Kapitel 7: Layer 3 / IP

Aufgaben des Network Layer

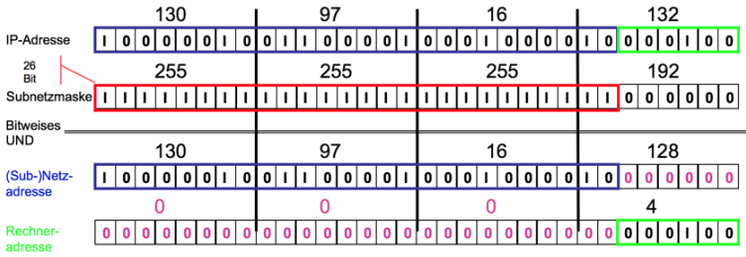
- Die Schnittstelle von **Layer 2** erlaubt uns, Daten von einer Station in einem lokalen Netz an eine andere Station im lokalen Netz zu senden.
- **Mögliche Schnittstellen für Layer 3:**
- Verbindungsorientiert, d. h. es werden in der Schnittstelle Funktionen wie „Baue Verbindung auf“, „Sende Daten über Verbindung x“, „Baue Verbindung ab“ angeboten. Beispiel: Asynchronous Transfer Mode (ATM) Netze Verbindungslos, d. h. es werden in der Schnittstelle Funktionen wie „Sende Paket“ oder „Empfange Paket“ angeboten. Beispiel: Internet Protocol (IP) Netze wie bspw. das Internet

IP-Adressen, Netze, der IP-Kopf

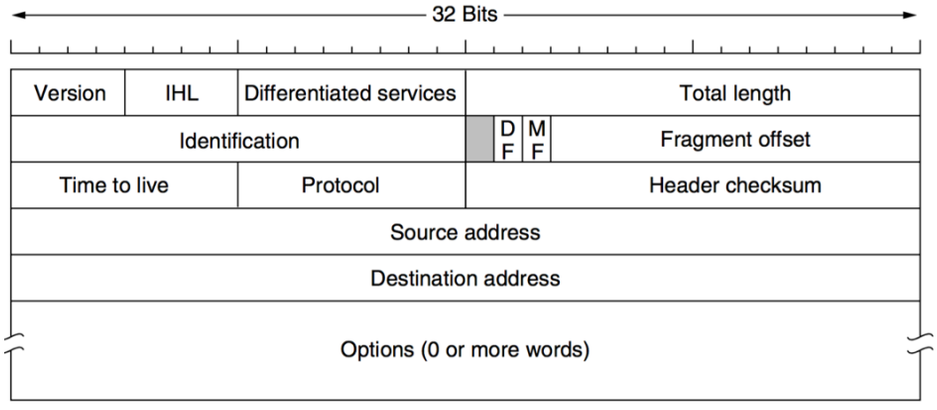
- Logische Adressen abstrahieren von der Hardware.
- IPv4-Adresse: **4 Byte** (32 Bit lang) z.B.: 141.71.31.220 => 2^32 Adressen
- Adressen bestehen aus **Netz- und Rechneradresse**

Classless Inter Domain Routing (CIDR)

- Subnetzmaske gibt an wo Netz- und Rechneradresse ist, indem sie angibt wie viele Bits Netzadresse hat.
  → 130.97.16.132/26
  => 26 Bits hat Netzadresse
  → 130.97.16.132/255.255.255.192
  => oder als Bitmaske



Aufbau von IP-Paketen



- **Version**: Protokollversion (z.B.: 4,6)
- **IP Header Length (IHL):** Länge des Headers
- **Type of Service (TOS):** Gewünschter Service-Typ
- **Total Length:** Gesamtlänge des Datengramms in Byte *(Header und Nutzdaten)*
- **Identification**: Steuert Zugehörigkeit von Fragmenten zu Datengrammen zwecks Zusammensetzung von zuvor fragmentierten IP-Datengrammen
- **Don’t Fragment (DF):** Signalisiert, dass das Paket nicht fragmentiert werden darf
- **More Fragments (MF):** Signalisiert, dass weitere Fragmente folgen
- **Fragment Offset:** Gibt die Stelle im Datengramm an, an die das Fragment gehört
- **Time to Live (TTL):** Gibt (eigentlich) die Lebenszeit des Pakets in Sekunden an in Wirklichkeit aber einfach die maximale Anzahl von Hops (engl. Hop-Count) jeder Router dekrementiert TTL; falls 0 wird Paket verworfen
- **Protocol:** Gibt an, zu welchem Protokoll die Nutzdaten gehören (gemäß RFC 3232 Wert 6 für TCP-Paket, Wert 17 für UDP-Paket, etc.)
- **Header Checksum**: Prüfsumme zur Erkennung von Fehlern im Header; muss in jedem Router neu generiert werden
- **Source und Destination Address**: IP-Adressen von Absender- (engl. source) und Empfänger-Rechnern (engl. destination)
- **Options:** Feld für Optionen

