FH Salzburg

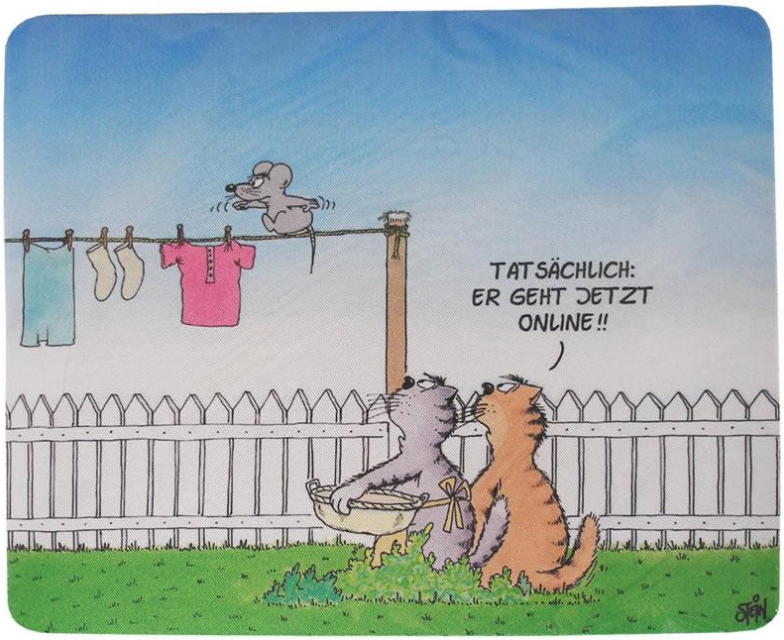
Studiengang ITS und WIN

Skript zur Vorlesung

Computernetze 1

Wintersemester 2024/25

Dipl.-Phys. Judith Schwarzer
judith.schwarzer@fh-salzburg.ac.at



Quelle: Uli Stein Mousepad

1 Einführung Datennetze

1.1 Einleitung

Unter einem Computer-, Daten- oder Rechnernetz versteht man grundsätzlich die Verknüpfung verschiedener, räumlich getrennter, elektronischer Systeme zum Zwecke des Datenaustauschs. Am bekanntesten ist hierbei sicher das Internet, aber auch Sensornetzwerke oder komplexe Steuer- und Regelungssysteme in Autos oder Industrieanlagen zählen dazu.

Derartige Kommunikationsnetzwerke unterscheiden sich hinsichtlich verschiedenster Aspekte. Zu nennen wären hier beispielsweise:

- realisierbare Bitrate
- Reichweite
- Position in einem übergeordneten Gesamtnetzwerk (Edge, Core, Access)
- Private und öffentliche Netze
- unterstützte Applikationen und Dienste (Daten, Sprache, Multimedia)
- verkabelte oder drahtlose Datenanbindung
- mobile oder fixe Stationen

Während in den Anfängen der elektronischen Kommunikation die Übertragung analoger Signale im Vordergrund stand, spielt bei heutigen Technologien der Austausch binärer Daten die Hauptrolle.

Die Lehrveranstaltung Computernetze soll einen ersten Überblick hierzu vermitteln. Der Schwerpunkt liegt dabei auf den gebräuchlichsten Technologien des Internets mit dem Internet Protocol (IP).

Im ersten Kapitel sollen zunächst die wichtigsten Grundbegriffe im Zusammenhang mit Computernetzen geklärt werden. Des Weiteren werden allgemeine Modelle vorgestellt, welche dazu dienen, die Kommunikation bzw. die verschiedenen Aufgaben im Rahmen einer Kommunikation in einem Rechnernetz zu strukturieren.

1.2 Grundbegriffe

1.2.1 Komponenten der Datenkommunikation

In einem Datennetz lassen sich folgende funktionalen Komponenten unterscheiden:

- Endgeräte:
  - Quelle oder Ziel einer Nachricht
  - z.B. PC's, Notebook, Handy, Sensor, …
- Netzwerkkomponenten:
  - Realisiert Verbindung zwischen Netzwerken
  - Anbindung von Endgeräten
  - Ermöglichen den Datenfluss im Netzwerk
  - z.B. Router, Switch, WLAN Access Point, …
- Übertragungsmedium:
  - Verbindung zwischen den Komponenten
  - Pfad der Datenübertragung
  - Drahtlos, Kupfer, Lichtwellenleiter

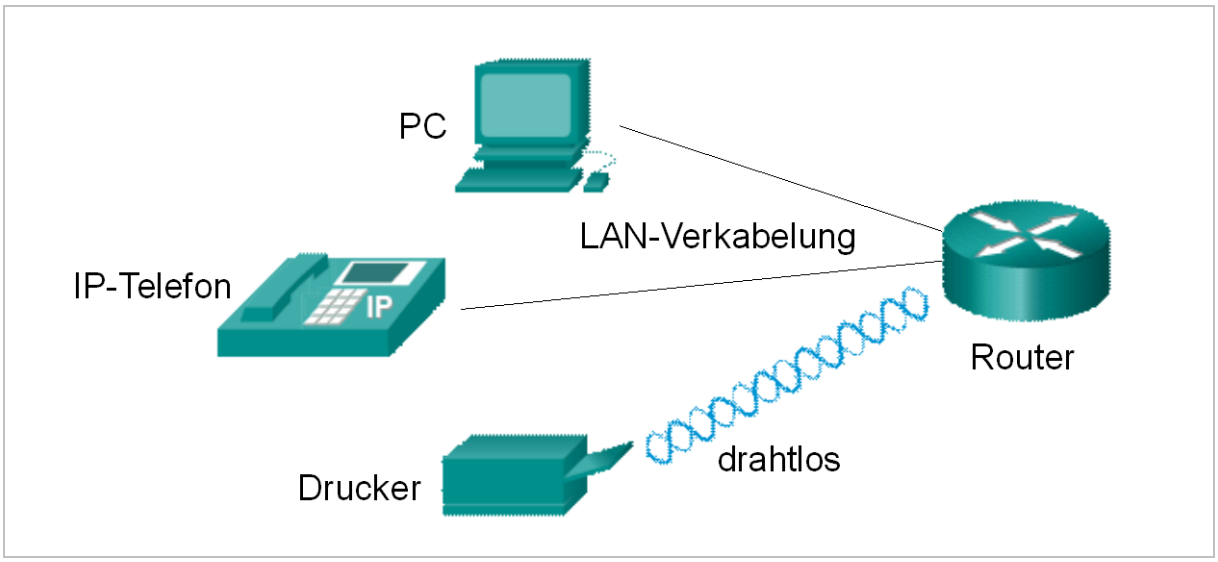


Abbildung 1: Komponenten der Datenkommunikation

1.2.2 Netzwerkabdeckung: LAN und WAN

Die Anforderungen an ein Netzwerk unterscheiden sich je nach Ausdehnung sehr stark.

Local Area Networks (LAN):

- Geografisch kleines Gebiet (Gebäude, Campus… über wenige Kilometer)
- An- und Verbindung von Endgeräten
- Administriert von einer Person/Organisation
- Bietet den Endgeräten üblicherweise hohe Bandbreite

Weitverkehrsnetz (Wide Area Network = WAN):

- Verbindet LANs, großes geografisches Gebiet
- Administriert von verschiedenen Personen/Organisationen
- Bietet eher niedrigere Bandbreite zwischen den LANs

Weitere Kategorien wie beispielsweise das *Personal Area Network (PAN)* bieten noch differenziertere Abstufungsmöglichkeiten hinsichtlich der Netzausdehnung.

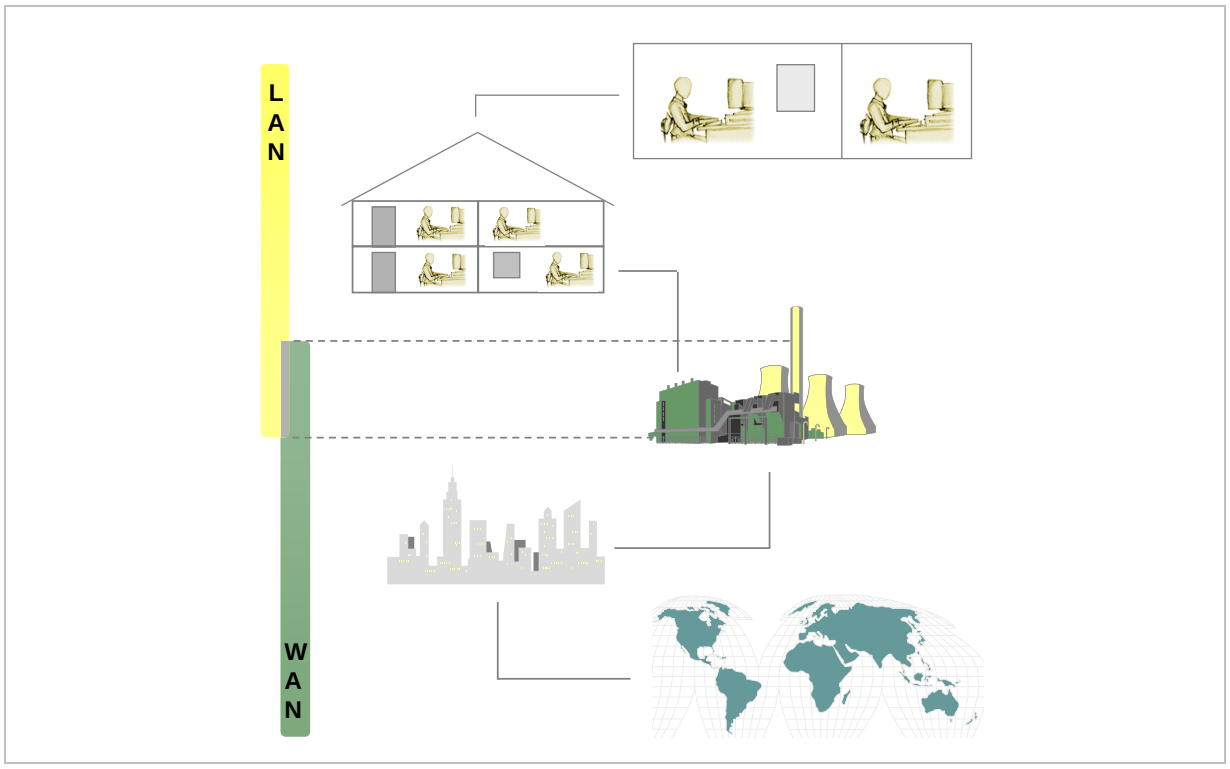


Abbildung 2: Geografisches Gebiet eines Netzwerkes: LAN und WAN

1.2.3 Netztopologie

Die Netztopologie beschreibt die Art und Weise der physikalischen oder logischen Verbindung zwischen den Netzkomponenten. Typische Formen sind:

- Bus (z.B. Feldbussysteme)
- Stern (z.B. Ethernet mit twisted pair Verkabelung)

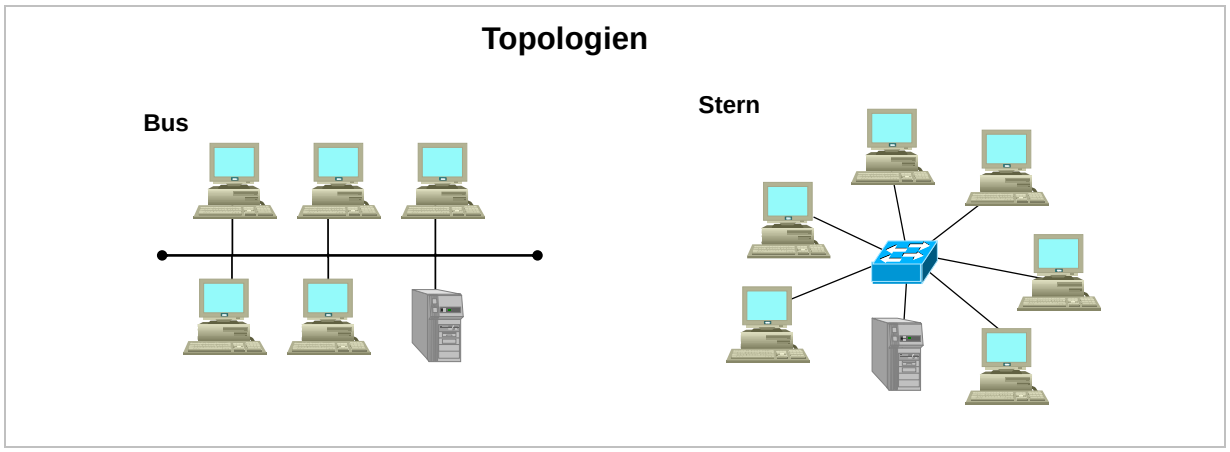


Abbildung 3: Netzwerktopologien

1.2.4 Uni-/Multi-/Broad-/Anycast von Nachrichten

Bzgl. der Kommunikationsform wird grundsätzlich auch darin unterschieden, ob eine Nachricht an einen, mehrere oder alle verfügbaren Teilnehmer eines Netzwerkes verschickt sollen:

- Unicast: Nachricht an genau einen Empfänger
- Broadcast: Nachricht an alle Teilnehmer eines Netzwerkes
- Multicast: Nachricht an mehrere Teilnehmer eines Netzwerkes
- Anycast: Nachricht an den „erstbesten“ einer bestimmten Teilnehmergruppe

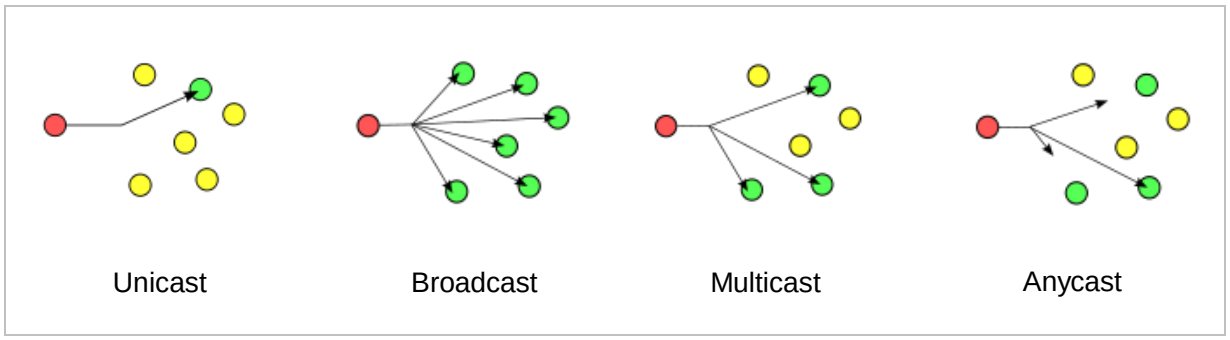


Abbildung 4: Netzwerktopologien (aus https://de.wikipedia.org/wiki/Broadcast, 09.09.2021)

1.3 Regeln, Protokolle und Modelle

1.3.1 Grundregeln der Datenkommunikation

Damit zwei Endgeräte miteinander kommunizieren können, muss klar sein, wie der Austausch der Informationen erfolgen soll. Sender und Empfänger verständigen sich auf ein gemeinsames Protokoll, welches u.a. Regeln zu folgenden Aspekten beinhaltet:

- (De-)Codierung der Information, z.B. Videocodierung
- Format, Struktur, Beginn, Ende… einer Nachricht
- Nachrichtengröße, relevant z.B. für Fragmentierung einer Nachricht
- Regelungen bzgl. Zeitpunkt der Sendung, Flusskontrolle, Timeout bei fehlender Rückmeldung…
- Optionen der Nachrichtenübertragung:
  - Uni-/Multi-/Broadcast,
  - bestätigt oder unbestätigt (Acknowledgement = ACK)
- Protokolle lassen sich außerdem noch unterscheiden hinsichtlich eines möglichen Verbindungsaufbaus zum Empfänger:
  - Verbindungsorientiert: Verbindungsaufbau (Teilnehmer "stellen sich vor", tauschen Kommunikationsparameter aus) -> Daten -> Verbindungsabbau
  - Verbindungslos: keine vorherige Absprache, Daten werden direkt versendet

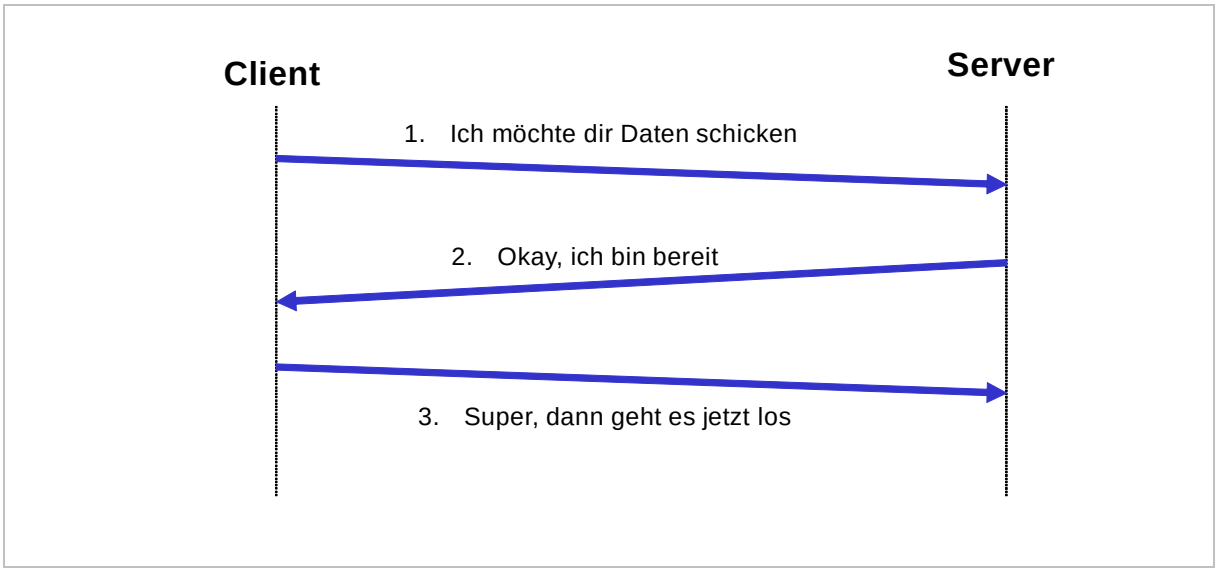


Abbildung 5: Verbindungsaufbau (symbolisch) bei einer verbindungsorientierten Kommunikation

1.3.2 Die Idee des Schichtenmodells

Ein vollständiger Kommunikationsablauf wird durch einen ganzen Satz von Protokollen/Regeln (prototol suite) festgelegt, die jeweils unterschiedliche Aufgaben im Rahmen der Kommunikation erfüllen. Die Protokolle können dabei in Form von aufeinanderliegenden Schichten dargestellt werden.

Jede Schicht erfüllt eine definierte Funktion und bietet ihrer darüberliegenden Schicht bestimmte Dienste an. Die Aufteilung der Aufgaben eines Datenkommunikationsablaufes in aufeinanderliegende Schichten wird als Referenzmodell bezeichnet und folgt drei Grundprinzipien, die in untenstehender Abbildung veranschaulicht werden (Kommunikation zwischen zwei Diplomaten):

- Horizontale Kommunikation: Botschaften haben nur auf der Ebene, auf der sie mit Hilfe eines Protokolls ausgetauscht werden, eine Bedeutung
- Vertikale Kommunikation: eine höher gelegene Schicht nutzt die Dienste der darunterliegenden Schicht und gibt die Nachricht entsprechend weiter
- Schichten sollten so eingeteilt sein, dass sie unabhängig voneinander ausgetauscht oder geändert werden können, z.B. unten: Änderung der Sprache

Das aktuell gängigste Referenzmodell ist das TCP/IP Modell.

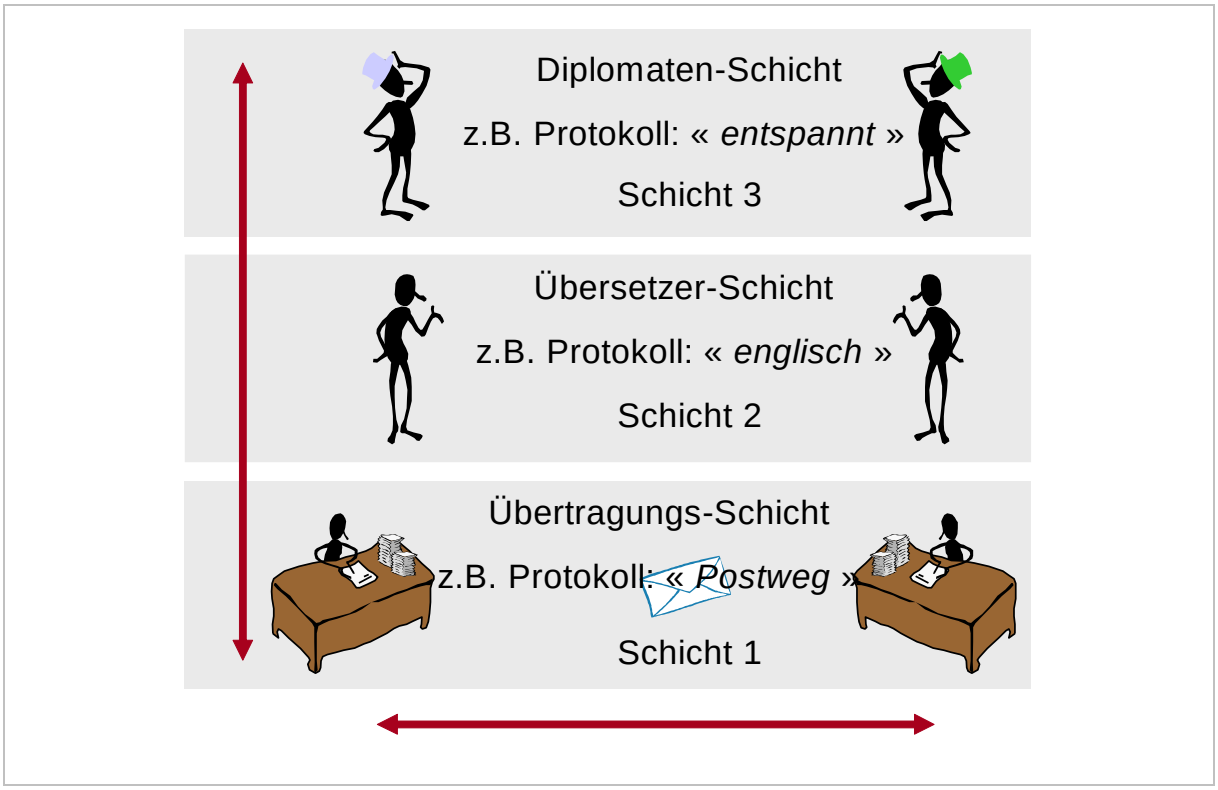


Abbildung 6: Grundprinzipien eine Referenzmodells

1.3.3 Die TCP/IP Protocol Suite und das OSI-Modell

Als TCP/IP Protocol Suite (TCP: Transmission Control Protocol) bezeichnet man eine Sammlung von Protokollen, die in IP-basierten Netzen eingesetzt werden. Das in diesem Zusammenhang definierte Modell basiert auf fünf (je nach Quelle nur vier) Schichten, demgegenüber steht das OSI-Modell mit sieben Schichten (siehe Abbildung 7). Den jeweiligen Schichten können bestimmte Protokolle zugeordnet werden, welche für diese Kommunikationsschicht typische Aufgaben definieren.

Grundsätzlich legt das **Modell** fest, **WAS** auf einer bestimmten Schicht passiert und das eigentliche **Protokoll** definiert, **WIE** es passiert.

Es ist sinnvoll, einen Kommunikationsprozess so in einzelne Aufgaben zu unterteilen, dass die Verfahren auf einer bestimmten Schicht ausgetauscht werden können, ohne dass das gesamte System betroffen ist (z.B. WLAN statt Ethernet nutzen). Ziel sollte außerdem sein, dass vertikal möglichst wenig Information zwischen den Schichten ausgetauscht werden muss.

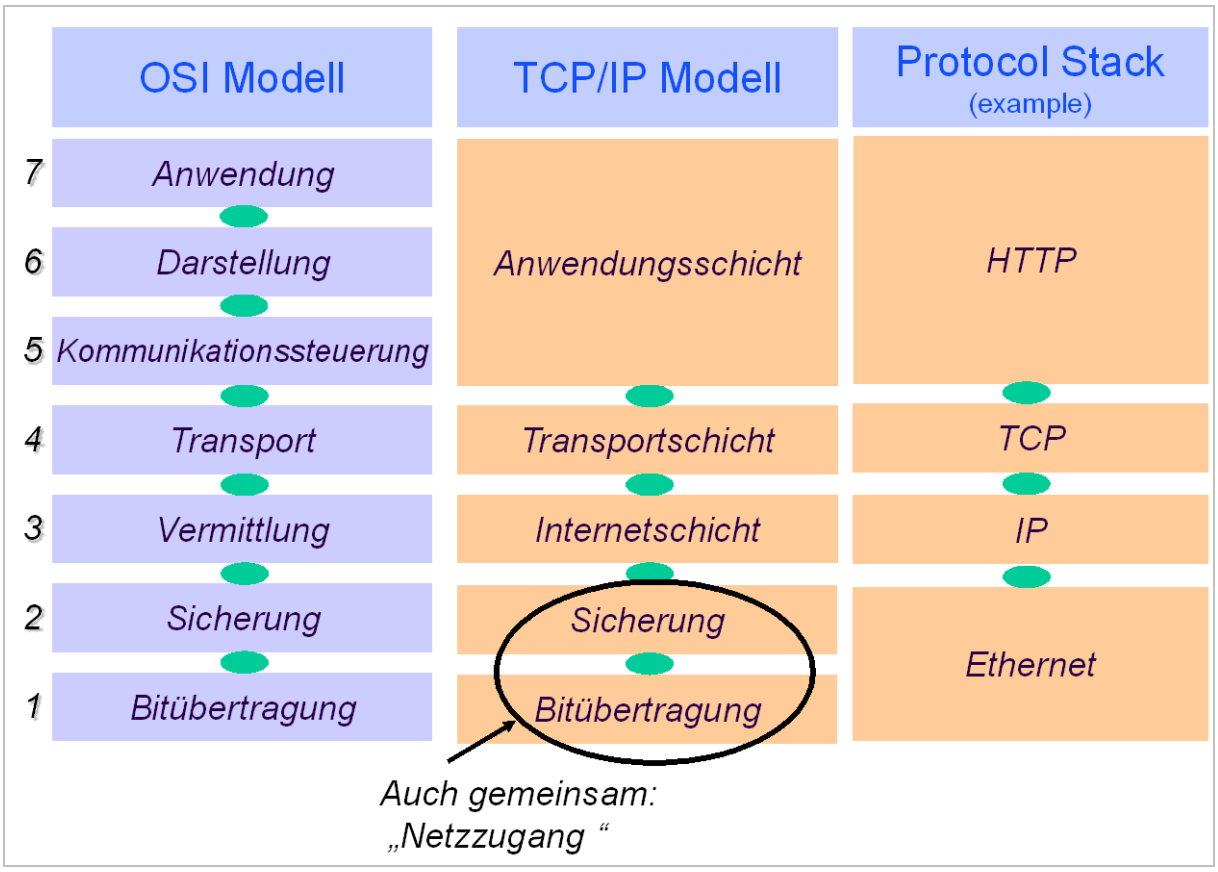


Abbildung 7: Die Schichten des OSI- und TCP/IP-Modells

Die Anwendungsschicht

Die Anwendungsschicht beschreibt Protokolle und Netzanwendungen, welche über mehrere Endsysteme verteilt sind wie z.B. zum Dateitransfer (FTP), für e-mail (SMTP, IMAP…) oder Webabfragen (HTTP).

