

Handlungsziele und handlungsnotwendige Kenntnisse

Modul 129 LAN-Komponenten in Betrieb nehmen

✓ 1. Anforderungen für ein neues Netzwerk aufnehmen und die erforderlichen Netzwerkkomponenten bestimmen (Switch, Router) ▾

1. Kennt die wichtigsten Gremien (IEEE, ISO) sowie die von ihnen definierten Standards (z.B. 100BaseT, IEEE 802.x).
2. Kennt die aktuellen LAN-Technologien und deren Einsatzgebiete und Funktionsweise.
3. Kennt die Funktionsweise von Switch und Router und deren Einsatzgebiete.
4. Kennt Eigenschaften und Zusatzfeatures von Switches (z.B. manageable, stackable, auto-sense, spanning tree).
5. Kennt die Sicherheitsschwachstellen von Switch und Routern (z.B. Defaultpasswort, telnet).
6. Kennt Symbole zur schematischen Darstellung von Netzwerken.

✓ 2. Adressschema für IP Netz mit Subnetzen anpassen und geeignetes Subnetting mit zugehöriger Netzmaske aus Vorgaben ableiten (z.B. Aufteilung in IP Netze, Anzahl Clients) ▾

1. Kennt die Elemente und Funktionen des IP-Protokolls (MAC- und IP-Adressen, IP-Adressklassen, private Adressen, Netzmasken, Routing, Adress Resolution Protocol (ARP)).
2. Kennt Gründe für die Aufteilung eines Netzwerks in IP-Subnetze.
3. Kennt die Algorithmen zur (binären) Berechnung von IP-Subnetzen.

✓ 3. Netzwerkkomponenten gemäss Netzwerkschema und Adressierung in Betrieb nehmen und konfigurieren ▾

1. Kennt die notwendigen Einstellungen für Router und Switch zur Sicherstellung der Kommunikation im Netzwerk.

✓ 4. Statisches Routing gemäss Netzwerkschema implementieren und Routing Tabelle interpretieren

1. Kennt die Unterschiede zwischen statischem und dynamischem Routing.
2. Kennt den Aufbau und den Inhalt von Routingtabellen und den Zusammenhang zum Netzwerkschema.

✓ 5. Konfigurationsfehler und ihre Ursachen mit geeigneten Hilfsprogrammen analysieren und beheben

1. Kennt Verfahren zur systematischen Eingrenzung von Fehlern im Netzwerk (z.B. Ausschlussverfahren, Einordnung im OSI-Schichtenmodell).
2. Kennt Werkzeuge zur Fehleranalyse und -behebung und weiß, bei welchen Symptomen welche Werkzeuge eingesetzt werden.

✓ 6. Netzwerkdokumentation erstellen bzw. nachführen (Konfiguration, Netzwerkschema)

1. Kennt Aufbau und Inhalt einer Netzwerkdokumentation.

✓ 7. Netzwerk mit einem Abnahmeprotokoll dem Kunden übergeben

1. Kennt den Aufbau und Inhalt eines Abnahmeprotokolls.

Grundlagen

Komponenten

Die physischen, sichtbaren Komponenten eines Netzwerkes können in folgende Kategorien eingeteilt werden:

Kategorie	Beschreibung	Beispiele
Endgeräte	Komponenten die von einem Benutzer verwendet werden	PC, Server, Drucker, Scanner,..
Verbindungsgeräte	Komponenten, die benötigt werden, damit die Endgeräte kommunizieren können	Switch, Router, Modem, Netzwerkkarte,..
Übertragungsmedien	Komponenten, die Signale zwischen den Geräten übertragen	Kupferkabel, Glasfaserkabel, elektromagnetisches Feld

Protokolle

Ein Netzwerkprotokoll (auch Netzprotokoll) ist ein Kommunikationsprotokoll für den Austausch von Daten zwischen Computern bzw. Prozessen, die in einem Rechnernetz miteinander verbunden sind (verteiltes System). Die Vereinbarung besteht aus einem Satz von Regeln und Formaten (Syntax), die das Kommunikationsverhalten der kommunizierenden Instanzen in den Computern bestimmen.



Abb. 1: Beispiel eines Protokolles

Für eine sichere Datenübertragung werden meistens mehrere Protokolle benötigt, wobei jedes Protokoll bestimmte Teilaufgaben übernimmt. Die Protokolle können als Software

implementiert sein, z.B. Treiber für TCP/IP Protokolle oder direkt in der Hardware, z.B. Ethernet-Protokoll in der Netzwerkkarte.

Die Protokolle definieren wie die einzelnen Datenpakete einer Datenübertragung aufgebaut sind.

Datenpakete

Der in einem Protokoll beschriebene Aufbau eines Datenpaketes enthält für den Datenaustausch wichtige Informationen über das Paket wie beispielsweise:

- ✓ dessen Absender und Empfänger, damit Nicht-Empfänger das Paket ignorieren
- ✓ den Typ des Pakets (beispielsweise Verbindungsaufbau, Verbindungsabbau oder reine Nutzdaten)
- ✓ die Paketgrösse, die der Empfänger zu erwarten hat
- ✓ bei mehrteiligen Übertragungen die laufende Nummer und Gesamtzahl der Pakete
- ✓ eine Prüfsumme zum Nachvollziehen einer fehlerfreien Übertragung

Diese Informationen werden den Nutzdaten als Header vorangestellt oder als Trailer angehängt



Abb. 2: Grundlegender Aufbau eines Datenpaketes

Der Header eines Datenpaketes lässt sich mit dem Couvert eines Briefes vergleichen, auf dem alle nötigen Informationen für die korrekte Zustellung vorhanden sind, wohingegen die Nutzdaten den eigentlichen Inhalt des Briefes ausmachen:



In der nächsten Abbildung sehen Sie den Aufbau des Headers eines IPv4 Paketes

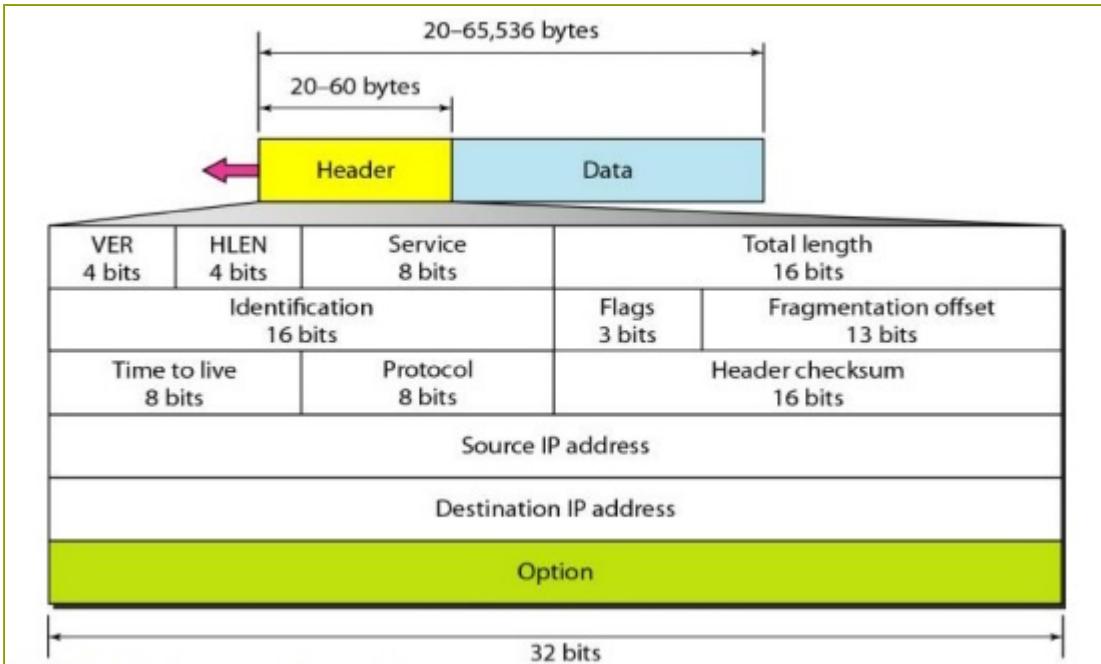


Abb. 3: Aufbau des Headers eines IPv4 Paketes

Die einzelnen Felder eines Headers lassen sich mit einem Protocol Analyzer, z.B. Wireshark auslesen:

```

Internet Protocol Version 4, Src: 192.168.82.147 (192.168.82.147), Dst: 192.243.232.2 (192.243.232.2)
  Version: 4
  Header Length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 1155
  Identification: 0x69de (27102)
  Flags: 0x02 (Don't Fragment)
    0... .... = Reserved bit: Not set
    .1... .... = Don't fragment: Set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to Live: 128
  Protocol: TCP (6)
  Header checksum: 0xd064 [validation disabled]
    [Good: False]
    [Bad: False]
  Source: 192.168.82.147 (192.168.82.147)
  Destination: 192.243.232.2 (192.243.232.2)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  Transmission Control Protocol, Src Port: 57487 (57487), Dst Port: 80 (80), Seq: 1102, Ack: 883, Len: 1115

```

Abb. 4: IPv4 Header mit Wireshark

Standards

Gremien

Im Zusammenhang mit Netzwerktechnik sind folgende Gremien wichtig:

- ✓ **IEEE**: Institute of Electrical and Electronics Engineers:
 - Standardisierung von Techniken, Hardware, Software
 - z.B. IEEE 802: Standards im Bereich der lokalen Netze (LAN)
- ✓ **RFC**: Request for Comments:
 - z.B. Regeln für die TCP/IP Protokollfamilie RFC 791: IPv4 Adressen
- ✓ **ISO**: International Organization for Standardization
 - z.B. ISO/IEC 11801: für strukturierte Verkabelung UGV
- ✓ **OSI**: Open System Interconnection Model:
 - Referenzmodell für Netzwerkprotokolle (ISO Standard Jahr 1984)
- ✓ **IANA** : Internet Assigned Numbers Authority:
 - Zuständig für die weltweite Zuordnung von Namen und IP-Adressen
- ✓ **RIPE**: Réseaux IP Européens:
 - Zuständig für Die IP-Adressen in Europa, Naher Osten, Zentralasien

Symbole

Bei den Symbolen für Netzwerkdigramme gibt es eigentlich keinen definierten Standard. Die Icons von Cisco sind jedoch global anerkannt und werden also De-Facto Standard akzeptiert. Ausserdem werden sie kostenlos angeboten und sind häufig in Diagrammtools integriert (z.B. [draw.io](#)).

Hier eine Auswahl der wichtigsten Symbole:

Symbol	Symbol	Symbol	Symbol
Repeater	Hub	Wireless Bridge	WLAN Controller



Symbol	Symbol	Symbol	Symbol
Access Point	Modem	Switch	Layer 3 Switch
			
Router	WLAN Router	Firewall	Pix Firewall
			
VPN-Gateway	IP-Telefon	Server	PC
			

Schichtenmodelle

Das Schichtenmodell ist ein häufig angewandtes Strukturierungsprinzip für die Architektur von Softwaresystemen. Dabei werden einzelne Aspekte des Softwaresystems konzeptionell einer Schicht (engl. tier oder layer) zugeordnet. Die erlaubten Abhängigkeitsbeziehungen zwischen den Aspekten werden bei einer Schichtenarchitektur dahingehend eingeschränkt, dass Aspekte einer höheren Schicht nur solche tieferer Schichten verwenden dürfen.

Dies bringt einige Vorteile mit sich:

- ✓ **Strukturierung:** Einteilung in kleine Schubladen, was der Übersichtlichkeit dient
- ✓ **Einheitlicher Sprachgebrauch:** Vereinfacht Kommunikation zwischen Netzwerkspezialisten
- ✓ **Flexibilität:** Protokolle einer Schicht können geändert werden ohne die anderen zu beeinflussen
- ✓ **Spezialisierung:** Protokolle können unabhängig voneinander entwickelt werden
- ✓ **Wahlfreiheit:** Entwickler können massgeschneiderte Lösungen zusammenstellen

OSI-Modell

Das OSI-Modell (Open System Interconnection) ist eines der verbreitetsten Schichtenmodelle in der Netzwerktechnik. Es handelt sich um ein Referenzmodell, d.h. in der Praxis wird dieses nicht wirklich umgesetzt

 **Schicht 1: Bitübertragungsschicht / Physical Layer** 

Massnahmen und Verfahren zur Übertragung von Bitfolgen

Die Bitübertragungsschicht definiert die elektrische, mechanische und funktionale Eigenschaften der Übertragungsmedien.

Zugehörige Begriffe/Geräte:

- ✓ Kabel: Twisted Pair, Koaxial, Glasfaser
- ✓ Stecker: RJ45, BNC-Stecker
- ✓ Geräte: Repeater, Hub
- ✓ Bandbreite, Strom, Spannung

Schicht 2: Sicherungsschicht / Data Link Layer



Logische Verbindungen mit Frames und elementare Fehlererkennungsmechanismen

Aufbau der Frames. 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.

Zugehörige Begriffe/Geräte/Protokolle:

- LAN-Protokolle: Ethernet, Token-Ring
- WLAN-Protokolle
- Geräte: Switch, Bridge, Netzwerkkarte
- MAC-Adresse, Prüfsummen

Schicht 3: Vermittlungsschicht / Network Layer



Routing und Datenflusskontrolle, Verbindungen über mehrere Netzwerke

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.

Zugehörige Begriffe/Geräte/Protokolle:

- Protokolle: IP, IPv6
- Netzwerkanteil, Hostanteil, Netzmaske, Subnetze
- Router, Routing-Tabelle

Schicht 4: Transportschicht / Transport Layer



Garantiert die Lieferung der Datenpakete in der richtigen Reihenfolge

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

Zugehörige Begriffe/Geräte/Protokolle:

- Protokolle: TCP, UDP, SPX
- Port, Portnummer
- Sequence Number, Acknowledge Number

Schicht 5: Kommunikationsschicht / Session Layer



Regelt die Eröffnung einer Kommunikationssitzung sowie deren geordnete Durchführung und Beendigung

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

Zugehörige Begriffe/Geräte/Protokolle:

- Sessionmanagement
- NETBIOS, RPC

Schicht 6: Darstellungsschicht / Presentation Layer



Ausgabe von Daten in Standardformate, legt Formate, Komprimierung und Verschlüsselung fest

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

Zugehörige Begriffe/Geräte/Protokolle:

- ASCII, UTF, ZIP, TLS



Schicht 7: Anwendungsschicht / Application Layer



Dienste, Anwendungen und Netzmanagement, Schnittstelle zur End-Applikation

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.

Zugehörige Begriffe/Geräte/Protokolle

✓ Protokolle: HTTP, FTP, SMTP, ...

Quellen: D.Aversa und J.Meier (2014), Modul 129, LAN-Komponenten in Betrieb nehmen, Compendio Bildungsmedien AG, Zürich

Die Nutzdaten einer unteren Schicht sind gemäss dem [Aufbau von Datenpaketen](#) jeweils aufgeteilt in Header und Nutzdaten der nächsten Schicht.

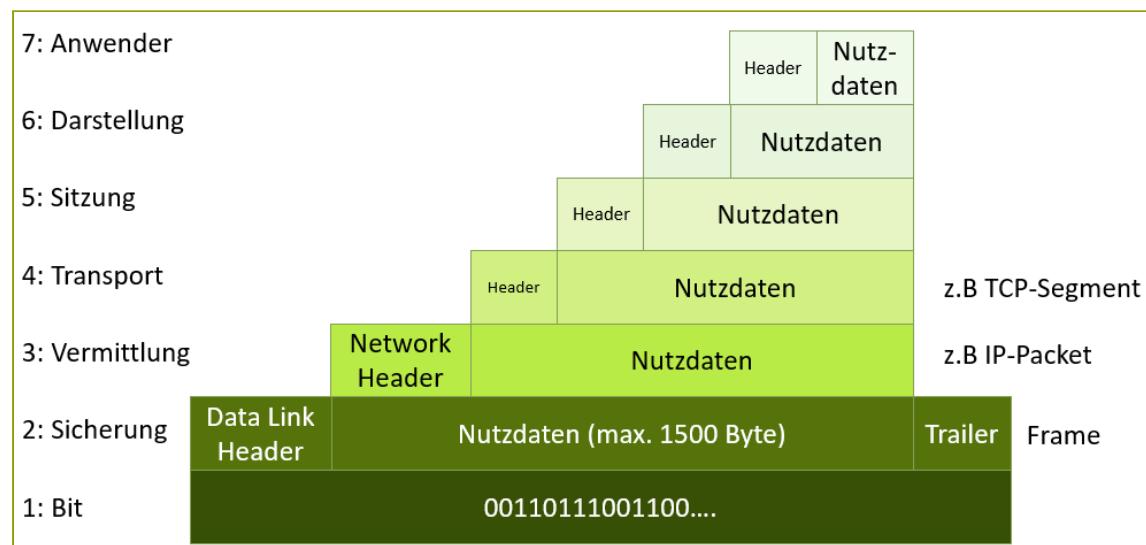


Abb. 1: Das OSI-Modell und seine Daten

Schiebt man den vertikalen Aufbau der Schichten zusammen ergibt sich damit folgendes Bild für den Aufbau eines Frames

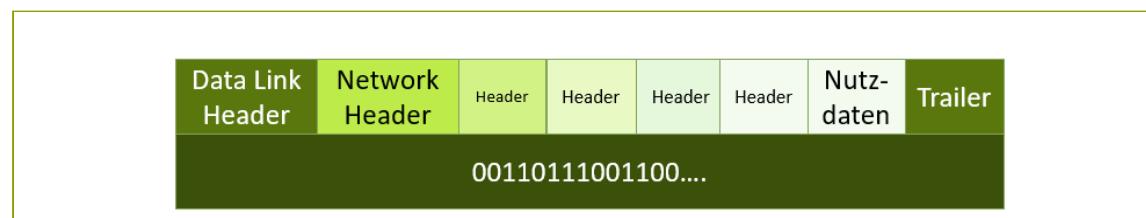


Abb. 2: Ein Frame im OSI-Modell

TCP/IP-Modell

Das OSI-Modell wurde erst einige Jahre nach dem TCP/IP-Schichtenmodell entwickelt. Das OSI-Modell ist feiner gegliedert und flexibler, jedoch wird in der Praxis das TCP/IP-Modell verwendet. In diesem Modell sind die IP-Protokolle und TCP-Protokolle fest verankert und lassen sich kaum ersetzen. Die Schichten 5-7 und 1-2 werden in diesem Modell zusammengefasst

OSI-Schicht	Schichtname englisch	Schichtname deutsch	Einordnung	TCP/IP-Schicht	Protokollbeispiele
7	Application	Anwendung	Anwendungsorientiert	Application	HTTP FTP HTTPS NCP
6	Presentation	Darstellung			
5	Session	Sitzung			
4	Transport	Transport	Transportorientiert	Transport oder Host to Host	TCP, UDP SPX
3	Network	Vermittlung		Internet	IP IPv6 IPX
2	Data Link	Sicherung			Ethernet Token Ring FDDI ARCNET
1	Physical	BitÜbertragung			

Abb. 3: Das TCP/IP-Modell

Ein Datenframe im TCP/IP-Modell lässt sich somit folgendermassen darstellen:

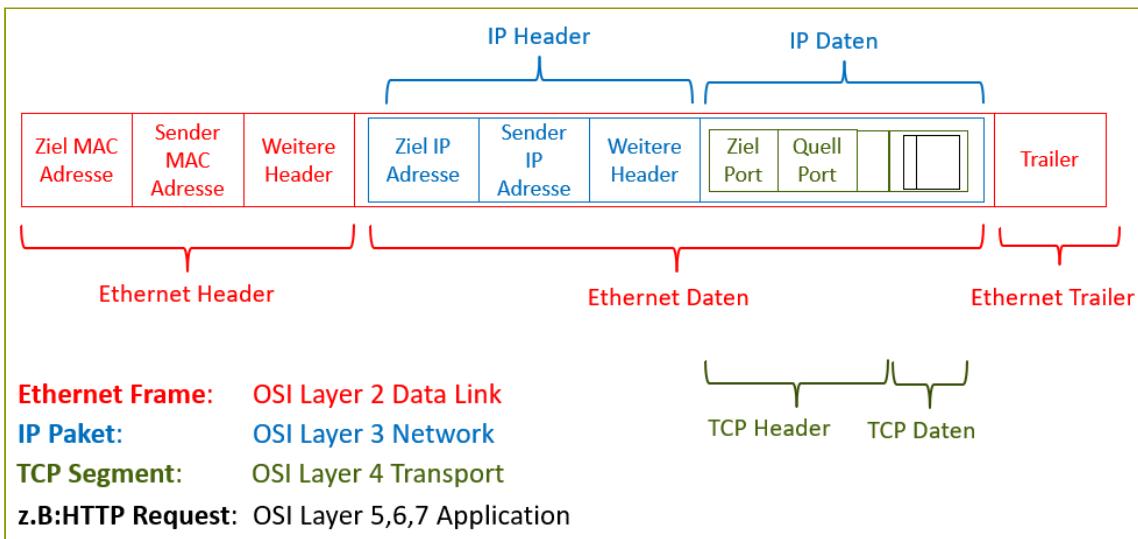


Abb. 4: Ein Frame im TCP/IP Modell

Man kann sich das so vorstellen, wie ineinander gesteckte Couverts:

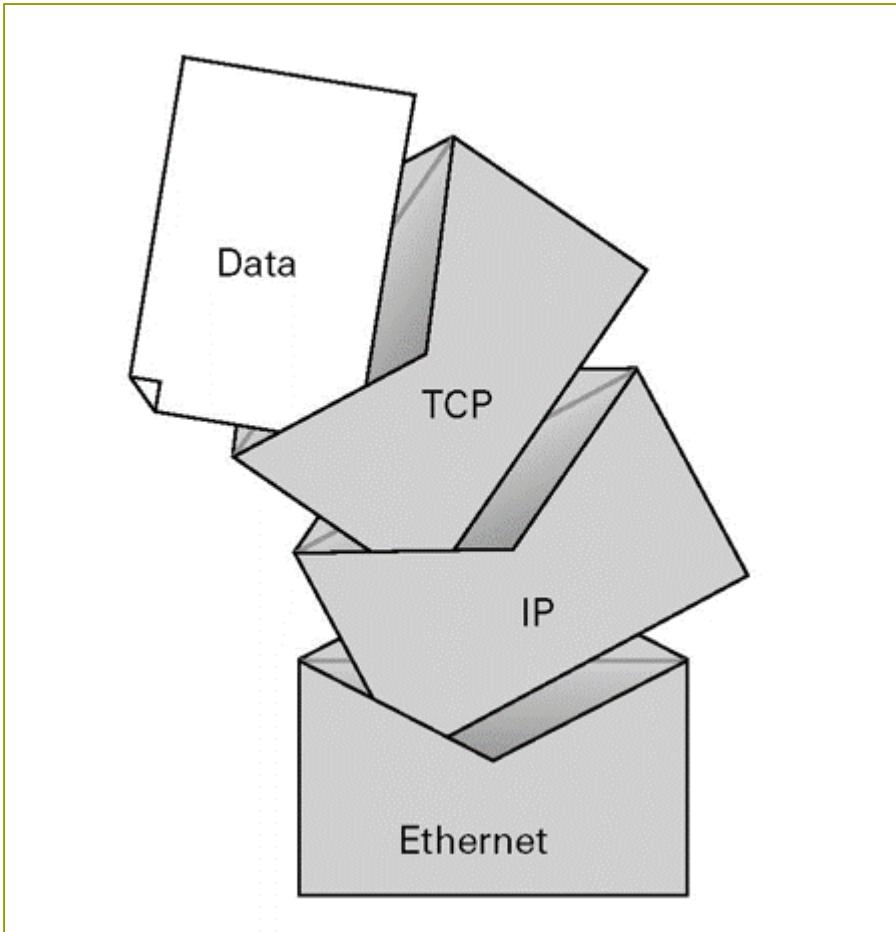


Abb. 4: Datenpakete im TCP/IP-Modell

Protokollstacks

Mehrere Protokolle auf den verschiedenen Schichten die zusammen eine Kommunikation ermöglichen, werden als Protokollfamilie (engl. Protokollstack) bezeichnet.

Beispiele:

- ✓ TCP/IP-Protokollstack: Ethernet - IP - TCP/UDP - Anwendungsprotokoll (z.B HTTP)
- ✓ Novell-Protokollstack: Ethernet - IPX - SPX - NCP: Bis vor einigen Jahren Standard für Novell-Dateiserver
- ✓ Appletalk-Protokollstack. Wurde für die Verneutzung von Apple-Rechnern verwendet, heute kommt jedoch auch der TCP/IP-Protokollstack zum Zug
- ✓ Microsoft-Protokollstack: NETBEUI für MS-Fileserver, ebenfalls nicht mehr im Einsatz

In der Praxis wird nur noch der TCP/IP-Protokollstack eingesetzt.

Ethernet

Die Ethernet Technologie umfasst Festlegungen für Kabeltypen und Stecker sowie für Übertragungsformen (Signale auf der Bitübertragungsschicht, Paketformate). Sie wird also ausschliesslich für kabelgebundene Verbindungen verwendet. Im OSI-Modell ist mit Ethernet sowohl die physische Schicht (OSI Layer 1) als auch die Data-Link-Schicht (OSI Layer 2) festgelegt. Ethernet ist in der [IEEE-Norm 802.3](#) spezifiziert. Es wurde ab den 1990ern zur meistverwendeten LAN-Technik und hat andere LAN-Standards wie Token Ring verdrängt.

Topologien

Ethernet lässt sich in verschiedenen Topologien realisieren. Eine Topologie beschreibt die spezifische Anordnung der Geräte und Leitungen, die ein Rechnernetz bilden, über das die Computer untereinander verbunden sind und Daten austauschen. In grossen Netzen findet man oftmals eine Struktur, die sich aus mehreren verschiedenen Topologien zusammensetzt. Die Topologie eines Netzes ist entscheidend für seine Ausfallsicherheit: Nur wenn alternative Wege zwischen den Knoten existieren, bleibt bei Ausfällen einzelner Verbindungen die Funktionsfähigkeit erhalten.

Die Kenntnis der Topologie eines Netzes ist außerdem nützlich zur Bewertung seiner Performance sowie notwendig für eine Investitionsplanung und für die Auswahl geeigneter Hardware.

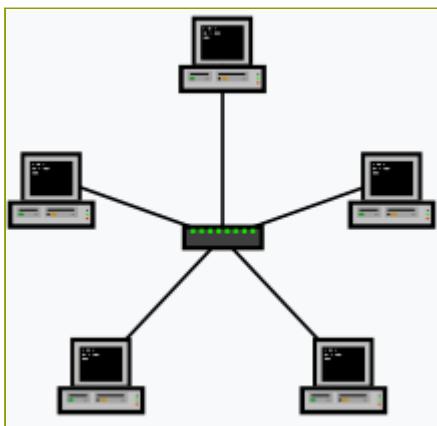


Abb. 1: Sterntopologie

Bei Netzen in Stern-Topologie sind an einen zentralen Teilnehmer alle anderen Teilnehmer mit einer Punkt-zu-Punkt-Verbindung angeschlossen. In Computernetzen kann es eine spezialisierte Einrichtung sein, zum Beispiel ein Switch

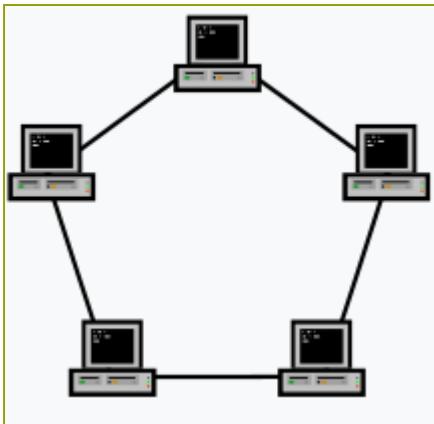


Abb. 2: Ringtopologie

Bei der Vernetzung in Ring-Topologie werden jeweils zwei Teilnehmer über Zweipunktverbindungen miteinander verbunden, so dass ein geschlossener Ring entsteht. Die zu übertragende Information wird von Teilnehmer zu Teilnehmer weitergeleitet, bis sie ihren Bestimmungsort erreicht. Da jeder Teilnehmer gleichzeitig als Repeater wirken kann, also das Signal wieder verstärkt/auffrischt, können auf diese Art große Entfernung überbrückt werden

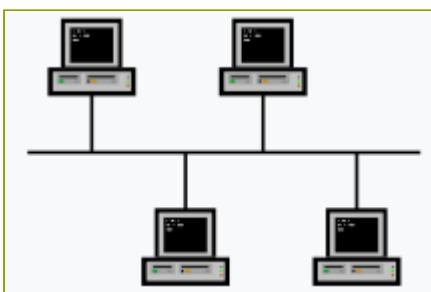


Abb. 3: Bustopologie

Bei einer Bus-Topologie sind alle Geräte direkt mit demselben Übertragungsmedium, dem Bus verbunden. Es gibt keine aktiven Komponenten zwischen den Geräten und dem Medium. Beispiele für ein Netzwerk mit Bus-Topologie sind die Koaxial-Varianten von 10 Mbit/s Ethernet und WLAN.



Abb. 4: Vermischte Topologie

In einem vermaschten Netz ist jedes Endgerät mit einem oder mehreren anderen Endgeräten verbunden. Wenn jeder Teilnehmer mit jedem anderen Teilnehmer verbunden ist, spricht man

von einem vollständig vermaschten Netz.

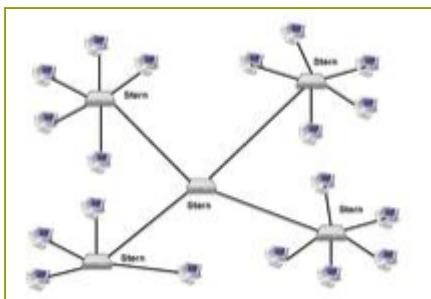


Abb. 5: Erweiterte Sterntopologie

Eine Sterntopologie ist in der Praxis immer als erweiterte Sterntopologie oder als Stern-Stern-Topologie ausgelegt. In einer solchen Struktur ist nicht nur ein Sternpunkt vorhanden; am Ende der Kabel eines Sternpunkts befinden sich wiederum Sternpunkte, wobei auch mehr als zwei Verzweigungsstufen vorhanden sein können.

