80::/10 LinkLocalUnicast Adresse
- FF00::/8 Multicast

Identifier (Suffix):
- Steht für den Hostteil.
- Der Interface Identifier kennzeichnet einen Host in diesem Netz.
- Er wird aus der 48-Bit MAC Adresse gebildet, und in eine 64-Bit Adresse umgewandelt. Daher ist er weltweit eindeutig.
- Zwecks Datenschutz und Privatsphäre werden Private Extension eingesetzt die regelmäßig einen zufälligen Interface Identifier erzeugen.

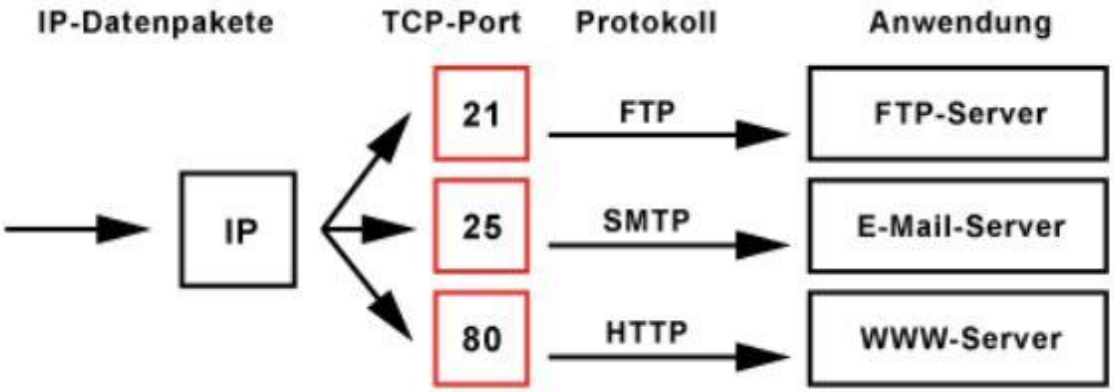


Fachbegriff Dual-Stack in Zusammenhang mit IPv4 und IPv6

- Mit Dual Stack bezeichnet man den Parallelbetrieb von IPv4 und IPv6 auf einer NIC.
- Diese Technik ist nötig da noch nicht alle Netzwerke auf IPv6 und vor allem nicht alle Provider Netze, sowie Heimrouter IPv6 unterstützen.
- Da keine direkte Umstellung von IPv4 auf IPv6 möglich und auch nicht sinnvoll ist, sieht eine "Transition Strategy" vor, dass alle Netzknoten sowohl IPv4 als auch IPv6 beherrschen.
- Der Plan ist, dass man längerfristig gesehen auf IPv4 verzichten könnte, und nur mehr IPv6 einsetzt.
- Der Schritt zu IPv6 wird meist nur deswegen nicht vollzogen, weil während des Parallelbetriebs doppelter Administrationsaufwand anfällt. (Routing, Filterregeln, Access Control Lists - alles doppelt)

Fachbegriff Port

- TCP und UDP Ports dienen zur Adressierung der Anwendungen und ihrer Verbindungen, die auf einem Rechner laufen.
- Sie sind dafür verantwortlich, dass Datenpakete den richtigen Programmen und Services zugeordnet werden können.
- Als Ports werden Adressen auf Layer 4 des OSI Modells bezeichnet.
- Ports können durch eine Firewall geblockt bzw. weitergeleitet werden.
- Ist eine 16 Bit Zahl



