Vermittlungsschicht

NETZWERKTECHNIK / SEMESTER 1 UND 2

1

AGENDA

01 VERMNITTLUNGSARTEN

02 VERMITTLUNGSSCHICHT

03 ADRESSAUFLÖSUNG

04 ICMP

05 DHCP

2

01

Vermittlungsarten

3

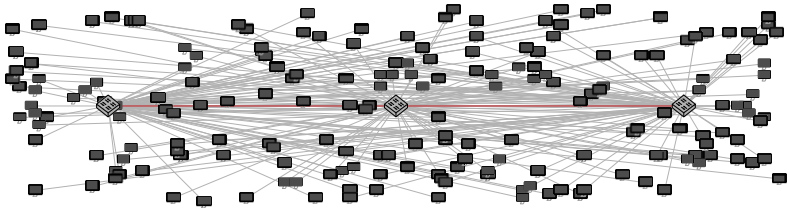
Eigenschaften von IP

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



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

4

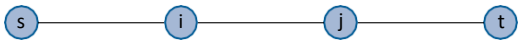
NETZWERKTECHNIK / SEMESTER 1 und 2

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.

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

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.

[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)

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

NETZWERKTECHNIK / SEMESTER 1 und 2

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

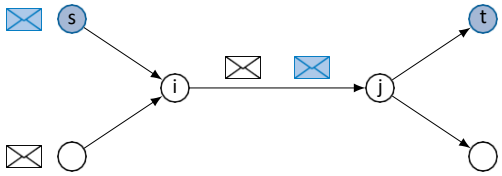
- Absender verpackt Ware und versieht das Paket mit Adressinformationen (Header)
- Die Adressen identifizieren Absender und Empfänger weltweit eindeutig und haben eine logische Struktur, die eine effiziente Zuordnung im Transportnetz der Post erlaubt

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

NETZWERKTECHNIK / SEMESTER 1 und 2

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

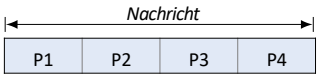
tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), Prof. Dr.-Ing. Georg Carle, TUM, 2025]

NETZWERKTECHNIK / SEMESTER 1 und 2

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]

NETZWERKTECHNIK / SEMESTER 1 und 2

Multiplexing auf Paketebene

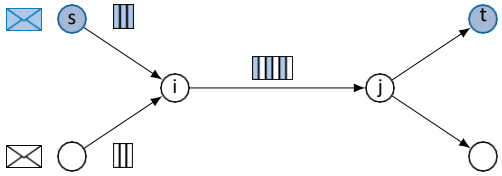
- Durch die Vermittlung kleiner Pakete statt langer Nachrichten werden Engpässe fairer genutzt
- Gehen Pakete verloren, müssen nur Teile einer größeren Nachricht wiederholt werden

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]

11

NETZWERKTECHNIK / SEMESTER 1 und 2

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]

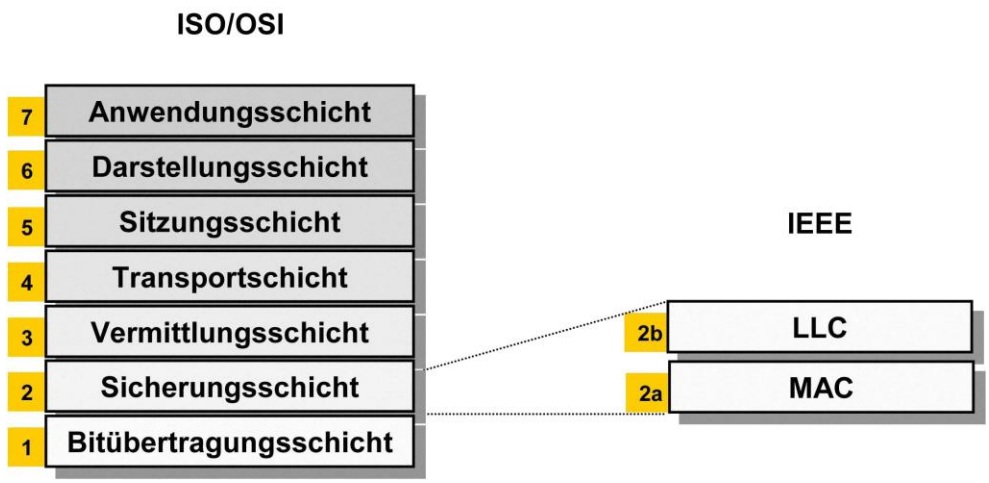
12

02

Vermittlungsschicht

13

Einordnung im ISO/OSI Modell



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

14

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

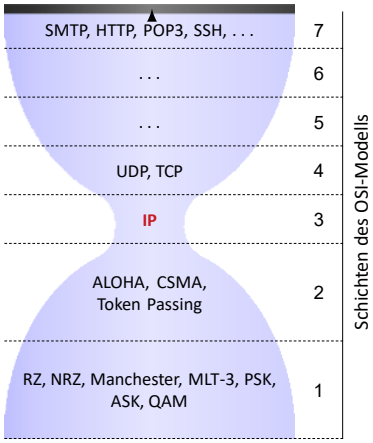
- Global eindeutigen und strukturierten / logischen Adressierung sowie
- Verfahren zur Bestimmung von (möglichst) optimalen Pfaden.