Das OSI-Modell nimmt hier eine präzisere Unterteilung vor und gliedert Funktionen oberhalb der transportorientierten Schichten in:

⇒ Kommunikationssteuerung (OSI Schicht 5): Absprache zwischen zwei Partnern bezüglich einer Sitzung (Session)

⇒ Darstellungsschicht (OSI Schicht 6): Absprache der Teilnehmer über die Darstellung der auszutauschenden Daten.

⇒ Anwendungsschicht (OSI Schicht 7): Schnittstelle zur Anwendung

In der Realität stößt diese Einteilung an ihre Grenzen. In den meisten Anwendungsprotokollen sind die Funktionen dieser OSI-Schichten 5, 6 und 7 oft gemeinsam implementiert.

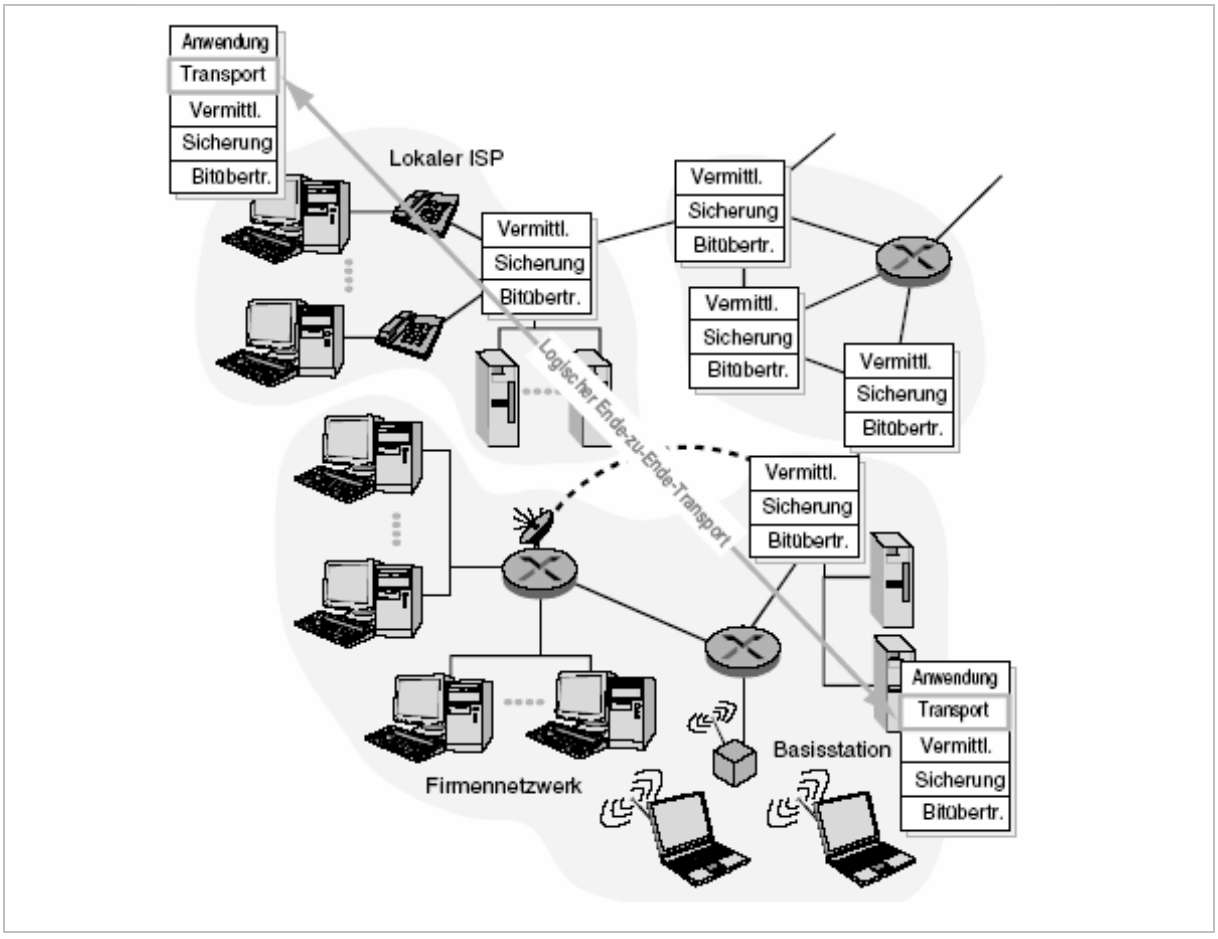


Abbildung 8: Funktion einer Transportverbindung (Transportschicht), aus [http://www.pearson-studium.de/media_remote/katalog/bsp/9783827370174bsp.pdf]

Die Transportschicht (Transport Layer)

Die Transportschicht überträgt Nachrichten der Anwendungsprotokolle zwischen den Endpunkten. Zu ihren Aufgaben zählen (teilweise optional):

⇒ Segmentierung der Daten

⇒ Flußsteuerung

⇒ Fehlersicherung und –behebung

⇒ Bereitstellung einer (oftmals gesicherten) logischen Verbindung

⇒ Die Identifikation einer bestimmten Anwendung durch einen Adressierungsmechanismus (z.B. Port-Nr.).

Die Transportschicht bietet der Anwendung somit einen einheitlichen Zugriff auf das Kommunikationsnetz, ohne dass dessen Eigenschaften konkret berücksichtigt werden müssen. Typische Vertreter im Internet sind das Transmission Control Protocol (TCP) und das User Datagramm Protocol (UDP).

Die Netzwerk- bzw. Vermittlungsschicht (Network Layer)

Die Vermittlungsschicht ist für den netzübergreifenden Transport von Daten zwischen Endsystemen verantwortlich. Höhere Schichten bleiben vom Problem der Wegewahl unberührt. Die Wegewahl über mehrere Teilnetze hinweg wird auch als Routing bezeichnet und ist somit eine Aufgabe dieser Schicht.

Eng mit der Aufgabe des Routings verbunden ist die Verwendung entsprechender netzwerkübergreifender Adressen, die hardwareunabhängig sind und ein Netz logisch strukturieren. Typischer Vertreter ist das Internet Protocol (IP) mit der IP-Adressierung.

Die Sicherungsschicht (Data Link Layer)

Um ein Paket von einem Knoten des Netzes zum nächsten zu bringen, verlässt sich die Netzwerkschicht auf die Dienste der Sicherungsschicht. Diese hat grundsätzlich folgende Aufgaben:

⇒ Organisation der Bits, Strukturierung der Informationen in logische Gruppen (sogenannten Frames bzw. Rahmen)

⇒ Auf- und Abbau gesicherter Verbindungen

⇒ Adressierung des Empfängersystems anhand der zugehörigen Hardwareadresse (z.B. MAC-Adresse)

⇒ Zugriffsregelung zur gemeinsamen Nutzung eines Mediums

⇒ Erstellung von Sicherungsinformation und Fehlererkennung

⇒ evtl. Fehlerüberwachung und -behebung; (z.B. Ethernet und WLAN: Kollisionsbehandlung)

⇒ evtl. Flusssteuerung

Die Bitübertragungsschicht (Physical Layer)

Die Aufgabe der Bitübertragungsschicht besteht darin, eine bitweise Übertragung zwischen Nachbarsystemen zu ermöglichen. Diese Schicht ist verantwortlich für:

⇒ Herstellen, Aufrechterhalten und Abbau von physikalischen Verbindungen

⇒ Transparente Bitübertragung zwischen zwei benachbarten Systemen

Innerhalb der Bitübertragungsschicht werden alle elektrischen und mechanischen Eigenschaften festgelegt, die zur Übermittlung von Signalen notwendig sind. Neben Spannungspegel und Bitdauer sowie die Form der Steckkontakte werden hier auch die physikalischen Eigenschaften des Übertragungsmediums beschrieben.

Hinweis: Im TCP/IP Modell werden häufig die Bitübertragungs- und die Sicherungsschicht in der sogenannten *Netzzugangsschicht* zusammengefasst (siehe Abbildung 7)

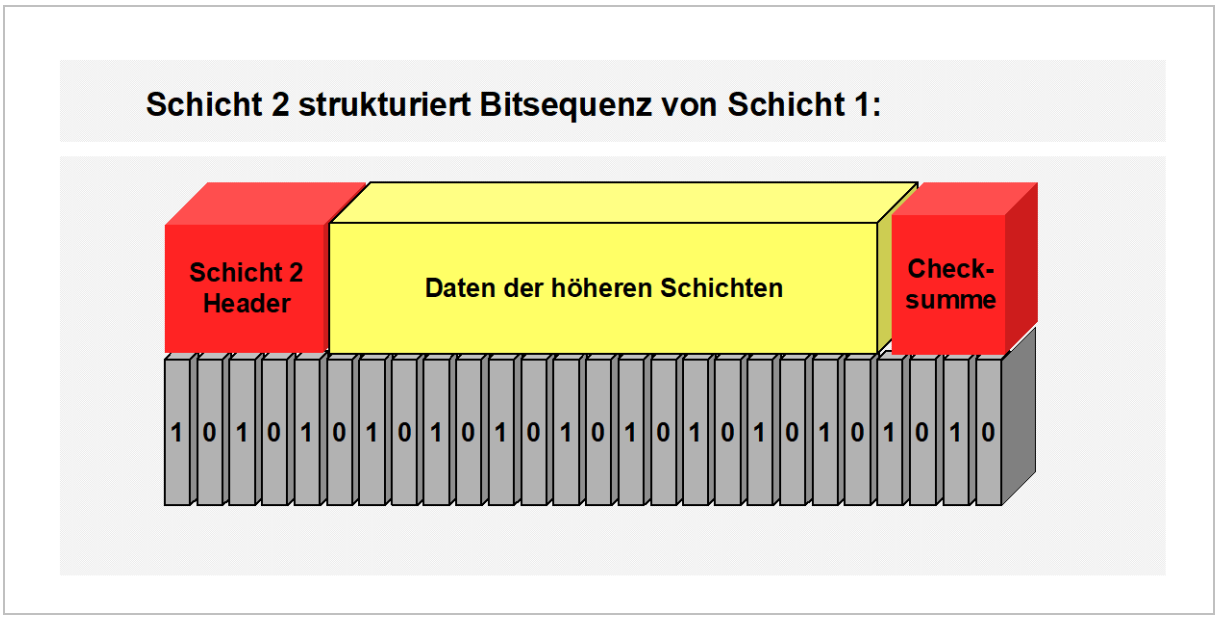


Abbildung 9: Gruppierung von Bits in Frames

1.3.4 Weitere Aspekte der Referenzmodelle

Vertikale Kommunikation zwischen den Protokollen

Die Kommunikation der Schichten untereinander lässt sich anhand von Schnittstellen und Diensten beschreiben. Die einzelnen Schichten erbringen ihrerseits Dienste oder nehmen Dienste anderer Schichten in Anspruch. Eine Schicht kommuniziert in der Regel mit zwei Partnern:

⇒ Mit ihrem *Service User* (Dienstbenutzer), der darüberliegenden Schicht: Dem Service User werden bestimmte, genau definierte Dienste angeboten.

⇒ Mit ihrem *Service Provider* (Dienstanbieter), der darunterliegenden Schicht. Die betrachtete Schicht ist nun selber Dienstbenutzer und fordert die Dienste der darunterliegenden Schicht an.

⇒ Die Übergabepunkte zwischen den Schichten nennt man Service Access Points (SAP). Die Information, an welche Applikation oder Protokoll die Daten beim Empfänger jeweils weitergegeben werden müssen, wird anhand des Service Access Points „mitgeliefert“ und befindet sich im jeweiligen Protokollheader.

⇒ Die jeweiligen Aufgaben der Schichten werden in sogenannten *Instanzen* realisiert

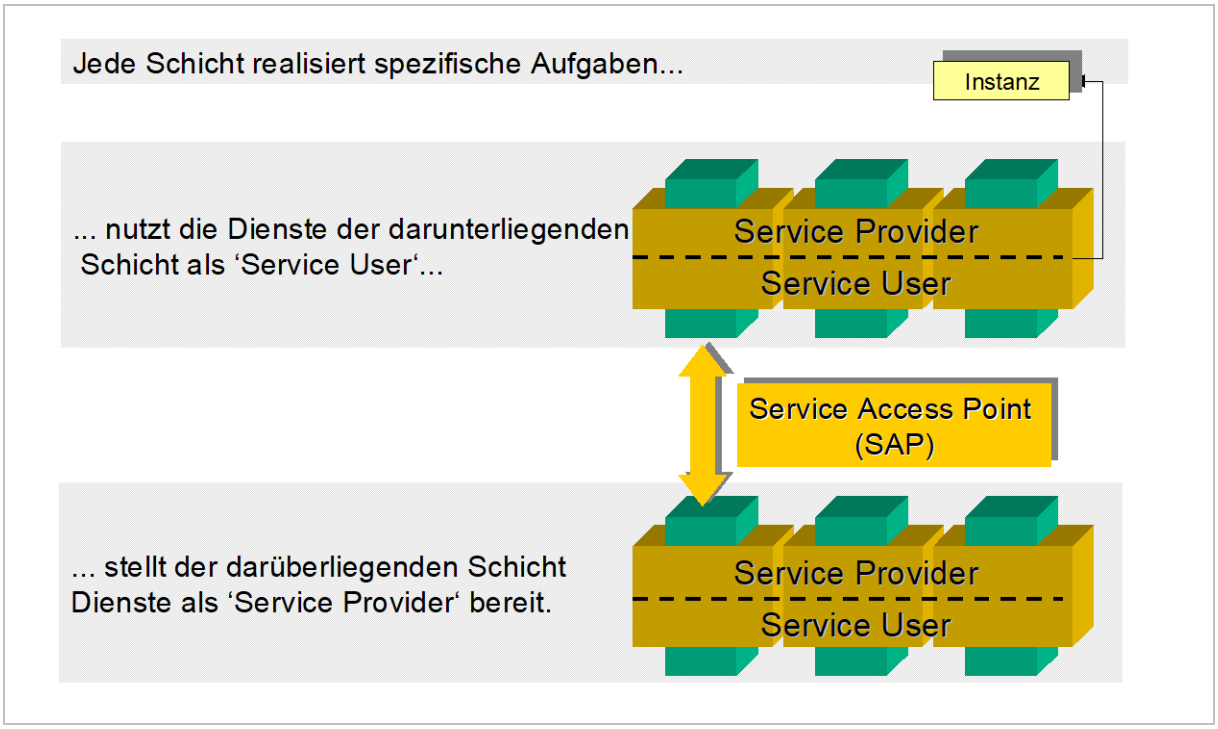


Abbildung 10: Service Access Points

Übergabe von Daten zwischen den Schichten und virtuelle Kommunikation

Bei der Inanspruchnahme der Dienste einer untergeordneten Schicht übergibt die höhere Schicht ihre Daten an die untergeordnete Schicht. Dabei werden auf der unteren Schicht schichtspezifische Informationen hinzugefügt und gegebenenfalls weiter nach unten gereicht. Man spricht hier auch von **Encapsulation**.

Bei der Verbindung von zwei Endsystemen durchlaufen die Daten im Sender die Schichten abwärts, während sie im Empfänger in den Schichten in umgekehrter Reihenfolge nach oben weitergegeben werden (**Decapsulation**).

Dabei werden die Daten von Schicht zu Schicht mit einem Header (Paketkopf) und gegebenenfalls auch mit einem Trailer (Information am Ende des Rahmens) versehen. Es entsteht so ein immer größer werdendes Datenpaket.

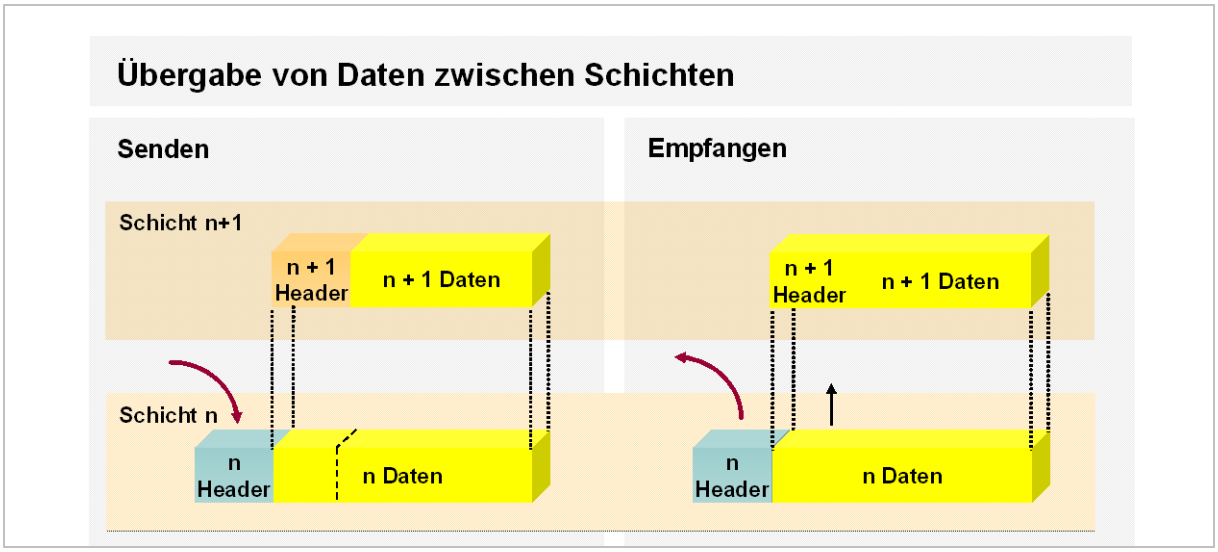


Abbildung 11: Senden und Empfangen von Daten im Schichtenmodell

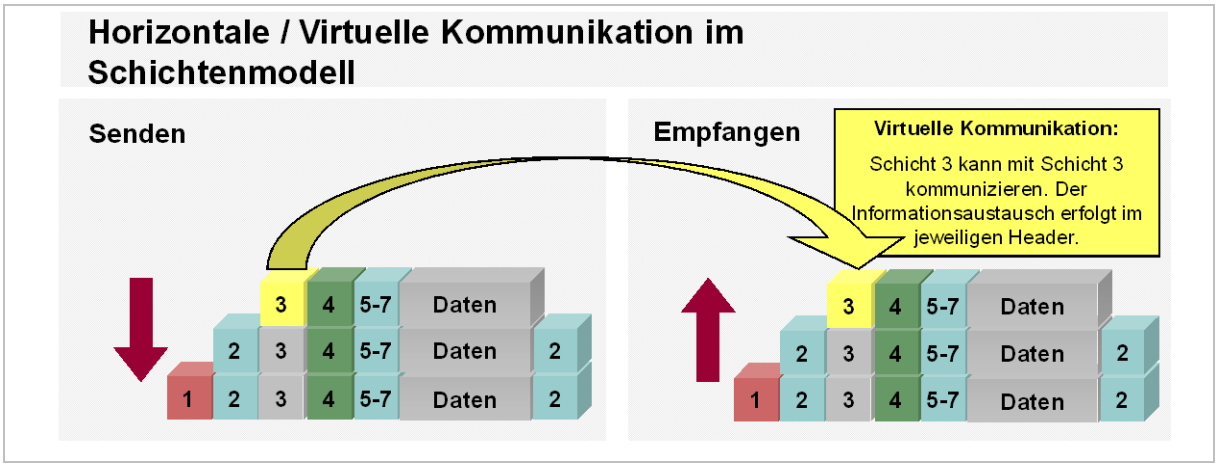


Abbildung 12: Horizontale/Virtuelle Kommunikation

Netzperformance

Die zusätzlich zu den Nutzdaten zu übertragenden Informationen bezeichnet man als Overhead.

Der Overhead stellt einen wichtigen Parameter bezüglich der Leistungsfähigkeit eines Netzwerkes dar. Die Daten müssen im Sender eingepackt und in der Zielstation wieder ausgepackt werden. Beide Funktionen sowie die zusätzliche Datenmenge beeinflussen damit die Performance im Netz.

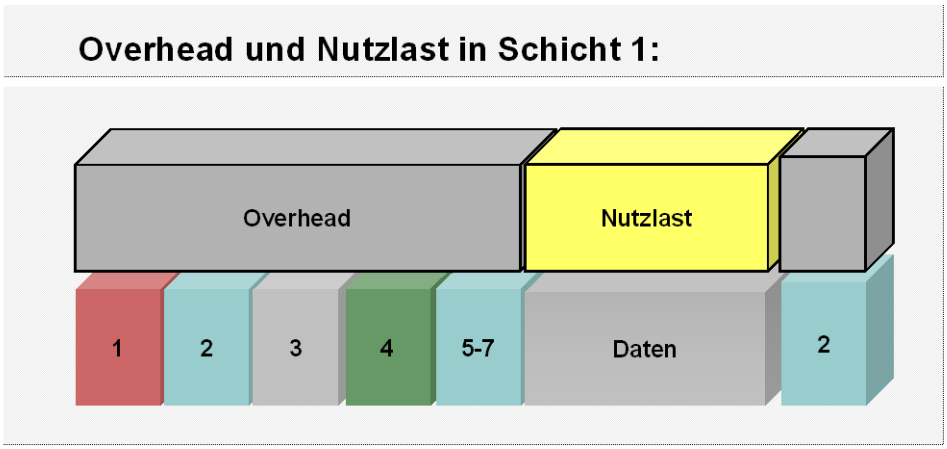


Abbildung 13: Overhead und Nutzlast

Wichtige Begriffe im Rahmen der vertikalen Kommunikation

Um sich auch in der formalen Sprache der Protokollspezifikationen zurecht zu finden, sollen im Folgenden einige wichtige Begriffe hierzu näher erläutert werden.
Abbildung 13 veranschaulicht noch einmal den Ablauf der vertikalen Kommunikation:

- Schicht (N+1) übergibt ihre zu übertragenden Nutzdaten als (N)_SDU (service data unit) an die darunter liegende Schicht am N_SAP (Dienstübergabepunkt)
- Zusätzliche Steuerinformationen N_ICI (interface control information) dienen der Abstimmung zwischen den Schichten
- Der N_Service übernimmt diese Nutzdaten und wertet die ICI aus.
- Schicht N fügt Protokollinformationen N_PCI (protocol control information) hinzu. Dies sind z.B. Zieladressen, Zielprozesse bei Empfänger etc.
- Die von der N-Schicht zu übertragenden Protokoll-Daten N_PDU (protocol data unit) ergeben sich aus: N_PCI gefolgt von N_SDU.
- Diese Daten übergibt nun die N-Schicht wieder an die darunter liegende Schicht (als (N-1)_SDU.
- Es gilt demnach N_PDU = (N-1)_SDU.
- Als grundsätzlicher Ablauf ergibt sich somit für jede Schicht:

N_SDU wird an N_SAP übergeben → N_SDU + N_PCI = N_PDU = (N-1)_SDU

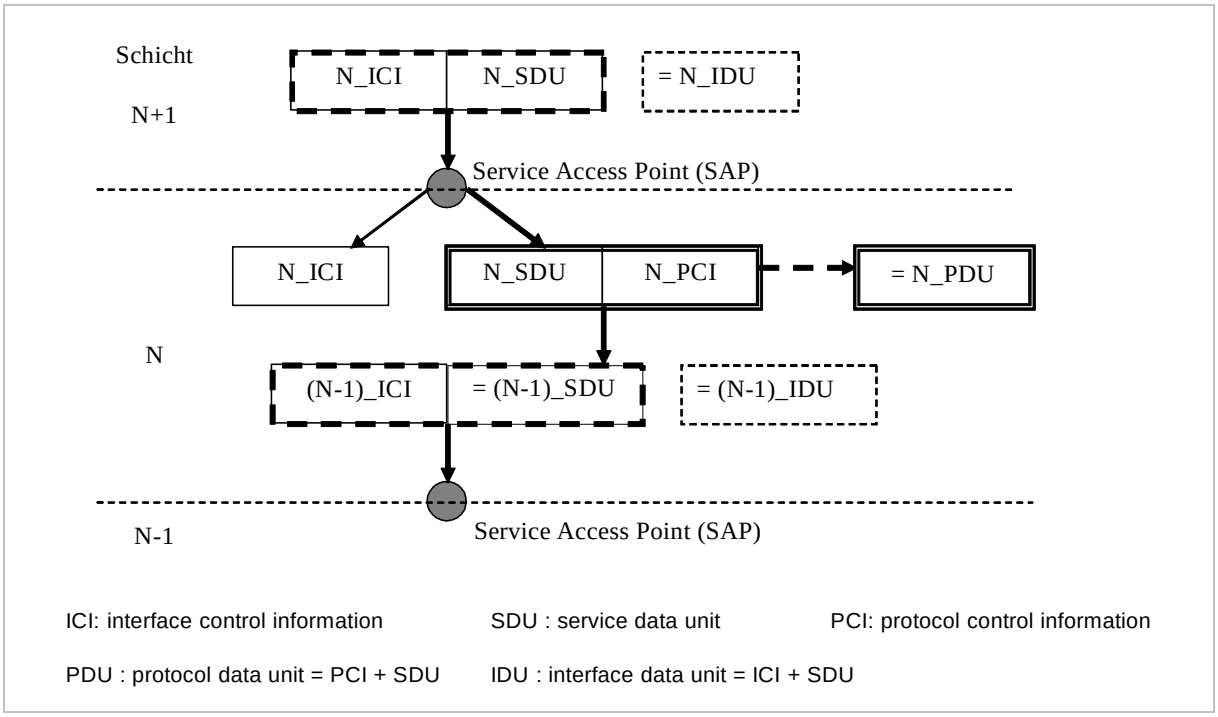


Abbildung 13: Begriffe im Rahmen der vertikalen Kommunikation

1.4 Wichtige Standardisierungsgremien

Lt. diverser Lexika versteht man unter Standardisierung grundsätzlich die Vereinheitlichung von Maßen, Typen, Verfahrensweisen oder anderem. Durch die Schaffung gemeinsamer Standards können Produkte (HW und SW), aber auch Abläufe so definiert bzw. gefertigt werden, dass sie kompatibel und herstellerunabhängig mit anderen zusammenarbeiten können.