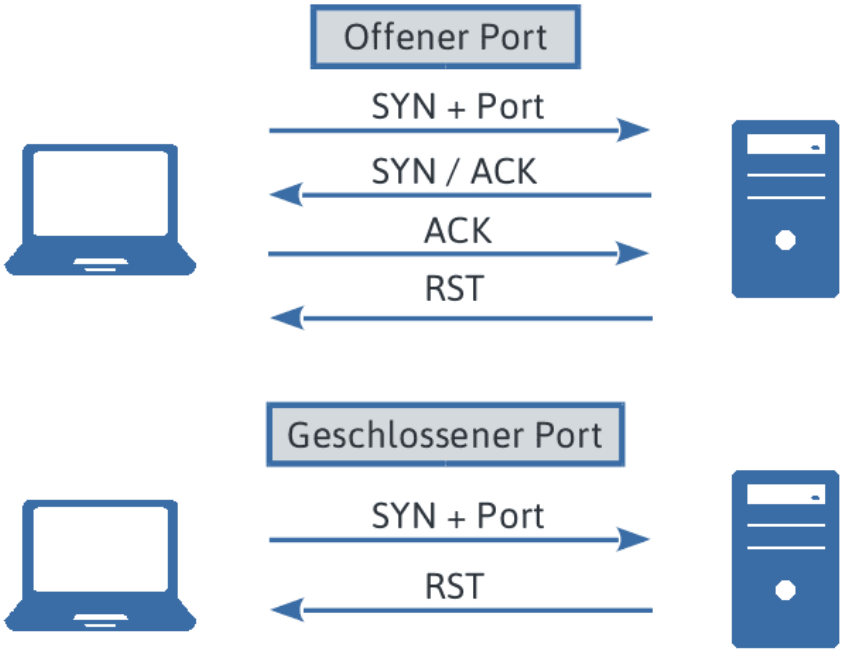
Port-Zustände:

Open:

- Port ist einer Anwendung zugeordnet.
- Anwendung lauscht.
- Verbindungen über diesen Port sind möglich.

Closed:

- Ist der Standardzustand eines Ports.
- Keine Anwendung lauscht.
- Verbindungen über diesen Port sind nicht möglich.



Filtered/Blocked:

- Port ist nicht offen und nicht geschlossen.
- Verbindungen über diesen Port sind nicht möglich, weil zum Beispiel eine Firewall-Regel diesen blockiert.
- Zustand kann aber entstehen, wenn der kontaktierte Host gar nicht erreichbar ist.

Es gibt 3 Bereiche, von der IANA (Internet Assigned Numbers Authority) verwaltet:

0 - 1.023 Well Known Ports:
- Für Serverdienste benötige erhöhte Rechte.
- TCP Ports: 21 - FTP, 23 - Telnet, 25 - SMTP, 80 - HTTP, 110 - POP, 119 - NNTP, 443 HTTPS
- UDP Ports: 53 - DNS, 69 - TFTP, 137 - NetBIOS-ns, 138 - NetBIOS-DGM, 161 - SNMP

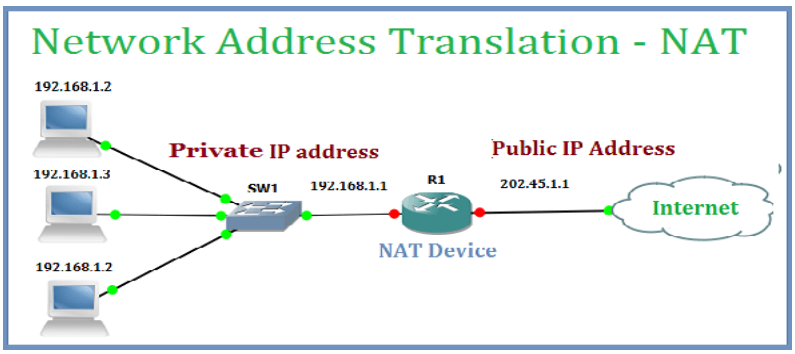
1.024 - 49.151 Registered Ports:
- Benötigen keine erhöhten Rechte.
- 8080 – HTTP

49.152 - 65.535 Dynamically Allocated Ports:
- Benötigen keine erhöhten Rechte.

Kenntnisse über NAT/PAT-Technologie

Warum NAT/PAT?
Öffentliche IP-Adressen zu wenig.
Private IP-Adressen werden nicht im Internet geroutet.
Für die Kommunikation nach außen (außerhalb des privaten Netzwerkes).
Erreichbarkeit der privaten IP-Adressen aus dem Internet.
Umsetzung der privaten IP-Adressen in öffentliche.
- Aufgrund des Mangels and IPV4-Adressen wurde es nötig jedem Internetanschluss nur mehr eine IP-Adresse zuzuordnen. Was PAT entspricht, aber fälschlicherweise als NAT bezeichnet wird.
- Durch PAT kommt ein privates Netz mit einer einzigen öffentlichen IP-Addresse aus.
- Dazu besitzt der Router neben der privaten IP-Adresse auch eine öffentliche IP-Adresse.
- Will ein Rechner vom privaten Netz auf das Internet zugreifen, tauscht der Router bei den ausgehenden Datenpakten die Quelladresse (also private IP-Adresse) durch seine eigene öffentlichen IP-Adresse aus. Die Port-Nummer wird durch eine andere Portnummer ersetzt.
- Damit der Router die eingehenden Datenpakte dem lokalen Host zuordnen kann, speichert er zusätzlich die Port-Nummern in einer NAT-Tabelle.