Wir beschränken uns auf die Betrachtung von

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

Alternative Protokolle der Netzwerkschicht:

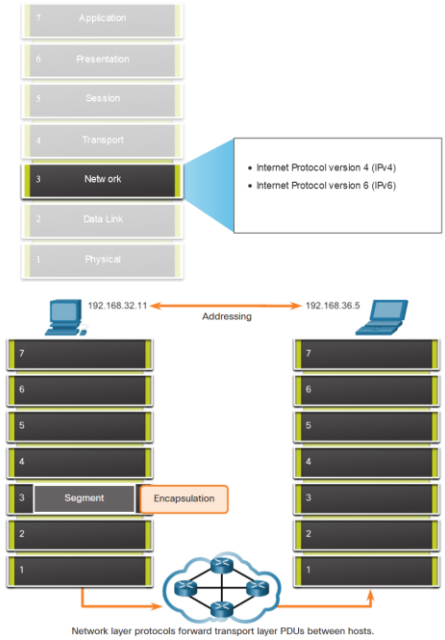
IPX (Internetwork Packet Exchange, 1990), DECnet Phase 5 (1987), AppleTalk (1983)



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

Die Vermittlungsschicht

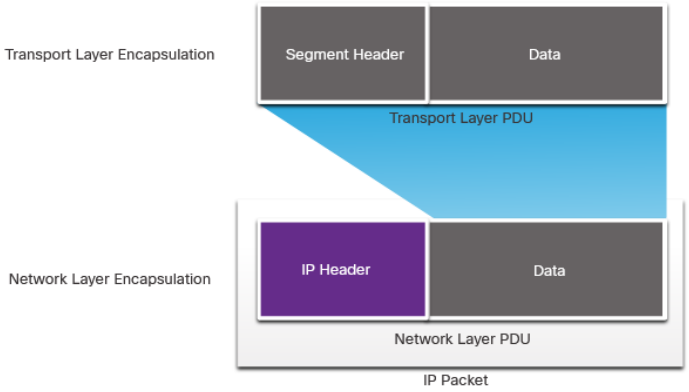
- Stellt Dienste bereit, mit denen Endgeräte Daten austauschen können
- **IP Version 4 (IPv4) und IP Version 6 (IPv6)** sind die wichtigsten Kommunikationsprotokolle auf Netzwerkebene.
- Die Netzwerkschicht führt **vier grundlegende Vorgänge** aus:
  - Adressierung von Endgeräten
  - Encapsulation
 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



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

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).

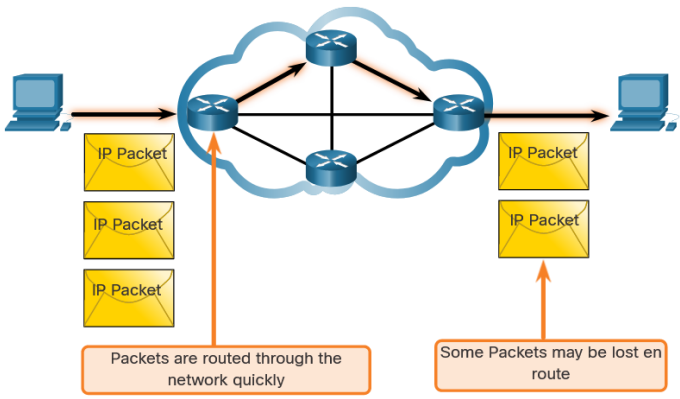
[Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

19

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]

