Vermittlungsschicht

NETZWERKTECHNIK / SEMESTER 1 UND 2

1

AGENDA

01 VERMNITTLUNGSARTEN

02 VERMITTLUNGSSCHICHT

03 ADRESSAUFLÖSUNG

04 IPV4 BEISPIELNETZWERK

05 ICMP

06 DHCP

2

01

Vermittlungsarten

3

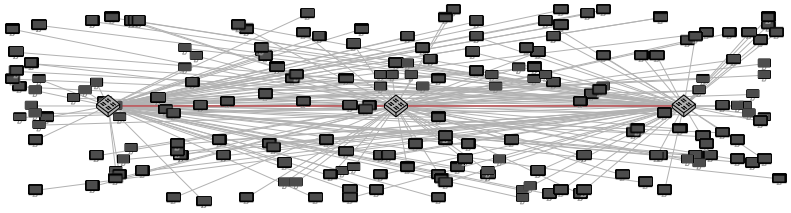
Eigenschaften von IP

Sind Direktverbindungsnetzewie Ethernet skalierbar?

- Alle angeschlossenen Hosts sind direkt bzw. über wenige Switches erreichbar
- MAC-Adressen bieten keine logische Struktur zur Adressierung
- Gruppierung von Geräten in kleinere Netze (Subnetze) durch MAC-Adressen nicht unterstützt

Aufgaben der Vermittlungsschicht:

- Kopplung unterschiedlicher Direktverbindungsnetze
- Strukturierte Aufteilung in kleinere Subnetze
- Logische und global eindeutige Adressierung von Geräten
- Wegwahl zwischen Geräten über mehrere Hops hinweg



[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), Prof. Dr.-Ing. Georg Carle, TUM, 2025]

4

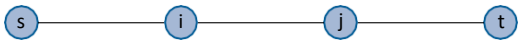
NETZWERKTECHNIK / SEMESTER 1 und 2

Vermittlungsarten

Es gibt **drei grundlegende Vermittlungsarten**:

- **Leitungsvermittlung** - „Reserviere eine dedizierte Leitung zwischen Sender und Empfänger“
- **Nachrichtenvermittlung** - „Wähle für jede Nachricht individuell einen Weg und leite die Nachricht als Ganzes weiter“
- **Paketvermittlung** - „Teile eine Nachricht in mehrere kleinere Pakete auf und versende jedes Paket unabhängig von den anderen“

Im Folgenden charakterisieren wir diese drei Vermittlungsarten anhand des Beispielnetzwerks



mit $n = 2$ Vermittlungsknoten (i und j) hinsichtlich der Gesamtdauer T einer Übertragung von L Datenbits über die Distanz d und motivieren so die Vorteile der Paketvermittlung.

tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), Prof. Dr.-Ing. Georg Carle, TUM, 2025]

5

NETZWERKTECHNIK / SEMESTER 1 und 2

Leitungsvermittlung

Während einer verbindungsorientierten Übertragung können drei Phasen unterschieden werden:

- **Verbindungsaufbau**
  - Austausch von Signalisierungsnachrichten zum Aufbau einer dedizierten Verbindung zwischen Sender und Empfänger.
  - Dieser Schritt beinhaltet die Wegwahl, welche vor Beginn der Datenübertragung durchgeführt wird.
- **Datenaustausch**
  - Kanal steht den Kommunikationspartnern zur exklusiven Nutzung bereit.
  - Auf die Adressierung des Kommunikationspartners kann während der Übertragung weitgehend verzichtet werden (Punkt-zu-Punkt-Verbindung).
- **Verbindungsabbau**
  - Austausch von Signalisierungsnachrichten zum Abbau der Verbindung.
  - Die durch die Verbindung belegten Ressourcen werden für nachfolgende Verbindungen freigegeben.

tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), Prof. Dr.-Ing. Georg Carle, TUM, 2025]

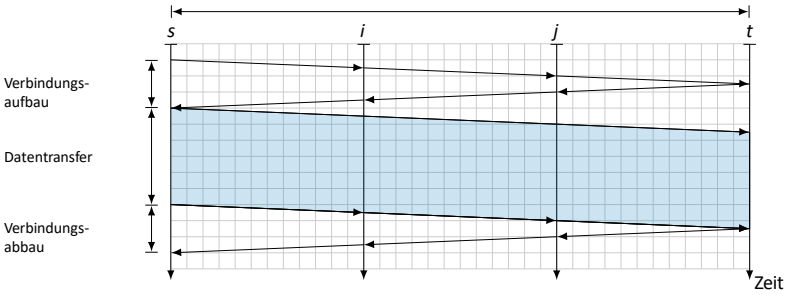
6

NETZWERKTECHNIK / SEMESTER 1 und 2

Übertragungszeit bei der Leitungsvermittlung

Wir nehmen an, dass

- die Serialisierungszeit von Signalisierungsnachrichten vernachlässigbar klein ist,
- die Verarbeitungszeiten und Wartezeiten in jedem Knoten vernachlässigbar klein sind und dass
- der Sender S einen Datenblock der Länge L an einem Stück übertragen möchte.



$$T_{LV} = 2 \cdot t_p + t_s + 2 \cdot t_p$$
$$= t_s + 4 \cdot t_p$$
$$= \frac{L}{r} + \frac{4 \cdot d}{v \cdot c_0} 4$$

[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), Prof. Dr.-Ing. Georg Carle, TUM, 2025]

NETZWERKTECHNIK / SEMESTER 1 und 2

Einsatz von Leitungsvermittlung

Vorteile der Leitungsvermittlung

- Gleichbleibende Güte der dedizierten Verbindung nach dem Verbindungsaufbau
- Schnelle Datenübertragung ohne Notwendigkeit, weitere Vermittlungsentscheidungen treffen zu müssen

Nachteile der Leitungsvermittlung

- Ressourcenverschwendung sofern Leitung nicht dauerhaft ausgelastet wird, da Leitung zur exklusiven Nutzung reserviert wird
- Verbindungsaufbau kann komplex sein und benötigt u. U. weit mehr Zeit, als die Ausbreitungsverzögerungen vermuten lassen (z. B. Einwahl ins Internet mittels Modems)
- Hoher Aufwand beim Schalten physikalischer Verbindungen

Einsatz in heutigen Netzwerken

- Leitungsvermittlung wird häufig durch Paketvermittlung ersetzt (z. B. Voice over IP)
- In vielen Vermittlungsnetzen wird Leitungsvermittlung zumindest virtualisiert in Form von Virtual Circuits unterstützt (z. B. Frame Relay, ATM1 , MPLS2)

[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), Prof. Dr.-Ing. Georg Carle, TUM, 2025]

Nachrichtenvermittlung

Modifikationen gegenüber Leitungsvermittlung:

- Aufbau und Abbau einer dedizierten Verbindung entfallen
- Der gesamten Nachricht der Länge L wird ein Header der Länge L_H vorangestellt
- Der Header beinhaltet insbesondere Adressinformationen, die geeignet sind, Sender und Empfänger auch über mehrere Zwischenstationen hinweg eindeutig zu identifizieren
- Die so entstehende PDU wird als Ganzes übertragen

Eigenschaften:

- Möglichkeit für asynchrone Kommunikation, d. h. Nachrichten können ggf. an Empfänger versendet werden, die zum Zeitpunkt des Sendens nicht empfangsbereit sind
- Mögliche Zeitersparnis, da die Phasen zum Aufbau und Abbau der Verbindung entfallen

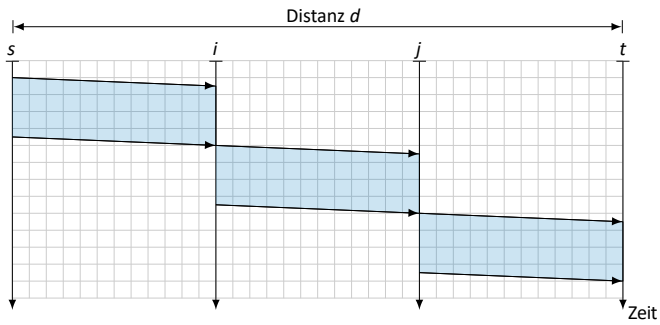
Analogie: Post / DHL / Paketdienste

- Absender verpackt Ware und versieht das Paket mit Adressinformationen (Header)
- Die Adressen identifizieren Absender und Empfänger weltweit eindeutig und haben eine logische Struktur, die eine effiziente Zuordnung im Transportnetz der Post erlaubt

tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), Prof. Dr.-Ing. Georg Carle, TUM, 2025]

Übertragungszeit bei der Nachrichtenvermittlung

Hier $n = 2$ Vermittlungsknoten i und j.

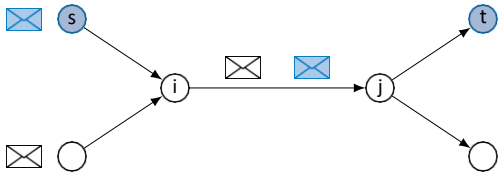


$$T_{NV} = (n+1) \cdot t_s + t_p$$
$$= (n+1)\frac{L_H + L}{r} + \frac{d}{v \cdot c_0}$$

tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), Prof. Dr.-Ing. Georg Carle, TUM, 2025]

Multiplexing auf Nachrichtenebene

- Das Wegfallen fest vorgegebener Pfade ermöglicht die gemeinsame Nutzung von Teilstrecken
- Dies entspricht dynamischem Zeitmultiplex (Time Division Multiplex, TDM)



Vorteile:

- Flexibles Zeitmultiplex von Nachrichten
- Bessere Ausnutzung der Kanalkapazität
- Keine Verzögerung beim Senden der Nachricht durch Verbindungsaufbau

Nachteile:

- Pufferung von Nachrichten, wenn (i, j) ausgelastet
- Verlust von Nachrichten durch begrenzten Puffer möglich
- Mehrfache Serialisierung der ganzen Nachricht

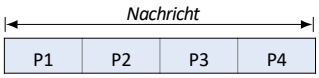
tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), Prof. Dr.-Ing. Georg Carle, TUM, 2025]

11

Paketvermittlung

Unterschiede zur Nachrichtenvermittlung:

- Nachrichten werden nicht mehr als Einheit übertragen sondern in kleinere Einheiten, den Datenteilen von Paketen, unterteilt:



- Jedes Paket wird mit einem eigenen Header versehen, der alle Informationen zur Weiterleitung und ggf. auch zur Reassemblierung enthält:

- Pakete werden unabhängig voneinander vermittelt, d. h. Pakete derselben Nachricht können über unterschiedliche Wege zum Empfänger gelangen.
- Im Allgemeinen müssen die einzelnen Pakete nicht gleich groß sein, es gibt aber Anforderungen an die maximale Paketgröße einhergehend mit Datenteilen maximaler Länge p_{max}.

tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), Prof. Dr.-Ing. Georg Carle, TUM, 2025]

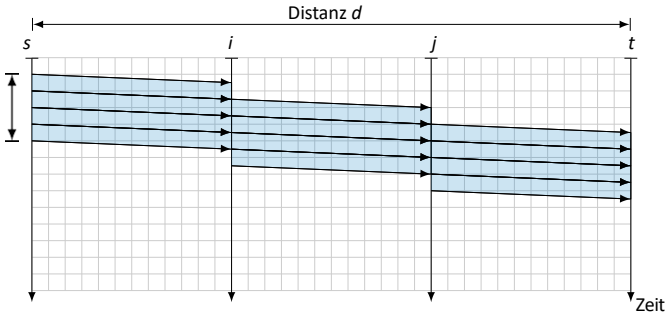
12

NETZWERKTECHNIK / SEMESTER 1 und 2

Übertragungszeit bei der Paketvermittlung

Hier n = 2 Vermittlungsknoten i und j.

Vereinfachend nehmen wir an, dass die Nachrichtenlänge ein Vielfaches von p_{max} ist. (⇒ alle Pakete haben dieselbe Nutzlastgröße p_{max}).



$$T_{PV} = \frac{1}{r}\left(\left\lfloor\frac{L}{p_{max}}\right\rfloor \cdot L_h + L\right) + \frac{d}{v \cdot c_0} + n \cdot \frac{L_H + p_{max}}{r}$$

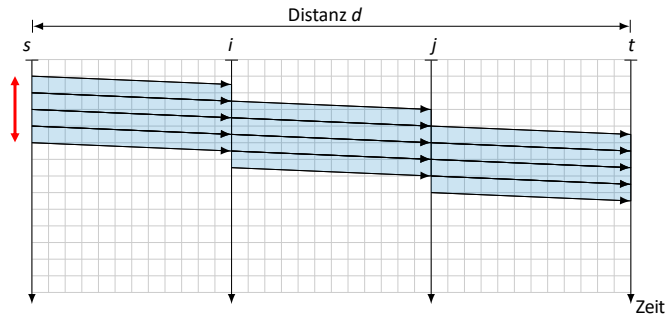
[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), Prof. Dr.-Ing. Georg Carle, TUM, 2025]

NETZWERKTECHNIK / SEMESTER 1 und 2

Übertragungszeit bei der Paketvermittlung

Hier n = 2 Vermittlungsknoten i und j.

Vereinfachend nehmen wir an, dass die Nachrichtenlänge ein Vielfaches von p_{max} ist. (⇒ alle Pakete haben dieselbe Nutzlastgröße p_{max}).



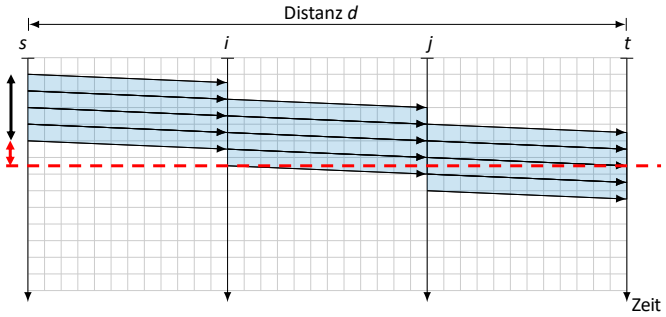
$$T_{PV} = \frac{1}{r}\left(\left\lfloor\frac{L}{p_{max}}\right\rfloor \cdot L_h + L\right) + \frac{d}{v \cdot c_0} + n \cdot \frac{L_H + p_{max}}{r}$$

[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), Prof. Dr.-Ing. Georg Carle, TUM, 2025]

Übertragungszeit bei der Paketvermittlung

Hier n = 2 Vermittlungsknoten i und j.

Vereinfachend nehmen wir an, dass die Nachrichtenlänge ein Vielfaches von p_{max} ist. (⇒ alle Pakete haben dieselbe Nutzlastgröße p_{max}).



$$T_{PV} = \frac{1}{r}\left(\left\lceil\frac{L}{p_{max}}\right\rceil \cdot L_h + L\right) + \frac{d}{v \cdot c_0} + n \cdot \frac{L_H + p_{max}}{r}$$

[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), Prof. Dr.-Ing. Georg Carle, TUM, 2025]

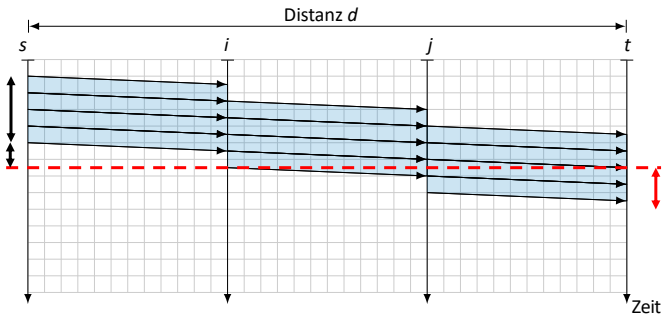
15

NETZWERKTECHNIK / SEMESTER 1 und 2

Übertragungszeit bei der Paketvermittlung

Hier n = 2 Vermittlungsknoten i und j.