NAT (Network Address Translation):



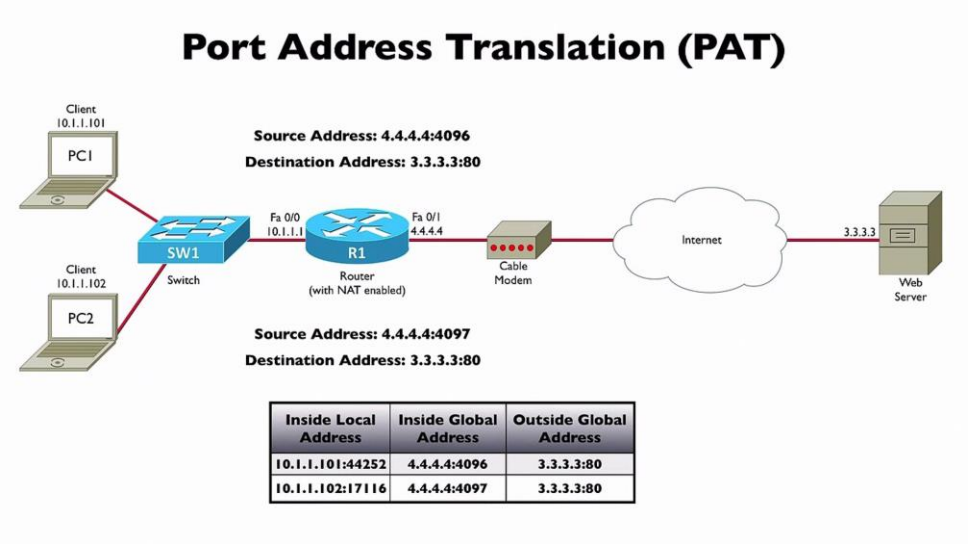
- Bei NAT wird einer privaten IP-Adresse eine öffentliche IP-Adresse zugeordnet.

- Es wird eine öffentliche IP-Adresse pro privater IP-Adresse benötigt.
- Verbindungen werden nur von innen nach außen aufgebaut. Zuordnungstabellen bleiben nur kurz gespeichert.

Vorteil:
- Nur eine öffentliche IP-Adresse nötig.
- Netzwerk Struktur bleibt nach Außen verborgen.
- Verbindungen werden nur von innen nach außen aufgebaut.
- Zuordnungstabellen bleiben nur kurz gespeichert.

Nachteil:
- Pro gleichzeitige Verbindung ist eine öffentliche IP-Adresse notwendig.
- Bei wenig und unregelmäßiger Kommunikation - Verbindungsabbrüche.
- Bei hohem Aufkommen Überlauf der NAT-Tabelle - Einträge fliegen raus, Verbindungsabbrüche.

PAT (Port Address Translation):



- Bei PAT tauscht der Router die Quell-Adresse und den Quell-Port aus.
- Bei PAT werden allen privaten IP-Adressen eine einzige öffentliche IP-Adresse zugeordnet.
- Für die Dauer der Verbindung bleibt der Port offen.
- Offene Ports sind nur von der Zieladresse aus erreichbar!
- Paketfilterung möglich.

Sicherheitsgewinn:
Angreifer muss mehrere Informationen haben, damit ein Paket ankommen kann.
- Ursprüngliche Ziel-IP vortäuschen.
- Router-IP (PAT-Router) kennen.
- Ausgangs-Port kennen.