20

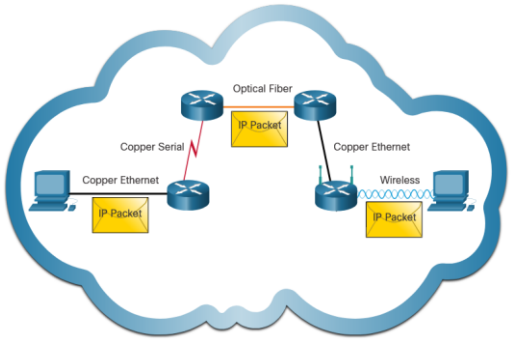
Medienunabhängig

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.**

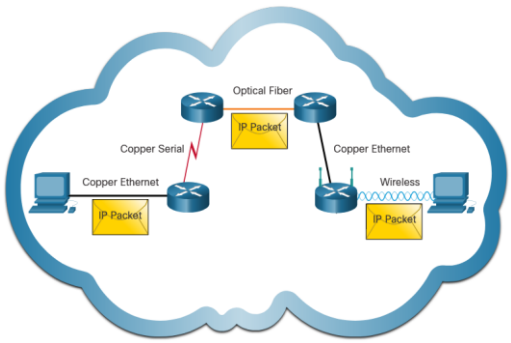


Medienunabhängig

- 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



NETZWERKTECHNIK / SEMESTER 1 und 2

IPv4-Paket-Header

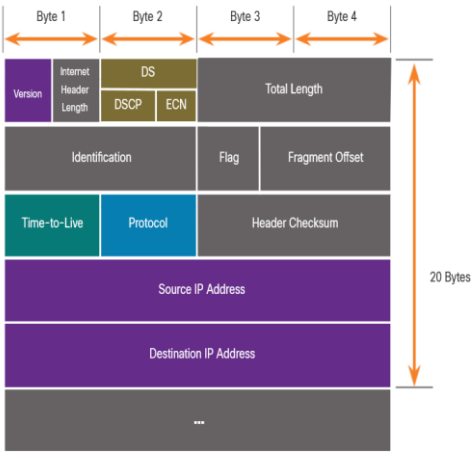
- IPv4 ist das **primäre Kommunikationsprotokoll** für die Netzwerkschicht.
- Der **Netzwerkheader** hat viele Zwecke:
  - Es stellt sicher, dass das Paket in **die richtige Richtung** (an das Ziel) gesendet wird.
  - Er enthält Informationen in **unterschiedlichen Feldern für die Verarbeitung** innerhalb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

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.



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.

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.

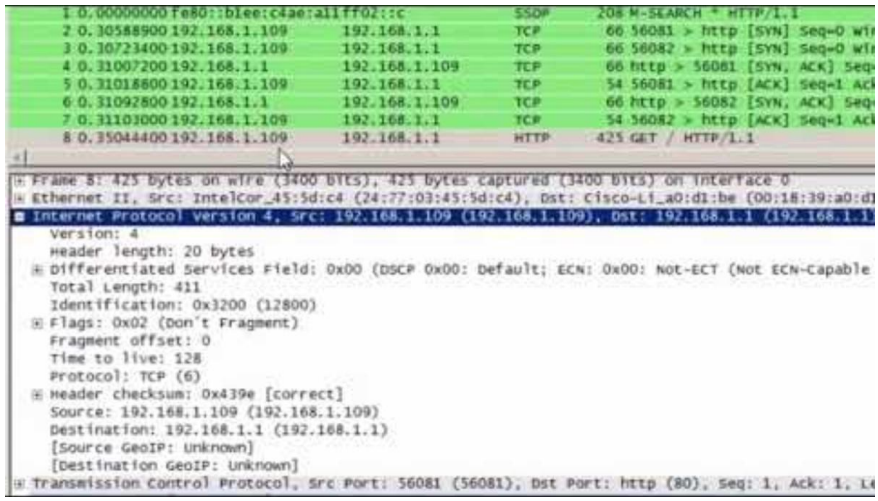
Felder des IPv4-Paket-Header

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.

Felder des IPv4-Paket-Header

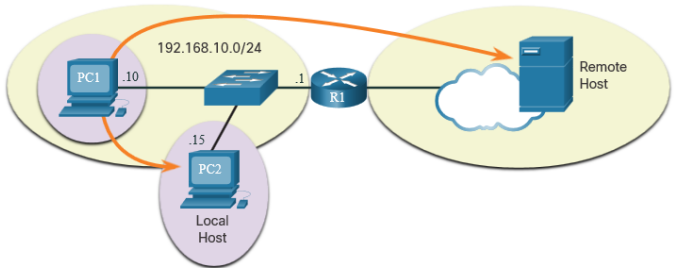
Function	Description
Source IPv4 Address	32-Bit-Quelladresse
Destination IPV4 Address	32 Bit Zieladresse
Options / Padding	▪ IP unterstützt eine Reihe von Optionen (z. B. Route Recording, Zeitstempel, . . .), welche als optionale Felder an den IP-Header angefügt werden können. ▪ Nicht alle diese Optionen 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.

Video – Beispiel-IPv4-Header in Wireshark



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

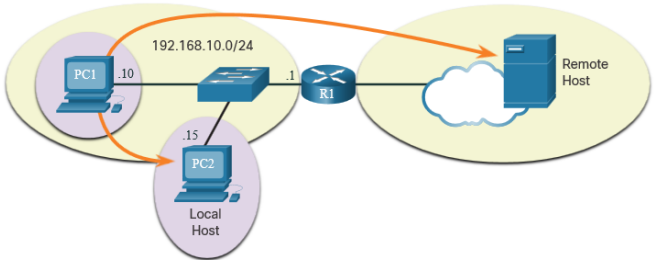


Entscheidung über die Weiterleitung

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.

