Technische Grundlagen der Informatik

Vermittlungsschicht (Network Layer)

Prof. Dr. phil. nat. habil. J. Haase, Dr.-Ing. Falko Schönteich

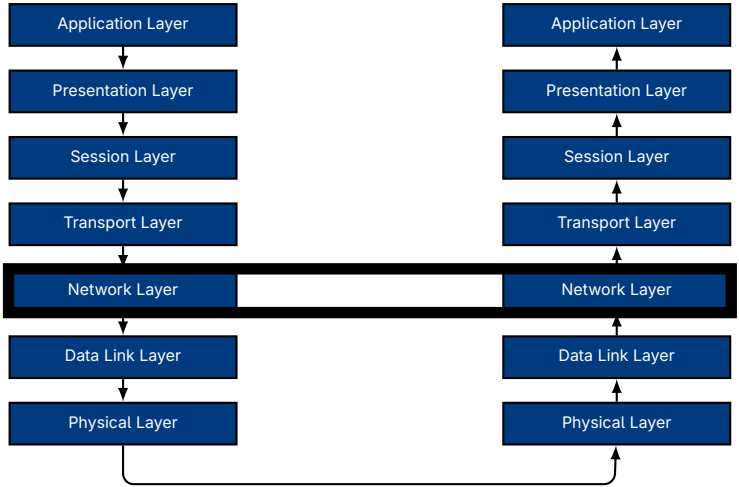
NORDAKADEMIE Hochschule der Wirtschaft

NORDAKADEMIE
HOCHSCHULE DER WIRTSCHAFT

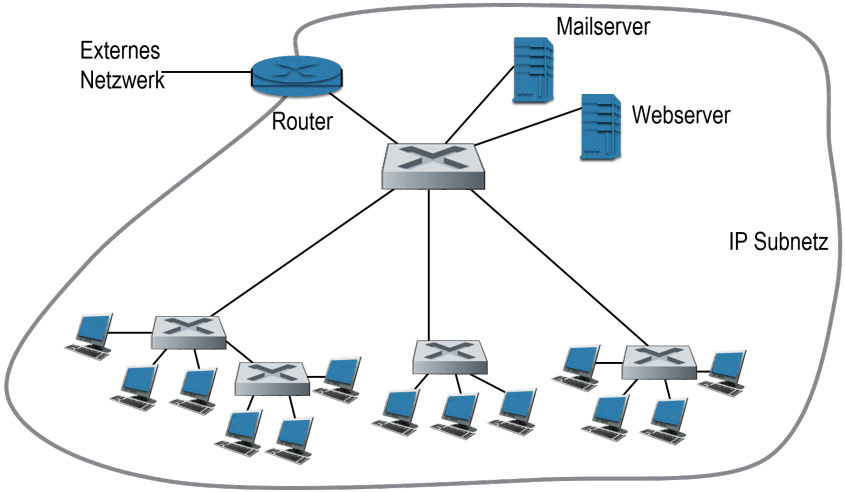
Überblick

1. Einleitung
2. IPv4
   - Datagramm-Aufbau
   - Router
   - Subnetze
3. ARP
4. Routing
5. ICMP
6. IP-Adressvergabe
7. IPv4 Übungen
8. IPv4 Probleme
9. IPv6
   - IPv6-Datagramm
   - IPv6-Adressierung

OSI-Referenzmodell



Netzwerk einer Institution

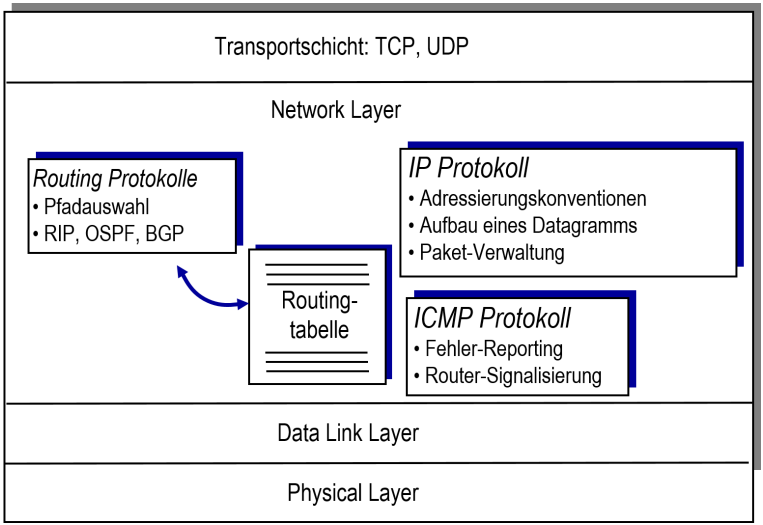


Aufgaben der Vermittlungsschicht?

Aufgaben der Vermittlungsschicht

- Adressierung über Netzwerkgrenzen und Technologien hinaus (globale Adressierung)
- Weiterleiten von Paketen in andere Netze (Routing)
- Signalisierung von Problemen

Aufgaben der Vermittlungsschicht



Internet Protokoll

- wichtigstes Protokoll der Vermittlungsschicht und der Grundpfeiler des Internets
- wurde in einer ersten Version 1974 von Vint Cerf und Bob Kahn vom IEEE entwickelt
- IP definiert unter anderem IP-Datagramme als Dateneinheit, die über das Netzwerk transportiert werden

Überblick

1. Einleitung
2. IPv4
   - Datagramm-Aufbau
   - Router
   - Subnetze
3. ARP
4. Routing
5. ICMP
6. IP-Adressvergabe
7. IPv4 Übungen
8. IPv4 Probleme
9. IPv6
   - IPv6-Datagramm
   - IPv6-Adressierung

Datagramm

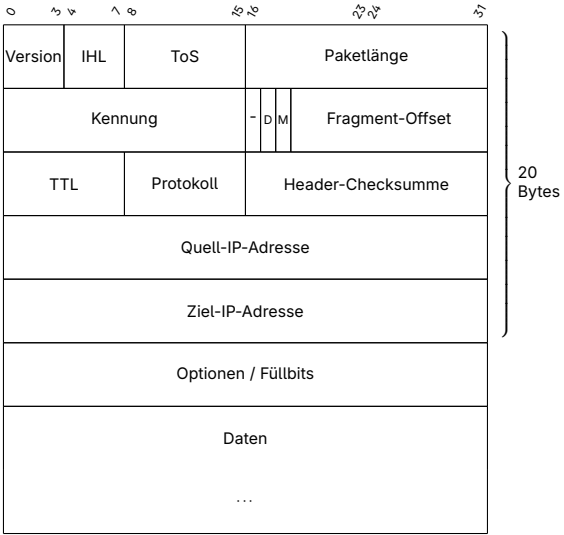
Definition

Datagramm Ein Datagramm ist eine in sich geschlossene, unabhängige Dateneinheit, die ohne weitere Verbindungssicherung zwischen zwei Endpunkten verschickt wird. Diese Dateneinheit enthält Informationen, die mittels eines Datagrammdienstes über ein Netzwerk transportiert werden sollen und Metainformationen, die zum Transport durch das Netzwerk erforderlich sind.