Kenntnisse über Port-Forwarding

- Wird auch DNAT (Destination NAT) genannt.
- Es werden alle externen Datenpakete, die über ihre Port-Adresse einem bestimmten Dienst zugeordnet werden können, an eine definierte IP-Adresse im privaten Netz weitergeleitet.
- Dabei ordnet der Router einer IP-Adresse einen festen Port zu. Der Router leitet dann all auf diesem Port eingehenden externen Datenpakte an diesen Host weiter.
- Das ermöglicht die Nutzung einer IP-Adresse für mehrere verschiedene Dienste auf verschiedenen Server. z.B. Mail-Server und Webserver.
- Eingehende Pakte werden mit Destination NAT und ausgehende mit Source NAT maskiert.

Fachbegriff QoS

QoS (Quality of Service):
- Beschreibt die Qualität eines Kommunikationsdienstes aus der Sicht des Anwenders.
- Auf Layer 3 wird eine Priorisierung von Paketen durchgeführt.
- Hierzu wird im IP-Header im Type of Service vermerkt, wie hoch die Priorität des Pakets ist.
- Wird z.B. bei VoIP Traffic zu priorisieren benutzt, um die Dienstgüte sicherzustellen.

Kriterien:
- Netzbelastung - Dauer der Übertragung.
- Paket-Verzögerungen.
- Rate der Paketverluste.

Prioritätsklassen:
- 1 Sprache
- 2 Video
- 3 VPN
- 4 WWW
- 5 Mail
- 6 Sonstiges

Gutes Quality of Service ist:
- Mehr Bandbreite als erforderlich.
- Reservierung der Bandbreite (für Anwendungen).
- Priorisierung bestimmte Datenpakete.
- Verbindungsorientiertes Protokoll unterhalb der IP-Schicht.

Jitter Buffer:
- Um bei Sprach- und Videoübertragungen Laufzeitunterschiede zu vermeiden, wird ein Jitter-Buffer eingesetzt.
- Verbessert den gleichmäßigen Fluss der Datenpakete.

Fachbegriff WOL

WOL (Wake on LAN):
- WOL ist eine Funktion, mit der ein ausgeschalteter PC aus der Ferne einschaltet werden kann.
- Dazu wird ein sogenanntes Magic Packet direkt oder mittels Broadcast an die Netzwerkkarte des PCs geschickt. Dann bootet der PC.
- WOL Muss von Mainboard, Netzwerkkarte und BIOS (aktiviert) unterstützt werden.

Wake-on-LAN-fähige Computer warten im Wesentlichen auf das Eintreffen eines Magic Packet, dass die MAC-Adresse der Netzwerkkarte enthält. Diese Pakete werden von professioneller Software für jede Plattform gesendet, können aber auch von Routern und internetbasierten Websites gesendet werden. Normalerweise aber werden diese über das gesamte Netzwerk gesendet und enthalten die Subnetzinformationen, die Netzwerk-Broadcast-Adresse und die MAC-Adresse der Netzwerkkarte des Zielcomputers - unabhängig davon, ob Ethernet oder Wireless.

Kenntnis über DSL-Technologien

DSL (Digital Subscriber Line):

- DSL nutzt die vorhandenen Kupfer-Telefonkabeln. Diese sind durch Sprachübertragung nicht ausgelastet).
- Die max. zulässige Dämpfung beschränkt den Betrieb auf einen ca. 5 km Umkreis zum Knoten.
- Je kürzer die Leitung zum Knoten ist umso höher kann die Datenrate sein.
- Für den Betrieb beim Teilnehmer sind ein Splitter und ein Modem notwendig. Der Splitter teilt die Leitung in Daten und Telefonie auf (Frequenzweiche).
- Die Übertragungstechniken werden laufend weiterentwickelt.

> Höhere Übertragungsrate

Unterscheidung zwischen:

ADSL (Asymmetrischen DSL):

- Download- und Upload Geschwindigkeit sind gleich.

SDSL (Symmetrischen DSL):

- Download- und Upload Geschwindigkeit sind unterschiedlich.

VDSL (Very High Speed Digital Subscriber Line):

- Ist ein Hybrides-Netz bestehend aus Glasfaser- und Kupferleitungen.
- Die Glasfaser-Leitungen müssen dabei so nahe wie möglich beim Kunden sein, um eine hohe Übertragungsrate zu erreichen.