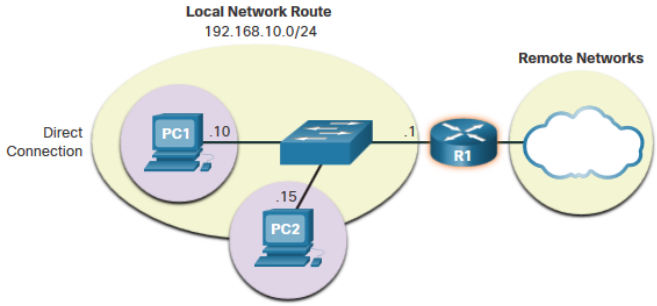


Default Gateway

- 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
```

NETZWERKTECHNIK / SEMESTER 1 und 2

Übung – Routing-Tabelle des eigenen Rechners untersuchen

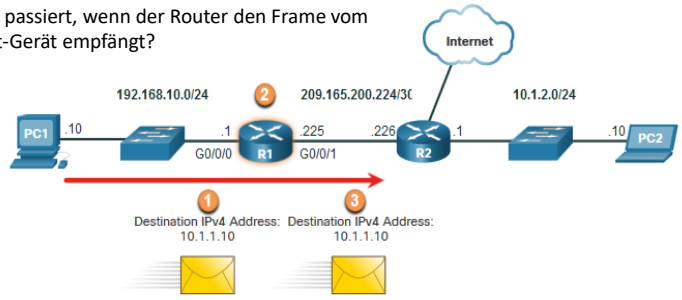
- Führe den passenden Befehl aus, um die Routing-Tabelle deines Systems zu sehen: `route print` (oder `netstat -r`)
- **Teil 1:** Was bedeutet die Route mit Ziel 0.0.0.0 bzw. default?
- **Teil 2:** Welche Route wird für dein Heimnetz verwendet (z. B. 192.168.x.x)?
- **Teil 3:** Was ist das „Gateway“ in deiner Tabelle?
- **Teil 4:** Gibt es Einträge für IPv6? Wie sehen sie aus?
- **Teil 5:** Visualisiere dein Heimnetzwerk (dein Rechner, Router, Internet, andere Geräte) und zeige wie Datenpakete laut Routing Tabelle weitergeleitet werden

35

NETZWERKTECHNIK / SEMESTER 1 und 2

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.

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

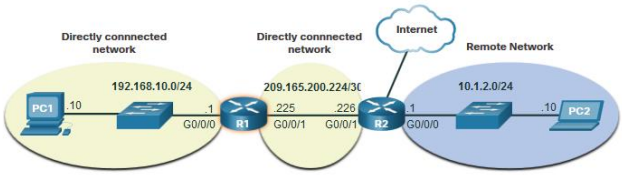
36

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.



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

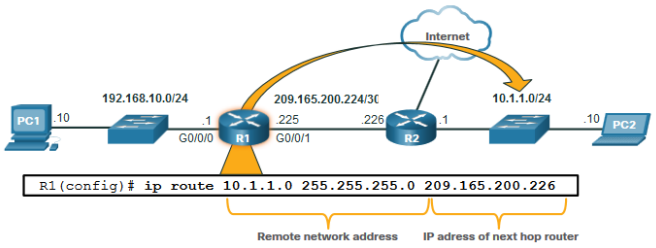