Paketversand in einem LAN mit ARP und über Router

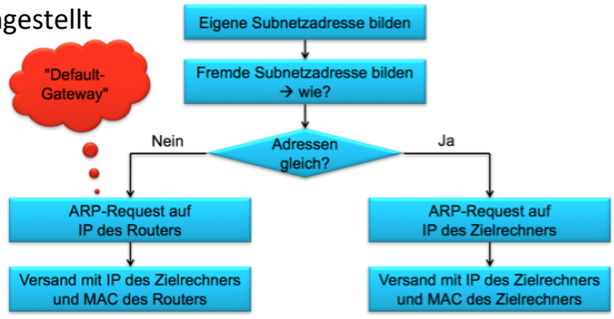
Paketversand innerhalb eines lokalen Netzes

1. Vergleiche Netzadressenanteil der IP-Adressen. **IP-Adresse A ∧ Netzmaske = IP-Adresse B ∧ Netzmaske**
2. **Benutzte das Address Resolution Protocol (ARP).**
   Sende einen MAC-Broadcast mit einem **ARP Request**. Jeder Rechner im Netz empfängt diese Nachricht und B antwortet dann mit einen Ethernet-Rahmen **ARP Reply** an die MAC-Adresse von A.

Paketversand an Rechner in einem anderen Netz

- Ist die Empfänger-IP-Adresse nicht in demselben Netz wie die Absender-IP-Adresse, dann muss das Paket über eine Zwischenstation (Router) gesendet werden.

1. Vergleiche Netzadressenanteil der IP-Adressen. **IP-Adresse A ∧ Netzmaske ≠ IP-Adresse B ∧ Netzmaske**
2. In der Konfiguration von A wird die IP-Adresse eines Routers eingestellt
3. **ARP**



Address Resolution Protocol (ARP)

Aufgabe: Abbildung von IP-Adressen auf MAC-Adresse
Zwei Vorgehensweisen sind möglich:

1. **Statische Lösung**: Konfigurationsdatei mit allen Abbildungen
2. **Dynamische Lösung**: Einsatz von ARP

Ablauf bei ARP:

1. **ARP-Request**: Layer 2 Broadcast-Nachricht mit der Frage: „Wer hat eine bestimmte IP-Adresse?“
2. **ARP-Reply**: Gezielte Antwort des Rechners mit der gesuchten IP-Adresse an den anfragenden Rechner. Die Antwort enthält die gesuchte MAC-Adresse.

Optimierungsmöglichkeiten:

- Statt immer wieder ARP Requests zu versenden speichert jeder Rechner bereits ermittelte Zuordnungen in der **ARP-Tabelle (ARP Cache).**
- Im jedem ARP Request steht nicht nur die angefragte IP-Adresse, sondern auch IP-Adresse und MAC-Adresse des anfragenden Rechners.
- ARP Requests sind Broadcasts, d. h. jeder Rechner im LAN empfängt den ARP Request. Jeder Rechner kann seinen ARP Cache mit einem Eintrag über den anfragenden Rechner füllen.
- Beim Einschalten sendet jeder Rechner einmal einen ARP Request nach seiner
- eigenen IP-Adresse.

arp-Kommando: Mit dem Linux-Kommando arp lässt sich der Inhalt der ARP-Tabelle anschauen.

Vorteile:

- Änderungen wie Austausch von Netzwerkkarten oder IP-Adressen werden automatisch an alle Rechner propagiert
- ARP-Cache-Einträge dürfen dazu nur eine begrenzte Gültigkeit haben Administrativer Aufwand zur Pflege der Abbildungen in jedem Rechner entfällt

Nachteile:

- In großen lokalen Netzen kommt es zu sehr vielen Broadcast-Nachrichten. Unbefugte Dritte können in einem lokalen Netz gefälschte ARP-Pakete versenden (ARP Spoofing) und damit unbefugt Daten mitlesen.

