Auswertung: Zusatzaufgabe Kapitel 3

- Wie können Sie feststellen, welche Prozesse/Threads Ihres Betriebssystems welche Sockets bzw. TCP-Verbindungen verwenden?
- Zeichnen Sie einen TCP-Verbindungsauf- und -abbau inkl. Flags und Portnummern. Welche Sequenz- und Acknowledgement-Nummern könnten hier vergeben werden?
- Wo können Sie den „Slow Start“ und „Sägezahn“ der Congestion Control von TCP bei einem Download, den Sie gerade durchführen, sehen?

Kommunikationsnetze und -protokolle
Vermittlungsschicht

Sommersemester 2023

Bachelor AI – Hochschule Fulda

Sebastian Rieger

4 Vermittlungsschicht

4.1 Aufgaben der Vermittlungsschicht

4.2 Internet Protocol Version 4 (IPv4)

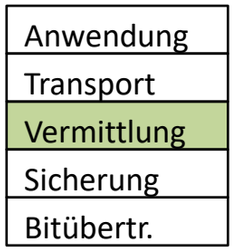
4.3 Network Address Translation (NAT)

4.4 Internet Protocol Version 6 (IPv6)

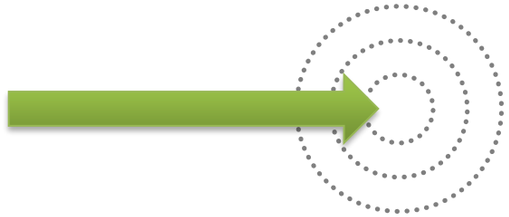
4.5 Router und Routing-Algorithmen

4.6 Hilfsprotokoll ICMP

4.7 Hilfsprotokoll ARP



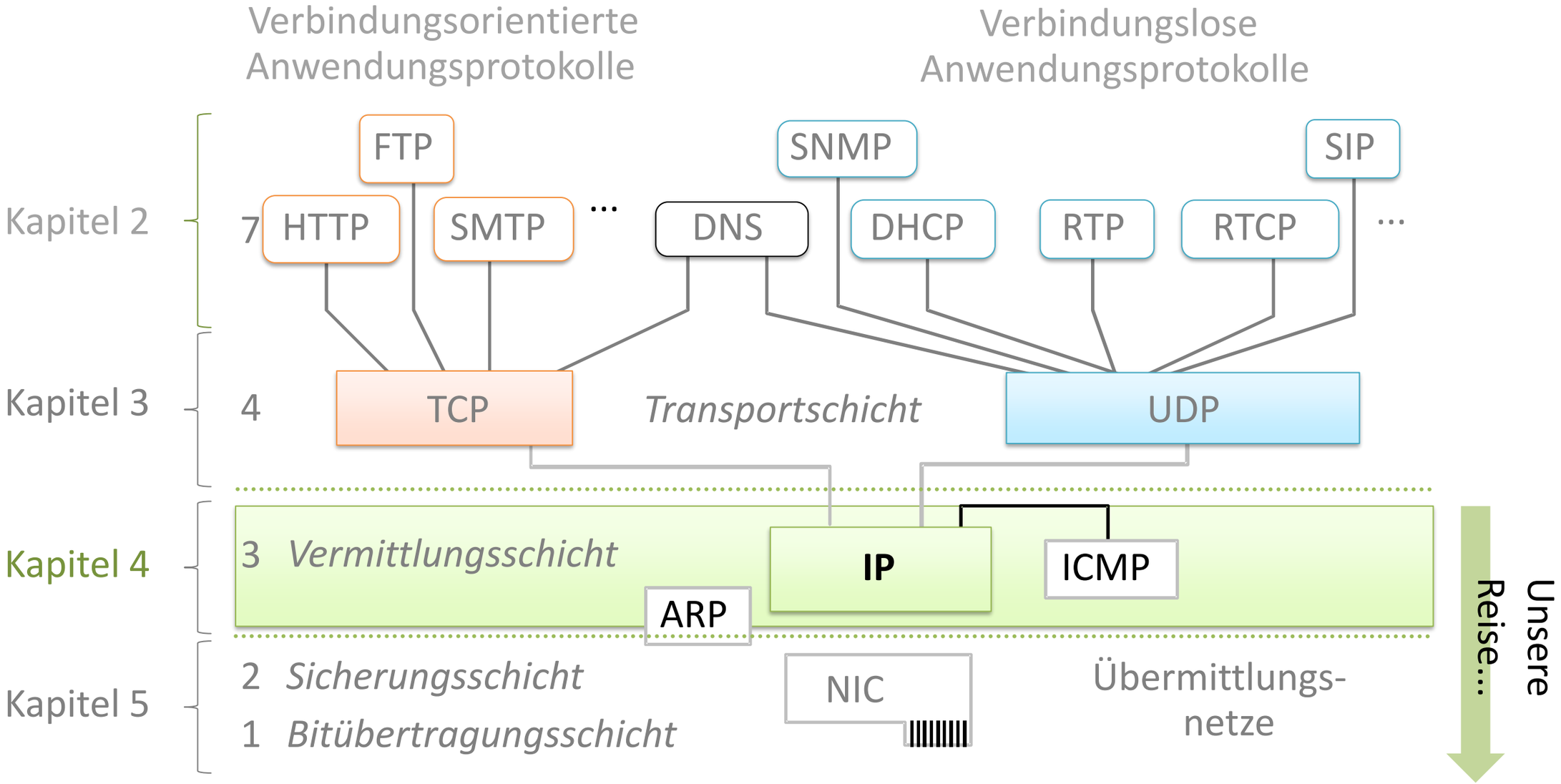
Lernziele



- Ziele
  - Aufgabe und Funktion der Vermittlungsschicht verstehen
  - Eigenschaften von IP und dessen Hilfsprotokollen kennen
  - Routing als primäre Aufgabe auf dem Layer 3 kennenlernen
- Nach diesem Kapitel sollten Sie wissen…
  - wie IP als Kernprotokoll des Internets funktioniert
  - welche Herausforderungen sich für IPv6 stellen