Im Bereich der Datennetze spielen hier die standardisierten Kommunikationsprotokolle eine entscheidende Rolle. Im Folgenden sollen kurz einige wichtige Standardisierungsgremien genannt werden, welche für das Umfeld der Netzwerktechnik relevant sind:

Gremium	Schwerpunkt	wichtige Standards
Internet Engineering Task Force (IETF) www.ietf.org	Netzwerkstandards, vorwiegend ab L3 aufwärts; Kryptostandards	RFC 791: IP RFC 793: TCP
Institute of Electrical and Electronics Engineers (IEEE) www.ieee.org	Netzwerkstandards, vorwiegend Layer 1 und 2	IEEE 802.11: WLAN, IEEE802.3: Ethernet
International Telecommunication Union (ITU) www.itu.int	Telekommunikationsstandards, inkl. Komprimierung von Audiosignalen	H.323: Packet-based multimedia communications systems
International Organization for Standardization (ISO) www.iso.org	Alle Bereiche, auch Netzwerke	ISO 7498: OSI Referenzmodell

Speziell in der Zeit der „zusammenwachsenden“ konvergenten Netze gibt es zunehmend Überschneidungen bzgl. der „Zuständigkeitsbereiche“ zwischen den einzelnen Standardisierungsgremien. Nicht selten wird dann ein gemeinsamer Standard von zwei Gremien verabschiedet.

2 Übersicht über IP Datennetze und Dienste

2.1 Das Internet Protocol (IP)

2.1.1 Das *Internet* vs. *Internet Protocol*

Folgende Kurzbeschreibung zum Begriff Internet ist sinngemäß Wikipedia zu entnehmen (http://de.wikipedia.org/wiki/Internet, 07.09.2022)

> *Das **Internet** (von englisch internetwork, zusammengesetzt aus dem Präfix inter und network ‚Netzwerk' oder kurz net ‚Netz'), umgangssprachlich auch Netz, ist ein weltweiter Verbund von Rechnernetzwerken, den autonomen Systemen. Es ermöglicht die Nutzung von Internetdiensten wie WWW, E-Mail, Telnet, Usenet und FTP. Dabei kann sich jeder Rechner mit jedem anderen Rechner verbinden. Der Datenaustausch zwischen den über das Internet verbundenen Rechnern erfolgt über die technisch normierten Internetprotokolle. Die Technik des Internets wird durch die RFCs der Internet Engineering Task Force (IETF) beschrieben.…*

Das Internet kann logisch in folgende drei Teilbereiche aufgegliedert werden:

- Backbones (Kern- oder Basisnetzwerk)
- Local Area Networks
- Access Networks (Verbindung zwischen LAN and Backbone)

Die Adressierung und Vermittlung der Nachrichtenpakete erfolgt basierend auf dem Internet Protokoll (IPv4 oder IPv6), welches aber auch ohne Anbindung an DAS INTERNET Anwendung findet.

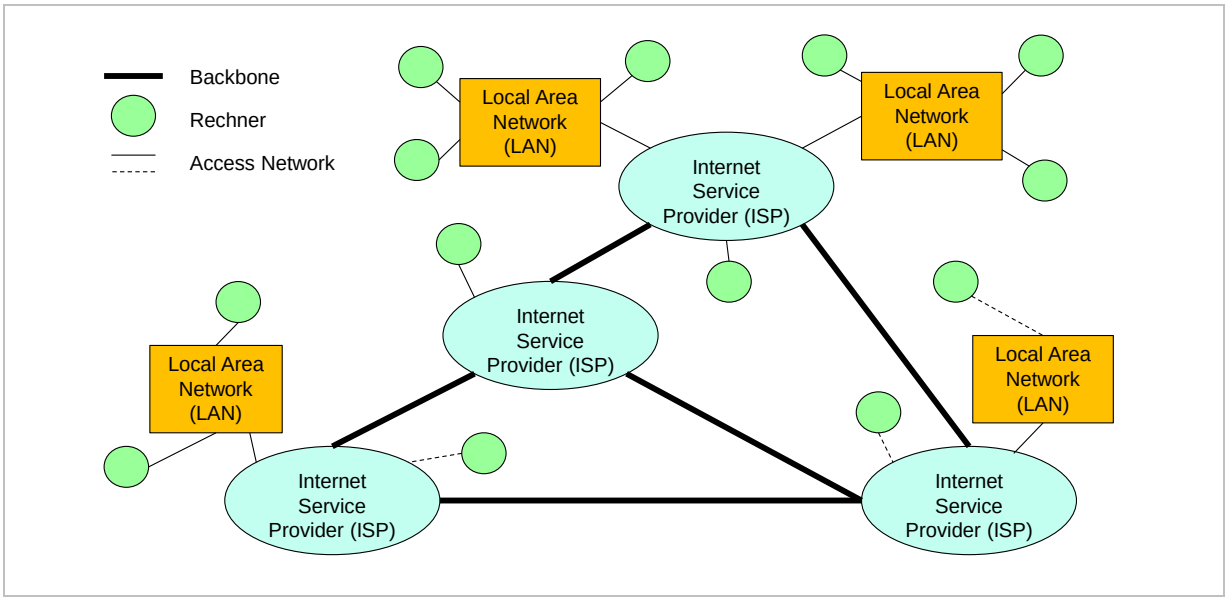


Abbildung 1: Logische Struktur des Internets

2.1.2 Das Internet Protocol im TCP/IP Stack

Das Internet Protokoll (IP) bildet die Grundlage des TCP/IP-Protokollstack. Nach den OSI-Prinzipien werden Aufgaben und Funktionen der Vermittlungsschicht (Layer 3) wahrgenommen, d.h. die Übertragung von Daten zwischen Geräten, die beliebig über verschiedene Netze verteilt sein können (Routing).

Das Internet Protokoll ist:

- **Paketvermittelt**: Jedes IP-Paket ist unabhängig und enthält alle Informationen, die für eine korrekte Weiterleitung erforderlich sind (Header), es werden keine Übertragungsressourcen reserviert.
- **Verbindungslos**: sofortige Übertragung der IP-Pakete, ohne Empfangsbereitschaft zu prüfen.
- **Unbestätigt:** der korrekte Empfang von Datenpaketen wird nicht quittiert

D.h. IP definiert keine spezielle Ende-zu-Ende-Route und die Pakete können in veränderter Reihenfolge ankommen.

Bzgl. der Terminologie ist auf den einzenen Protokollschichten auf die korrekte Bezeichnung der entsprechenden Protocol Data Units (PDU) zu achten

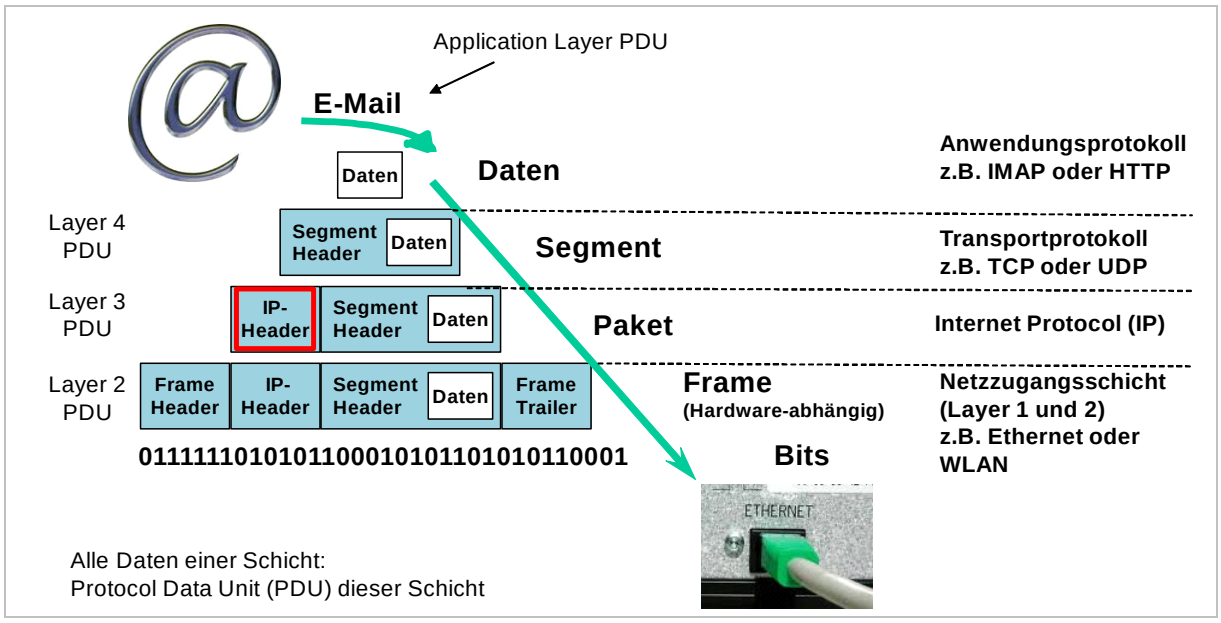


Abbildung 2: Versendung eines Datagramms: Rolle des Internet Protokolls und allgemeine Terminologie

2.1.3 Headerstruktur Internet Protocol Version 4

Die folgende Tabelle und Abbildung zeigt die Struktur eines IPv4 Headers. Auf Details der Adressierung wird in Kapitel 3 näher eingegangen.

Feld	Bedeutung
VERS	Version des IP Protokolls (IPv4 oder IPv6)
IHL	IP Header Length: Länge des IP-Headers, gezählt in 32-bit Einheiten
DS auch Type of Service	Priorisierung von Datenpaketen
Total Length	Länge des gesamten Pakets (inkl. Header) in Bytes (max. 65535 Bytes)
Identification	Kennzeichnung einzelner Fragmente eines Paketes im Falle von Fragmentierung
Flags	
Fragment Offset	
Time to Live (TTL)	Lebensdauer des Pakets. Jede Station (Router) auf dem Weg des Pakets verringert diesen Wert um eins. TTL =0 → Paket wird verworfen.
Protocol No.	Code für L4-Protokoll, zu dem die Daten „geliefert“ werden sollen (SAP)
Header Checksum	Prüfsumme über den Header
Source IP Address	32-bit IP Adresse des Senders
Destination IP Addr.	32-bit IP Adresse des Ziels
Options	Zusatzinformationen (max. 40 Byte)
Padding	Pakete werden auf Vielfache von 32 Bit mit 0-Bits aufgefüllt

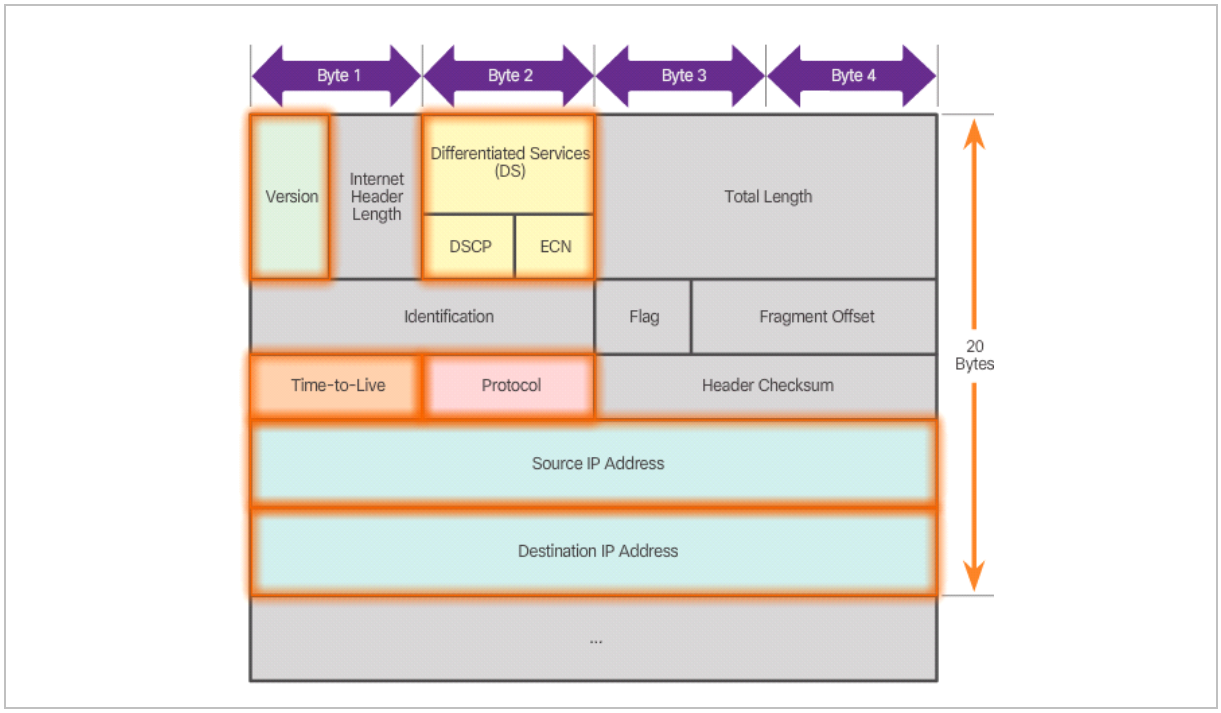


Abbildung 3 IPv4 Header (markiert sind Felder, die auch im IPv6-Header enthalten sind)

2.1.4 Headerstruktur Internet Protocol Version 6

Warum IPv6?

Hauptgrund für die Entwicklung der Internet Protocol Version 6 war die bereits Anfang der 90erJahre vorhersehbare Adressknappheit der 32 Bit langen IPv4 Adressen. Immer mehr Endgeräte weltweit arbeiten vernetzt und benötigen eine eindeutige IP-Adresse. Mit der Erweiterung der Adresse auf 128 Bit in der Version IPv6 sind zukünftige Engpässe auszuschließen.

Der IPv6 Header im Vergleich zu IPv4

Der IPv6 Header hat eine fixe Länge von 40 Byte. Im Vergleich dazu kann der IPv4 Header je nach Anzahl der „Options“ zwar kürzer sein, ein Header fixer Länge generell aber schneller verarbeitet werden. Die Felder im IPv6-Header haben folgende Bedeutung:

- Version: Kennzeichnung der IP-Version (also IPv6)
- Traffic Class (Verkehrsklasse): Priorisierung von Datagrammen
- Flow Label: Markierung von zusammengehörenden Datenflüssen
- Payload Length (Datenlänge): Länge des Datenfelds nach dem IP-Header
- Next Header (nächster Header): An welches Protokoll oder IPv6-Extension sollen die Daten übergeben werden (Vgl. Service Access Point: SAP)? Beispiel: TCP
- Hop Limit: Beim Durchlaufen eines Routers wird die im Hop-Limit-Feld eingetragene Zahl um Eins reduziert. Hat das Hop-Limit-Feld den Wert Null erreicht, wird es verworfen.

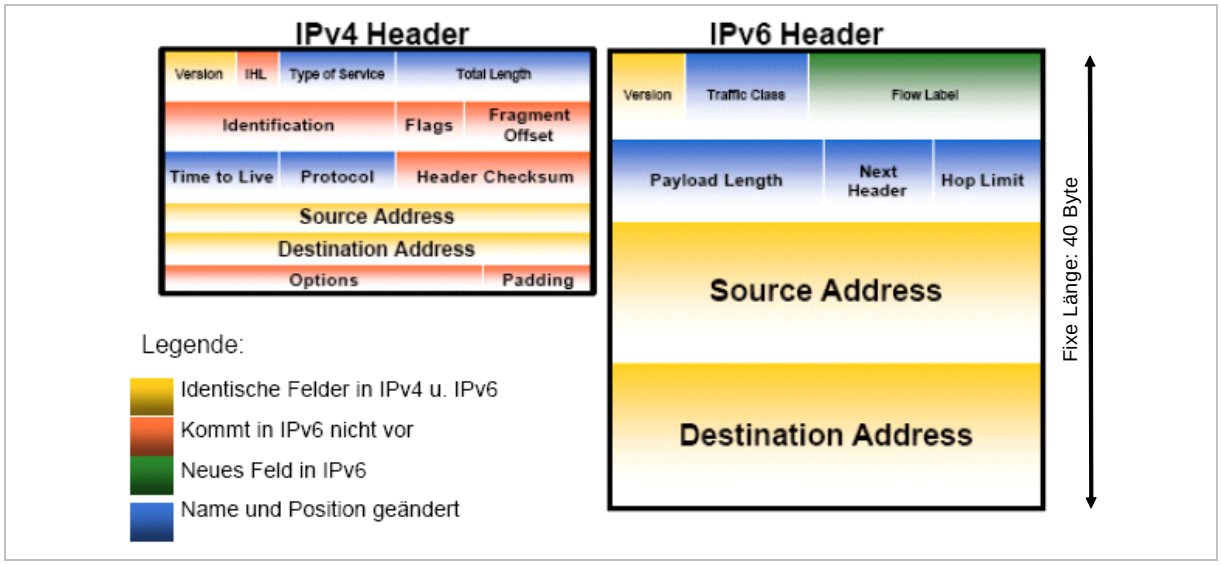


Abbildung 4 IPv4 vs. IPv6 Header (aus http://www.csg.uzh.ch/teaching/ws0405/inteco/extern/talk12.pdf, 6.4.2011)

2.2 Transportprotokolle im TCP/IP Stack

Während ein Protokoll auf der Netzwerkschicht (Schicht 3), speziell Aufgaben der logischen Adressierung und des Routings übernimmt, dienen die Transportprotokolle auf Schicht 4 der grundsätzlichen Unterstützung des Datenaustauschs zwischen zwei Applikationen. Diesbzgl. können Transportprotokolle grundsätzlich folgende Dienste anbieten (teilweise optional):

- Verbindungsorientierte Datenübertragung
- Bestätigte Datendienste
- Flusskontrolle
- Zuordnung der Datensegmente zu Applikationen (Multiplexing)

Die zwei wichtigsten Schicht-4-Protokolle im TCP/IP Stack sind TCP und UDP.

2.2.1 User Datagram Protocol (UDP)

Die wichtigsten Eigenschaften von UDP sind:

- UDP arbeitet als verbindungsloser Datagramm-Zustelldienst ohne Bestätigung
- UDP übernimmt die Beförderung von sogenannten Datagrammen im Netz inkl. Der Zuordnung zu den Applikationen basierend auf der (Socket-)Port-Nummer
- Eine Checksumme zur Überprüfung der Datenintegrität ist optional

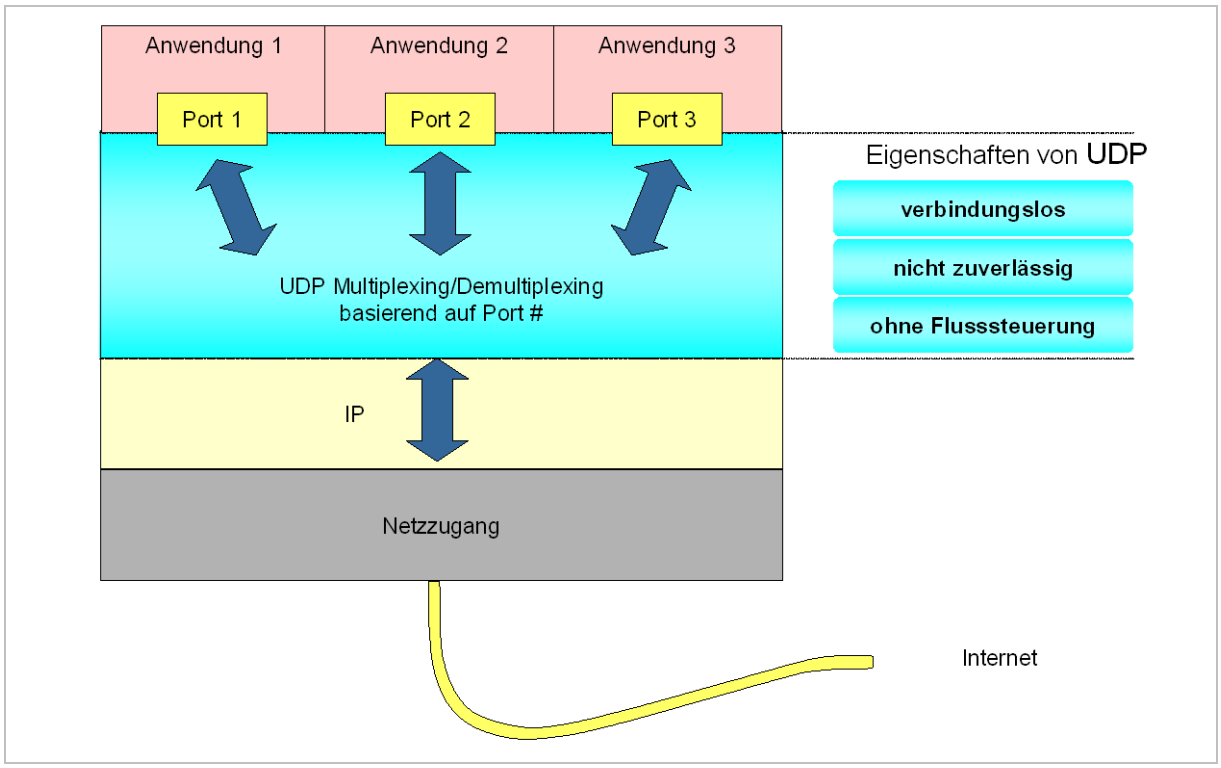


Abbildung 5 UDP und seine Eigenschaften

2.2.2 Transmission Control Protocol (TCP)

Im Vergleich zu UDP stellt TCP den Netzanwendungen die folgenden weiteren wichtigen Dienste bzw. Funktionalitäten zur Verfügung:

- TCP arbeitet als verbindungsorientiert (Three-Way-Handshake)
- Garantierte Zustellung
- Quittierungen und Retransmission bei Paketverlust
- Flusskontrolle (adaptive Anpassung der Senderate)

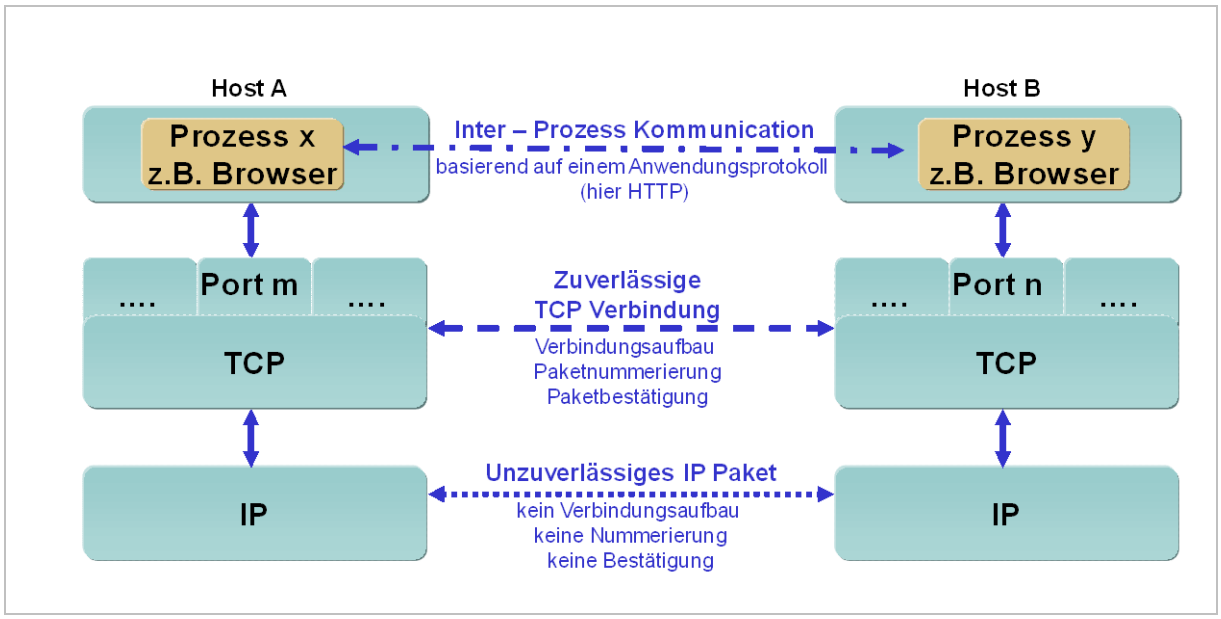


Abbildung 6 Leistungsmerkmale von TCP

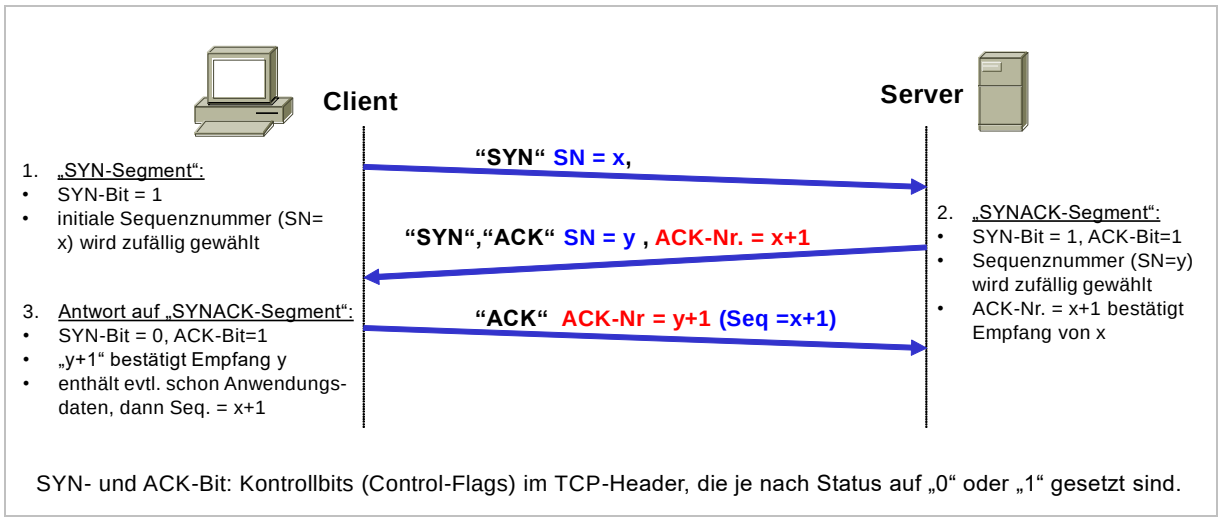


Abbildung 7 Einfacher Three-Way-Handshake im TCP Protokoll

2.2.3 Headerstruktur TCP und UDP

Nachfolgende Abbildung zeigt den TCP-Header. Türkis dargestellt ist die Port-Nummer als Dienstübergabepunkte (Service Acces Point) zur darüberliegenden Anwendung. Gelb sind die für den Three-Way-Handshake wichtigen Felder.