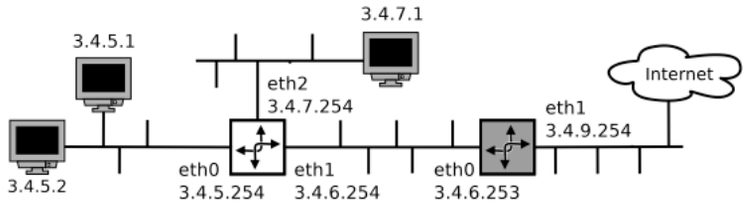
Exkurs: ARP-Spoofing
Das Senden von gefälschten (engl. to spoof, dt. täuschen) ARP-Paketen
***Ziel**: ARP-Tabellen so verändern, dass anschließend Datenverkehr abgehört oder manipuliert werden kann.*
Beispiel-Angriff:

- *Host A will Daten auf Layer 3 an Host B senden und führt dazu eine ARP-Anfrage aus: Wer kennt die MAC-Adresse zu der IP-Adresse von Host B?*
- *Angriffs-Host C antwortet: Ich kenne die MAC-Adresse von B. Sie lautet MAC-Adresse von C.*
- *Host A trägt in die eigene ARP-Tabelle ein: IP-Adresse von B und MAC-Adresse von C gehören zueinander.*
- *Host A überträgt Daten auf Layer 3 an Host B und schaut daher im eigenen ARP-Cache nach der MAC-Adresse von B nach. Dort steht für den Host B die MAC-Adresse von Host C.*
- *Host A überträgt daher Daten auf Layer 2 an Host C.*

Routing in IP-Netzen

- Hat ein Netz zwei Ausgänge, muss geklärt werden, welcher Ausgang genommen werden soll.

Routing Tabellen



Routingtabelle des weißen Routers:

Ziel	Router	Genmask	Flags	Iface
0.0.0.0	3.4.6.253	0.0.0.0	UG	eth1
3.4.5.0	0.0.0.0	255.255.255.0	U	eth0
3.4.6.0	0.0.0.0	255.255.255.0	U	eth1
3.4.7.0	0.0.0.0	255.255.255.0	U	eth2

Für jede Zeile der Routingtabelle:

- Berechne Ziel-IP ∧ Genmask = Ziel-Netz-Adresse
- Wenn Ziel-Netz-Adresse = Ziel, dann ist Zeile ein Kandidat

Wähle beste Kandidatenzeile nach **Longest Prefix Match**.

Eigenschaften des Routing in IP

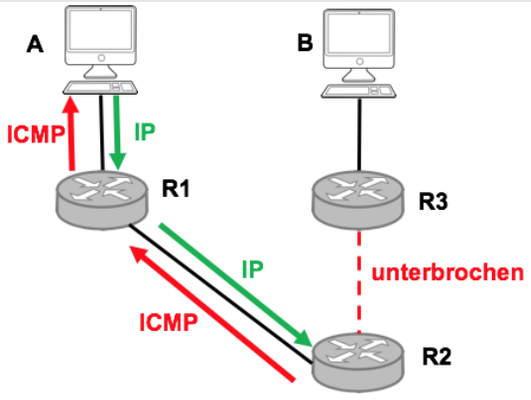
- Trifft keine der Zeilen in der Routing-Tabelle auf ein Paket zu, dann ist es nicht zustellbar und wird verworfen.
- Gibt es eine Standardgateway-Zeile (0.0.0.0), dann trifft diese immer zu. Sie wird aber nur dann ausgeführt, wenn es keine besser passende Zeile gibt.
- Zur korrekten Konfiguration der Routing-Tabellen gibt es dynamische Methoden, mit denen sich Router über ihre Tabelleninhalte austauschen.
- Bei falsch konfigurierten Routern können Schleifen beim Pakettransport auftreten. Pakete könnten ewig im Kreis laufen. Das wird mit dem **IP-Header Time To Live (TTL)** verhindert.