Hier eine Zusammenstellung der Vor- und Nachteile:

Topologie	Vorteile	Nachteile
Bustopologie	<ul style="list-style-type: none"> - Geringe Kosten - geringe Kabelmengen - Einfache Verkabelung und Netzerweiterung - keine aktiven Netzwerkkomponenten notwendig 	<ul style="list-style-type: none"> - Datenübertragungen können leicht abgehört werden - bei Kabelbruch fällt Netz aus - Es kann zu jedem Zeitpunkt immer nur eine Station Daten senden
Ringtopologie	<ul style="list-style-type: none"> - verteilte Steuerung - grosse Netzausdehnung 	<ul style="list-style-type: none"> - aufwendige Fehlersuche bei Störungen Netzausfall - Datenübertragungen können leicht abgehört werden
Sterntopologie	<ul style="list-style-type: none"> - Ausfall eines Endgerätes hat keine Auswirkung auf den Rest des Netzes - einfache Erweiterung - Leichte Fehlersuche 	<ul style="list-style-type: none"> - hoher Verkabelungsaufwand - Netzausfall bei Ausfall oder Überlastung des Hubs/Switch
Vermaschte Topologie	<ul style="list-style-type: none"> - Sehr leistungsfähig - hohe Ausfallsicherheit 	<ul style="list-style-type: none"> - aufwendige Administration - teure und hochwertige Vernetzung

Heutzutage werden im LAN nur noch Stern- bzw. erweiterte Sterntopologien eingesetzt

Zugriffsverfahren

Der englische Begriff Carrier Sense Multiple Access/Collision Detection (CSMA/CD) bezeichnet ein Protokoll, das den Zugriff verschiedener Stationen auf ein gemeinsames Übertragungsmedium regelt

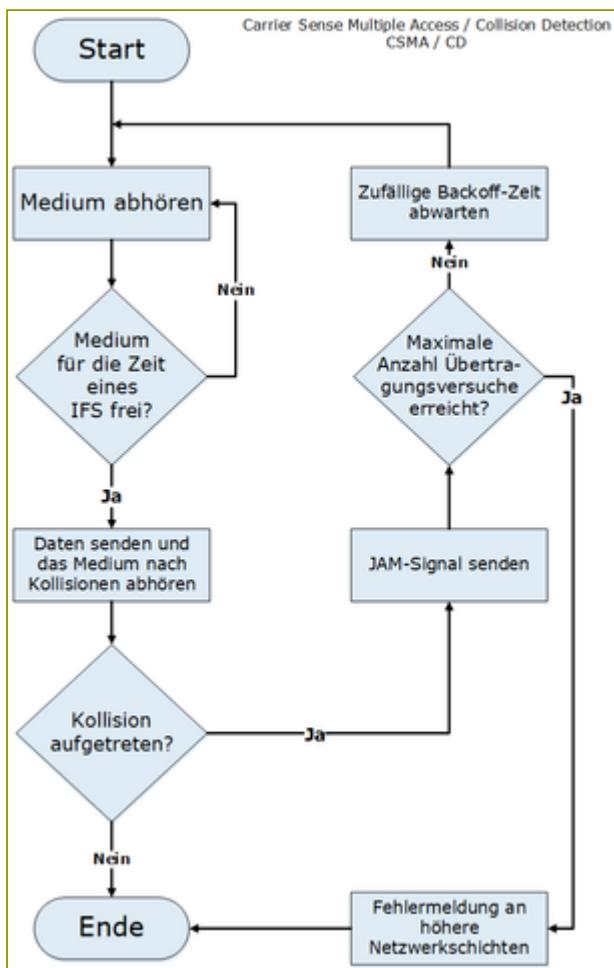


Abb. 6: Das TCP/IP-Modell (Bildquelle: Von Heimdall 793 - Eigenes Werk, CC BY-SA 4.0)

Die Stelle, die Daten senden möchte, lauscht also auf dem Medium (Carrier Sense), ob es bereits belegt ist und sendet erst, wenn die Leitung frei ist. Da zwei Stellen gleichzeitig zu senden anfangen können, kann es trotzdem zu Kollisionen kommen, die dann festgestellt werden (Collision Detection), woraufhin beide Stellen noch kurz ein "Störung-Erkannt"-Signalmuster erzeugen, dann mit dem Senden aufhören und eine zufällige Zeit warten, bis sie einen erneuten Sendeversuch starten.

In der Praxis funktioniert dieser Algorithmus bildlich wie eine Diskussionsrunde ohne Moderator, auf der alle Gäste ein gemeinsames Medium (die Luft) benutzen, um miteinander zu sprechen. Bevor sie zu sprechen beginnen, warten sie höflich darauf, dass

der andere Gast zu reden aufgehört hat. Wenn zwei Gäste zur gleichen Zeit zu sprechen beginnen, stoppen beide und warten für eine kurze, zufällige Zeitspanne, bevor sie einen neuen Anlauf wagen.

Auch wenn die Norm IEEE 802.3 den Namen "CSMA/CD" im Titel hat, spielt die Kollisionsauflösung heute nur mehr in geringem Masse eine Rolle. Die meisten Netzwerke werden heute im Vollduplexmodus betrieben, bei dem Teilnehmer (Router, Switches, Endgeräte etc.) mittels Punkt-zu-Punkt-Verbindung die Sende- und Empfangsrichtung unabhängig voneinander nutzen können und somit keine Kollisionen mehr entstehen. Trotzdem blieb das Frame-Format, insbesondere der Frame-Header und die für die Kollisionserkennung vorgeschriebene minimale Frame-Länge, bis hinauf zu 400-Gbit/s-Ethernet, unverändert

Verkabelung

Koaxial-Kabel

Bei einer **VollDuplex** Kommunikation können beide Teilnehmer gleichzeitig senden und empfangen. Die ist vergleichbar mit dem Telefon, bei dem beide Gesprächsteilnehmer gleichzeitig sprechen und hören können. Bei **Halbduplex** funktioniert die Kommunikation jeweils nur in eine Richtung, dh. entweder Senden oder Empfangen, dies lässt sich z.B mit einem Funkgerät vergleichen. Ältere Koaxialkabel verfügen nur über eine Adernpaar (der Innenleiter und die Ummantelung), somit ist bei diesem Kabeltypen nur eine Halbduplexkommunikation möglich. Ethernet-Varianten mit Twisted-Pair-Kabeln verfügen mindestens über zwei Adernpaare, somit ist bei diesen eine Vollduplex Kommunikation möglich.

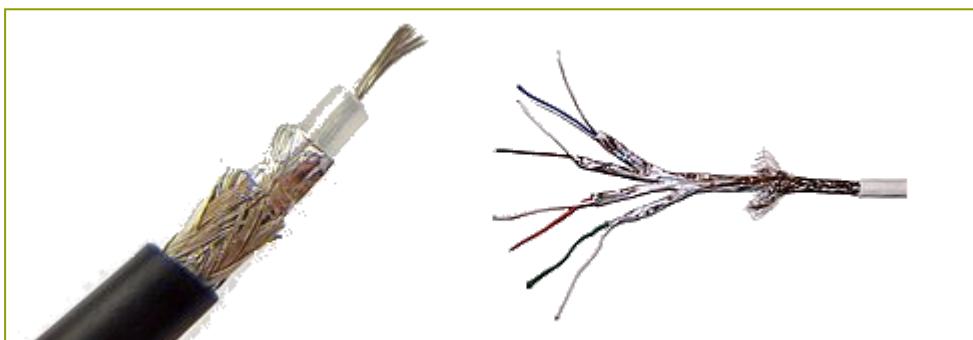


Abb. 7: Koaxial-Kabel und Twisted-Pair-Kabel

Koaxial-Kabel spielen heutzutage in der Hochfrequenztechnik (Rundfunk, Fernseher) noch eine Rolle. Seit den 1990-er Jahren wurde ihr Einsatz in Netzwerken durch Twisted-Pair-Kabel abgelöst.

Twisted-Pair-Kabel

Bei diesem Kabeltyp, der vor allem im LAN zum Einsatz kommt, werden je 2 (oder 4) Adernpaare miteinander verdrillt (engl. twisted), wobei die Verdrillung bei den einzelnen Paaren unterschiedlich gross ist. Verdrillte Adernpaare bieten gegenüber parallel geführten Adern einen besseren Schutz gegenüber elektrischen und magnetischen Störfeldern. Zusätzlich können die Adernpaare einzeln und/oder in der Gesamtheit durch Drahtgeflechte oder Aluminiumfolie geschirmt werden, um Störsignale zu minimieren.

Die Nomenklatur der TP-Typen ist in ISO/IEC 11801 geregelt. Folgendes Bezeichnungsschema der Form **XX/YZZ** ist darin definiert:

- ✓ **XX** steht für die Gesamtschirmung
- ✓ U = ungeschirmt
- ✓ F = Folienschirm
- ✓ S = Geflechtsschirm (engl. screened)

- ✓ SF = Geflechts- und Folienschirm
- ✓ Y steht für die Adernpaarschrimung

 - ✓ U = ungeschirmt
 - ✓ F = Folienschirm
 - ✓ S = Geflechtsschirm

- ✓ ZZ steht für
 - ✓ TP = Twisted Pair
 - ✓ QP = Quad Pair



Abb. 8: U/UTP, U/STP, S/UTP und S/FTP Kabel

Die folgende Tabelle zeigt eine Übersicht der TP-Typen

Übersicht der Schirmungsarten								
Twisted-Pair-Kabel (TP)		U/UTP	S/UTP	U/FTP	S/FTP	S/STP	F/FTP	SF/FTP
Gesamtschirm	Drahtgeflecht (S)		X		X	X		X
	Folie (F)						X	X
Aderpaarschirm	Drahtgeflecht (S)					X		
	Folie (F)			X	X		X	X

Abb. 9: TP-Typen und die Schirmung

Die Schirmung (zusammen mit den Stecker) bestimmt die Leistungsfähigkeit einer Übertragung. Diese wird in ISO/IEC 11801 in Kategorien eingeteilt.

Kategorie	Typ	Datenrate (Mbit/s)	Bandbreite
Cat 5	U/UTP	100	100 MHz
Cat 5e	U/UTP, F/UTP, U/FTP	1'000	100 MHz
Cat 6	U/UTP, F/UTP, U/FTP	1'000	250 MHz
Cat 6a	U/UTP, F/UTP, U/FTP, S/FTP	1'000	500 MHz
Cat 7	S/FTP, F/FTP	10'000	600 MHz

Kategorie	Typ	Datenrate (Mbit/s)	Bandbreite
Cat 7a	S/FTP, F/FTP	10'000	1 GHz
Cat 8.1	F/UTP, U/FTP	40'000	2 GHz
Cat 8.2	S/FTP, F/FTP	40'000	2 GHz

Kategorien unter 5 werden in der Netzwerktechnik nicht verwendet

Glasfaserkabel

Für schnelle Datenübertragungen werden Glasfaserkabel eingesetzt. Bei dieser Technologie werden elektrische Spannungen in Licht umgewandelt und entlang der Glasfaser übertragen. Die Lichtsignale brechen und reflektieren sich am Mantel der Glasfaser. Als Sender und Empfänger dienen Laserdioden. Je häufiger sich die einzelnen Lichtstrahlen am Mantel brechen, desto "verwaschener" wird das Ausgangssignal im Vergleich zum Eingangssignal, da die einzelnen Lichtstrahlen unterschiedlich lange Laufstrecken zurücklegen.

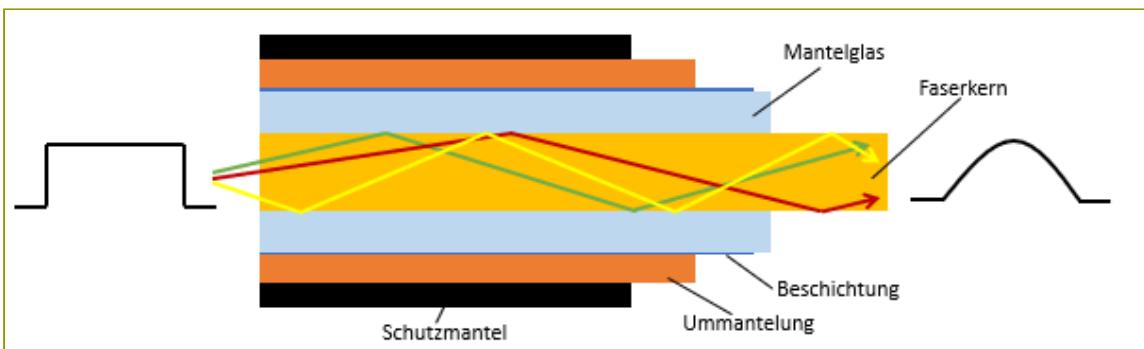


Abb. 10: Multimode Glasfaser

Dies bedeutet, dass je kleiner der eigentliche Faserkern ist, desto besser und weiter können Signale übertragen werden. Dies unterscheidet **Singlemode** Glasfaser von der **Multimode** Glasfaser

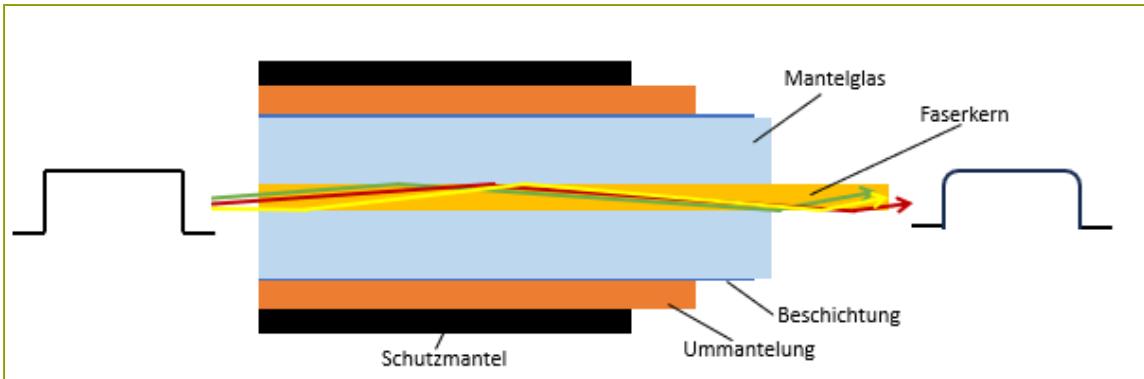


Abb. 11: Singlemode Glasfaser

Die folgende Tabelle stellt die gebräuchliche Typen zusammen:

Typ	Durchmesser Faserkern	Bandbreite	Kosten	Anwendung
Multimode mit Stufenprofil	100-400 µm	100 Mhz	tiefe	Entfernung unter 1 km, wenig verbreitet
Multimode mit Gradientenprofil	50 µm	1 Ghz	mittel	LAN-Backbone
Singelmode mit Stufenprofil	9 µm	100 Ghz	hoch	LAN-Backbone, Telefongesellschaften

Stufen- und Gradientenprofil unterscheiden sich in ihrem Reflexionsverhalten der Lichtstrahlen.

Zusammenfassen die Vor- und Nachteile:

Vorteile Multimode	Nachteile Multimode
<ul style="list-style-type: none"> - geringerer Aufwand in der Herstellung der Glasfasern - einfache Verbindungstechnik aufgrund des größeren Kerndurchmessers - Fasern mit Stufenindex- und Gradientenindexprofil verfügbar 	<ul style="list-style-type: none"> - grösere Signaldämpfung und Laufzeitverschiebung - geringere maximale Bandbreiten - kürzere Distanzen überbrückbar - Verstärker oder Signalaufbereiter bei größeren Distanzen notwendig

Vorteile Singlemode	Nachteile Singlemode
<ul style="list-style-type: none"> - geringe Dämpfung des Signals - kaum Laufzeitverschiebungen - grosse Distanzen überbrückbar - hohe Bandbreiten 	<ul style="list-style-type: none"> - teurere Laser zur Einspeisung des Lichts notwendig - grössterer Aufwand bei der Herstellung der Glasfasern aufgrund der sehr kleinen Faserkerne - hohe Präzision beim Verbinden der Glasfasern durch Stecker oder Spleissen notwendig

Ethernet-Frame

Aufbau

Ein Ethernet-Frame stellt auf OSI-Layer 2 die Einheit dar, in der Datenpakete aufgebaut und versendet werden. Die einzelnen Bits eines Datenstroms werden in Frames zusammengefasst und dann als Einheit versendet. Beachten Sie die Sprechweise: **Frames** und nicht etwa Pakete. Ein Ethernet-Frame ist zwischen 64 und 1518 Bytes gross, je nach Menge der zu transportierenden Daten.

Wie bei jedem Protokol besitzt ein Ethernet-Frame einen Header und die eigentliche Nutzlast. Speziell besitzt ein Frame auch noch einen Trailer (Abschluss), welcher eine Prüfsumme enthält.

Präambel	Ziel-MAC	Quell-MAC	Typ	Nutzdaten	FCS
8 Byte	6 Byte	6 Byte	2 Byte	46- 1500 Bytes	4 Byte
101010..	MAC-Adresse	MAC-Adresse	0x80

- ✓ **Präambel:** 8 Bytes lang die Bitfolge 101010.. Diese dient der Synchronisation, der Frame kündigt sich sozusagen an. Diese 8 Bytes werden nicht zur Gesamtgrösse des Frames von 64 bis 1518 Bytes gerechnet.
- ✓ **Ziel-MAC-Adresse:** Empfänger des Frames
- ✓ **Quell-MAC-Adresse:** Absender des Frames
- ✓ **Typ:** Kennzahl für das Protokoll der nächsthöheren OSI-Ebene, Protokoll welches für die Nutzlast verwendet wird
- ✓ **Nutzdaten:** Der eigentliche Dateninhalt des Frames
- ✓ **FCS:** Frame Check Sequence, eine Prüfsumme zur Kontrolle von Übertragungsfehlern.

MAC-Adressen

Bei Ethernet erhalten grundsätzlich alle Stationen die gesendeten Frames. Diese müssen deshalb adressiert werden, damit ein Empfänger weiss, dass der Frame für ihn bestimmt ist. Diese Adressen sind die sogenannten MAC-Adressen (Media Access Control), welche weltweit einmalig ist und in der Netzwerkkarte fix gespeichert ist. Die bestehen aus 6 Bytes die üblicherweise in hexadezimaler Schreibweise dargestellt werden. Die ersten drei Bytes stellen einen Vendor-Code dar, die zweite Hälfte eine eindeutige Zahl innerhalb des Herstellers

00-20-AF-FC-34-2B (00-20-AF = 3COM)

Typ

Das Typfeld legt fest, welches Protokol bei der Nutzlast auf OSI-Ebene 3 verwendet wird.

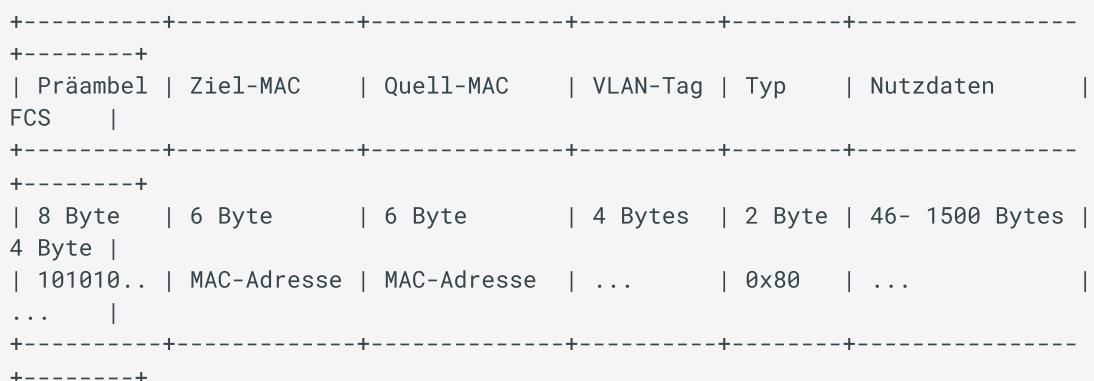
Häufig verwendete Codes sind:

Typ	Protokoll
0x0800	IPv4
0x0806	ARP (Adress Resolution Protocol)
0x86DD	IPv6

Die vollständige Liste findet sich z.B. bei [Wikipedia](#).

VLAN Tag

Bei Verwendung von tagged VLAN wird die Framegrösse um 4 Bytes erweitert (auf max. 1522 Bytes), um das sogenannte VLAN-Tag mitzusenden. Dieses stellt eine ID für ein bestimmtes VLAN dar. Damit kann ein Frame einem bestimmten VLAN zugeordnet werden



Ethernet-Varianten

Übersicht

Es gibt zahlreiche Ethernet-Varianten, die sich durch die Übertragungsmedien (Coaxial-Kabel, Twisted-Pair, Glasfaser) und die Übertragungsgeschwindigkeit unterscheiden. Die folgende Tabelle listet die wichtigsten Varianten auf.

Bezeichnung	Standard	Datenrate	Kabeltechnik	maximale Kabellänge [m]	Erscheinungsjahr
10Base2 Thin Ethernet	802.3a	10 MBit/s	Koaxalkabel	Halbduplex: 185	1990
10Base-T	802.3i	10 MBit/s	Twisted Pair	100	1990
100Base-TX Fast Ethernet	802.3u	100 MBit/s	Twisted Pair	100	1995
100Base-FX Fast Ethernet	802.3u	100 MBit/s	Glasfaser	2000	1995
1000Base- LX Gigabit- Ethernet	802.3z	1 GBit/s	Glasfaser	Multimode: 550 Singlemode: 5000	2002
1000Base- TX Gigabit- Ethernet	802.3ab	1 GBit/s	Twisted Pair	100	2002
10GBase SR Short Reach	802.3ae	10 GBit/s	Glasfaser	400	2002

Bezeichnung	Standard	Datenrate	Kabeltechnik	maximale Kabellänge [m]	Erscheinu
10GBase LR Long Reach	802.3ae	10 GBit/s	Glasfaser	10'000	
10GBase ER Extended Reach	802.3ae	10 GBit/s	Glasfaser	40'000	
10GBase CR	-	10 GBit/s	Koaxialkabel	15	
10GBase T	802.3an	10 GBit/s	Twisted Pair	100	
40GBase T	802.3ba	40 GBit/s	Twisted Pair	30	
40GBase SR4	802.3ba	40 GBit/s	Glasfaser	100	
100GBase LR4	802.3ba	100 GBit/s	Glasfaser	10'000	
200GBase-LR4	802.3cn	200 GBit/s	Glasfaser	10'000	
400GBase-LR8	802.3bs	400 GBit/s	Glasfaser	10'000	
800GBase	802.3df	800 GBit/s	Glasfaser	?	ev

Nomenklatur

Die Nomenklatur der Bezeichnung lässt sich so darstellen:

100Base TX

Medium:

T = Twisted Pair

F = Glasfaser

S = Glasfaser short (kurze Wellenlänge) über Multimode-Faser

L = Glasfaser long (lange Wellenlänge) über Singlemode-Faser

E = Glasfaser extended über Singlemode-Faser (bis 40 km)

C = Copper (Koaxialkabel)

Nutzbare Geschwindigkeit:

10Mbit/s, 100Mbit/s, 1000Mbit/s, 10Gbit/s, ...

Base=Basisband
(Art der Datenübertragung)

Abb. 1: Nomenklatur der Ethernet Varianten

Repeater / Hub

Sowohl Repeater als auch Hubs arbeiten auf Layer 1 des OSI-Modells

Repeater

Ein Repeater ist nicht anderes als ein Signalverstärker um Streckenbegrenzungen einer Ethernet-Variante zu umgehen. Er empfängt Signale bereitet sie auf und leitet sie weiter. Im einfachsten Fall hat ein Repeater zwei Ports, die wechselweise als Ein- und Ausgang funktionieren. Der Repeater übernimmt keinerlei regulierende Funktion in einem Netzwerk. Er kann nur Signale empfangen und weiterleiten. Für angeschlossene Geräte ist nicht erkennbar, ob sie an einem Repeater angeschlossen sind. Er verhält sich völlig transparent.

Hub

Ein Hub ist ein Kopplungselement, das mehrere Hosts in einem Netzwerk miteinander verbindet. In einem Ethernet-Netzwerk, das auf der Stern-Topologie basiert dient ein Hub als Verteiler für die Datenpakete. Ein Hub ist somit eigentlich nichts anderes wie ein Multiport Repeater. Die Ethernet-Frames werden an alle Ausgänge weitergeleitet. Logisch gesehen entspricht dies einer Bustopologie mit den gleichen Nachteilen einer Bustopologie, also leichte Abhörbarkeit und beschränkte Bandbreite, da zu jedem Zeitpunkt nur eine Station senden kann (mit CSMA/CD). Die verfügbare Bandbreite teilt sich also durch die Anzahl der angeschlossenen Geräte.

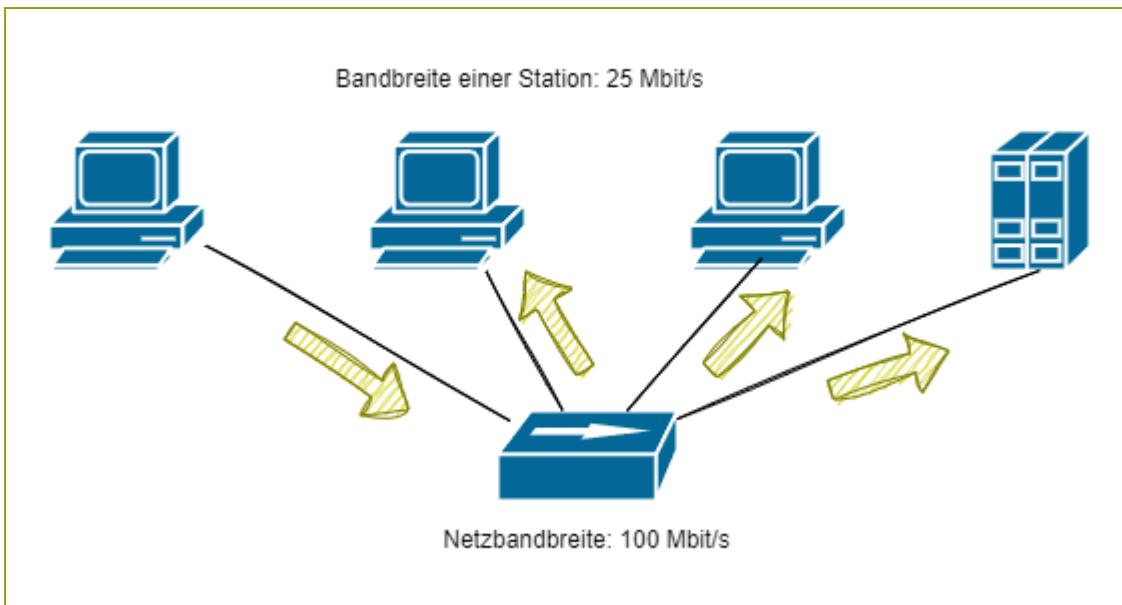


Abb. 1: Hub

Hubs wurden in den letzten Jahren mehr oder weniger vollständig durch Switches ersetzt, da diese bei gleichem Preis (wenn solche überhaupt noch erhältlich sind) bessere Leistungen erbringen.

WLAN Repeater

Eine gewisse Bedeutung haben WLAN Repeater, welche das Funksignal aufbereiten und weiterleiten und somit eine grössere Reichweite für ein WLAN ermöglichen.



Abb. 1: WLAN-Repeater

Switch

Ein Switch arbeiten auf OSI-Layer 2, d.h. er wertet die MAC-Adressen der Ethernet-Frames aus.

Switching Ports

Die Ports eines Switches haben **keine** IP-Adresse, sie arbeiten auf Layer 2

Unterschied zum Hub

Zunächst funktioniert auch ein Switch wie der Hub als Verteiler für Datenpakete. Allerdings sendet er einen Frame nicht an alle seine Ausgänge (Ports), sondern nur an denjenigen Port von dem er auf Grund der Ziel-MAC-Adresse weiss, dass das Zielgerät an diesem angeschlossen ist. Andere am Switch angeschlossenen Geräte erhalten den Frame nicht. Dadurch werden die Nachteile eines Hubs behoben. Der Netzwerkverkehr kann nicht mehr so einfach ausspioniert werden und den einzelnen Stationen steht die volle Bandbreite zur Verfügung (im Uplink natürlich nicht).

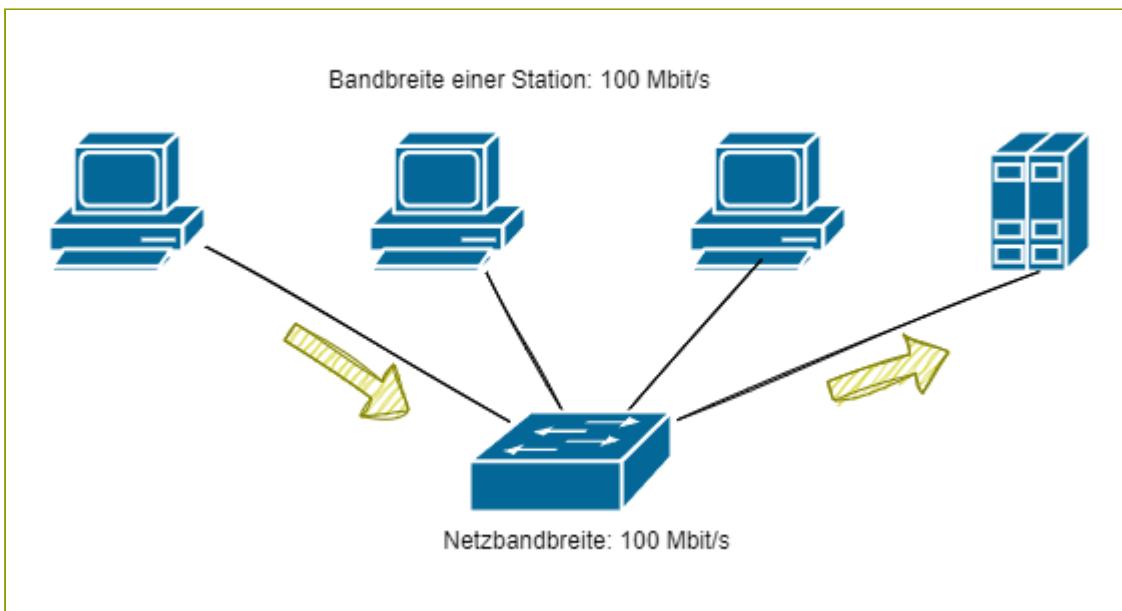


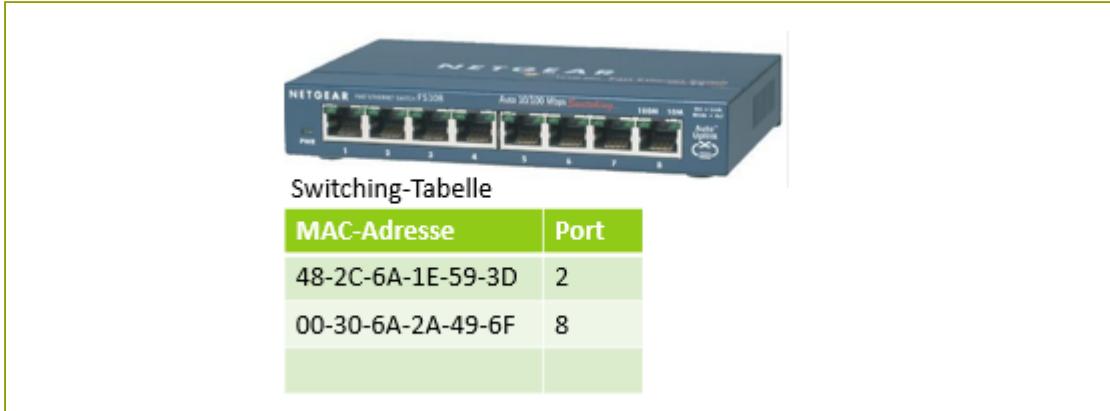
Abb. 1: Switch

Switching Tabelle

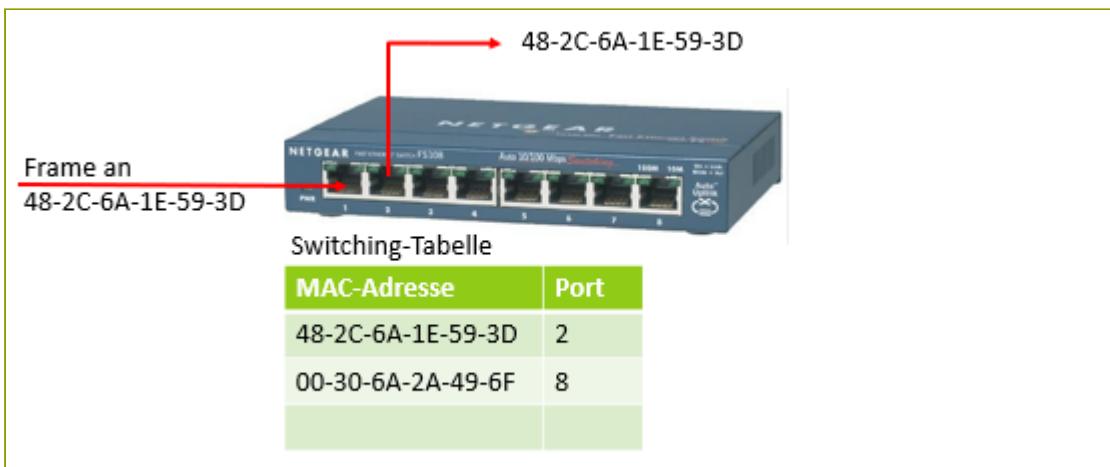
Woher weiss der Switch, an welchen seiner Ports er einen Frame weiterleiten muss? Diese Information speichert der Switch in seiner Switching Tabelle. Die folgende Bildserie beschreibt die Funktionsweise und den Aufbau einer Switching Tabelle.