Vereinfachend nehmen wir an, dass die Nachrichtenlänge ein Vielfaches von p_{max} ist. (⇒ alle Pakete haben dieselbe Nutzlastgröße p_{max}).



$$T_{PV} = \frac{1}{r}\left(\left\lceil\frac{L}{p_{max}}\right\rceil \cdot L_h + L\right) + \frac{d}{v \cdot c_0} + n \cdot \frac{L_H + p_{max}}{r}$$

[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), Prof. Dr.-Ing. Georg Carle, TUM, 2025]

16

NETZWERKTECHNIK / SEMESTER 1 und 2

Multiplexing auf Paketebene

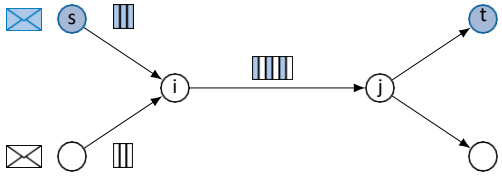
- Durch die Vermittlung kleiner Pakete statt langer Nachrichten werden Engpässe fairer genutzt
- Gehen Pakete verloren, müssen nur Teile einer größeren Nachricht wiederholt werden

Vorteile:

- Flexibles Zeitmultiplex einzelner Pakete
- Pufferung kleiner Pakete statt ganzer Nachrichten

Nachteile:

- Verlust von Paketen durch begrenzten Puffer möglich
- Jedes Paket benötigt seinen eigenen Header (Over- head)
- Empfänger muss Pakete wieder zusammensetzen



tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), Prof. Dr.-Ing. Georg Carle, TUM, 2025]

17

NETZWERKTECHNIK / SEMESTER 1 und 2

Vergleich der drei Verfahren

- Die Distanz zwischen Sender und Empfänger beträgt $d = 1000\ km$
- Für Glasfaserleitungen beträgt $v = 0.7$
- Es kommen $n = 2$ Vermittlungsknoten zum Einsatz
- Die Datenrate beträgt auf allen Teilstrecken $r = 777\ kbit/s$
- Die Länge der zu sendenden Nachricht beträgt $L = 5\ MiB$
- Die maximale Nutzlastgröße betrage $p_{max} = 1480\ B$
- Die Headergröße pro Nachricht / Paket betrage $L_h = 20\ B$

Es ergeben sich folgende Zahlenwerte:

- $T_{LV} \approx 54\ s$
- $T_{NV} \approx 162\ s$
- $T_{PV} \approx 55\ s.$

$$T_{LV} = 2 \cdot t_p + t_s + 2 \cdot t_p$$
$$= t_s + 4 \cdot t_p$$
$$= \frac{L}{r} + \frac{4 \cdot d}{v \cdot c_0} 4$$

$$T_{NV} = (n+1) \cdot t_s + t_p$$
$$= (n+1)\frac{L_H + L}{r} + \frac{d}{v \cdot c_0}$$

$$T_{PV}$$
$$= \frac{1}{r}\left(\left\lceil \frac{L}{p_{max}} \right\rceil \cdot L_h + L\right) + \frac{d}{v \cdot c_0}$$
$$+ n \cdot \frac{L_H + p_{max}}{r}$$

tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), Prof. Dr.-Ing. Georg Carle, TUM, 2025]

18

Wo werden die Verfahren eingesetzt?

Leitungsvermittlung:

- Analoge Telefonverbindungen (POTS)
- Interneteinwahl („letzte Meile“)
- Standortvernetzung von Firmen
- Virtuelle Kanäle (engl. Virtual Circuits) in unterschiedlichen Arten von Vermittlungsnetzen (Frame Relay, ATM, MPLS, . . .)

Nachrichtenvermittlung:

- Kaum praktische Anwendung auf Schicht 3
- Aber: Nachrichtenvermittlung existiert aus Sicht höherer Schichten (ab Schicht 4 aufwärts), z. B. nachrichtenorientierte Transportprotokolle wie UDP oder Anwendungsprotolle wie SMTP
- **Paketvermittlung:**
  - In den meisten modernen Datennetzen
  - Zunehmend auch zur Sprachübertragung (Voice over IP), ebenfalls im Mobilfunknetz
  - Digitales Radio / Fernsehen
  - Viele Peripherieschnittstellen an Computern (PCI, USB, Thunderbolt)

tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), Prof. Dr.-Ing. Georg Carle, TUM, 2025]

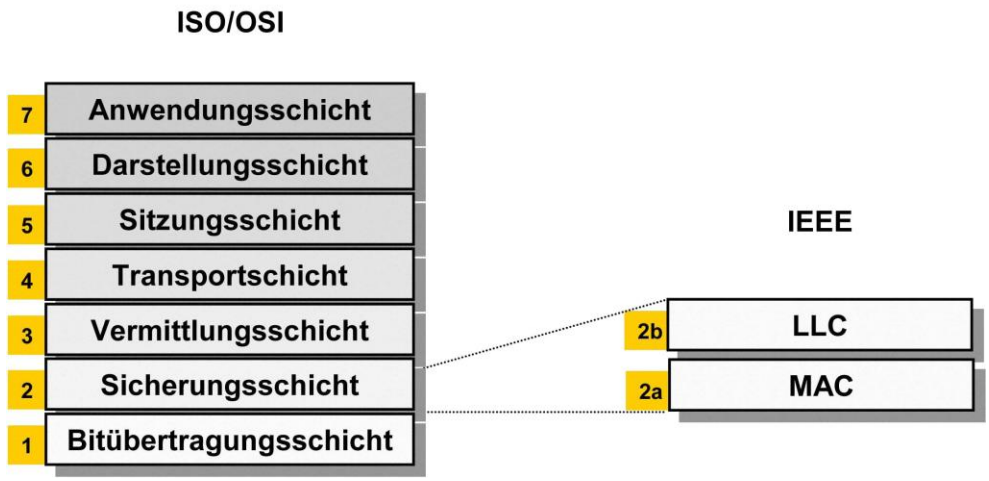
19

02

Vermittlungsschicht

22

Einordnung im ISO/OSI Modell



[Quelle: https://www.airnet.de/cr1-gfe/de/html/TrFddiIEEE802_learningObject6.xml - letzter Abruf 21.07.2025]

Adressierung im Internet

Die **Sicherungsschicht** (Schicht 2) bietet

- fairen Medienzugriff bei von mehreren Hosts geteilten Medien,
- einen „ausreichenden" Schutz vor Übertragungsfehler und
- Adressierung innerhalb eines Direktverbindungsnetzes.

Die **Vermittlungsschicht** (Schicht 3) ergänzt dies um

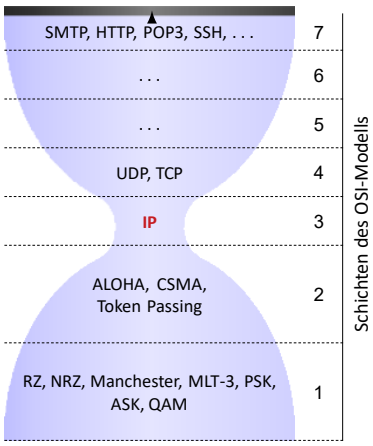
- Global eindeutigen und strukturierten / logischen Adressierung sowie
- Verfahren zur Bestimmung von (möglichst) optimalen Pfaden.

Wir beschränken uns auf die Betrachtung von

- **IPv4** (Internet Protocol v4, 1981) bzw.
- seinem Nachfolger **IPv6** (1998).

Alternative Protokolle der Netzwerkschicht:

IPX (Internetwork Packet Exchange, 1990), DECnet Phase 5 (1987), AppleTalk (1983)



[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), Prof. Dr.-Ing. Georg Carle, TUM, 2025]

Eigenschaften

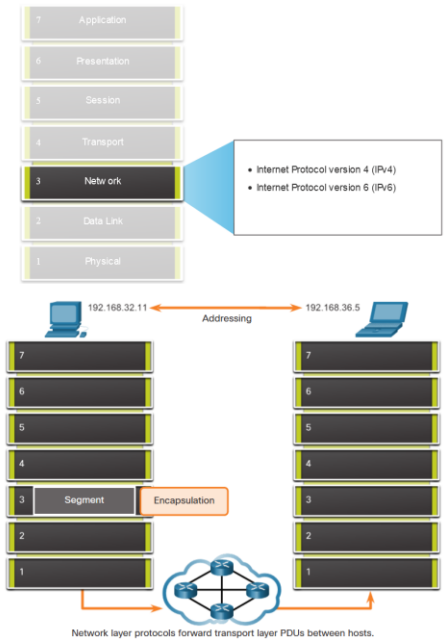
25

25

NETZWERKTECHNIK / SEMESTER 1 und 2

Die Vermittlungsschicht

- Stellt Dienste bereit, mit denen Endgeräte Daten austauschen können
- **IP Version 4 (IPv4) und IP Version 6 (IPv6)** sind die wichtigsten Kommunikationsprotokolle auf Netzwerkebene.
- Die Netzwerkschicht führt **vier grundlegende Vorgänge** aus:
  - Adressierung von Endgeräten
  - Encapsulation
  - Routing
  - De-Encapsulation

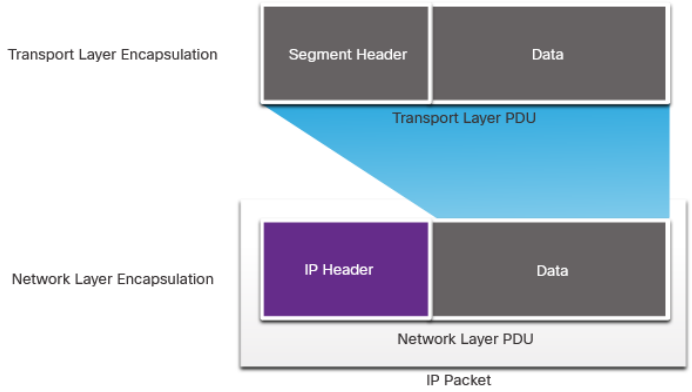


tgm [Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

26

Kapselung

- IP **kapselt das Segment** der Transportschicht.
- IP kann **entweder ein IPv4- oder ein IPv6-Paket verwenden** und wirkt sich nicht auf das Layer-4-Segment aus.
- Das IP-Paket wird **von allen Layer-3-Geräten untersucht**, während es das Netzwerk durchläuft.
- Die **IP-Adressierung** ändert sich nicht von Quelle zu Ziel.



Eigenschaften von IP

IP hat einen geringen Overhead und kann wie folgt beschrieben werden:

- **Verbindungslos**
- **Best-Effort („Nach besten Kräften“)**
- **Medienunabhängig**

Verbindungslos

IP ist verbindungslos

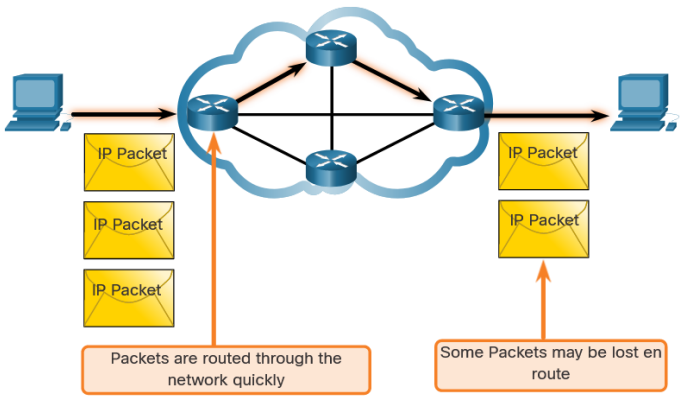
- IP baut **vor dem Senden des Pakets keine Verbindung mit dem Ziel** auf.
- Es werden **keine Steuerungsinformationen** (Synchronisationen, Bestätigungen usw.) benötigt.
- Das Ziel empfängt das Paket, wenn es eintrifft, aber es werden **keine Vorabbenachrichtigungen** vom IP gesendet.
- Wenn ein **Bedarf an verbindungsorientiertem Datenverkehr besteht, wird dies von einem anderen Protokoll verarbeitet** (in der Regel TCP auf der Transportschicht).

[Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

Best-Effort

IP ist Best Effort

- IP übernimmt **keine Garantie für die Zustellung** des Pakets.
- IP hat den Overhead reduziert, da es **keinen Mechanismus zum erneuten Senden von Daten** gibt, die nicht empfangen wurden.
- IP erwartet **keine Bestätigungen**.
- IP weiß nicht**, ob das andere Gerät betriebsbereit ist oder ob es das Paket empfangen** hat.



[Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

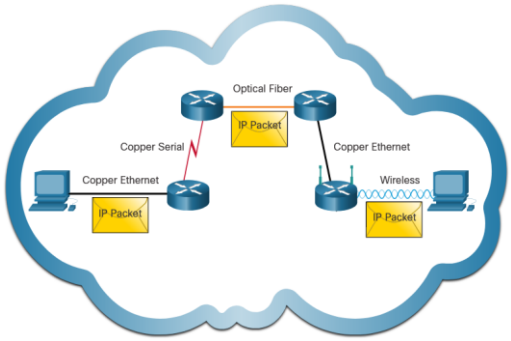
Medienunabhängig

IP ist **unzuverlässig**:

- **Nicht zugestellte oder beschädigte Pakete** können nicht verwaltet oder repariert werden.
- IP kann nach einem **Fehler** nicht erneut übertragen.
- IP kann nicht **Sequenzfehler** (vertauschte Pakete) korrigieren.
- IP muss sich für diese Funktionen auf **andere Protokolle** verlassen.

IP ist **medienunabhängig**:

- IP befasst sich nicht mit der Art des Frames, der auf der Sicherungsschicht erforderlich ist, oder dem Medientyp auf der physikalischen Ebene.
- **IP kann über jeden Medientyp gesendet werden: Kupfer, Glasfaser oder drahtlos.**

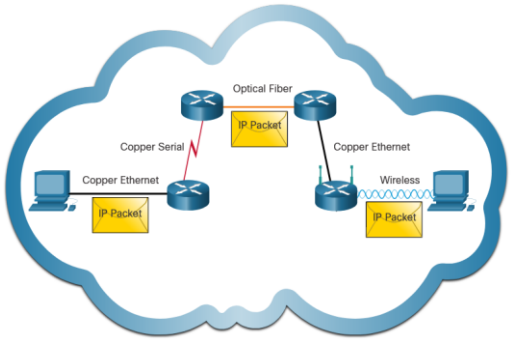


Medienunabhängig

- Die Netzwerkschicht legt die **Maximum Transmission Unit (MTU)** fest.
- Die Netzwerkschicht ermittelt dies aus Steuerinformationen, die von der Sicherungsschicht bereitgestellt werden.
- Das Netzwerk ermittelt dann die MTU-Größe.

Fragmentierung liegt vor, wenn Layer 3 das IPv4-Paket in kleinere Einheiten aufteilt.