ICMP

- IP nur für Datenaustausch
- Kein Austausch von Steuerungs- oder Fehlermeldungen

ICMP-Nachrichtentypen:

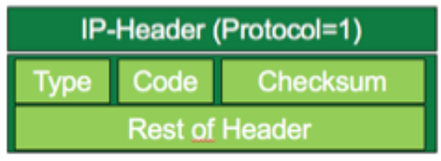
- Fehlermeldungen, Diagnosemeldungen



Beispiel:

- R2 empfängt Paket von A
- R2 sieht, dass Route unterbrochen ist
- R2 sendet ICMP Destination unreachable an A
- A kann Fehlermeldung ausgeben

ICMP-Nachrichten



Eingebettet in IP-Paket

- Protokoll Typ 1 (reguläres IP hat 4)

Format:

- **Type (1 Byte):** Typ der Meldung
- Grobe Kategorisierung. Beispiel: Type 3 = „Destination unreachable“
- **Code (1 Byte):** Sub-Typ der Meldung
- Jeder Nachrichtentyp wird in weitere Meldungen aufgeschlüsselt. Beispiel: ***Code 6 = „Destination network unknown“***
- **Checksum (2 Bytes):** Prüfsumme (Internet Checksum nach RFC 1071)
- **Rest of Header (4 Bytes):** weitere Informationen Sub-Typ-spezifische weitere Informationen, z. B. Zeitstempel

Fehlernachrichten:

- *Destination unreachable: d. h. IP-Paket konnte nicht zugestellt werden (bspw. weil ein Host zur Zeit ausgeschaltet ist)*
- *Time exceeded: d. h. TTL-Wert erreichte den Wert 0, Paket wurde verworfen*
- *Source quench: d. h. ein Kommunikationskanal ist überlastet, sendender Rechner soll langsamer senden*
- *Redirect: d. h. ein Gerät soll seine Routen anpassen, bspw. wegen Ausfall einer Strecke*

Diagnosenachrichten:

- *Echo und Echo Reply: d. h. sendender Rechner schickt eine Echo-Anfrage zum Ziel-Rechner, dieser antwortet mit Echo Reply*

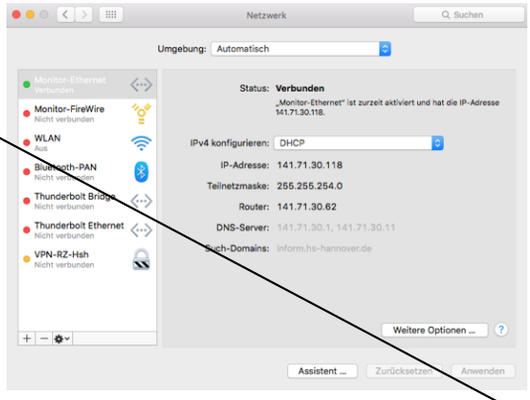
Netz-Konfiguration in modernen Betriebssystemen

Konfigurationsparameter

- IP-Adresse: Hier wird die IP-Adresse des Geräts eingetragen.
  Beispiel: 141.71.31.118
- Netzmaske: Hier wird die Netzmaske eingetragen.
  Beispiel: 255.255.254.0
- Default Gateway: Hier wird die IP-Adresse des „Ausgangs aus dem LAN“ also die IP-Adresse des Routes eingetragen.
  Beispiel: 141.71.30.62

Wie kommen diese Parameter in den Rechner?

- Der Administrator trägt sie manuell in die entsprechenden Konfigurations-Dateien/-Fenster ein.
- Der Rechner bekommt sie von einem DHCP-Server im lokalen Netz automatisch zugewiesen.



IPv4 Netzkonfiguration in Apple Mac OS X

Einstellungen -> Netzwerk
Bei IPv4 konfigurieren lässt sich auswählen, ob DHCP benutzt werden soll oder ob manuell Werte eingetragen werden.

Zusammenfassung Layer 3/IP

- Mit Hilfe von IP-Adressen wird eine Abstraktionsebene oberhalb der Hardware eingeführt. Diese erhält ein weltweites Adressschema. IP-Adressen bestehen aus einer Netzadresse und einer Adresse innerhalb des Netzes.
- Mit Hilfe von ARP finden Rechner die MAC-Adresse zu einer IP-Adresse aus demselben Netz heraus.
- Rechner können mit Hilfe der Netzmaske erkennen, ob eine Ziel-IP-Adresse in demselben Netz wie der Rechner selbst ist.
- Mit Hilfe von Routingtabellen entscheiden Rechner dann, wohin das Paket weiter geleitet wird.
- Mit den ICMP-Nachrichten werden Verwaltungs- und Steuerinformationen im Netz ausgetauscht.
- Zur korrekten IP-Konfiguration eines Rechner im Netz werden benötigt (1) die IP-Adresse des Rechners, (2) die Netzmaske und (3) die IP-Adresse des Standard-Gateways.