In diesem Beispiel haben wir einen Switch mit 2 Einträgen in seiner Switching Tabelle.

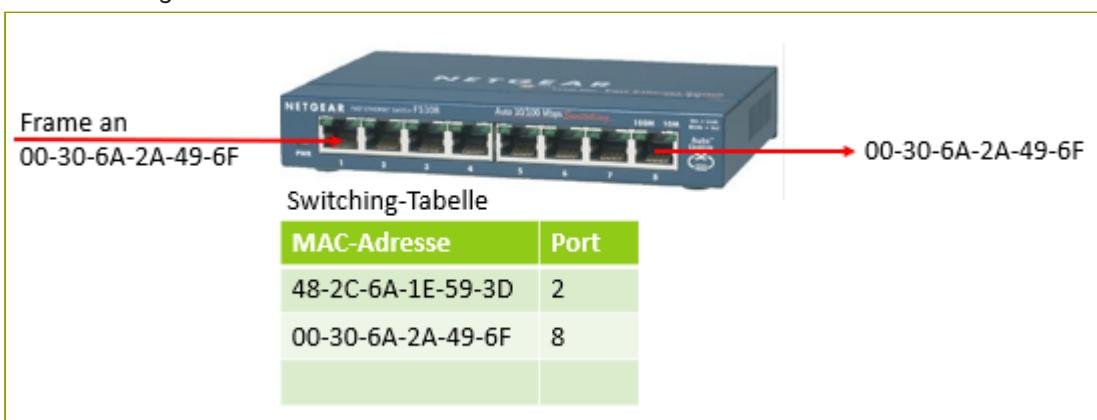
In dieser ist einer MAC-Adresse ein Ausgangsport zugeordnet.



Erhält der Switch einen Frame an Port 1 für 48-2C-6A-1E-59-3D wird dieser gemäss Switching Tabelle an Port 2 weitergeleitet.



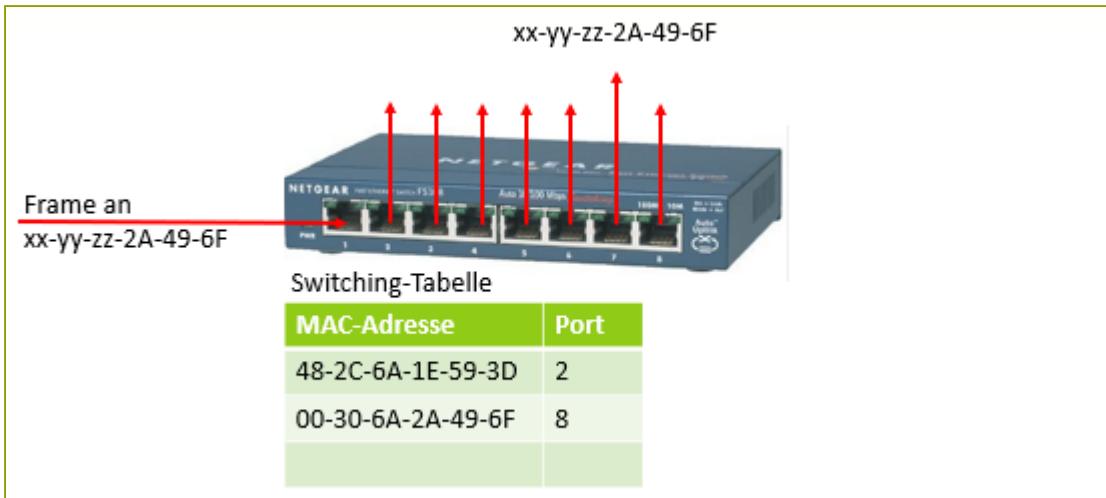
Erhält der Switch einen Frame für 00-30-6A-2A-49-6F wird dieser gemäss Switching Tabelle an Port 8 weitergeleitet.



Erhält der Switch einen Frame, der nicht in seiner Switching Tabelle vorhanden ist, wird dieser an alle Ports weitergeleitet.

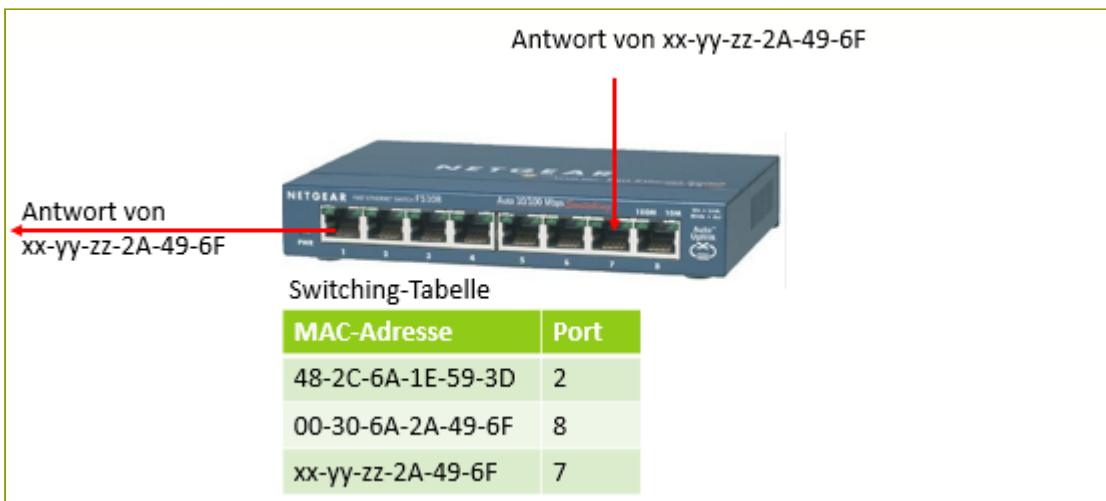
Dies ist ein sogenannter Layer 2 Broadcast (nicht zu verwechseln mit IP Broadcast).

Der Switch funktioniert in diesem Moment gleich wie ein Hub.



Wenn das Gerät xx-yy-zz-2A-49-6F am Switch angeschlossen ist, antwortet dieses auf einem bestimmten Port (im Bild Port 7)

und die Switching Tabelle wird automatisch um den neuen Eintrag erweitert.



STP Protokoll

Zu Redundanzzwecken ist es wünschenswert, dass alternative Pfade zur Verfügung stehen. Fällt eine Verbindung aus, steht eine weitere Verbindung zur Verfügung. Da Switches zu Beginn einer Kommunikation Ethernet-Frames an alle ihre Ports weiterleiten, führt das dazu, dass die Frames in einem Loop anfangen zu kreisen. Es kommt zu einem sogenannten Layer 2 Broadcast Sturm. Ein Frame gelangt von mehreren Seiten zu einem Switch, dieser schickt es an alle Ausgänge weiter und erhält die Frames vervielfältigt zurück. In der Konsequenz bricht der Netzwerkverkehr schlussendlich zusammen. Dies ist vergleichbar mit einer akustischen Rückkopplung bei der ein Mikrofon vor den Lautsprecher gehalten wird.

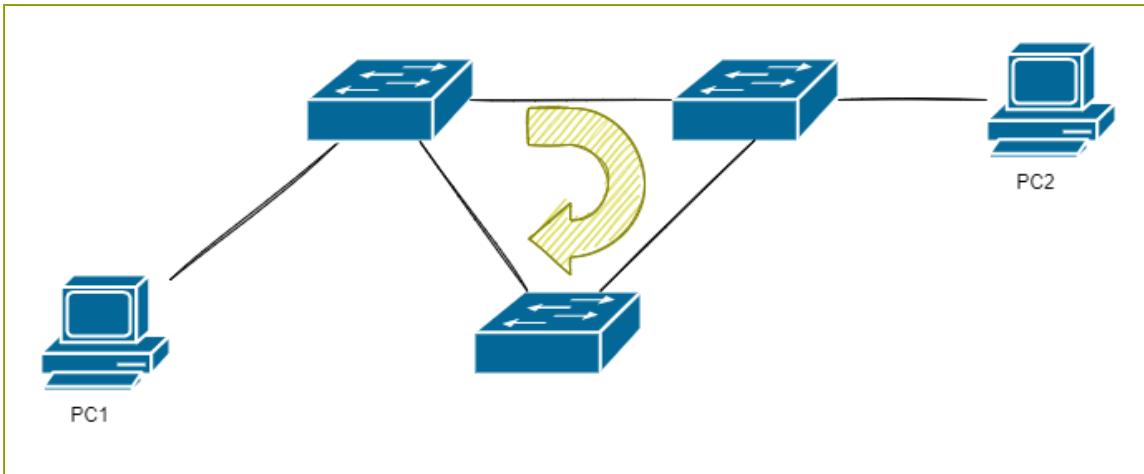


Abb. 3: Redundante Pfade führen zu einem Layer 2 Broadcast Sturm

An dieser Stelle kommt **STP** (Spanning-Tree-Protokoll) zum Zug. Die Switches tauschen mit Hilfe von STP Informationen darüber aus, welche Ports gesperrt sein müssen, bzw. offen sind, um den Broadcast Sturm zu vermeiden. Im nächsten Bild sieht man, dass der Port beim untersten Switch im Normalbetrieb dank STP gesperrt ist (roter Punkt).

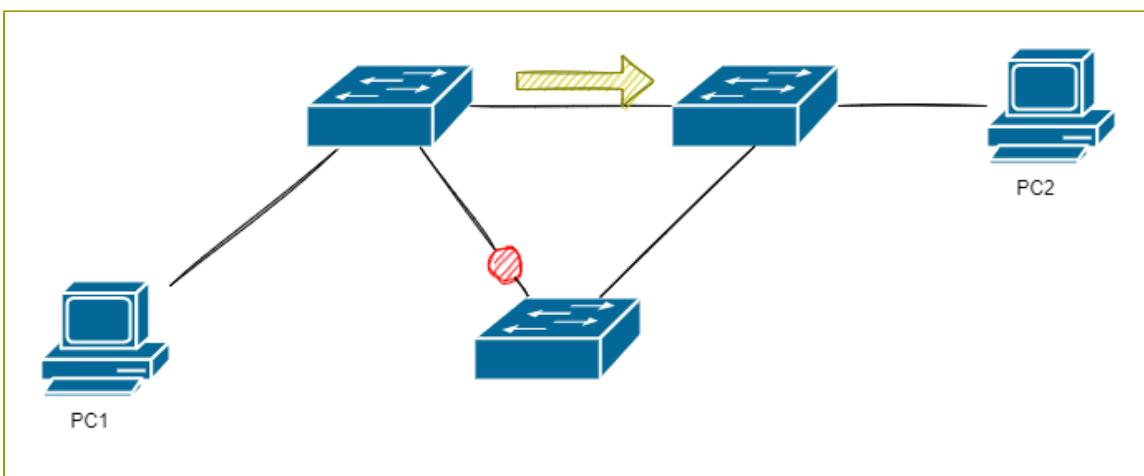


Abb. 4: Der Pfad beim ruten Punkt ist wegen STP gesperrt

Fällt eine Verbindung aus, können die alternativen Pfade wieder aktiviert werden und die Kommunikation läuft ohne Unterbrechung weiter

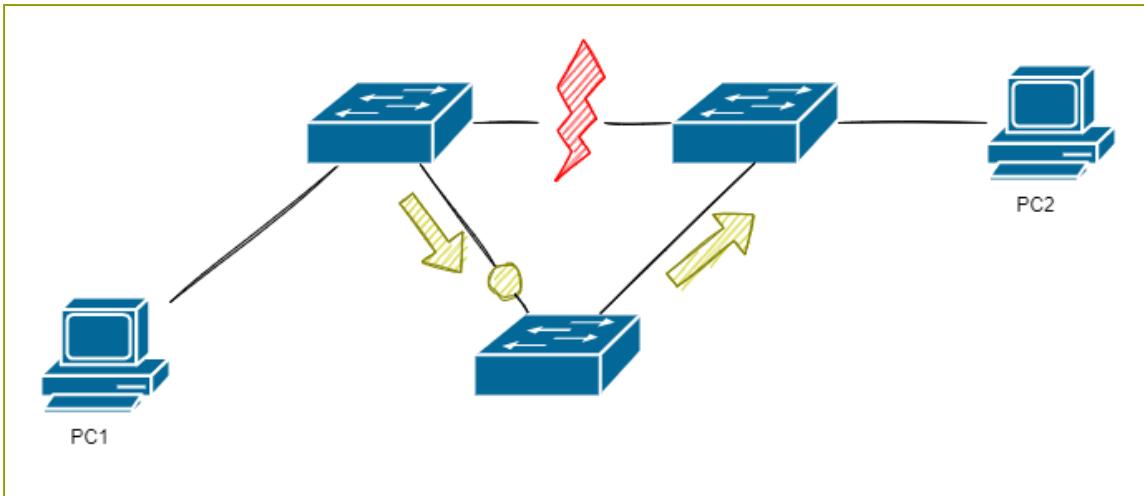


Abb. 5: Bei einem Unterbruch werden gesperrte Ports automatisch wieder aktiviert

STP Erklärvideo

CCNA3 - Part 5 - Spanning Tree Protocol STP

Qualitätsmerkmale

Der Preis von Switches reicht von 50.- bis mehrere 1000 Franken. Dieser Unterschied ergibt sich auf Grund der unterschiedlichen Merkmale verschiedener Switches. Diese sind in der folgenden Tabelle zusammengetragen.

Eigenschaft	Varianten
Anzahl Ports	4, 8, 16, 24, 36 oder 48, spezielle modulare Switches bis 512
Übertragungsgeschwindigkeit	10, 100, 1 000 Mbit/s oder 10 Gbit/s.
Asymmetrisches Switching	Der Datenverkehr in einem LAN ist normalerweise nicht symmetrisch, sondern meist wollen viele Stationen mit dem Server kommunizieren. Zu diesem Zweck verfügen viele Switches über Ports verschiedener Geschwindigkeiten (meist viele 100-Mbit/s- und wenige 1'000-Mbit/s-Ports). Wegen der unterschiedlichen Geschwindigkeiten muss der Switch die Frames zwischenspeichern. Wie viel er zwischenspeichern kann, d. h., wie viel asymmetrischen Datenverkehr er verarbeiten kann, hängt von der Speichergrösse des Switches ab.
Uplink-Ports	Spezielle Ports (oft als Steckmodule), deren Verbindungen intern nicht gekreuzt sind, die somit zur Verbindung von Switches und Multiport-Repeaters genutzt werden können. Solche Ports haben oft eine höhere Geschwindigkeit als andere Ports.
10-Gigabit-Ethernet-Ports	Glasfaser- oder Twisted-Pair-Anschlüsse für 10 Gbit/s, oft auch als Steckmodule.
Auto mdi	Ports, die erkennen, ob eine gekreuzte Verbindung nötig ist oder nicht bzw. ob sie mit einem anderen Switch und Multiport-Repeater verbunden sind und sich dann automatisch als Uplink Port einstellen.
Modularer Aufbau	Switches, die Steckplätze zum Einschub von unterschiedlichen Modulen anbieten (z. B. Module mit 24x 1000BaseTX oder 4x 100BaseSR)

Eigenschaft	Varianten
manageable	Switches, deren Einstellungen über das Netzwerk vorgenommen und abgefragt werden können. Aus diesem Grund verstehen die Switches das TCP/IP-Protokoll und benötigen eine IP-Adresse. Das hat jedoch nichts mit den eigentlichen Funktionen des Switches auf Layer 2 zu tun. Meistens werden damit Merkmale wie das Spanning Tree Protocol oder Virtual LANs konfiguriert.
STP	Diese Switches können doppelte Verbindungen erkennen, die sonst bei Ethernet das ganze Netz lahmlegen würden. Mit dem Spanning Tree Protocol teilen alle Switches sich gegenseitig ihre Verbindungen mit. Daraus kann die Topologie des Netzes berechnet werden und redundante Verbindungen können abgeschaltet werden. Beim Ausfall der ursprünglichen Verbindung wird die redundante Verbindung automatisch wieder aktiviert.
Port-Trunking	Parallelschalten von mehreren Verbindungen zur Bandbreitenerhöhung (z. B. 4x 1 Gbit/s zu 4 Gbit/s). Funktioniert nur, wenn beide Seiten Trunking unterstützen, ansonsten entsteht auch eine verbotene doppelte Verbindung (Loop).
Virtual LANs (VLAN)	Mit Switches, deren Ports einzelnen virtuellen LANs zugewiesen werden können, ist man nicht mehr an den physikalischen Aufbau eines Netzes gebunden. So können Sie z. B. alle Computer einer Abteilung zu einem virtuellen LAN zusammenfassen, auch wenn diese physisch über mehrere Stockwerke verteilt sind
Stackable Switch	Stackable Switches können direkt über eine schnelle herstellerspezifische Steckverbindung gekoppelt werden und verhalten sich dann gemeinsam wie ein grösserer Switch. Sie sind untereinander mit hoher Bandbreite verbunden, müssen aber alle vom gleichen Typ sein.

Quelle: D.Aversa und J.Meier (2014), Modul 129, LAN-Komponenten in Betrieb nehmen, Compendio Bildungsmedien AG, Zürich

Router

Ein Router arbeitet auf Layer 3 des OSI-Modells, dh. er wertet die IP-Adressen aus.

Routing Ports

Die Ports eines Routers haben immer eine IP-Adresse, sie arbeiten auf Layer 3

Routing Funktion

Exakterweise müsste man davon sprechen, dass die Routing Funktion eines Routers auf Layer 3 arbeitet. In der Regel sind Router jedoch Multifunktionsgeräte, die z.B. auch NAT beherrschen (Layer 4 mit TCP/UDP Ports) oder zusätzliche Firewall Aufgaben übernehmen (Layer 2, 3 , 4 und höher)

Aufgaben

Die Hauptaufgabe eines Routers besteht darin unterschiedliche Netzwerke miteinander zu verbinden. Das beinhaltet:

- Ermitteln der verfügbaren Routen
- Auswahl der geeigneten Route
- Herstellen der Verbindung
- Anpassen der Datenpakete

Details zu diesen Aufgaben werden im Kapitel **Routing** behandelt

Layer-3-Switch

- Kombination aus Router und Switch
- Arbeitet auf OSI-Layer 2 und 3
- Entscheidung zur Weiterleitung erfolgt über MAC-Adresse und IP-Adresse
- Einzelne Ports können verschiedenen Subnetzen zugeordnet werden (-> virtual LAN = VLAN kann aufgebaut werden)
- Vorteile gegenüber Router:

- ✓ Billiger
 - ✓ Höherer Durchsatz
 - ✓ Hohe Flexibilität
- ✓ Nachteile gegenüber Router :
- ✓ Weniger Features

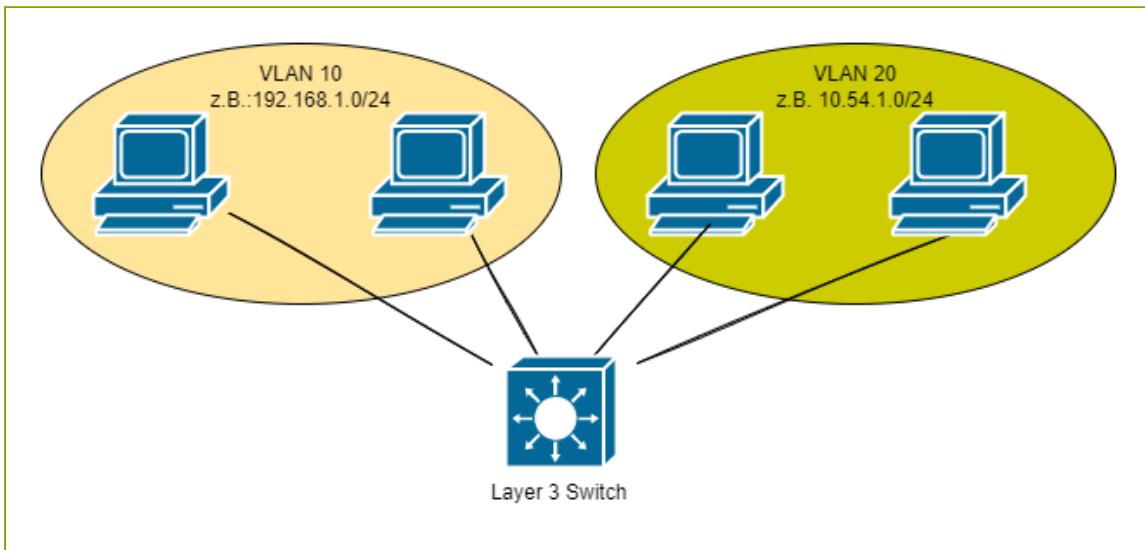


Abb. 1: Layer 3 Switch mit 2 VLAN's

Weitere Geräte

Firewall

Eine Firewall im klassischen Sinn wertet typischerweise IP-Adressen und TCP/UDP-Ports aus. Sie arbeitet damit auf Layer 3 und 4 und wird als Paketfilter bezeichnet. Solche sind meistens als Software im Kernel des Betriebssystems integriert (z.B. iptables oder nftables bei Linux, Windowsfirewall)



Abb. 1: Firewall Appliance

Die meisten Hardware Firewalls sind jedoch als eigenständige Appliance ausgelegt und übernehmen zusätzliche Aufgaben auf Layer 5 - 7. Das bedeutet sie können auch die Inhalte der Datenpakete auswerten und filtern (z.B. Virenscanner, Contentfilter, etc.)

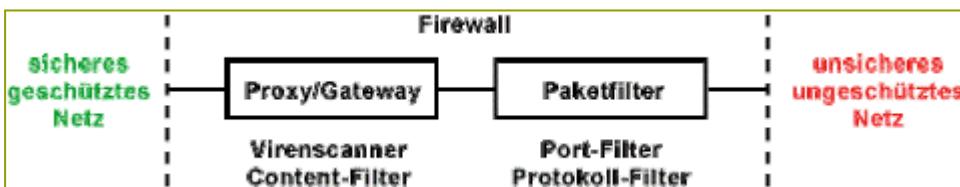


Abb. 1: Eine Firewall Appliance ist eine Kombination von Paketfilter und Contentfilter

Gateway

Der Begriff Gateway wird uneinheitlich verwendet. In der eigentlichen Bedeutung bezeichnet eine Gateway jedoch ein Gerät das physikalisch inkompatible Netze verbindet. Einige Beispiele dazu:

- ✓ Ein ADSL-Modem, das zwischen dem LAN und dem öffentlichen Telefonnetz verbindet.
- ✓ Ein Access-Point, der zwischen LAN und WLAN verbindet.
- ✓ Ein LoRaWAN Gateway, das zwischen dem LoRa-Funktprotokoll und dem LAN verbindet.

Verbindungen zwischen Netzwerkgeräten

Crossover Kabel

Die meisten Geräte im LAN sind mit Twisted-Pair-Kabeln im Vollduplex-Mode verbunden. Die bedeutet, dass jedes Gerät über eine eigene Sendeleitung (Tx = Transmitt) und Empfängerleitung (Rx = Recive) verfügt. Diese werden mit den beiden Adernpaare des TP-Kabels miteinander verbunden. Da nun die Sendeleitung des ersten Gerätes mit der Empfangsleitung des zweiten Gerätes verbunden sein muss, bedeutet dies, dass sich die Adernpaare kreuzen müssen. Das folgende Bild veranschaulicht die Situation:

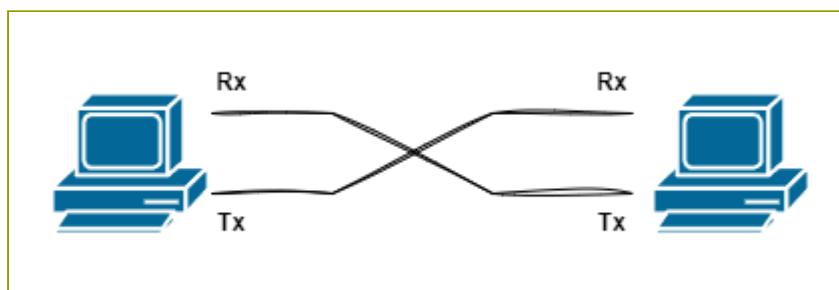


Abb. 1: Verbindung zweier Endgeräte

Diese Aufgabe wird durch sogenannte gekreuzte Twisted-Pair-Kabel (engl. Crossover) übernommen, bei denen die Adernpaare entsprechend verkreuzt werden.

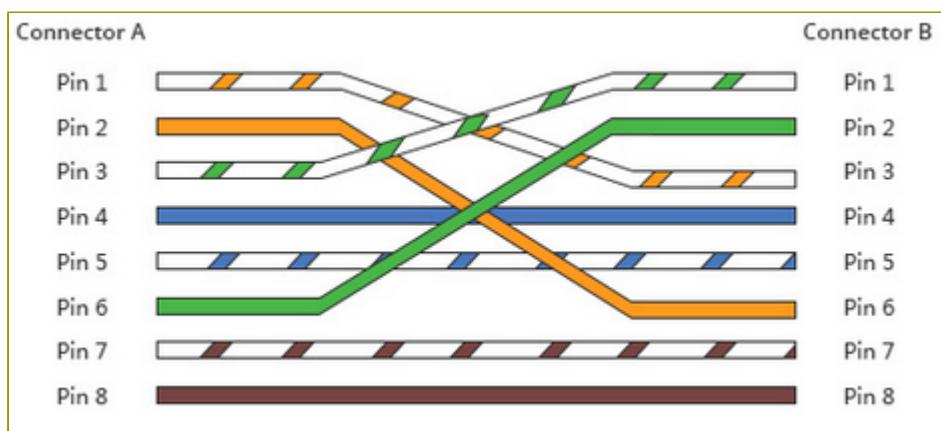


Abb. 2: Crossover Kabel

Um ein Kreuzkabel zu erkennen, genügt meist ein kurzer Blick auf die Steckerenden. Legen Sie diese mit gleicher Ausrichtung nebeneinander und vergleichen Sie die Farben der einzelnen Adern. Ergeben sich Unterschiede in der Reihenfolge, handelt es sich nicht um ein 1:1-Kabel.

Endgeräte-Switch/Hub

Ein Hub oder Switch sind intern bereit so verkabelt, dass für die Verbindung von Endgeräten zum Switch/Hub ein ungekreuztes Kabel verwendet werden kann. Das folgende Bild veranschaulicht die Situation:

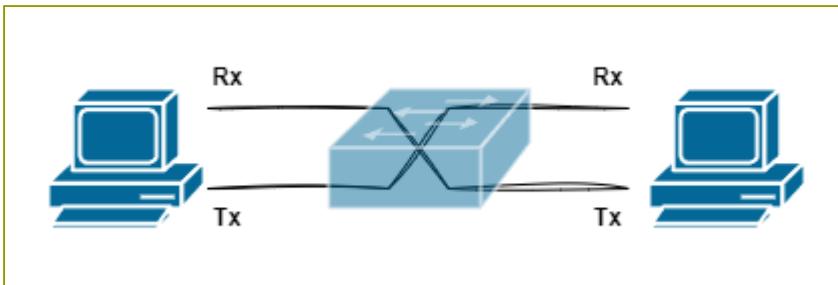


Abb. 2: Verbindung zweier Endgeräte mit Switch/Hub

Hingegen müssen nun Verbindungen zwischen Switches wieder mit Crossover-Kabeln vorgenommen werden (ausser bei Verwendung eines Uplink Portes).