- Die **Fragmentierung führt zu Latenz**.
- **IPv6 fragmentiert keine Pakete.**
- Beispiel: Der Router wechselt von Ethernet zu einem langsamen WAN mit einer kleineren MTU



IPv4 Paket

33

33

IPv4-Paket-Header

- IPv4 ist das **primäre Kommunikationsprotokoll** für die Netzwerkschicht.
- Der **Netzwerkheader** hat viele Zwecke:
  - Es stellt sicher, dass das Paket in **die richtige Richtung** (an das Ziel) gesendet wird.
  - Er enthält Informationen in **unterschiedlichen Feldern für die Verarbeitung** innerhalb der Netzwerkschicht
  - Die Informationen im Header werden **von allen Layer-3-Geräten ausgewertet**, die das Paket verarbeiten

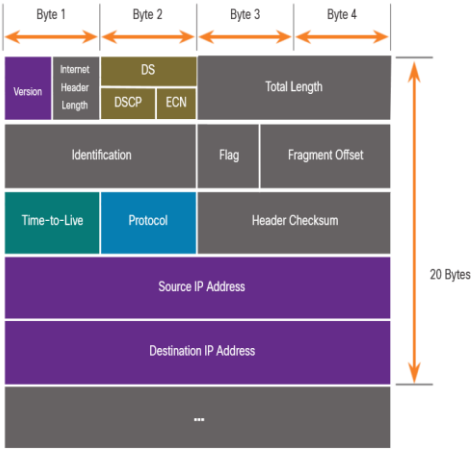
34

NETZWERKTECHNIK / SEMESTER 1 und 2

Felder des IPv4-Paket-Header

Die Eigenschaften des IPv4-Netzwerkheaders:

- Es ist binär.
- Enthält mehrere Informationsfelder
- Das Diagramm wird von links nach rechts gelesen, 4 Byte pro Zeile
- Die beiden wichtigsten Felder sind die Quelle und das Ziel.



tgm [Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

35

NETZWERKTECHNIK / SEMESTER 1 und 2

Felder des IPv4-Paket-Header

Function	Description
Version	Gibt die verwendete IP-Version an. Gültige Werte sind 4 (IPv4) und 6 (IPv6).
IHL (Internet Header Length)	Gibt die Länge des IP Headers inkl. Optionen in Vielfachen von 32 bit an. Wichtig, da der IPv4-Header durch Optionsfelder variable Länge hat.
Differentiated Services	Wird für QoS verwendet: DiffServ – DS-Feld oder das ältere IntServ – ToS oder Servicetyp ▪ Dient der Klassifizierung und Priorisierung von IP-Paketen (z. B. Hinweis auf zeitsensitive Daten wie Sprachübertragungen). ▪ Möglichkeit zur Staukontrolle (Explicit Congestion Notification) auf L3 (optional).
Total Length	▪ Gibt die Gesamtlänge des IP-Pakets (Header + Daten) in Bytes an. ▪ Die Maximallänge eines IP-Pakets beträgt damit 65 535 B. ▪ Der Sender passt die Größe ggf. an, um Fragmentierung zu vermeiden. ▪ Die maximale Paketlänge, so dass keine Fragmentierung notwendig ist, bezeichnet man als Maximum Transmission Unit (MTU). Diese ist abhängig von Schicht 2/1 und beträgt bei FastEthernet 1500 B.

tgm

36

NETZWERKTECHNIK / SEMESTER 1 und 2

Felder des IPv4-Paket-Header

Function	Description
Identification	▪ Für jedes IP-Paket (zufällig) gewählter 16 bit langer Wert. ▪ Dient der Identifikation zusammengehörender Fragmente (IP-Fragmentierung).
Flags	▪ Bit 16: Reserviert und wird auf 0 gesetzt. ▪ Bit 17: Don't Fragment (DF). Ist dieses Bit 1, so keine Fragmentierung erlaubt. ▪ Bit 18: More Fragments (MF). Gibt an, ob weitere Fragmente folgen (1) oder dieses Paket das letzte Fragment ist (0). Wurde das Paket nicht fragmentiert, wird es ebenfalls auf 0 gesetzt.
Fragment Offset	▪ Gibt die absolute Position der Daten in diesem Fragment bezogen auf das unfragmentierte Paket in ganzzahligen Vielfachen von 8 B an. ▪ Ermöglicht zusammen mit dem Identifier und MF-Bit die Reassemblierung fragmentierter Pakete in der richtigen Reihenfolge.
Time to Live (TTL)	▪ Leitet ein Router ein IP-Paket weiter, so dekrementiert er das TTL-Feld um 1. ▪ Erreicht das TTL-Feld den Wert 0, so verwirft ein Router das Paket und sendet eine Benachrichtigung an den Absender (ICMP Time Exceeded). ▪ Dieser Mechanismus beschränkt die Pfadlänge im Internet und verhindert endlos kreisende Pakete infolge von Routing Loops.

NETZWERKTECHNIK / SEMESTER 1 und 2

Felder des IPv4-Paket-Header

Function	Description
Protocol	▪ Identifiziert das Protokoll auf Schicht 4, welches in der Payload (Datenteil) des IP-Pakets enthalten ist. ▪ Relevant u. a. für das Betriebssystem, um Pakete dem richtigen Prozess zuordnen zu können. ▪ Gültige Werte sind beispielsweise 0x06 (TCP) und 0x11 (UDP).
Header Checksum	▪ Einfache, auf Geschwindigkeit optimierte Prüfsumme, welche nur den IP-Header (ohne Daten) schützt. ▪ Die Prüfsumme ist so ausgelegt, dass die Dekrementierung des TTL-Felds einer Inkrementierung der Prüfsumme entspricht. Es ist also keine komplette Neuberechnung der Prüfsumme bei der Weiterleitung von Paketen notwendig, ▪ lediglich eine Inkrementierung +1. ▪ Es ist lediglich Fehlererkennung aber keine Korrektur möglich.

NETZWERKTECHNIK / SEMESTER 1 und 2

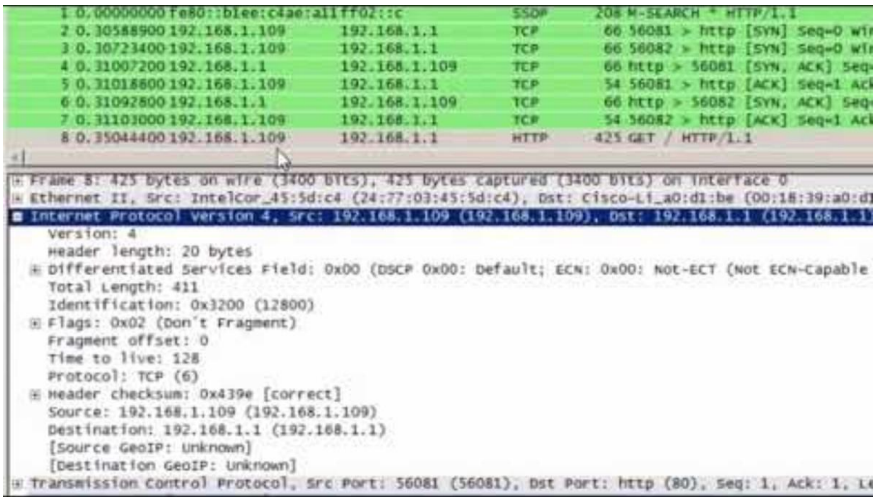
Felder des IPv4-Paket-Header

Function	Description
Source IPv4 Address	32-Bit-Quelladresse
Destination IPV4 Address	32 Bit Zieladresse
Options / Padding	▪ IP unterstützt eine Reihe von Optionen (z. B. Route Recording, Zeitstempel, . . .), welche als optionale Felder an den IP-Header angefügt werden können. ▪ Nicht alle diese Optionen sind 4 B lang. Da die Länge des IP-Headers jedoch ein Vielfaches von 4 B betragen muss, werden kürzere Optionen ggf. durch Padding auf ein Vielfaches von 4 B ergänzt.

tgm [Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

NETZWERKTECHNIK / SEMESTER 1 und 2

Video – Beispiel-IPv4-Header in Wireshark



tgm [Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

IPv6 Paket

42

42

Einschränkungen von IPv4

IPv4 hat **drei Haupteinschränkungen**:

- **Erschöpfung der IPv4-Adressen** – Uns ist im Grunde die IPv4-Adressierung ausgegangen.
- **Fehlende Ende-zu-Ende-Konnektivität** – Damit IPv4 diese lange Zeit überlebt, wurden private Adressierung und NAT erstellt. Damit endete die direkte Kommunikation mit der Beschallung.
- **Erhöhte Netzwerkkomplexität** – NAT war als vorübergehende Lösung gedacht und verursacht Probleme im Netzwerk als Nebeneffekt der Manipulation der Netzwerkheader-Adressierung. NAT verursacht Latenz- und Problembehandlungsprobleme.

tgm [Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

43

NETZWERKTECHNIK / SEMESTER 1 und 2

Internet Protocol Version 6 (IPv6)

- IPv6 wurde Ende 1995 [6] als Nachfolger für IPv4 vorgeschlagen und mit RFC 2460 [7] 1998 standardisiert.
  - und hat IPv4 noch lange nicht obsolet gemacht.
- Hauptgrund dafür ist, dass
  - in erster Linie die Adressknappheit treibende Kraft für die Verbreitung von IPv6 ist und diese erst in den vergangenen Jahren zum Problem wurde.
- Die wesentlichen Änderungen gegenüber IPv4 umfassen:
  - Vergrößerung des Adressraums von 2^{32} auf 2^{128}
  - Vereinfachung des Headerformats (effizientere Verarbeitung auf Routern).
  - Änderungen bei der IP-Fragmentierung.
  - Flexibilität durch sog. Extension Header bei gleichzeitiger Vereinfachung des Headerformats.
  - Stateless Address Autoconfiguration (SLAAC) mittels ICMPv6.
  - Möglichkeit für Stateful Autoconfiguration durch DHCPv6.
  - Nativer Einsatz von Multicast, beispielsweise um alle Router in einem Segment zu adressieren.

tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), Prof. Dr.-Ing. Georg Carle, TUM, 2025]

NETZWERKTECHNIK / SEMESTER 1 und 2

Überblick IPv6

- IPv6 wurde von der Internet Engineering Task Force (**IETF**) entwickelt.
- IPv6 **überwindet die Einschränkungen von IPv4**.
- **Verbesserungen**, die IPv6 bietet:
  - **Erweiterter Adressraum** – basierend auf 128-Bit-Adressen, nicht 32-Bit
  - **Verbessertes Pakethandling** – vereinfachter Header mit weniger Feldern
  - **Eliminiert die Notwendigkeit von NAT** – da es eine große Menge an Adressierungen gibt, ist es nicht erforderlich, intern private Adressierung zu verwenden und einer gemeinsam genutzten öffentlichen Adresse zuzuordnen

IPv4 and IPv6 Address Space Comparison

Number Name	Scientific Notation	Number of Zeros
1 Thousand	10^3	1,000
1 Million	10^6	1,000,000
1 Billion	10^9	1,000,000,000
1 Trillion	10^12	1,000,000,000,000
1 Quadrillion	10^15	1,000,000,000,000,000
1 Quintillion	10^18	1,000,000,000,000,000,000
1 Sextillion	10^21	1,000,000,000,000,000,000,000
1 Septillion	10^24	1,000,000,000,000,000,000,000,000
1 Octillion	10^27	1,000,000,000,000,000,000,000,000,000
1 Nonillion	10^30	1,000,000,000,000,000,000,000,000,000,000
1 Decillion	10^33	1,000,000,000,000,000,000,000,000,000,000,000
1 Undecillion	10^36	1,000,000,000,000,000,000,000,000,000,000,000,000

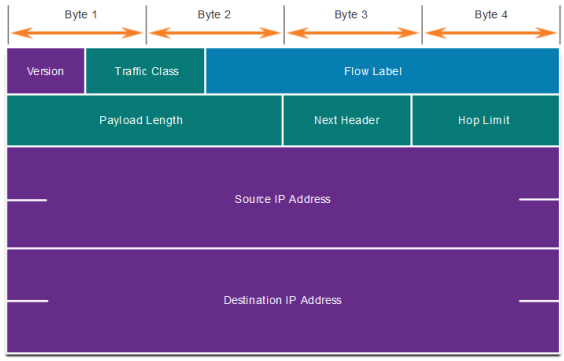
Legend
There are 4 billion IPv4 addresses
There are 340 undecillion IPv6 addresses

tgm [Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

NETZWERKTECHNIK / SEMESTER 1 und 2

Felder des IPv6 Header

- Der **IPv6-Header ist vereinfacht, aber nicht kleiner**.
- Der Header ist auf **40 Byte** oder Oktette festgelegt.
- **Mehrere IPv4-Felder wurden entfernt**, um die Leistung zu verbessern.
  - Flag
  - Fragment Offset
  - Header Checksum



tgm [Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

NETZWERKTECHNIK / SEMESTER 1 und 2

Felder des IPv6 Header

Function	Description
Version	▪ Gibt die verwendete IP-Version an. ▪ Gültige Werte sind 4 (IPv4) und 6 (IPv6).
Traffic Class	▪ Äquivalent zum TOS-Feld des IPv4-Headers. ▪ Wird zur Verkehrspriorisierung / Quality of Service (QoS) verwendet.
Flow Label	▪ Ursprünglich vorgesehen für Echtzeitanwendungen. ▪ Wird heute in erster Linie von Routern verwendet, um zusammengehörende Pakete (Flows) auf Schicht 3 zu erkennen. ▪ Pakete, die zum selben Flow gehören sollen ggf. gleich behandelt werden, z. B. im Fall mehrerer möglicher Pfade zum Ziel alle über denselben Pfad geroutet werden.
Payload Length	▪ Gibt die Länge der auf den IPv6-Header folgenden Daten (inkl. Extension Header, mehr dazu gleich) an. ▪ Angabe in Vielfachen von 1 B. ▪ Der IPv6-Header inkl. seiner Extension Header muss immer ein Vielfaches von 8 B sein.

tgm

Felder des IPv6 Header

Function	Description
Next Header	▪ Gibt den Typ des nächsten Headers an, der am Ende des IPv6-Headers folgt. ▪ Dies kann entweder ein L4-Header (z. B. TCP oder UDP), ein ICMPv6-Header oder ein sog. IPv6 Extension Header sein.
Hop Limit	▪ Entspricht dem TTL-Feld des IPv4-Headers. ▪ Wird beim Weiterleiten eines Pakets durch einen Router um jeweils 1 dekrementiert. ▪ Erreicht der Wert 0, wird das Paket verworfen und ein ICMPv6 Time Exceeded an den ursprünglichen Sender des Pakets zurückgeschickt.
Source IPv4 Address	128-Bit-Quelladresse
Destination IPV4 Address	128 Bit Zieladresse

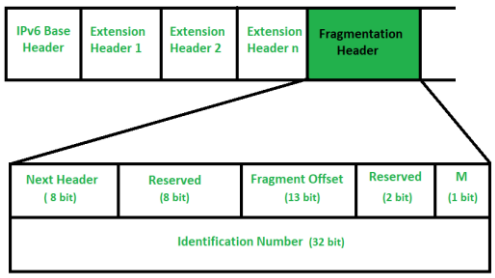
Felder des IPv6 Header

- IPv6-Pakete können auch **Erweiterungsheader (EH)** enthalten.
- Extension Header erlauben es zusätzliche Layer 3 Informationen in einem IPv6 Paket anzufügen.
- Das jeweilige Next Header Feld gibt den jeweils nächsten Extension Header oder das L4 Protokoll an.
- Die Next Header Felder des IPv6 Pakets bzw. der Extension Header bilden hierbei eine Kette, z. B.
  - **IPv6 Header**, Next Header: Routing
  - **Routing Header**, Next Header: Fragment
  - **Fragment Header**, Next Header: TCP
  - **TCP Payload**
- Das Format hängt vom jeweiligen Header ab.
- Mit Ausnahme des Hop-by-Hop Options Header und des Routing Header werden Extension Header nur vom Empfänger ausgewertet.
- Unbekannte Extension Header können vom Empfänger nicht verarbeitet werden → Paket wird mit ICMP Error Message verworfen

Beispiel Extension Header (Fragment Header)

- Rahmen haben auf Schicht 2 eine maximale Größe, z. B. 1514 B für die L2-PDU (ohne CRC-Checksumme) bei IEEE 802.3u (100 Mbit/s Ethernet).
- Diese gibt auch die maximale Größe einer L3-PDU vor, welche als Maximum Transmission Unit (MTU) bezeichnet wird.
- Überschreitet eine L3-PDU diese Größe, muss die L3-SDU fragmentiert und in Form unabhängiger Pakete versendet werden.
- Der Empfänger muss die einzelnen Fragmente im Anschluss reassemblieren.

