**Netzwerktechnik**

**Hub**

**(Nicht intelligent & unsicher & Unnötige Last im Netzwerk)**

Anwendungssicht 5

Transportschicht 4

Sicherungssicht 2

Bitübertragungssicht 1

**Switch**

**(Erhöhte Intelligenz & Mac-Tabelle & Erhöhte Sicherheit & Weniger Traffic)**

Anwendungssicht 5

Transportschicht 4

Netzwerksicht 3

Sicherungssicht 2

Bitübertragungssicht 1

**Router**

**(Routing auf Basis der IP-Adressen & Gateway)**

Anwendungssicht 5

Transportschicht 4

Netzwerksicht 3

Sicherungssicht 2

Bitübertragungssicht 1

**Mit Hub‘s und Switch’s baut man Netzwerke auf und mit Router verbindet man Netzwerke.**

**Übertragungsgeschwindigkeit**

Die tatsächliche Übertragungsgeschwindigkeit (Netto-Datenrate) von Ethernet hängt von der Geschwindigkeitsstufe und der TCP-Verbindungsqualität ab.

* Bei Fast Ethernet mit 100 MBit/s erreicht man knapp 0,094 GBit/s, also ca. 10 MByte/s.
* Bei Gigabit Ethernet mit 1 GBit/s erreicht man knapp 0,94 GBit/s, also ca. 100 MByte/s.
* Bei Gigabit Ethernet mit 2,5 GBit/s erreicht man knapp 2,4 GBit/s, also fast 300 MByte/s.
* Bei Gigabit Ethernet mit 10 GBit/s erreicht man netto 9,4 GBit/s, also umgerechnet etwas über 1.100 MByte/s.

Diese Geschwindigkeitsangaben entsprechen in etwa den zu erwartenden Durchsätzen für HTTP-Verbindungen, FTP-Downloads und Windows-Freigaben.  
Die Differenz zwischen der Brutto- und Netto-Datenrate geht für die Protokoll-Header auf Layer 2 und 3 drauf.

Zum Vergleich die Übertragungsgeschwindigkeit von PC-Schnittstellen:

* USB 2.0: ca. 40 MByte/s
* USB 3.0: ca. 450 MByte/s
* SATA-Festplatten: ca. 500 MByte/s
* PCIe-SSDs: über 3.000 MByte/s

**OSI-Model**

**Data 7 Application (Anwendung)**

**(Network Process to Application)**

**Anwendungs-Orientiert**

**Data 6 Presentation(Darstellung)**

**(Data representation and Encryption)**

**Data 5 Session (Kommunikation)**

**(Interhost communication)**

**Segments 4 Transport**

**(End-to-End connections and Reliability)**

**(TCP & UDP)**

**Packets 3 Network(Vermittlung)**

**Transport-Orientiert**

**(Path Determination and IP)**

**Frames 2 Data link (Sicherung)**

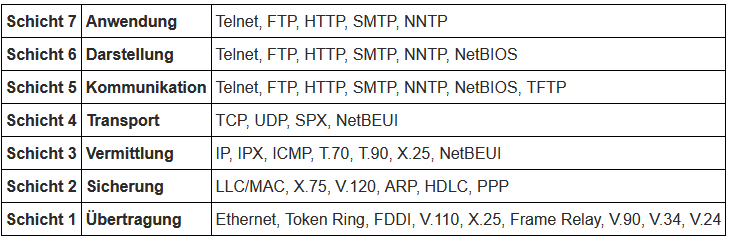
**(MAC and LLC / Physical addressing)**

**(Ethernet + TSN)**

**Bits 1 Physical (Bitübertragung)**

**(Media, Signal and Binary Transmission)**

**(Ethermet,Fast-Ethernet,Gigabit, Wifi. 10SPE, Ethernet-APL)**

****

**Ein Bild, das Text, Screenshot, Schrift, Reihe enthält.

Automatisch generierte Beschreibung**

**Schicht 1: Bitübertragungsschicht / Physical Layer**

**Maßnahmen und Verfahren zur Übertragung von Bitfolgen**

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

**Schicht 2: Sicherungsschicht / Data Link Layer**

Logische Verbindungen mit Datenpaketen und elementare Fehlererkennungsmechanismen

Die Sicherungsschicht sorgt für eine zuverlässige und funktionierende Verbindung zwischen Endgerät und Übertragungsmedium. Zur Vermeidung von Übertragungsfehlern und Datenverlust enthält diese Schicht Funktionen zur Fehlererkennung, Fehlerbehebung und Datenflusskontrolle.  
Auf dieser Schicht findet auch die physikalische Adressierung von Datenpaketen statt.

**Schicht 3: Vermittlungsschicht / Network LayerRouting und Datenflusskontrolle**

Die Vermittlungsschicht steuert die zeitliche und logische getrennte Kommunikation zwischen den Endgeräten, unabhängig vom Übertragungsmedium und der Topologie. Auf dieser Schicht erfolgt erstmals die logische Adressierung der Endgeräte. Die Adressierung ist eng mit dem Routing (Wegfindung vom Sender zum Empfänger) verbunden.

**Schicht 4: Transportschicht / Transport Layer**

**Logische Ende-zu-Ende-Verbindungen**

Die Transportschicht ist das Bindeglied zwischen den transportorientierten und anwendungsorientierten Schichten. Hier werden die Datenpakete einer Anwendung zugeordnet.

**Schicht 5: Kommunikationsschicht / Session Layer**

**Prozess-zu-Prozess-Verbindungen**

Die Kommunikationsschicht organisiert die Verbindungen zwischen den Endsystemen. Dazu sind Steuerungs- und Kontrollmechanismen für die Verbindung und dem Datenaustausch implementiert.

**Schicht 6: Darstellungsschicht / Presentation Layer**

**Ausgabe von Daten in Standardformate**

Die Darstellungsschicht wandelt die Daten in verschiedene Codecs und Formate. Hier werden die Daten zu oder von der Anwendungsschicht in ein geeignetes Format umgewandelt.