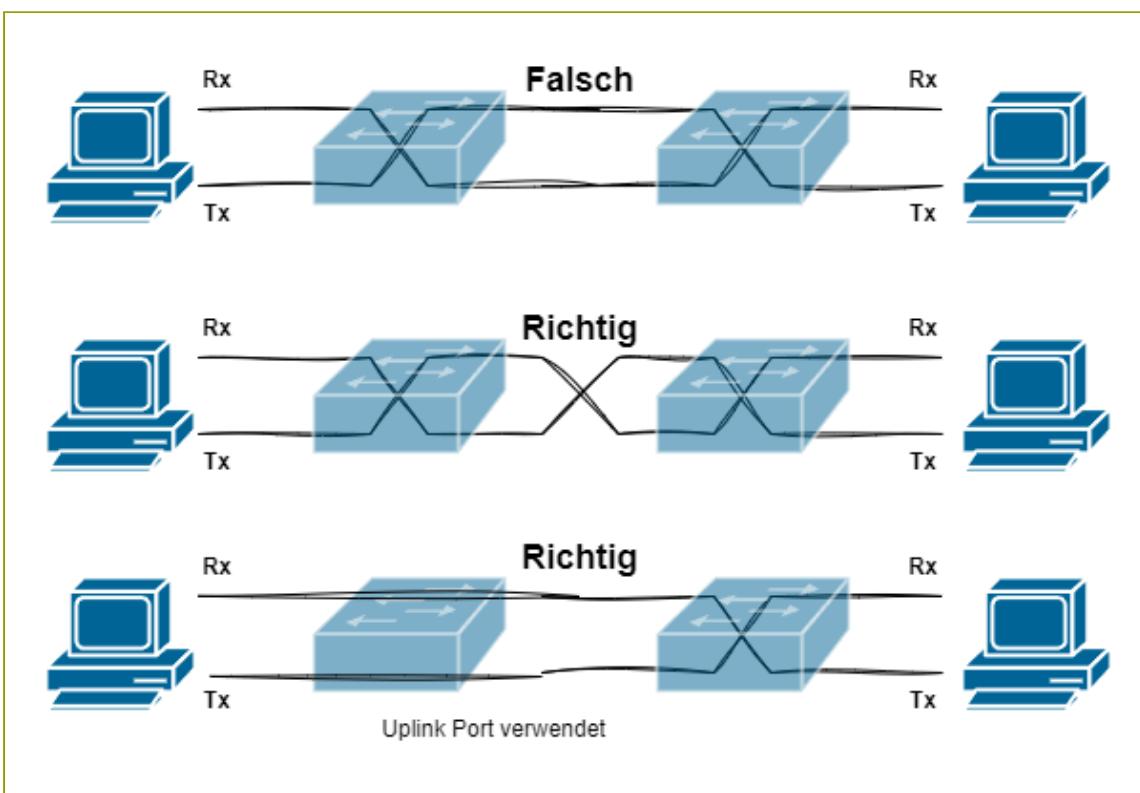


Abb. 3: Verbindung zwischen Switches

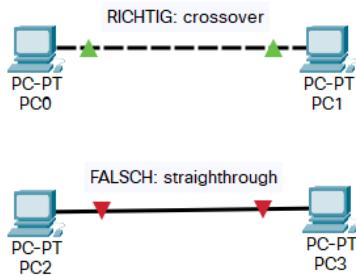
Auto-MDI und 1000BASE-T

Crossover-Kabel haben mittlerweile stark an Bedeutung verloren und kommen nur noch relativ selten zum Einsatz. Grund hierfür sind die Verbreitung von Auto-MDI und 1000BASE-T. Auto-MDI erkennt automatisch die Adernpaare und sorgt für die korrekte interne Belegung der Buchsen. Dadurch können Sie alle Geräte direkt mit einem Straight-Through-Kabel (ungekreuztes Kabel) anschliessen. Beim 1000BASE-T Standard sind gekreuzte Netzwerkkabel

ebenfalls überflüssig, da dieser Standard in der Lage ist, die einzelnen Adernpaare zu identifizieren und beliebige Zuordnungen zu treffen. Moderne Geräte unterstützen diese Standards. Dadurch ist es prinzipiell egal, welchen Kabeltyp Sie für die Verbindung verwenden. Die Netzwerkverbindung lässt sich sowohl über ein Kreuzkabel als auch über ein Straight-Through-Kabel herstellen.

Packettracer

Die Switches/Hubs und Computer bei Packettracer verfügen über kein Auto-MDI. Entsprechend ist es wichtig, dass Sie korrekte Kabel verwenden. Die roten Markierungen in der Abbildung lassen erkennen, dass keine Verbindung zwischen den unteren beiden PC's zustande kommt. Der Grund liegt in der Verwendung eines ungekreuzten Kabels.



Grösseres LAN aufbauen

Um ein Netzwerk in einem mehrstöckigen Gebäude aufzubauen gibt es verschiedene Verbindungsvarianten. In der Abbildung sehen sie 3 Varianten mit einem Coreswitch im Erdgeschoss, je einem Stockwerkswitch und je einem weiteren Switch für die Feinverteilung. Jede Variante hat ihre Vor- und Nachteile.

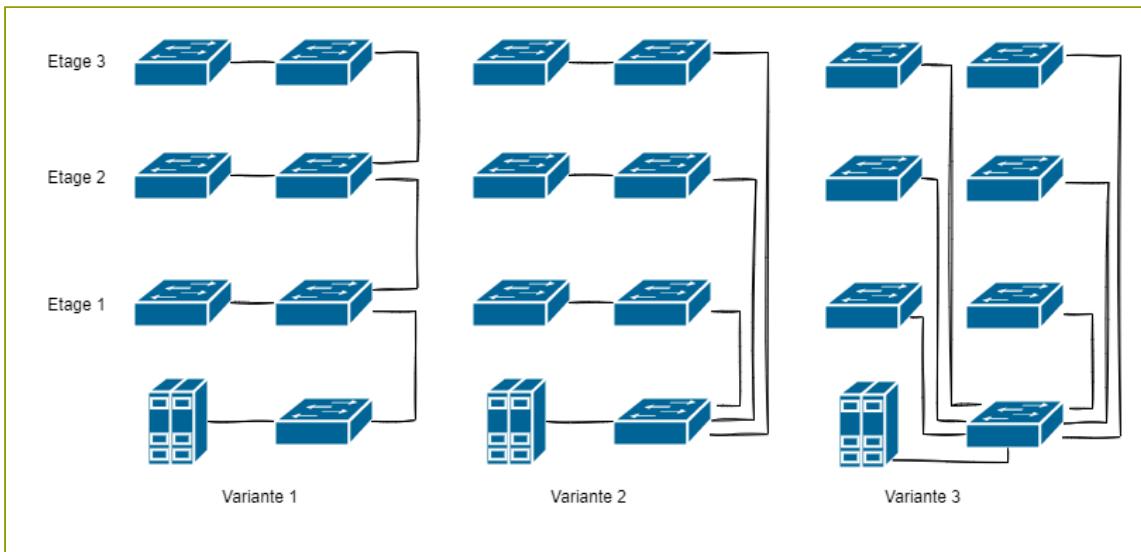


Abb. 2: Verbindungsvarianten für Stockwerkverkabelung

Variante	Ausfallsicherheit	Bandbreite für die angeschlossenen PC's	Verkabelungsaufwand	Kosten
Variante 1	niedrig	gering	gering	niedrig
Variante 2	mittel	mittel	mittel	mittel
Variante 3	gut	hoch	hoch	hoch

Variante 3 benötigt einen leistungsfähigen Coreswitch mit vielen Gigabit Ports und hoher Ausfallsicherheit. Kommen noch unterschiedliche Netzwerke oder VLAN's dazu, werden auch Router oder Layer-3-Switches benötigt.

Address Resolution Protocol

Das Address Resolution Protocol (ARP) ist ein zentraler Bestandteil um den Zusammenhang zwischen logischen IP-Adressen (Layer 3) und den dazugehörigen physikalischen MAC-Adressen (Layer 2) aufzulösen.

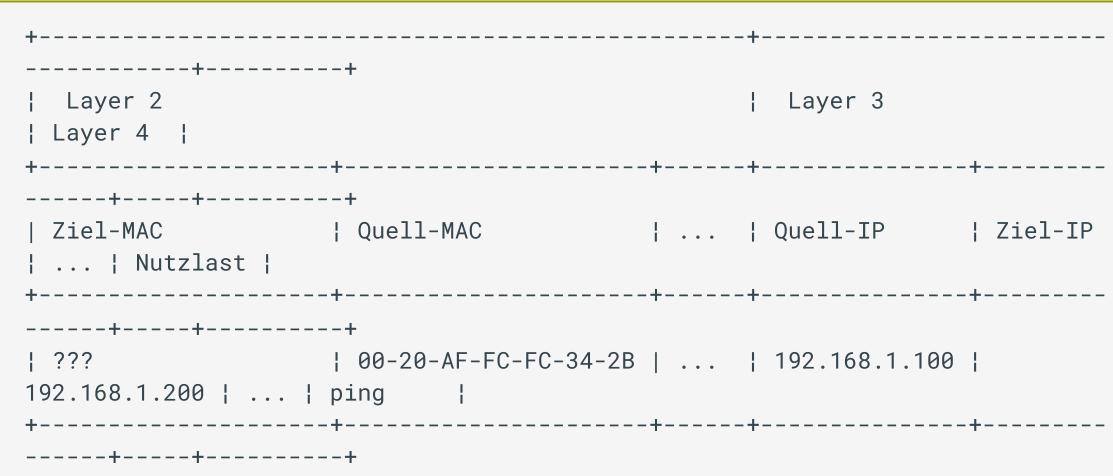
Vor jeder Datenübertragung muss über die verschiedenen OSI-Layer hinab letztendlich ein Ethernet-Frame zusammengebaut werden. Dabei fügt jedes Protokoll seine Headerdaten hinzu:
Bei Layer 3 und 2 sind das:

- ✓ Layer 3 : Angaben zu Ziel- und Quell IP-Adressen
- ✓ Layer 2 : Angaben zu Ziel- und Quell MAC-Adressen

Schauen wir dazu dieses Beispielskommando, abgesendet von der Station 192.168.1.100 mit MAC-Adresse 00-20-AF-FC-FC-34-2B an:

```
ping 192.168.1.200
```

Dazu wird ein Frame wie abgebildet aufgebaut:



Der sendende Rechner kennt natürlich seine eigene IP- und MAC-Adresse: Diese kann er in den entsprechenden Feldern des Frames einbauen. Die Ziel IP-Adresse kennt er ebenfalls, die wurde ja mit dem ping-Kommando eingegeben. Was jedoch noch fehlt ist die MAC-Adresse des Zielrechners. Ohne diese Angabe kann der Frame nicht losgesendet werden. Wie bring nun der sendende Rechner diese Adresse in Erfahrung?

An dieser Stelle kommt das ARP zum Zug. Das Verfahren lässt sich so skizzieren:

- ✓ **ARP-Request:** Ein Layer 2 Broadcast (Ziel-MAC-Adresse: FF-FF-FF-FF-FF-FF) an alle Stationen mit der Frage:
Wer hat die IP-Adresse 192.168.1.200?
- ✓ **ARP-Reply:** Dasjenige Gerät, das sein IP-Adresse erkennt antwortet mit:
Hier, das bin ich! Meine MAC-Adresse lautet: 9C-6B-00-01-F7-D1
Alle anderen verwerfen die Anfrage.
- ✓ Nun kann der Frame mit der Ziel-MAC Adresse komplettiert werden und das eigentliche ping-Kommando abgesetzt werden.
- ✓ **ARP-Cache:** Damit dieser Vorgang nicht für jedes Paket erneut ausgeführt werden muss, speichert der sendende Rechner die IP-Adresse zusammen mit der MAC-Adresse in seinem ARP-Cache. Der ARP-Cache kann mit dem Kommando `arp -a` angezeigt werden:

```
C:\>arp -a
Schnittstelle: 192.168.1.100
  Internetadresse      Physische Adresse      Typ
    192.168.1.200        9C-6B-00-01-F7-D1    dynamisch
  ...
```

Wie man sieht, ist zu einer IP-Adresse die entsprechende MAC-Adresse gespeichert. Dynamisch bedeutet, dass der Eintrag automatisch hinzugefügt wurde. In der Regel läuft ein Eintrag im ARP-Cache nach 5 Minuten ab und wird dann automatisch gelöscht. Auch ein Neustart löscht den ARP-Cache komplett. Mit `arp -d` kann der ARP-Cache manuell gelöscht werden.

⚠️ ARP-Spoofing

Da der ARP-Cache keine Authentifizierung vorsieht, kann dieser für Angriffe, sogenanntes ARP-Spoofing missbraucht werden.



Analogiebeispiel

Wenn der Lehrer zu Beginn des Schuljahrs vor einer neuen Klasse steht, kennt er die Namen seine Schüler (=logische Adressen). Die Liste mit den Namen hat er ja von der Schulverwaltung bekommen. Er kennt jedoch nicht die Gesichter (=physikalische Adressen) hinter den Namen. Der ARP-Cache des Lehrers (Gedächtnis) ist quasi leer. Was tut nun der Lehrer?



Er fragt z.B. in die Klasse hinein: **Wer ist Jonathan Fischer?** (ARP-Request: Broadcast an alle). **Jonathan Fischer streckt auf** (ARP-Reply). Alle anderen

Schüler ignorieren die Frage. Der Lehrer weiss nun, welches Gesicht zu diesem Namen gehört und merkt sich dieses, dh. er macht einen Eintrag in seinem ARP-Cache. Beim nächsten Mal kann der Lehrer Jonathan Fischer direkt ansprechen, er weiss ja nun wer dieser ist.

Um den Lehrer zu ärgern, könnte auch ein anderer Schüler als Jonathan Fischer aufstrecken, z.B. Hans Vader. Nun verknüpft der Lehrer das Gesicht von Hans Vader fälschlicherweise mit dem Namen Jonathan Fischer (ARP-Spoofing). Eine Authentifizierung ist nicht vorgesehen: der Lehrer verlangt ja normalerweise keine ID der Schüler.

IP-Protokol

Das IP-Protokol (IP steht bereits für Internet Protocol!) ist das am häufigsten verwendete Protokol auf OSI-Layer 3. Weitere sind z.B. IPsec, ICMP (ping) oder ARP. Das IP-Protokol gibt es in den 2 Versionen IPv4 und IPv6. In diesem Kapitel wird IPv4 behandelt. Gemeinsam an allen Layer 3 Protokollen ist die Eigenschaft, dass Datenpakete nebst der physikalischen Adressierung durch MAC-Adressen eine logische Adressierung durch die IP-Adressen erhalten und somit die Kommunikation über die eigentlichen Netzgrenzen hinaus ermöglichen. Dies ermöglicht erst das weltumspannende Internet.

Header

Der Header eines IP-Paketes besteht aus 20 Bytes (+optional 40 zusätzliche Bytes). Die wichtigsten Felder darin sind die Quell- und Ziel-IP-Adressen (je 4 Bytes)

+-----+-----+-----+-----+								
Version IHL TOS Total Length 1. -								
4. Byte								
+-----+-----+-----+-----+								
Identification Flags Fragment Offset 5. -								
8. Byte								
+-----+-----+-----+-----+								
TTL Protocol Header Checksum 9. -								
12. Byte								
+-----+-----+-----+-----+								
Source Address 13. -								
16. Byte								
+-----+-----+-----+-----+								
Destination Address 17. -								
20. Byte								
+-----+-----+-----+-----+								
Options (optional) max. -								
+40 Bytes								
+-----+-----+-----+-----+								

Hier eine Übersicht über die weiteren Felder:

- ✓ **Version:** IPv4 oder IPv6
- ✓ **IHL:** Internet Header Length = Länge des Headers inkl. optionale Headerdaten
- ✓ **TOS:** Type of Service: Für die Priorisierung von IP-Paketen
- ✓ **Total Length:** Länge des gesamten IP-Paketes, inkl. Header
- ✓ **Identification:** Identifiziert zusammengehörende fragmentierte IP-Pakete

- ✓ **Flags:** Geben an ob ein Paket fragmentiert werden darf oder nicht
- ✓ **Fragment Offset:** Position eines Fragmentes innerhalb des Gesamt IP-Paketes
- ✓ **TTL:** Time To Live: Zu Begin z.B. 64, jeder Router reduziert den Wert um 1, bei 0 wird ein Paket verworfen. Dies soll verhindern, dass Pakete ewig weitergeleitet werden
- ✓ **Protocol:** Protokoll der Nutzdaten auf Layer 4 (TCP hat z.B. den Wert 0x06, UDP 0x11)

Fragmentation tritt ein, wenn ein IP-Paket grösser als die MTU (Maximum Transmission Unit) ist. Bei Ethernet Frames liegt diese bei 1500 Bytes Nutzdaten. Ist das Paket grösser, passt es nicht in einen Frame hinein. Das IP-Protokoll teilt dann das IP-Paket auf mehrere Teilpakete auf. Die Felder zur Fragmentation steuern diesen Vorgang und ermöglichen das korrekte Wiederzusammensetzen der Teilpakete in das ursprüngliche IP-Paket.

Fragmentation ist im Allgemeinen nicht erwünscht, da es grössere Performance Probleme mit sich bringt. Fragmentation ist nicht zu verwechseln mit der normalen TCP-Segmentation, bei der grosse Datenmengen (z.B. ein Bild) für die Übertragung in mehrere Segmente aufgeteilt werden. Diese Segmente sollten jedoch nicht grösser als die MTU (minus IP/TCP Header) sein um Fragmentation zu vermeiden.

IP Adressen

IPv4 Adressen bestehen aus 32 Bits und werden in Dezimalschreibweise von 0.0.0.0 bis 255.255.255.255 geschrieben. Beispiel: 25.126.31.160 Zu jeder IP-Adresse gehört die sogenannte (Sub-)Netzmaske. Diese ist ebenfalls 32 Bit gross, kann jedoch nur aus einer ununterbrochenen Folge von 1-er Bits gefolgt von einer ununterbrochenen Folge von 0-er Bits bestehen. Auch die Netzmaske wird dezimal in 4 Blöcken geschrieben. Beispiel:

```
1111'1111 1111'1111 1111'0000 0000'0000 = 255.255.240.0
1111'1111 1111'1111 1111'0000 0000'1111 ist keine gültige Netzmaske
```

Eine IP-Adresse teilt sich auf in den sogenannten Netzwerkanteil und den Hostanteil. Diejenigen Bits die zum Netzwerkanteil gehören sind diejenigen bei denen die Netzmaske eine 1 hat, die anderen gehören zum Hostanteil. Der Netzwerkanteil aller Stationen eines Netzes muss gleich sein, damit die Kommunikation direkt (d.h. ohne Router) funktioniert. Für die Kommunikation von Stationen mit unterschiedlichem Netzwerkanteil werden Router benötigt.

Beispiel:

```
192.168.1.10  = 1100'0000 1010'1000 0000'0001 0000'1010 : IP-Adresse
255.255.255.0 = 1111'1111 1111'1111 1111'1111 0000'0000 : Netzmaske
```

```
192.168.1. 0 = Netzwerkanteil
0. 0.0.10 = Hostanteil
```

Bei den ersten 24 Bits ist die Netzmaske jeweils 1, somit ist der Netzwerkanteil der IP-Adresse 192.168.1 der Hostanzeil ist 10.

Die Station 192.168.1.10 kann direkt mit der Station 192.168.1.20 (255.255.255.0) kommunizieren, da beide Stationen denselben Netzwerkanteil haben.

Merke

- Alle Geräte innerhalb eines Netzes müssen den gleichen Netzwerkanteil haben, damit sie kommunizieren können. PCs mit unterschiedlichen Netzwerkanteil können nicht einfach so kommunizieren, sondern brauchen dazu einen Router.
- Alle Geräte innerhalb eines Netzes müssen unterschiedliche Hostanteile haben, damit sie kommunizieren können. Ansonsten ist das Ziel der Datenpakete nicht eindeutig.

Netzklassen

Die IP-Adressen werden in verschiedene Adressklassen (A, B, C) eingeteilt. Obwohl diese Klassen keine Bedeutung mehr haben, werden die Begriffe Klasse-A, B, C Netz immer noch verwendet, deshalb sollten Sie diese Klassen kennen.

Veraltete Lehre

- Ursprünglich gab es nur A-Klasse Netze mit fix 256 Netzen und 2^{24} Teilnehmern
- Ein erweiterte Konzept sah die Einteilung in drei (später 5) Netzklassen A, B ,C vor
- 1993 wurde die starre Aufteilung der Netzklassen durch CIDR (Classless Interdomain Routing) ersetzt. Die ursprünglichen Netzklassen erhielten dabei die Standardsubnetzmasken 255.0.0.0 255.255.0.0 bzw. 255.255.255.0. Andere Subnetzmasken sind jedoch nun auch möglich z.B. 255.255.255.128
- Die Netzklassen A, B, C haben deshalb keine Bedeutung mehr
- Die Grösse eines Netzes ist nicht mehr aus der IP-Adresse abzuleiten, sondern erfordert zwingend die Angabe der Subnetzmaske

In der folgenden Abbildung sehen Sie die Aufteilung in Klasse A, B und C.

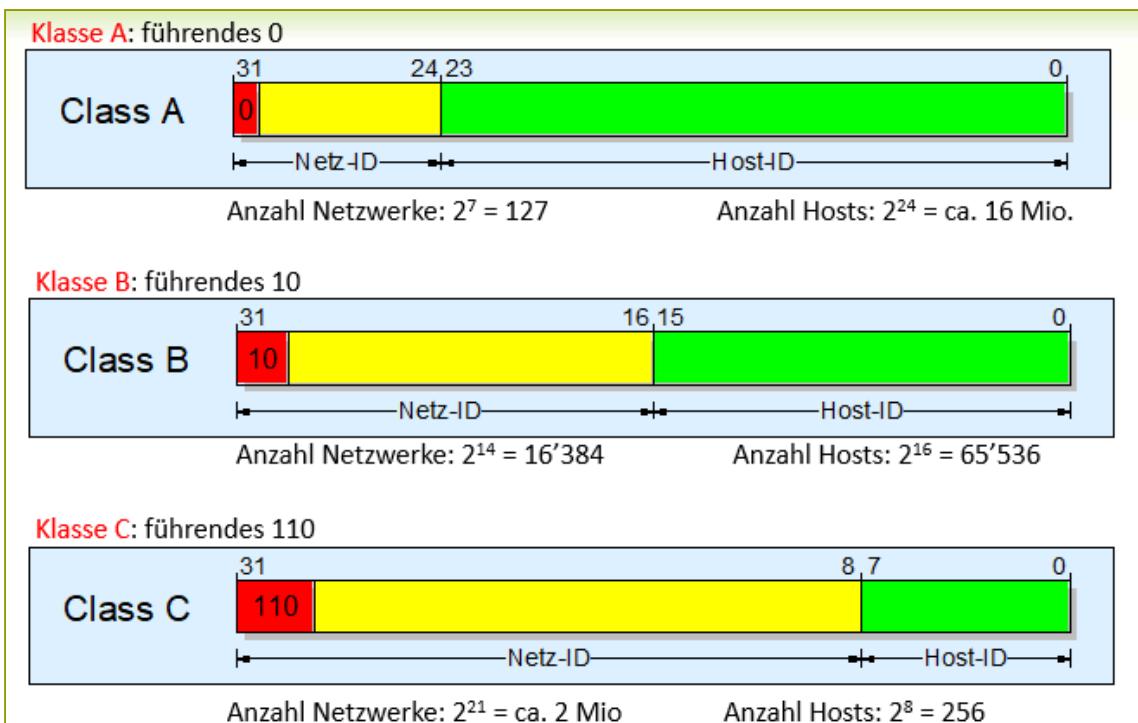


Abb. 1: Klasse A, B und C

Die rot markierten Bits sind fix und erlauben die eindeutige Unterscheidung nach Klasse A, B oder C.

Die Klassen haben die fixen Netzmasken 255.0.0.0 (A), 255.255.0.0 (B) und 255.255.255.0 (C). Im Rahmen des Subnettings sind jedoch auch andere Netzmasken zulässig.

Daraus ergeben sich die folgenden Bereiche

Klasse	Netzwerkanteil	Netzmaske	Anzahl Netzwerke	Anzahl Hostadressen
A	1 - 127	255.0.0.0	127	16'777'214
B	128.0 - 192.255	255.255.0.0	65'384	65'534
C	192.0.0 - 223.255.255	255.255.255.0	2'097'152	254

Spezielle Adressen

Öffentliche IP-Adressen

Öffentliche IP-Adressen können über das Internet erreicht werden. Typischerweise hat z.B. ein Webserver eine öffentliche IP-Adresse. Die Verwendung der öffentlichen IP-Adressen ist global

geregelt. In Europa ist z.B. die RIPE (Réseaux IP Européens) dafür zuständig. Privatanwender und Firmenkunden können öffentliche IP-Adressen über ihrem Internetprovider beziehen.

Private IP-Adressen

Bei gewissen Adressbereichen handelt es sich um private Adressbereiche, welche nicht ins Internet geroutet werden. Die Verwaltung von Adressen in privaten Bereichen liegt in den Händen eines LAN-Betreibers.

Folgende Bereiche sind privat:

Klasse	Bereiche
A	10.0.0.0–10.255.255.255
B	172.16.0.0–172.31.255.255
C	192.168.0.0–192.168.255.255

Wenn mit einer privaten IP-Adresse eine Verbindung zum Internet hergestellt werden soll, braucht es einen Router mit PAT (Port Address Translation), der die privaten IP-Adressen in öffentliche IP-Adressen umwandelt (mit Hilfe von Portnummern). Gängige Router haben diese Funktionalität standardmäßig eingeschaltet.

Reservierte IP-Adressen

Die tiefste IP-Adresse eines Netzwerks, d. h. die Adresse mit dem tiefsten Hostanteil, bezeichnet keinen Host, sondern das gesamte jeweilige Netzwerk und heißt deshalb **Netzadresse**.

Die höchste IP-Adresse eines Netzwerks, d. h. die Adresse mit dem höchsten Hostanteil, bezeichnet keinen Host, sondern wird für Übertragungen an alle Hosts gebraucht und heißt deshalb **Broadcastadresse** (Layer 3 Broadcast).



Netzadresse und Broadcast

Schauen wir das Netzwerk 192.168.1.0 mit der Netzmaske 255.255.255.0 an:

Der Bereich der IP-Adressen geht in diesem Netzwerk von 192.168.1.0 bis 192.168.1.255

- Die tiefste Adresse 192.168.1.0 kann nicht an eine Station vergeben werden, sondern bezeichnet zusammen mit der Netzmaske das Netzwerk als ganzes.
- Die höchste Adresse 192.168.1.255 kann nicht an eine Station vergeben werden, sondern bezeichnet die Adresse für ein Datenpaket das an alle Hosts im Netzwerk gesendet wird.

Loopback Adressen

Eine Sonderstellung unter den IP-Adressen nimmt auch das Klasse A 127 ein. Alle Adressen, die mit 127 anfangen, sind sogenannte Loopback-Adressen. Diese werden von vom sendenden Gerät sofort wieder empfangen. Dazu kann auch der Hostname **localhost** verwendet werden, welche z.B. nach 127.0.0.1 auflöst.

Subnetting

Prinzip

Bis 1993 gab es die 3 Netzklassen A, B und C. Diese zeichneten sich durch ihre Netzmasks A: 255.0.0.0, B: 255.255.0.0 und C: 255.255.255.0 aus. Daraus folgte automatisch die jeweilige maximale Netzgrösse: A: $2^{24} \sim 16$ Mio, B: $2^{16} = 65'536$ und C: $2^8 = 256$.

Am Beispiel eines C-Klasse Netzwerkes lässt sich das so darstellen:

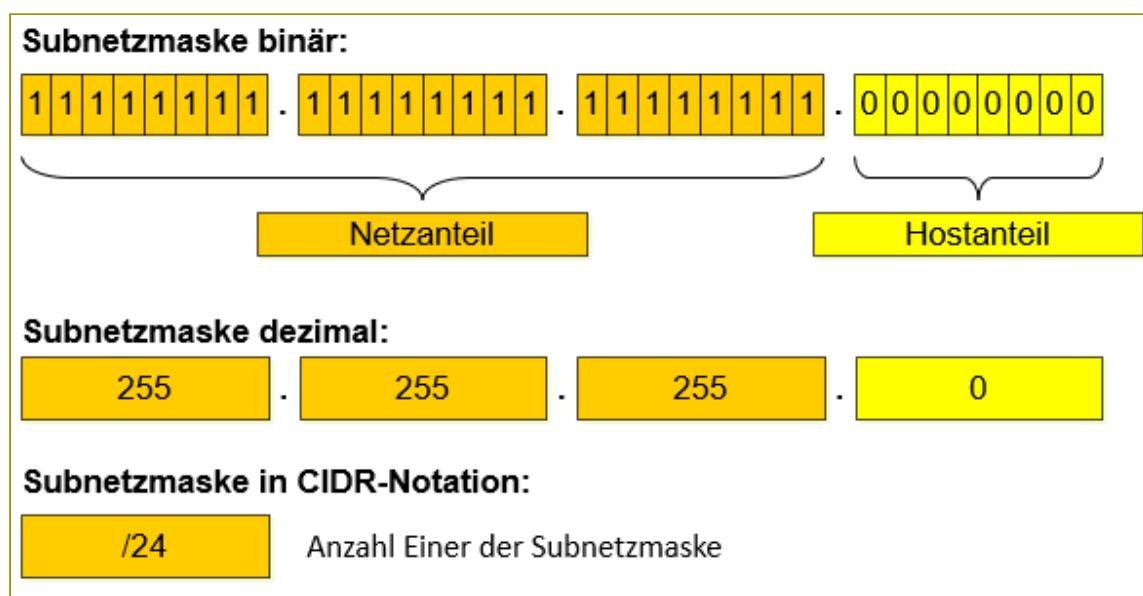


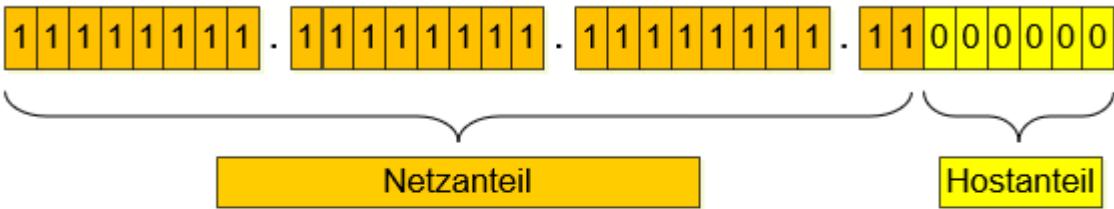
Abb. 1: Netzmaske eines C-Klasse Netzwerkes

Das Bitmuster kennzeichnet den Übergang zwischen Netzanteil und Hostanteil.

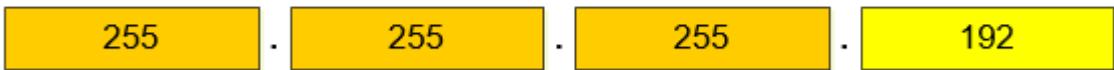
Dieses Prinzip hat sich als zu unflexibel herausgestellt, da viele IP-Adressen verschwendet werden, wenn die zur Verfügung stehende Netzgrösse nicht ausgeschöpft wird. Da bereits absehbar war, dass IP-Adressen knapp würden, hat man deshalb das Classless Interdomain Routing (CIDR) eingefügt und die Netzmasks verallgemeinert.