37

NETZWERKTECHNIK / SEMESTER 1 und 2

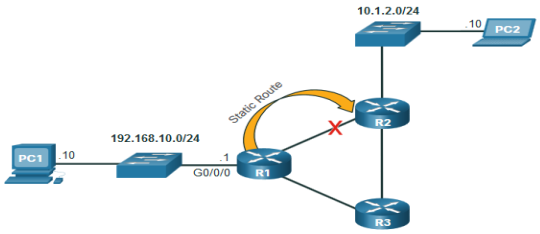
Statisches Routing

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.

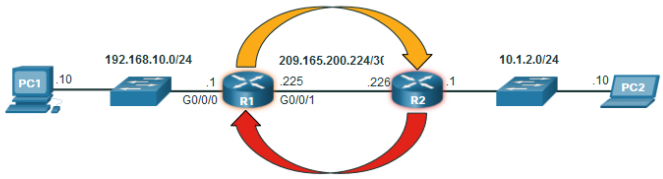
tgm [Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

38

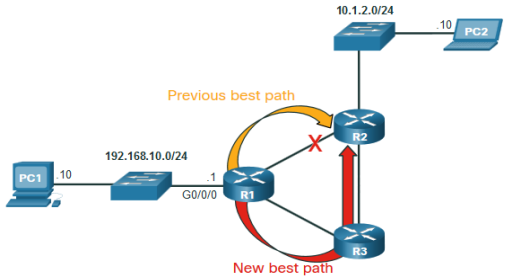
Dynamisches Routing

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.



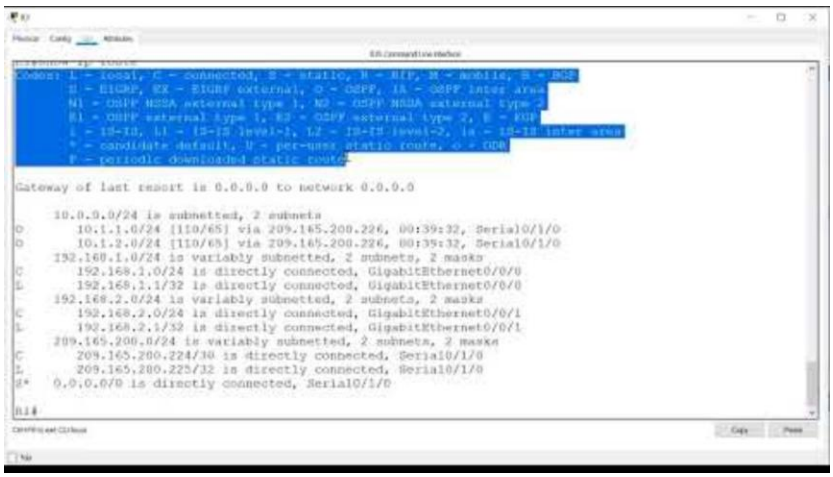
- R1 is using the routing protocol OSPF to let R2 know about the 192.168.10.0/24 network.
- R2 is using the routing protocol OSPF to let R1 know about the 10.1.1.0/24 network.



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



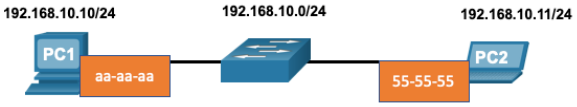
tgm [Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

03

Adressauflösung

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.**



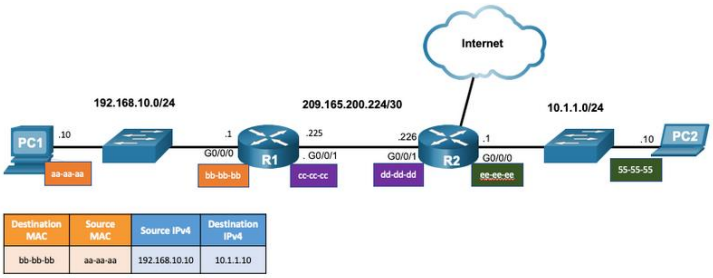
Destination MAC	Source MAC	Source IPv4	Destination IPv4
55-55-55	aa-aa-aa	192.168.10.10	192.168.10.11

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

NETZWERKTECHNIK / SEMESTER 1 und 2

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.