Das Internet Protokoll (IP) definiert den Aufbau von IP-Datagrammen.

Aufbau eines IP-Datagramms

- Version: 4 oder 6
- IHL: Headerlänge in 32-Bit Worten
- ToS: Priorität der Paketbehandlung
- Paketlänge in Bytes
- Flags: **D**o Not Fragment, **M**ore Fragments Follow
- Fragment-Offset in 8 Bytes vom Beginn des Datagramms
- TTL: Time To Live
- Protokoll spezifiziert nächsthöheres Protokoll (z. B. 6 für TCP, 17 für UDP)



IP-Header-Checksumme

- Viele Protokollschichten fügen Checksummen hinzu, auch IP
- IP-Header-Checksumme ist Einer-Komplement der Summe aller 16-Bit-Worte des IP-Headers
- Summe aller 16-Bit-Worte des Headers (mit Addition der Überlaufbits) inklusive Checksumme sollte 0xFFFF ergeben bzw. die Negation 0

Beispiel IP-Header-Checksumme

Ermittlung der Checksumme des folgenden Strings, der in ASCII kodiert sein soll:

`"TGdI ist toll!"`

String entspricht:

`0x5447 0x6449 0x2069 0x7374 0x2074 0x6F6C 0x6C21`

1. Checksumme bilden:
   `0x5447+0x6449+0x2069+0x7374+0x2074+0x6F6C+0x6C21`
   `=0x2486E`
2. Übertrag von 2 wieder auf 16-Bit-Anteil addieren:
   `0x486E + 0x2 = 0x4870`
3. Ergebnis logisch negieren: `0x4870 = 0xB78F`

Übung: Checksumme

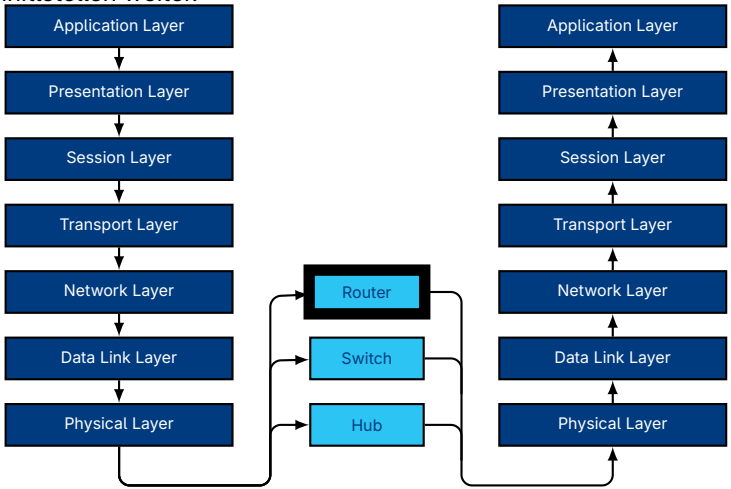
Nun wird die Checksumme an den String angehängt und versendet:

```
0x5447 0x6449 0x2069 0x7374 0x2074 0x6F6C 0x6C21 0xB78F
```

Überprüfen Sie die Korrektheit des Pakets!

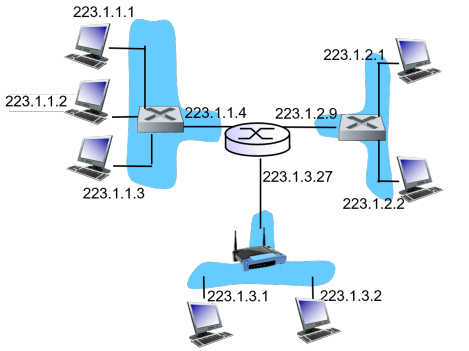
Router

Router haben mehrere Netzwerkschnittstellen (z. B. Ethernet und WLAN) und leiten Pakete zwischen den Netzwerkschnittstellen weiter.



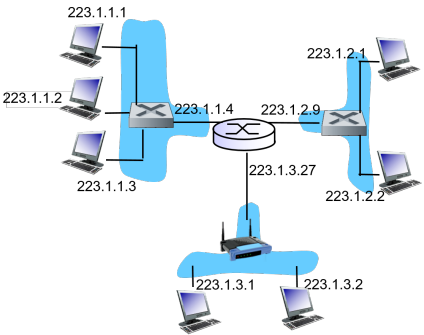
IP-Adressen

- IP-Adresse: 32-Bit-ID für eine *Netzwerkschnittstelle* eines Hosts/Routers.
- Darstellung typischerweise in Form von vier Bytes, die mit Punkten voneinander getrennt sind (Bytes in dezimaler Darstellung)



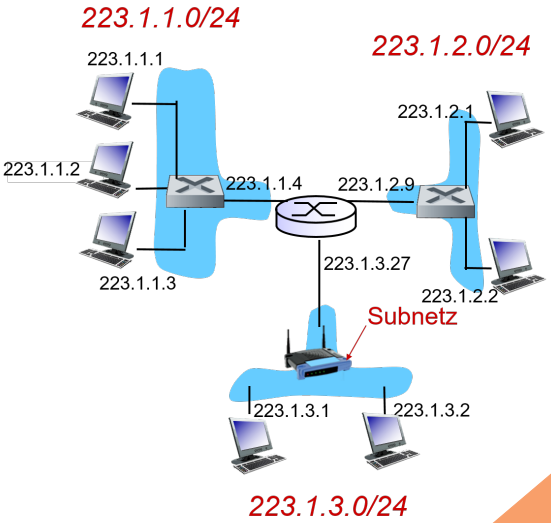
Subnetze

- IP-Adresse is zweigeteilt: Netzanteil und Hostanteil
- Netzanteil ist ein Adressteil, der eindeutig ein Subnetz bestimmt (d. h. alle Hosts eines Subnetzes haben den gleichen Netzanteil)
- Hostanteil ist eindeutig für jeden Host in einem Subnetz
- Beispiel rechts besteht aus 3 Bytes/24 Bit Netzanteil und 1 Byte/8 Bit Hostanteil
- Anzahl der Bits für Netz- und Hostanteil kann variieren und wird durch die Subnetzmaske bestimmt