Im dargestellten Beispiel haben wir eine Netzmase bestehend aus 26 Einern und 6 Nullen. Dieses Netz hat deshalb nur noch die Grösse $2^6 = 64$. Man spricht von Subnetting wenn das ursprüngliche Netz verkleinert wird und entsprechend heisst die Netzmase nun Subnetzmaske. Die Netzadresse und Subnetzmaske lässt sich immer noch dezimal aufschreiben (z.B. 192.168.1.0 255.255.255.192), praktischer ist jedoch die CIDR-Notation mit einem Slash und der Grösse der Subnetzmaske (z.B. 192.168.1.0/26)

Subnetzmaske binär:



Subnetzmaske dezimal:



Subnetzmaske in CIDR-Notation:

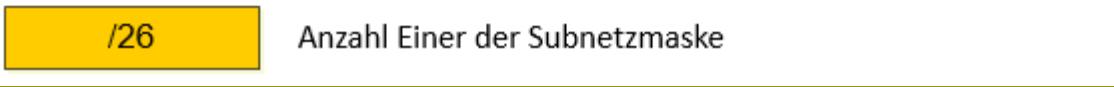


Abb. 2: Subnetzmaske eines 26er Netzwerkes

Die Subnetzmaske stellt also einen Regler für die Grösse eines Netzes dar, je weniger 1-er Bits gesetzt sind, deso mehr IP-Adressen sind verfügbar und umgekehrt

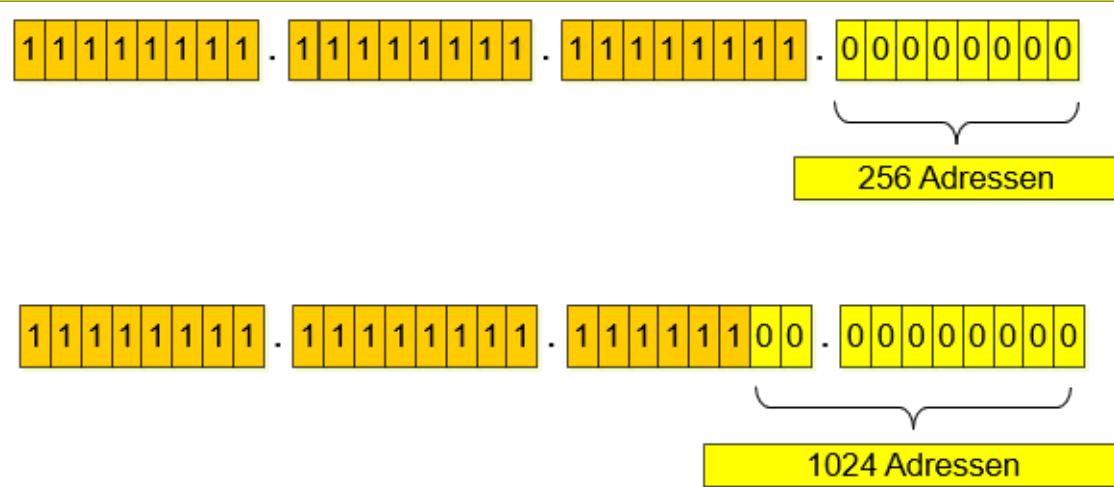


Abb. 3: Die Subnetzmaske ist ein Regler für die Grösse eines Netzes

Gründe für Subnetting

Für eine Firma kann es mehrere Gründe geben, wieso ein gegebenes Netz in Subnetze aufgeteilt wird. Hier einige Gründe:

- ✓ Verkleinerung des Netzes: Ein grossen Netzen wird der Datenverkehr verlangsamt (z.B. viele Paketkollisionen)

- ✓ Netzwerke entsprechend der Firmenorganisation: z.B. Subnetze entsprechend der Abteilungen oder Standorte für bessere Strukturierung
- ✓ Sicherheit: Zugriffe auf sicherheitskritische Abteilungen oder Gastnetze können im Router/Firewall eingeschränkt werden
- ✓ Öffentliche Adressen sparen: Öffentliche Adressen werden nach Anzahl bezahlt, d.h. man möchte ein möglichst kleines Subnetz bezahlen

In der Regel wird ein gegebenes Netz auf Grund der Anzahl Teilnehmer im jeweiligen Subnetz aufgeteilt werden. Dazu müssen für die einzelnen Subnetze die maximale Anzahl Teilnehmer, Netzadressen und Broadcastadressen berechnet werden. Anschliessend kann den einzelnen Stationen eine konkrete IP-Adresse zugewiesen werden (statisch oder per DHCP). Damit diese Berechnungen durchgeführt werden können, muss man die Rechenregeln für IP-Berechnungen kennen. Diese werden im nächsten Abschnitt vorgestellt.

IP-Berechnungen

Die grundlegende Rechenoperationen für IP-Berechnungen sind bitweises AND, OR und NOT. Diese sind hier zusammengefasst:

Bit 1 Bit 2 AND			Bit 1 Bit 2 OR			Bit NOT	
-----	-----	-----	-----	-----	-----	-----	-----
0 0	0	0	0 0	0	0	0 1	1
0 1	0	0	0 1	1	1	1 0	0
1 0	0	0	1 0	0	1		
1 1	1	1	1 1	1	1		

Mit diesen Operatoren kann aus einer IP-Adresse und der Subnetzmaske das Netzwerk (Netzwerkadresse, Broadcast, Grösse) berechnet werden:

- ✓ **Netzadresse:** IP-Adresse AND Subnetzmaske
- ✓ **Hostanteil:** IP-Adresse AND NOT Subnetzmaske
- ✓ **Broadcast:** IP-Adresse OR NOT Subnetzmaske
- ✓ **kleinste IP-Adresse:** Netzadresse + 1
- ✓ **grösste IP-Adresse:** Broadcast - 1
- ✓ **Anzahl Hosts:** $2^{32-\text{CIDR}} - 2$ (abzüglich Netzadresse und Broadcast, welche nicht als IP-Adresse vergeben werden können.)

Dies soll am folgenden Beispiel durchgerechnet werden:

IP-Adresse: 150.10.10.10

Subnetzmaske: 255.255.252.0

CIDR-Notation: 150.10.10.10 / 22

✓ **Netzadresse:** 150.10.8.0

IP:	1	0	0	1	0	1	1	0	.	0	0	0	1	0	1	0	.	0	0	0	1	0	1	0
Maske:	1	1	1	1	1	1	1	1	.	1	1	1	1	1	1	1	.	1	1	1	1	1	0	0
Netz- adresse:	1	0	0	1	0	1	1	0	.	0	0	0	1	0	1	0	.	0	0	0	0	0	0	0
	150				10					8								0						

Abb. 3: Netzadresse: IP-Adresse AND Subnetzmaske

✓ **Hostanteil:** 0.0.2.10

IP:	1	0	0	1	0	1	1	0	.	0	0	0	1	0	1	0	.	0	0	0	1	0	1	0
Maske:	0	0	0	0	0	0	0	0	.	0	0	0	0	0	0	0	.	0	0	0	0	1	1	1
Host- anteil:	0	0	0	0	0	0	0	0	.	0	0	0	0	0	1	0	.	0	0	0	1	0	1	0
	0				0					0				2				10						

Abb. 4: Hostanteil: IP-Adresse AND NOT Subnetzmaske

✓ **Broadcast:** 150.10.11.255

IP:	1	0	0	1	0	1	1	0	.	0	0	0	1	0	1	0	.	0	0	0	1	0	1	0
Maske:	0	0	0	0	0	0	0	0	.	0	0	0	0	0	0	0	.	0	0	0	0	1	1	1
Broadcast:	1	0	0	1	0	1	1	0	.	0	0	0	1	0	1	0	.	0	0	0	1	0	1	1
	150				10					11								255						

Abb. 5: Broadcast: IP-Adresse OR NOT Subnetzmaske

✓ **kleinste IP-Adresse:** 150.10.8.1

✓ **grösste IP-Adresse:** 150.10.11.254

✓ **Anzahl Hosts:** $2^{32-22} - 2 = 2^{10} - 2 = 1022$

Hier die Zusammenfassung zu diesem Beispiel:

IP-Adresse:	150.10.10.10
Subnetz:	255.255.252.0
CIDR:	150.10.10.10 / 22
Netzadresse:	150.10.8.0
Hostanteil:	0.0.2.10
Broadcast:	150.10.11.255
Kleinste IP-Adresse:	150.10.8.1
Grösste IP-Adresse:	150.10.11.254
Anzahl Hosts:	1022

Kontrolle: Netzadresse + Hostanteil muss wieder die IP-Adresse ergeben (150.10.8.0 + 0.0.2.10 = 150.10.10.10)

Vorgehen beim Subnetting

In der Regel wird ein gegebenes Netz auf Grund der Anzahl Teilnehmer im jeweiligen Subnetz aufgeteilt werden.

Das Vorgehen soll an einem Beispiel demonstriert werden:

Sie verwenden das Netzwerk 192.168.1.0. Dieses soll in 2 Teile segmentiert werden. In einem Subnetz werden sich künftig 19 Teilnehmer aufhalten im anderen 80 Teilnehmer.

Der Lösungsweg lässt sich so skizzieren:

- ✓ **Schritt 1:** Benötigte Subnetze anhand der Grösse sortieren
- ✓ **Schritt 2:** Subnetzmasken der Subnetze anhand der Teilnehmer bestimmen
- ✓ **Schritt 3:** Netzadresse und Broadcastadresse des 1. Subnetzes bestimmen
- ✓ **Schritt 4:** Netzadresse und Broadcastadresse des 2. Subnetzes bestimmen
- ✓ **Schritt 5:** kleinste und grösste IP-Adresse berechnen

Die einzelnen Schritte werden nun durchgeführt:

- ✓ **Schritt 1:** Benötigte Subnetze anhand der Grösse sortieren:
Subnetz 1: dasjenige mit **80** Teilnehmern
Subnetz 2: dasjenige mit **19** Teilnehmern
- ✓ **Schritt 2:** Subnetzmasken der Subnetze anhand der Teilnehmer bestimmen

CIDR	Adressen	nutzbar	CIDR	Adressen	nutzbar
/8	16'777'216	16'777'214	/21	8 x 256	2056
/9	128 x 65'536	8'388'606	/22	4 x 256	1022
/10	64 x 65'536	4'194'302	/23	2 x 256	510
/11	32 x 65'536	2'097'150	/24	256	254
/12	16 x 65'536	1'048'574	/25	128 x 1	126
/13	8 x 65'536	524'286	/26	64 x 1	62
/14	4 x 65'536	262'142	/27	32 x 1	30
/15	2 x 65'536	131'070	/28	16 x 1	14
/16	65'536	65'534	/29	8 x 1	6
/17	128 x 256	32'766	/30	4 x 1	2
/18	64 x 256	16'382	/31	2 x 1	0
/19	32 x 256	8'190	/32	1	1
/20	16 x 256	4'094			

Abb. 6: Nutzbare Adressen

Aus dieser Tabelle entnimmt man, dass :

Subnetz 1: 80 Teilnehmern: / **25**

Subnetz 2: 19 Teilnehmern: / **27**

Achtung: Hier muss zusätzlich berücksichtigt werden, dass das Default-Gateway am Router ebenfalls eine IP-Adresse benötigt

✓ **Schritt 3:** Netzadresse und Broadcastadresse des 1. Subnetzes bestimmen

Das 1. Subnetz startet bei der Netzadresse des Ursprungsnetztes

Netzwerk :			
192.	168.	1.	0
1100'0000.	1010'1000.	0000'0001.	0000'0000
1111'1111.	1111'1111.	1111'1111.	1000'0000 (25)
<hr/>			
1100'0000.	1010'1000.	0000'0001.	0000'0000 (AND)
192.	168.	1.	0
Broadcast:			
192.	168.	1.	0
1100'0000.	1010'1000.	0000'0001.	0000'0000
0000'0000.	0000'0000.	0000'0000.	0111'1111 (25)
<hr/>			
1000'0000.	1010'1000.	0000'0001.	0111'1111 (OR)
192.	168.	1.	127

Abb. 7: Subnet 1

✓ **Schritt 4:** Netzadresse und Broadcastadresse des 2. Subnetzes bestimmen

Die Netzadresse des 2. Subnetztes schliesst direkt an das Subnet 1 an

Netzwerk :			
192.	168.	1.	128
1100'0000.	1010'1000.	0000'0001.	1000'0000
1111'1111.	1111'1111.	1111'1111.	1110'0000 (27)
<hr/>			
1100'0000.	1010'1000.	0000'0001.	1000'0000 (AND)
192.	168.	1.	128
Broadcast:			
192.	168.	1.	128
1100'0000.	1010'1000.	0000'0001.	1000'0000
0000'0000.	0000'0000.	0000'0000.	0001'1111 (27)
<hr/>			
1100'0000.	1010'1000.	0000'0001.	1001'1111 (OR)
192.	168.	1.	159

Abb. 8: Subnet 2

✓ **Schritt 5:** kleinste und grösste IP-Adresse berechnen

Kleinste IP = Netzadresse + 1: 192.168.1.1 bzw. 192.168.1.128

Grösste IP = Broadcast – 1: 192.168.1.126 bzw. 192.168.1.158

Hier nochmals die Ausgangslage und das Resultat in der Zusammenfassung:

Sie verwenden das Netzwerk 192.168.1.0. Dieses soll in 2 Teile segmentiert werden. In einem Subnetz werden sich künftig 19 Teilnehmer aufhalten im anderen 80 Teilnehmer.

Subnet	Netzadresse	Subnetzmase	Kleinste IP	Grösste IP
Subnet 1	192.168.1.0	255.255.255.128	192.168.1.1	192.168.1.126
Subnet 2	192.168.1.128	255.255.255.224	192.168.1.129	192.168.1.158

Wer sieht wen?

Geräte können direkt miteinander kommunizieren wenn:

1. sie dieselbe Netzadresse haben und
2. sich im selben IP-Range befinden.

Ansonsten müssen die Daten über einen Router weitergeleitet werden

PC	IP / Subnetz	Netz-Adresse	IP-Range von	IP-Range bis
1	205.1.54.192 / 24	205.1.54.0	205.1.54.1	205.1.54.254
2	205.1.54.92 / 24	205.1.54.0	205.1.54.1	205.1.54.254
3	50.1.54.192 / 8	50.0.0.0		
4	150.1.54.192 / 16	150.1.0.0		
5	192.168.0.165 / 23	192.168.0.0	192.168.0.1	192.168.1.254
6	192.168.0.54 / 26	192.168.0.0	192.168.0.1	192.168.0.62

Gerät 1 und 2 können direkt miteinander kommunizieren.

Gerät 3 und 4 können nicht direkt miteinander kommunizieren. (unterschiedliche Netzadresse)

Gerät 5 und 6 können nicht direkt miteinander kommunizieren. (PC 5 befindet sich ausserhalb des Subnetzes von PC 6)

Abb. 9: Wer sieht wen?

Arbeitsweise

Funktionen

Was macht ein Router?

- ✓ Er verbindet 2 oder mehrere Netzwerke
- ✓ Er ermöglicht den Datenaustausch über die Netzwerkgrenzen hinaus
- ✓ Er hat mindestens 2 Netzwerkanschlüsse, somit mindestens 2 IP-Adressen
- ✓ Die Netzwerkanschlüsse sind jeweils Mitglied des jeweiligen Netzes
- ✓ Als IP-Adresse eines Netzwerkanschlusses wird häufig die kleinste IP-Adresse des jeweiligen Netzes verwendet
- ✓ Die Geräte eines Netzwerkes müssen die IP-Adresse des Routers als Standardgateway (GW) eintragen
- ✓ Alle Frames die nicht für das eigene Netzwerk bestimmt sind, werden an das Standardgateway gesendet
- ✓ Das Standardgateway ist damit Ein- und Ausgang eines Netzes

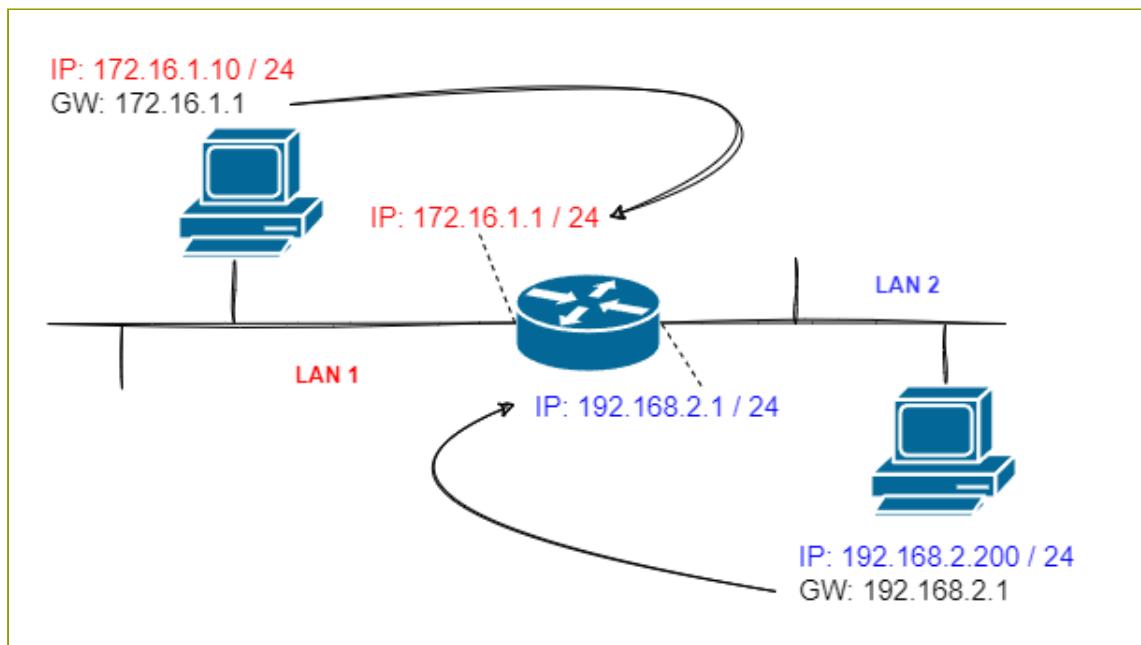
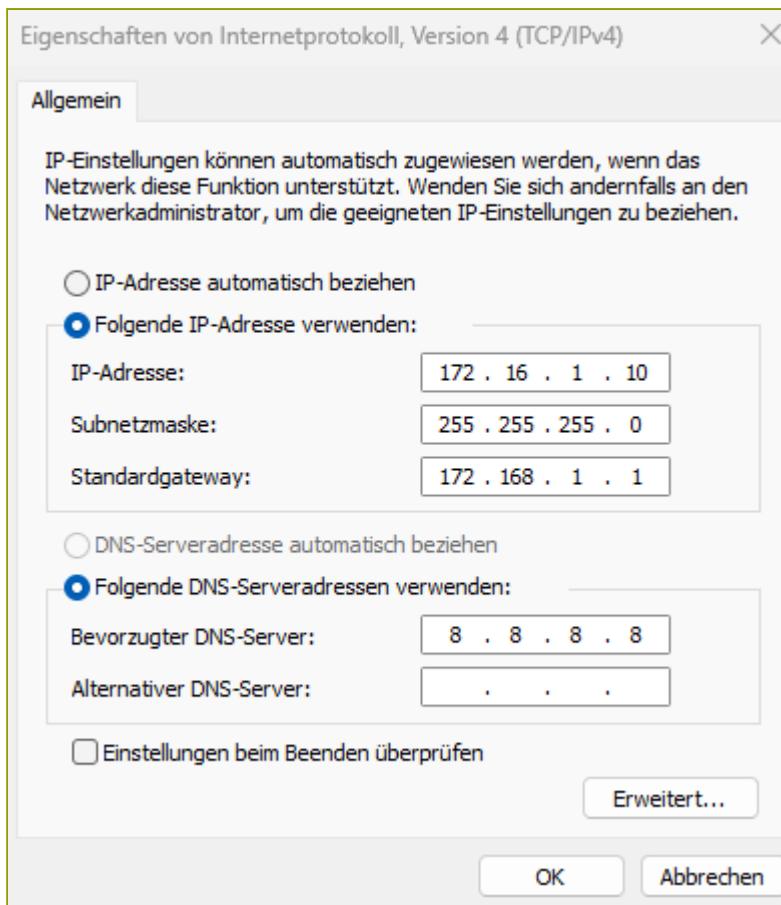


Abb. 1: Router verbinden 2 (oder mehrere) unterschiedliche Netze

Bei Windows wird das Standardgateway unter den Eigenschaften von Internetprotokoll



eingestellt.

Abb. 2: Standardgateway bei Windows eingeben

Bei Linux erfolgt die Eingabe des Gateway rein textbasiert, verschiedene Distributionen haben jedoch unterschiedliche Tools um die Einstellungen ebenfalls graphisch zu machen. Bei Ubuntu Desktop finden Sie die Einstellungen unter den Settings für Wired.

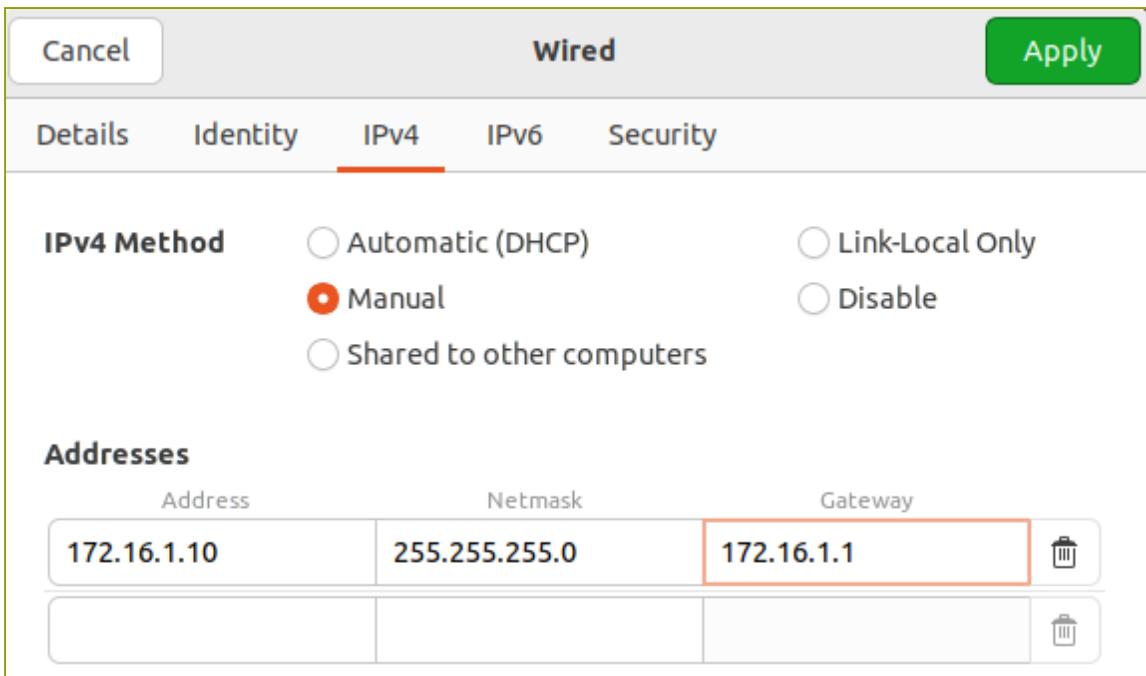


Abb. 3: Standardgateway bei Ubuntu eingeben

Wann braucht es Routing?

Der Router kommt immer dann ins Spiel, wenn sich eine Ziel IP-Adresse nicht im selben Netz befindet wie die Sender IP-Adresse. In diesem Fall wird ein Frame an das Default Gateway weitergeleitet, der Router entscheidet dann, was mit dem Frame weiterpassiert. Im folgenden Diagramm ist der Ablauf dargestellt. Je nach dem ob die Ziel MAC-Adressen schon bekannt sind oder nicht findet noch ein ARP-Request statt.

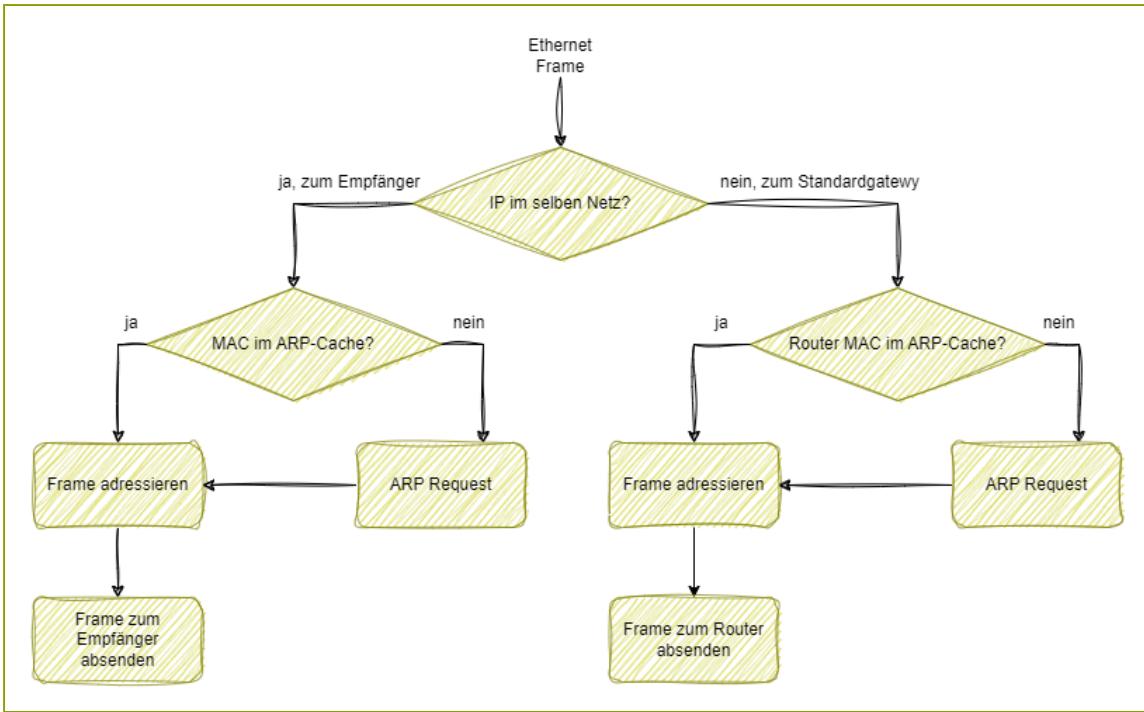


Abb. 4: Ist die Ziel IP-Adresse nicht im selben Netz, wird der Frame zum Router weitergeleitet

Ermitteln der nächsten Station

Trifft ein Frame beim Router ein, wird zuerst überprüft, ob das Zielnetz direkt am Router angeschlossen ist. Ist das der Fall, wird der Frame neuadressiert (allenfalls mit einem zusätzlichen ARP-Request) und weitergeleitet. Die Details der **Neuadressierung** sind im nächsten Abschnitt erläutert.

Ist das Zielnetz **nicht** direkt am Router angeschlossen, wird mit Hilfe der **Routingtabelle** die IP-Adresse der nächsten Zwischenstation ermittelt und anschliessend der Frame zu dieser Zwischenstation weitergeleitet. Die Funktionsweise der Routingtabelle wird im Kapitel **Routingtabelle** erläutert.

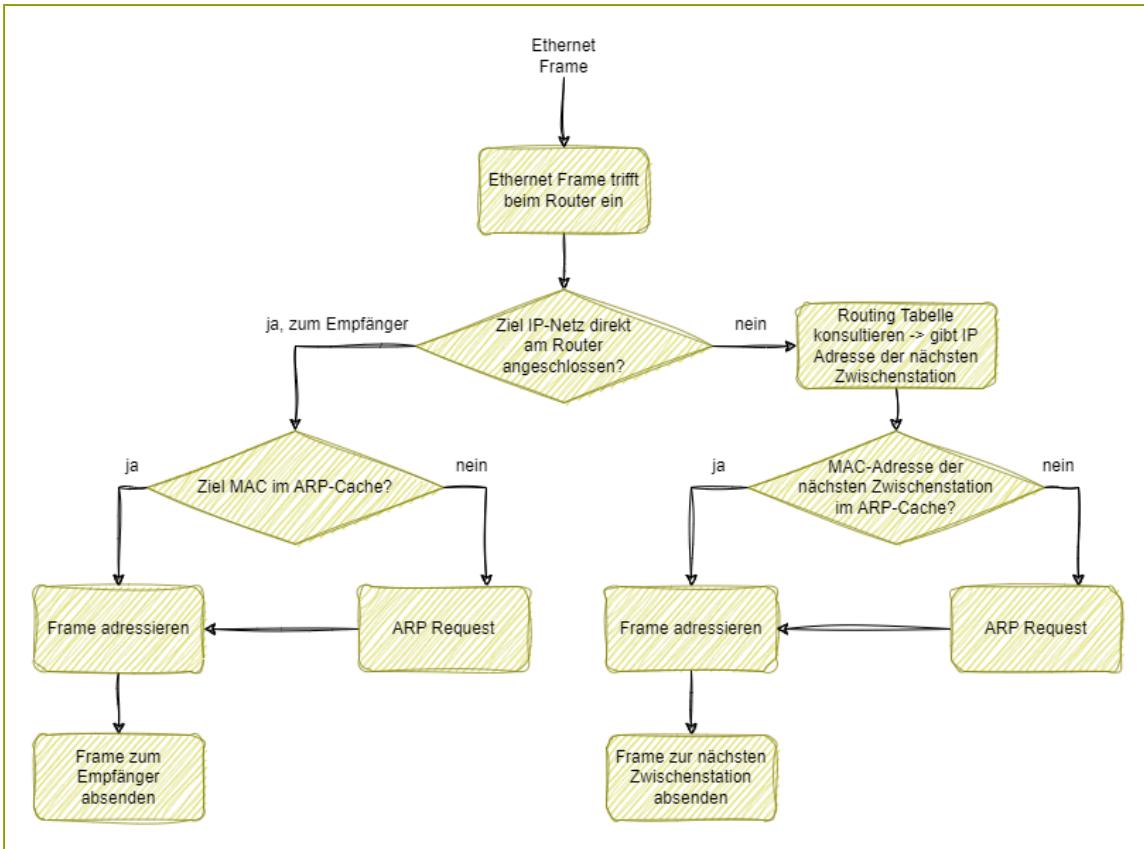


Abb. 5: Ist das Ziel IP-Netz nicht direkt am Router angeschlossen wird die Routingtabelle konsultiert

Frames neu adressieren

Wird ein Frame von einem IP-Netz in ein durch einen Router verbundenes zweites Netz gesendet, findet eine Neuadressierung der MAC-Adressen statt. Die IP-Adressen bleiben jedoch erhalten. Auf Teilstrecke 1 des Frames zum Router, ist die Ziel MAC-Adresse diejenige des Routers, da MAC-Adressen nur innerhalb desselben Netzes adressierbar sind. Erst auf Teilstrecke 2 hat man als Ziel MAC-Adresse diejenige des Zielcomputers, hingegen ist dort die Sender MAC-Adresse wiederum diejenige des Routers an Anschluss 2.