**Schicht 7: Anwendungsschicht / 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.

**Was ist eine IP-Adresse?**

Eine IP-Adresse ist eine **individuelle Adresse, die ein Gerät im Internet oder auf einem lokalen Netzwerk identifiziert**. IP steht für „Internetprotokoll“, wobei es sich um einen Satz von Regeln handelt, der das Format der Daten bestimmt, die über das Internet oder das lokale Netzwerk gesendet werden.

**Wie ist eine IPv4-Adresse aufgebaut?**

**32 Bit lang. 232 = 4.3 Milliarden IP-Adressen. 1 Block 8 Bit groß.**

**Oktett 1 Oktett 2 Oktett 3 Oktett 3**

**142.250.185.99**

**100011102 111110102 101110012 011000112**

**Bsp.: Subnetzmaske**

**192.128.0.0/24**

**11111111.11111111.11111111.00000000**

**255.255.255.0**

Subnetzmaske

Netzteil Hostteil

**Bsp. Hostanteil bestimmen.**

**192.128.0.0/24**

**11111111.11111111.11111111.00000000**

**255.255.255.0**

**28 = 256-2=254**

**Hostanteil**

**Wieso – 2?** Weil die niedrigste IP-Adresse und die höchste IP-Adresse **(Broadcastadresse)** sind schon vergeben.

**Wie ist eine IPv6-Adresse aufgebaut?**

**128 Bit lang. 2128 = 340 Sextillionen IP-Adressen.**

**1 Block 16 Bit groß.**

**Öffentliche Topologie Standorttopologie**

**2001:0db8:0000:0000:0000:54f3:dd6b:0001/64**

**Standortpräfix 48Bit Teilnetz-ID 16Bit Schnittstelle-ID 64Bit**

Das Standortpräfix legt die **öffentliche Topologie** Ihres Netzwerks gegenüber einem Router fest. Sie beziehen das Standortpräfix für Ihr Unternehmen von einem ISP oder der Regional Internet Registry (RIR).

In IPv6 definiert die **Teilnetz-ID** ein administratives Teilnetz des Netzwerks und umfasst bis zu 16 Bit. Sie weisen die Teilnetz-ID während der Konfiguration eines IPv6-Netzwerks zu. Das **Teilnetzpräfix** legt die Standorttopologie für einen Router fest, indem es den Link angibt, dem das Teilnetz zugewiesen wurde.

IPv6-Teilnetze gleichen konzeptuell IPv4-Teilnetzen, da jedes Teilnetz in der Regel einem Hardware-Link zugewiesen ist. IPv6-Teilnetz-IDs werden jedoch in hexadezimaler Notation, IPv4-Teilnetz-IDs hingegen in getrennter dezimaler Notation ausgedrückt.

Die **Schnittstellen-ID** gibt eine Schnittstelle für einen bestimmten Knoten an. Eine Schnittstellen-ID muss innerhalb des Teilnetzes einmalig sein. IPv6-Hosts können das Neighbor Discovery-Protokoll verwenden, um eigene Schnittstellen-IDs automatisch zu erzeugen. Neighbor Discovery generiert basierend auf der MAC- oder der EUI-64-Adresse der Host-Schnittstelle automatisch die Schnittstellen-ID. Sie können Schnittstellen-IDs auch manuell zuweisen. Dies wird für IPv6-Router und IPv6-konforme Server empfohlen.

**Das Präfix beschreibt den ersten Teil der IP-Adresse. Die Länge des Präfixes steht als Dezimalzahl hinter einem Schrägstrich. Für das hier genannte Beispiel lautet das Präfix**:

2001:db8::/**6410**

Die folgenden Präfixe wurden für besondere Zwecke reserviert:

**2002::/16** gibt an, dass ein 6to4-Routing-Präfix folgt.

**fe80::/10** gibt an, dass eine Link-lokale Adresse folgt.

**ff00::/8** gibt an, dass eine Multicast-Adresse folgt.

**Kürzen einer IPv6-Adresse.**

**Die führende Nullen und die 4-Blöcke mit Nullen können gestrichen werden.**

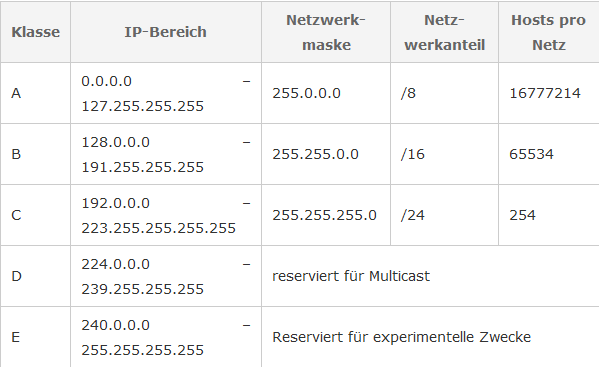
**2001:0db8:0000:0000:0000:54f3:dd6b:0001/64**

**Achtung: Es dürfen nur maximal zwei Doppelpunkte hintereinanderstehen.**

**2001:db8::54f3:dd6b:1/64**

**Es gibt unterschiedliche Netzwerkklassen (Classful).**

Netzklassen (Classful network) sind eine **1981 eingeführte Strukturierung des IPv4-Adressbereiches beim Internet Protocol (IP)**. Eine Netzklasse legt dabei die Aufteilung einer IP-Adresse in Netzadresse und Geräteadresse fest.

****

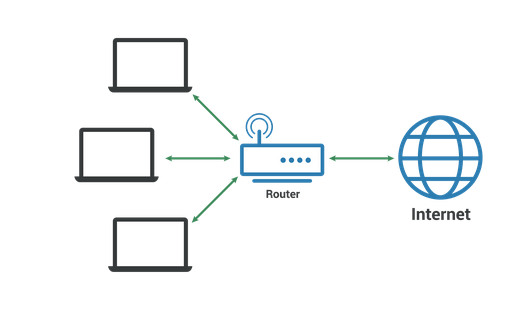
**Was ist ein Netzwerk?**

Unter einem [Netzwerk](https://www.ionos.de/digitalguide/server/knowhow/was-ist-ein-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 vernetzende Systeme vorhanden sein. Letztere wird durch spezielle Netzwerkprotokolle wie [TCP (Transmission Control Protocol)](https://www.ionos.de/digitalguide/server/knowhow/tcp-vorgestellt/) hergestellt. Bereits zwei miteinander verbundene Rechner können als Netzwerk betrachtet werden.