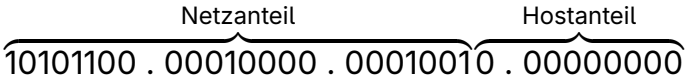
(Sub-)Netzmaske

- Subnetzmaske wird mit */xx* an die IP angehängt, wobei xx die Anzahl der Bits definiert, die zum Netzanteil gehören
- alternative Darstellungsart der Subnetzmaske durch eine IP-Adresse in der alle Bits „1" sind, die zum Netzanteil gehören
- Adressierungsart wird als CIDR (Classless InterDomain Routing) bezeichnet
- Beispiel: /24 oder 255.255.255.0



Beispiel CIDR

Classless InterDomain Routing



Entspricht dem folgenden Netz:

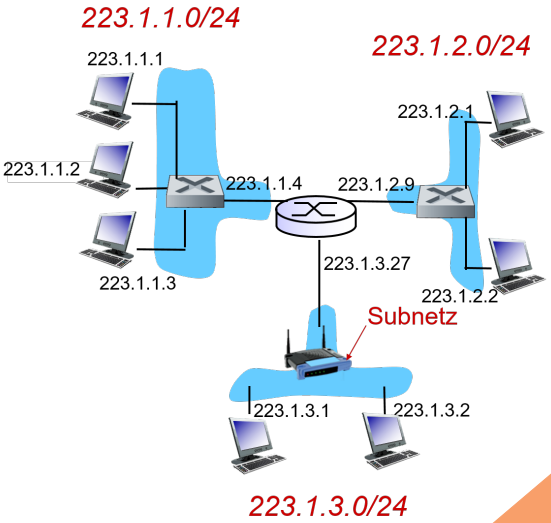
- 172.16.18.0/23
- oder: 172.16.18.0 mit Netzmaske 255.255.254.0

Übung: IP Adressen

- Gegeben sei das Netz 200.23.16.0/24
- Netzwerk-Adresse?
- mögliche IP-Adressen für Hosts?
- Broadcast-Adresse?

Erzeugen von Subnetzen

- Administratoren bekommen i. d. R. ein Subnetz zugewiesen, z. B. 223.1.0.0/22
- da jedes Netzwerkinterface eines Routers in einem eigenen Subnetz liegt, ist die Unterteilung des Netzes notwendig (sog. Subnetting)
- Beispiel: Unterteilung des o. g. Netzes in drei Subnetze (alle liegen im Subnetz 223.1.0.0/22 und werden durch externe Router gleich behandelt)



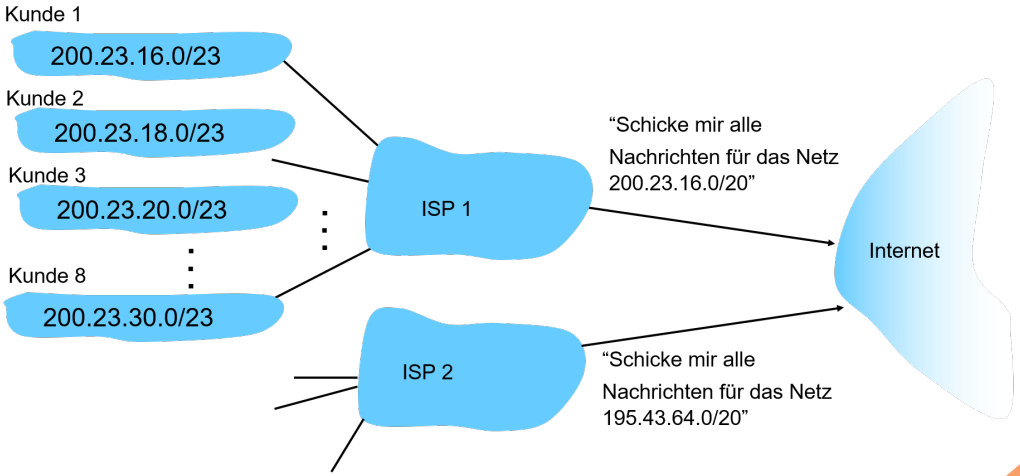
Beispiel Adressraumvergabe

Ein Internetservice-Provider (ISP) vergibt Adressräume an seine (acht) Kunden:

ISP Block	11001000 00010111 00010000 00000000	200.23.16.0/20
Kunde 1	11001000 00010111 00010000 00000000	200.23.16.0/23
Kunde 2	11001000 00010111 00010010 00000000	200.23.18.0/23
Kunde 3	11001000 00010111 00010100 00000000	200.23.20.0/23
...		
Kunde 8	11001000 00010111 00011110 00000000	200.23.30.0/23

Hierarchische Adressierung

Hierarchische Adressierung erlaubt effizientes Routing:



Besondere Subnetze

- RFC1918 definiert ein paar Subnetze, die privat genutzt werden dürfen
- diese privaten Adressbereiche werden nicht von Internetdienstanbietern geroutet
- Liste privater Adressbereiche:
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
- zusätzlich ist noch der Bereich 169.254.0.0/16 für IP-Autokonfiguration reserviert (reden wir später drüber) und 100.64.0.0/10 für die interne Nutzung bei Internetdienstanbietern

Übung: Subnetting

Gegeben ist folgendes Netzwerk:
IP-Adresse: 40.1.1.96
Subnetzmaske: 255.255.255.224

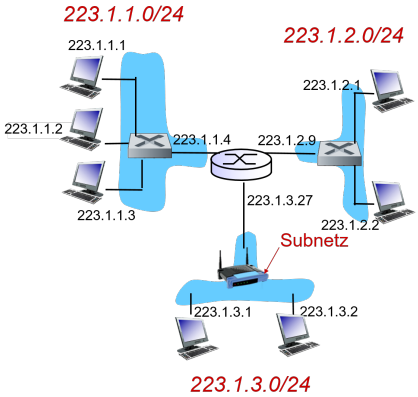
- Wie viele IP-Adressen stehen für den Geräteanteil zur Verfügung? Wie lauten die erste und letzte IP-Adresse, die für Hosts verwendet werden können?
- Unterteilen Sie das o. g. Netz in zwei Subnetze für jeweils mindestens 10 Hosts. Geben Sie die Netzadressen und Subnetzmasken der beiden Teilnetze an.