Fachbegriff CATV-Modem

CATV-Modem (Cable TV Modem = Kabel TV Modem):

- Als Kabelmodem bezeichnet man ein Gerät, das Daten über Kabelfernsehnetze überträgt und zur Realisierung von Breitband-Internetzugängen über Kabelanschlüsse (Kabelinternet) eingesetzt wird.
- Das Kabelmodem befindet sich beim Endkunden zwischen dem Kabelfernsehanschluss und dem Router bzw. Computer.
- Die Signale werden einem Trägersignal auf-moduliert.
- Verstärker sorgen dafür, dass die notwendige Signalqualität beim Kunden ankommt.
- Die Verbindung vom Modem zum Computer erfolgt entweder über Ethernet oder über den USB-Port.
- Es gibt auch Kabelmodems, die mit einem Wireless Access Point kombiniert sind und eine Funkverbindung zum Computer aufbauen. Solche Ausführungen werden oft als Wireless Cable Modem Gateway bezeichnet.
- Zum Ansteuern des Kabelmodems über eine Ethernet-Verbindung müssen in der Regel keine kabelmodemspezifischen Treiber auf dem Computer installiert werden.
- Häufig kann direkt am Kabelmodem ein Router oder WLAN-Router zur gemeinsamen Nutzung von mehreren Computern angeschlossen werden.

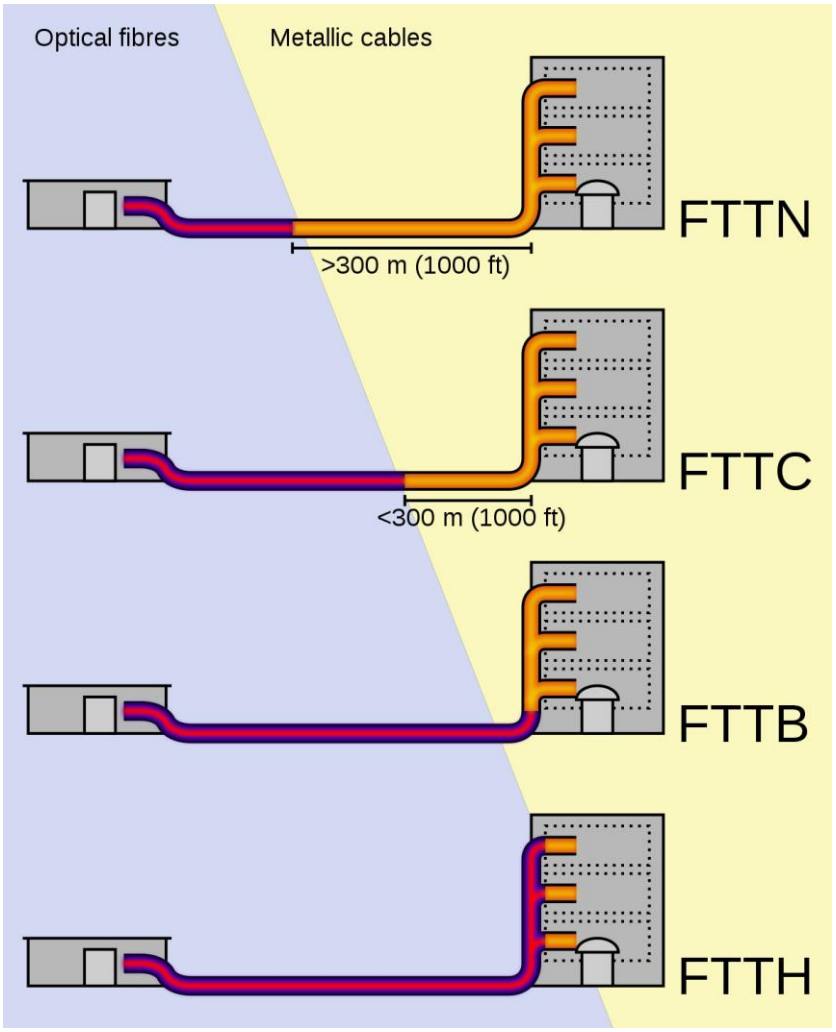
Fachbegriff FTTH

FTTH (Fibre to the Home):

Ist eine Glasfaseranschlusstechnik, bei der die Glasfaser von der Ortsvermittlungsstelle bis zum Endkunden in dessen Wohnung geführt wird.