**Was ist ein Lan (Local Area Network)?**

Ein lokales Netzwerk (LAN) ist ein Netzwerk, das auf einen kleinen geografischen Bereich beschränkt ist, in der Regel innerhalb desselben Gebäudes. Heim-WiFi-Netzwerke und kleine Unternehmensnetzwerke sind gängige Beispiele für LANs.

LANs können auch recht groß ausfallen, obwohl es, wenn sie mehrere Gebäude umfassen, in der Regel genauer ist, sie als [Wide Area Network (WAN)](https://www.cloudflare.com/learning/network-layer/what-is-a-wan/) oder [Metropolitan Area Network (MAN)](https://www.cloudflare.com/learning/network-layer/what-is-a-metropolitan-area-network/) zu klassifizieren.

****

**Wie funktionieren LANs?**

Die meisten LANs sind an einem zentralen Punkt mit dem [Internet](https://www.cloudflare.com/learning/network-layer/how-does-the-internet-work/) verbunden: einem [Router](https://www.cloudflare.com/learning/network-layer/what-is-a-router/). In Heim-LANs wird oft ein einziger Router verwendet, während man in LANs in größeren Räumen zusätzlich [Netzwerk-Switches](https://www.cloudflare.com/learning/network-layer/what-is-a-network-switch/) für eine effizientere Paketzustellung einsetzen kann.

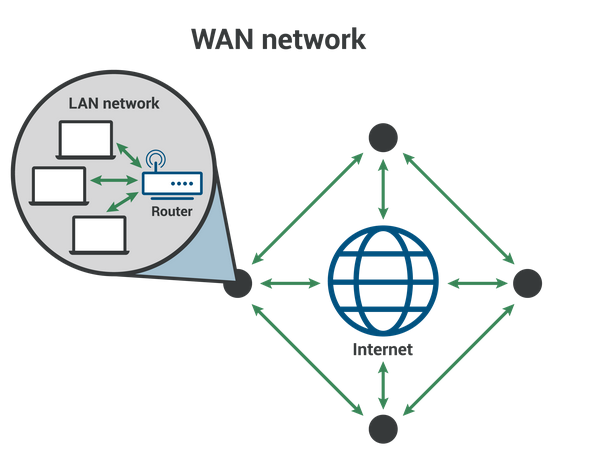
LANs verwenden fast immer Ethernet, WiFi oder beides, um Geräte innerhalb des Netzwerks zu verbinden. Ethernet ist ein Protokoll für physikalische Netzwerkverbindungen, dass die Verwendung von Ethernet-Kabeln erfordert. WiFi ist ein Protokoll, um sich mit einem Netzwerk über Funkwellen zu verbinden.

Man kann eine Vielzahl von Geräten an LANs anschließen, darunter Server, Desktop-Computer, Laptops, Drucker, IoT-Geräte und sogar Spielkonsolen. In Büros werden LANs häufig verwendet, damit die internen Mitarbeiter auf die angeschlossenen Drucker oder Server zugreifen können.

**Was ist ein Wan (Wide Area Network)?**

Ein Wide Area Network (WAN) ist ein großes Computer[netzwerk](https://www.cloudflare.com/learning/network-layer/what-is-the-network-layer/), das Gruppen von Computern über große Entfernungen miteinander verbindet. WANs werden häufig von großen Unternehmen verwendet, um ihre Büronetzwerke zu verbinden. Jedes Büro verfügt in der Regel über ein eigenes lokales Netzwerk oder [LAN](https://www.cloudflare.com/learning/network-layer/what-is-a-lan/) und diese LANs sind über ein WAN miteinander verbunden. Diese langen Verbindungen können auf verschiedene Weise hergestellt werden, z. B. über Standleitungen, [VPNs](https://www.cloudflare.com/learning/access-management/what-is-a-vpn/) oder IP-Tunnel (siehe unten).

Die Definition von WAN ist ziemlich weit gefasst. Technisch gesehen ist jedes große Netzwerk, das sich über ein großes geografisches Gebiet erstreckt, ein WAN. Das [Internet](https://www.cloudflare.com/learning/network-layer/how-does-the-internet-work/) selbst gilt als WAN.

****

**Was ist ein MAN (Metropolitan Area Network)**

Ein Bild, das Diagramm, Screenshot, Reihe, Text enthält.

Automatisch generierte BeschreibungEin Metropolitan Area Network (MAN) ist ein Computernetzwerk, das Computer in einem Ballungsraum miteinander verbindet. Dabei kann es sich um eine einzelne Großstadt, mehrere Städte und Gemeinden oder ein beliebiges großes Gebiet mit mehreren Gebäuden handeln. Ein MAN ist größer als ein [Local Area Network (LAN)](https://www.cloudflare.com/learning/network-layer/what-is-a-lan/), aber kleiner als ein [Wide Area Network (WAN)](https://www.cloudflare.com/learning/network-layer/what-is-a-wan/). MANs müssen sich nicht in städtischen Gebieten befinden. Der Begriff „metropolitan“ bezieht sich auf die Größe des Netzwerks, nicht auf die Demographie des Gebiets, das es bedient.

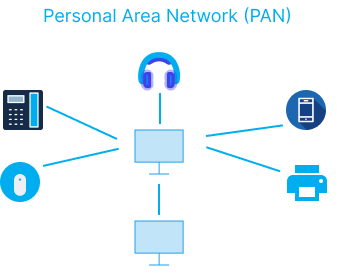
**Was ist ein Pan (Personal Area Network)?**

Bei einem PAN-Netzwerk handelt es sich um einen [Netzwerktypen](https://www.ionos.de/digitalguide/server/knowhow/diese-netzwerktypen-sollten-sie-kennen/), der Geräte in unmittelbarer Nähe zur Nutzerin bzw. zum Nutzer miteinander verbindet. Ein PAN ist speziell für die **Verbindung von Kleingeräten untereinander** konzipiert. Für den Verbindungsaufbau werden weder Router noch eine direkte Verbindung zum Internet benötigt. Mittels Personal Area Network ist es Kleingeräten möglich, Daten untereinander auszutauschen oder ein Ad-hoc-Netzwerk aufzubauen.