Übung: Subnetting

Überblick

1. Einleitung
2. IPv4
   - Datagramm-Aufbau
   - Router
   - Subnetze
3. ARP
4. Routing
5. ICMP
6. IP-Adressvergabe
7. IPv4 Übungen
8. IPv4 Probleme
9. IPv6
   - IPv6-Datagramm
   - IPv6-Adressierung

Beispiel Datenversand

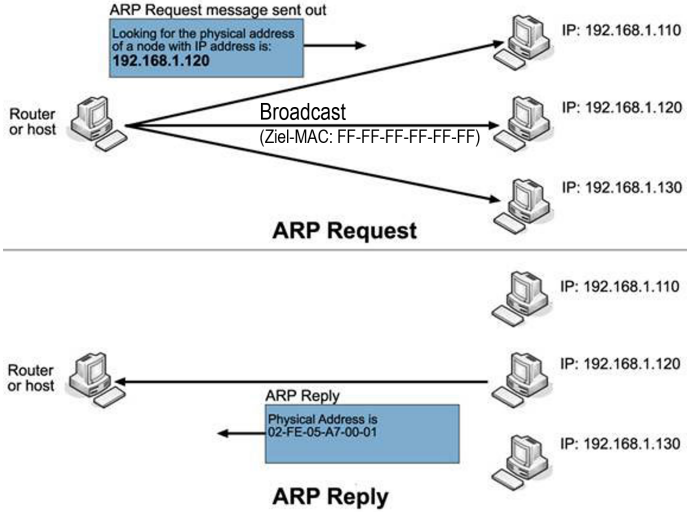


- 223.1.1.1 muss an Router 223.1.1.4 senden
- IP-Adresse kennt er nun.
- Wie erfährt 223.1.1.1 die MAC-Adresse des Routers?

ARP (Address Resolution Protocol)

- ARP ist ein Link-Layer-Protokoll zur Ermittlung einer MAC-Adresse, die zu dem Netzwerkinterface einer IP-Adresse gehört
- Router sendet weiter an 223.1.3.2
- Wie erfährt 223.1.1.1 die MAC-Adresse des Routers?

ARP (Address Resolution Protocol)



ARP-Tabelle

- IP-MAC-Übersetzung wird in einer ARP-Tabelle gespeichert
- Ausgabe des Inhalts der ARP-Tabelle unter Windows/Linux mit `arp -a`

Beispiel:

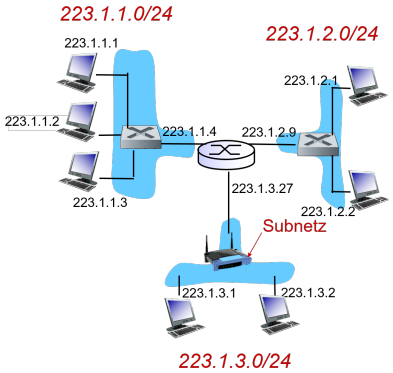
```
Schnittstelle: 192.168.110.1 --- 0x13
Internetadresse        Physische Adresse     Typ
192.168.110.255        ff-ff-ff-ff-ff-ff     statisch
224.0.0.22             01-00-5e-00-00-16     statisch
224.0.0.251            01-00-5e-00-00-fb     statisch
224.0.0.252            01-00-5e-00-00-fc     statisch

Schnittstelle: 192.168.91.1 --- 0x14
Internetadresse        Physische Adresse     Typ
192.168.91.255         ff-ff-ff-ff-ff-ff     statisch
224.0.0.22             01-00-5e-00-00-16     statisch
224.0.0.251            01-00-5e-00-00-fb     statisch
224.0.0.252            01-00-5e-00-00-fc     statisch
```

Überblick

1. Einleitung
2. IPv4
   - Datagramm-Aufbau
   - Router
   - Subnetze
3. ARP
4. Routing
5. ICMP
6. IP-Adressvergabe
7. IPv4 Übungen
8. IPv4 Probleme
9. IPv6
   - IPv6-Datagramm
   - IPv6-Adressierung

Beispiel Datenversand



223.1.1.1 will Datagramm an 223.1.3.2 senden.
Wie funktioniert das?

Prozess

- 223.1.1.1 muss an Router 223.1.1.4 senden
- Router sendet weiter an 223.1.3.2
- Wie erfährt 223.1.1.1 die IP-Adresse des Routers?

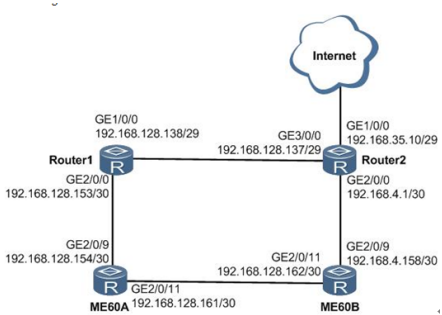
Routing-Tabellen

- Jeder Host/Router legt intern Routing-Tabellen an, die angeben, welches Netzwerk hinter welchem Interface liegt.
- Routing-Tabellen können statisch konfiguriert werden (oder durch Routing-Protokolle dynamisch - dazu später)
- Routing-Tabelle kann mittels `route`-Befehl konfiguriert und angezeigt werden

Beispiel:

```
versick@ubuntu:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         [...]  Iface
default         192.168.91.2    0.0.0.0         [...]  ens33
link-local      0.0.0.0         255.255.0.0     [...]  ens33
172.17.0.0      0.0.0.0         255.255.0.0     [...]  docker0
192.168.91.0    0.0.0.0         255.255.255.0   [...]  ens33
```

Routing-Schleifen

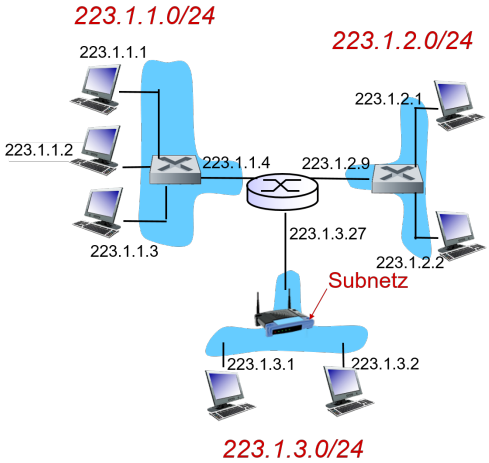


- Ausfall des Links im Internet könnte bei falscher Konfiguration von Router2 dazu führen, dass dieser als alternative Route zum Beispiel zu Router3 weiterleitet
- führt zu eine unendlichen Hin-und-Her der Pakete, die eigentlich ins Internet geroutet werden sollten
- Was tun?

Time-to-Live

- TTL (Time-to-Live) wird bei jeder Weiterleitung durch einen Router verringert
- Paket wird verworfen, sobald TTL den Wert 0 erreicht
- Header-Checksumme?
- Maximaler Wert der TTL?
- Standardwert der TTL?

Übung: Routing und ARP



Aufgabe auf der nächsten Folie.