FTTx sind Hypridlösungen mit Glasfaser- und Kupferleitungen.

- Soll große Übertragungsdistanzen bei hoher Bandbreite gewährleisten
- Dazu rückt Glasfaser immer näher zum Kunden. Je näher umso höher kann die Bandbreite beim Kunden sein.
- Ist mit hohen Herstellungskosten verbunden.



Es gibt verschieden Glasfaser-Netzarchitekturen:

- FTTN - Fibre to the Node: Glasfaser geht bis zur Vermittlungsstelle (Hauptverteiler).
- FTTC - Fibre to the Curb: Glasfaser geht bis zum Kabelverzweiger, (Bordstein/Straßenrand).
- FTTB - Fibre to the Building: Glasfaser geht bis zum Übergabepunkt im Gebäude.
- FTTH - Fibre to the Home: Glasfaser geht bis zum Teilnehmeranschluss in der Wohnung.

- FTTD - Fibre to the Desk: Glasfaser geht bis zum Teilnehmerendgerät (Telefon, PC, Router).

VSt = Vermittlungsstelle
KvZ = Kabelverzweiger (grauer Verteilkasten am Straßenrand – Verbindet mehrere Gebäude)
APL = Übergabepunkt innerhalb eines Gebäudes bei dem verschiedene Teilnehmer Anschlüsse zusammenlaufen.
TA = Teilnehmeranschluss (Anschlussdose)
TE = Teilnehmerendgerät (Telefon, PC, Router)

Fachbegriff Hotspot

- Ein Hotspot ist ein öffentlich zugänglicher drahtloser Internetzugangspunkt (Knotenpunkt).
- Er ist ein WLAN Access Point über den Benutzer entweder gratis (Open WLAN) oder kostenpflichtig sich anmelden können.
- Anmeldung erfolgt meist über eine Anmeldeseite im Browser. Login mit einem Code oder Passwort.
- Nutzungsdauer ist zeitgesteuert.
- Funktioniert nicht wie ein normaler Access Point. Eine Benutzerisolierung ist konfiguriert. Daten werden nicht an die anderen Benutzer desselben Hot Spots weitergeleitet. Unterbindet den Zugriff der Geräte untereinander.
- Einsatzgebiet: z.B. Hotels, Gastronomie, Öffentliche Plätze, usw.

Auch bei Smartphone einsetzbar. Man konfiguriert einen Hotspot, und stellt für andere Geräte einen WLAN-Hotspot für die Internetnutzung bereit.

Kenntnis der aktuellen WLAN-Standards und Verschlüsselungen

WLAN-Standards:
Entwickelt von IEEE (Institute of Electrical and Electronics Engineers)

IEEE 802.11 PHY Standards							
Release date	Standard	Frequency Band	Bandwidth	Transmission Scheme	Max Modulation	MIMO	Max Data Rate
1997	802.11	2.4 GHz	20 MHz	DSSS, FHSS	QPSK	N/A	2 Mb/s
1999	802.11b	2.4 GHz	20 MHz	DSSS	QPSK	N/A	11 Mb/s
1999	802.11a	5 GHz	20 MHz	OFDM	64QAM	N/A	54 Mb/s
2003	802.11g	2.4 GHz	20 MHz	DSSS, OFDM	64QAM	N/A	54 Mb/s
2009	802.11n	2.4 GHz 5 GHz	20 MHz 40 MHz	OFDM	64QAM	4x4	600 Mb/s
2013	802.11ac	5 GHz	20 MHz 40 MHz 80 MHz 160 MHz	OFDM	256QAM	8x8	6.93 Gb/s
2018	802.11ad	60 GHz	2160 MHz	SC, OFDM	256QAM	Beamforming	6.93 Gb/s

Verschlüsselungen:

WEP (Wired Equivalent Privacy):

- Verwendet RC4 zur Verschlüsselung.
- Authentifizierung erfolgt ein 4 Nachrichten (Request, Challenge, Response, Ergebnis) Verfahren mit einem WEP-Schlüssel.
- Das WLAN-Passwort ist einfach zu entschlüsseln.
- Sollte nicht mehr verwendet werden.
- Wird bei neuen Geräten nicht mehr verwendet.