Die Verbindung ist entweder **kabellos oder kabelgebunden** und auf wenige Meter beschränkt. Je nach genutzter Technologie wird außerdem eine Sichtverbindung vorausgesetzt. Folgende Technologien ermöglichen den Verbindungsaufbau bei kabellosen PANs:

* Bluetooth
* Infrarot (IrDA)
* WLAN

Ein kabelgebundenes PAN-Netzwerk greift in den meisten Fällen auf eine USB-Verbindung zurück

****

**PICONET (Ad Hoc)** Entsteht, wenn sich mindestens zwei Geräte in

einem Pan verbinden.

**SCATTERNETZ** ist der Zusammenschluss mehrerer Piconet.

**Was ist VPN (Virtual Private Network)?**

**VPN** isteine Software, die deinen Internetzugriff durch die Bereitstellung einer geschützten und privaten Verbindung sogar dann sicherstellt, wenn du dich über ein öffentliches Netzwerk verbindest.

* Öffentliche WLAN-Netzwerke gefahrlos nutzen möchtest.
* Deine Aktivitäten im Internet besser schützen möchtest.
* Auf eine größere Auswahl an Inhalten zugreifen und Zensur umgehen möchtest.
* Dafür sorgen willst, im Internet nicht getrackt oder aufgezeichnet zu werden.
* Dir Preisdiskriminierung zu Nutze machen möchtest.

**Wie funktioniert ein VPN?**

1. **VPN stellt eine sichere Verbindung her**

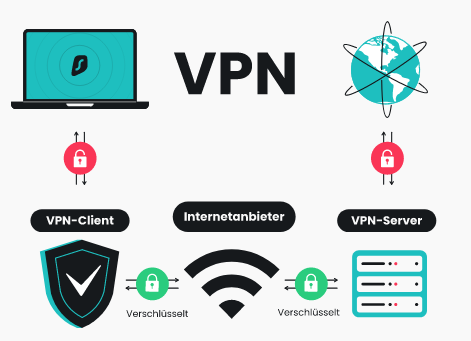
Bei der Internetverbindung über VPN wird ein sicherer virtueller Tunnel zwischen dem VPN und einem seiner Server hergestellt. Über diesen Tunnel wird dann dein ganzer Internetverkehr übertragen.

1. **VPN ändert deine IP-Adresse**

Sobald dein Internetverkehr durch den VPN-Tunnel fließt, ändert sich deine IP-Adresse, und du erhältst vorübergehend jene des VPN-Servers. Dadurch wird dein Standort den von dir genutzten Webseiten und Services als derjenige angegeben, an dem sich der von dir gewählte Server befindet.

1. **VPN-Zugang verschlüsselt deine Daten**

Um die Sicherheit des Tunneling-Prozesses zu gewährleisten, verbirgt ein VPN deine übermittelten Daten hinter einem Code (verschlüsselt sie also), damit keine Informationen verloren gehen und niemand deine Identität in Erfahrung bringen kann.

****

**Was bedeutet VPN-Tunneling?**

[Ein VPN-Tunnel](https://surfshark.com/de/blog/was-ist-tunnel-vpn) ist eine sichere Verbindung zwischen deinem Gerät und dem Server.

Tunneling basiert auf **Verkapselung**, wodurch VPN-Kommunikation im öffentlich zugänglichen Internet verborgen wird. Jeder, der deine Internetverbindung überprüft, wird sehen, dass du ein VPN verwendest, hat jedoch keinen Einblick darin, was du im Internet tust.

Die Möglichkeiten der Schaffung eines VPN-Tunnels sind vielfältig, deshalb existieren auch mehrere VPN-Protokolle.

**VLAN**

VLANs sind virtuelle lokale Netze, die in IEEE 802.1q standardisiert sind und auf der Schicht 2 des OSI-Schichtenmodells arbeiten. Typischerweise arbeitet man in einem Ethernet-basierten Netzwerk mit VLAN- bzw. Multi-LAN-Technik.  
Der Standard IEEE 802.1q ist für die VLAN-Technik bekannt, beinhaltet aber auch die Möglichkeit zur Priorisierung von Datenverkehr.

* Trennung der Datenströme bzw. Segmentierung durch virtuelle LANs (VLAN-ID)
* Priorisierung der Datenströme durch Class of Service (CoS)

Damit beide Verfahren funktionieren, müssen die Netzwerk-Komponenten auf der gesamten Übertragungsstrecke in der Lage sein, alle Datenpakete zu klassifizieren und zu priorisieren.

**Was ist mit „virtuelle LANs mit logischer Trennung“ gemeint?**

Die Trennung der Datenströme auf Schicht 2 durch virtuelle LANs sorgt dafür, dass sich Computer unterschiedlicher Subnetze (auf IP-Ebene) nicht sehen können. Denn VLAN-fähige Switche \*\*schalten Ethernet-Frames nur zwischen Ports, die zum selben VLAN gehören\*\*.

* Beispiel Voice-VLAN: Ein Switch erkennt VoIP-Telefone anhand der MAC-Adresse und weist diesen Geräten eine für Telefonie reserviertes VLAN zu. Der Sprachdatenverkehr wird dadurch vom herkömmlichen Datenverkehr im selben lokalen Netzwerk abgeschottet.
* Beispiel Private-VLAN: Jeder Switch-Port ist ein eigenes VLAN. Auf diese Weise können die Clients im lokalen Netzwerk nicht direkt miteinander kommunizieren. Auf diese Weise kann der Datenverkehr durch Fremde nicht ausgespäht werden (ARP Spoofing). Die einzelnen Endgeräte bekommen nur Zugriff aufs Internet. Sinnvoll für Gäste in Hotels und Unternehmen.

Ein Bild, das Text, Diagramm, Plan, Screenshot enthält.