Übung: Routing und ARP

Der Router habe die folgende Routing-Tabelle:

```
Kernel IP routing table
Destination     Gateway         Genmask         Iface
default         223.1.1.1       0.0.0.0         eth0
223.1.1.0       0.0.0.0         255.255.255.0   eth0
223.1.2.0       0.0.0.0         255.255.255.0   eth1
223.1.3.0       0.0.0.0         255.255.255.0   eth2
```

An welches/n Interface/Host werden Pakete mit den folgenden Zieladressen geschickt? Ergänzen Sie die Tabelle mit Interface, an das geroutet wird und der IP des ARP-Requests für den nächsten Hop.

Ziel-IP	Interface	IP des ARP Requests
223.1.1.3		
193.99.144.85		
223.1.3.34		

Überblick

1. Einleitung
2. IPv4
   - Datagramm-Aufbau
   - Router
   - Subnetze
3. ARP
4. Routing
5. ICMP
6. IP-Adressvergabe
7. IPv4 Übungen
8. IPv4 Probleme
9. IPv6
   - IPv6-Datagramm
   - IPv6-Adressierung

ICMP

Internet Control Message Protocol

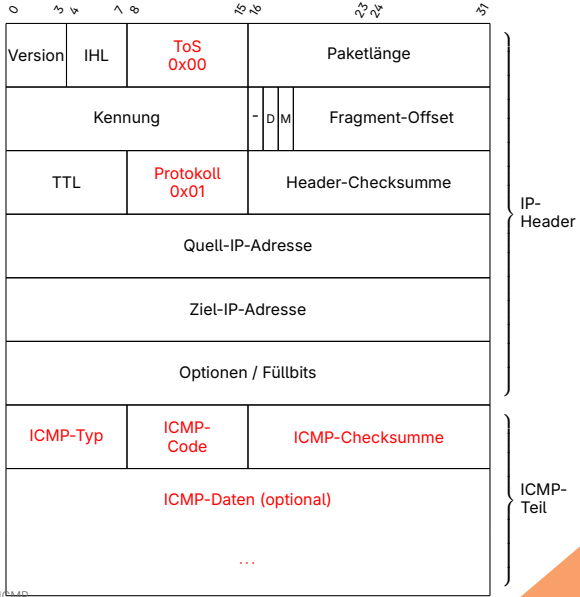
- wird von Rechnern und Routern verwendet, um Kontrollinformationen über die Vermittlungsschicht auszutauschen
- ICMP-Nachrichten sind in IP-Datagramme eingepackt (damit ist ICMP eigentlich ein Protokoll oberhalb von IP)

Wichtige ICMP-Nachrichtentypen:

Typ	Code	Beschreibung
0	0	Echo Reply (ping)
3	0	Zielnetzwerk nicht erreichbar
3	1	Zielhost nicht erreichbar
3	2	Zielprotokoll nicht erreichbar
3	3	Zielport nicht erreichbar
3	6	Zielnetzwerk unbekannt
3	7	Zielhost unbekannt
8	0	Echo Request (ping)
11	0	TTL abgelaufen
12	0	Fehler im IP Header

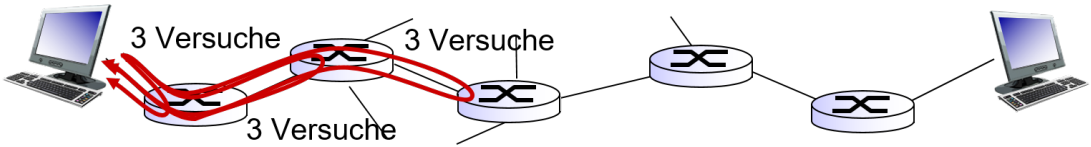
Aufbau eines ICMP-Pakets

- ICMP nutzt den IP-Header mit Protokoll 1 (ICMP)
- ToS wird auf 0 gesetzt
- ICMP Header und -Daten liegen im Datenteil des IP-Pakets



Traceroute und ICMP

- Traceroute ermittelt alle Router auf dem Weg zu einem Ziel
- Vorgehen:
  - setze TTL des ersten ICMP-Requests auf 1 und versende Paket zum Ziel
  - erster Router dekrementiert TTL, verwirft Paket und sendet ICMP-TTL-Expired-Nachricht zurück (dieses Paket hat Router-IP als Absender)
  - versende nun ein Paket mit TTL=2 und versende dies erneut
  - nun wird der zweite Router das Paket verwerfen und eine ICMP-TTL-Expired-Nachricht mit seiner IP als Absender zurückschicken
  - usw.



Traceroute Beispiel

```
[root@LVLX09 ~]# traceroute www.google.de
traceroute to www.google.de (172.217.21.227), 30 hops max,
                                        60 byte packets
1  gateway (192.168.51.254) 0.339 ms 0.234 ms 0.182 ms
2  192.168.236.1 (192.168.236.1) 0.392 ms 0.529 ms 0.559 ms
3  62.156.244.28 (62.156.244.28) 13.923 ms 14.039 ms 14.107 ms
4  62.156.246.98 (62.156.246.98) 13.928 ms 14.554 ms 14.682 ms
5  * * *
6  87.128.238.13 (87.128.238.13) 18.783 ms 17.777 ms 18.758 ms
7  * * *
8  216.239.40.58 (216.239.40.58) 18.357 ms * 19.414 ms
9  108.170.235.251 (108.170.235.251) 18.688 ms * 18.670 ms
10 72.14.239.167 (72.14.239.167) 18.943 ms 18.572 ms 18.491 ms
```

Überblick

1. Einleitung
2. IPv4
   - Datagramm-Aufbau
   - Router
   - Subnetze
3. ARP
4. Routing
5. ICMP
6. IP-Adressvergabe
7. IPv4 Übungen
8. IPv4 Probleme
9. IPv6
   - IPv6-Datagramm
   - IPv6-Adressierung

IP-Adressvergabe

Welche Möglichkeiten der IP-Adressvergabe kennen Sie?