  - wie das Routing im Internet mit Routern und geeigneten Algorithmen realisiert wird
  - was Routing von Forwarding unterscheidet
  - wie ICMP für die Kontrolle von IP verwendet werden kann
  - wie mit ARP IP- in MAC-Adressen aufgelöst werden

Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Die Protokollfamilie TCP/IP



NIC: Network Interface Controller (Netzwerkkarte)

Quelle: Badach, Skript Kommunikationsnetze

Die Protokollfamilie TCP/IP

IP (Internet Protocol) dient als Netzwerkprotokoll und ermöglicht die Vermittlung von Paketen zwischen Endsystemen. IP stellt **verbindungslose** Paketvermittlung bereit und garantiert daher weder Bitrate, Latenz, Reihenfolge noch Fluss- bzw. Staukontrolle.

„Hilfsprotokolle“

ARP (Address Resolution Protocol) unterstützt die Adressierung und hat die Aufgabe, für eine IP-Adresse die entsprechende physikalische Adresse des Rechners im Netzwerk (in LANs die sog. MAC-Adresse) zu bestimmen.

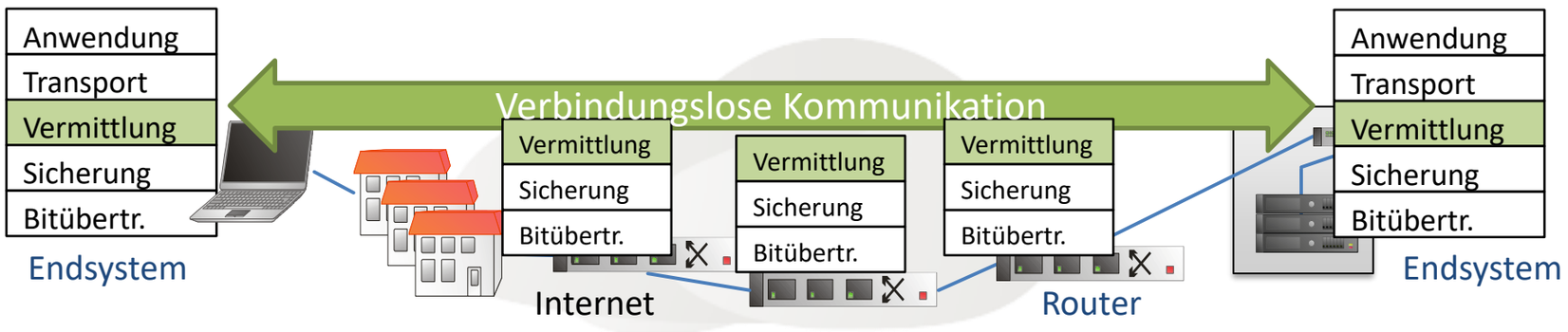
ICMP (Internet Control Message Protocol) wird für die Übertragung von Fehlermeldungen und Steuerungsinformationen verwendet.
Bemerkung: ICMP wird oft der Schicht 3 zugeordnet. Da die Nachrichten von ICMP in IP-Paketen übermittelt werden, könnte man ICMP nach den im Schichtenmodell geltenden Prinzipien zwar der Schicht 4 zuordnen, ICMP ist jedoch kein Transportprotokoll.