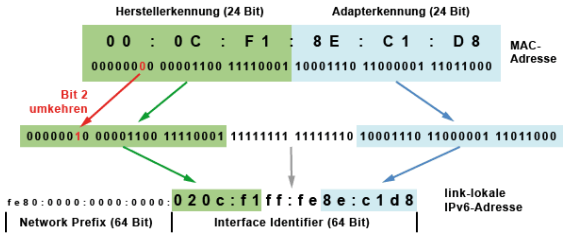
Beispiel Extension Header (Fragment Header)



- **Next Header** - Gibt den nächsten Extension Header oder das verwendete L4 Protokoll an
- **Reserved** - Hat derzeit beim Fragmentation Header keine Verwendung. Bei den meisten anderen Extension Headers gibt dieses Feld die Länge des jeweiligen Extension Headers an.
- **Fragment Offset** - Offset der fragmenierten L3-SDU in Vielfachen von 8 B.
  - Bei IPv6 erfolgt die Fragmentierung ausschließlich am Sender.
  - Bei IPv4 können Pakete, falls nicht explizit über das DF-Bit untersagt, bei Bedarf auch von Routern fragmentiert werden.
- **More Fragments (MF)** - Gibt an, ob auf das aktuelle Paket weitere Fragmente folgen oder ob es sich um das letzte Fragment (gemäß des Fragment Offsets) handelt.
- **Identification** - 32 bit langer, vom Sender zufällig gewählter Wert, welcher alle Fragmente identifiziert, die zu einer L3-SDU reassembliert werden sollen.

Stateless Address Autoconfiguration (SLAAC)

- IPv6 erlaubt eine automatische Konfiguration von Hosts innerhalb eines einzelnen Subnetzes. Ein Host generiert sich die für ein Interface benötigte link-local IPv6-Adresse wie folgt:
- Das **Präfix ist fe80::/10**.
- Der **Subnet Identifier (die folgenden 54 bit) werden auf 0 gesetzt**.
- Die **verbleibenden 64 bit stellen den Interface Identifier dar**, welcher aus der MAC-Adresse des jeweiligen Interfaces als modifizierter EUI-64 Identifier generiert wird:
  - Die ersten 24 bit sind der OUI der MAC-Adresse.
  - Die nachfolgenden 16 bit werden mit ff:fe „gestopft“.
  - Die restlichen 24 bit werden mit dem Device Identifier der MAC-Adresse aufgefüllt.
- Dabei ist das vorletzte Bit des ersten Oktett des OUI (global/local-Bit) invertiert.



[Quelle: https://www.elektronik-kompendium.de/sites/net/1902131.htm - letzter Abruf 21.08.2025]

Warum invertivert?

- Als man den Adressraum für MAC-Adressen festgelegt hat, hat man vorausschauend einen Adressbereich festgelegt, den man sich selber ausdenken kann. Die also nicht zugewiesen werden.
- Im zweiten Bit vom ersten Byte steckt ein Indikator drin, der diese Information enthält
  - ob die MAC-Adresse von der IEEE zugewiesen wurde
  - oder ob sie selber ausgedacht ist.
- Wenn das Bit auf "0" ist, dann handelt es sich um eine MAC-Adresse, die von der IEEE zugewiesen wurde.
- Ist das Bit auf "1", dann ist es eine Phantasie-Adresse.

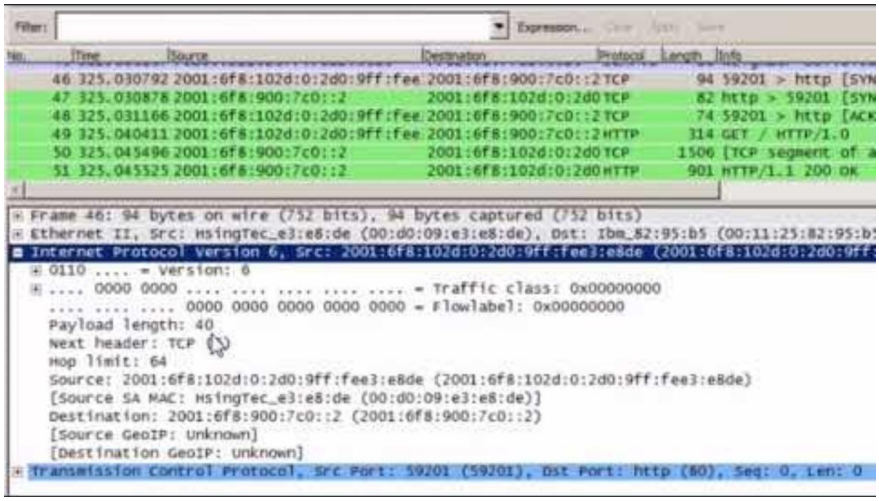
[Quelle: https://www.elektronik-kompendium.de/sites/net/1902131.htm - letzter Abruf 21.08.2025]

Globale Adressen über SLAAC konfigurieren

- Um eine globale Adresse konfigurieren zu können, muss der Host zunächst wissen, welche IPv6 Präfixe von den lokalen Routern bedient werden.
- Präfix Informationen können von den Routern über das **Neighbor Discovery Protocol** in Form von Router Advertisements versendet werden.
- Der Host kann sich über das /64 Präfix und dem modifizierten EUI-64 Identifier selbstständig eine Adresse erzeugen.
- **SLAAC heißt stateless, da die Adressen nicht von einem Server vergeben werden**
  - Globale Adressen können auch über DHCPv6 vergeben werden
- Welche Konsequenzen hat die Erzeugung des Interface Identifiers aus der MAC-Adresse einer Netzwerkkarte hinsichtlich Privacy?
  - Da MAC-Adressen i. d. R. eindeutig sind, kann ein Host durch die in seine IPv6-Adresse eingebettete MAC-Adresse unabhängig von Standard, Anschluss oder Provider verfolgt werden.
- Abhilfe schaffen die IPv6 Privacy Extensions: Erzeugung und regelmäßige Erneuerung von zufälligen Device Identifiern und damit einhergehende Wechsel der globalen IPv6 Adresse.

tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), Prof. Dr.-Ing. Georg Carle, TUM, 2025]

Video – Beispiel-IPv6-Header in Wireshark



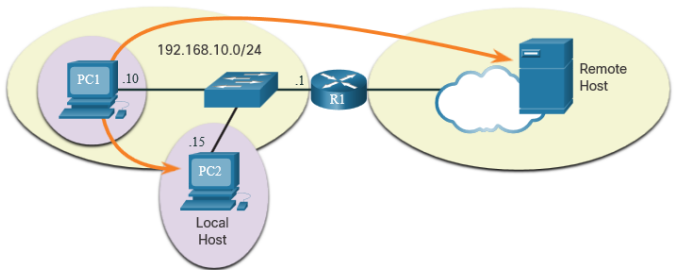
tgm [Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

Weiterleitungs-entscheidungen

57

Entscheidung über die Weiterleitung

- Pakete werden immer **an der Quelle erstellt**.
- **Jedes Hostgerät erstellt eine eigene Routing-Tabelle.**
- Ein Host kann Pakete an folgende Stellen senden:
- **Sich selbst** – 127.0.0.1 (IPv4), ::1 (IPv6)
- **Lokale Hosts** – Ziel befindet sich im selben LAN
- **Remote-Hosts** – Geräte befinden sich nicht im selben LAN



tgm [Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

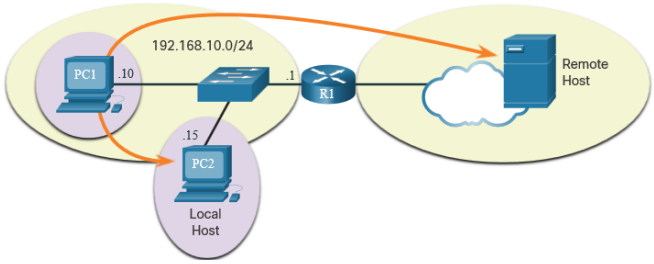
58

Entscheidung über die Weiterleitung

Das Quellgerät bestimmt, ob es sich um ein lokales oder ein Remote-Ziel handelt

Methode zur Bestimmung:

- **IPv4** – Die Quelle verwendet ihre eigene IP-Adresse und Subnetzmaske zusammen mit der Ziel-IP-Adresse.
- **IPv6** – Die Quelle verwendet die Netzwerkadresse und das Präfix, die vom lokalen Router angekündigt werden.
- **Lokaler Datenverkehr wird über die Hostschnittstelle ausgegeben**, um von einem zwischengeschalteten Gerät verarbeitet zu werden.
- Der **Remote-Datenverkehr wird direkt an das Standard-Gateway** im LAN weitergeleitet.

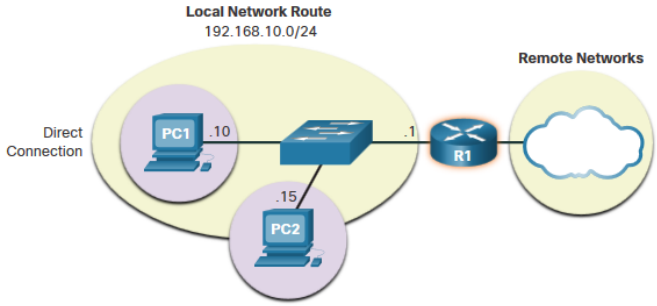


Default Gateway

- Ein **Router oder Layer-3-Switch** kann ein Standard-Gateway sein.
- **Funktionen** eines Standard-Gateways (DGW):
  - Er muss über eine **IP-Adresse** verfügen, die sich **im selben Bereich** wie der Rest des LAN befindet.
  - Es kann Daten aus dem LAN akzeptieren und den Datenverkehr **aus dem LAN rausleiten**.
  - Es kann **zu anderen Netzwerken** weiterleiten.
  - Wenn ein Gerät über kein Standard-Gateway oder ein **fehlerhaftes Standard-Gateway verfügt, kann der Datenverkehr das LAN nicht verlassen**.

Ein Rechner schickt an das Default Gateway

- Der **Host kennt das Standard-Gateway** (DGW) entweder statisch oder über DHCP in IPv4.
- **IPv6 sendet den DGW über eine Router Solicitation (RS)** oder kann manuell konfiguriert werden.
- **Eine DGW ist eine statische Route**, die in der Routing-Tabelle als letzter Ausweg gilt.
- Alle Geräte im LAN benötigen das DGW des Routers, wenn sie beabsichtigen, **Datenverkehr remote zu senden**.



Routing Tabelle eines Hosts

- Unter Windows **route print oder netstat -r**, um die PC-Routing-Tabelle anzuzeigen

Drei Abschnitte, die von diesen beiden Befehlen angezeigt werden:

- **Schnittstellenliste** – alle potenziellen Schnittstellen und MAC-Adressierung
- **IPv4-Routing-Tabelle**
- **IPv6-Routing-Tabelle**

IPv4 Routing Table for PC1

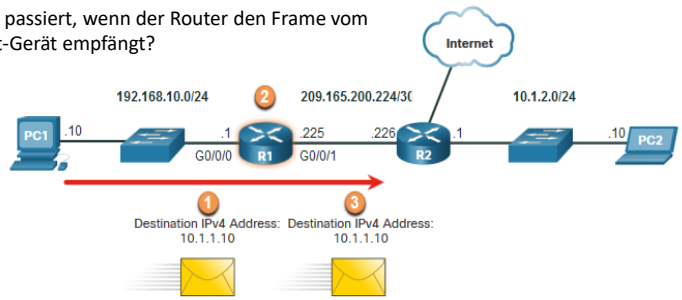
```
C:\Users\PC1> netstat -r

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.10.1    192.168.10.10      25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1     306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1     306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1     306
    192.168.10.0    255.255.255.0         On-link    192.168.10.10     281
   192.168.10.10  255.255.255.255         On-link    192.168.10.10     281
  192.168.10.255  255.255.255.255         On-link    192.168.10.10     281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1     306
        224.0.0.0        240.0.0.0         On-link    192.168.10.10     281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1     306
  255.255.255.255  255.255.255.255         On-link    192.168.10.10     281
```

Einführung in Routing

64

Entscheidung über Paketweiterleitung

Was passiert, wenn der Router den Frame vom Host-Gerät empfängt?



R1 Routing Table

Route	Next Hop or Exit Interface
192.168.10.0 /24	G0/0/0
209.165.200.224/30	G0/0/1
10.1.1.0/24	**via R2**
Default Route 0.0.0.0/0	via R2

1. Packet arrives on the Gigabit Ethernet 0/0/0 interface of router R1. R1 de-encapsulates the Layer 2 Ethernet header and trailer.
2. Router R1 examines the destination IPv4 address of the packet and searches for the best match in its IPv4 routing table. The route entry indicates that this packet is to be forwarded to router R2.
3. Router R1 encapsulates the packet into a new Ethernet header and trailer, and forwards the packet to the next hop router R2.

tgm [Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

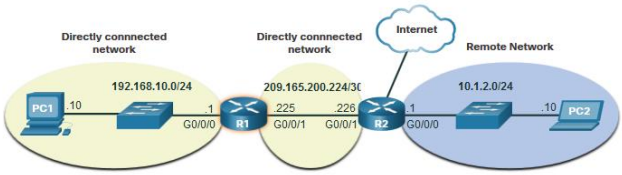
65

NETZWERKTECHNIK / SEMESTER 1 und 2

IP Router Routing Tabelle

Es gibt drei Arten von Routen in der Routing-Tabelle eines Routers:

- **Direkt verbunden** – Diese Routen werden automatisch vom Router hinzugefügt, sofern die Schnittstelle aktiv ist und über eine Adressierung verfügt.
- **Remote** – Dies sind die Routen, mit denen der Router keine direkte Verbindung hat und die möglicherweise gelernt werden können:
  - **Manuell** – mit einer statischen Route
  - **Dynamisch** – durch die Verwendung eines Routing-Protokolls, damit die Router ihre Informationen miteinander teilen
- **Standardroute**: Hiermit wird der gesamte Datenverkehr in eine bestimmte Richtung weitergeleitet, wenn in der Routing-Tabelle keine Übereinstimmung vorhanden ist.



[Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

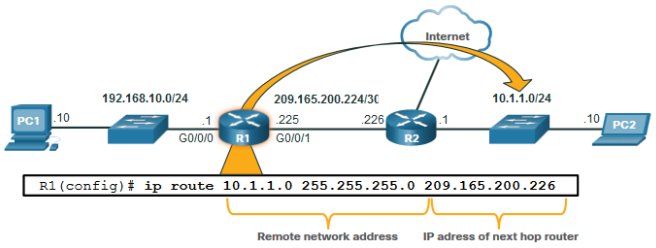
66

NETZWERKTECHNIK / SEMESTER 1 und 2

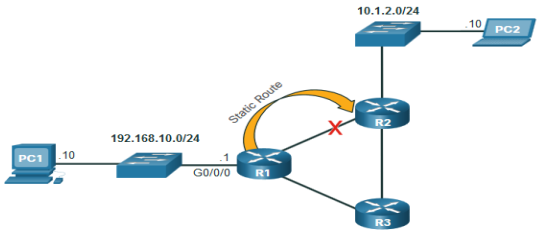
Statisches Routing

Eigenschaften der statischen Route:

- Muss **manuell** konfiguriert werden
- Muss vom Administrator manuell **angepasst werden, wenn sich die Topologie ändert**
- Gut für **kleine, nicht redundante Netzwerke**
- Wird **häufig in Verbindung mit einem dynamischen Routing-Protokoll** zur Konfiguration einer Standardroute verwendet



R1 is manually configured with a static route to reach the 10.1.1.0/24 network. If this path changes, R1 will require a new static route.



If the route from R1 via R2 is no longer available, a new static route via R3 would need to be configured. A static route does not automatically adjust for topology changes.

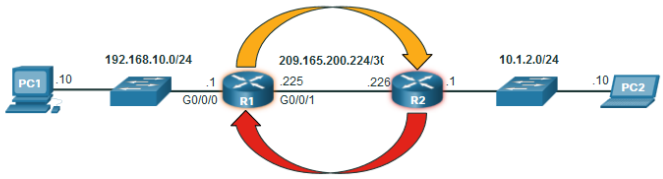
[Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

67

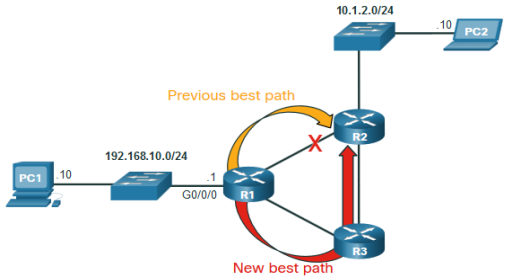
Dynamisches Routing

Dynamische Routing automatisiert das:

- **Erkennen** von Remote-Netzwerken
- **Pflegen** aktuelle Informationen
- **Wählen des besten Weg** zum Ziel
- **Finden neuer optimalere Pfade** bei einer Topologieänderung
- Dynamisches Routing kann auch statische Standardrouten mit den anderen Routern teilen.