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

43

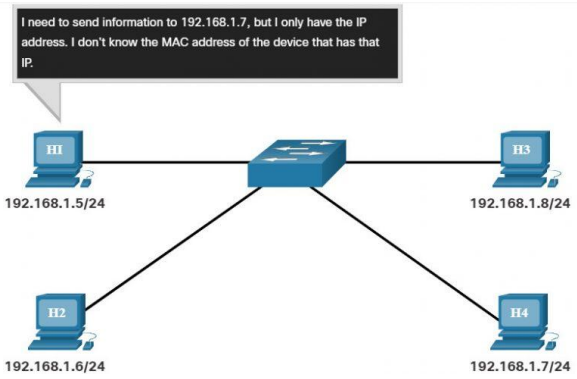
NETZWERKTECHNIK / SEMESTER 1 und 2

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



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

44

NETZWERKTECHNIK / SEMESTER 1 und 2

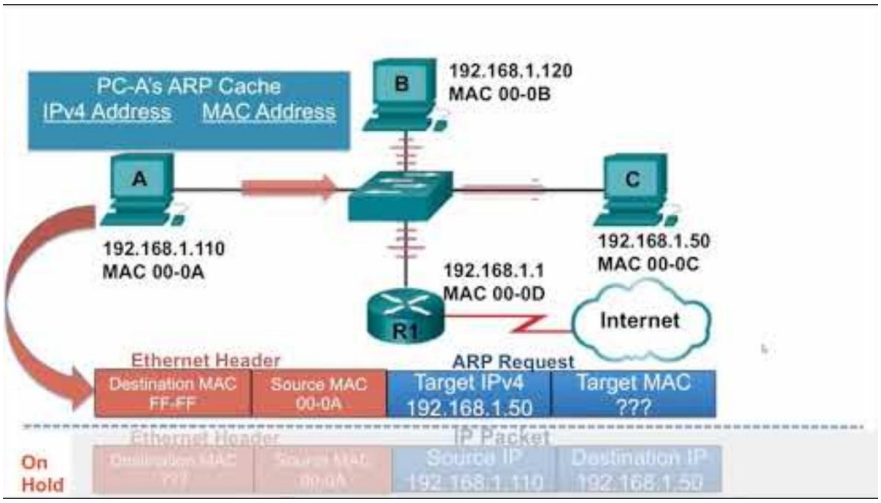
ARP Funktionen

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

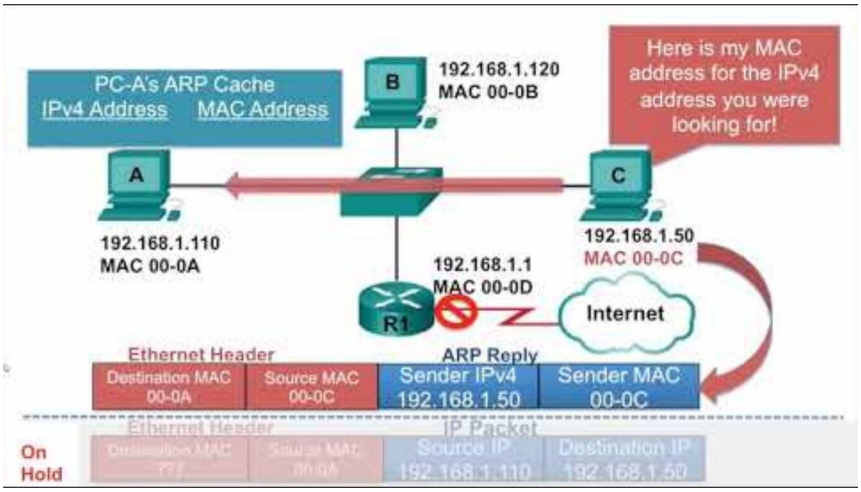
- Wenn sich die IPv4-Zieladresse des Pakets **im selben Netzwerk** befindet, durchsucht das Gerät die ARP-Tabelle nach der IPv4-Zieladresse.
- Wenn sich die IPv4-Zieladresse **in einem anderen Netzwerk** befindet, durchsucht das Gerät die ARP-Tabelle nach der IPv4-Adresse des Standardgateways.
- Wenn 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**.

NETZWERKTECHNIK / SEMESTER 1 und 2

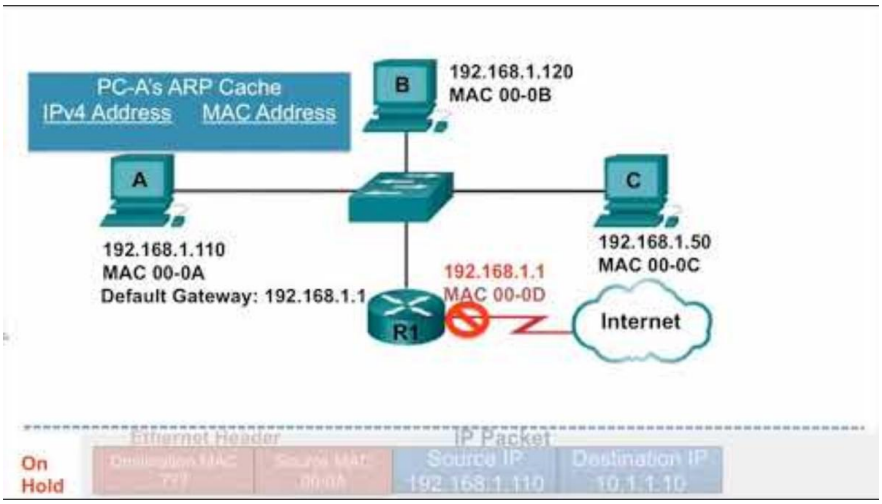
Video - ARP Request



Video – ARP Operation - ARP Reply

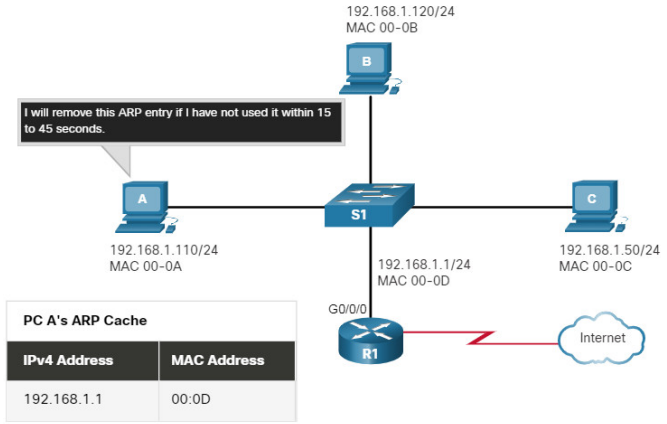


Video - ARP Role in Remote Communications



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]

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
```