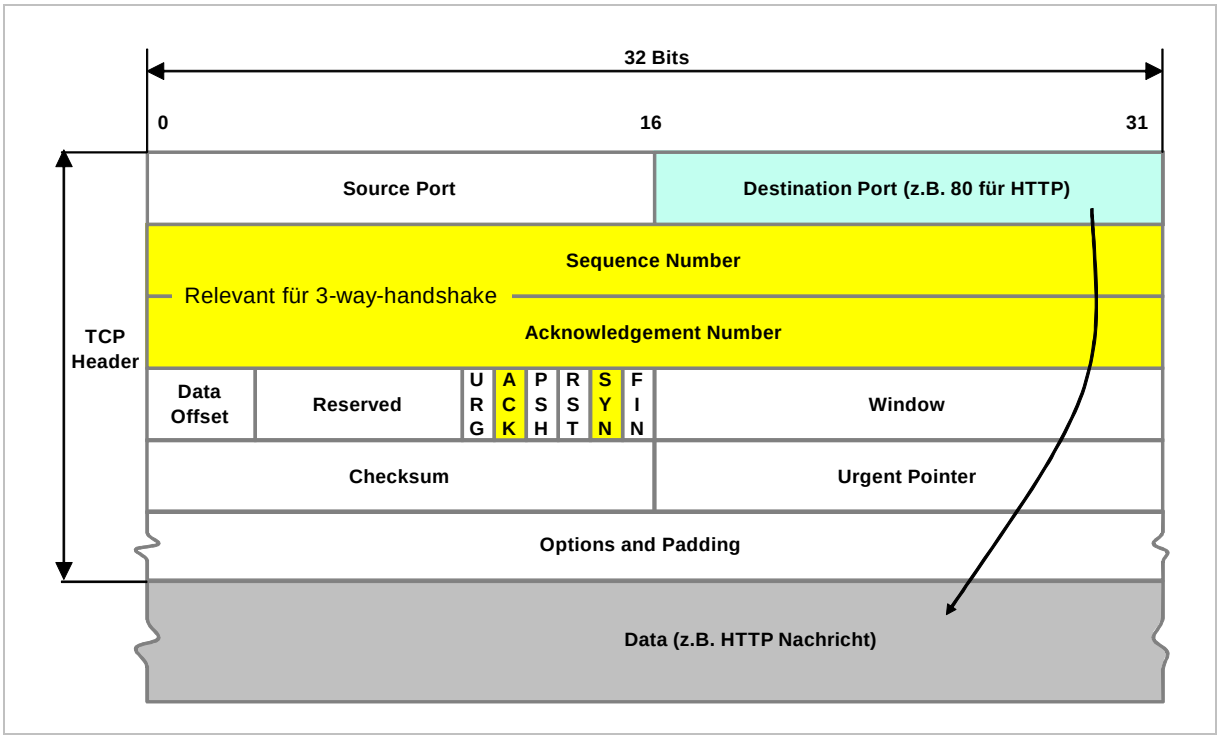


Abbildung 8 TCP Header

Abbildung 9 zeigt ein Datenpaket mit UDP- und IP-Header. Auch hier türkis dargestellt die Dienstübergabepunkte an die nächsthöhere Schicht.

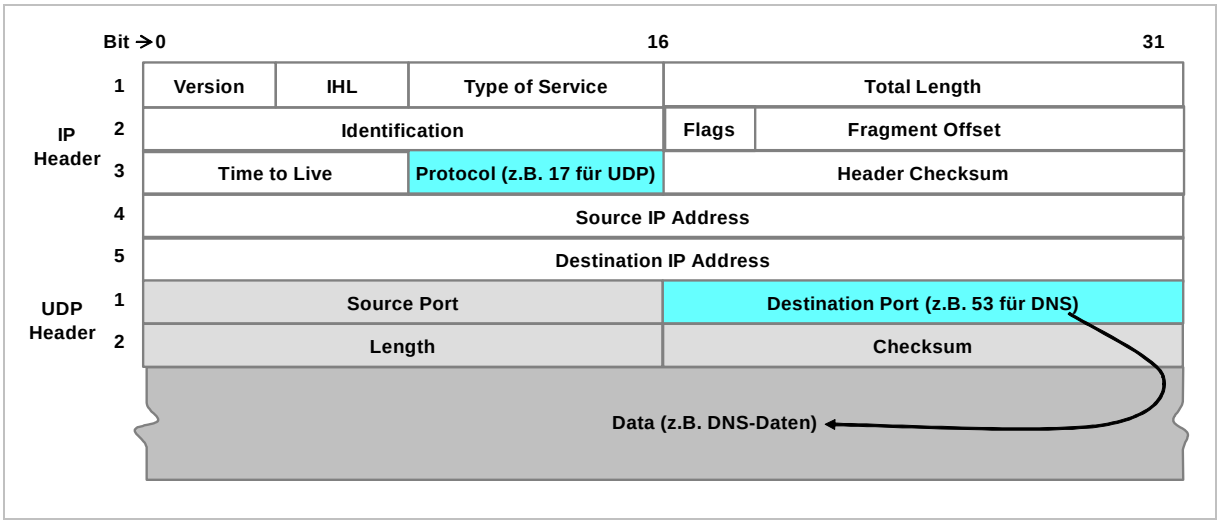


Abbildung 9 UDP Header mit Encapsulation in IP Header

2.3 Netzzugangs- bzw. Sicherungsschicht

2.3.1 IP- und MAC-Adresse

Eine Grundfunktion des Internet Protokolls ist die logische Adressierung eines Datenpakets, um eine weltweit eindeutige Zustellung über Netzgrenzen hinweg zu ermöglichen. Es handelt sich hierbei um eine Ende-zu-Ende-Adressierung, welche bereits von der Applikation festgelegt wird (IP-Adresse).

Jeder Netzwerkadapter/Netzwerkkarte verfügt zusätzlich über eine weitere Adresse auf der Sicherungsschicht. Diese wird auch physikalische, Hardware- oder MAC-Adresse genannt, die sich nicht ändert und üblicherweise auch nicht konfiguriert wird.

Für jedes IP-Paket, das verschickt werden soll, muss die MAC-Adresse bekannt sein, zu der das Paket im nächsten Schritt zugestellt werden soll. Dies ist nicht zwangsläufig bereits der Zielrechner, sondern beispielsweise ein Router, der sich um die Weiterleitung kümmert (z.B. Default Gateway).

Als **Default Gateway** (auch Standardgateway) wird grundsätzlich der Router bezeichnet der ein lokales Netz mit entfernten IP-Netzen verbindet. IP-Pakete, die lt. Adressierung nicht im eigenen Subnetz zugestellt werden können, schickt ein Host immer an dieses Gateway (Gateway-Adresse ist aus der Konfiguration bekannt).

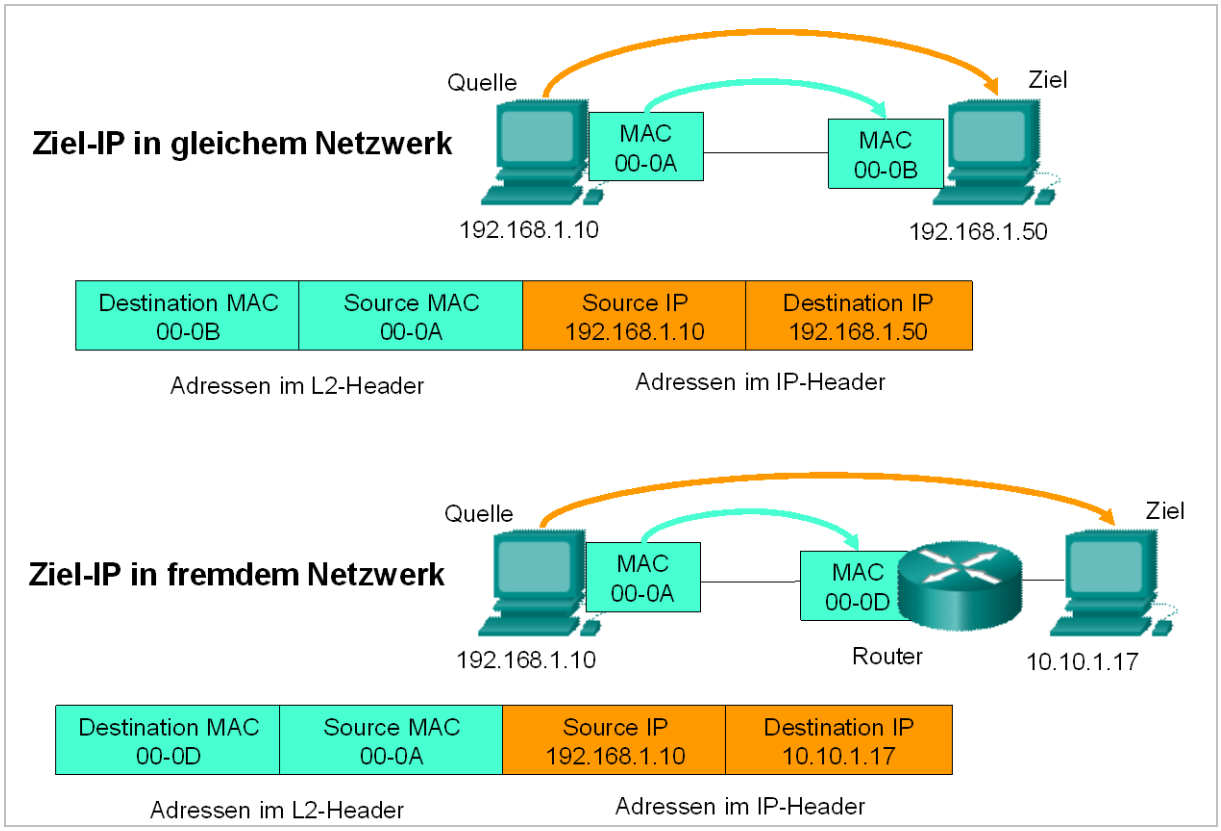


Abbildung 10 MAC- und IP-Adressen bei der Framezustellung

2.3.2 Address Resolution Protocol

Das Address Resolution Protocoll ermöglicht in **IPv4 Umgebungen** das Auflösen/Zuordnen der richtigen Ziel-MAC-Adresse zu einer bekannten Ziel-IP-Adresse.

Üblicherweise dient dem Sender eine Lookup-Tabelle dazu, die zu einer IP-Adresse zugehörige MAC Adresse zu bestimmen (Adress Resolution). Sofern kein Eintrag zu einer bestimmten IP-Adresse gefunden wird, erfolgt mit Hilfe des **Address Resolution Protocols (ARP)** ein Broadcast auf Layer 2 mit einer entsprechenden **ARP request** message. ARP setzt dabei unmittelbar auf den Diensten der Schicht 2 auf.

Ziel-IP im eigenen Netz

Sobald einer der Hosts die gewünschte/gesuchte IP-Adresse als seine eigene erkennt, schickt er eine **ARP reply** message an den anfragenden Host zurück. Diese Antwort enthält die HW-Adresse (MAC) des Zielhosts, welche nun auch im ARP cache (Lookup-Tabelle) gespeichert wird. ARP-Einträge werden nach einem bestimmten Zeitintervall wieder gelöscht (je nach System 2-20 Minuten).

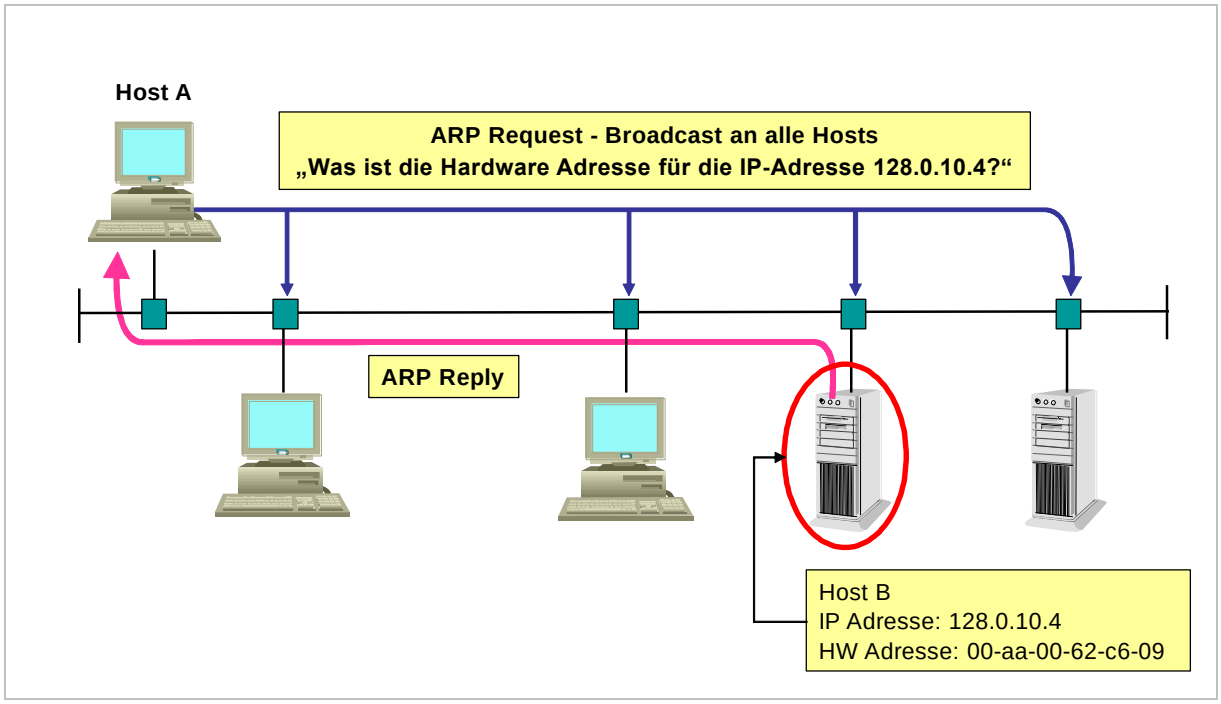


Abbildung 11 Funktionsweise von ARP (Zielhost lokal)

Ziel-IP in entferntem Netz

Befindet sich eine Ziel-IP-Adresse nicht im gleichen lokalen Netz (Subnetz) muss das Paket grundsätzlich an das Default Gateway geschickt werden. D.h. ARP sucht nicht die IP des Zielrechners, sondern die des Gateways. Diese ist entweder im ARP-Cache des Ursprungshosts vorhanden oder wird über einen lokalen ARP-Request aufgelöst, sodass letztendlich die MAC-Adresse des Default Gateways bekannt ist.

In den weiteren Hops wird sich dieser ARP-Ablauf wiederholen, bis das Paket den Zielrechner erreicht hat.

Die MAC-Adresse für einen Layer-2 Broadcast lautet FF-FF-FF-FF-FF-FF

MAC-Adressen Auflösung in IPv6 Netzwerken

Auch in IPv6 Netzwerkumgebungen muss für die Paketzustellung eine gültige MAC-Adresse gefunden werden. Verantwortlich hierfür ist nicht ARP, sondern das Anwendungsprotokoll Internet Control Message Protocol (ICMPv6), welches im folgenden Abschnitt näher behandelt wird.

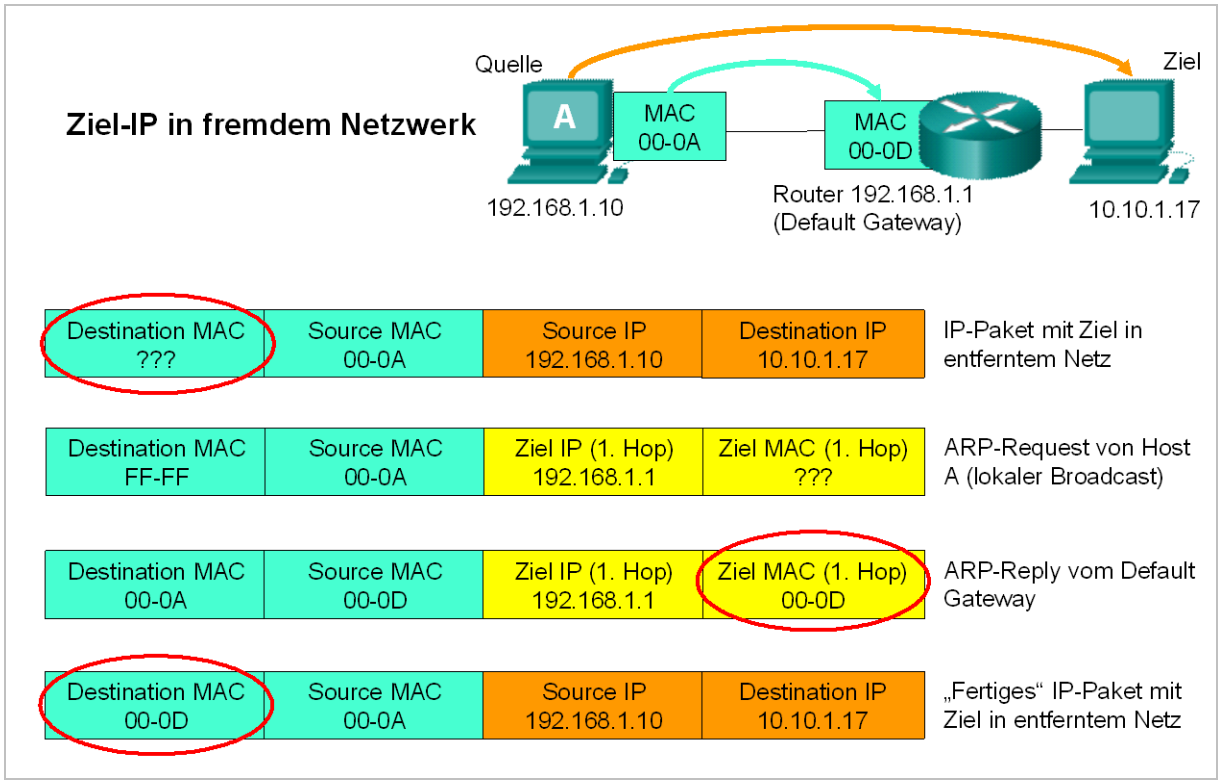


Abbildung 12 Funktionsweise von ARP (Zielhost remote)

2.4 Das Internet Control Message Protocol

2.4.1 ICMP: Grundfunktionen und Headeraufbau

Das Internet Control Message Protocol (ICMP) wird verwendet, um Informations- und Fehlermeldungen in IP basierten Netzen auszutauschen. Nachrichten dieses Protokolls sind dem OSI-Layer 3 zuzuordnen und werden in Standard IP-Paketen versendet. Sie sollten von jedem IP-fähigen Endgerät verstanden und auch generiert werden können. Eine der bekanntesten ICMP-Anwendungen ist das Ping-Kommando, welches die grundsätzliche Erreichbarkeit eines Rechners prüft und auch Aussagen bzgl. der Verarbeitungs- und Signallaufzeiten zulässt.

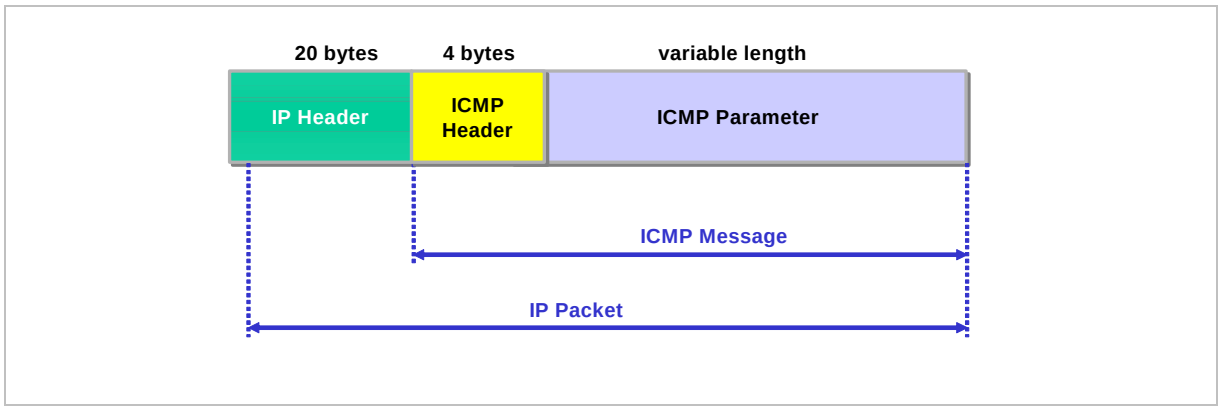


Abbildung 13 Encapsulation einer ICMP Nachricht

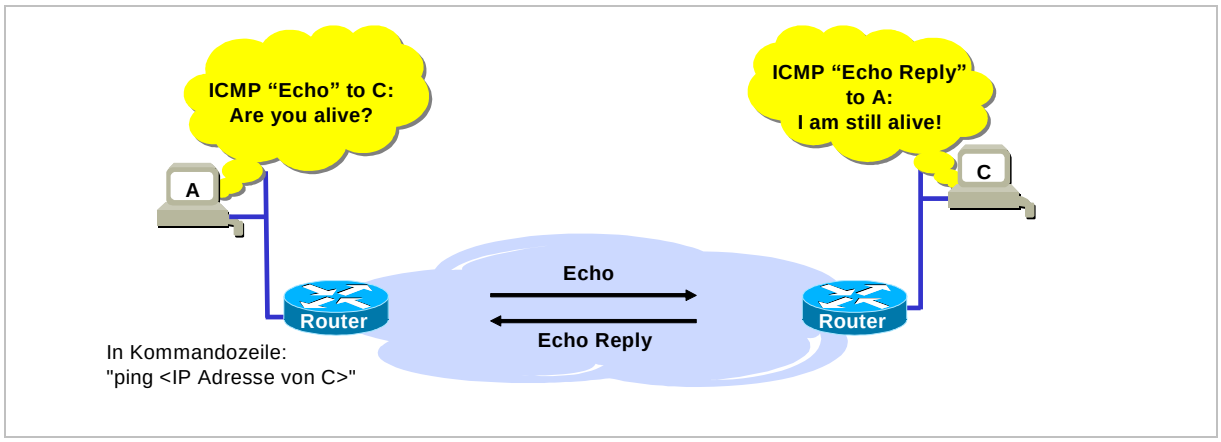


Abbildung 14 ping Anwendung mithilfe ICMP

2.4.2 Adressierungsdienste mit ICMPv6

Im Zusammenhang mit IPv6 wurden einige erweiterte Funktionen des Internet Control Message Protocol (ICMPv6) definiert. Diese beinhalten u.a. fünf neue Nachrichtentypen für das sogenannte *Neighbor Discovery Protocol* (NDP). Eine Aufgabe dieses Protokolls ist die Zuordnung von MAC-Adressen zu bekannten IP-Adressen (vergleichbar mit ARP für IPv4):

1. Versendung einer ICMP-Neighbor-Solicitation-Nachricht als Multicast auf dem lokalen Link
2. Antwort in Form einer ICMP-Neighbor-Advertisement-Nachricht als Unicast

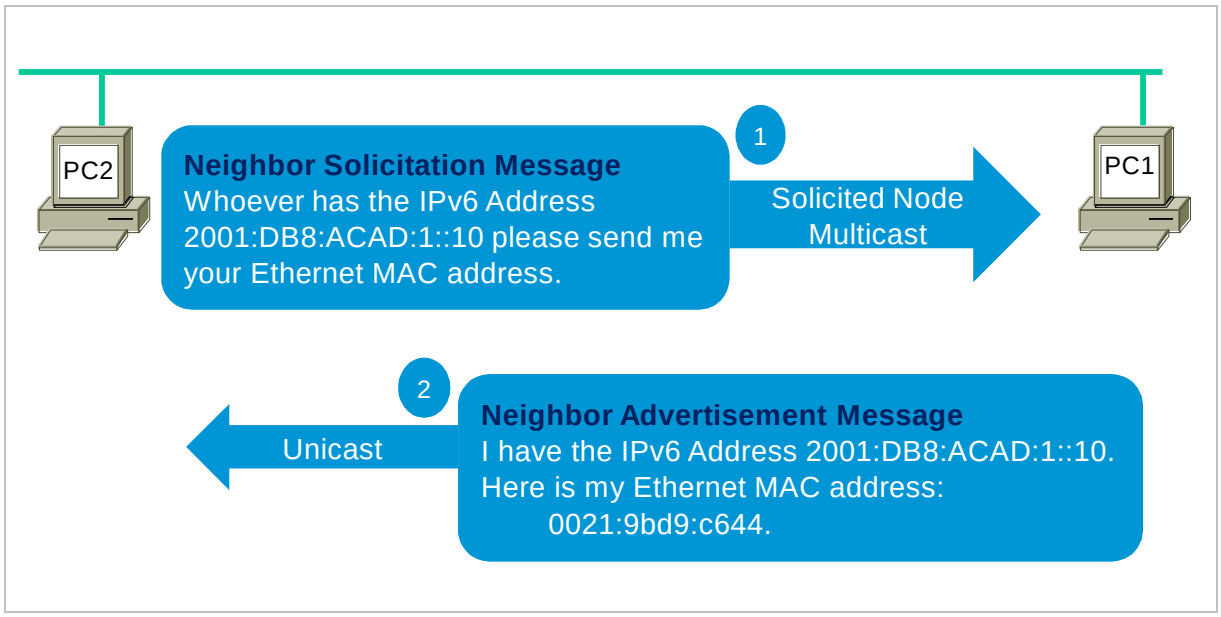


Abbildung 15 Adressauflösung IPv6 -> MAC mit Hilfe von ICMPv6

2.5 Wichtige Netzwerkkomponenten

Wie im Kapitel 1 bereits erwähnt gibt es neben den Endgeräten einige wichtige Komponenten im Netz, deren Hauptfunktion speziell durch ihre Arbeit auf einem bestimmten TCP/IP-Layer definiert ist. Dies sind:

- Router, Layer 3 Switch: Schicht 3 = Network Layer

  Router sind Netzwerkgeräte, die mehrere Rechnernetze (auch weltweit) miteinander verbinden. Dabei analysiert der Router die ankommenden Datenpakete nach ihrer Ziel-IP-Adresse und leitet sie entsprechend weiter. Die Pakete gelangen entweder direkt an ihr am Router angeschlossenes Zielnetz oder werden zu einem anderen direkt angeschlossenen Router weitergeleitet.

- Klassischer Switch: Schicht 2 = Data Link Layer

  Ein klasischer Switch (NICHT Layer3-Switch) agiert als Relaisstationen zwischen LANs und arbeiten auf Layer2. Ein Switch leitet Informationen selektiv basierend auf der MAC-Adresse zwischen den Netzen weiter, anders als der Layer3-Switch, der auch IP-Adressen „versteht“.