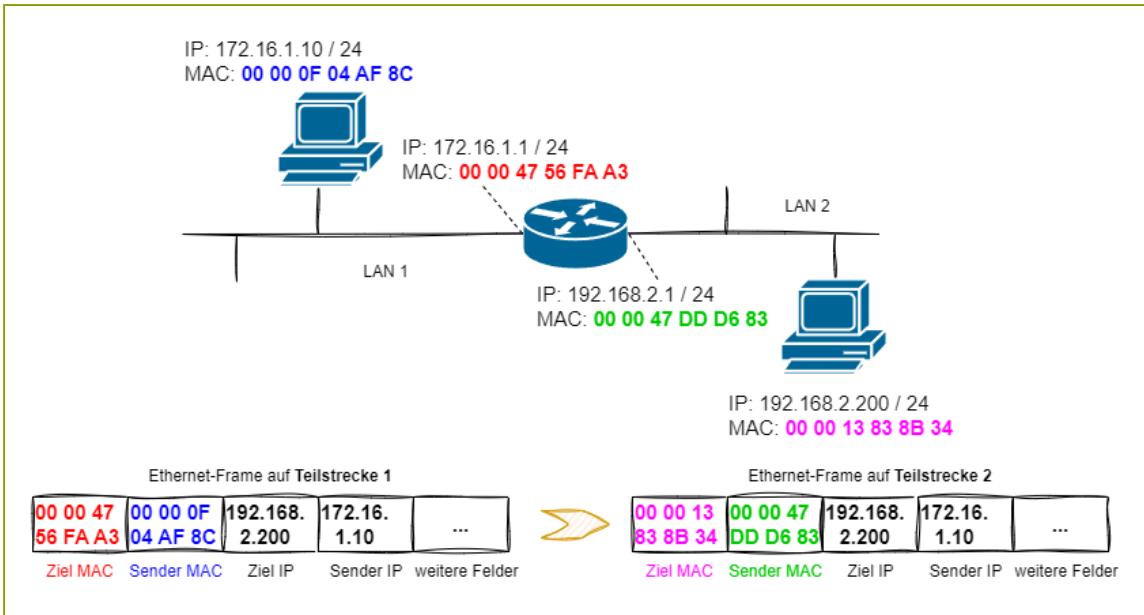


Abb. 6: Neuadressierung eines Ethernet-Frames beim Übergang in ein nächstes Netz

Frames umladen

Der Router hat quasi die Aufgabe einer Umladestation. Der Ablauf ist in den folgenden Schritten dargestellt:

1. Wenn ein Frame beim Router eintrifft wird aus der Ziel IP-Adresse die Ziel MAC-Adresse des nächsten Knoten bestimmt

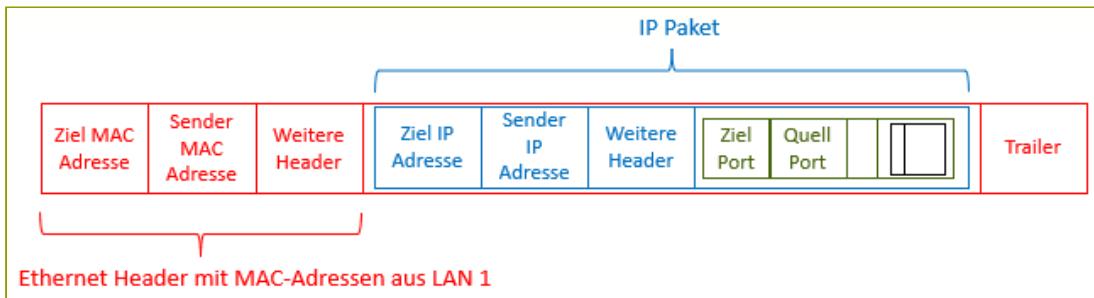


Abb. 7: Der Frame aus LAN 1 trifft beim Router ein

2. Mit der neuen Ziel MAC-Adresse wird ein neuer leerer Frame erstellt

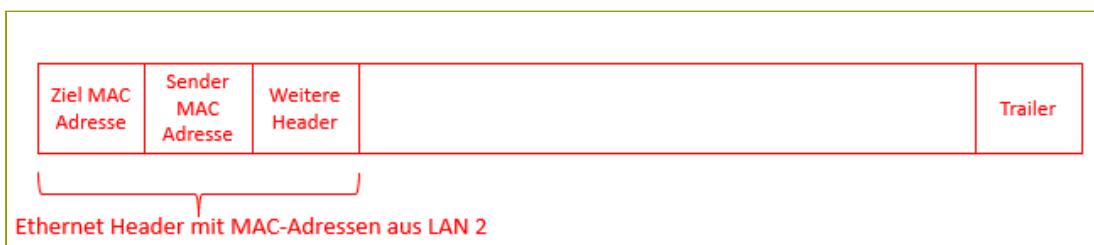


Abb. 8: Erstellt einen neuen Frame mit den MAC-Addressen für LAN 2

3. Zum Schluss wird das IP-Paket aus dem ursprünglichen Frame herausgelöst und im neuen Frame eingefügt

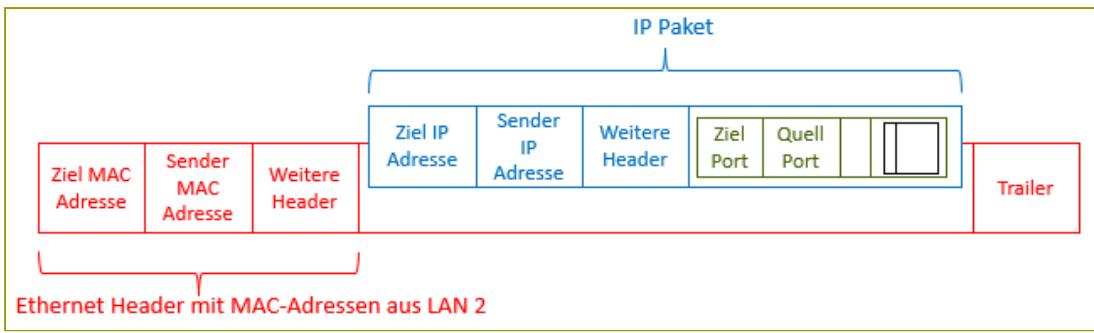


Abb. 9: Löst das IP Packet (blau) aus Frame 1 heraus und fügt es in Frame 2 ein

4. Anschliessen wird der Frame weitergesendet

Routingtabelle

Grundlagen

Jeder Router verfügt über eine sogenannte Routingtabelle, in der Netzwerkadressen und die dazugehörige nächste Zwischenstation festgehalten werden.

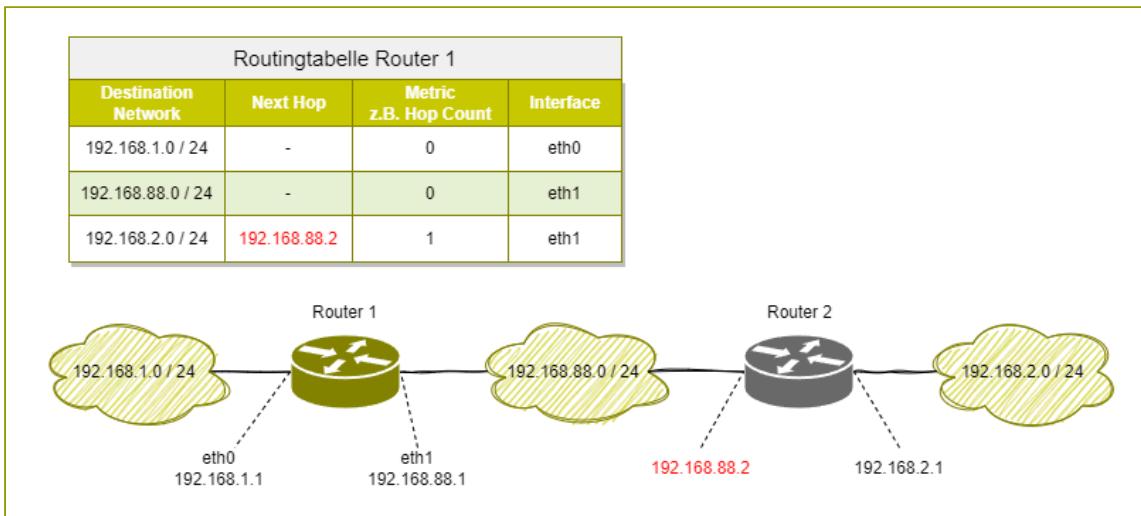


Abb. 1: Routing Tabelle von Router 1

Wie ist diese Routingtabelle zu interpretieren?

- ✓ **1. Zeile:** Erhält der Router ein Paket an das **Zielnetzwerk 192.168.1.0/24**, weiß er, dass dieses Netzwerk direkt an einem seiner Netzwerkanschlüsse angehängt ist. Er kann somit das Paket neuadressieren (MAC) und es direkt an die Zieladresse senden. Es gibt somit keine nächste Zwischenstation, deshalb bleibt die Spalte **Next Hop leer**. Die Anzahl der Zwischenstationen ist somit **0**, die Schnittstelle über die das Zielnetzwerk erreicht werden kann ist **eth0**.
- ✓ **2. Zeile:** Analog 1 Zeile. Erhält der Router ein Paket an das **Zielnetzwerk 192.168.88.0/24**, weiß er, dass dieses Netzwerk direkt an einem seiner Netzwerkanschlüsse angehängt ist. Er kann somit das Paket neuadressieren (MAC) und es direkt an die Zieladresse senden. Es gibt somit keine nächste Zwischenstation, deshalb bleibt die Spalte **Next Hop leer**. Die Anzahl der Zwischenstationen ist somit **0**, die Schnittstelle über die das Zielnetzwerk erreicht werden kann ist **eth1**.
- ✓ **3. Zeile:** Erhält der Router ein Paket an das **Zielnetzwerk 192.168.2.0/24**, kann er dieses nicht direkt an den Empfänger weiterleiten, da es ja in einem ihm unbekannten Netzwerk liegt. Die 3. Zeile besagt aber, dass die nächste Zwischenstation zum Ziel die IP-Adresse **192.168.88.2** ist, welche zum Router 2 gehört. Diese IP-Adresse ist befindet sich in einem

seiner eigenen Netzwerke. Somit kann er das Paket an diese IP-Adresse (Router 2) weiterleiten.

Der Weg zum endgültigen Ziel führt über einen zusätzlichen Router, deshalb ist der **Hop Count 1**. Das Paket muss über die Schnittstelle **eth1** gesendet werden.

Damit ist die Arbeit für Router 1 erledigt. Die Verantwortung für die weitere korrekte Zustellung liegt nun bei Router 2.

Zusammenfassend: Eine Routingtabelle enthält folgende Einträge

- ✓ **Zielnetzadresse:** Eintrag des Ziel-Netzes das erreicht werden soll
- ✓ **Next Hop:** IP-Adresse des nächsten Routers zum Ziel-Netz
- ✓ **Metric:** Ein Mass für die Güte eines Weges, häufig Hop Count, dh. Anzahl Zwischenstationen
- ✓ **Interface:** Schnittstelle über die das Paket weitergesendet wird

Router 2 hat natürlich seine eigene Routingtabelle die analog zur Routingtabelle von Router 1 aufgebaut ist. Insbesondere muss diese Routingtabelle einen Eintrag für das Netzwerk **192.168.1.0/24** haben. Sonst kann er zwar Anfragen aus diesem Netz korrekt zustellen, die Antworten würden aber ohne diesen Eintrag den Weg zurück nicht finden.

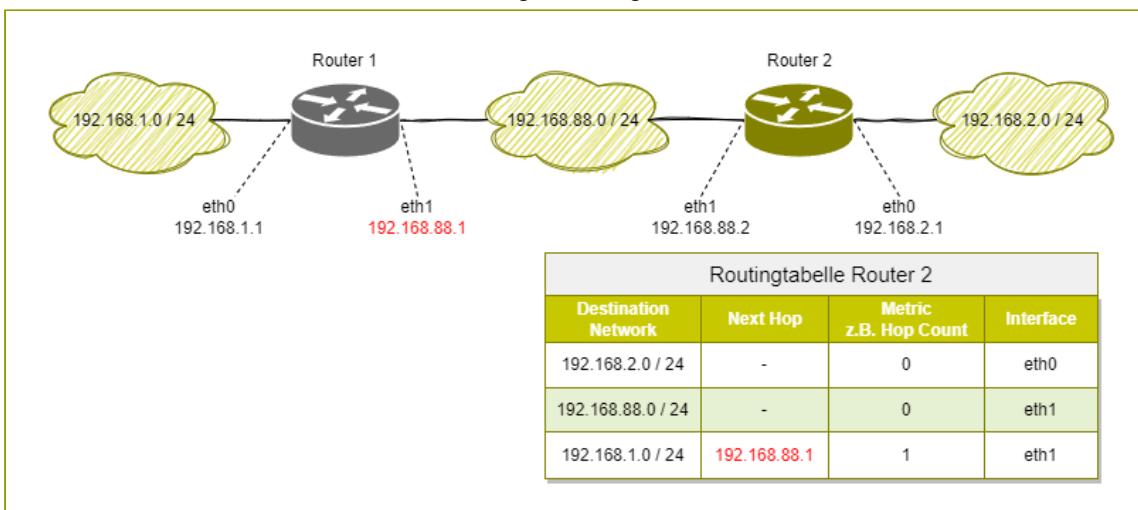


Abb. 2: Routing Tabelle von Router 2

Default Route

Ein Router kann natürlich nicht für sämtliche Netzwerke auf der Welt einen Eintrag in seiner Routingtabelle haben. Zu diesem Zweck gibt es die sogenannte Default Route (bezeichnet als 0.0.0.0/0). An den eingetragenen Next Hop werden sämtliche Pakete gesendet für die es in der Routingtabelle keinen spezifischen Eintrag gibt. Typischerweise sind das Adressen im Internet. Wird im gezeigten Beispiel eine Anfrage an den Google DNS-Server 8.8.8.8 gestellt besagt die Defaultroute, dass diese Anfrage über die IP-Adresse 192.168.88.2 weitergeleitet wird. Wie vorher ist für Router 1 die Arbeit erledigt, auch die Routingtabelle von Router 2 enthält

(hoffentlich) einen Eintrag für die Defaultroute und leitet die Anfrage zum Internetprovider weiter.

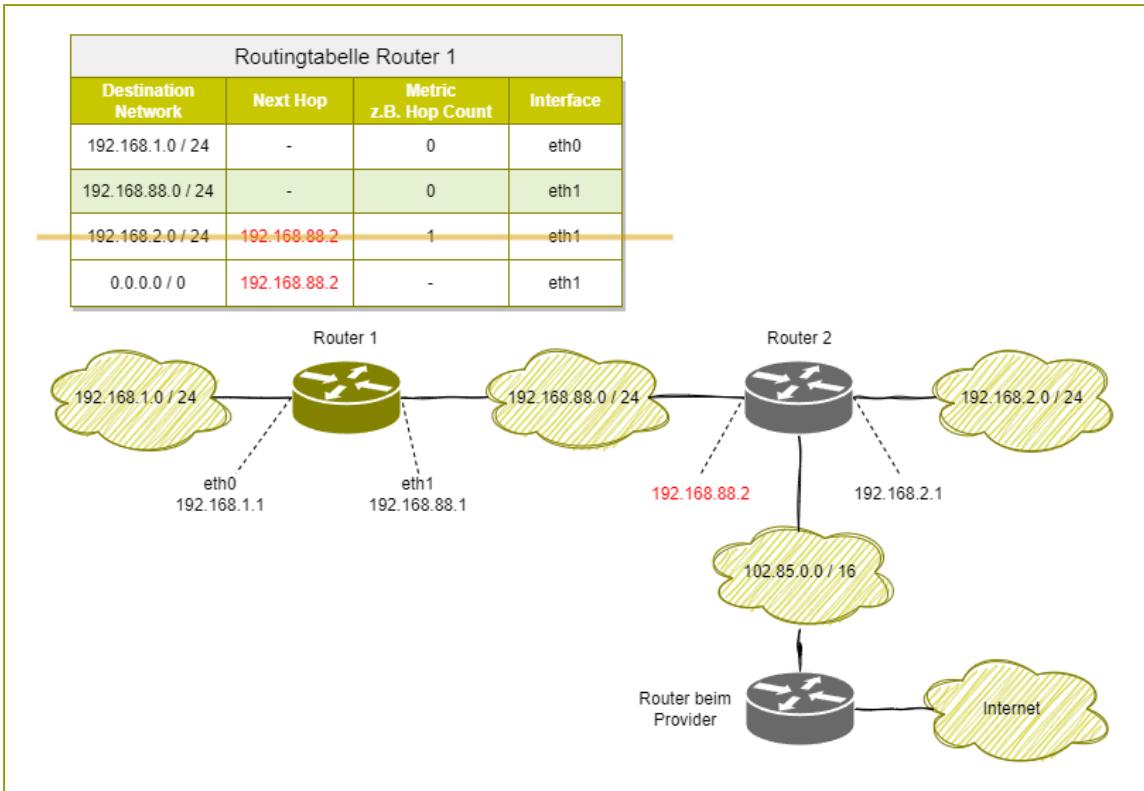


Abb. 3: Defaultroute Router 1

Bei der Defaultroute kann keine Metric angegeben werden, da ja nicht bekannt ist, wieviele Zwischenstationen bis zum Ziel durchlaufen werden.

Der urprüngliche Eintrag für das Netz 192.168.2.0/24 ist nicht mehr nötig, da dieses Netz und die Defaultroute denselben Next Hop haben. Netz 192.168.2.0/24 ist also durch 0.0.0.0/0 bereits mit abgedeckt. Der Eintrag kann somit gelöscht werden.

Bei Router 2 wird die Sache jetzt etwas komplizierter, da ja drei Netzwerke angeschlossen sind. Außerdem kann der Eintrag für das Netz 192.168.1.0/24 nicht gelöscht werden, da ja ansonsten Antworten aus dem Internet den Weg dorthin zurück nicht finden würden.

Routingtabelle Router 2			
Destination Network	Next Hop	Metric z.B. Hop Count	Interface
192.168.1.0 / 24	-	0	eth0
192.168.88.0 / 24	-	0	eth1
102.85.0.0 / 16	-	0	eth3
192.168.1.0 / 24	192.168.88.1	1	eth1
0.0.0.0 / 0	102.85.0.1	-	eth3

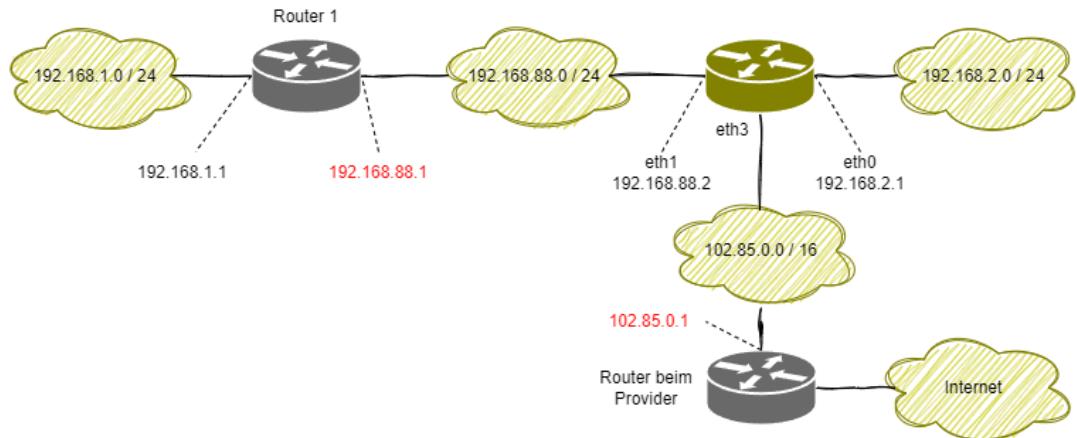


Abb. 3: Defaultroute Router 2

Statisches Routing

Wie wird nun eine Routingtabelle erstellt. Beim statischen Routing wird diese manuell aufgebaut und die korrekten Einträge durch den Administrator konfiguriert. Dieses Vorgehen ist natürlich nur bei einer begrenzten Anzahl Routern und Netzwerken möglich, da sich der administrative Aufwand ab einer bestimmten Größe nicht mehr lohnt und die Fehleranfälligkeit stark ansteigt. Trotzdem muss man wissen, wie in einfacheren Fällen eine Routintabelle aufgebaut wird.

Routingtabelle aus dem Netzwerkschema ableiten

Folgendes Vorgehen hat sich für das Erstellen einer Routingtabelle bewährt:

1. Direkt angeschlossene Netzwerke eintragen
2. Netzwerke hinter benachbarten Routern eintragen
3. Netzwerke hinter übernächsten Routern eintragen
4. usw.
5. Default Route eintragen
6. Einträge mit dem selben Next Hop wie die Default Route können gelöscht werden

Diese 6 Schritte werden hier an diesem Beispiel demonstriert. Die Netzwerke zwischen den Routern sind für die Übersichtlichkeit nicht mehr eingezeichnet. Als Subnetzmasken werden die Standardklassen A, B, C verwendet.

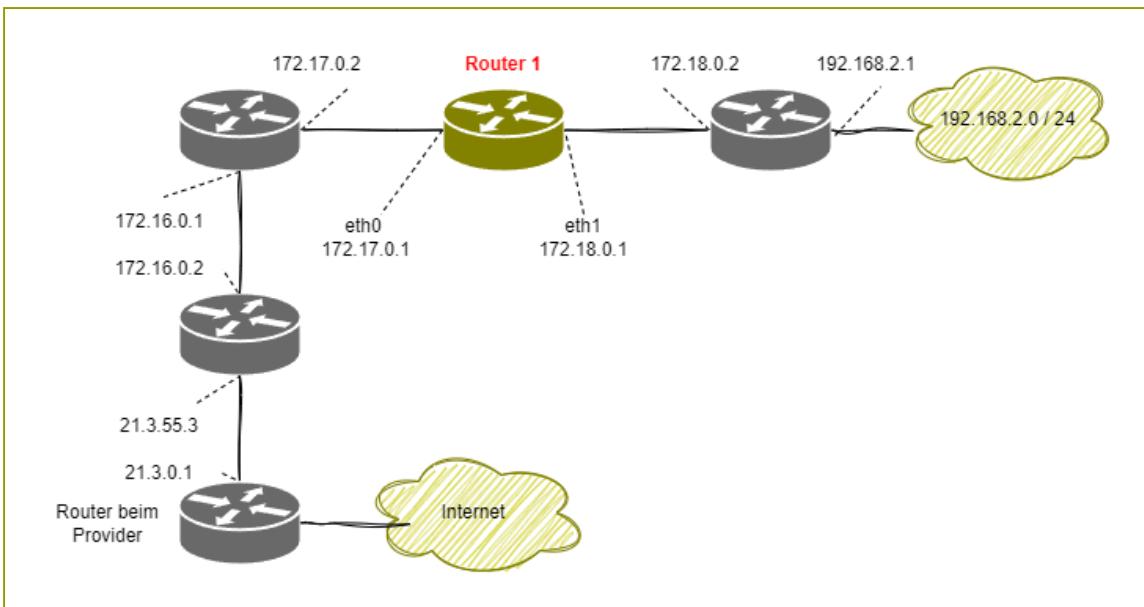


Abb. 3: Routingtabelle für Router 1 aufbauen

Schritt 1: Direkt angeschlossene Netzwerke eintragen.

Destination Network	Next Hop	Metric	Schnittstelle
172.17.0.0/16	-	0	eth0
172.18.0.0/16	-	0	eth1

Schritt 2: Netzwerke hinter benachbarten Routern eintragen.

Destination Network	Next Hop	Metric	Schnittstelle
172.17.0.0/16	-	0	eth0
172.18.0.0/16	-	0	eth1
172.16.0.0/16	172.17.0.2	1	eth0
192.168.2.0/24	172.18.0.2	1	eth1

Schritt 3: Netzwerke hinter übernächsten Routern eintragen

Destination Network	Next Hop	Metric	Schnittstelle
172.17.0.0/16	-	0	eth0
172.18.0.0/16	-	0	eth1
172.16.0.0/16	172.17.0.2	1	eth0
192.168.2.0/24	172.18.0.2	1	eth1
21.0.0.0/8	172.17.0.2	2	eth0

Schritt 4: usw. Hier gibt es keine Router mehr die der eigenen Kontrolle unterliegen, also hier Schluss

Schritt 5: Default Route eintragen

Destination Network	Next Hop	Metric	Schnittstelle
172.17.0.0/16	-	0	eth0
172.18.0.0/16	-	0	eth1
172.16.0.0/16	172.17.0.2	1	eth0
192.168.2.0/24	172.18.0.2	1	eth1
21.0.0.0/8	172.17.0.2	2	eth0
0.0.0.0/0	172.17.0.2	-	eth0

Schritt 6: Einträge mit dem selben Next Hop wie die Default Route können gelöscht werden
Diese sind die 3. und 5. Zeile. Die fertige Routingtabelle für Router 1 sieht also so aus:

Destination Network	Next Hop	Metric	Schnittstelle
172.17.0.0/16	-	0	eth0
172.18.0.0/16	-	0	eth1

Destination Network	Next Hop	Metric	Schnittstelle
192.168.2.0/24	172.18.0.2	1	eth1
0.0.0.0/0	172.17.0.2	-	eth0

Netzwerkschema aus der Routingtabelle ableiten

Aus der Routingtabelle eines Routers kann umgekehrt bis zu einem gewissen Grad das Netzwerkschema abgeleitet werden. Auch hier bewährt sich ein schrittweises Vorgehen:

1. Router um dessen Routingtabelle es geht einzeichnen
2. Netzwerke ohne Next Hop sind direkt angeschlossen, das loopback-Netzwerk kann weggelassen werden
3. Schnittstellen beschriften
4. Router am anderen Ende der Netzwerke einzeichnen
5. IP-Adressen der Next Hops einzeichnen
6. Netzwerke und Router hinter Next Hops einzeichnen, Hop Count berücksichtigen

Als Beispiel sehen wir folgende Routingtabelle an und leiten daraus das Netzwerkschema ab:

Destination Network	Next Hop	Hop Count	Schnittstelle
217.162.112.0/24	-	0	eth0
192.168.1.0/24	-	0	eth1
127.0.0.0/8	-	0	lo
192.168.20.0/24	192.168.1.254	1	eth1
0.0.0.0/0	217.162.112.1	-	eth0

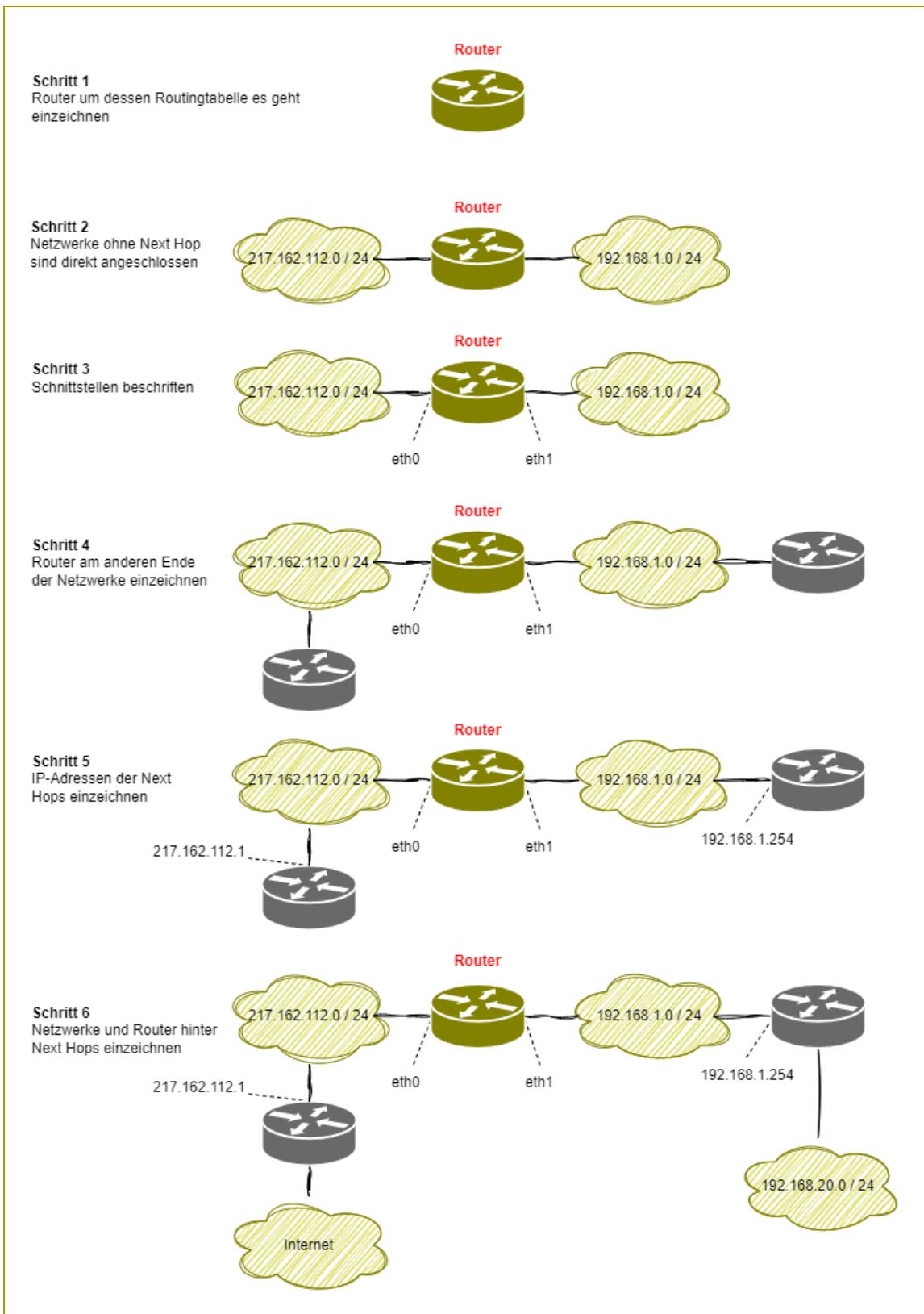


Abb. 3: Netzwerkschema aus der Routingtabelle ableiten

Wichtige Kommandos

Routingtabelle anzeigen:

Windows

```
c:\> route print
```

Linux (Ubuntu)

```
vmadmin@lp-22-04:~$ ip route
```

Cisco

```
Router> show ip route
```

Statische Route hinzufügen

Windows

```
c:\> route add 172.16.0.0 mask 255.255.0.0 192.168.10.1
```

Linux (Ubuntu)

```
vmadmin@lp-22-04:~$ sudo ip route add 172.16.0.0/16 via 192.168.10.1
```

Cisco

```
Router(config)# ip route 172.16.0.0 255.255.0.0 192.168.10.1
```

Default Route eintragen

Windows

```
c:\> route add 0.0.0.0 mask 0.0.0.0 161.99.1.1
```

Linux (Ubuntu)

```
vmadmin@lp-22-04:~$ sudo ip route add 0.0.0.0/0 via 161.99.1.1
```

Cisco

```
Router(config)# ip route 0.0.0.0 0.0.0.0 161.99.1.1
```

Statische Route löschen

Windows

```
c:\> route del 172.16.0.0 mask 255.255.0.0
```

Linux (Ubuntu)

```
vmadmin@lp-22-04:~$ sudo ip route del 172.16.0.0/16
```

Cisco

```
Router(config)# no ip route 172.16.0.0 255.255.0.0
```

Bei Windows und Linux sind die so gemachten Einträge nicht permanent, sondern gehen beim Neustart verloren. Alle Kommandos bieten ausserdem viele weitere Optionen an (Referenz konsultieren).

Bei Cisco muss mit enable, und configure in den Rootmodus gewechselt werden:

```
Router> enable  
Router# configure terminal  
Router(config)#
```

Dynamisches Routing

Sobald die Anzahl der zu verwaltenden Router grösser wird, ist statisches Routing nicht mehr praktikabel da der administrative Aufwand um die Routingtabellen aller Router korrekt zu definieren viel zu gross wird. An dieser Stelle kommt das sogenannte dynamische Routing zum Zug, bei dem die Router ihre Routingtabellen selbstständig aufbauen.