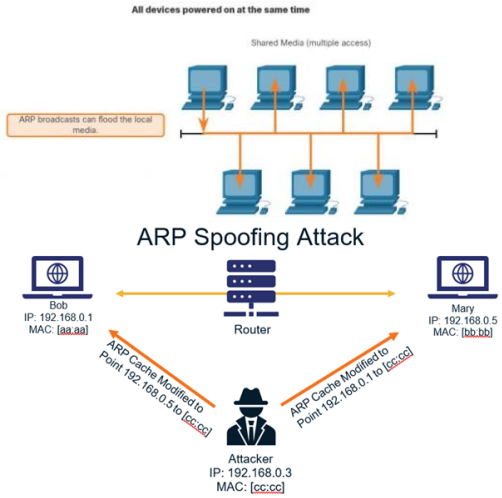
```
C:\Users\PC> arp -a

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
```

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

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.



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

04

ICMP

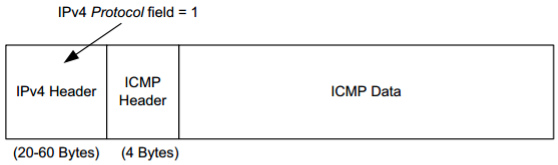
Internet Control Message Protocol (ICMP)

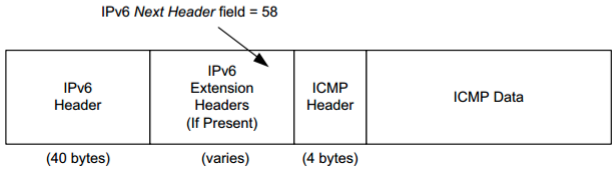
Das IP-Protokoll unterstützt
Dabei kann es zu Fehlern ko

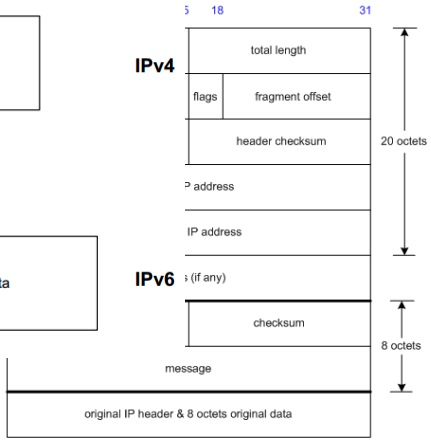
- ein Paket gerät in eine F
- ein Router kennt keinen
- der letzte Router zum Z nicht auflösen . . .

Das Internet Control Messa

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







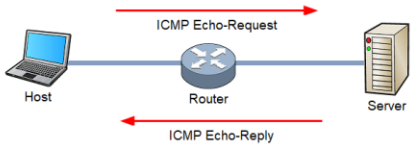
[Quelle: https://homepages.uc.edu/~thomam/Net1/Packet_Formats/icmp.html - letzter Abruf 21.08.2025]

„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]

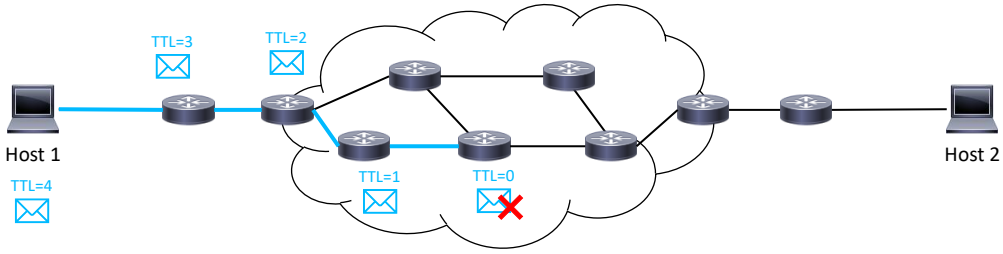
NETZWERKTECHNIK / SEMESTER 1 und 2

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]