Motivation für Layer 3? Welche Aufgaben soll diese erfüllen?

- Die Schnittstelle von Layer 2 erlaubt uns, Daten von einer Station in einem lokalen Netz an eine andere Station im lokalen Netz zu senden.
- Offene Frage: Wie verbinden wir mehrere lokale Netze? bzw. Wie transportieren wir Daten von Station 1 zu Station 2, wenn diese *nicht* im selben LAN sind?
- Mögliche Schnittstellen für Layer 3:
  - Verbindungsorientiert, d. h. es werden in der Schnittstelle Funktionen wie „Baue Verbindung auf“, „Sende Daten über Verbindung x“, „Baue Verbindung ab“ angeboten. Beispiel: Asynchronous Transfer Mode (ATM) Netze
  - Verbindungslos, d. h. es werden in der Schnittstelle Funktionen wie „Sende Paket“ oder „Empfange Paket“ angeboten. Beispiel: Internet Protocol (IP) Netze wie bspw. das Internet

Aufgaben

- Biete einheitliches Adressierungsschema für Stationen, unabhängig von der Technik der unterliegenden (lokalen) Teilnetze.
- Bestimme einen Weg von der Quell-Station (Absender, (engl. *source*)) zur Ziel-Station (Empfänger, (engl. *destination*)).
- Grundsätzliche Lösungsideen:
  - Teile Datenstrom in einzelne Pakete (engl. *packet*).
  - Benutzer Layer 2 zum Versand der Pakete in Datenrahmen.
  - Zwischenstationen (engl. *router*) kümmern sich um die Weiterleitung der Pakete

Vorderseite

Welche speziellen Rechneradressen & Netzadressen gibt es?

Rückseite

Nicht alle Rechneradressen in einem Subnetz können tatsächlich für Rechner benutzt werden. Ausnahmen sind:

- Netzadresse: Alle Bits der Rechneradresse haben den Wert 0.
- Broadcastadresse: Alle Bits der Rechneradresse haben den Wert 1.

Ein Berechnungsbeispiel; gegeben sei:

- IP-Adresse: 100.200.66.10
- Netzmaske: 255.255.192.0

Berechnen Sie:

- Die Netzadresse:
- Die Rechneradresse:
- Die Broadcastadresse:

Private Netzadressen:

- Soll ein IP-Netz eingerichtet werden, das nicht an das Internet angeschlossen wird, dann sollten private Adressen verwendet werden.
- Router im Internet verwerfen Pakete von oder an eine dieser privaten Adressen.
- Es gibt drei private Adressbereiche:
  - 10.0.0.0 bis 10.255.255.255: Platz für insgesamt $2^{24} \approx 16$ Mio Rechner.
  - 172.16.0.0 bis 172.31.255.255: Platz für insgesamt $2^{20} \approx 1$ Mio Rechner.
  - 192.168.0.0 bis 192.168.255.255: Platz für insgesamt $2^{16} \approx 65$ Tsd Rechner.
- Soll so ein Netz nun trotzdem an das Internet angeschlossen werden, wird ein Router benötigt, der Network Address Translation (NAT) unterstützt.
  - Bei jedem ausgehenden Paket wird die Absender-IP-Adresse aus dem privaten Netzbereich durch die öffentliche IP-Adresse, die der ISP zugewiesen hat, ersetzt. Bei eingehenden Pakete muss diese Ersetzung rückgängig gemacht werden.

Adressblock und Präfix	Verwendung
0.0.0.0/8	Das vorliegende Netzwerk
127.0.0.0/8	Loopback (Lokale Station)
192.0.2.0/24	Test-Netzwerk (TEST-NET-1)
224.0.0.0/4	Multicasts
240.0.0.0/4	Reserviert für zukünftige Zwecke
255.255.255.255/32	Broadcast

Tabelle: Übersicht über ausgewählte besondere Netzwerkadressen