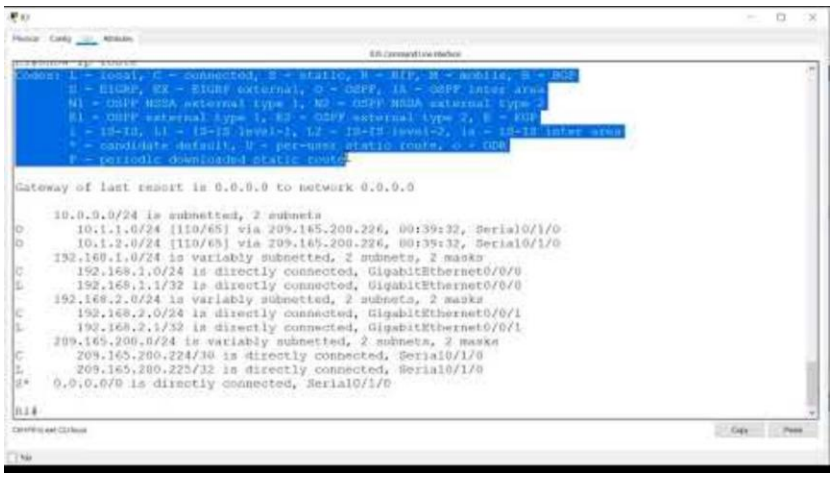
- R1 is using the routing protocol OSPF to let R2 know about the 192.168.10.0/24 network.
- R2 is using the routing protocol OSPF to let R1 know about the 10.1.1.0/24 network.



R1, R2, and R3 are using the dynamic routing protocol OSPF. If there is a network topology change, they can automatically adjust to find a new best path.

tgm [Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

Video – IPv4 Router Routing Tables



tgm [Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

03

Adressauflösung

Ziele

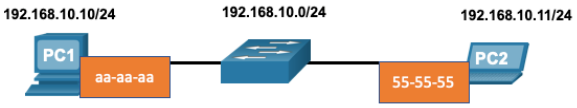
- Vergleichen Sie die Rollen der MAC-Adresse und der IP-Adresse.
- Beschreiben Sie den Zweck von ARP.
- Beschreiben Sie den Betrieb der IPv6-Nachbarerkennung.

MAC und IP

73

Ziel im selben Netzwerk

- Es gibt **zwei primäre Adressen**, die einem Gerät in einem Ethernet-LAN zugewiesen sind:
- **Physische Layer-2-Adresse** (die MAC-Adresse) – Wird für die NIC-zu-NIC-Kommunikation im selben Ethernet-Netzwerk verwendet.
- **Logische Layer-3-Adresse** (die IP-Adresse) – Wird verwendet, um das Paket vom Quellgerät an das Zielgerät zu senden.
- Layer-2-Adressen werden verwendet, um Frames von einer Netzwerkkarte zu einer anderen Netzwerkkarte im selben Netzwerk zu übermitteln. **Wenn sich eine Ziel-IP-Adresse im selben Netzwerk befindet, ist die Ziel-MAC-Adresse die des Zielgeräts.**



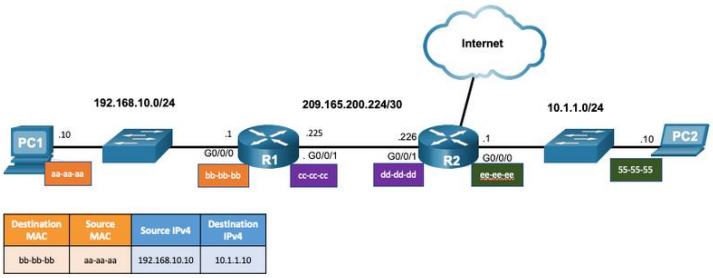
Destination MAC	Source MAC	Source IPv4	Destination IPv4
55-55-55	aa-aa-aa	192.168.10.10	192.168.10.11

tgm [Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

74

Ziel in einem Remote Netzwerk

- Wenn sich die Ziel-IP-Adresse in einem Remotenetzwerk befindet, ist die **Ziel-MAC-Adresse die des Standardgateways.**
- **ARP wird von IPv4 verwendet**, um die IPv4-Adresse eines Geräts mit der MAC-Adresse der Geräte-NIC zu verknüpfen.
- **ICMPv6 wird von IPv6 verwendet**, um die IPv6-Adresse eines Geräts mit der MAC-Adresse der Geräte-NIC zu verknüpfen.



Destination MAC	Source MAC	Source IPv4	Destination IPv4
bb-bb-bb	aa-aa-aa	192.168.10.10	10.1.1.10

tgm [Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

75

ARP

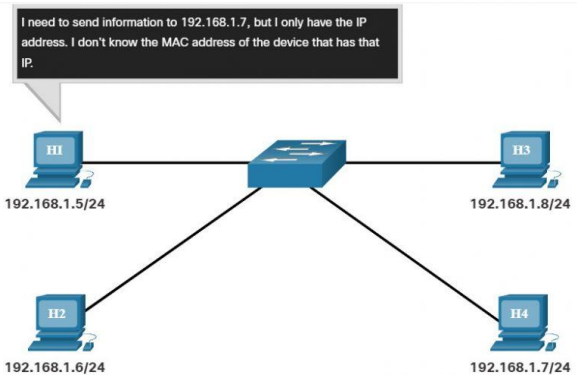
76

ARP Überblick

- Ein Gerät verwendet ARP, **um die Ziel-MAC-Adresse eines lokalen Geräts zu bestimmen**, wenn es seine IPv4-Adresse kennt.

ARP bietet zwei grundlegende Funktionen:

- **Auflösen** von IPv4-Adressen in MAC-Adressen
- **Verwalten einer ARP-Tabelle** mit IPv4- und MAC-Adresszuordnungen



[Quelle: https://itexamanswers.net/ccna-1-v7-0-curriculum-module-9-address-resolution.html - letzter Abruf 21.08.2025]

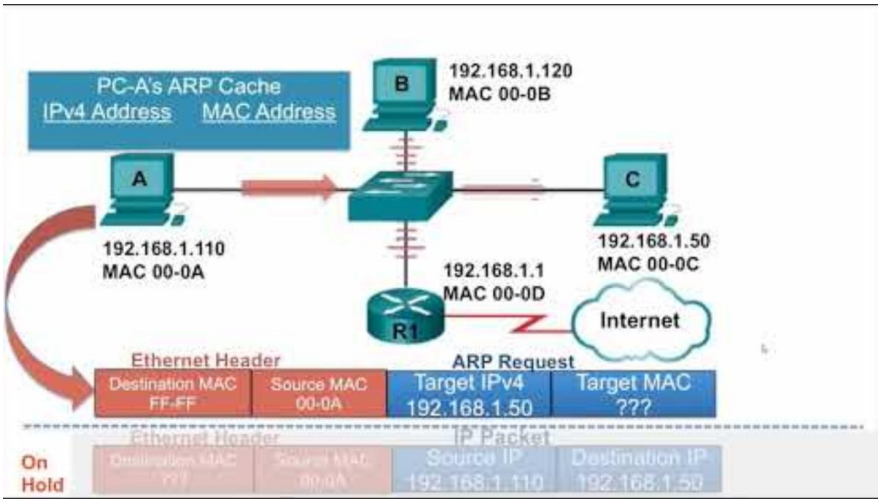
ARP Funktionen

Um einen Frame zu senden, **durchsucht ein Gerät seine ARP-Tabelle nach einer IPv4-Zieladresse** und einer entsprechenden MAC-Adresse.

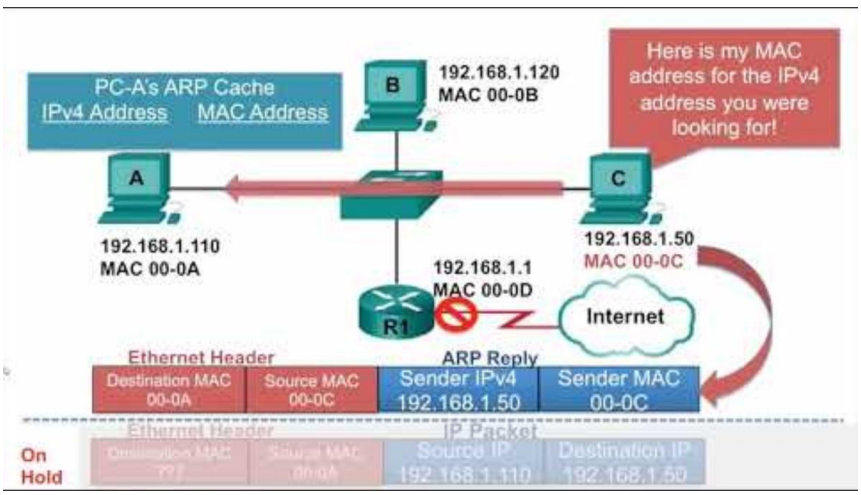
- Wenn sich die IPv4-Zieladresse des Pakets **im selben Netzwerk** befindet, durchsucht das Gerät die ARP-Tabelle nach der IPv4-Zieladresse.
- Wenn sich die IPv4-Zieladresse **in einem anderen Netzwerk** befindet, durchsucht das Gerät die ARP-Tabelle nach der IPv4-Adresse des Standardgateways.
- Wenn das Gerät die IPv4-Adresse findet, wird die entsprechende MAC-Adresse als Ziel-MAC-Adresse im Frame verwendet.
- Wenn kein ARP-Tabelleneintrag gefunden wird, sendet das Gerät eine **ARP-Anforderung**.

[Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

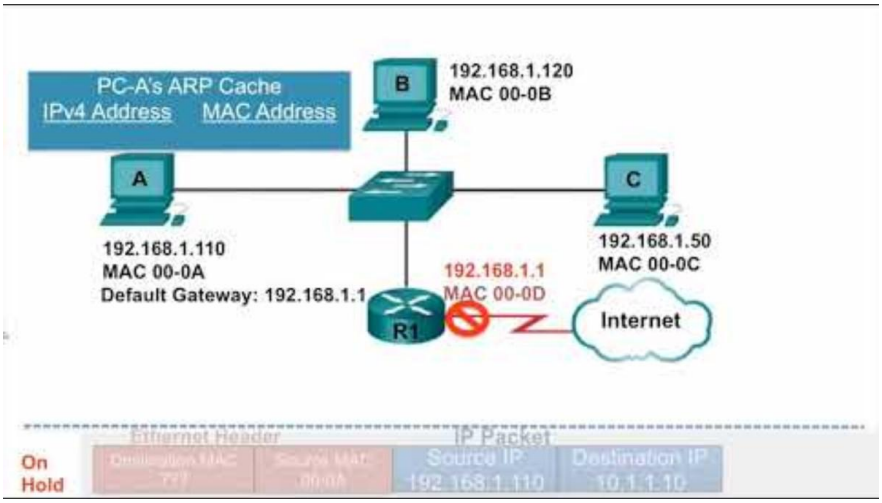
Video - ARP Request



Video – ARP Operation - ARP Reply



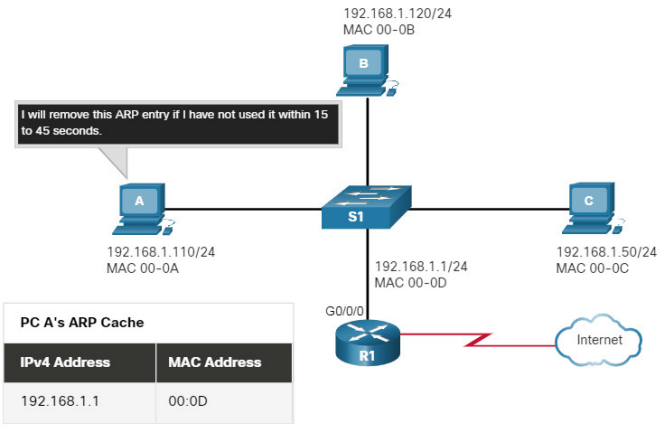
Video - ARP Role in Remote Communications



[Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

Entfernen von Einträgen aus einer ARP-Tabelle

- **Einträge in der ARP-Tabelle sind nicht dauerhaft** und werden entfernt, wenn ein ARP-Cache-Timer nach einem bestimmten Zeitraum abläuft.
- Die Dauer des **ARP-Cache-Timers** ist je nach Betriebssystem unterschiedlich.
- ARP-Tabelleneinträge können auch **manuell vom Administrator entfernt werden**.



PC A's ARP Cache

IPv4 Address	MAC Address
192.168.1.1	00:0D

Note: MAC addresses are shortened for demonstration purposes.

[Quelle: https://itexamanswers.net/ccna-1-v7-0-curriculum-module-9-address-resolution.html - letzter Abruf 21.08.2025]

NETZWERKTECHNIK / SEMESTER 1 und 2

ARP-Tabellen auf Netzwerkgeräten

- Der Befehl `show ip arp` zeigt die ARP-Tabelle auf einem Cisco Router an.
- Der Befehl `arp -a` zeigt die ARP-Tabelle auf einem Windows 10-PC an.

```
R1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.10.1           -   a0e0.af0d.e140  ARPA   GigabitEthernet0/0/0
```

```
C:\Users\PC> arp -a

Interface: 192.168.1.124 --- 0x10
  Internet Address      Physical Address      Type
  192.168.1.1           c8-d7-19-cc-a0-86     dynamic
  192.168.1.101         08-3e-0c-f5-f7-77     dynamic
```

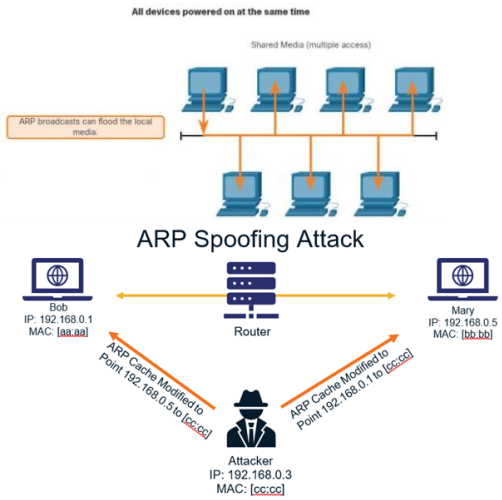
tgm [Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

83

NETZWERKTECHNIK / SEMESTER 1 und 2

ARP-Probleme – ARP-Broadcasting und ARP-Spoofing

- ARP-Anfragen werden von jedem Gerät im lokalen Netzwerk empfangen und verarbeitet.
- **Übermäßige ARP-Broadcasts können zu Leistungseinbußen führen.**
- **ARP-Antworten können von einem Bedrohungsakteur gefälscht werden**, um einen ARP-Poisoning-Angriff durchzuführen.
- Switches auf Unternehmensebene umfassen Abwehrtechniken zum Schutz vor ARP-Angriffen.