Dynamisches Routing und Routingtabellen

Auch beim dynamischen Routing definieren die Routingtabellen, wohin die IP-Pakete weitergeleitet werden. Im Unterschied zum statischen Routing werden diese jedoch automatisch aufgebaut.

Der wesentliche Vorteil des dynamischen Routing gegenüber dem statischen liegt darin, dass die Wegwahl dynamisch ist, also bei laufendem Netzbetrieb erfolgt, und Netzerweiterungen, Laständerungen und Überlastungen vom Routing-Algorithmus berücksichtigt werden.

Dynamisches Routing beschreibt in der Netzwerktechnik die Fähigkeit von Routing-Algorithmen, selbstständig neue Routen zu finden, um beispielsweise ein beschädigtes, überlastetes oder fehlendes Netzwerkelement zu umgehen. Ändern sich die Verhältnisse im Netzwerk zu einem späteren Zeitpunkt – etwa durch Ausfall oder Überlastung eines Verbindungselements – können diese Systeme automatisch darauf reagieren.

Beim dynamischen Routing fliessen Metriken in die Entscheidungsfindung ein. Dabei können verschiedene Metriken wie Länge, Sicherheit oder Kosten berücksichtigt werden. Hinzu kommen Netzwerkeigenschaften wie Bandbreite, die Übertragungsverzögerung oder der Hop Count. Ziel ist oft die Netzlast gleichmässig zu verteilen, also auch unausgelastete Nebenstrecken in die Datenübertragung miteinzubeziehen.

Dynamisches Routing erfordert im Vergleich zu statischem Routing aufgrund der selbständigen Informationsverarbeitung einen geringeren Verwaltungsaufwand. Hingegen funktioniert statisches Routing oft stabiler, unter anderem weil das Netz beim adaptiven Routing zusätzlich mit Routinginformationen belastet wird. In vielen Netzwerken kommt heute daher eine Mischstrategie zum Einsatz.

Über spezielle Routingprotokolle tauchen die Router untereinander Erreichbarkeitsdaten aus:

Folgende Routingprotokolle sind dazu im Einsatz:



- Interior Gateway Protokolle (IGP): für grosse Unternehmensnetzwerke, dazu gehören:

- ✓ OSPF (**O**pen **S**hortest **P**ath **F**irst)
- ✓ RIP (**R**outing **I**nformation **P- ✓ IS-IS (**I**ntermediate **S**ystem to **I**ntermediate **S**ystem)
- ✓ **E**xterior **G**ateway **P**rotokolle (EGP): für Router im Internet, dazu gehören:
 - ✓ BGP (**B**order **G**ateway **P**rotocol)**

RIP

Beim RIP- Protokoll schicken alle Router in Intervallen ihre eigenen Routingtabellen als Broadcast an die anderen Router. Die Entfernung zu anderen Netzwerken wird dabei in Relation, d.h. aus der Sichtweise der eigenen Routing-Tabelle angegeben. Auf der Basis der empfangenen Tabellen berechnen die Router die kürzesten übermittelten Entfernung zu jedem Zielnetz und nehmen den Nachbar-Router, der diese Entfernung bekannt gegeben hat, als Ziel-Router zur Weiterleitung. Das RIP-Protokoll gibt es in zwei Versionen: RIP und RIPv2

OSPF

OSPF ist vielleicht das am häufigsten verwendete Interior Gateway Protocol in grossen Unternehmensnetzen. Die Hauptvorteile von OSPF gegenüber RIP bestehen in der schnelleren Konvergenz (d.h. benötigte Zeit um die Routingtabellen aufzubauen) und der besseren Skalierbarkeit für grössere Netzwerke.

Routertypen

Geräte die nur die Routingfunktion unterstützen gibt es eigentlich nicht. Alle Geräte stellen eine Kombination aus unterschiedlichen Funktionen wie WLAN, Modem, Switch, VPN-Server, LTE und Firewall dar. Entsprechend uneinheitlich sind die Bezeichnungen der verschiedenen Routertypen

WLAN-Router

Die Kombination aus Wireless Access Point, Switch und Router wird häufig als WLAN-Router bezeichnet. Das Routing findet zwischen den mindestens zwei Netzen, meist dem WLAN und WAN statt (und falls vorhanden zwischen LAN und WAN). Die LAN Ports sind in der Regel nicht eigenständische IP-Netze, sondern Switch Ports ein und desselben IP Netzwerkes.

(Quelle: [Wikipedia Router](#))



DSL-Router

Ein Router, der einen PPPoE-Client zur Einwahl in das Internet via xDSL eines ISPs beinhaltet und gegenwärtig Network Address Translation (NAT) in IPv4-Netzen zur Umsetzung einer öffentlichen IPv4-Adresse auf die verschiedenen privaten IPv4-Adressen des LANs beherrscht, wird als DSL-Router bezeichnet. Häufig sind diese DSL-Router als Multifunktionsgeräte mit einem Switch, einem WLAN Access Point, nicht selten mit einer kleinen TK-Anlage, einem VoIP-Gateway oder einem DSL-Modem (xDSL jeglicher Bauart) ausgestattet.

(Quelle: [Wikipedia Router](#))



Edge-Router

Wie der Name schon sagt, befindet sich ein Edge-Router am Rand oder an der Grenze eines

Netzwerks, in der Regel verbunden mit dem Netzwerk eines Internet Service Providers (ISP) oder einer anderen Organisation, und er verteilt Pakete über mehrere Netzwerke. Häufig unterstützen solche Geräte den Aufbau von VPN-Verbindungen und werden dann als VPN-Router bezeichnet.

(Quelle: [computerweekly](#))



Backbone-Router

Die Hochgeschwindigkeitsrouten (auch Carrier-Class-Router) im Internet (oder bei großen Unternehmen) sind heute hochgradig auf das Weiterleiten von Paketen optimierte Geräte, die viele Terabit Datendurchsatz pro Sekunde in Hardware routen können. Die benötigte Rechenleistung wird zu einem beträchtlichen Teil durch spezielle Netzwerkinterfaces dezentral erbracht, ein zentraler Prozessor (falls überhaupt vorhanden) wird nicht oder nur sehr wenig belastet. Die einzelnen Ports oder Interfaces können unabhängig voneinander Daten empfangen und senden. Sie sind entweder über einen internen Hochgeschwindigkeitsbus (Backplane) oder kreuzweise miteinander verbunden (Matrix).

Meist sind solche Geräte für den Dauerbetrieb ausgelegt (Verfügbarkeit von 99,999 % oder höher) und besitzen redundante Hardware (Netzteile), um Ausfälle zu vermeiden.

(Quelle: [Wikipedia Router](#))



LTE-Router

LTE-Router verfügen über einen Slot zur Aufnahme einer SIM-Karte. Die Internetverbindung der verwendeten SIM-Karte wird von einem LTE-Router per WLAN an weitere Geräte bereitgestellt. Einige LTE-Router bieten zusätzlich die Möglichkeit, Geräte auch über einen RJ45-Anschluss per Netzwerkkabel zu verbinden. Es existieren LTE-Router für den mobilen Einsatz, die über einen eingebauten Akku verfügen und ohne einen Stromanschluss betrieben werden können.

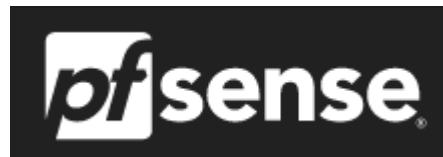
(Quelle: [Wikipedia LTE-Modem](#))



Virtuelle Router

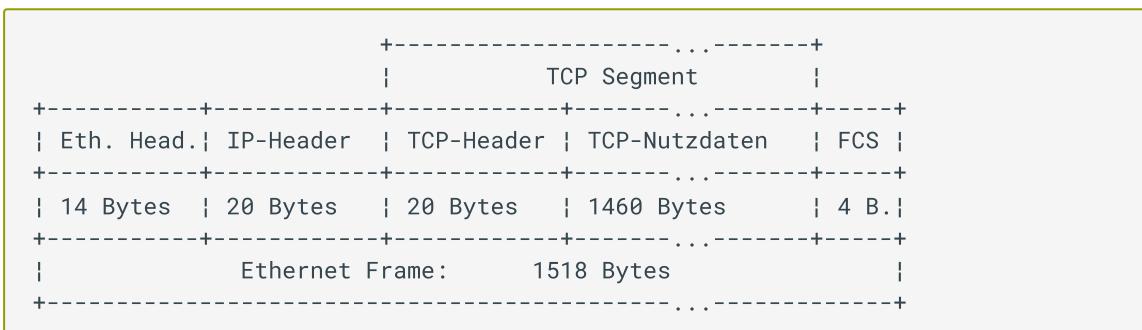
Ein virtueller Router, kurz vRouter, übernimmt die Funktionalität eines Routers in einem virtuellen Format, anstatt ein dediziertes Hardwaregerät zu nutzen. Er wird insbesondere in Netzwerken mit virtuellen Maschinen genutzt und verbindet zwei oder mehr virtuelle Netzwerke oder das virtuelle mit dem physischen Netzwerk. Außerdem können mehrere zusammengeschlossene Router zur Redundanz eine virtuelle Routerinstanz abbilden.

(Quelle: [Wikipedia Router](#))



TCP

Das Transmission Control Protocol (TCP) gehört zusammen mit UDP, SCTP oder QUIC zur Gruppe der Transportprotokolle auf Layer 4 des OSI-Modells. Es erlaubt den Aufbau einer Verbindung, welche eine beidseitige Datenübermittlung zulässt. Die grundlegende Übertragungseinheit sind die Segmente. Die Grösse der Segmente richtet sich nach der Grösse der darunterliegenden Einheiten IP-Paket und Ethernetframe.



Wie man sieht beträgt die Segmentgrösse 1480 Bytes, für die Nutzdaten bleiben damit 1460 Bytes übrig. Diese Grösse wird auch als MSS (Maximum Segment Size) bezeichnet.

Aufgaben von TCP

- ✓ Segmentierung (Data Segmenting): Dateien oder Datenstrom in Segmente teilen, Reihenfolge der Segmente wieder herstellen und zu Dateien oder einem Datenstrom zusammensetzen
- ✓ Verbindungsmanagement (Connection Establishment and Termination): Verbindungsaufbau und Verbindungsabbau
- ✓ Fehlerbehandlung (Error Detection): Bestätigung von Datenpaketen und Zeitüberwachung
- ✓ Flusssteuerung (Flow Control): Dynamische Auslastung der Übertragungsstrecke
- ✓ Anwendungsunterstützung (Application Support): Adressierung spezifischer Anwendungen und Verbindungen durch Port-Nummern

Segmentierung

Eine Funktion von TCP besteht darin, den von den Anwendungen kommenden Datenstrom in Datenpakete bzw. Segmente aufzuteilen (Segmentierung) und beim Empfang wieder zusammenzusetzen. Die Segmente werden mit einem Header versehen, in dem Steuer- und Kontroll-Informationen enthalten sind. Danach werden die Segmente an das Internet Protocol

(IP) übergeben. Da beim IP-Routing die Datenpakete unterschiedliche Wege gehen können, entstehen unter Umständen zeitliche Verzögerungen, die dazu führen, dass die Datenpakete beim Empfänger in einer anderen Reihenfolge eingehen, als sie ursprünglich hatten. Deshalb werden die Segmente beim Empfänger auch wieder in die richtige Reihenfolge gebracht und erst dann an die adressierte Anwendung übergeben. Dazu werden die Segmente mit einer fortlaufenden Sequenznummer versehen (Sequenzierung).

Segmentierung ist nicht zu verwechseln mit der **Fragmentierung** auf IP-Ebene. Fragmentation ist im Allgemeinen nicht erwünscht, da es grösste Performance Probleme mit sich bringt.

TCP-Header

Der TCP-Header hat die folgende Struktur:

	source port		destination port	1.	-
4. Byte					
	sequence number			5.	-
8. Byte					
	acknowledgment number			9.	-
12. Byte					
	offset res. flags		window	13.	-
16. Byte					
	checksum		urgent pointer	17.	-
20. Byte					
	options (optional)			max.	
+40 Bytes					

- ✓ **source port:** Quellport: 2 Bytes, dh. max 65535
- ✓ **destination port:** Zielport: 2 Bytes, dh. max 65535
- ✓ **sequence number:** Wird benötigt um die Segmente wieder in der richtigen Reihenfolge zusammenzusetzen
- ✓ **acknowledgment number:** Zur Bestätigung, dass die Segmente angekommen sind
- ✓ **offset:** Grösse des Headers
- ✓ **reserved:** Für zukünftige Entwicklungen reserviert, im Moment immer 0
- ✓ **flags:** Flags für den Verbindungsaufbau und -abbau (URG, ACK, PSH, RST, SYN, FIN)
- ✓ **window:** Für die Datenflusssteuerung
- ✓ **checksum:** Zur Kontrolle der Daten

- ✓ **urgent pointer:** Datenbereich ab dem die Urgent-Daten aufhören (diese kommen direkt nach dem Header)

Bekanntermassen ist TCP ein zuverlässiges Protokoll, dh. das Protokoll stellt sicher, dass alle Daten vollständig übertragen werden (im Gegensatz zu UDP). Die zu diesem Zweck relevanten Header-Daten sind die Sequenznummer und die Acknowledgment Nummer. Bildlich lässt sich dieses Verfahren so skizzieren:

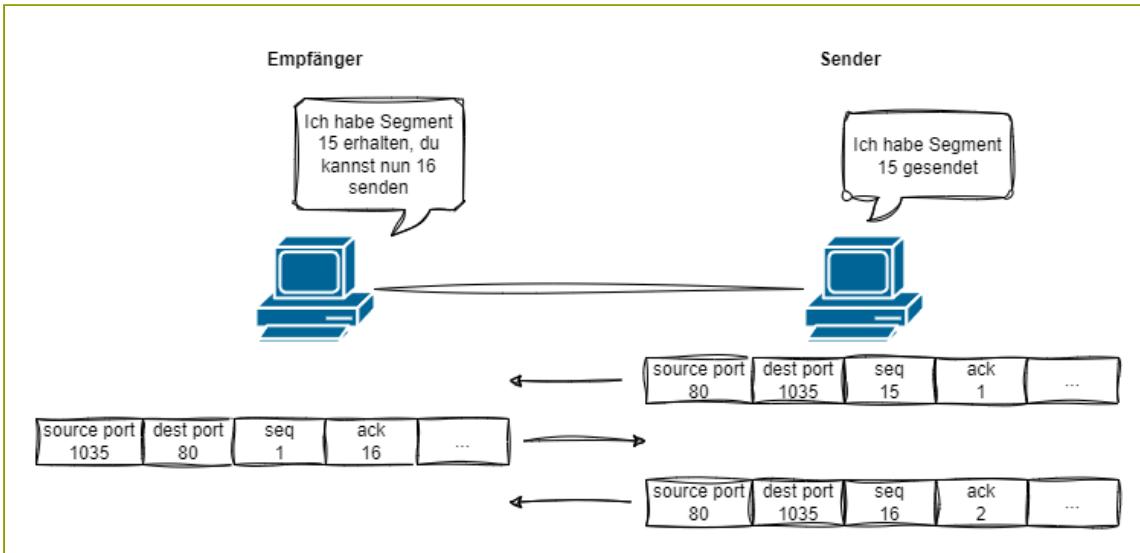


Abb. 1: Sequenznummer und die Acknowledgment Nummer

Die Sequenznummern und die Acknowledgment Nummer laufen in beide Richtungen unabhängig voneinander. So ist z. B. ist der Sender schon bei Sequenznummer 15 angelangt, während der Empfänger erst bei der Sequenznummer 1 steht.

Die Darstellung ist jedoch vereinfacht. Die Segmente werden nicht nummeriert, sondern die Anzahl der übertragenen Bytes angegeben. Die folgende Abbildung stellt den Sachverhalt etwas genauer dar. Man sieht auch, dass nicht jedes Segment einzeln bestätigt wird, sondern die jeweils erhaltene Datenmenge insgesammt. Wird ein Segment nicht bestätigt (im Bild Nr. 3), wird es nach einem Timeout erneut gesendet.

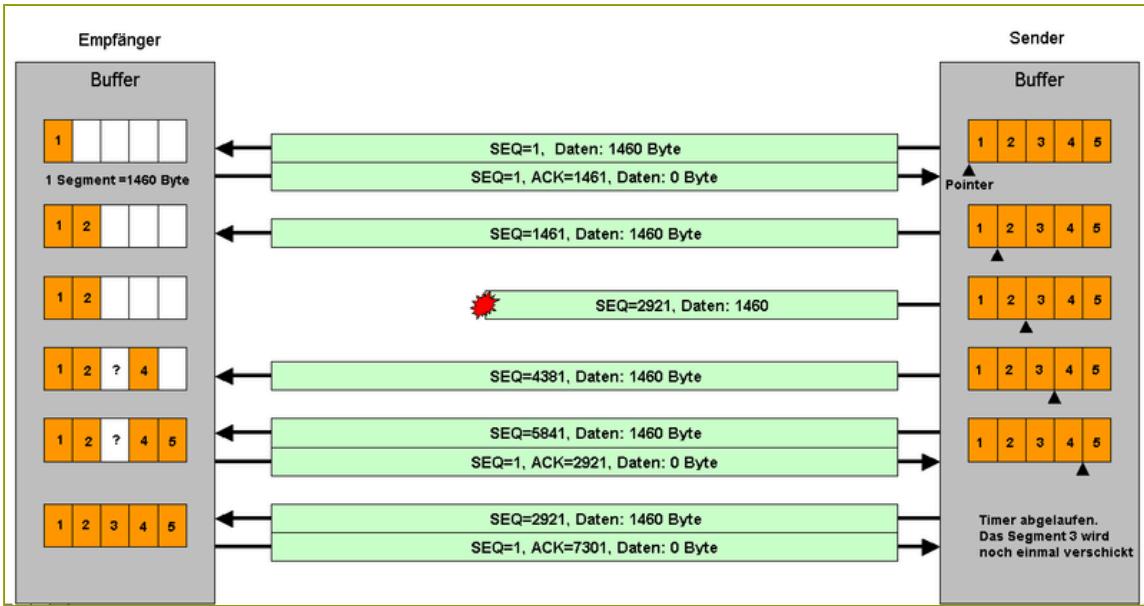
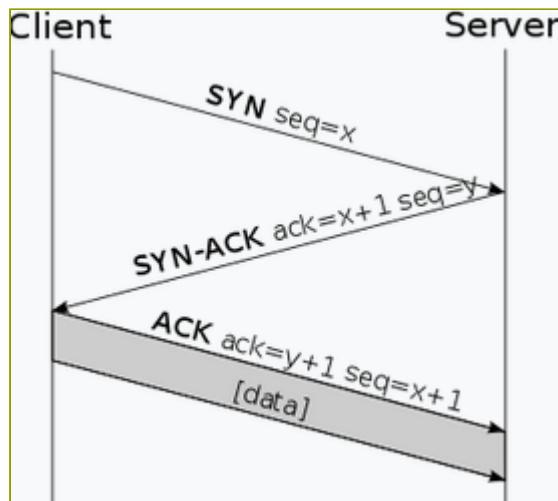


Abb. 2: Sequenznummer und die Acknowledgment Nummer detailliert (Quelle: Wikipedia)

Verbindungsauftau



Der Client, der eine Verbindung aufbauen will, sendet dem Server ein SYN-Segment mit einer Sequenznummer x . Es handelt sich also um ein Segment, dessen SYN-Bit im Paketkopf gesetzt ist (siehe TCP-Header). Die Start-Sequenznummer ist eine beliebige Zahl x . Sie sollte jedoch möglichst zufällig sein, um Sicherheitsrisiken zu vermeiden.

Der Server empfängt das Segment. Ist der Port geschlossen, antwortet er mit einem TCP-RST, um zu signalisieren, dass keine Verbindung aufgebaut werden kann. Ist der Port geöffnet,

bestätigt er den Erhalt des ersten SYN-Segmentes und stimmt dem Verbindungsauftau zu, indem er ein SYN/ACK-Segment zurückschickt. Das gesetzte ACK-Flag im TCP-Header kennzeichnet diese Segmente, welche die Sequenznummer $x+1$ des SYN-Segment im Header enthalten. Zusätzlich sendet er im Gegenzug seine Start-Sequenznummer y , die ebenfalls beliebig und unabhängig von der Start-Sequenznummer des Clients ist.

Der Client bestätigt zuletzt den Erhalt des SYN/ACK-Segment durch das Senden eines eigenen ACK-Segment mit der Sequenznummer $x+1$. Aus Sicherheitsgründen sendet der Client den Wert $y+1$ (die Sequenznummer des Servers + 1) im ACK-Segment zurück. Die Verbindung ist damit aufgebaut.

Der ganze Ablauf wird als **Three-Way-Handshake** bezeichnet.

(Quelle: [Wikipedia](#))

Ports

Wie in den darunterliegenden Header von iP und Ethernet gibt es bei TCP immer einen Empfänger und einen Absender. Die Adressen werden als sogenannte Ports angegeben. Wenn ein Webbrower von einem Webserver um Daten bittet (eine Webseite) richtet er seine Anfrage an den Zielport 80 (bzw. 443 bei HTTPS), als Absenderport wird ein vom Betriebssystem zufällig gewählter Wert oberhalb von 1023 gewählt. Anhand des Quellportes identifiziert der Webserver eine Verbindung eines Clients.

Die verwendeten Ports lassen sich mit dem netstat Kommando anzeigen

```
netstat -n -p TCP
  Proto Lokale Adresse      Remoteadresse      Status
  TCP    192.168.1.105:52719 52.123.128.14:443  HERGESTELLT
  TCP    192.168.1.105:52722 52.98.219.34:443  HERGESTELLT
  TCP    192.168.1.105:52723 51.104.167.186:443 HERGESTELLT
  TCP    192.168.1.105:52724 23.214.205.186:443 HERGESTELLT
  TCP    192.168.1.105:52726 34.107.243.93:443 HERGESTELLT
  ...
```

Hier handelt es sich offensichtlich um HTTPS Verbindungen (Port 443) von einem Client 192.168.1.105. Die Zahlen 52719, etc. sind die Quellports.

Die Ports für wichtige Dienste sind festgelegt

Serverport	Protokoll	Anmerkung
20/tcp	FTP-Daten	File Transfer Protocol (Daten)
21/tcp	FTP-Kommandos	File Transfer Protocol (Befehle)
22/tcp	SSH	Secure Shell
23/tcp	TELNET	Telecommunication Network
25/tcp	SMTP	Simple Mail Transfer Protocol (E-Mail)
53/tcp	DNS	Domain Name System (Namensauflösung)
53/udp	DNS	Domain Name System (Namensauflösung)

Serverport	Protokoll	Anmerkung
80/tcp	HTTP	Hypertext Transfer Protocol (Webseiten)
110/tcp	POP3	Post Office Protocol V3 (E-Mail)
123/tcp	NTP	Network Time Protocol
143/tcp	IMAP2	Interactive Mail Access Protocol V2 (E-Mail)
161/tcp	SNMP	Simple Network Management Protocol
194/tcp	IRC	Internet Relay Chat
220/tcp	IMAP3	Interactive Mail Access Protocol V3 (E-Mail)
443/tcp	HTTPS	Secure HTTP (sichere Webseiten)
465/tcp		Message Submission over TLS protocol
587/tcp		Message Submission with STARTTLS
631/tcp	IPP	Internet Printing Protocol
993/tcp	IMAPS	Internet Message Access Protocol over TLS/SSL

UDP

Einsatz

UDP ist ein verbindungsloses, nicht-zuverlässiges und ungesichertes wie auch ungeschütztes Übertragungsprotokoll. Das bedeutet, es gibt keine Garantie, dass ein einmal gesendetes Paket auch ankommt, dass Pakete in der gleichen Reihenfolge ankommen, in der sie gesendet wurden, oder dass ein Paket nur einmal beim Empfänger eintrifft. Es gibt auch keine Gewähr dafür, dass die Daten unverfälscht oder unzugänglich für Dritte beim Empfänger eintreffen. Eine Anwendung, die UDP nutzt, muss daher gegenüber verlorengegangenen und unsortierten Paketen unempfindlich sein oder selbst entsprechende Korrekturmassnahmen und ggf. auch Sicherungsmassnahmen vorsehen.

Da vor Übertragungsbeginn nicht erst eine Verbindung aufgebaut werden muss, kann ein Partner oder können beide Partner schneller mit dem Datenaustausch beginnen. Das fällt vor allem bei Anwendungen ins Gewicht, bei denen nur kleine Datenmengen ausgetauscht werden müssen. Einfache Frage-Antwort-Protokolle wie DNS (das Domain Name System) verwenden zur Namensauflösung hauptsächlich UDP, um die Netzwerkbela stung gering zu halten und damit den Datendurchsatz zu erhöhen. Ein Drei-Wege-Handschlag wie bei TCP für den Aufbau der Verbindung würde in diesem Fall unnötigen Overhead erzeugen.

Daneben bietet die ungesicherte Übertragung auch den Vorteil von geringen Übertragungsverzögerungsschwankungen: Geht bei einer TCP-Verbindung ein Paket verloren, wird es automatisch neu angefordert. Das braucht Zeit, die Übertragungsdauer kann daher schwanken, was für Multimediaanwendungen schlecht ist. Bei VoIP z. B. käme es zu plötzlichen Aussetzern, bzw. die Wiedergabepuffer müssten grösser angelegt werden. Bei verbindungslosen Kommunikationsdiensten bringen verlorengegangene Pakete dagegen nicht die gesamte Übertragung ins Stocken, sondern vermindern lediglich die Qualität.

Somit ergeben sich für UDP folgende Einsatzgebiete:

- ✓ Wenn die Sicherheit der Übertragung weniger wichtig ist als die Geschwindigkeit der Übertragung, z. B. bei Streaming von Audio oder Video. Dort zeigt sich ein fehlendes Paket lediglich durch einen leichten Knackser oder einen kleinen Bildfehler.
- ✓ Wenn die Funktionen einer sicheren, zuverlässigen Kommunikation durch beteiligte Anwendungen selbst übernommen werden, z. B. bei einer Bankensoftware oder einer anderen Anwendung mit kritischen Transaktionen

UDP Header

Der UDP-Header ist entsprechend einfach, ausser Quell- und Zielport gibt es nur noch ein Feld für die Länge des Datagrammes und eine Checksumme

	source port		destination port		1.	-
4. Byte						
	Länge		Check-Summe		5.	-
8. Byte						

Befehle und Werkzeuge

Die folgende Tabelle stellt nützliche Hilfsmittel um Fehler einzugrenzen zusammen:

Hilfsmittel	OSI-Layer	Erläuterungen
Visuelle Inspektion	1	- Kabel und Stecker ok? - Richtige Kabel verwendet?
Leuchtdioden an NIC, Switch, Router	1, 2	Die Diode leuchtet permanent, wenn eine Ethernet Verbindung besteht
Leuchtdioden blinken	1, 2	Gibt es Datenverkehr?
ipconfig, ifconfig, ip	2, 3	Korrekte IP-Einstellungen, MAC-Adressen überprüfen
arp	2, 3	ARP-Cache anzeigen oder löschen
route	3	Defaultgateway und Routingtabelle überprüfen
ping	3	Erreichbarkeit der Stationen testen
tracert, traceroute	3	Zwischenstationen auf dem Weg zum Ziel anzeigen
netstat, ss	4	TCP/UDP Verbindungen anzeigen, lokale Ports überprüfen
Portscanner (z.B. nmap)	3 - 7	Offene Ports von Remoterechnern überprüfen (und mehr)
wireshark	2 - 7	Allzweck-Werkzeug für detaillierte Untersuchungen

Entscheidungshilfe

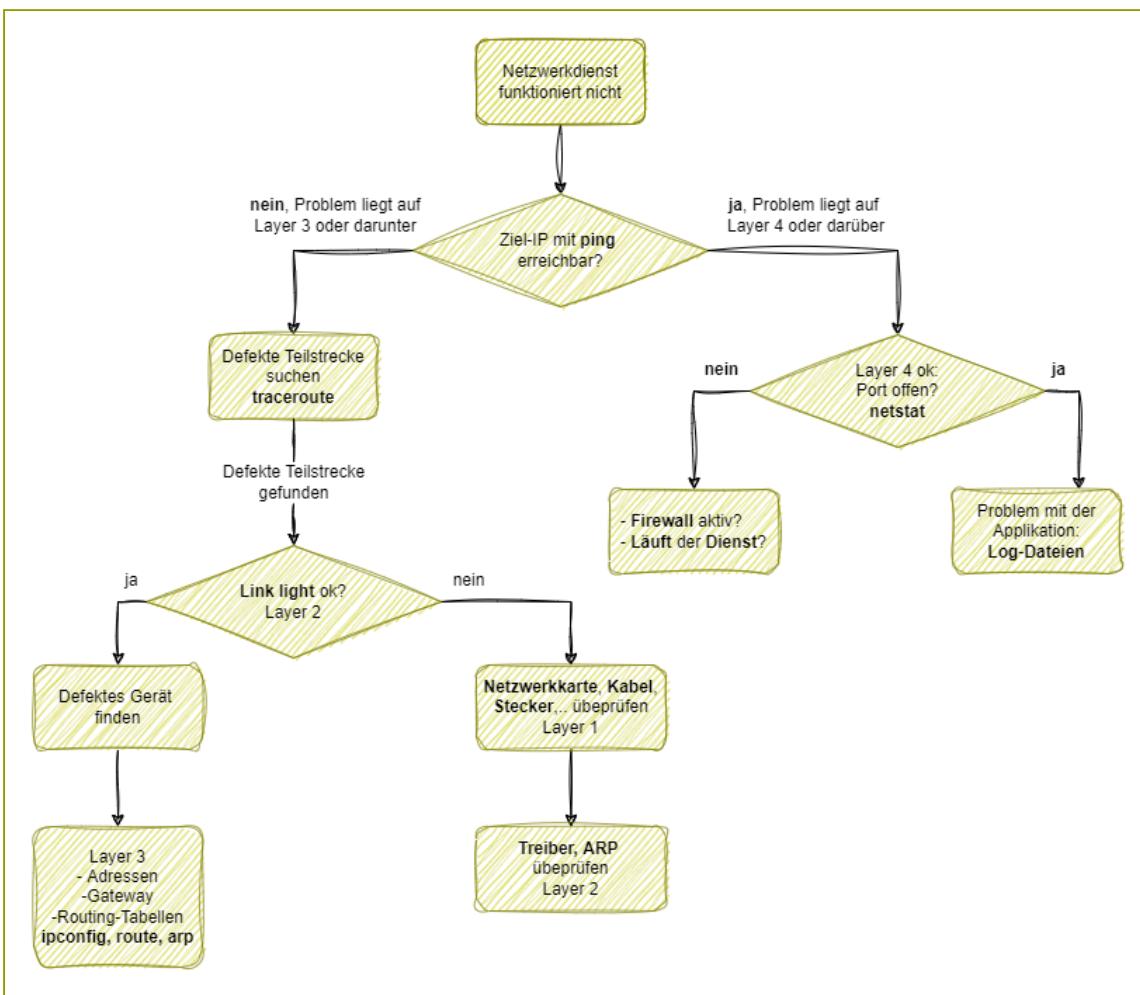


Abb. 1: Entscheidungshilfe

Netzwerkdokumentation

Eine Netzwerkdokumentation gliedert sich in eine Dokumentation für den Netzwerkadministrator und den Auftraggeber

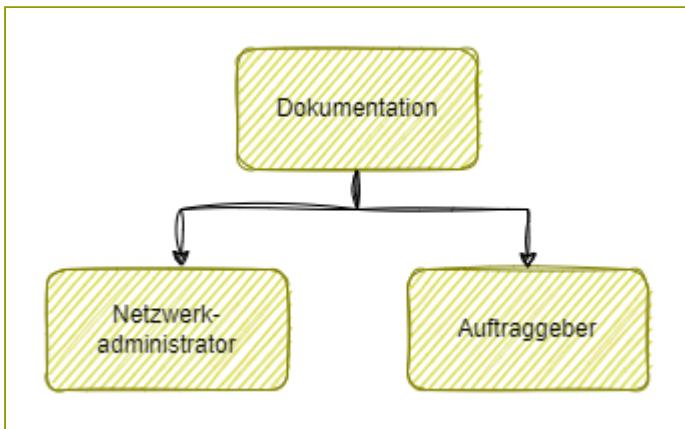


Abb. 1: Netzwerkdokumentation

✓ **Netzwerkadministrator:** Detailliertes Installation- und Konfigurationsdokument mit:

- ✓ Technische Spezifikationen
- ✓ Pläne
- ✓ Diagramme
- ✓ Daten der LAN-Komponenten
- ✓ Softwareversionen
- ✓ aktuelle Konfigurationen
- ✓ Leistungsfähigkeit
- ✓ Ausfallsicherheit
- ✓ Monitoring
- ✓ Wartung
- ✓ Risiken
- ✓ ...