Automatisch generierte Beschreibung

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

**Ein Bild, das Text, Screenshot, Schrift, Zahl enthält.

Automatisch generierte Beschreibung**

Insgesamt wird das Ethernet-Frame um 4 Byte verlängert und zusätzliche Informationen in den Header gepackt.  
Das VID-Feld enthält das 12 Bit lange VLAN-Tag für die Segmentierung bzw. Trennung des Datenverkehrs.  
Im ToS-Feld des Ethernet-Headers können drei Bit für die Priorisierung verwendet werden (IP-Precedence). Mit drei Bit können 8 Prioritätsstufen abgebildet und Dienstklassen bzw. einem Class of Service (CoS) zugeordnet werden.

**Anwendung von VLANs**

VLANs können dann sinnvoll eingesetzt werden, wenn man zwei oder mehrere voneinander physikalisch getrennte Netze haben möchte, aber keine zusätzliche Hardware installieren will.

* Trennung von Zugängen zum lokalen Netzwerk mit Zugriff aufs lokale Netzwerk und nur mit Internet-Zugang.
* Trennung von Test- und Produktivumgebungen.
* Normalen Datenverkehr von Anwendungen und Backup trennen.
* Minimierung des Datenverkehrs innerhalb des lokalen Netzwerks. Beispielsweise Begrenzung von Broadcast durch ARP, DHCP, MAC-Flooding, usw. (Hinweis: Broadcasts lassen sich auch durch Subnetting begrenzen.)

**FDDI (Fiber Distributed Data Interface)**

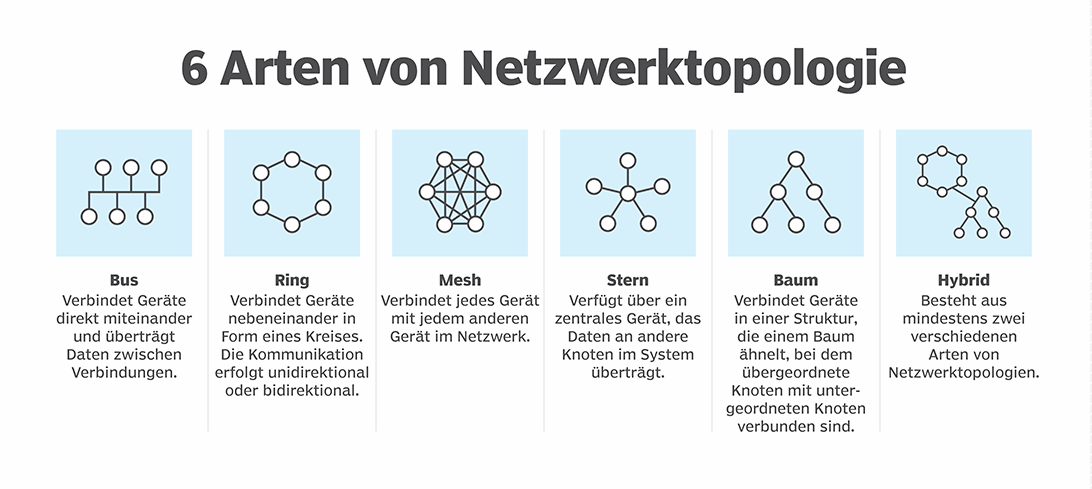
FDDI (Fiber Distributed Data Interface) ist ein Satz an [ANSI](https://www.computerweekly.com/de/definition/ANSI-American-National-Standards-Institute)- und ISO-Standards für die Datenübertragung via Glasfaserkabel in einem [LAN (Local Area Network)](https://www.computerweekly.com/de/definition/LAN-Local-Area-Network). Damit lassen sich Entfernungen von bis zu 200 Kilometer überbrücken. Das FDDI-[Protokoll](https://www.computerweekly.com/de/definition/Protokoll) basiert auf dem [Token-Ring](https://www.computerweekly.com/de/definition/Token-Ring)-Protokoll. Man kann damit nicht nur große Bereiche abdecken, ein mit FDDI-realisiertes LAN kann auch Tausende an Anwender bedienen. FDDI wird häufig als Backbone verwendet für ein [WAN (Wide Area Network)](https://www.computerweekly.com/de/definition/Was-ist-WAN-Optimierung).

Ein FDDI-Netzwerk besteht aus zwei Token Rings. Dabei ist ein Ring als Backup gedacht, falls der primäre ausfällt. Der primäre Ring liefert bis zu 100 Mbps. Wird der sekundäre Ring nicht als Backup benötigt, lassen sich darüber ebenfalls Daten übertragen. So erhöht sich die Kapazität auf 200 Mbps. Die Verwendung eines einzelnen Rings erhöht die maximale Distanz. Ein Dual-Ring kann bis zu 100 Kilometer abdecken.

**Was ist eine Netzwerktopologie?**

Eine Netzwerktopologie wird normalerweise durch eine Linien- und Objektzeichnung dargestellt, di die gesamte physische und logische Anordnung wiederspielt.

Es gibt zwei verschiedene Arten von Netzwerktopologien:

* Die **physische** Netzwerktopologie ist die Anordnung verschiedener Komponenten eines Netzwerks. Die verschiedenen Anschlüsse repräsentieren die physischen Netzwerkkabel und die Noten repräsentieren die physischen Netzgeräte (z.B. Switches)
* ****Die **logische** Netzwerktopologie veranschaulichen auf einer höheren Ebene, wie Daten innerhalb eines Netzwerks fließen.
* **Bus-Topologie**: Alle Geräte/Knoten sind an eine einzige Kommunikationsleitung, den Bus, angeschlossen. Der Bus dient als Backbone, der alle Geräte im Netzwerk miteinander verbindet.  
  dem Netzwerk verbindet. Dies ist eine einfache, kostengünstige Topologie, aber wenn der Bus ausfällt, kann der Single Point of Failure (SPOF) das gesamte Netz lahmlegen.
* **Sterntopologie:** Alle Knoten des Netzes sind mit einem zentralen Hub oder Switch verbunden. Der Hub oder Switch fungiert als zentraler Punkt für die Kommunikation, und jedes Gerät hat eine eigene Verbindung zu ihm. Diese Topologie ist beliebt, weil sie einfach zu verwalten ist und eine Unterbrechung einer Verbindung keine Auswirkungen auf die anderen Geräte hat.
* **Ring-Topologie:** Alle Knoten des Netzes sind in einer geschlossenen Schleife verbunden, und die Daten fließen in einer Richtung um die Schleife herum. Ringtopologien sind in der Regel redundant ausgelegt, um sicherzustellen, dass eine Unterbrechung des Rings nicht zum Ausfall des gesamten Netzes führt.
* **Baum-Topologie:** Alle Knoten sind in einer hierarchischen Struktur angeordnet, die einem physischen Baum ähnelt. Der zentrale Knoten an der Spitze des Baums (in der Regel ein Hub oder Switch) kann eine Verbindung zu mehreren anderen Knoten herstellen, die wiederum eine Verbindung zu anderen zusätzlichen Knoten herstellen können.
* **Mesh-Topologie:** Jeder Knoten ist direkt mit einigen (oder allen) anderen Netzwerkknoten verbunden. Die Redundanz macht diese Art von Topologie hochgradig fehlertolerant, aber sie erfordert mehr Bandbreite und kann teuer in der Implementierung sein.

**Subnetz**

Ein Subnetz ist ein oder mehrere LAN-Segmente, die durch Router begrenzt werden und das gleiche IP-Adresspräfix verwenden. Statt Subnetz sind auch die Begriffe Netzwerksegment oder Link gebräuchlich.

**Gateway**

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

**Protokoll**

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

**Domäne**

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

**Datenpaket / Paket**

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

**Frame**

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

**Port**

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

**Tunneling**

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

**Datagramm**

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

**Unicast, Multicast, Broadcast und Anycast**

* **Unicast:** Unicast-Adressen adressieren genau einen Host. Die Übertragung erfolgt von einem Host zu einem anderen Host.
* **Multicast:** Hinter einer Multicast-Adresse verbergen sich ein ganzes Gruppen von Hosts. Die Übertragung erfolgt von einem Host an mehrere Hosts.
* **Broadcast:** Broadcast-Adressen adressieren alle Hosts. Die Übertragung erfolgt von einem Host an alle anderen Hosts.
* **Anycast:** Anycast-Adressen werden von mehreren Hosts in einem Netzwerk verwendet. Die Übertragung erfolgt von einem Host an einen Host aus einer Gruppe bzw. einem Verbund.

**Node**

Ein Node ist ein allgemeiner Begriff für eine physikalisch vorhandene Komponente in einem Netzwerk. Es handelt sich um ein Gerät, dass an einem oder mehreren Netzwerken angeschlossen ist. Dazu verfügt es über eine oder mehrere Schnittstellen.  
Ein Node kann ganz allgemein ein Host, ein Client oder ein Server sein.

**Link**

Ein physikalisches Netzwerk bezeichnet man manchmal auch als Link, was Verbindung bedeutet. Zu diesem Netzwerk gehören alle Nodes, die an demselben Link angeschlossen sind bzw. die direkt miteinander verbunden sind.

**Site**

Ein Netzwerk und die daran angeschlossenen Nodes bilden eine Site, wenn sie einer gemeinsamen und zusammenhängenden Verwaltung unterstellt sind.  
Dieser Begriff ist eher unüblich. Oft ist eine Site das lokale Netzwerk und wird als LAN bezeichnet.

**Host**

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

**Knoten**

Allgemein formuliert ist ein Knoten ein Verzweigungspunkt in einem Kommunikationsnetzwerk, an dem mehrere Verbindungen zusammenlaufen. Knoten sind im Telefonnetz die Vermittlungsstellen oder auch Telefonanlagen. In einem IP-Netzwerk sind Router und in einem Ethernet-Netzwerk sind Switche die Knoten.  
Zugangspunkte zu einem Netzwerk, z. B. WLAN-Access-Points, werden häufig auch als Knoten bezeichnet.

**Client**

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

**Server**

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

**Ressourcen**

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

**Unidirektionale Kommunikation**

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

**Bidirektionale Kommunikation**

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

**Masquerading**

Masquerading bezeichnet das Verbergen ganzer Netze hinter einer einzigen IP-Adressen.

Masquerading finde ich häufig bei SOHO-Umgebungen, die vom Internet-Provider nur eine IP-Adresse bekommen und hinter dieser sich verschiedene Endgeräte verbergen, die alle eine Verbindung in das Internet benötigen. Das bedeutet, mehrere interne Adressen werden über ein NAT-Verfahren auf eine externe Adresse gebündelt. Von der externen Seite sind die internen Rechner nicht direkt adressierbar, da von außen nur eine IP-Adresse sichtbar ist.

**Bonding**

Beim Bonding werden mehrere physikalisch vorhandene Leitungen zu einer logischen Leitung zusammengeschaltet. In der Regel, um eine höhere Geschwindigkeit zu erreichen.

**Backbone**

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

**Distance Vector**

Distance-Vector-Protokolle basieren auf der Idee, den besten Pfad zu einem Zielnetzwerk basierend auf der Entfernung (Anzahl der Hops) und der Richtung (Vektor) zum Ziel zu wählen. Router, die Distance-Vector-Protokolle verwenden, teilen ihre Routingtabellen nur mit ihren direkten Nachbarn.

**Link State**

Ein **Link*-*State*-***Routing-Protokoll ist ein Netzwerkprotokoll, das von Routern benutzt wird, um eine komplexe Datenbank mit Topologie-Informationen aufzubauen.

**Was ist ein Port?**

Ein Port ist ein virtueller Punkt, an dem Netzwerkverbindungen beginnen und enden. Ports sind softwarebasiert und werden vom Betriebssystem eines Computers verwaltet. Jeder Port ist mit einem bestimmten Prozess oder Dienst verbunden. Mithilfe von Ports können Computer, leicht zwischen verschiedenen Arten von Traffic unterscheiden.