Manuelle IP-Adressvergabe

- IP-Adresse und Netzmaske wird durch Administrator zugewiesen und muss manuell konfiguriert werden
- Unter Windows: In den Einstellungen
- Linux-Tool zur IP-Adresskonfiguration: `ip` oder `ifconfig`

Beispiel:

```
ifconfig eth0 192.168.0.1 netmask 255.255.255.0 up
```

Automatische IP-Adressvergabe: DHCP

Dynamic Host Configuration Protocol

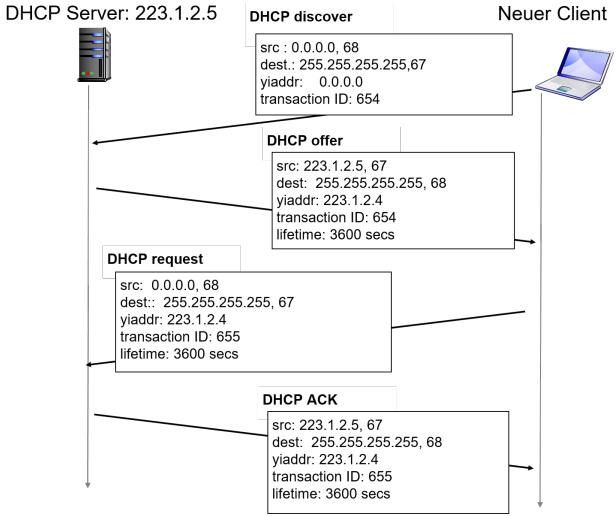
- Ziel: Hosts erhalten automatisch eine IP von einem Server im Internet, sobald sie das Netzwerk betreten
- Hosts müssen den Lease der IP regelmäßig erneuern, sonst wird die IP neu vergeben
- effiziente Nutzung des IP-Adressraums

Aufbau eines DHCP-Paketes

- DHCP Header und -Daten liegen im Datenteil des IP-Pakets
- Wichtige Felder:
  - op - 1 BOOTREQUEST, 2 - BOOTREPLY
  - htype, hlen - Hardware Adresstyp und -länge
  - xid - Transaction ID (zufällige Zahl, die der Client erzeugt - damit spezifiziert der Server, welche Antwort zu welcher Anfrage gehört)
  - ciaddr - Client Address (wird ausgefüllt, wenn der Client bereits eine Adresse hat und diese verlängern möchte)
  - yiaddr - Your Address (Server sendet diese Adresse zum Client)

DHCP-Ablauf

- DHCP-Discover um Server zu finden
- DHCP-Offer enthält ein Angebot
- Client fordert dieses Angebot an (DHCP-Request) und Server bestätigt es (DHCP ACK)



DHCP - Mehr als nur Adressen

DHCP kann mehr als nur IP-Adressen zuweisen, z. B.:

- Netzwerkmaske
- IPs von DNS-Servern
- Bootfiles
- ...

AdHoc-Netzwerke?

- Mobile Geräte können ad-hoc ohne DHCP-Server oder manuelle Konfiguration kommunizieren.
- Wie funktioniert IP-Adressvergabe?

IP-Autoconfiguration

Wenn kein DHCP-Server existiert, kann sich ein Gerät selbst eine IP geben
Ablauf:

- Wahl eines zufälligen IP-Adresskandidaten aus dem Netz 169.254.0.0/16
- ARP-Anfrage, um zu ermitteln, ob diese IP bereits vergeben ist
- wenn vergeben, Vorgang wiederholen
- wenn nicht vergeben, IP-Kandidaten dem Interface zuordnen

Wiederholungsübung IP-Adressvergabe

Erstellen Sie ein Ablaufdiagramm, das den Vorgang der IP-Adressvergabe in aktuellen Betriebssystemen möglichst genau beschreibt.

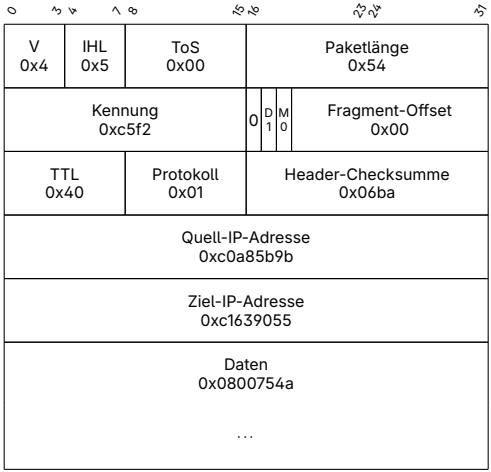
Überblick

1. Einleitung
2. IPv4
   - Datagramm-Aufbau
   - Router
   - Subnetze
3. ARP
4. Routing
5. ICMP
6. IP-Adressvergabe
7. IPv4 Übungen
8. IPv4 Probleme
9. IPv6
   - IPv6-Datagramm
   - IPv6-Adressierung

Übung: IP-Datagramm

Gegeben sei das folgende IP-Paket:

- Ermitteln Sie die Quell- und Ziel-IP in der üblichen dezimalen Schreibweise.
- Welches Protokoll ist in der Payload dieses Pakets zu finden? Was macht das Paket?
- Überprüfen Sie die Korrektheit des IP-Headers anhand der Prüfsumme.



Übung: IP-Datagramm

Übung: Wiederholung Routing

Zeichnen Sie ein Ablaufdiagramm mit den einzelnen Schritten, die ein Router durchführt, wenn ein Paket eintrifft.

Cisco Packet Tracer

- Starten Sie den Cisco Packet Tracer in der VDI-Umgebung (Login als Guest)
- Erstellen Sie ein Netzwerk mit einem Server, drei PCs und einem Netzwerk-Sniffer
- Der Server sollte IP-Adressen per DHCP vergeben (Adressraum: 192.168.1.0/24)
- Starten Sie ein ping zwischen zwei Rechnern und analysieren Sie sowohl die ARP, als auch die ICMP-Pakete.

Überblick

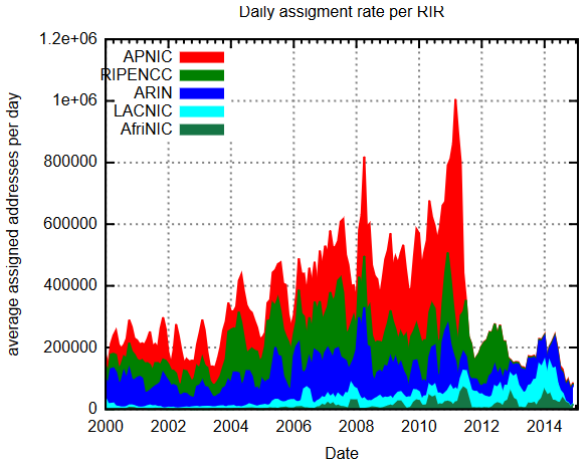
1. Einleitung
2. IPv4
   - Datagramm-Aufbau
   - Router
   - Subnetze
3. ARP
4. Routing
5. ICMP
6. IP-Adressvergabe
7. IPv4 Übungen
8. IPv4 Probleme
9. IPv6
   - IPv6-Datagramm
   - IPv6-Adressierung

Diskussion IP-Adressen

- Wie viele IP-Adressen gibt es?
- Wo gehen IP-Adressen verloren?
- Wie viele Hosts gibt es im Internet?

Verbrauch von IPv4-Adressen

Verbrauch von IP-Adressen bei den fünf weltweit agierenden regionalen Internet Registrierungen (RIR).