WPA (WiFi Protected Access):

- Nachfolger von WEP.
- Verwendet TKIP (Temporal Key Integrity Protocol) zur Verschlüsselung, das auf RC4 basiert.
- Passwort kann per Wörterbuch Angriff erraten werden.
- Kurze schwache Passwörter sind unsicher.
- ARP-Spoofing möglich (gefälschte ARP Pakete werden gesendet, damit die ARP Tabelle beim Switch geändert wird, sodass Datenpakete zum Angreifer geschickt werden).
- Authentifizierung über einen Radius Server.

WPA2 (WiFi Protected Access2):

- Verwendet AES (Advanced Encryption Standard) zur Verschlüsselung.
- Wörterbuch Angriffe sind möglich.
- Damit WPA2 geschützte WiFi-Netze bisher nur über die Ermittlung des Passworts als angreifbar gelten, ist ein möglichst langes Passwort mit Sonderzeichen, Zahlen sowie Groß- und Kleinbuchstaben zu wählen. Zudem sind sinnvolle Wörter, die in Lexika geführt sind, zu vermeiden.

WPA3 (WiFi Protected Access3):

- robustere Authentifizierung und verbesserte Kryptografie.
- einfache Konfiguration für Geräte, die keine Bedienelemente haben.
- individuelle Verschlüsselung für jedes Gerät.
- Interoperabilität mit WPA2-Geräten.

Radius:

- Der Accesspoint leitet die Anfrage an den Radius Server weiter dieser genehmigt oder verweigert dann den Zugriff auf das WLAN.
- Radius ist Tripple-A (Authentification, Autorisation, Accounting)

VPN/IP Based encryption:

- Die Daten werden bereits vor dem Versenden durch eine Verschlüsselung geschützt und sind so unabhängig von der darunterliegenden WLAN-Verschlüsselung.

Standortwahl bei WLAN-Aufbau in Gebäuden

- Baulich meist eingeschränkt. Wasserleitungen und Stahlbeton sind ein großer Störfaktor.
- Betonböden, Wände und Mauern können das WLAN-Signal um 25 Prozent abschwächen.
- Router nicht im Keller aufstellen.
- Einen möglichst zentralen Ort innerhalb der Wohnung oder des Hauses suchen.
- Aufstellung, wo es die Infrastruktur zulässt.
- Aufstellung, wo ein Kabelgebundenes Netzwerk möglich ist.

- Es empfiehlt sich ein Test vor Ort oder eine genaue Analyse der Örtlichkeit.

Das WLAN-Signal schafft im Optimalfall zwischen 50 und 100 Meter, in der Realität häufig sehr viel weniger.
Haltet den Abstand zwischen Router und Empfangsgeräten möglichst gering.
Für große, mehrgeschossige Häuser mit Garten lohnt sich die Anschaffung eines WLAN-Repeaters.

Fachbegriff Roaming in Zusammenhang mit Access-Points

WLAN-Roaming:
Wenn sich ein WLAN über eine größere Fläche erstrecken soll, dann reicht ein Access Point in der Regel nicht aus. Um einen Bereich funktechnisch vollständig auszuleuchten bzw. abzudecken, muss man mehrere Access Points räumlich klug platzieren. Wenn sich die Funkbereiche der Access Points gegenseitig ein klein wenig überlappen, dann kann sich der Client zwischen den Access Points bewegen, ohne dass laufende Netzwerk-Verbindungen unterbrochen werden.
Als Roaming wird der Funkzellenwechsel bezeichnet. Damit WLAN-Roaming ohne Verlust der Verbindungen möglich ist, sind Helferfunktionen nötig.

Als Roaming bei Access Points bezeichnet man den Wechsel zwischen mehreren Access Points in großen Infrastructure WLAN-Umgebungen.
- Hierbei werden die Access Points so installiert das sie leicht überlappen, damit der Client zwischen den Access Points wechseln kann.
- Methoden sind ESSID (Extended Service Set Identifier) bei dem eine erweiterte SSID bei selbem Passwort verwendet wird und IEEE 802.11f das IAPP (Inter Access Point Protocol), bei dem die Access Points sich gegenseitig über die Clients informieren.