  Bei der Verbindung von unterscheidlichen LAN-Technologien redet man auch von einer Bridge (statt Switch)

- Repeater, Hub: Schicht 1 = Physical Layer

  Der Repeater übernimmt den Empfang von Signalen zwischen zwei LAN-Segmenten, regeneriert und verstärkt sie und gibt sie weiter. Er verbindet somit mehrere Netzwerk-Segmente, allerdings ohne die verfügbare Bandbreite in jedem einzelnen Segment zu erhöhen.

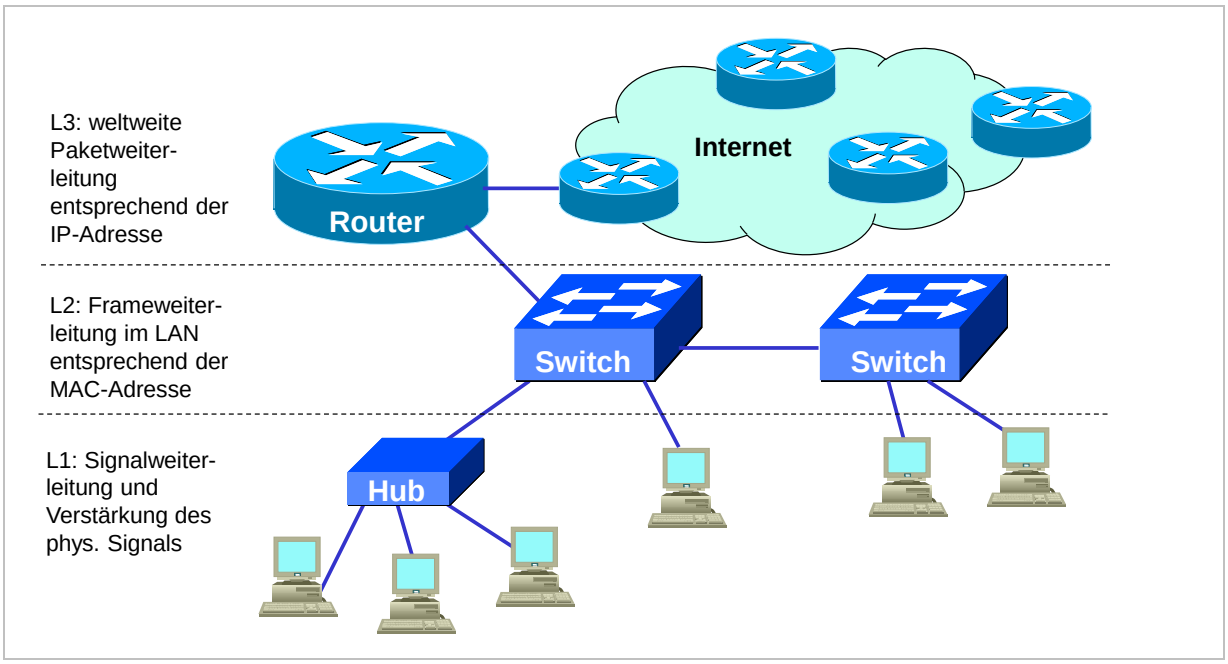


Abbildung 16: Wichtige Hardware Komponenten in einem Netzwerk

2.5.1 Die Grundfunktionen eines Routers

Grundsätzlich zuständig für die Wegewahl in einem IP Netz sind die **Router**. Sie treffen ihre Entscheidung, auf welchem Interface ein eingehendes Paket ausgesandt werden muss, entsprechend einer **Routing-Tabelle**.

Hop-by-Hop-Routing

IP-Pakete, die in großen Netzen unterwegs sind, passieren häufig eine Vielzahl von IP-Routern, ehe sie ihr Ziel erreichen. Ihr Weg wird dabei nicht durch eine zentrale Stelle bestimmt. Jeder Router legt lediglich den nächsten Streckenabschnitt ("Hop") des Weges fest und sendet das IP-Paket entsprechend seiner Routingtabelle weiter. Dieser Vorgang gilt für jedes einzelne IP-Paket.

Routing-Protokolle

Grundsätzlich können Routingtabellen manuell in jedem Router durch den Netzadministrator eingegeben werden. Meist wird dieser Vorgang jedoch mit Hilfe von Routing-Protokollen automatisiert. Routing-Protokolle dienen dem Austausch von Routinginformationen zwischen den Netzen/Routern und sorgen dafür, dass die Routingtabellen automatisch aufgebaut und aktualisiert werden. Die ordentliche Verwaltung und Pflege der Routingtabellen speziell in einem großen Netzwerk gestaltet sich dabei oft als schwierige Aufgabe, da sich Netzkonfigurationen laufend ändern können. Fehler in den Routingtabellen können die Kommunikation stark beeinträchtigen.

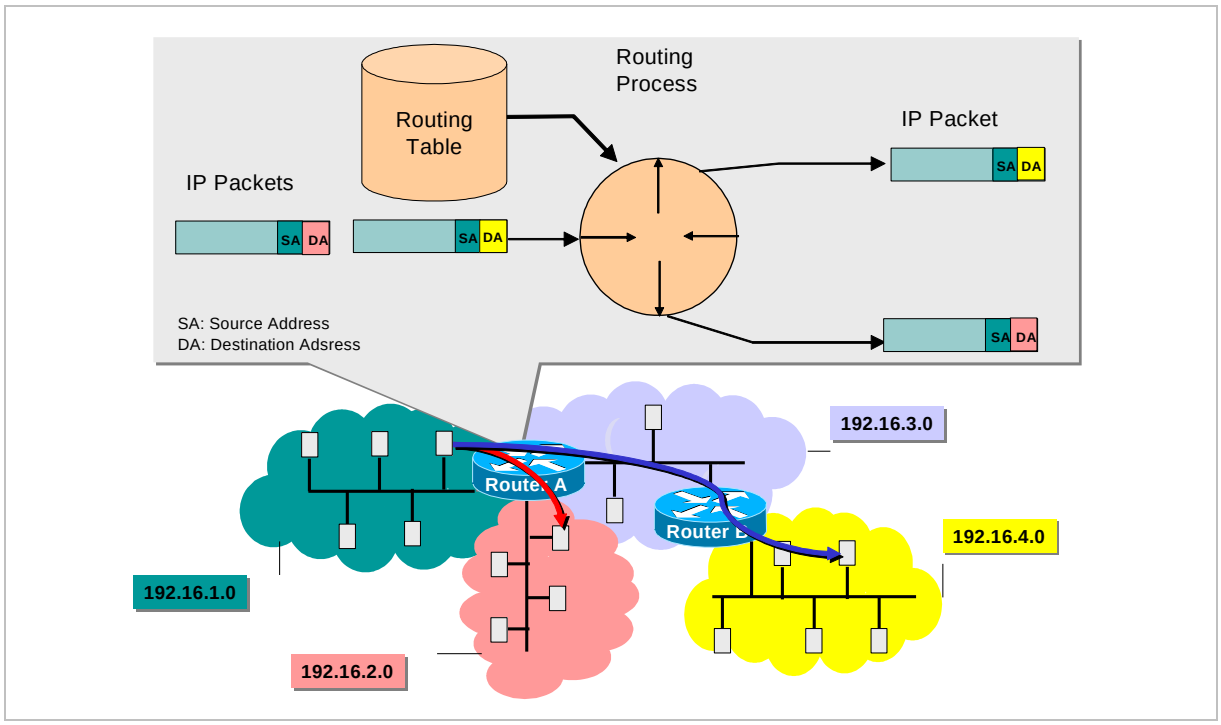


Abbildung 17 Routing Tabelle und Routing Entscheidung

2.5.2 Die Grundfunktionen eines Switches

Die Hauptfunktion eines Switches ist die Weiterleitung eines Daten-Frames basierend auf der Ziel-MAC-Adresse. Das Durchschalten der Datenframes basiert auf einer Adressdatenbasis, auch ***content addressable memory* (CAM).** Um diese Datenbasis sinnvoll zu füllen, lernt ein Switch automatisch anhand der Source Adressen aller ankommenden Frames. Falls kein Eintrag bzgl. der Zieladresse zu finden sind, wird der Frame an allen Ports ausgesendet (außer Eingangsport)

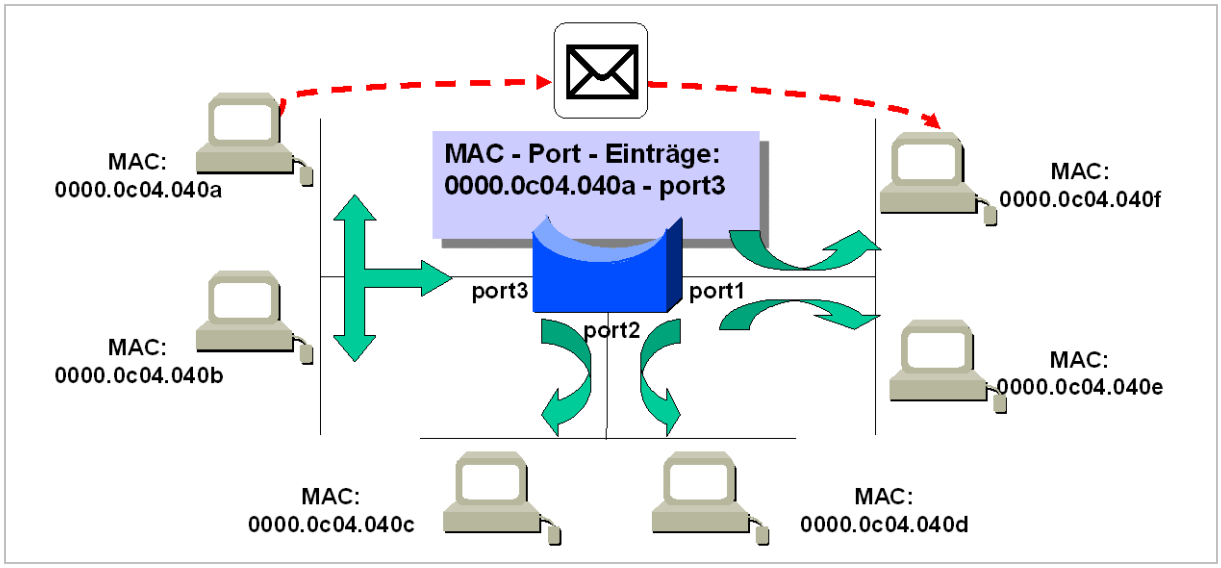


Abbildung 18 Address Learning Mechanismus (a)

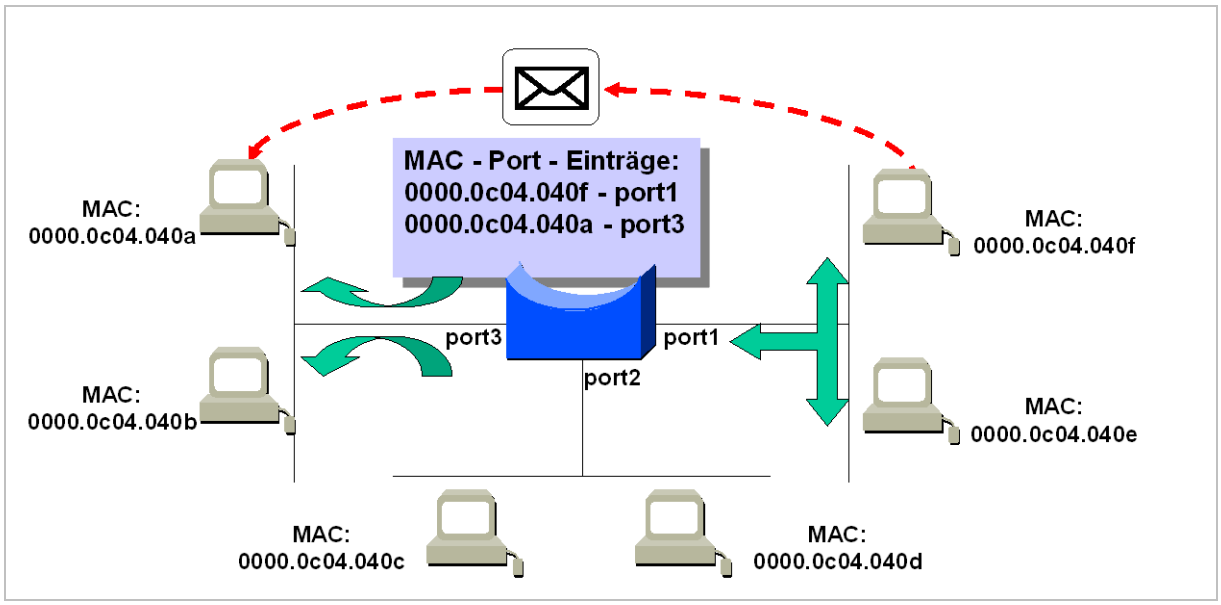


Abbildung 19 Address Learning Mechanismus (b)

2.5.3 Das Prinzip des Virtuellen LAN

Ein LAN ist prinzipiell ein Netz, welches auf einen engen geografischen Bereich eingeschränkt ist. Ethernet ist der diesbzgl. am weitesten verbreitete Standard. Im Falle des Ethernet endet das LAN logisch gesehen am Router. Alle Rechner eines LAN's befinden sich in einer Broadcastdomäne und sind über die Hardwareadresse FF:FF:FF:FF:FF:FF (MAC-Adresse) gemeinsam ansprechbar. Üblicherweise ist ein Endgerät dabei direkt an einem Switch angeschlossen.

Unter einem virtuellen LAN (VLAN) versteht man die organisatorische Strukturierung eines physikalischen LANs in mehrere (virtuelle) Gruppen, was im Standard IEEE 802.1Q spezifiziert ist. VLANs haben folgende Eigenschaften:

- Jedes VLAN stellt eine eigene Broadcastdomäne dar (eigenes IP-Netz)
- Zwischen verschiedenen VLANs können Pakete nur über Router ausgetauscht werden
- Die Strukturierung/Organisation der VLANs erfolgt im Layer2-Gerät (Switch)
- Endgeräte sind sich ihrer jeweiligen VLAN-Zugehörigkeit nicht bewusst

Virtuelle LANs haben u.a. folgende wichtige Vorteile:

- Verkleinerte Broadcastdomänen
- Leichteres Netzwerkmanagement
- Erhöhte Netzsicherheit

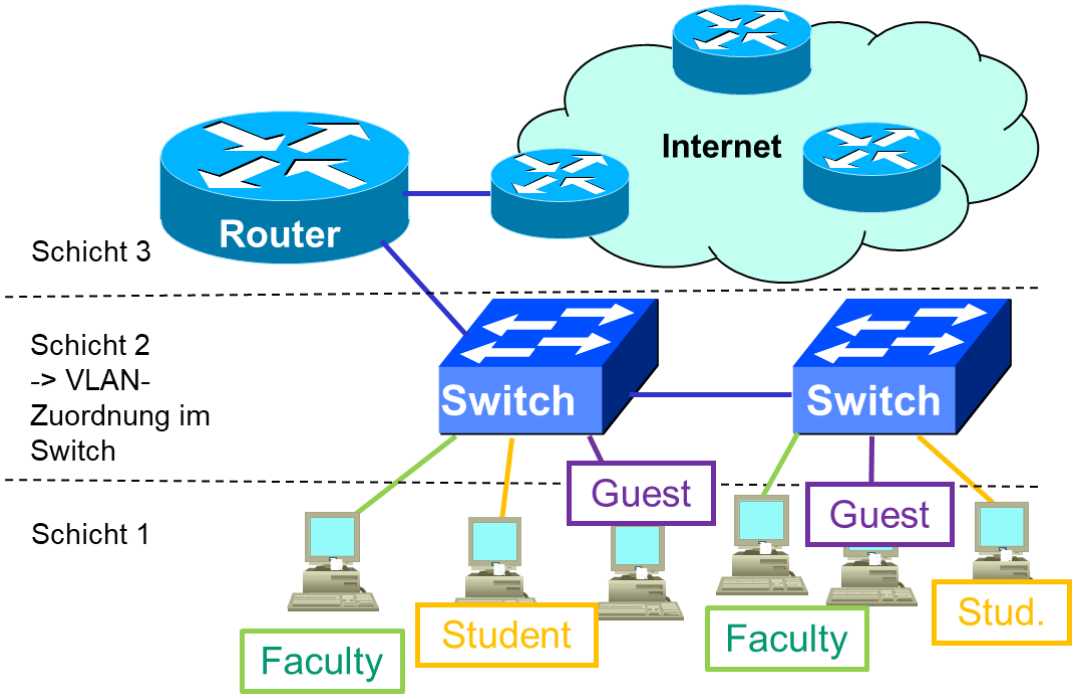


Abbildung 20 Virtuelles LAN

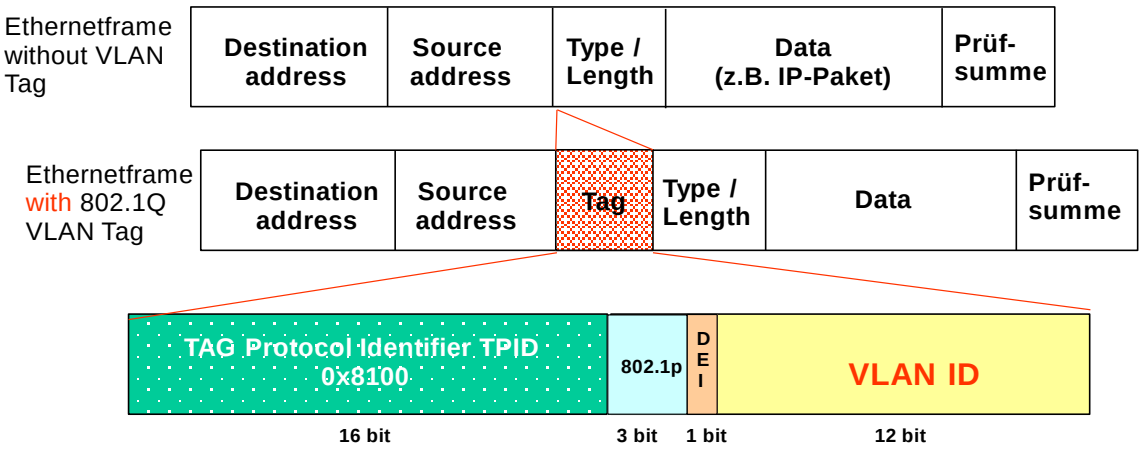
Die Zugehörigkeit zu einem VLAN kann unterschiedlich definiert werden:

- VLAN Zugehörigkeit basierend auf der Portnr. des Anschlusses am Switch.
- VLAN Zugehörigkeit basierend auf der MAC-Adresse. Damit können Stationen auch an andere Ports angeschlossen werden (umziehen), ohne, dass sich die VLAN-Zugehörigkeit ändert.
- VLAN Zugehörigkeit basierend auf Informationen aus dem Layer 2 Header (VLAN-Tag).

Tagging

Um VLAN-Zugehörigkeiten über Switchgrenzen hinaus zu realisieren, müssen die Frames entsprechend gekennzeichnet werden (engl. Tagging). Jedes VLAN bekommt dazu eine bestimmte VLAN-ID zugewiesen, die den einzelnen Frames bei der Kommunikation zwischen den Switches hinzugefügt wird.

Das VLAN Tagging Schema nach 802.1Q beschreibt das Einfügen von vier Bytes in den MAC-Frame. Das TPID oder "802.1Q Tag Type" Feld enthält dabei immer den Wert "**0x8100**", um den Frame als „getaggt“ zu kennzeichnen.



802.1p: 3-bit Feld, in dem Prioritätsinformationen bzgl. des Frames eingefügt werden können.
DEI: Flag, um den Frame zu markieren, dass er im Fall einer Überlastung verworfen werden könnte
VLAN-ID: Spezifiziert das VLAN, zu dem ein Frame gehört.

Abbildung 21 802.1Q VLAN Tag Header

3 Adressierung mit dem Internet Protokoll

3.1 Grundsätzliche Eigenschaften von IP Adressen

Grundsätzlich sind Network-Layer Adressen logisch und meist hierarchisch organisiert und werden administrativ vergeben, so auch die IP-Adressen. Jedes IP-Paket enthält in seinem Header neben anderen Informationen eine Ziel- und eine Ursprungs-IP-Adresse.

IP Adressen bestehen aus einem **network part** (network prefix) und einem **host part**. D.h. sie sind in der Form strukturiert, dass sie grundsätzlich aus einem Adressteil bestehen, der das Netzwerk identifiziert und einem weiteren Teil, der einen bestimmten Host innerhalb dieses Netzwerks adressiert.

Routing basiert auf der Netzwerkadresse: Router leiten IP-Pakete allein aufgrund der Netzwerkadresse durch das Netz. Erst der letzte Router, welcher zum Zielnetz gehört, evaluiert die gesamte Adresse und übergibt das Paket in das lokale Netz bzw. an den Zielhost.

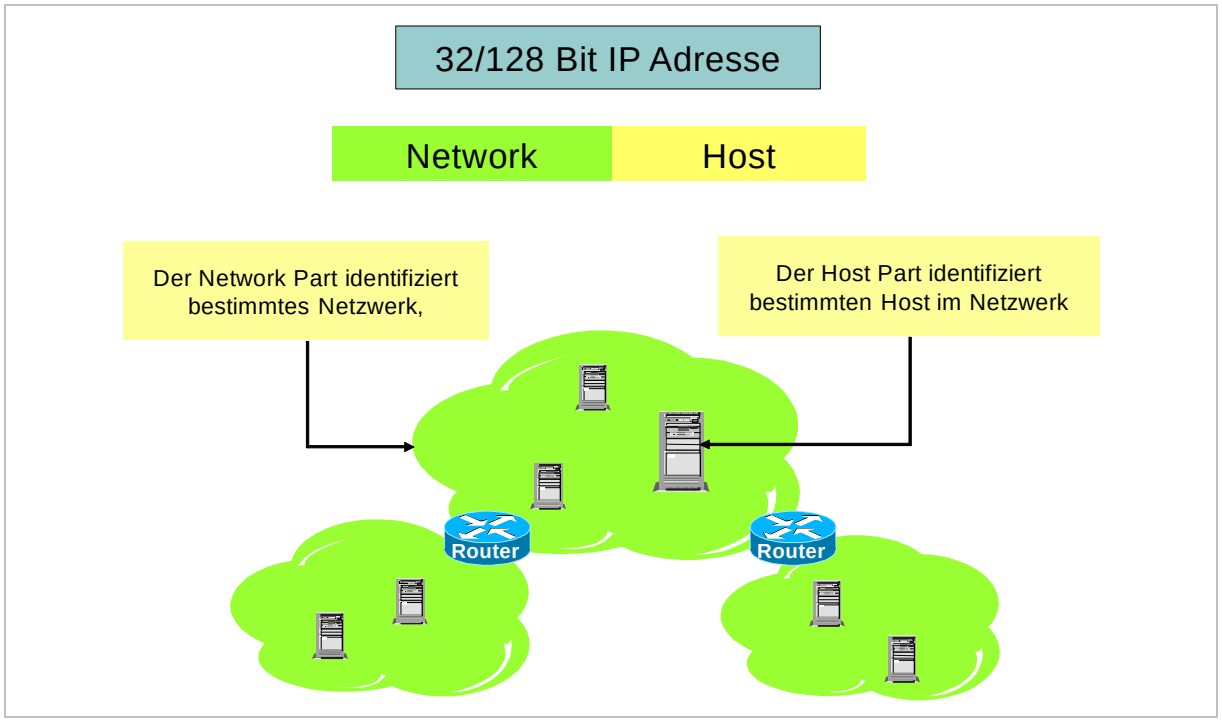


Abbildung 1 Network und Host Part der IP Adresse

Im Folgenden wird zunächst auf die momentan noch gängigere Version 4 des Internet Protokolls (IPv4) eingegangen. Ein Überblick zu Version 6 (IPv6) folgt im dritten Abschnitt dieses Kapitels.

3.2 Adressierung IPv4

Die IP Version 4 (IPv4) definiert eine 32-bit Adresse. Das bedeutet, dass insgesamt nur 2^{32} IPv4 Adressen zur Verfügung stehen. Einer der Gründe, weshalb IPv6 entwickelt wurde.

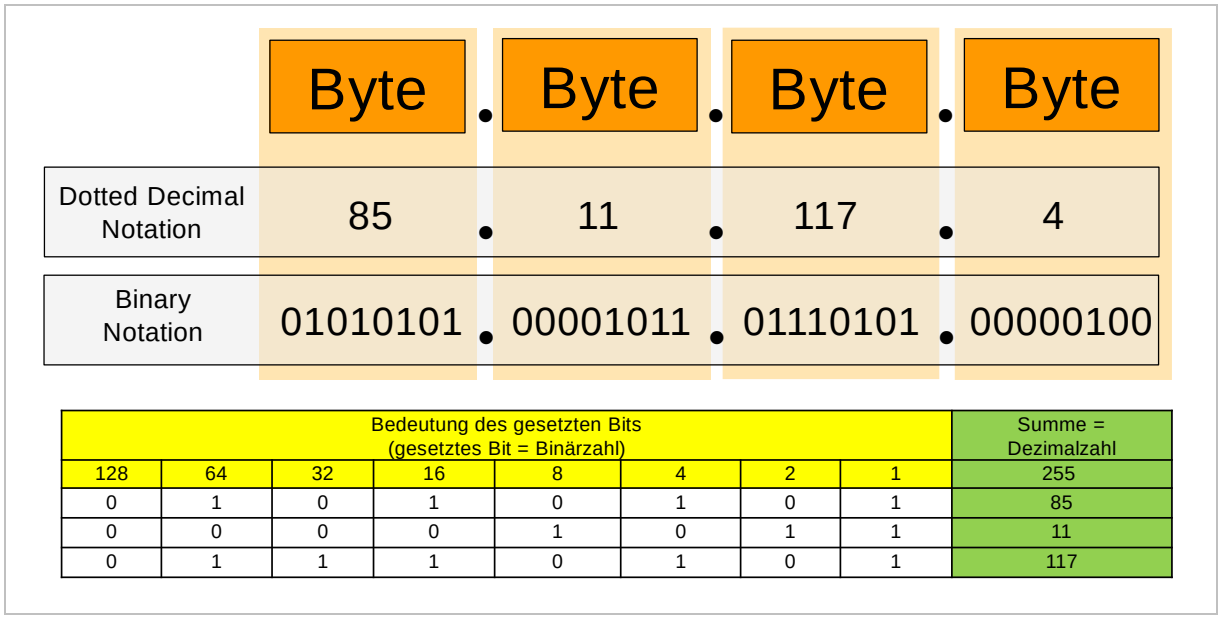
3.2.1 Dezimale und Binäre Notation von IP Adressen

Eine IP Adresse besteht aus 32 Bits, d.h. 4 Oktetts bzw. 4 Byte. Um die Les- und Schreibbarkeit der Adressen zu vereinfachen, werden IP-Adressen meist als vier Dezimalzahlen dargestellt, welche mit einem Punkt voneinander abgetrennt werden ("dotted-decimal notation").