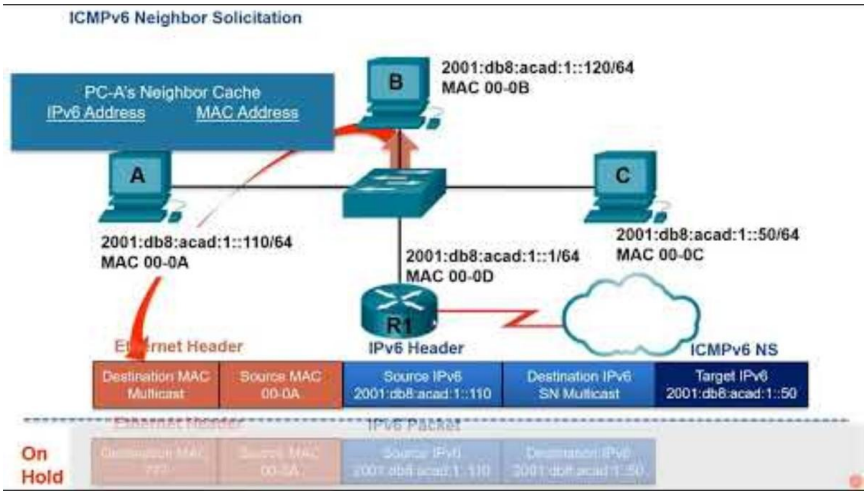
tgm [Quelle: https://www.thesslstore.com/blog/everything-you-need-to-know-about-arp-spoofing/ - letzter Abruf 21.08.2025]

84

Neighbour Discovery

86

Video – IPv6 Neighbor Discovery



[Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

87

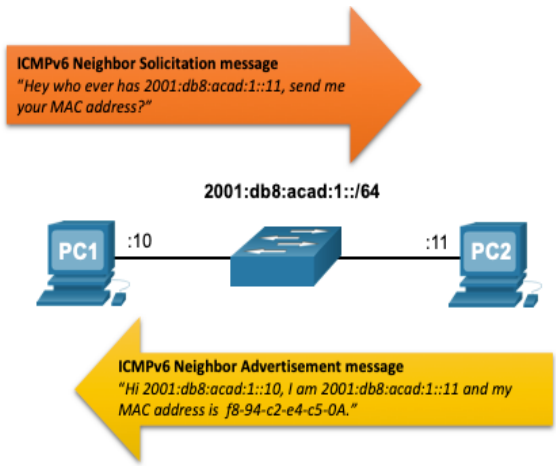
IPv6 Neighbor Discovery Messages

Das IPv6 Neighbor Discovery (ND)-Protokoll bietet Folgendes:

- **Adress-Auflösung**
- **Router-Erkennung**
- **Nachleitungsdienste**
- ICMPv6-Nachrichten **Neighbor Solicitation (NS**) und **Neighbor Advertisement (NA)** werden für Device-to-Device-Messaging verwendet, z. B. für die Adressauflösung.
- ICMTPv6 **Router Solicitation (RS)** und **Router Advertisement (RA)** Nachrichten werden für Messaging zwischen Geräten und Routern für die Router-Erkennung verwendet.
- ICMPv6-**Redirect** Nachrichten werden von Routern verwendet, um die Auswahl des nächsten Hops zu verbessern.

IPv6 Neighbor Discovery – Auflösung von Adressen

- IPv6-Geräte verwenden **NDP (Network Discovery Protocol)**, um die MAC-Adresse einer bekannten IPv6-Adresse aufzulösen.
- ICMPv6 Neighbor Solicitation-Nachrichten werden über spezielle Ethernet- und **IPv6-Multicast-Adressen** gesendet.

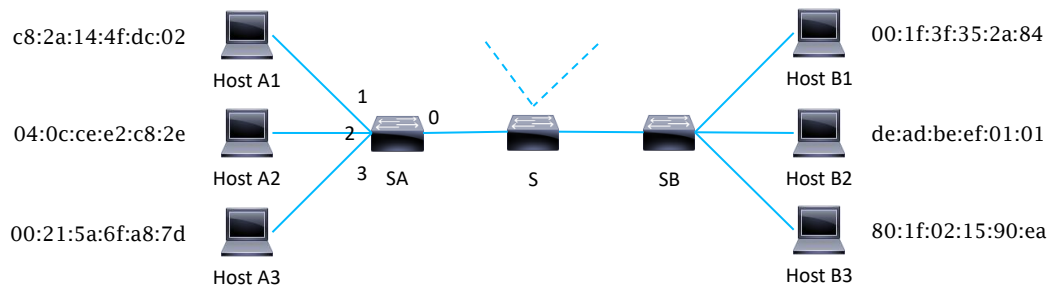


04

IPv4 Beispiel-netzwerk

90

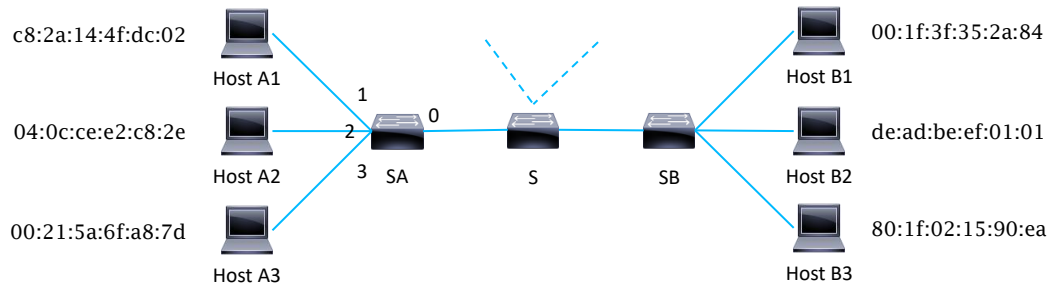
Beispielnetz, basierend auf aktuellen Ethernet-Standard



91

NETZWERKTECHNIK / SEMESTER 1 und 2

Beispielnetz, basierend auf aktuellen Ethernet-Standard



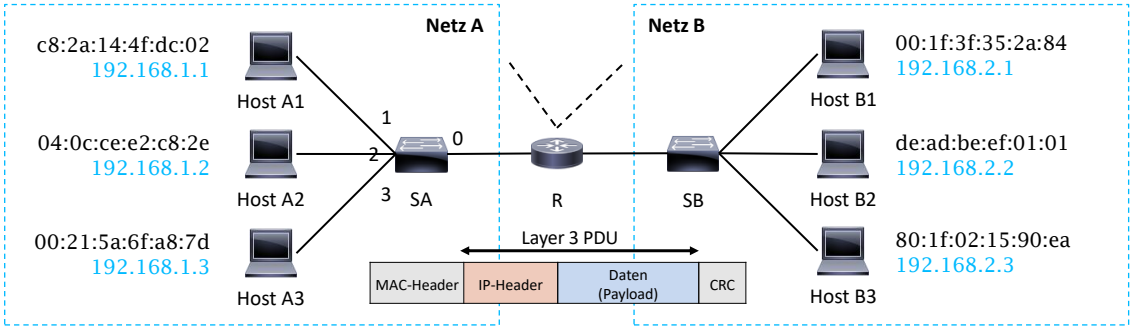
- Wie viele Einträge enthält die Switching-Tabelle von Switch SA?
- Genau einen Eintrag für jeden bekannten Host
- Die meisten MAC-Adressen werden auf Port 0 abgebildet
- Eine Zusammenfassung von Einträgen ist i. A. nicht möglich, da MAC-Adressen nicht die Position eines Knotens innerhalb eines Netzwerks widerspiegeln

Port	MAC
0	00:1f:3f:35:2a:84
0	de:ad:be:ef:01:01
0	80:1f:02:15:90:ea
1	c8:2a:14:4f:dc:02
2	04:0c:ce:e2:c8:2e
3	00:21:5a:6f:a8:7d

92

NETZWERKTECHNIK / SEMESTER 1 und 2

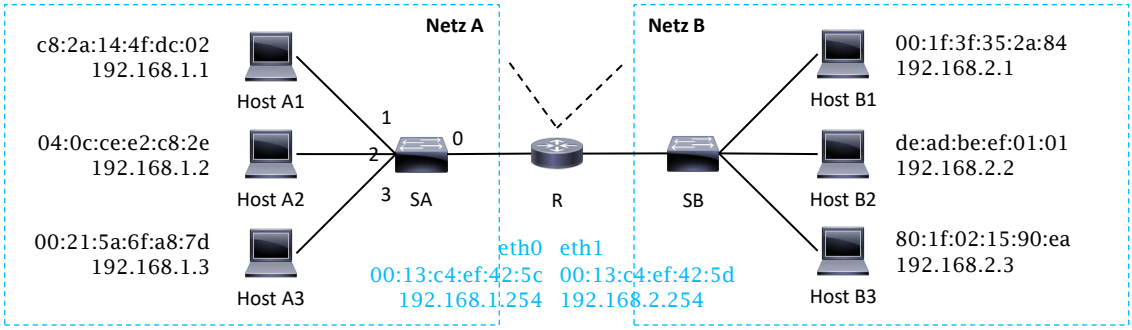
Beispielnetz, basierend auf aktuellen Ethernet-Standard



- Jedem Host ist eine IP-Adresse zugewiesen.
- Jede IP-Adresse ist in vier Gruppen zu je 1 Byte, durch Punkte getrennt, dargestellt (Dotted Decimal Notation).
- In diesem Beispiel identifiziert das 4. Oktett einen Host innerhalb eines Netzes.
- Die ersten drei Oktette identifizieren das Netzwerk, in dem sich der Host befindet.
- Der Router R trifft Weiterleitungsentscheidungen auf Basis der Ziel-IP-Adresse ⇒ Jedes Paket muss mit einer Absender- und Ziel-IP-Adresse (im IP-Header) versehen werden

93

Beispielnetz, basierend auf aktuellen Ethernet-Standard



- Innerhalb von Netz A erreichen sich alle Hosts weiterhin direkt über SA.
- Will Host A1 nun ein Paket an Host B2 schicken, so geht das nicht mehr direkt: Die Weiterleitung von A nach B erfolgt über R auf Basis von IP-Adressen
- Host A1 muss also dafür sorgen, dass R das Paket erhält, dazu verwendet Host A1 als Ziel-MAC-Adresse die des lokalen Interfaces von R, als Ziel-IP-Adresse wird die IP-Adresse von Host B2 verwendet

⇒ R muss adressierbar sein und verfügt auf jedem Interface über eine eigene MAC- und IP Adresse

Beispielnetz, basierend auf aktuellen Ethernet-Standard

Offene Probleme:

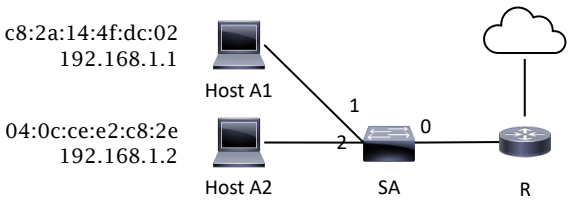
- Angenommen der Sender kennt nur die IP-Adresse des Ziels. Wie kann die MAC-Adresse des Next-Hops bestimmt werden? (**Adressauflösung**)
- Woher weiß Host A1, dass er Netz B über R erreichen kann? (**Routing Table**)
- Angenommen das Ziel eines Pakets befindet sich nicht in einem direkt an R angeschlossenen Netz. Woher kennt R die richtige Richtung? (Genauer: Den richtigen Next Hop?) (**Routing Table**)
- Wie wird diese „Routing Table“ erzeugt? (**statisches Routing, Routing-Protokolle**)
- Was ist, wenn R mehrere Wege zu einem Ziel kennt? (**Longest Prefix Matching**)
- Wie funktioniert die Unterteilung einer IP-Adresse in Netz- und Hostanteil? (**Classful Routing, Classless Routing, Subnetting**)
- Woher kennt der Sender überhaupt die IP-Adresse des Ziels? (**DNS → Schicht 7**)

NETZWERKTECHNIK / SEMESTER 1 und 2

Beispielnetz, basierend auf aktuellen Ethernet-Standard

Adressauflösung

- Host A1 will eine Nachricht an Host A2 senden
- Die IP-Adresse von Host A2 (192.168.1.2) sei ihm bereits bekannt
- Wie erhält Host1 die zugehörige MAC-Adresse?



NETZWERKTECHNIK / SEMESTER 1 und 2

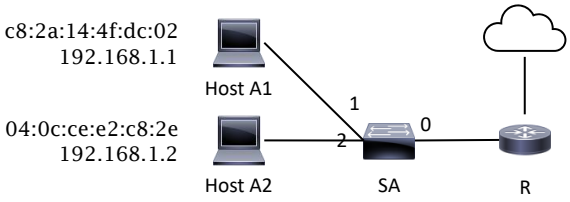
Beispielnetz, basierend auf aktuellen Ethernet-Standard

Adressauflösung

- Host A1 will eine Nachricht an Host A2 senden
- Die IP-Adresse von Host A2 (192.168.1.2) sei ihm bereits bekannt
- Wie erhält Host1 die zugehörige MAC-Adresse?

Address Resolution Protocol (ARP)

- Host A1 sendet einen ARP-Request: „Who has 192.168.1.2? Tell 192.168.1.1 at c8:2a:14:4f:dc:02“
- Host A2 antwortet mit einem ARP-Reply: „192.168.1.2 is at 04:0c:ce:e2:c8:2e“



Beispielnetz, basierend auf aktuellen Ethernet-Standard

Address Resolution Protocol (ARP) - ARP-Paket für IPv4 über Ethernet

Hardware Type		Protocol Type
Hardware Length	Protocol Length	Operation
Sender Hardware Address		
Sender Protocol Address		
Target Hardware Address		
Target Protocol Address		

FIELD	SIZE	PURPOSE
HARDWARE TYPE	16	Define the Type of hardware the ARP is running. Eg. Ethernet is type 1.
PROTOCOL TYPE	16	Define for which higher level protocol is ARP used. Eg. IPv4 value is 0x0800
HARDWARE LENGTH	8	Length of Hardware Address in bytes. Eg. Ethernet MAC address is 6 bytes
PROTOCOL LENGTH	8	Length of Protocol Address in bytes. Eg. IPv4 address is 4 bytes
OPCODE	16	Define type of Operation. There 4 values - 1 - ARP Request, 2 - ARP Reply, 3 - RARP Request, 4 - RARP Reply
SENDER HARDWARE ADDRESS	48	Physical Address of the sender
SENDER PROTOCOL ADDRESS	32	Logical Address of the sender
TARGET HARDWARE ADDRESS	48	Physical Address of the Target
TARGET PROTOCOL ADDRESS	32	Logical Address of the Target

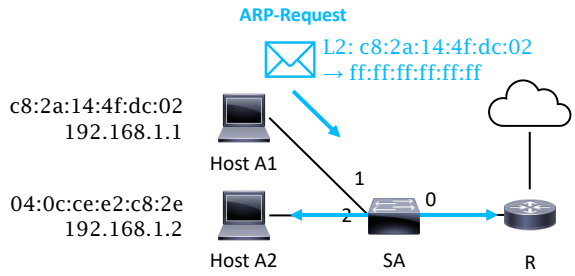
tgm [Quelle: https://networkinglessons.wordpress.com/2015/05/30/lesson-8-address-resolution-protocol-arp/ - letzter Abruf 21.08.2025]

Beispielnetz, basierend auf aktuellen Ethernet-Standard

Beispiel: (L2: xx:xx:xx:xx:xx:xx → yy:yy:yy:yy:yy:yy stellt Quell- und Ziel-MAC-Adresse auf Schicht 2 dar.)

- Der ARP-Request wird an die MAC-Broadcast-Adresse ff:ff:ff:ff:ff:ff geschickt, weswegen der Switch SA den Rahmen an alle angeschlossenen Hosts weiterleitet.

0x0001 (Ethernet)		0x0800 (IPv4)
0x06	0x04	0x0001 (Request)
0xc82a144fdc02 (Sender)		
0xc0c80101 (Sender)		
0x00000000 (Target)		
0xc0a80102 (Target)		



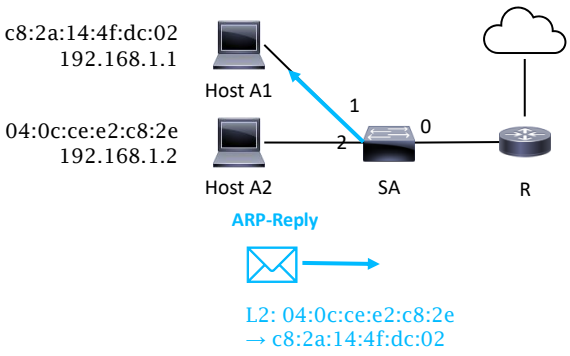
tgm

Beispielnetz, basierend auf aktuellen Ethernet-Standard

Beispiel: (L2: xx:xx:xx:xx:xx:xx → yy:yy:yy:yy:yy:yy stellt Quell- und Ziel-MAC-Adresse auf Schicht 2 dar.)