**Was ist eine Portnummer?**

Ports sind für alle mit dem Netzwerk verbundenen Geräte standardisiert, wobei jedem Port eine Nummer zugewiesen wird. Die meisten Ports sind für bestimmte [Protokolle](https://www.cloudflare.com/learning/network-layer/what-is-a-protocol/) reserviert – zum Beispiel gehen alle [Hypertext Transfer Protocol (HTTP)](https://www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-protocol-http/)-Nachrichten an Port 80. Genauso wie [IP-Adressen](https://www.cloudflare.com/learning/dns/glossary/what-is-my-ip-address/) es ermöglichen, Nachrichten an und von bestimmten Geräten zu senden, ermöglichen Portnummern das Senden an bestimmte Dienste oder Anwendungen innerhalb dieser Geräte.

[**TCP**](https://www.ionos.de/digitalguide/server/knowhow/tcp-vorgestellt/) **(umfangreicher)**und[**UDP**](https://www.ionos.de/digitalguide/server/knowhow/udp-user-datagram-protocol/) (**kleiner und schneller**) sorgen für die Verbindung zwischen zwei Geräten über das Internet oder andere Netzwerke. Damit Datenpakete allerdings einen Eingang beim PC oder Server auf der anderen Seite der Verbindung finden können, müssen hier Türen geöffnet sein. Solche **Öffnungen in das System** nennt man Ports. Für die beiden Protokolle gibt es einige bekannte und wichtige Ports, die man bei der Entwicklung von Web-Anwendungen kennen sollte.

**Was sind die verschiedenen Portnummern?**

Es gibt 65.535 mögliche Portnummern, von denen jedoch nicht alle gebräuchlich sind. Einige der gebräuchlichsten Ports, zusammen mit dem zugehörigen Netzwerkprotokoll, lauten:

**Ports 20 und 21:** File Transfer Protocol (FTP). FTP dient der Übertragung von Dateien zwischen einem Client und einem Server. Bei diesen Ports sind einmal Datenkanal und Steuerungskanal.

* **Port 22:** Secure Shell (SSH). SSH ist eines von vielen [Tunneling](https://www.cloudflare.com/learning/network-layer/what-is-tunneling/)-Protokollen, die sichere Netzwerkverbindungen herstellen.
* [Port 25](https://www.cloudflare.com/learning/email-security/smtp-port-25-587/): In der Vergangenheit [Simple Mail Transfer Protocol (SMTP)](https://www.cloudflare.com/learning/email-security/what-is-smtp/). SMTP wird für [E-Mail](https://www.cloudflare.com/learning/email-security/what-is-email/)verwendet.
* **Port 53:** [Domain Name System (DNS)](https://www.cloudflare.com/learning/dns/what-is-dns/). DNS ist ein wesentlicher Prozess für das moderne Internet; es ordnet von Menschen lesbare [Domainnamen](https://www.cloudflare.com/learning/dns/glossary/what-is-a-domain-name/) maschinenlesbaren IP-Adressen zu. So können Nutzer, Websites und Anwendungen zu laden, ohne sich eine lange Liste von IP-Adressen merken zu müssen.
* **Port 80:** Hypertext Transfer Protocol (HTTP). HTTP ist das Protokoll, das das World Wide Web möglich macht.
* **Port 123:** [Network Time Protocol (NTP)](https://blog.cloudflare.com/secure-time/). NTP ermöglicht die Synchronisierung von Computeruhren untereinander, ein Prozess, der für die [Verschlüsselung](https://www.cloudflare.com/learning/ssl/what-is-encryption/) unerlässlich ist.
* **Port 179:** [Border Gateway Protocol (BGP)](https://www.cloudflare.com/learning/security/glossary/what-is-bgp/). BGP ist ein unerlässliches Protokoll für die Einrichtung effizienter Routen zwischen den großen Netzen, aus denen das Internet besteht (diese großen Netze werden [autonome Systeme](https://www.cloudflare.com/learning/network-layer/what-is-an-autonomous-system/) genannt). Autonome Systeme verwenden BGP, um mitzuteilen, welche IP-Adressen sie kontrollieren.
* **Port 443:** [HTTP Secure (HTTPS)](https://www.cloudflare.com/learning/ssl/what-is-https/). HTTPS ist die sichere und verschlüsselte Version von HTTP. Der gesamte HTTPS-Web-Traffic läuft über den Port 443. Netzwerkdienste, die HTTPS zur Verschlüsselung verwenden, wie [DNS over HTTPS](https://www.cloudflare.com/learning/dns/dns-over-tls/), stellen ebenfalls eine Verbindung über diesen Port her.
* **Port 500:** Internet Security Association and Key Management Protocol (ISAKMP), das Teil des Prozesses zum Aufbau sicherer [IPsec](https://www.cloudflare.com/learning/network-layer/what-is-ipsec/) Verbindungen ist.
* **Port 587:** Modernes, sicheres SMTP, das Verschlüsselung verwendet.
* **Port 3389:** [Remote Desktop Protocol](https://www.cloudflare.com/learning/access-management/what-is-the-remote-desktop-protocol/) (RDP). RDP ermöglicht es Nutzern, von einem anderen Gerät aus einer Fernverbindung zu ihrem Desktop-Computer herzustellen.

**Well Kown Ports**

* HTTP: 80/TCP
* HTTPS: 443/TCP
* SMTP: 25/TCP
* SMTP (TLS): 587/TCP
* SSH: 22/TCP (optional UDP)
* RDP: 3389/TCP (optional UDP)
* DNS: 53/TCP und UDP
* Telnet: 23/TCP
* FTP (Data): 20/TCP
* FTP (Control): 21/TCP
* POP unverschlüsselt 110
* SMTP unverschlüsselt 25
* SSL POP 995  
  SSL IMAP 993  
  SSL SMTP 465  
  TLS POP 995  
  TLS IMAP 143  
  TLS SMTP 587

**Was ist DHCP (Dynamic Host Configuration Protocol)?**

Das Dynamic Host Configuration Protocol (DHCP) ist ein Kommunikationsprotokoll für Computernetzwerke, das 1997 im RFC 2131 definiert wurde. Nach dem Client-Server-Prinzip sorgt es dafür, dass verbindungssuchende Geräte automatisch eine wiederverwendbare Netzwerkadresse und alle weiteren relevanten Parameter beziehen.