Dabei entspricht eine Dezimalzahl genau einem 8-Bit-Feld der ursprünglichen binären Notation.

Die dezimale Notation ist die gebräuchlichere Form. Speziell beim Arbeiten und Rechnen mit Subnetzen macht es jedoch oft Sinn, zumindest byteweise das binäre Format zu verwenden.

Die zentrale Vergabe und Verwaltung der IP Adressen erfolgt durch die Internet Assigned Numbers Authority (IANA), diese wiederum vergibt Adressblöcke an regionale Registrare zur Weitergabe im jeweiligen Zuständigkeitsbereich.



Bedeutung des gesetzten Bits (gesetztes Bit = Binärzahl)								Summe = Dezimalzahl
128	64	32	16	8	4	2	1	255
0	1	0	1	0	1	0	1	85
0	0	0	0	1	0	1	1	11
0	1	1	1	0	1	0	1	117

Abbildung 2 Struktur einer IP Adresse

3.2.2 Reservierte IP Adressen und Adressbereiche

Untenstehende Tabelle zeigt IP Adressen, welche eine vordefinierte Rolle im Rahmen von TCP/IP Kommunikationsabläufen spielen.

Host-Bits alle 0	ID des jeweiligen Netzwerks
Host-Bits alle 1	Broadcast des jeweiligen Netzes (directed Broadcast)
Adresse 127.x.x.x	Loopback Adresse
0.0.0.0	als Source Adresse (falls keine gültige IP Konfiguration vorhanden) oder Default Route (in der Routing Tabelle eines Routers)
255.255.255.255	Broadcast Adresse des aktuellen lokalen Netzes

Multicast Adressen

Multicast beschreibt die Kommunikation eines Hosts mit einer ausgewählten Gruppe anderer Host (vgl. Broadcast: ALLE anderen Host). Wie auch beim Broadcast, wird nur ein Paket vom Sender-Host ausgesandt, welches entsprechend der Adressierung aber mehrere Ziel-Hosts erreichen kann. Der hierfür reservierte IP-Adressbereich ist:

⇒ 224.0.0.0 – 239.255.255.255 (Klasse D)

Private IP Adressen

Bestimmte Adressbereiche können nur innerhalb eines privaten bzw. lokalen Netzes genutzt werden. Man redet hier von privaten IP-Adressen, welche zwar innerhalb eines solchen Netzes eindeutig sein müssen, in einem anderen privaten Netz aber wieder verwendet werden können. Sie werden von Routern im öffentlichen Netz ignoriert und müssten für eine Kommunikation "nach draußen" in eine öffentliche IP-Adresse übersetzt werden (Network Address Translation: NAT).

Folgende Adressbereiche sind für den privaten Gebrauch reserviert und können innerhalb entsprechender Netzen frei verwendet werden:

⇒ 10.0.0.0 - 10.255.255.255

⇒ 172.16.0.0 - 172.31.255.255

⇒ 192.168.0.0 - 192.168.255.255

Weiterhin steht der Adressbereich ***240.0.0.0 – 255.255.255.255*** nicht zur freien Vergabe zur Verfügung, kann aber zu Test- und Forschungszwecken verwendet werden (Klasse E).

3.2.3 Subnetzmasken

Subnetzmasken bestimmen die Anzahl der Bits, welche als Network Part anzusehen sind. Sie werden in der gleichen dezimalen Notation wie die IP-Adressen angegegeben. In binärer From geschrieben bedeutet jede gesetzte "1" der Subnetzmaske, dass das entsprechende Bit der IP-Adresse zum Network-Part gehört, eine "0" in der Subnetzmaske definiert den Hostteil der IP-Adresse.

Es gibt auch die so genannte Prefix-Notation:

<IP-Adresse> / <Anzahl der Bits im Networkpart>

Die Anzahl der Bits im Network-Part wird *Prefix-Length* genannt.

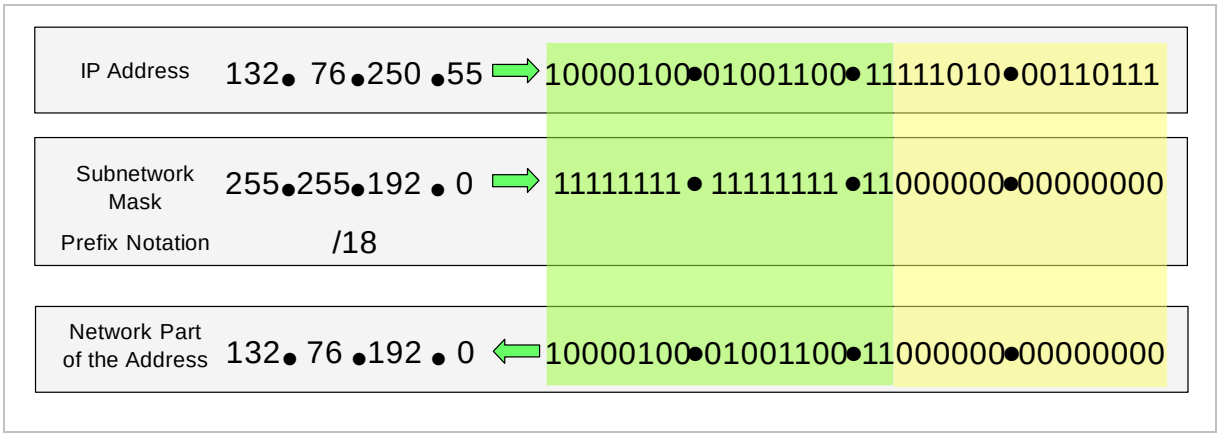


Abbildung 3 Rechnen mit der Subnetzmaske

Die in einem IP-Netz für den Hostpart verbleibenden Bits dienen der Adressierung der Hosts. Bzgl. der möglichen Binärkombinationen sind zwei Adressen vorgegeben:

- Alle Hostbits „0“: Netzwerk-Adresse des entsprechenden Netzes
- Alle Hostbits „1“: Broadcast-Adresse des entsprechenden Netzes

Beispiel: Rechnen mit IP-Adressen und Subnetzmasken (Spalte 2 selber ausfüllen)

IP Adresse	153.1.14.97	192.168.237.143
Prefix (auch Classless Interdomain Routing: CIDR)	/22	/25
Subnetzmaske	255.255.252.0	
Anzahl der Host Bits	10	
Anzahl verwendbarer Hosts	2^10-2	
Netzadresse	153.1.12.0	
Broadcastadresse	153.1.15.255	
Host IP Adressbereich	153.1.12.1-153.1.15.254	

3.2.4 IP-Adressklassen (in der Praxis veraltet)

Ursprünglich wurden IP-Adressen strikt in Class A, B und C Adressen unterteilt und eindeutige Adressbereiche den jeweiligen Klassen zugeordnet. Diese Klassen unterscheiden sich grundsätzlich in der Anzahl der Bytes, welche für die Identifizierung des Network-Part verwendet werden. Dadurch ergeben sich für die verschiedenen Adressklassen unterschiedlich viele verfügbare/verwaltbare Netze bzw. Hostadressen. Auch Class D und E Adressen wurden definiert, welche allerdings nie zur Adressierung von Geräten verwendet werden (Multicast bzw. "zukünftige Anwendungen").

Address Class	Binary Subnetmask	Decimal Subnetmask	Prefix
Class A	11111111 00000000 00000000 00000000	255.0.0.0	/8
Class B	11111111 11111111 00000000 00000000	255.255.0.0	/16
Class C	11111111 11111111 11111111 00000000	255.255.255.0	/24

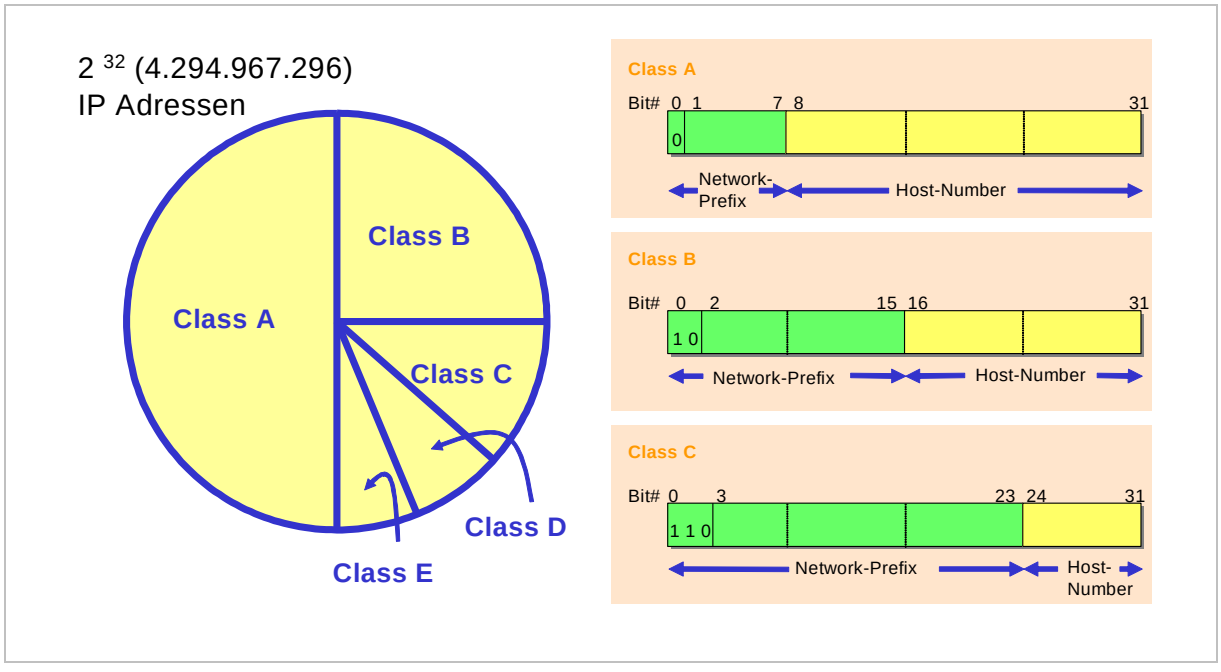


Abbildung 4 IPv4 Adressklassen

3.2.5 Subnetze

Das starre Schema der Class A, B and C Adressen wurde immer weniger den wachsenden Kommunikations- und Adressierungsanforderungen gerecht. Deshalb wurde das Konzept der Subnetze eingeführt.

Bzgl. der Adressierung passiert beim Subnetting folgendes: Ursprünglich für die Hostadressierung bestimmte Bits der 32 Bit langen IP-Adresse dienen nun zur Identifizierung der Subnetze.

Zur Identifizierung der Grenze zwischen Netzwerk- und Hostanteil in einer IP-Adresse dient die bereits beschriebene Subnetzmaske.

Subnetze und Subnetzmasken ermöglichen dem Administrator, ein ursprünglich großes Netzwerk in mehrere kleinere Subnetze aufzuteilen. Diese Subnetze haben nur Bedeutung in der internen Netzverwaltung, nach außen hin wird das gesamte Netz mit einer registrierten Adresse repräsentiert. Dadurch können u.a. Umstrukturierungen des Netzwerks leicht und ohne großen Einfluß auf benachbarte Netzwerke bzw. das Internet vorgenommen werden.

Subnetze und Router

Router werden verwendet, um verschiedene Netzwerke miteinander zu verbinden (Layer 3 Funktion). Über entsprechende Schnittstellen sind Router gleichzeitig mit mehreren (Sub-)Netzwerken verbunden, was wiederum bedeutet, dass jedes Subnetz über ein dediziertes Routerinterface angeschlossen sein muss.

Ein Subnetz widerspiegelt oft ein bestimmtes Ethernet-basiertes lokales Netz bzw. ein bestimmtes virtuelles LAN (VLAN). Hier werden Router benötigt, um diese auf Layer 2 getrennten Netze logisch miteinander zu verbinden.

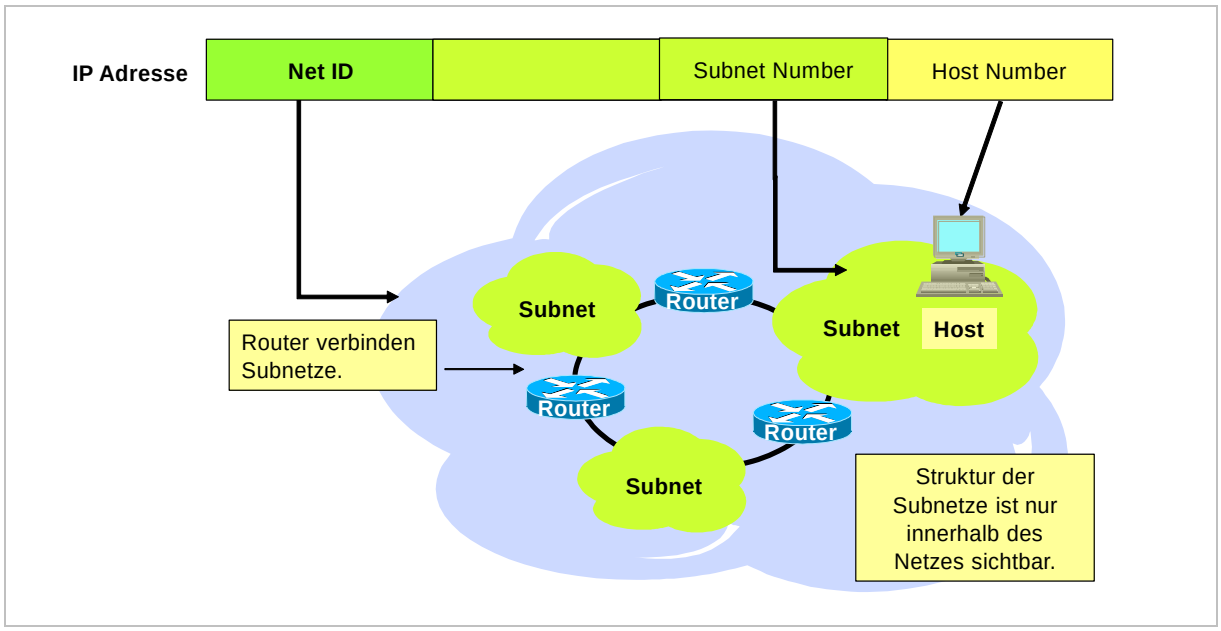


Abbildung 5 Net ID, Subnetze und Hosts

3.3 Adressierung IPv6

3.3.1 Wichtige Eigenschaften und Unterschiede zu IPv4

An dieser Stelle sind nur die wichtigsten Neuerungen in IPv6 gelistet.

- Erweiterung des Adressraums: $2^{32} \rightarrow 2^{128}$

  (Vgl.: 600 Billiarden Adressen auf jeden Quadratmillimeter der Erdoberfläche)
- Autokonfiguration: Zuweisung einer eindeutigen Adresse ohne DHCP ist möglich
- Keine Broadcastadressen
- Vereinfachtes Headerformat (40 Byte fix) zur schnelleren Verarbeitung im Router
- Erweiterungen und Optionen werden (nur bei Bedarf) in sog. Extension Headern transportiert. Neue Header für neue Features können somit leicht dazu definiert werden, ohne Änderungen in der Protokoll-Definition vornehmen zu müssen.

3.3.2 Format der IPv6 Adressen

Länge und Schreibweise:

- Eine IPv6 Adresse ist 128 Bit lang und wird in hexadezimaler Form dargestellt. Dabei werden jeweils 16Bit-Blöcke durch Doppelpunkte getrennt, z.B.:

  1080:AF4C:0000:0000:0000:0060:200C:417A

Vereinfachungen:

- Führende Nullen in einem Block können weggelassen werden. Aus der obigen Adresse wird somit:

  1080:AF4C: 0:0:0:60:200C:417A
- Adressblöcke, welche nur aus Nullen bestehen, können durch zwei Doppelpunkte dargestellt werden. Dies ist jedoch nur einmal pro Adresse erlaubt.

  1080:AF4C:0000:0000:0000:0060:200C:417A → 1080:AF4C::0060:200C:417A

  Nicht:

  1080:0000:AF4C:0000:0000:0060:200C:417A → 1080::AF4C::0060:200C:417A

  da eindeutige Rückgewinnung der ursprünglichen Adresse nicht möglich!!!

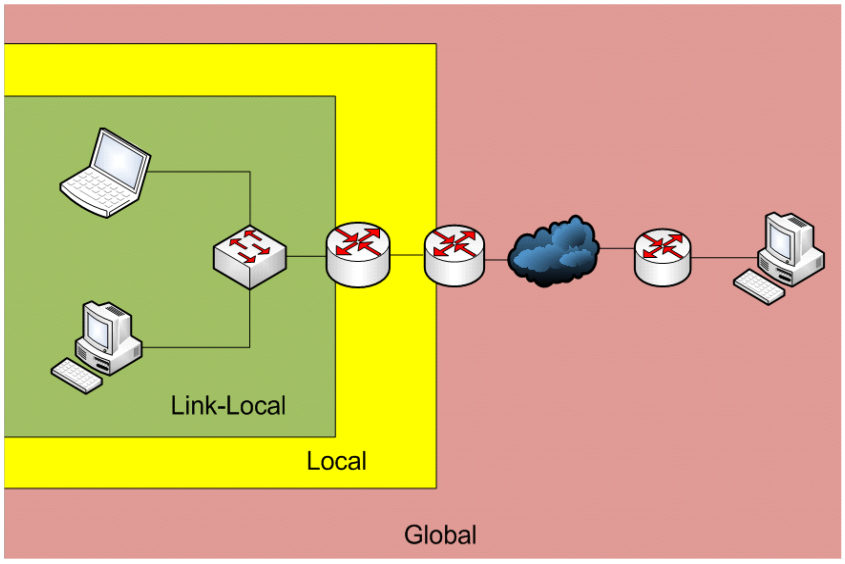
3.3.3 Adresstypen in IPv6

Folgende Adresstypen werden in IPv6 grundsätzlich unterschieden:

- Unicast Adresse: identifiziert ein Interface eines IPv6 Knotens eindeutig.
- Multicast Adresse: identifiziert eine Gruppe von IPv6 Interfaces. Ein Paket, das an eine Multicast Adresse gesendet wird, wird von allen Mitgliedern der Gruppe verarbeitet.
- Anycast Adresse: ist mehreren Interfaces zugewiesen (üblicherweise auf unterschiedlichen IPv6 Knoten). Ein an eine Anycast Adresse gesendetes Paket wird nur an eines dieser Interfaces (überlicherweise das naheliegendste) gesendet.

Gültigkeitsbereich einer IPv6-Adresse (Scope)

- Link local: nur auf lokalem Link gültig, wird nicht geroutet
- Unique local: werden nur im privaten Netz geroutet (ähnlich private IP-Adressen in IPv4)
- Global unicast: öffentliche IP Adresse



aus (07.09.22): https://sephi42.wordpress.com/2015/09/13/ipv6-adresstypen-und-der-gueltigkeitsbereich-von-ipv6-adressen/

Address type	Binary prefix	IPv6 notation
Multicast	11111111	FF00::/8
Global unicast	001	2000::/3
Link-local unicast	1111111010	FE80::/10

Abbildung 6 Adresstypen und Gültigkeitsbereiche in IPv6

3.3.4 Prefix-Notation und Adress-Struktur

Auch IPv6 Adressen bestehen grundsätzlich aus einem Netz- und eine Hostanteil (jetzt Interface ID), was für die Routingabläufe entscheidend ist. Die Interface ID definiert hierbei eindeutig ein Interface in einem bestimmten Subnetz und kann beispielsweise von der Hardware-Adresse abgeleitet werden. Abgesehen von wenigen Ausnahmen ist die Interface ID 64 Bit lang. Die Notation ist gleich der IPv4 Prefix-Notation:

IPv6-Adresse /Prefix-Länge (Anzahl der Bits im Prefix)

z.B. 2001:0DB8:0000:CD30:0000:0000:0000:0000/60 oder

2001:0DB8::CD30:0:0:0:0/60 oder

2001:0DB8:0:CD30::/60

<table>
<tr><td colspan="3">128 bits node address</td></tr>
<tr><td colspan="2">64 bits</td><td>64 bits</td></tr>
<tr><td colspan="2">subnet prefix</td><td rowspan="3">interface ID</td></tr>
<tr><td>n bits</td><td>64-n bits</td></tr>
<tr><td>global routing prefix</td><td>subnet ID</td></tr>
</table>

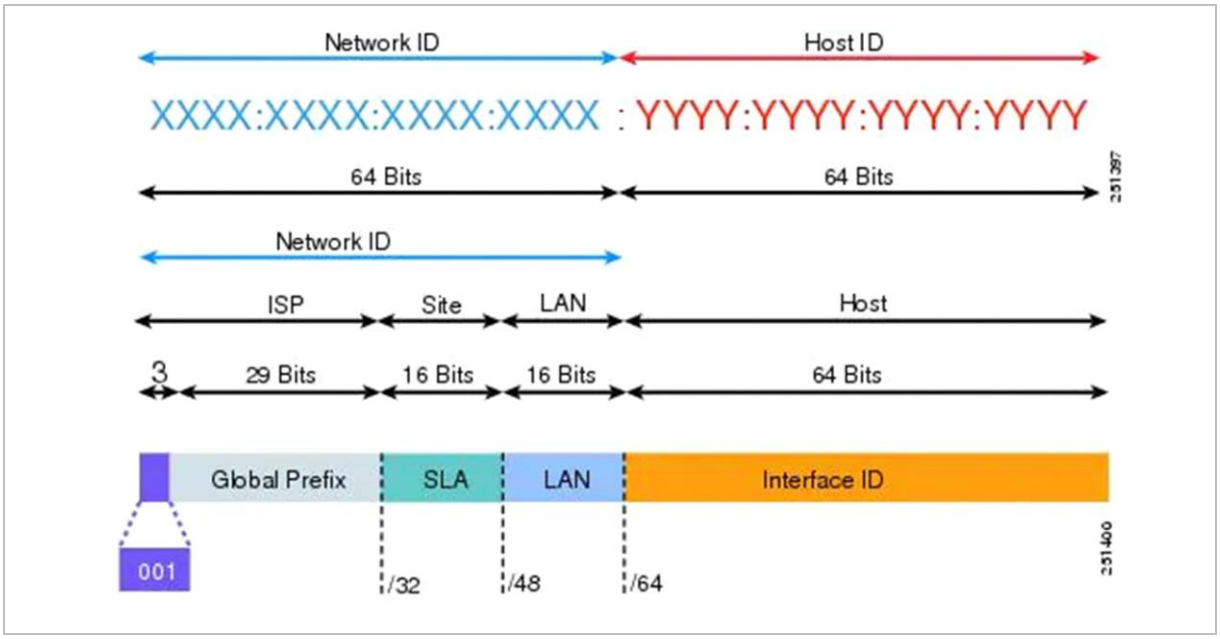


Abbildung 7 IPv6 Adressvergabe (https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/IPv6/vtgs_b_ipv6-deployment-guide-for-cisco/vtgs_b_ipv6-deployment-guide-for-cisco_chapter_01.html, 07.09.2022)

3.4 Koexistenz von IPv4 und IPv6

Auch wenn aktuell noch IPv4 Netzwerkstrukturen überwiegen, ist es nur eine Frage der Zeit, wann IPv6 hier dominieren wird. Treibende Faktoren sind u.a.:

- IPv4 Adressknappheit
- Vorherrschende IPv6-Implementierungen im asiatischen Raum
- Bessere Unterstützung bestimmter Features (QoS, Security…)

Im Zuge einer geplanten Umstellung auf IPv6 ist insbesondere eine passende Migrationsstrategien zu finden. Technisch sind grundsätzlich drei Varianten der Koexistenz von IPv4 und IPv6 zu unterscheiden, wobei erstere grundsätzlich zu favorisieren ist:

- Dual Stack
- Tunneling
- Translation

Dual Stack

Im Dual Stack Modus unterstützen die Komponenten sowohl IPv4 als auch IPv6. Beide Protokolle existieren zur gleichen Zeit im Netz und die Ende-zu-Ende-Kommunikation findet durchgängig über ein und dasselbe Protokoll statt (IPv6 <-> IPv6 ODER IPv4 <-> IPv4). Die beteiligten Komponten unterstützen optimalerweise beide Protokolle simultan bzw. sind anderenfalls nur in einem der beiden Netze integriert.

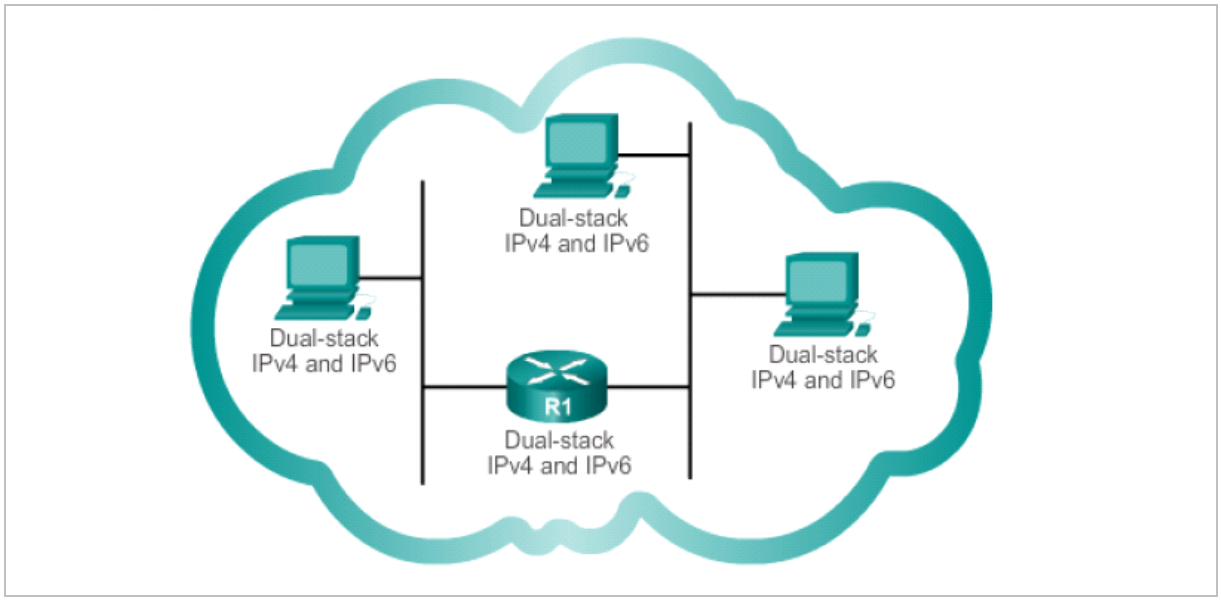


Abbildung 8 IPv4 und IPv6 Dual Stack

Tunneling

Für die Kommunikation zwischen Netzen eines Protokolls (in Abbildung 9 IPv6) über ein zwischengeschaltetes Netz, welches nur die andere IP-Version unterstützt (z.B. Backbone-Provider, hier IPv4) können Pakete getunnelt werden.