- Der ARP-Reply wird als MAC-Unicast versendet (adressiert an Host1).
- Die Rollen Sender / Target sind zwischen Request und Reply vertauscht.

0x0001 (Ethernet)		0x0800 (IPv4)
0x06	0x04	0x0002 (Reply)
0x040ccee2c82e (Sender)		
0xc0a80102 (Sender)		
0xc82a144fdc02 (Target)		
0xc0a80101 (Target)		

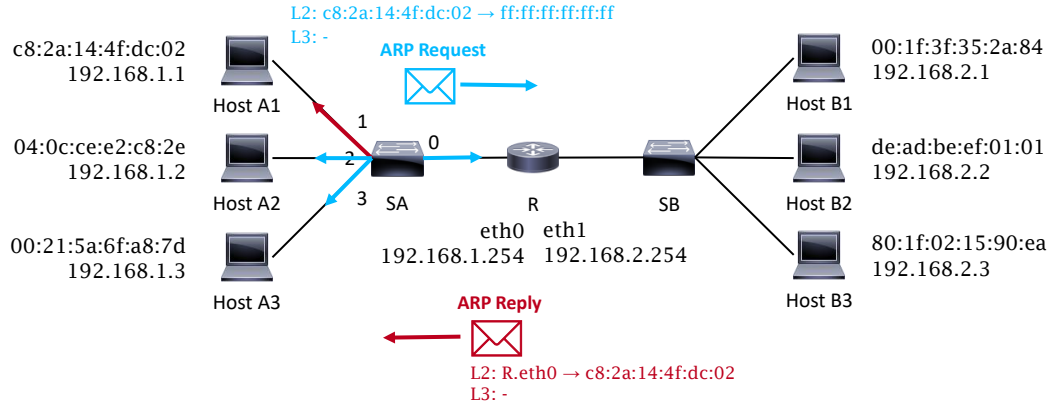


Beispielnetz, basierend auf aktuellen Ethernet-Standard

Was ist nun, wenn das Ziel nicht im selben Netz liegt (z. B. Host A1 an Host B2)?

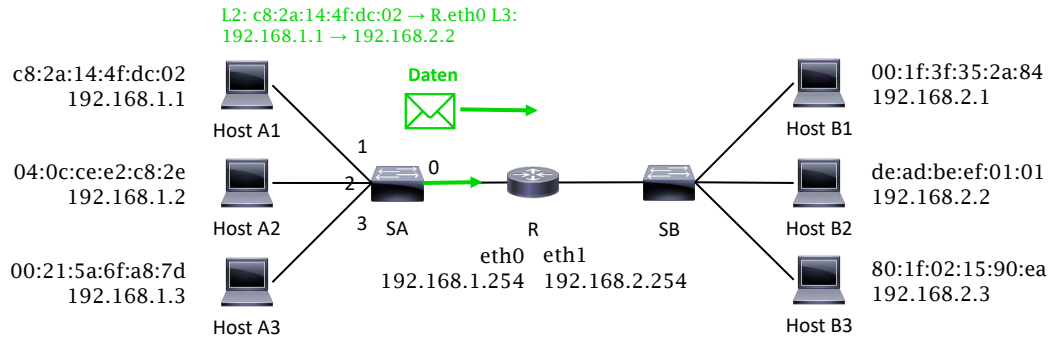
- Jeder Host sollte einen Router zum Internet, das sog. Default Gateway, kennen, an das er alle Pakete schickt, deren Zieladressen nicht im eigenen Netz liegen, und für die in seiner Routing-Tabelle nicht ein spezifisches Gateway eingetragen ist.
- Ob eine Zieladresse zum eigenen Netz gehört erkennt ein Host durch Vergleich der Zieladdresse mit der eigenen Netzadresse.
- Im Moment gehen wir noch davon aus, dass die ersten 3 Oktette einer IP-Adresse das Netz identifizieren
- ⇒ 192.168.1.1 und 192.168.2.2 liegen in unterschiedlichen Netzen.

Beispielnetz, basierend auf aktuellen Ethernet-Standard



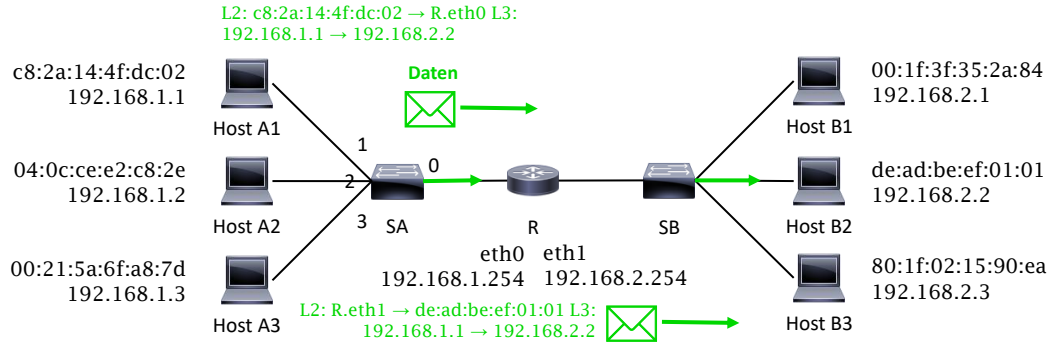
1. Host A1 erkennt, dass 192.168.2.2 nicht im eigenen Netz liegt. Sein Default-Gateway ist 192.168.1.254.
2. Host A1 löst die MAC-Adresse zu 192.168.1.254 auf.

Beispielnetz, basierend auf aktuellen Ethernet-Standard



1. Host A1 erkennt, dass 192.168.2.2 nicht im eigenen Netz liegt. Sein Default-Gateway ist 192.168.1.254.
2. Host A1 löst die MAC-Adresse zu 192.168.1.254 auf.
3. Host A1 sendet das Datenpaket an R: Dabei adressiert er R mittels der eben bestimmten MAC-Adresse (Schicht 2). Als Ziel-IP- Adresse (Schicht 3) verwendet er die IP-Adresse von Host B2.

Beispielnetz, basierend auf aktuellen Ethernet-Standard



1. Host A1 erkennt, dass 192.168.2.2 nicht im eigenen Netz liegt. Sein Default-Gateway ist 192.168.1.254.
2. Host A1 löst die MAC-Adresse zu 192.168.1.254 auf.
3. Host A1 sendet das Datenpaket an R: Dabei adressiert er R mittels der eben bestimmten MAC-Adresse (Schicht 2). Als Ziel-IP- Adresse (Schicht 3) verwendet er die IP-Adresse von Host B2.
4. R akzeptiert das Paket, bestimmt das ausgehende Interface und leitet das Paket weiter an Host B2. Dabei adressiert R wiederum Host B2 anhand seiner MAC-Adresse (erfordert ggf. einen weiteren ARP-Schritt).

Anmerkungen

WICHTIG:

- **MAC-Adressen dienen zur Adressierung innerhalb eines (Direktverbindungs-)Netzes und werden beim Forwarding durch einen Router verändert.**
- **IP-Adressen dienen der End-zu-End-Adressierung zwischen mehreren (Direktverbindungs-)Netzen und werden beim Forwarding durch einen Router nicht verändert.**

Anmerkungen

- Das Ergebnis einer Adressauflösung wird i. d. R. im ARP-Cache eines Hosts zwischengespeichert, um nicht bei jedem zu versenden- den Paket erneut eine Adressauflösung durchführen zu müssen.
- Die Einträge im ARP-Cache altern und werden nach einer vom Betriebssystem festgelegten Zeit invalidiert (z.B. 5 – 10 Minuten).
- Den Inhalt des ARP-Caches kann man sich unter Linux, OS X und Windows mittels des Befehls `arp -a` anzeigen lassen.
- ARP-Replies können auch als MAC-Broadcast verschickt werden, so dass alle Hosts innerhalb einer Broadcast-Domain den Reply erhalten. Abhängig vom Betriebssystem werden derartige „unaufgeforderten ARP-Replies“ (engl. unsolicited ARP replies) häufig ebenfalls im ARP-Cache gespeichert.

Was würde passieren, wenn . . .

zwei Hosts innerhalb derselben Broadcast-Domain identische MAC-Adressen aber unterschiedliche IP-Adressen haben?

ein Host absichtlich auf ARP-Requests antwortet, die nicht an ihn gerichtet waren?

05

ICMP

106

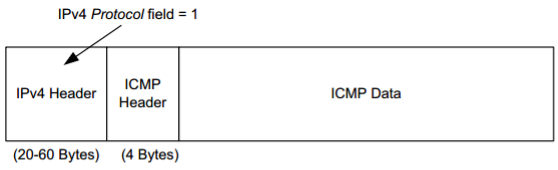
Internet Control Message Protocol (ICMP)

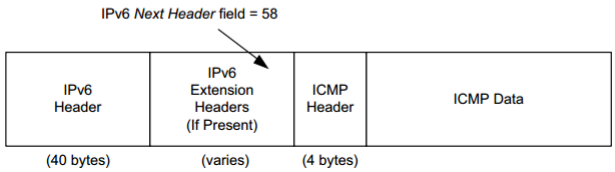
Das IP-Protokoll unterstützt
Dabei kann es zu Fehlern ko

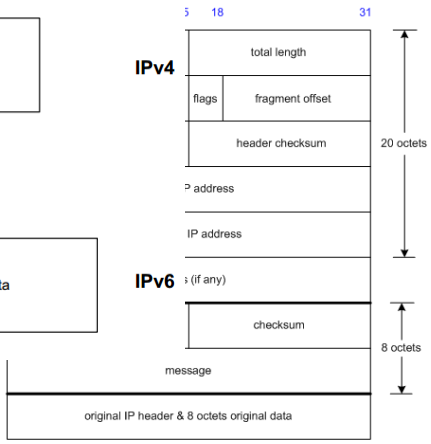
- ein Paket gerät in eine F
- ein Router kennt keinen
- der letzte Router zum Z
  nicht auflösen . . .

Das Internet Control Messa

- in derartigen Fällen den
  benachrichtigen und
- stellt zusätzlich Möglich
  - die Erreichbarkeit von Hosts zu prüfen („Ping“) oder
  - Pakete umzuleiten (Redirect).







[Quelle: https://homepages.uc.edu/~thomam/Net1/Packet_Formats/icmp.html - letzter Abruf 21.08.2025]

107

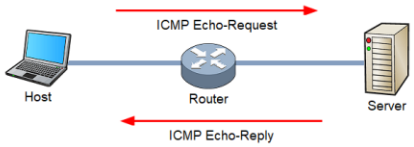
NETZWERKTECHNIK / SEMESTER 1 und 2

„Ping“ von Host 1 nach Host 2

- Host 1 wählt einen zufälligen Identifier (16 bit), die Sequenznummer wird für jeden gesendeten Echo-Request um eins inkrementiert.
- Der **Echo Request (Type 0x08)** wird von Routern wie jedes IP-Paket weitergeleitet.
- Erhält Host 2 den Echo Request, so antwortet er mit einem **Echo Reply (Type 0x00)**. Dabei werden Identifier, Sequenznummer und Daten aus dem Request kopiert und zurückgeschickt.
- Sollte die Weiterleitung zu Host 2 fehlschlagen, so wird eine ICMP-Nachricht mit dem entsprechenden Fehlercode an Host 1 zurückgeschickt.
- Wozu dient der Identifier?

IPv4 Datagram

	Bits 0–7	Bits 8–15	Bits 16–23	Bits 24–31
Header (20 bytes)	Version/IHL	Type of service	Length	
	Identification		*flags* and *offset*	
	Time To Live (TTL)	Protocol	Header Checksum	
	Source IP address			
	Destination IP address			
ICMP Header (8 bytes)	Type of message	Code	Checksum	
	Header Data			
ICMP Payload (*optional*)	Payload Data			



[Quelle: https://gursimarsm.medium.com/customizing-icmp-payload-in-ping-command-7c4486f4a1be - letzter Abruf 21.08.2025]

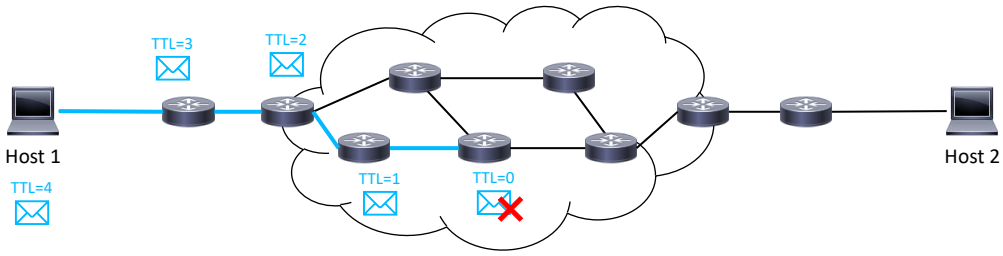
NETZWERKTECHNIK / SEMESTER 1 und 2

ICMP Time Exceeded

- **Der IP-Header besitzt ein TTL-Feld, welches bei der Weiterleitung eines Pakets durch den jeweiligen Router um 1 dekrementiert wird.**
- Erreicht es den Wert 0, so wird das betreffende Paket verworfen.

IPv4 Datagram

	Bits 0–7	Bits 8–15	Bits 16–23	Bits 24–31
Header (20 bytes)	Version/IHL	Type of service	Length	
	Identification		*flags* and *offset*	
	Time To Live (TTL)	Protocol	Header Checksum	
	Source IP address			
	Destination IP address			
ICMP Header (8 bytes)	Type of message	Code	Checksum	
	Header Data			
ICMP Payload (*optional*)	Payload Data			



[Quelle: http://www.tcpipguide.com/free/t_ICMPv4EchoRequestandEchoReplyMessages-2.htm - letzter Abruf 21.08.2025]

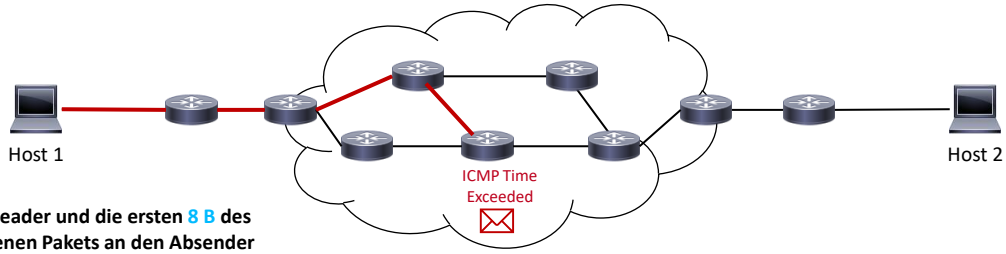
ICMP Time Exceeded

- Der IP-Header besitzt ein TTL-Feld, welches bei der Weiterleitung eines Pakets durch den jeweiligen Router um 1 dekrementiert wird.
- Erreicht es den Wert 0, so wird das betreffende Paket verworfen.