55

NETZWERKTECHNIK / SEMESTER 1 und 2

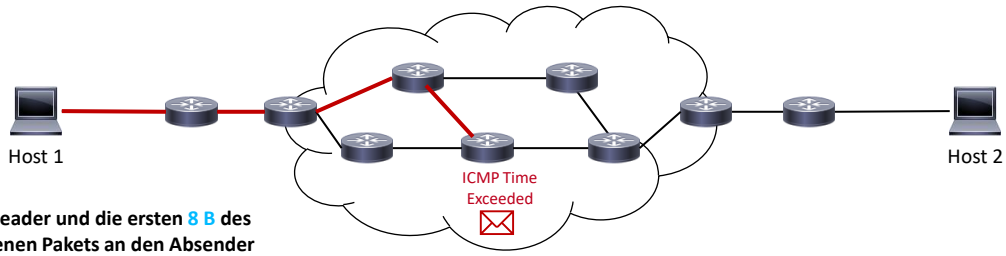
ICMP Time Exceeded

- 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			

- **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.**

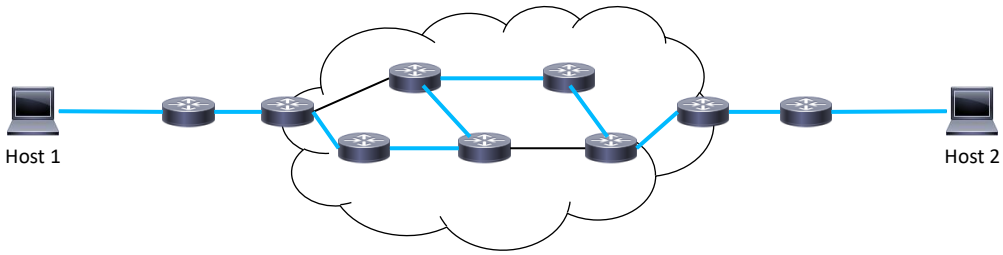
[Quelle: http://www.tcpipguide.com/free/t_ICMPv4EchoRequestandEchoReplyMessages-2.htm - letzter Abruf 21.08.2025]

56

NETZWERKTECHNIK / SEMESTER 1 und 2

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?**



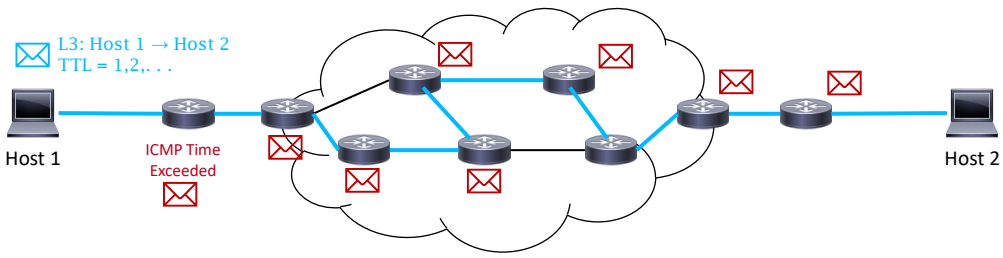
NETZWERKTECHNIK / SEMESTER 1 und 2

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.

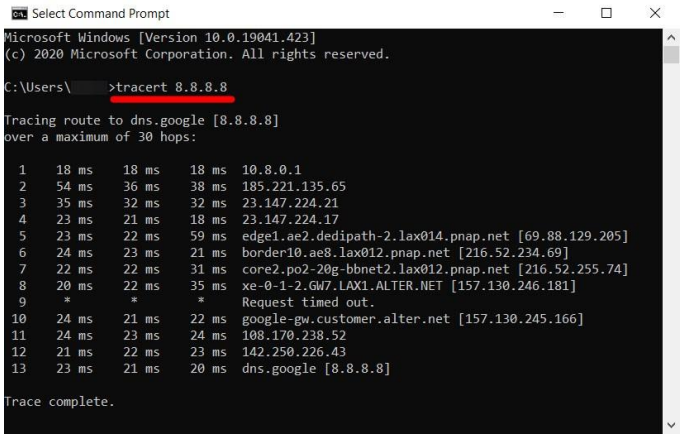
⇒ Router entlang des Pfads von Host 1 nach Host 2 werden schrittweise die Pakete verwerfen und jeweils ein TTLExceeded an Host 1 zurücksenden. Anhand der IP-Quelladresse dieser Fehlernachrichten kann Host 1 den Pfad hin zu Host 2 nachvollziehen.



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]

05

DHCP

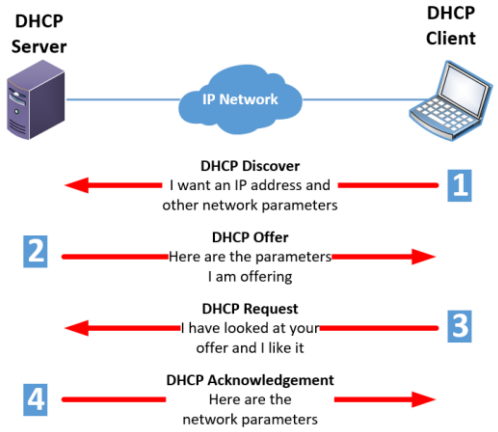
Dynamic Host Configuration Protocol (DHCP)

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 angebotene 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



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