Dabei wird ein Protokoll in ein anderes "eingepackt" (IPv6 in IPv4 oder umgekehrt). Auf diese Weise können bestehende IPv4-Infrastrukturen über einen Backbone geführt werden, der bereits IPv6 unterstützt, oder umgekehrt.

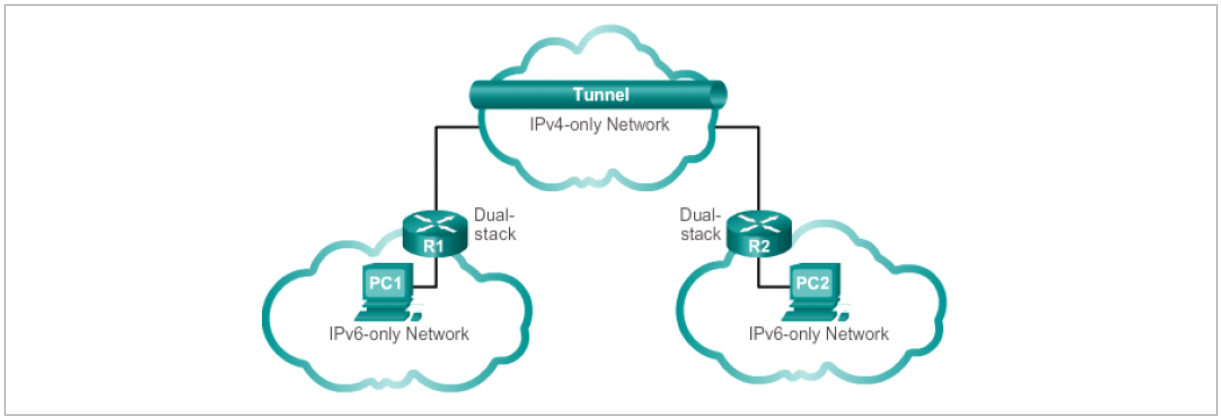


Abbildung 9 Getunnelter Transport von IPv6 Paketen über ein IPv4 Netzwerk

Translation

Bei der Translation-Technik wird das Protokoll IPv4 in IPv6 und umgekehrt übersetzt (Network Adress Translation: NAT). Ein so genannter 64Router nimmt die entsprechende Umsetzung vor. Ein IPv6 Engerät kann dadurch mit einem IPv4 Endgerät und umgekehrt kommunizieren.

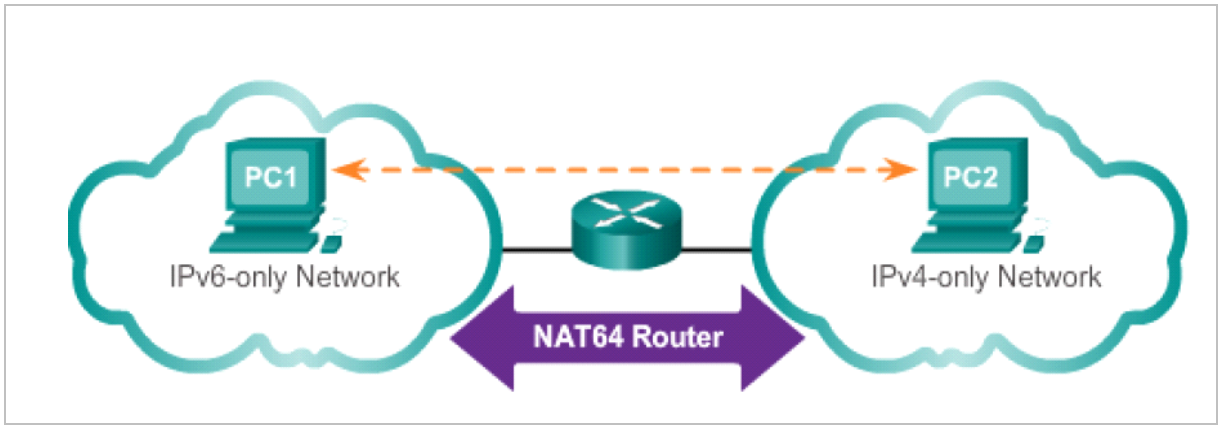


Abbildung 10 Network Address Translation 64 (NAT64)

3.5 Adressierungsdienste in IP-Netzwerken

3.5.1 IP Konfiguration: Übersicht

Für die Kommunikation in einem Netzwerk benötigt jedes Endgerät eine entsprechende IP-Konfiguration. Diese beinhaltet zumindest:

- IP-Adresse inkl. Subnetzinformation (Subnetmaske oder Prefix)
- Default (Standard)-Gateway für die Kommunikation in externe Netze
- DNS Server zur Namensauflösung von Domänennamen in IP-Adressen

Diese Konfigurationen können manuell oder über DHCP vorgenommen werden, bei IPv6 zusätzlich mit Hilfe der Stateless Address Autoconfiguration Funktion (SLAAC). In dem Fall ist weder ein externer Server, noch eine Eingabe erforderlich.

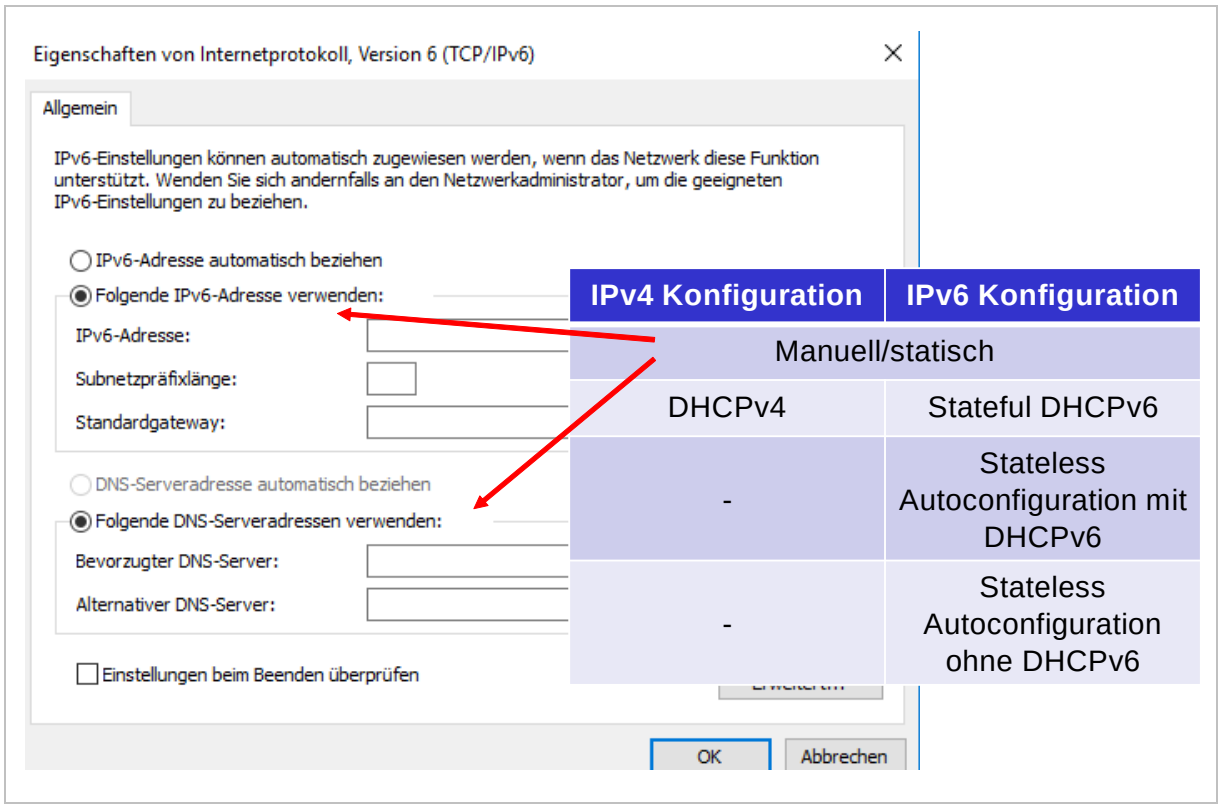


Abbildung 11 Übersicht IP-Konfiguration

3.5.2 Adresskonfiguration in IPv4 mittels DHCP

Grundsätzlich ermöglicht das Dynamic Host Configuration Protocol (DHCP) die Verwaltung und Verteilung der IP-Konfiguration an Hosts in einem TCP/IP-Netzwerk. Die ursprüngliche DHCP-Spezifikation lt. RFC 2131 unterstützt IPv4-Konfigurationen, für IPv6 benötigt man DHCPv6 (RFC 3315) um die gleichen Funktionalitäten zu realisieren (siehe 3.5.3).

DHCP arbeitet in einer Client-Server-Architektur in welcher der DHCP-Server (üblicherwesie ein Router mit dieser Zusatzfunktion) über einen Pool von IP-Adressen verfügt, die er den Clients zuteilen kann. Der DHCP-Client hat zunächst keine gültige IP-Konfiguration und kann lediglich IP-Broadcasts verschicken. Es folgt ein Ablauf mit vier Nachrichten:

- **DHCP-Discover:** UDP-Paket als IP-Broadcast (255.255.255.255) an alle verfügbaren DHCP-Server (optimalerweise gibt es nur einen).
- **DHCP-Offer:** Antwort des DHCP-Servers (IP-Adresse und weitere Parameter)
- **DHCP-Request:** positive Meldung an den gewählten DHCP-Server (bei mehreren „Angeboten“ als Broadcast, evtl. andere DHCP-Server sind so auch informiert)
- **DHCP-Acknowledgement:** Bestätigung durch den Server und evtl. Vergabe von weiteren Parametern

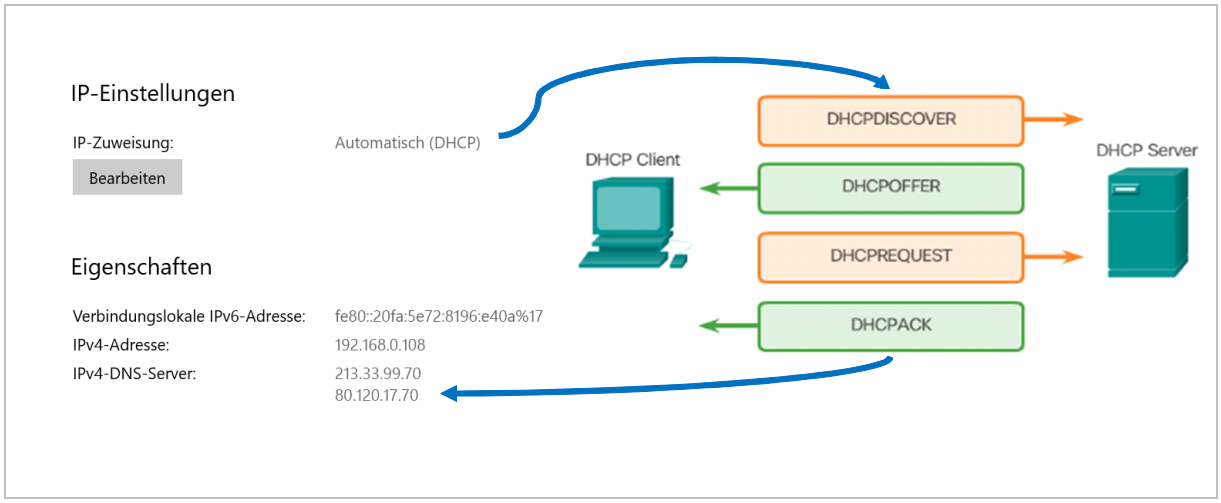


Abbildung 12 Ablauf einer DHCP-Kommunikation in IPv4

3.5.3 Adresskonfiguration in IPv6

Grundsätzlich “hört” ein IPv6-Host auf verschiedene IP-Adressen. Dies sind:

- link-lokale IPv6-Adresse (nur lokal gültig, siehe Abb. 13)
- globale IPv6-Adresse
- diverse Multicast-IPv6-Adressen
- optional weitere, meist temporäre IPv6-Adressen

Für eine vollständige IPv6-Konfiguration kommen außerdem hinzu:

- Standard-Gateway
- DNS-Server
- Optional weitere netzwerkrelevante Einstellungen

Neben der manuellen Eingabe gibt es in IPv6 verschiedene Optionen der IP-Konfiguration:

- Stateless Address Autoconfiguration (SLAAC) ohne DHCPv6
- Stateless Address Autoconfiguration (SLAAC) mit DHCPv6
- Stateful DHCPv6

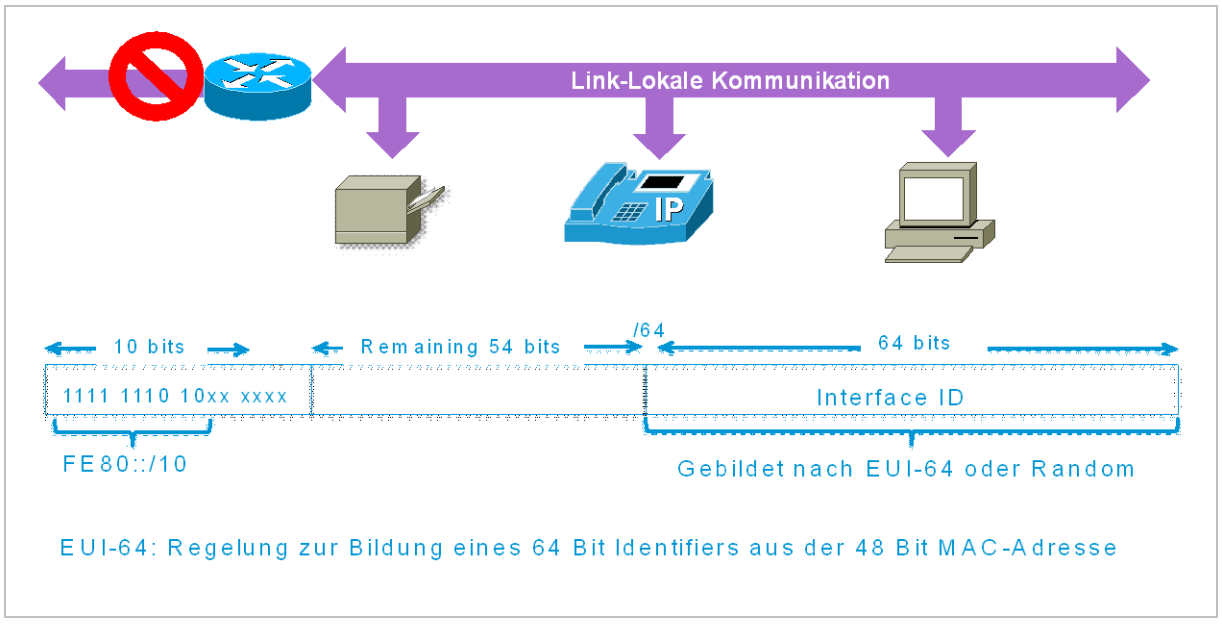


Abbildung 13 Link-lokale Kommunikation und Adressen

Stateless Address Autoconfiguration (SLAAC) mit/ohne DHCP

Im Rahmen der SLAAC wird auf einem IPv6 Interface zumindest eine link-lokale Adresse generiert. Sofern sich ein IPv6-fähiger Router im Netz befindet, wird außerdem eine globale Unicast-Adresse und auch das Default Gateway zugewiesen.

DHCPv6 dient in dieser Konstellation optional zur Ergänzung weiterer Konfigurationsdaten (z.B. DNS-Server), jedoch nicht zur Adresszuweisung.

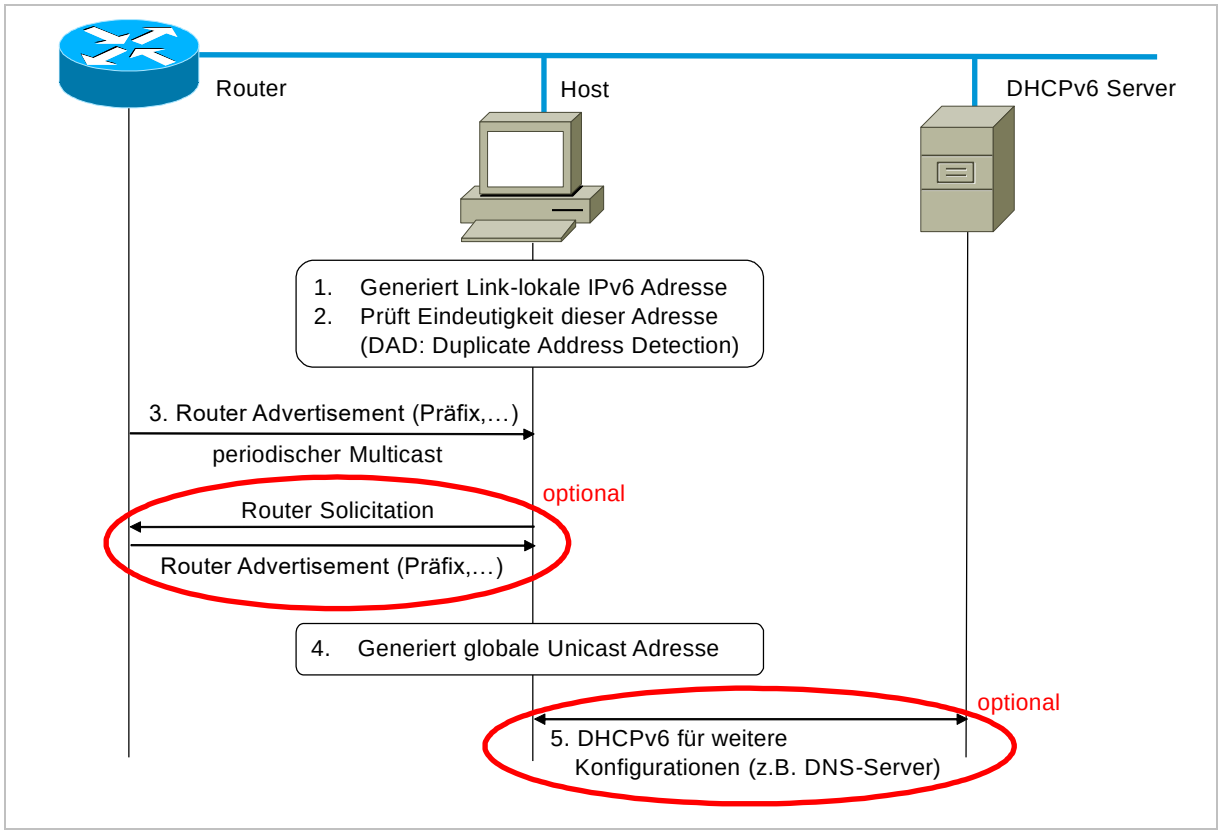


Abbildung 14 Stateless Address Autoconfiguration (SLAAC) mit/ohne DHCPv6

Stateful Adress-Konfiguration mit DHCPv6

Soll die gesamte IP-Konfiguration zentral vergeben und gespeichert werden, ist die "Stateful" Adress-Konfiguration zu bevorzugen. Die ersten Konfigurationsschritte sind hierbei gleich wie bei der SLAAC, nur so kann dem Interface eine link-lokale Adresse zugewiesen werden. Durch den im Router-Advertisement enthalten Flag “managed” wird der Host jedoch aufgefordert, seine globalen IP-Konfigurationsdaten von einem DHCPv6 Server zu beziehen (ähnlich DHCP in IPv4)

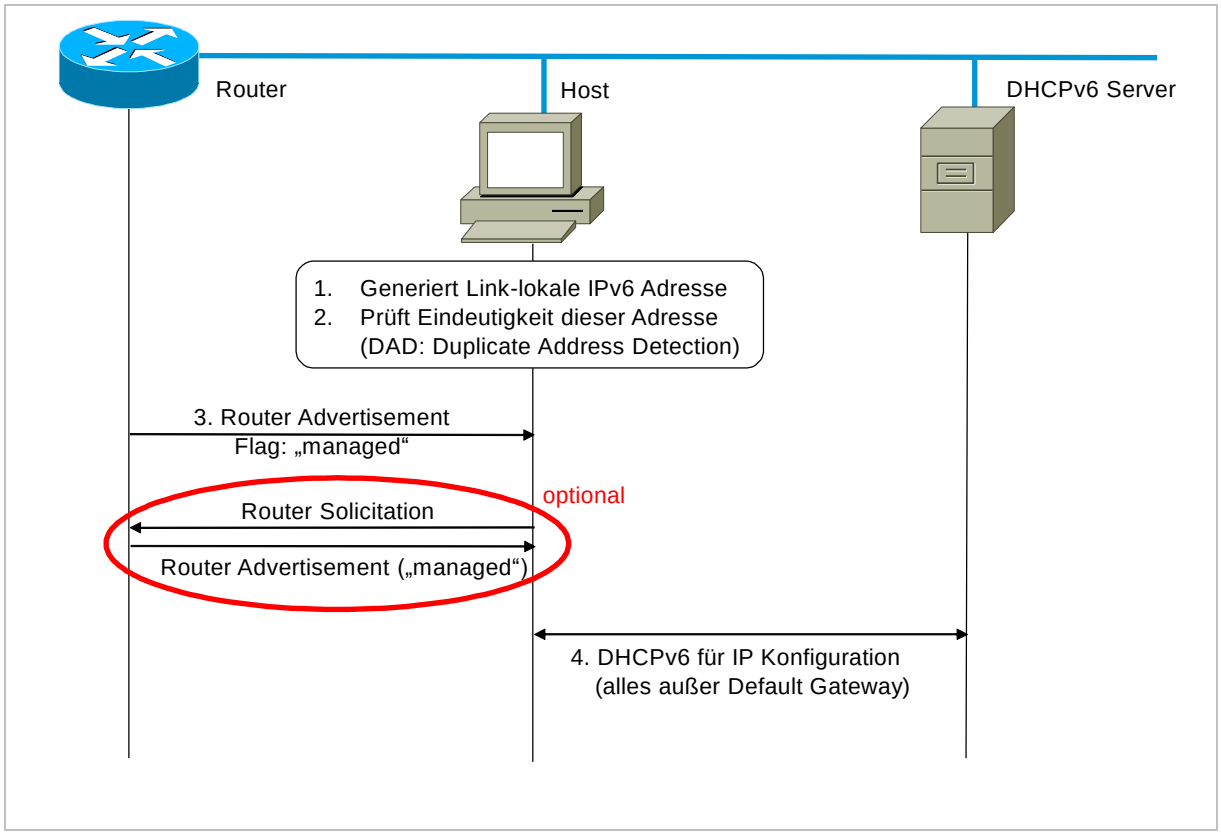


Abbildung 15 Stateful Adress-Konfiguration mit DHCPv6

3.5.4 Domain Name System (DNS)

Für die alltägliche Verwendung und Adressierung von Endgeräten und Diensten in einem Netzwerk bevorzugen Personen sogenannte Domain- oder Hostnamen (z.B. www.fh-salzburg.ac.at), die leichter zu merken sind, als IP-Adressen. Die in dann für eine Netzwerkkommunikation noch erforderliche Auflösung des Namens in eine IP-Adresse übernimmt das sogenannte Domain Name System (DNS). Dieses System besteht streng genommen aus:

- einer verteilten Datenbank (hierarchisch strukturierte DNS-Server) und
- einem Protokoll zur Abfrage der Datenbank

DNS Hierarchie

Ein Domainname wird grundsätzlich von rechts nach links aufgelöst, für die einzelnen Namensbereiche sind unterschiedliche Server verantwortlich.

Abbildung 16 zeigt den Ablauf einer möglichen DNS-Anfrage. Es ist erkennbar, dass der verantwortliche (bevorzugte) DNS-Server, welcher im Schritt 1 angefragt wird, auf iterative Weise den Domainnamen auflöst (Schritt 2-9).

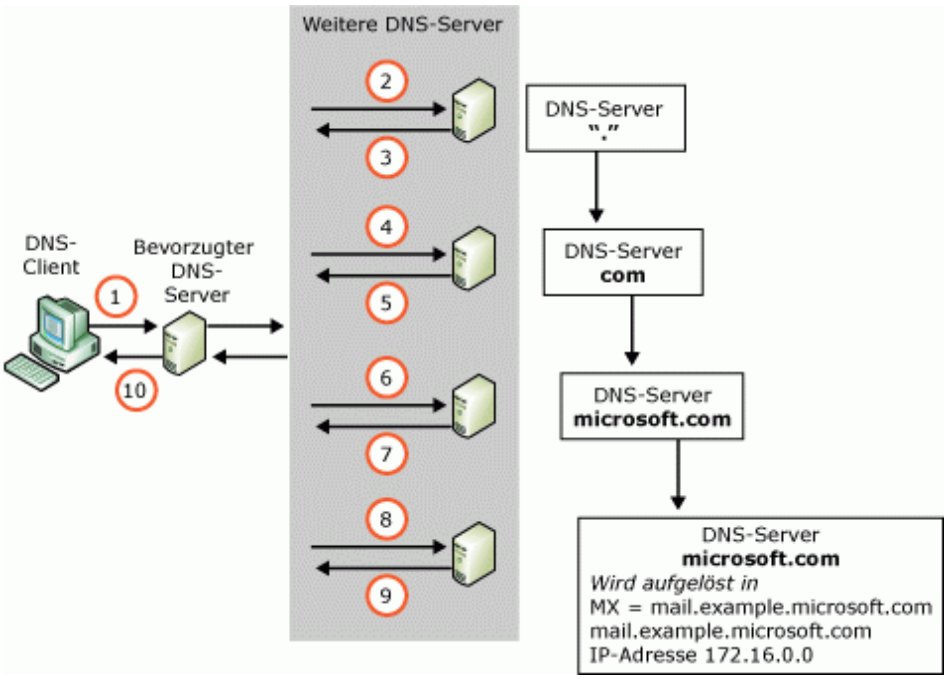


Abbildung 16 DNS Hierarchie (aus https://technet.microsoft.com/de-de/library/aa996356(v=exchg.65).aspx, 27.10.2017)

4 Grundlagen von VoIP

4.1 Die Idee

Um Sprachdienste zu realisieren wurde in den Anfängen der Telefonnetze bis teilweise in die heutige Zeit ein *leitungsvermittelter Datendienst* genutzt. *Leitungsvermittelt* bedeutet, dass anders als beim paketvermittelten Dienst über das IP-Protokoll hierbei für die gesamte Dauer einer Verbindung fixe Übertragungsressourcen ausschließlich für die jeweiligen Kommunikationspartner reserviert werden (aktuell weitestgehend über ISDN: Integrated Services Digital Network).