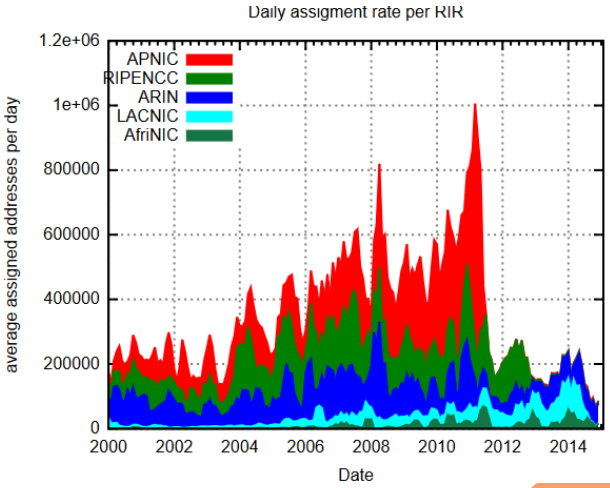


Gründe?

Verbrauch von IPv4-Adressen

Verbrauch von IP-Adressen bei den fünf weltweit agierenden regionalen Internet Registrierungen (RIR).

- 15.04.2011: letzter Adressbereich der Asia-Pacific Network Information Centre (APNIC) vergeben
- 14.09.2012: letzter Adressbereich der Réseaux IP Européens Network Coordination Centre (RIPENCC) vergeben
- 06.10.2014: letzter Adressbereich der Latin American and Caribbean Internet Addresses Registry (LACNIC) vergeben



Was kann man tun?

Überblick

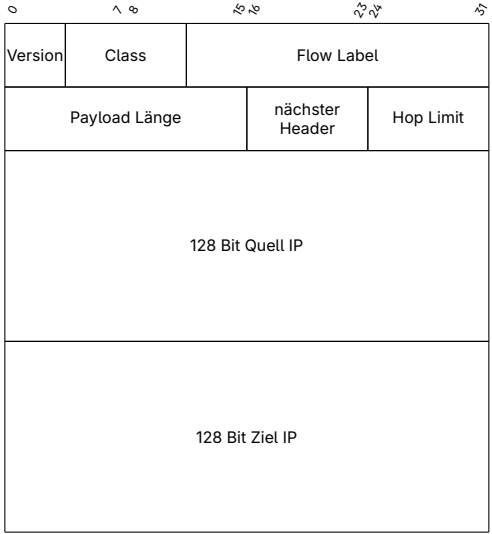
1. Einleitung
2. IPv4
   - Datagramm-Aufbau
   - Router
   - Subnetze
3. ARP
4. Routing
5. ICMP
6. IP-Adressvergabe
7. IPv4 Übungen
8. IPv4 Probleme
9. IPv6
   - IPv6-Datagramm
   - IPv6-Adressierung

IPv6 - Highlights

- IPv6 besitzt 128-Bit IP-Adressen
- unterstützt Authentifizierung und Verschlüsselung bereits im Standard („IPsec")
- QoS-Unterstützung
- Unterstützung mobiler Geräte

Aufbau des IPv6-Headers

Unterschiede zu IPv4?



IPv6 - Header-Unterschiede zu IPv4

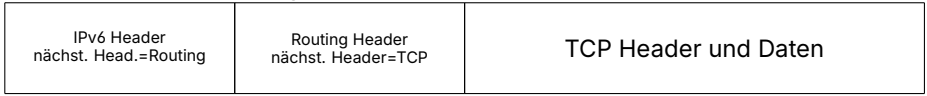
- Vereinfachungen
  - Fragmentierungsinformation in Zusatz-Headern
  - IP-Optionen in Zusatz-Headern
  - Entfernung der Header Checksumme und Header-Länge
  - Alignment von 32 Bit auf 64 Bit
- Anpassungen
  - TTL -> Hop Limit
  - Protokoll -> nächster Header
  - ToS -> Traffic Class
  - Adressen vergrößert von 32 Bit auf 128 Bit
- Erweiterungen
  - Flow Label

Konzept der Erweiterungsheader

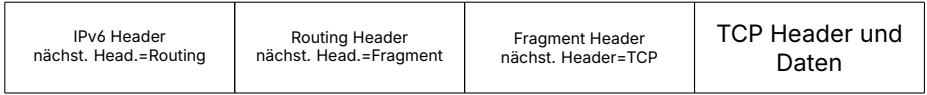
Beispiele

Nur Basis-Header

Basis-Header und Routing-Header



Basis-, Routing-und Fragment-Header



Extension Header werden i. d. R. nur vom Zielhost benutzt!

Text Repräsentation von Adressen

- Standardform: `1080:0:FF:0:8:800:200C:417A`
- komprimierte Form: `FF01:0:0:0:0:0:0:43` wird zu `FF01::43`
- IPv4-kompatible: `0:0:0:0:0:0:13.1.68.3` oder `::13.1.68.3`

IPv6-Adressierungsmodell

- Adressen sind Schnittstellen zugeordnet
- aber: jede Schnittstelle hat typischerweise mehrere Adressen
- Adressen haben unterschiedlichen Scope:
  - Link-local
  - Site-local
  - Global

IPv6-Adresstypen

Je nach gewünschter Kommunikation werden unterschiedliche Adressen verwendet:

- Unicast:
  - Adresse eines einzelnen Interfaces
  - Nachricht wird an genau dieses Interface zugestellt
- Multicast:
  - Adresse einer Interfacemenge
  - Nachricht wird an alle Interfaces der Menge zugestellt
- Anycast:
  - Adresse einer Interfacemenge
  - Nachricht wird an ein Interface der Menge zugestellt

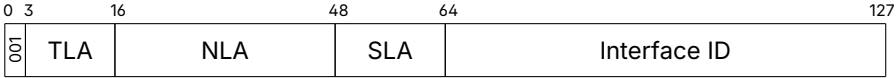
Adresstyp und Scope ist anhand des Adresspräfixes erkennbar

Adress-Präfixes

Adresstyp	Präfix (binär)
IPv4-kompatibel	`0000...0` (96 Null-Bits)
globaler Unicast	`001`
Link-lokaler Unicast	`1111 1110 10`
Site-lokaler Unicast	`1111 1110 11`
Multicast	`1111 1111`

- alle anderen Präfixe sind für die Zukunft reserviert
- Anycast-Adressen haben Unicast-Präfixe