IPv4 Datagram

	Bits 0–7	Bits 8–15	Bits 16–23	Bits 24–31
Header (20 bytes)	Version/IHL	Type of service	Length	
	Identification		*flags* and *offset*	
	Time To Live (TTL)	Protocol	Header Checksum	
	Source IP address			
	Destination IP address			
ICMP Header (8 bytes)	Type of message	Code	Checksum	
	Header Data			
ICMP Payload (*optional*)	Payload Data			

- **Der Router generiert ein ICMP Time Exceeded und schickt es an den Absender des verworfenen Pakets zurück.**



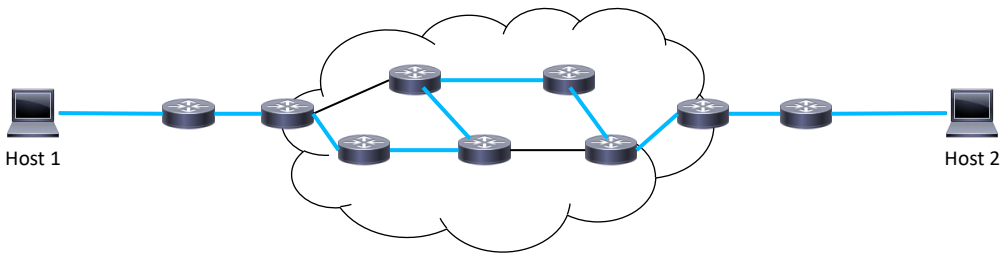
- **Da der Header und die ersten 8 B des verworfenen Pakets an den Absender zurückgeschickt werden, kann dieser genau bestimmen, welches Paket verworfen wurde.**

[Quelle: http://www.tcpipguide.com/free/t_ICMPv4EchoRequestandEchoReplyMessages-2.htm - letzter Abruf 21.08.2025]

110

Traceroute mit ICMP

- Obwohl Pakete zwischen Host 1 und Host 2 (in Hin- und Rückrichtung) jeweils unterschiedliche Wege nehmen können, werden in der Praxis meist nur einer oder sehr wenige genutzt.
- **Welchen Pfad nehmen Pakete von Host 1 nach Host 2?**



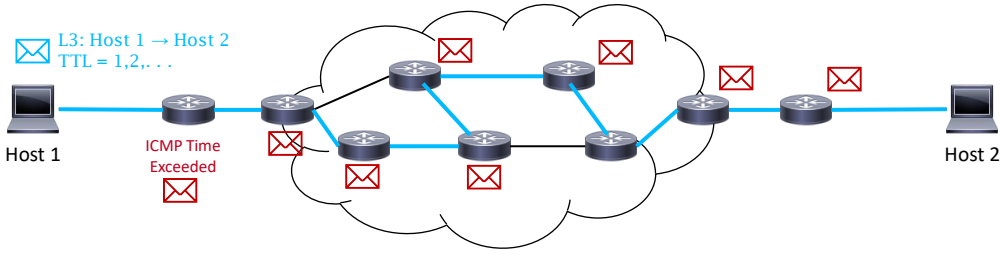
111

Traceroute mit ICMP

Host 1 sendet z. B. ICMP Echo Requests an Host 2

- wobei das TTL-Feld zu Beginn auf 1 gesetzt wird und
- danach schrittweise um jeweils 1 erhöht wird.

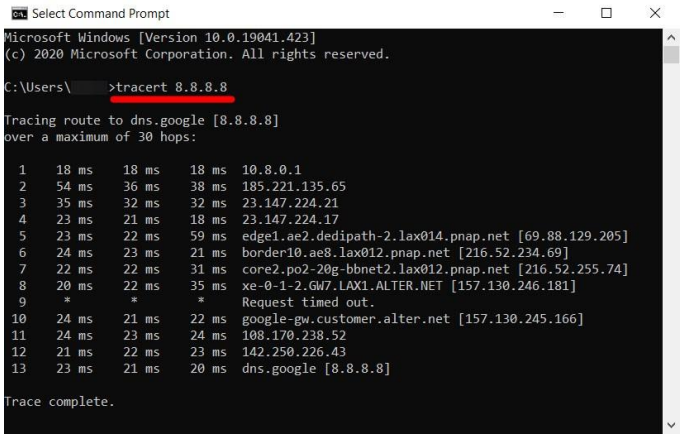
⇒ Router entlang des Pfads von Host 1 nach Host 2 werden schrittweise die Pakete verwerfen und jeweils ein TTLExceeded an Host 1 zurücksenden. Anhand der IP-Quelladresse dieser Fehlernachrichten kann Host 1 den Pfad hin zu Host 2 nachvollziehen.



Traceroute mit ICMP

Probleme

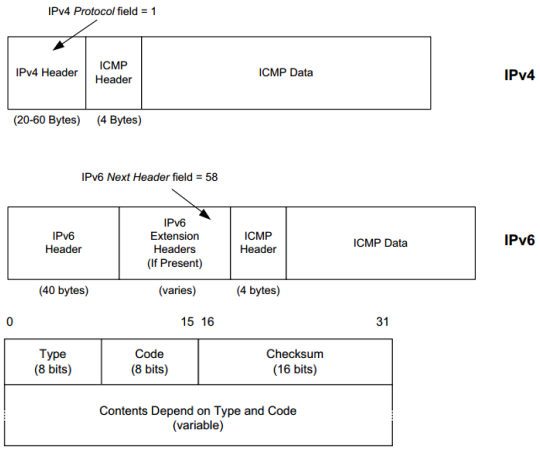
- Ein Router hat mehrere IP-Adressen. Welche wählt er als Absender-Adresse für die Fehlerbenachrichtigungen? Wählt er immer dieselbe Adresse?
- Was ist, wenn es tatsächlich mehrere gleichzeitig genutzte Pfade oder Pfadabschnitte gibt?
- Müssen Router überhaupt Fehlerbenachrichtigungen versenden?
- Angenommen der Pfad von A → B ist symmetrisch. Warum werden sich die Ausgaben von Traceroute dennoch unterscheiden?



[Quelle: https://www.hellotech.com/guide/for/how-to-run-a-traceroute-windows-10?srsltid=AfmBOoqcfXQUdrVgUQMyB_lxkoLFwkq6YY34X75SLL-nAeVrPdKmtcTu - letzter Abruf 21.08.2025]

Internet Control Message Protocol v6 (ICMPv6)

- ICMPv6 spielt eine weitaus wichtigere Rolle beim Betrieb von IPv6 als ICMPv4 für IPv4.
- In IPv6 wird ICMPv6 für verschiedene Zwecke verwendet, die über die einfache Fehlerberichterstattung und Signalisierung hinausgehen.
- Es wird verwendet für:
  - **Neighbor Discovery (ND)**, das die gleiche Rolle spielt wie ARP für IPv4.
  - Die **Router-Discovery-Funktion** wird für die Konfiguration von Hosts und die Verwaltung von Multicast-Adressen verwendet.
  - Verwaltung von **Übergaben in Mobile IPv6**.



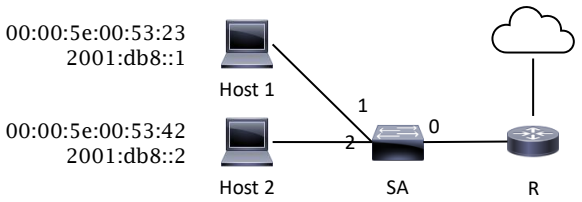
[Quelle: https://notes.shichao.io/tcpv1/ch8/ - letzter Abruf 21.08.2025]

Neighbor Discovery Protocol (NDP)

- IPv6 bietet mit seiner Neighbor Discovery, welche Bestandteil von ICMPv6 ist, eine Reihe von Funktionalitäten, für die bei IPv4 nicht oder nur unvollständig standardisiert sind und eigene Protokolle notwendig gemacht haben.
- **Funktionen der Neighbor Discovery sind insbesondere:**
  - Adressauflösung, Duplicate Address Detection und Neighbor Unreachability Detection: Neighbor Solicitations und Advertisements.
  - Automatisches Auffinden von Routern innerhalb des lokalen Netzsegments, Adress-Präfixen und Parameter Konfiguration: Router Discovery und Router Advertisements.
  - Umleitung zu anderen Gateways: Redirects.

Beispiel: Adressauflösung bei IPv6

- Host1 will eine Nachricht an Host2 senden
- Die IP-Adresse von Host2 (2001:db8::2) sei ihm bereits bekannt
- Wie erhält Host1 die zugehörige MAC-Adresse?



[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), Prof. Dr.-Ing. Georg Carle, TUM, 2025]

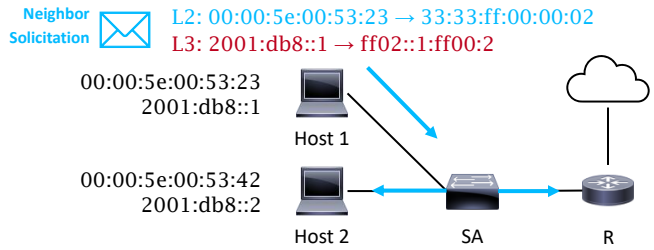
Neighbor Solicitation (Request)

Type = 135 (10)	Code = 0	Checksum
Reserved (set to zero)		
Target Address (2001:db8::2)		
Type = 1	Length = 1	Source Link Address
00:00:5e:00:53:23		
Additional Options		

- **ICMPv6 Header** - ICMPv6 **Type und Code (0x87 und 0x00)** für eine Neighbor Solicitation Nachricht) sowie die ICMPv6 Checksumme.
- **Neighbor Discovery Body**
  - Die ersten 32 bit sind reserviert, so dass die Nachricht insgesamt wieder ein Vielfaches von 8 B lang wird.
  - Im Anschluss folgt die Ziel-IPv6-Adresse, zu der die entsprechende MAC-Adresse gesucht wird.
- **Neighbor Discovery Options**
  - Neighbor Discovery Pakete können selbst wiederum Optionen enthalten.
  - Type und Length geben den Typ (1 für Source Link Layer Address) und Gesamtlänge der Option in Vielfachen von 8 B an.
  - Im Fall eines Neighbor Solicitation Pakets folgt L2-Adresse des anfragenden Knotens (Source Link Address).

tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), Prof. Dr.-Ing. Georg Carle, TUM, 2025]

Neighbor Discovery Protocol (NDP)



Beispiel

- Host 1 sendet eine „Neighbor Solicitation for 2001:db8::2 from 00:00:5e:00:53:23“ an die zur bekannten IPv6 Adresse gehörende Solicited-Node Adresse (Multicast).

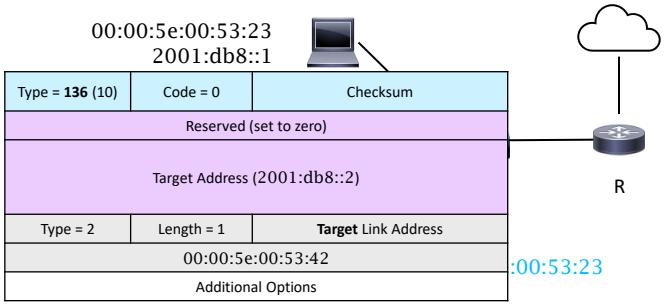
Type = **135** (10)	Code = 0	Checksum
Reserved		
Target Address (2001:db8::2)		
Type = 1	Length = 1	**Source** Link Address
00:00:5e:00:53:23		
Additional Options		

tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), Prof. Dr.-Ing. Georg Carle, TUM, 2025]

Neighbor Discovery Protocol (NDP)

Beispiel

- Host 2 empfängt diese Nachricht und antwortet mit einer „Neighbor Advertisement 2001:db8::2 (sol, ovr) is at 00:00:5e:00:53:42“ Nachricht (Unicast).



Type = **136** (10)	Code = 0	Checksum
Reserved (set to zero)		
Target Address (2001:db8::2)		
Type = 2	Length = 1	**Target** Link Address
00:00:5e:00:53:42		
Additional Options		

Type = **135** (10)	Code = 0	Checksum
Reserved (set to zero)		
Target Address (2001:db8::2)		
Type = 1	Length = 1	**Source** Link Address
00:00:5e:00:53:23		
Additional Options		

Type = **136** (10)	Code = 0	Checksum
R S O	Reserved (set to zero)	
Target Address (2001:db8::2)		
Type = 2	Length = 1	**Target** Link Address
00:00:5e:00:53:42		
Additional Options		

Neighbor Advertisement (Reply)

Type = 136 (10)	Code = 0	Checksum
R S O	Reserved (set to zero)	
Target Address (2001:db8::2)		
Type = 2	Length = 1	Target Link Address
00:00:5e:00:53:42		
Additional Options		

- **ICMPv6 Header** - ICMPv6 **Type und Code (0x88 und 0x00)** für eine Neighbor Advertisement Nachricht) sowie die ICMPv6 Checksumme.
- **Neighbor Discovery Body**
  - **Router-Flag R** wird gesetzt, wenn der antwortende Knoten ein Router ist.
  - **Solicited Flag S** gibt an, ob das Advertisement infolge einer Solicitation geschickt wird.
  - **Override Flag O** wird gesetzt, wenn das Advertisement eine möglicherweise gecached Link-Layer Adresse beim Empfänger aktualisieren soll.
- **Neighbor Discovery Options**
  - Type und Length geben den Typ (2 für Target Link Layer Address) und Gesamtlänge der Option in Vielfachen von 8 B an.
  - Im Fall eines Neighbor Advertisements folgt die L2-Adresse des angefragten Knotens (Target Link Address).

06

DHCP

121

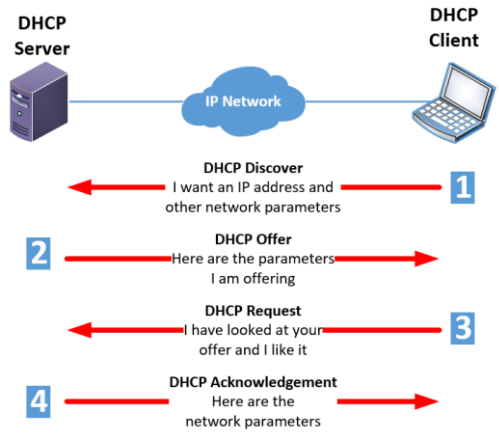
Dynamic Host Configuration Protocol (DHCP)

Woher bekommen Hosts eigentlich ihre IP-Adresse?

- Statische Konfiguration von Hand
- Dynamisch von einem DHCP-Server zugewiesene IP-Adresse

Ablauf:

1. Client sendet DHCP-Discover (Layer 2 Broadcast)
2. DHCP-Server antwortet mit DHCP-Offer, wodurch er dem Cli- ent eine IP-Adresse anbietet
3. Client antwortet mit DHCP-Request, wodurch er die angebote- ne Adresse anfordert
4. DHCP-Server antwortet mit DHCP-ACK, wodurch er die angeforderte Adresse zur Nutzung freigibt, oder mit DHCP-NACK, wodurch er die Nutzung der Adresse untersagt



tgm [Quelle: https://info.teledynamics.com/blog/dhcp-options-for-voip-and-uc-systems - letzter Abruf 21.08.2025]

122

Anmerkungen

- Die vom DHCP-Server zugewiesene Adresse wird auch als Lease bezeichnet und ist in ihrer Gültigkeit zeitlich begrenzt
- Clients erneuern ihr Lease in regelmäßigen Abständen beim DHCP-Server.
- Gerade in kleineren (privaten) Netzwerken übernimmt häufig ein Router die Rolle des DHCP-Servers.
- Zusammen mit der IP-Adresse und Subnetzmaske können DHCP-Server weitere Optionen ausliefern:
  - DNS-Resolver zur Namensauflösung (→ Kapitel 5)
  - Hostname und Domänen-Suffix (→ Kapitel 5)
  - Statische Routen, insbesondere einen Default-Gateway
  - Maximum Transmission Unit
  - NTP-Server zur Zeitsynchronisation
  - . . .
- Aus Redundanzgründen werden manchmal mehrere DHCP-Server pro Netzwerk verwendet, wobei
  - sich die Adressbereiche der beiden Server nicht überschneiden dürfen oder
  - zusätzliche Mechanismen zur Synchronisation der Adresspools notwendig sind.
- Ein versehentlich ins Netzwerk eingebrachter DHCP-Server (z. B. durch einen achtlos angeschlossenen Router oder Access Point) kann beträchtliche Auswirkungen auf das Netzwerk haben und ist häufig schwer zu finden.

tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), Prof. Dr.-Ing. Georg Carle, TUM, 2025]