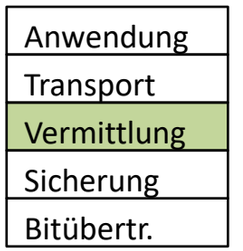
Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Quelle: Badach, Skript Kommunikationsnetze

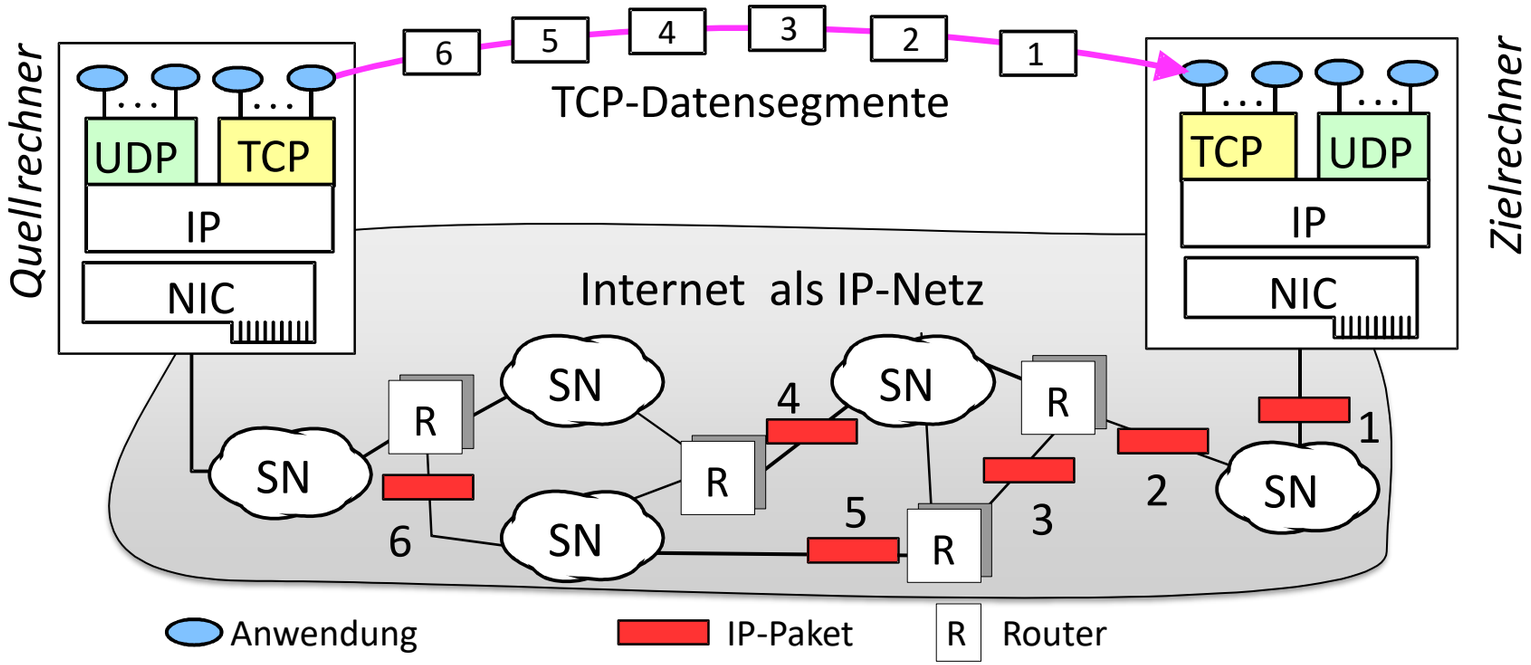
Anforderungen auf der Vermittlungsschicht in IP-Netzen