Erfolgt die Übertragung der Sprachdaten hingegen im IP-Netz (VoIP: Voice over IP), ist eine fixe Reservierung/Durchschaltung der Verbindung nicht notwendig.

Leitungsvermittlung (Circuit Switching)

Im Fall der Leitungsvermittlung stellt das Netz vor Beginn des eigentlichen Datenaustauschs eine physikalische Verbindung zwischen den einzelnen Teilnehmern her. Dieser Übertragungsweg mit einer fest eingerichteten Bandbreite existiert für die gesamte Dauer einer Verbindung, unabhängig davon, ob tatsächlich Daten gesendet werden oder nicht. Der Prozess des **Verbindungsaufbaus und –abbaus** nimmt einige Zeit in Anspruch, so dass Leitungsvermittlung hinsichtlich des Zeitfaktors nur sinnvoll ist, wenn die Verbindung für einen längeren Zeitraum aufrechterhalten wird. Vorteilhaft ist, dass die eigentlichen Daten nicht mehr adressiert werden müssen und der Overhead somit geringer ist.

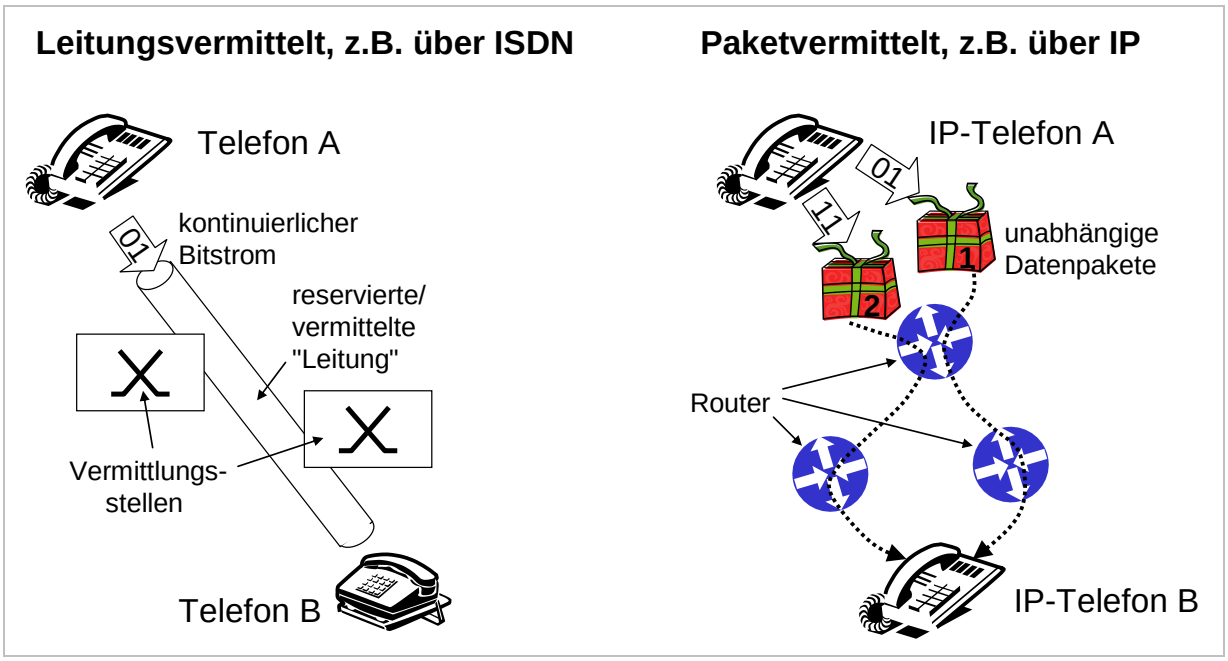


Abbildung 1 Leitungsvermittlung vs. Paketvermittlung

Paketvermittlung (Packet Switching)

Bei der Paketvermittlung wird zu Beginn des Datenaustauschs keine Verbindung aufgebaut, sondern jede Nachricht in Pakete zerlegt, welche, mit Hilfe eines **Nachrichtenkopfs (Header)** mit Zielinformationen, abschnittsweise durch das Netz geroutet werden (Postprinzip). In jedem Netzknoten wird dabei die Nachricht gespeichert und an die Zieladresse weitergeleitet. Der Vorteil gegenüber der Leitungsvermittlung besteht darin, dass die Bandbreitenzuordnung dynamisch nach Bedarf erfolgt und keine Zeit für Verbindungsauf- und abbauprozeduren verloren geht.

Signalisierung

Unter dem Begriff der Signalisierung wird im Sinne der Telefonie der Austausch aller vermittlungstechnischen Informationen verstanden, die der Steuerung der Nutzsignalübertragung dienen. Diese Form des Informationsaustauschs vor der eigentlichen Übertragung der Multimediadaten ist sowohl für paket- als auch leitungsvermittelte Echtzeitkommunikation (Sprache, Video) erforderlich und wird durch speziell dafür definierte Protokolle und Standards realisiert. Im Falle der Leitungsvermittlung schließt Signalisierung zusätzlich die Steuerung des Verbindungsauf- und abbaus mit ein (z.B. Belegung eines Nutzkanals).

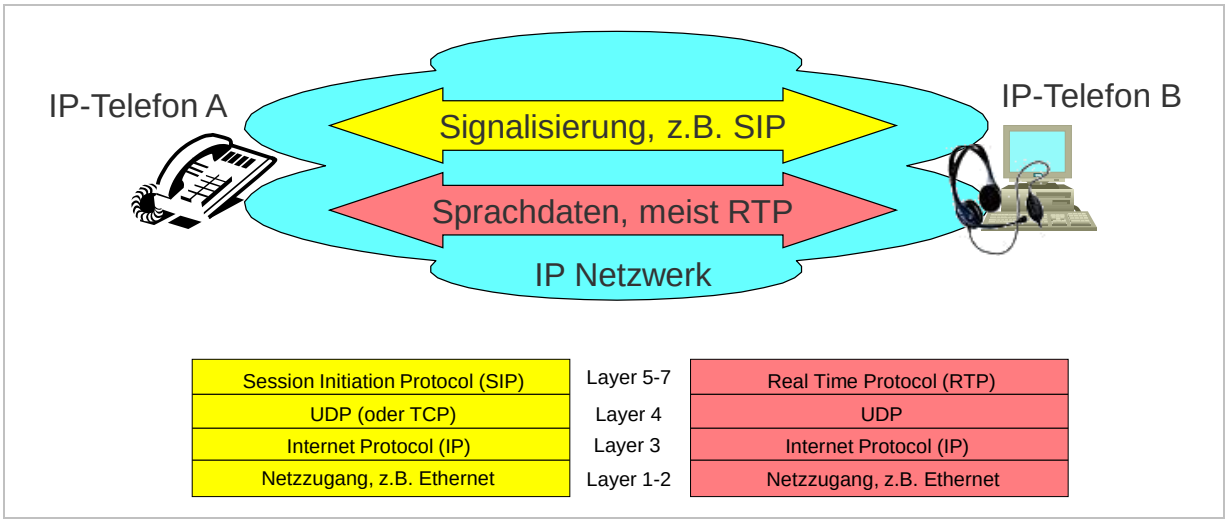


Abbildung 2: Überblick VoIP Ablauf und Protokolle

4.2 Das VoIP Signalisierungsprotokoll SIP

Für Aufbau und Steuerung einer Kommunikationsverbindung basierend auf dem Internetprotokoll ist momentan das Session Initiation Protocol (SIP) der meist verwendete Standard:

Die beliebte Alltagslösung für Internettelefonie *Skype* arbeitet nicht mit standardisierten, sondern mit proprietären, nicht offen gelegten Protokollen

4.2.1 Grundfunktionen von SIP

Das Session Initiation Protocol (SIP, RFC 3261) ist ein Protokoll, das für die Signalisierung von Multimedia Verbindungen in IP-Netzen eingesetzt wird. Dazu gehört neben dem Aufbau der Verbindung auch deren Verwaltung und Abbau.

SIP unterstützt die folgenden fünf Anforderungen:

- Lokation eines Nutzers (User Location)
- Austausch der Leistungsmerkmale der Terminals (Capability Exchange)
- Reaktion auf Nutzer, die nicht verfügbar sind (User Availability)
- Aufbau einer Verbindung (Call Setup)
- Verwaltung einer Verbindung (Call Handling) inklusive Anrufweiterleitung

Dabei beschreibt SIP ausschließlich die Verbindungssteuerung, der eigentliche Medientransport geschieht außerhalb des Definitionsbereichs von SIP.

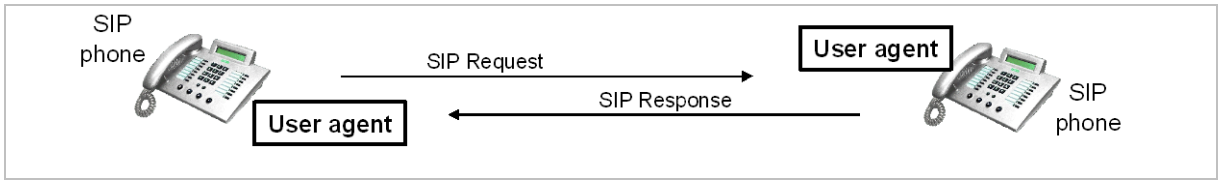


Abbildung 3 End-to-end SIP-Signalisierung ohne Proxy

4.2.2 Das SIP Nachrichtenformat

Untenstehende Abbildung 4 zeigt den Aufbau einer typischen SIP Nachricht. Die SIP Spezifikation beschreibt im Rahmen einer solchen Nachricht nur das Aushandeln der generellen Kommunikationsmodalitäten.

Weitere, für die Kommunikation wichtige Daten wie Kompressionsalgorithmus etc. werden über andere „mit-transportierte“ Protokolle ausgetauscht werden.

SIP verwendet hier meist das Session Description Protocol (SDP, RFC 4566) um die Details der Video- und/oder Audio-Übertragung auszuhandeln. Dabei teilen sich die Geräte gegenseitig mit, welche Methoden der Video- und Audio-Übertragung sie beherrschen (die sogenannten Codecs), mit welchem Protokoll sie das tun möchten und an welcher Netzadresse sie senden und empfangen wollen.

Diese Medien-Aushandlung ist also kein direkter Bestandteil von SIP, sondern wird durch die Einbettung eines weiteren Protokolls in SIP erreicht. Diese Trennung von Sitzungs- und Medienaushandlung ist einer der Vorteile von SIP, da sie eine große Flexibilität bei der unterstützten Nutzlast erlaubt: Möchte zum Beispiel ein Hersteller SIP für eine spezialisierte Anwendung verwenden, so kann er dafür eine eigene Medienaushandlung entwerfen, falls dafür noch kein Protokoll existiert.

Bei der Internet-Telefonie findet für die Medienübertragung das Realtime Transport Protocol (RTP, deutsch Echtzeit-Transportprotokoll, RFC 3550) Verwendung. SIP handelt hier die Sitzung aus, das eingebettete SDP handelt die Medien-Details aus, und RTP ist dann dasjenige Protokoll, welches letztendlich die Video- und Audio-Ströme überträgt.

Text teils übernommen aus http://de.wikipedia.org/wiki/Session_Initiation_Protocol (30.08.2012)

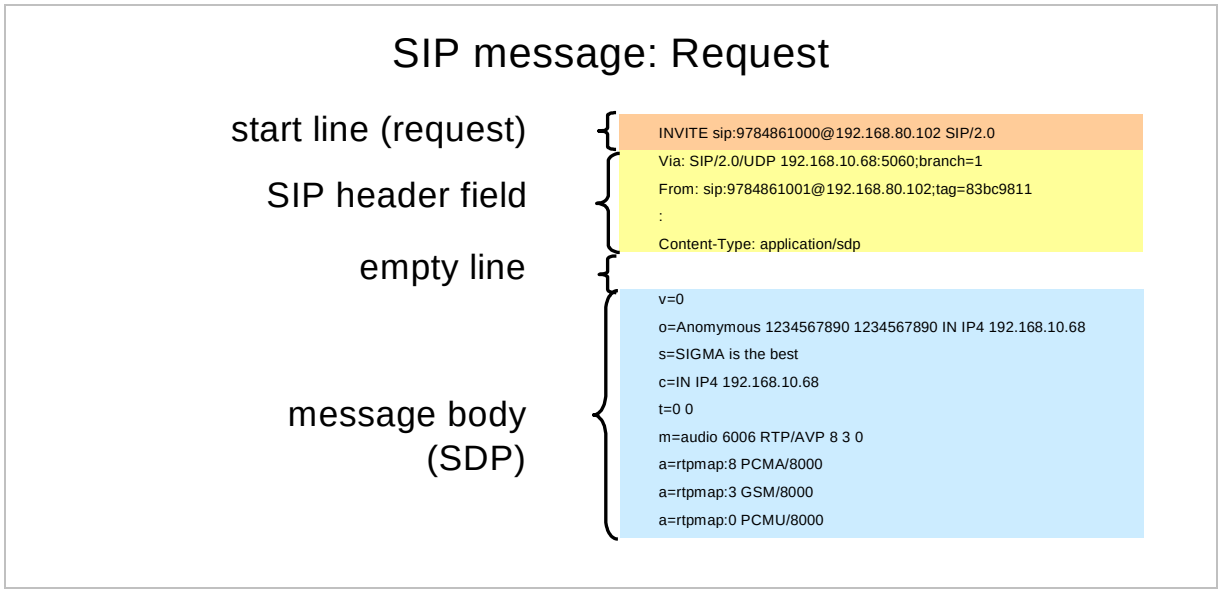


Abbildung 4: SIP Nachrichtenformat

4.2.3 SIP Architektur

Die funktionalen Hauptkomponenten einer SIP-Umgebung sind:

- SIP User Agent: Endgerät
- SIP Proxy Server: „Vermittlung mit Weiterleitung“
- SIP Redirect Server: „Vermittlung ohne Weiterleitung“
- SIP Registrar: Registrierung von SIP-Usern
- SIP Gateway: Übergang in andere Netze (z.B. ISDN)

Die (SIP-)Kommunikation zwischen SIP User Agents wird typischerweise über Proxyserver geroutet (siehe Abbildung 5). Deren Hauptaufgabe ist es, SIP-Endpunkte bzgl. aufwendiger Adressierungsverwaltungs- und Routingfunktionen zu entlasten.
Ein Proxy Server bearbeitet demzufolge eine SIP Nachricht und schreibt ihren Header neu. Er tritt somit als eigenständiger Sender auf und ist auch Empfänger entsprechender Antworten.

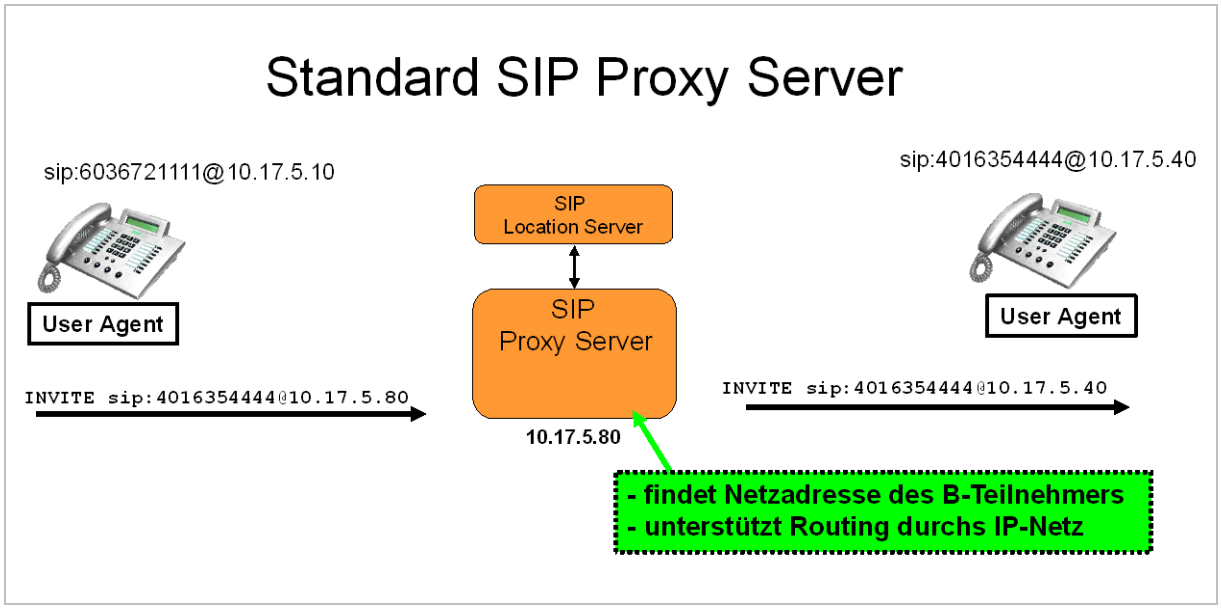


Abbildung 5 SIP proxy server

Für mehr Details siehe z.B. https://www.tech-invite.com/fo-sip/tinv-fo-sip-ex3261.html (09.09.2021)

4.3 Das Real Time Protocol RTP

4.3.1 Einleitung

Nachdem durch ein Signalisierungsprotokoll wie SIP alle Absprachen bzgl. der Kommunikation (z.B. Sprachkodierung) getroffen wurden, beginnt der eigentliche Datentransfer in einer so genannten RTP-Session, welche auch als logischer Übermittlungskanal (media channel) für VoIP angesehen werden kann.

RTP ist das zentrale Protokoll, um Echtzeitverkehr über ein Netzwerk ohne Qualitätsgarantien zu senden. Die primäre Idee bei diesem Protokoll ist, dass der Mensch bzgl. Sprache oder Bildern zwar fehlende Daten, sofern deren Anzahl nicht zu groß ist, akzeptieren kann, jedoch andere Faktoren wie Verzögerungen oder Jitter (unterschiedliche Verzögerungen der einzelnen Datenpakete) sich äußerst ungünstig auf die Qualität der Echtzeitanwendungen auswirken.

Aufgrund dieser Tatsache ist es nicht nötig, Pakete, die zu spät kommen, noch an die Applikation auszuliefern, bzw. solche, die verloren gegangen sind, erneut anzufordern, da sie doch „viel zu spät“ kämen. Quittungen sind daher nicht notwendig, vielmehr bedarf es in erster Linie einer Kontrolle und Überwachung der Echtzeitkommunikation bzgl. der zeitlichen Verzögerung und Reihenfolge der Datenpakete, was mit RTP realisiert wird. Die wichtigsten RTP-Headerinformationen sind in dem Zusammenhang:

- Time Stamp
- Sequence Number

Ergänzt wird RTP durch das RTP Control Protocol RTCP, welches mit Hilfe von periodisch ausgesendeten Kontroll- und Statusinformationen (Reports) die Qualität einer RTP-Session überwacht. Sowohl RTP als auch RTCP sind im RFC 3550 spezifiziert und setzen auf UDP auf.

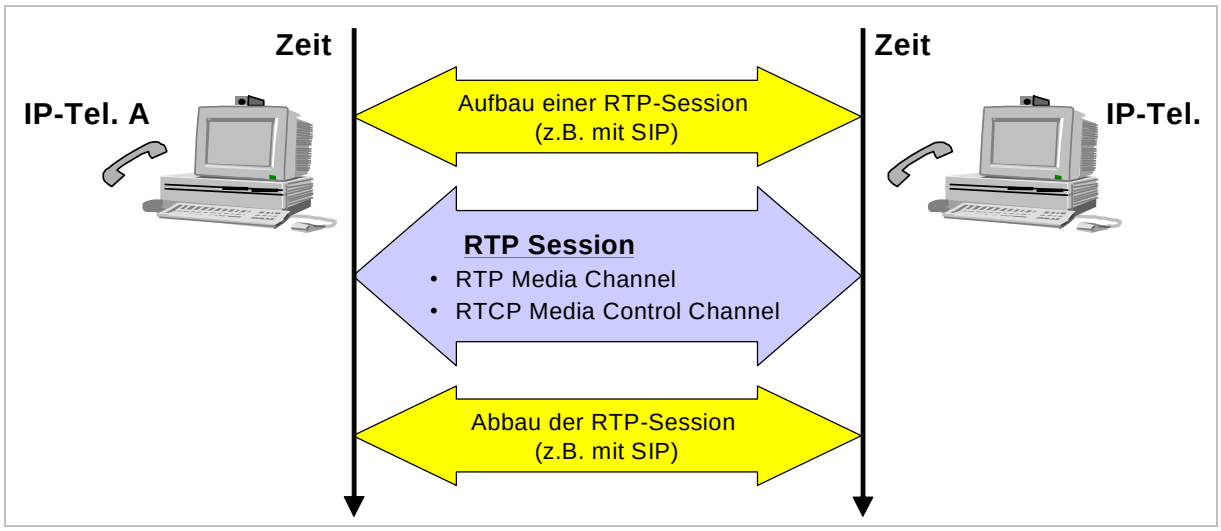


Abbildung 6 Prinzip einer RTP Session

4.3.2 Encapsulation von RTP in IP-Pakete

Nimmt man die Header von IP, UDP und RTP zusammen, ergibt sich eine Größe von mindestens 40 Byte (ausgehend von den Standard Größen für IP und RTP Header).

Die RTP Payload ist in der Regel relativ klein und liegt typischerweise zwischen 20 und 150 Byte, wodurch der relative Datendurchsatz relativ gering ist. Die Versendung größerer Datenpakete macht bei Echtzeitanwendungen jedoch keinen Sinn, da hierdurch das länger dauernde "Packen" eines Pakets zu nicht akzeptablen Verzögerungen führen würde.

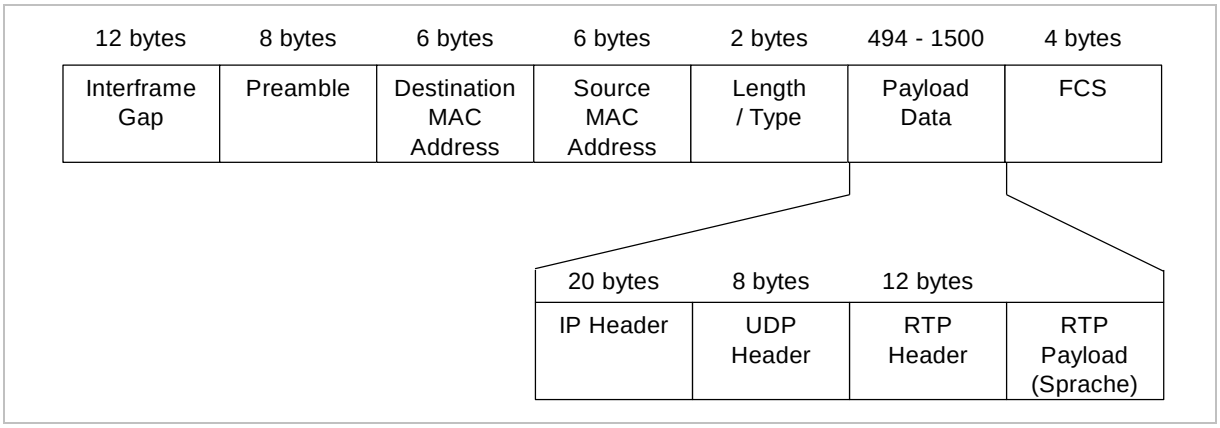


Abbildung 7 RTP Paket mit Ethernet Overhead

Beispiel: Erforderliche Bandbreite für 64 kbit/s Link

Codec	Native bitrate	Framing	RTP payload	Ethernet bitrate
G.723 low rate	5,3 kbit/s	30 ms	20 bytes	26 kbit/s
G.723 high rate	6,3 kbit/s	30 ms	24 bytes	27 kbit/s
G.729A	8 kbit/s	20 ms	20 bytes	39 kbit/s
G.711	64 kbit/s	10 ms	80 bytes	126 kbit/s

Abbildung 8 Bitrate bei verschiedenen Kodierungsverfahren

4.3.3 Digitalisierung der Sprachdaten

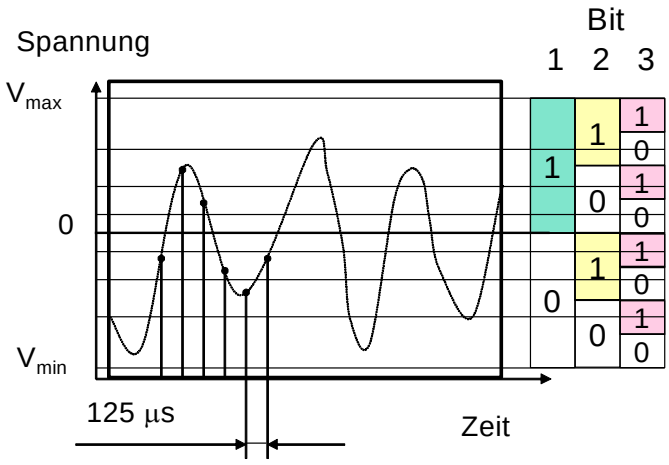
Die zunächst analogen Sprach- und Datensignale müssen für den Transport in IP-Netzen in binärer (digitaler Form) vorliegen. Die entsprechende Digitalisierung des Sprachsignals erfolgt mit Hilfe der Puls Code Modulation, kurz PCM. Dabei wird das analoge Signal abgetastet und der ermittelte Amplitudenwert in binärer Form codiert.

Um den ursprünglichen Informationsgehalt des analogen Signals (Bandbreite bis 3400 Hz) vollständig auf der Empfängerseite zurück gewinnen zu können, wählt man eine Abtastfrequenz von 8000 Hz, was einem diskreten Signalwert alle 125 µs entspricht.

Der Amplitudenwert, der nun alle 125µs ermittelt wird, muss binär dargestellt werden. Dazu teilt man den Bereich aller möglichen Amplitudenwerte in 256 Intervalle ein, die jeweils mit einem 8-Bit-Wert eindeutig dargestellt werden können. Die resultierende Übertragungsrate für ein Gespräch ist somit 64 kbit/s.

Da das menschliche Ohr Lautstärke-Unterschiede bei leisen Tönen besser auflösen kann als bei lauten, werden für Telekommunikationsanwendungen die Quantisierungsschritte nicht äquidistant verteilt, sondern sind bei kleinen Amplituden wesentlich feiner gewählt.

Die in VoIP-Netzen gängigen Kompressionsverfahren (Codec) erreichen durch die Verwendung komplexer mathematischer Verfahren deutlich geringe Bitraten bei der effizienten Digitalisierung eines Sprachsignals (siehe z.B. Abbildung 8).



Pulse Code Modulation

- Abtastung alle 125 µs
- Spannungsbereich in N Stufen unterteilt
- Stufen werden binärcodiert dargestellt (hier 3 Bit)
- Telekommunikation: 8 Bit Auflösung entspricht 256 Stufen
- Nichtlineare Stufung zur feineren Auflösung leiser Töne

Abbildung 9 Pulse Code Modulation