Fachbegriff MAC-Filtering

- Ist ein Netzwerk-Zugangsschutz, der nur Geräte mit bestimmter MAC-Adresse Zugang zum Netzwerk erlaubt.
- Das wird über eine Whitelist erlaubt. Oder über eine Blaclist verboten.
- Dieses Vorgehen erlaubt die Verbindung von Geräten auf Layer-2 zu unterbinden bzw. zu erlauben.
- Sinnvoller ist der Einsatz einer White-List, da bei der Blacklist durch einfaches Ändern der eigenen MAC der Filter umgangen werden kann.

Kenntnisse über VPN und Tunneling

VPN (Virtual Private Network):
- Ist ein logisches privates Netzwerk auf einer öffentlich zugänglichen Infrastruktur. Also ein Tunnel durch das Internet.
- Für VPN ist ein Server nötig auf den verbunden wird. Das wird meist bei Unternehmen verwendet wo der Benutzer von zu Hause aus auf das Unternehmensnetzwerk zugreifen möchte.
- Hier wird ein Punkt zu Punkt Verbindung aufgebaut über die Daten verschlüsselt übertragen werden.
- Nur die Benutzer, die zum privaten Netzwerk gehören können, untereinander kommunizieren und Daten austauschen.
- Voraussetzung ist Authentizität, Vertraulichkeit und Integrität.
- Einmalige Kosten fallen für die Einrichtung an, Laufende Kosten für den Internet Service Provider.

- Ist billiger, als wenn man eine Standleitung zur Verbindung nutzt.
- Wird auch im Bereich Internet Zensur eingesetzt, weil man die Möglichkeit hat all seine Anfragen über einen Server in einem anderen Land umzuleiten, um Zugriff auf gesperrte Webseiten zu erhalten.

Typen:

End to Site VPN:
Verbindet einen Heimarbeitsplatz oder mobilen Benutzer mit dem Firmennetzwerk
Wird auch Remote Access genannt

Remote Access VPN:
Werden verwendet, um entfernte Stationen so mit einem Netzwerk zu verbinden, als wären sie direkt im Netzwerk verbunden.

Site to Site VPN / LAN to LAN-VPN:
- Verbindet mehrere lokale Netzwerke von Außenstellen/Niederlassungen einer Firma.
- Als wären sie durch eine Standleitung verbunden.

Branch Office VPN:
- Verbindet mehrere lokale Netzwerke einer Firma.

Extranet Office VPN:
- Verbindet Netzwerke unterschiedlicher Firmen.

End to End VPN / Host to Host PVN / Remote Desktop VPN:
- Verbindet einen Client mit einem anderen Client in einem entfernten Netzwerk.
- Dazu muss bei beiden Clients eine VPN-Software installiert sein.
- Die Verbindung erfolgt über einen Tunnel.
- Die Clients bauen eine Verbindung zu einem Gateway auf, dass die beiden Verbindungen dann zusammenschaltet.

Zum Aufbau benötigt man ein Tunnelprotokoll:
- IPsec
- PPTP
- L2TP, L2TP over IPsec, SSL-VPN, Hamachi, OpenVPN (Software, kein Protokoll)

Tunneling:
- Beim Tunneling wird eine verschlüsselte Verbindung aufgebaut.
- Der Tunnel ist eine logische Verbindung zwischen zwei beliebigen Endpunkten. (VPn-Clients, VPN-Server, VPN-Gateways).
- Tunneling erlaubt es Pakete eines Netzwerkprotokolls in die Pakete eines anderen Netzwerkprotokolls einzukapseln.
- Beim Startpunkt des Tunnels werden die Pakete eingekapselt. Beim Endpunkt wieder entkapselt.
- Jedes Paket wird verschlüsselt, und der Inhalt der Datenpakete ist für andere nicht sichtbar.

Varianten:
- Tunnel ohne Verschlüsselung und Authentifizierung
- IPSEC Tunnel mit Authentifizierung
- IPSEC Tunnel mit Verschlüsselung