Die Adresszuordnung mit DHCP funktioniert nach **dem Client-Server-Prinzip**: Die verbindungssuchenden Geräte fordern die IP-Adresskonfiguration von einem DHCP-Server an, der seinerseits auf eine Datenbank zurückgreift, in der **die einzustellenden Netzwerkparameter** vorgegeben sind. Unter anderem kann dieser Server, der Bestandteil jedes modernen DSL-Routers ist, dem Client mithilfe seiner Datenbankinformationen folgende Einstellungen zuweisen:

* eindeutige **IP-Adresse**
* **Subnetzmaske**
* Standard-**Gateway**
* **DNS**-Server
* **Proxy**-**Konfiguration** via WPAD (Web Proxy Auto-Discovery Protocol)

**Was ist NAT (Network Address Translation)?**

NAT bezeichnet das **Übersetzen von Netzwerkadressen** (Network Address Translation). Es ist eines der wichtigsten Verfahren, wenn es um die Verbindung eines lokalen Netzwerks mit dem Internet geht.

Ein Bild, das Text, Schrift, Reihe, Diagramm enthält.

Automatisch generierte Beschreibung

**Welche Vorteile hat NAT?**

**NAT hilft die Verknappung der IPv4-Adressen zu entschleunigen**. Dies geschieht durch die Ersetzung mehrerer Adressen für mehrere Endsysteme durch eine einzige IP-Adresse. IP-Adressen eines Netzes können vor einem anderen Netz verborgen werden.

**IPv6 vs NAT!**

Durch IPv6 wird NAT überflüssig. Der Wegfall von NAT verbessert den Betrieb von Netzwerken erheblich. Fehler, die durch NAT verursacht wurden, fallen weg. Außerdem lassen sich Fehler schneller finden und beheben.  
Ohne NAT werden Protokolle, wie STUN überflüssig. Das freut besonders Entwickler, weil jedes Protokoll, dass nicht implementiert werden muss, erst gar keine Sicherheitslücken aufreißen kann. Doch ohne NAT wird in Zukunft eine gut konfigurierte Firewall wichtiger werden. Bei IPv6 sollte die Firewall Verbindungsversuche von außen nach innen verhindern, wenn vorher keine Verbindung von innen nach außen bestanden hat.

**STP (Spanning Tree Protocol)**

Das Spanning Tree Protocol (STP) verhindert in Netzwerken mit mehreren Switches parallele Verbindungen und unterbindet dadurch die Bildung von Schleifen. STP funktioniert in beliebig vermaschten Netzstrukturen und erzeugt eine Baumtopologie mit eindeutigen Verbindungspfaden.

Das Spanning Tree Protocol, abgekürzt STP, wurde 1990 in der **IEEE-Norm 802.1D** standardisiert.

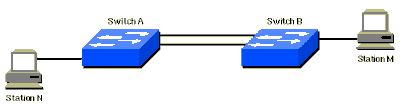
Verbindungen zwischen Quelle und Ziel mehr vorhanden sind. Gleichzeitig ist jeder vernetzte Punkt von einem anderen vernetzten Punkt über die bestmögliche Verbindung erreichbar. Kommt es zu einer Unterbrechung einer Verbindung oder zum Ausfall eines Switches, reorganisiert das Spanning Tree Protocol dem Baum und ermittelt neue Verbindungspfade.

**Die verschiedenen Zustände eines Port-Switches im Spanning Tree**

Ein Switchport erkennt 5 Zustände:

1. **Forwarding**
2. **Blocking**
3. **Learning**
4. **Listening**
5. **Disabled**

Ports im Zustand **Forwarding** leiten Frames weiter, empfangen BPDUs und lernen Adressen. Sie sind komplett aktiv. **Blocking** Ports verwerfen Frames, lernen keine Adressen, empfangen aber BPDUs. Diese Ports sind nicht an der Frameweiterleitung beteiligt. Nach der Aktivierung des STP durchlaufen die Ports eines Switches abhängig von der Position im **Spanning** Tree die Zustände **Blocking**, **Listening**, **Learning** und **Forwarding**. Timer und BPDUs sorgen für den Übergang der einzelnen Zustände und bestimmen die Konvergenzzeit, die benötigt wird, um den Spanning Tree zu berechnen oder bei einem Verbindungsausfall neu zu bestimmen.

****

**Was sind BPDU-Pakete?**

STP nutzt sogenannte Bridge Priority Data Units (BPDU) für den Informationsaustausch in einem Netzwerk. Bei BPDU handelt es sich um Pakete, die Switche untereinander austauschen, um mit Hilfe der übermittelten Informationen eine zuverlässige Netzwerk-Topologie und -Hierarchie zu errichten.

Grundeinheiten der Physik:

Meter

Sekunde

Zeitspannen werden seit jeher über die Dauer eines periodischen Vorgangs definiert. (24 Stunden · 60 Minuten · 60 Sekunden)

Kilogramm

Die Einheit der Masse ist die einzige der sieben physikalischen Basiseinheiten des SI-Systems, die noch immer über einen Referenzgegenstand – einen Zylinder aus einer Platin-Iridium-Legierung – festgelegt ist.

Ampere

Diese Basiseinheit für die Stromstärke.

Candela

Früher nutzte man als Einheit der Lichtstärke Kerzen mit einer bestimmten Dochthöhe. Anhand dieser Standardkerzen ließ sich feststellen, wie hell eine Lichtquelle leuchtet.

Mol

Das Mol erlaubt es Chemikern, die Mengenverhältnisse und die Konzentration von Substanzen auszurechnen, die für eine chemische Reaktion benötigt werden.

Kelvin

Will man die Phänomene der Wärmelehre in Zahlen fassen, so bedarf es eines Maßstabes für die Temperatur. Im SI-System ist das nicht das vertraute Grad Celsius, sondern das Kelvin.

**Farme Relay**

**GSM Umts GPS LTE**

**Satellitennetze**