✓ **Auftraggeber:** wichtigste Informationen mit:

- ✓ Service Level Agreements (SLA)
- ✓ Leistungsfähigkeit
- ✓ Ausfallsicherheit

 Monitoring

 ...

2. Abnahmeprotokoll

Cisco Packet Tracer

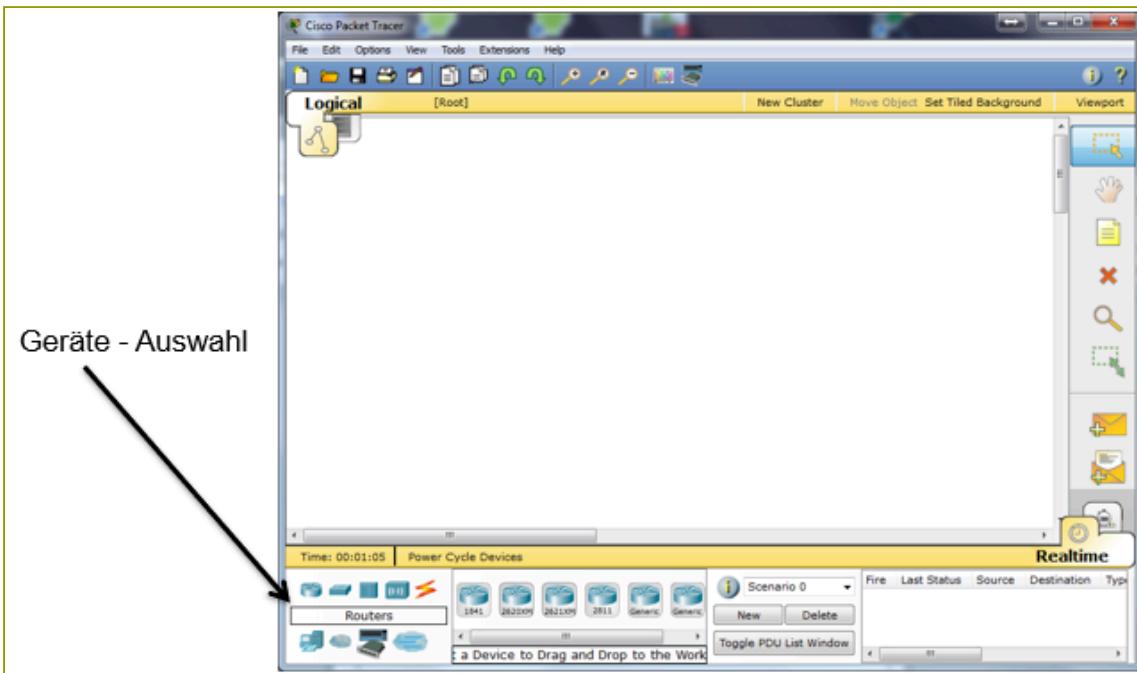


Abb. 1: Geräteauswahl

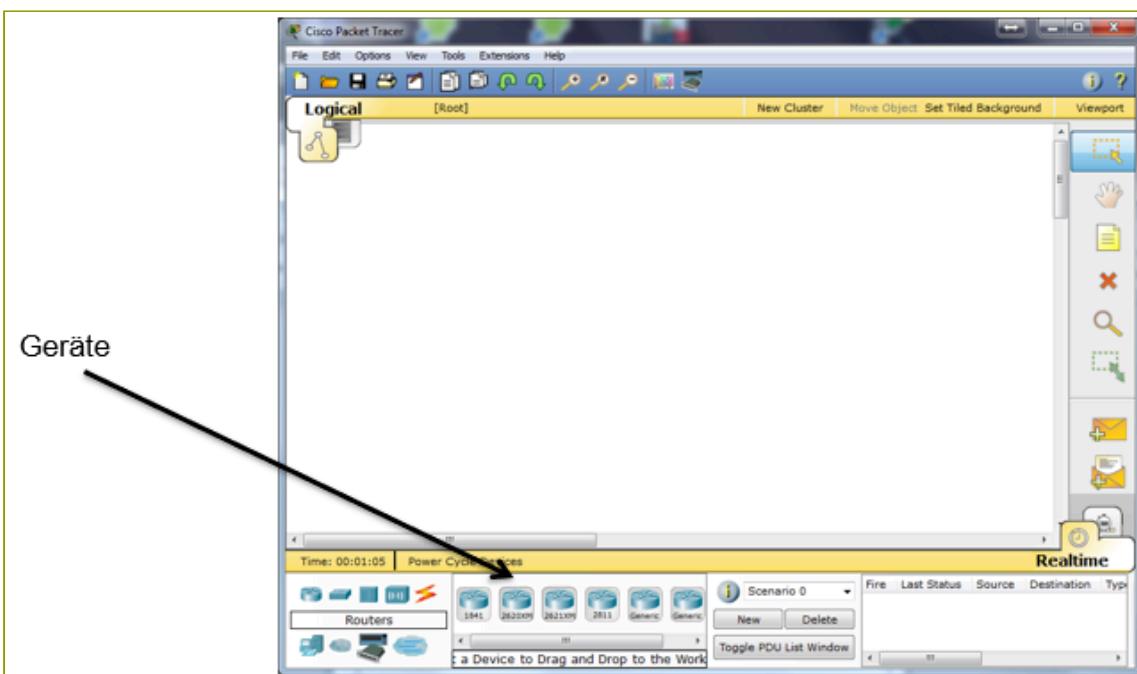


Abb. 2: Modellauswahl

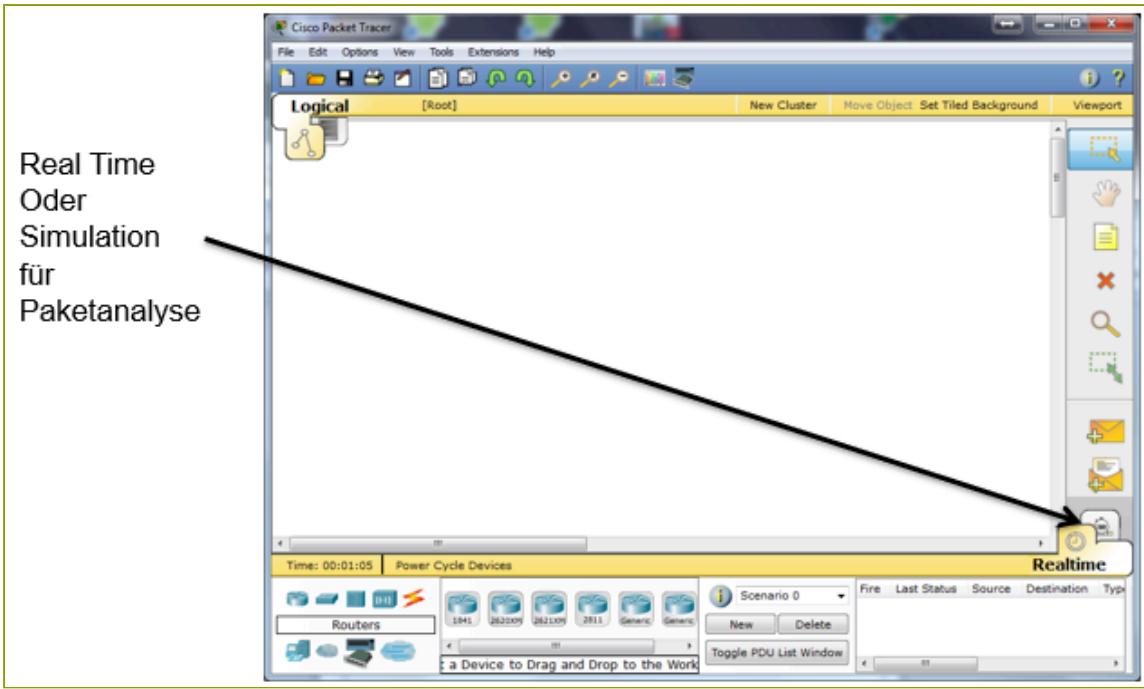


Abb. 3: Realtime / Simulation Modus

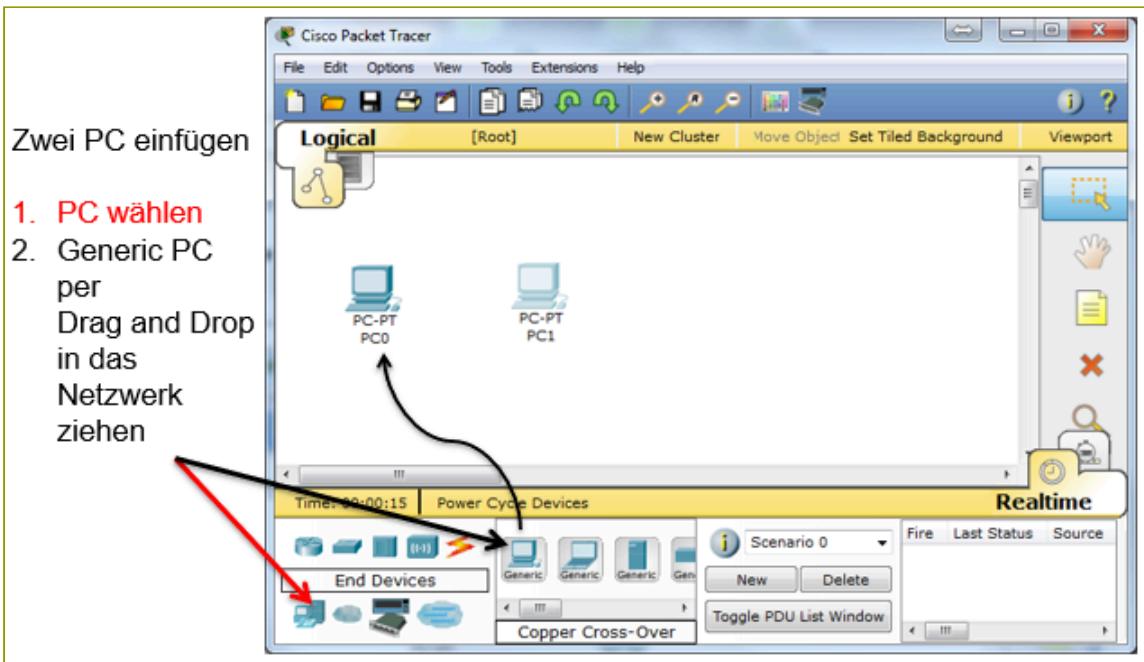


Abb. 4: PC's einfügen

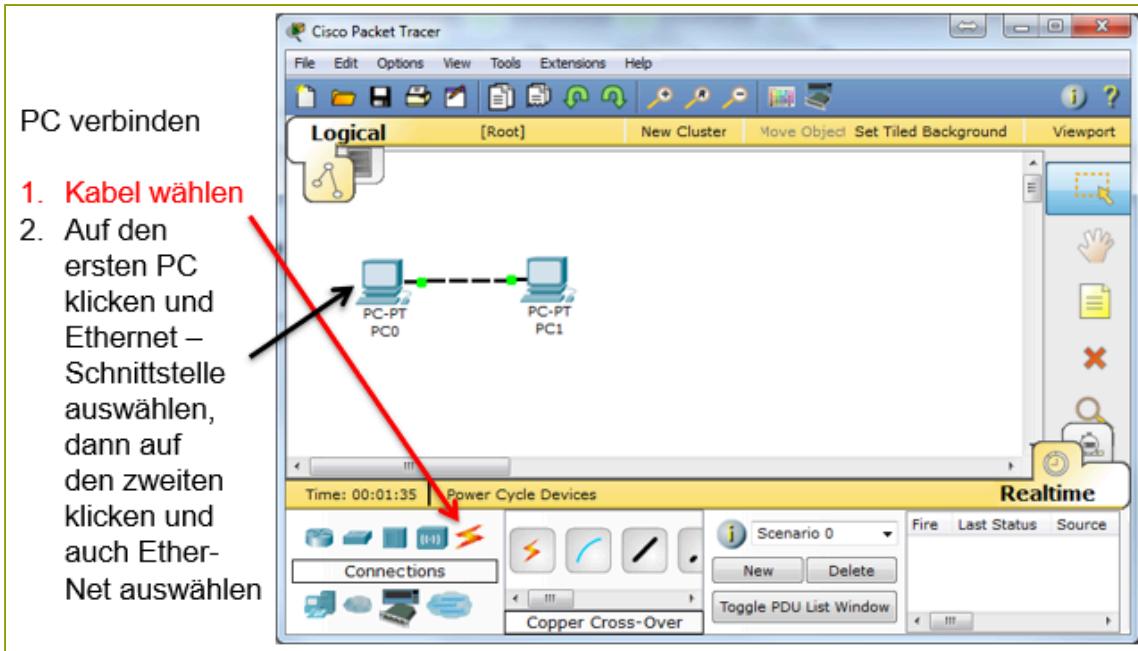


Abb. 5: PC's verbinden

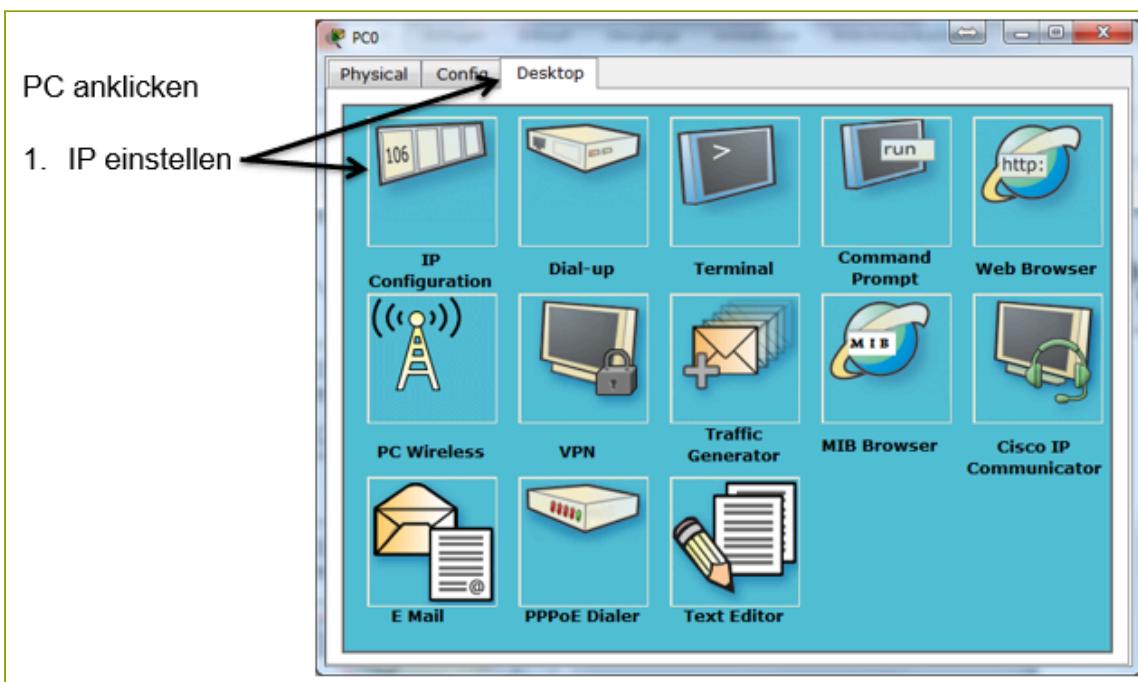


Abb. 6: IP-Einstellungen 1

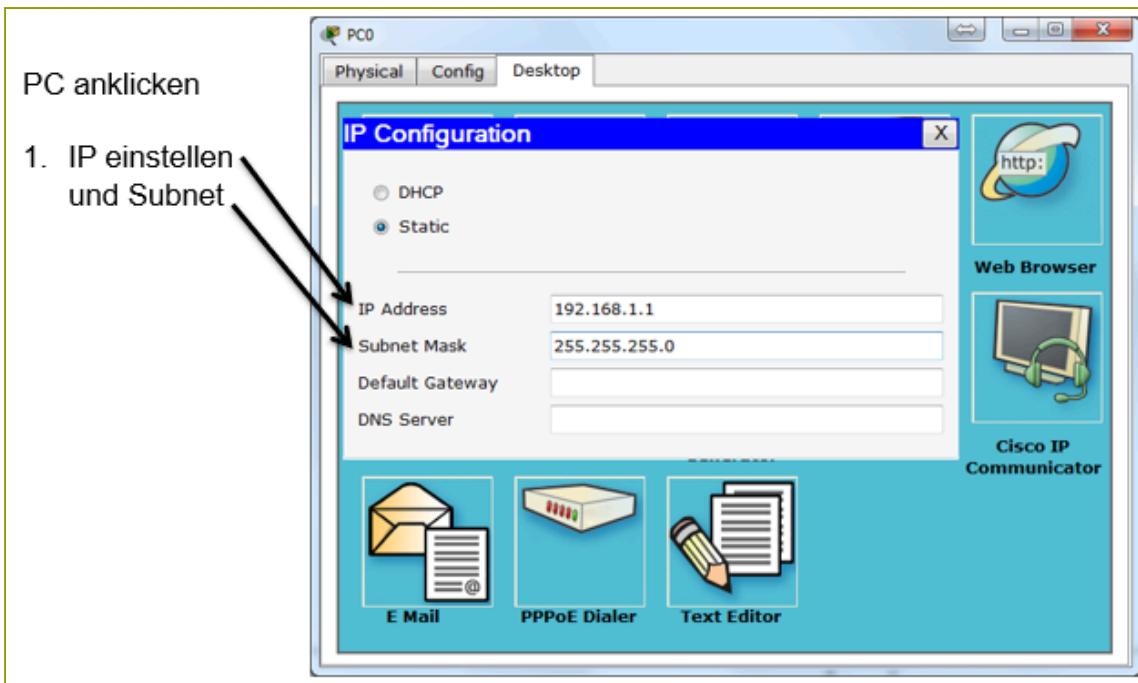


Abb. 7: IP-Einstellungen 2

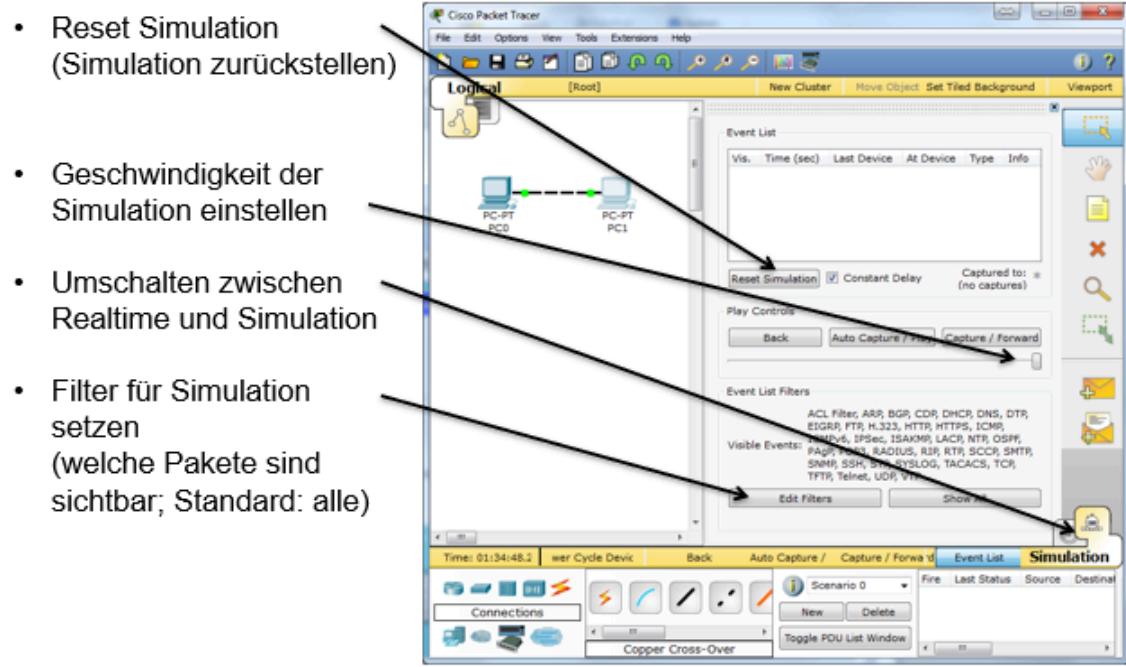


Abb. 8: Simulationsmodus Einstellungen

- PC öffnen
- Command Prompt öffnen
- Einen Ping auf den andern PC mit dem Befehl:

Ping 192.168.1.1

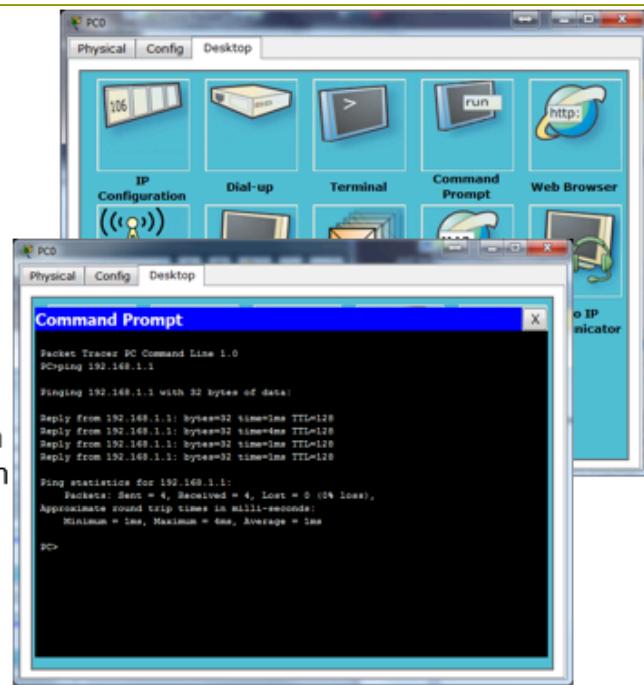


Abb. 9: Simulation starten

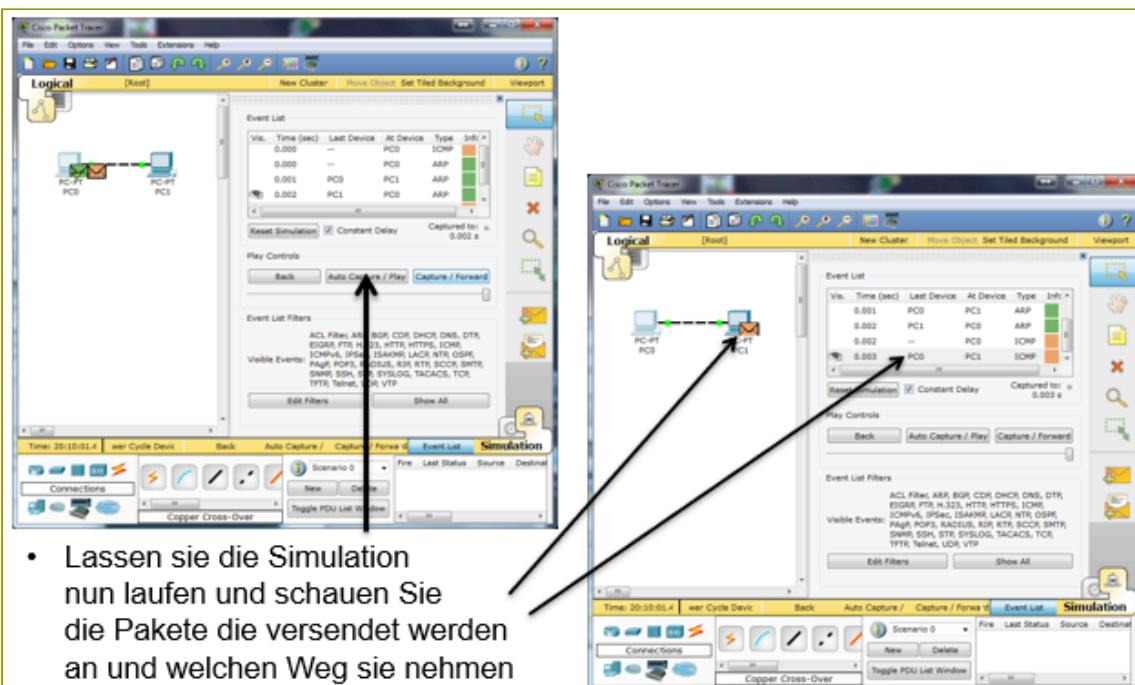


Abb. 10: Simulation verfolgen

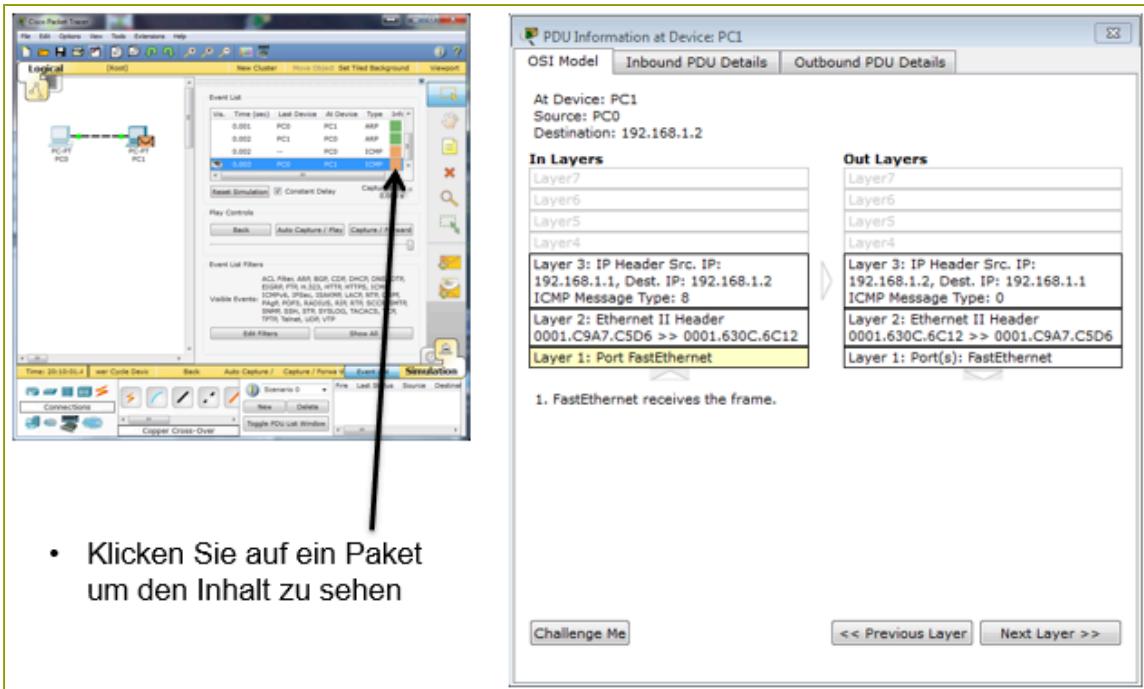


Abb. 11: Simulation Paket anschauen

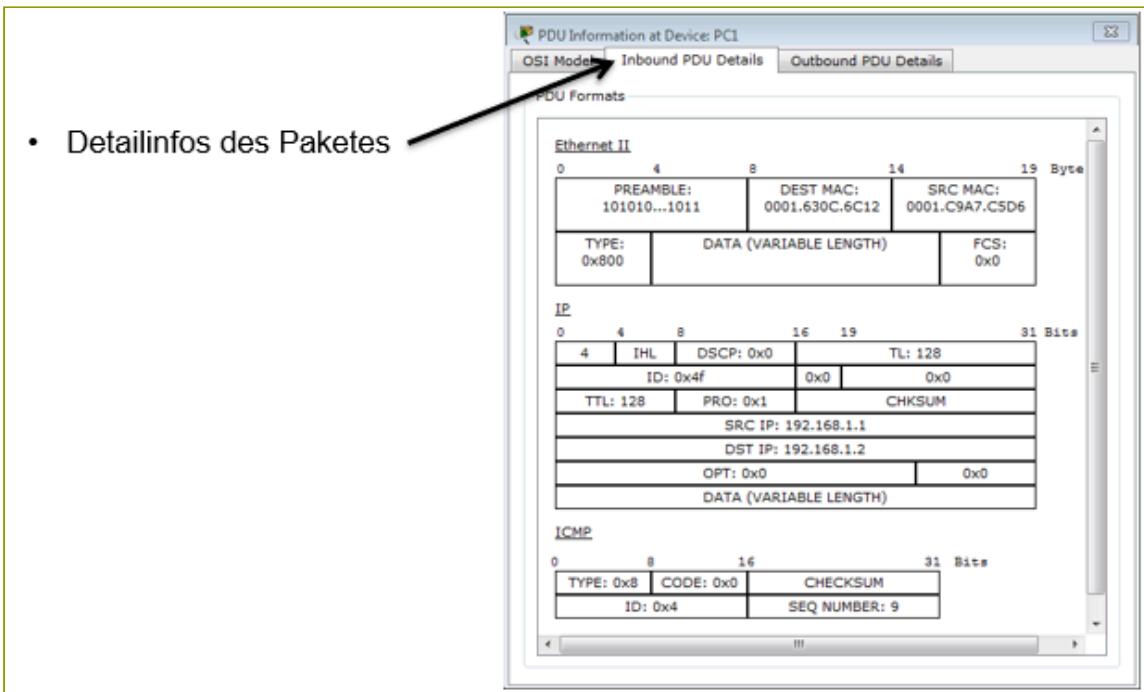


Abb. 12: Simulation Details eines Paketes anschauen