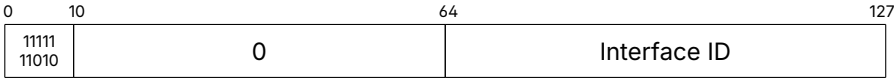
Globale Unicast Adresse



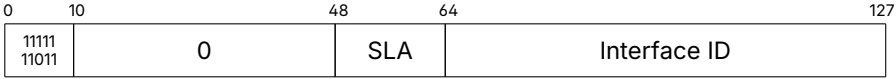
- TLA (Top-Level-Aggregator) - definiert große Adressblöcke z. B. von Internetprovidern; zum Routing auf oberster Ebene werden ausschließlich die 13 Bit der TLA verwendet
- NLA (Next-Level-Aggregator) - Adressblöcke zwischen den das Routing beim Provider durchgeführt wird; Organisation erhält Adressblock spezifiziert durch TLA und NLA
- SLA (Site-Level-Aggregator) - Aufteilung des Netzes innerhalb einer Organisation durch veränderte SLAs
- Interface ID - ID einer jeden Netzwerkschnittstelle

Link-lokale und Site-lokale Adressen

Link-lokale Adressen dienen der Autokonfiguration bzw. wenn kein Router existiert:

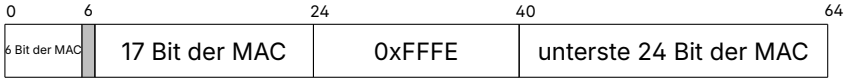


Site-lokale Adressen sind unabhängig von TLA/NLA:



Zuweisung von Interface IDs

- Auto-Konfiguration durch Expandierung der 48-Bit-MAC zu einer 64-Bit EUI-64



  IPv6 invertiert außerdem das siebte Bit von links (U/L-Bit) in der MAC-Adresse
  EUI-64 wird von der IEEE aufgrund von potentiellen Adresskollisionen nicht mehr empfohlen
- Autogenerierte Pseudozufallszahl (v. a. zur Sicherstellung von Privatheit)
- Zuweisung via DHCP
- Manuelle Konfiguration
- weitere Möglichkeiten mögen in Zukunft definiert werden

Besondere Adressen

`0:0:0:0:0:0:0:0` - Platzhalter (keine Adresse wurde definiert)
`0:0:0:0:0:0:0:1` - loopback-Schnittstelle
Broadcasts kennt IPv6 nicht, daher gibt es keine Broadcast-Adresse (Nutzung von Multicasts anstelle von Broadcasts)

Übung: IPv6-Adresserstellung

Wie lautet die globale Unicast-IPv6 Adresse einer Schnittstelle für einen Rechner mit folgenden Daten (die MAC werde zu einer EUI-64 erweitert):

- TLA: 0x2
- NLA: 0x55b117ca
- SLA: 0x0
- MAC-Adresse: 3c:15:c2:e3:cb:10

Übung: IPv6-Adresserstellung

Übung: IPv6-Adressen

Folgendes ist die Ausgabe von `ifconfig` auf einem Rechner in einem IPv6-Netzwerk:

```
Daniels-MacBook-Pro:~ dave$ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        options=3<RXCSUM,TXCSUM>
        inet6 ::1 prefixlen 128
        inet 127.0.0.1 netmask 0xff000000
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=1<PERFORMNUD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether 3c:15:c2:e3:cb:10
        inet6 fe80::3e15:c2ff:fee3:cb10%en0 prefixlen 64 scopeid 0x4
        inet 172.16.1.16 netmask 0xffffff00 broadcast 172.16.1.255
        inet6 2002:55b1:17ca::3e15:c2ff:fee3:cb10 prefixlen 64 autoconf
        inet6 2002:55b1:17ca::4918:b00d:6f7:b987 prefixlen 64 autoconf temporary
        nd6 options=1<PERFORMNUD>
        media: autoselect
        status: active
```

Was bedeuten die existierenden IPv6-Adressen?

IP-Adressvergabe SLAAC

Stateless Address Autoconfiguration

- insbesondere kleinere IPv6-Netze verwenden kein DHCP zur Adressvergabe, sondern SLAAC
- SLAAC ähnelt IP-Autoconfiguration, kann aber auf beliebige Adresspräfixes angewendet werden
- daher: DHCP-Server nicht notwendig

Ablauf SLAAC:

1. Router Advertisement (RA): Ein IPv6-Router sendet regelmäßig Router Advertisement-Nachrichten an alle Geräte im Netzwerk.
2. Präfix-Erkennung: Ein Gerät empfängt eine RA-Nachricht und extrahiert das Präfix aus der Nachricht.
3. Adresse erstellen: Das Gerät erstellt eine IPv6-Adresse, indem es das Präfix mit einer selbst generierten Schnittstellenkennung kombiniert (früher EUI-64, heute oft Zufallsadresse).
4. Doppelte Adressprüfung: Das Gerät überprüft, ob die erstellte Adresse bereits im Netzwerk verwendet wird.
5. Adressverwendung: Wenn die Adresse einzigartig ist, verwendet das Gerät diese als seine IPv6-Adresse.

Arbeiten mit IPv6

- nahezu alle verbreiteten Tools unterstützen seit Jahren IPv6 (Browser, Email-Clients, Netzwerktools)
- die meisten Internetprovider stellen ein IPv6-Prefix für das private Subnetz bereit
- aktuelle Router unterstützen IPv6 ebenfalls
- Warum nicht verwenden?

Tools - Beispiele

```
Daniels-MBP:~ dave$ ping6 www.heise.de
PING6(56=40+8+8 bytes) 2a02:8108:1600:e32:d8bb:f66d:1547:5e45
                    --> 2a02:2e0:3fe:1001:7777:772e:2:85
16 bytes from 2a02:2e0:3fe:1001:7777:772e:2:85, icmp_seq=0
                                  hlim=52 time=33.562 ms
16 bytes from 2a02:2e0:3fe:1001:7777:772e:2:85, icmp_seq=1
                                  hlim=52 time=27.023 ms
16 bytes from 2a02:2e0:3fe:1001:7777:772e:2:85, icmp_seq=2
                                  hlim=52 time=26.194 ms


Daniels-MBP:~ dave$ nslookup www.heise.de
Server:     2a02:8108:1600:e32:8a71:b1ff:fe84:90a
Address:    2a02:8108:1600:e32:8a71:b1ff:fe84:90a#53

Non-authoritative answer:
Name:    www.heise.de
Address: 193.99.144.85
```

Wechsel von IPv4 auf IPv6

Wo sehen Sie Probleme?

Weitere Features von IPv6

- IPSec ist Teil des Standards - Authentifizierung, Authorisierung und Verschlüsselung
- Mobility-Support (Mobile IP) - erlaubt den Verbindungsaufbau zu Hosts, die Ihre IP regelmäßig aufgrund von Netzwerkänderungen variieren (z. B. Laptops)