- Pakete zwischen Sender und Empfänger vermitteln
- Verpacken von Segmenten der Transportschicht in Datagramme (IP-Pakete) am Sender, Entpacken am Empfänger
- Vermittlungsschicht wird in jedem Host und Vermittler (Router) in IP-Netzen (Internet) realisiert, IP als universelle Schnittstelle:
  - Verlässt sich auf Fehler-/Flusskontrolle in Transportschicht
  - Unterstützt unterschiedlichste Links auf der Sicherungsschicht
- Router analysiert IP-Header, insb. Adressen eingehender Pakete
  - Forwarding: Weiterleitung von Paketen von Eingangs- zu Ausgangsport
  - Routing: Verwendung von Routing-Algorithmen für Wegewahl
  - Vgl. Paketvermittlung: Kein Verbindungsaufbau, keine Garantien, Pakete anhand ihrer Ziel-Adresse weiterleiten





Wie werden IP-Pakete im Internet übermittelt?



Das Internet stellt eine weltweite Kopplung von unterschiedlichen physikalischen Subnetzen (SN) dar, in denen IP verwendet wird. Daher bildet das Internet ein heterogenes IP-Netz.

Das Bild illustriert den Fall, in dem eine Folge von TCP-Datensegmenten gesendet wird. Jedes Datensegment wird als ein IP-Paket gesendet. Im Zielrechner setzt TCP die empfangenen Datensegmente wieder zusammen. Gehen einige Datensegmente bei der Übertragung verloren bzw. werden sie verfälscht, so fordert TCP (nicht IP!) vom Quellrechner ihre wiederholte Übertragung. Aufeinanderfolgende Segmente/IP-Pakete können über unterschiedliche Router geleitet werden.

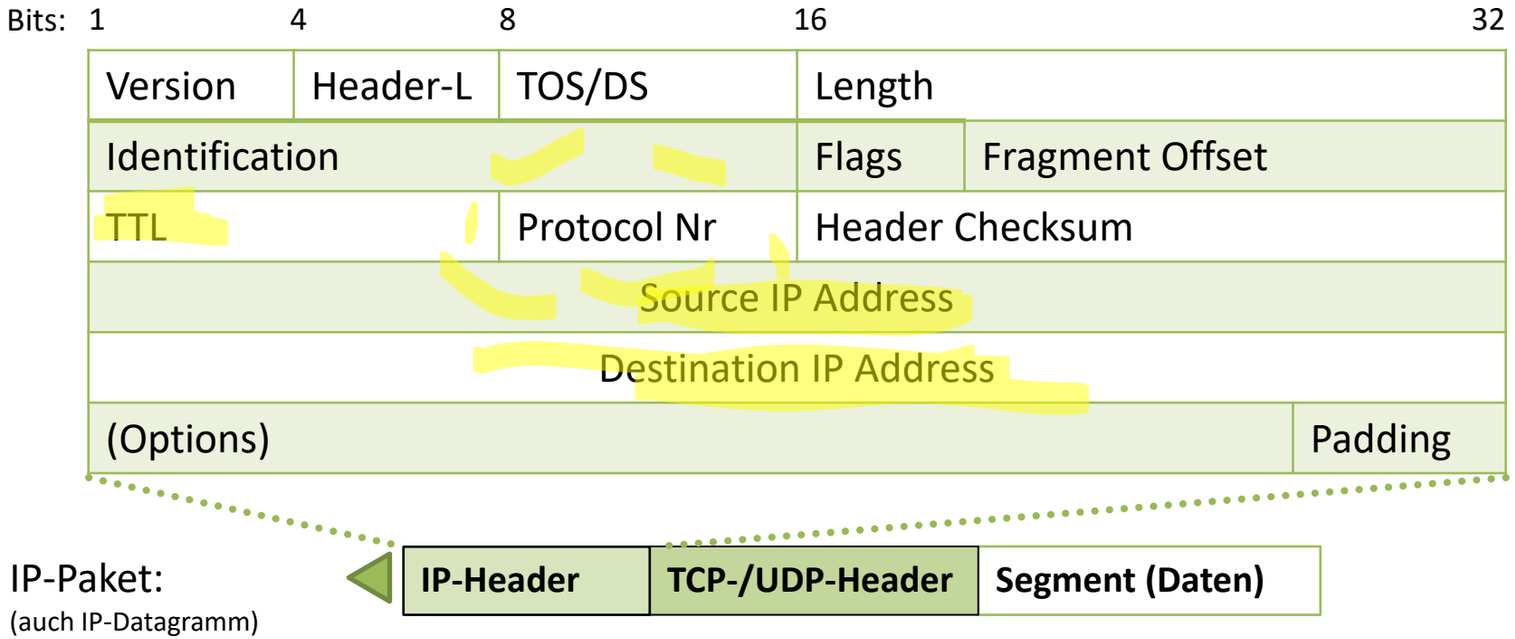
IP ist verbindungslos, dies bedeutet, dass die IP-Pakete wie Briefe bei der Post unabhängig voneinander zum Zielrechner gesendet werden. Das Internet als IP-Netz setzt sich aus einer Vielzahl von IP-Subnetzen zusammen, die mit Hilfe von Routern miteinander vernetzt sind. Ein Router leitet jedes empfangene IP-Paket unabhängig von der aktuellen Lage im Gesamtnetz weiter.

Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Quelle: Badach, Skript Kommunikationsnetze

Aufbau und Header von IPv4-Paketen

IP wird definiert in RFC 791 (9/1981)



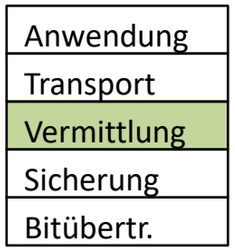
Overhead: IP-Header 20, TCP 20 = 40 Bytes (UDP nur 8 Bytes), jeweils ggf. + Layer 7-Header…

- **Version**: Beim klassischen IP-Protokoll = 4
- **Header-L**: Header Length (Header Länge) in 32-Bit-Worten
- **TOS/DS**: (Type of Service bzw. Differentiated Services): Diese Angabe ermöglicht es, IP-Pakete zu differenzieren, d.h. die Art und Weise ihrer Behandlung in Routern zu spezifizieren. Sie wird für die QoS-Unterstützung (Quality of Service) benutzt. Beispiel: Internettelefonie soll Vorrang vor Upload haben…

Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Header von IPv4-Paketen

- **Length** (Paketlänge): Gesamte Länge des IP-Pakets in Bytes
- **Identification**: Eindeutige Kennzeichnung des Gesamtpakets, wird bei der Fragmentierung von Paketen verwendet
- **Flags**: Dieses Feld enthält die Flags DF (don‘t fragment) = 1, wenn das Paket nicht fragmentiert werden darf, und MF (more fragments) = 1, wenn noch weitere Fragmente folgen.
- **Fragment Offset** (Fragmentabstand): Ist MF=1, dann gibt der Fragmentabstand die relative Position des Teilpakets in Bezug auf den Datenanfang an und ermöglicht es, mehrere Teilpakete eines IP-Pakets in der richtigen Reihenfolge zusammenzusetzen.
- **TTL** (Time to Live): Die maximale Anzahl von Routern, die das IP-Paket unterwegs zum Zielrechner durchlaufen darf. Wird in jedem Router um 1 verringert (dekrementiert). Pakete könnten ohne TTL im Internet unendlich zirkulieren (Schleife zwischen Routern).
- **Protocol Number**: Nummer des Protokolls der Schicht 4 (Transportschicht), welches im IP-Paket enthalten ist (z.B. 6 (TCP), = 17 (UDP)).
- **Header Checksum**: Header Prüfsumme zur Überprüfung des Headers auf Fehler. Wird aufgrund der TTL in jedem Router neu berechnet.



Header von IPv4-Paketen

- **Source IP Address** (Quell-IP-Adresse): IP-Adresse des Quellrechners
- **Destination IP Address** (Ziel-IP-Adresse): IP-Adresse des Zielrechners
- **Options** (Optionen): Variable Länge und optional, kann Zeitstempel, Unterstützung von Routing-Informationen (feste Route vorgeben, Route aufzeichnen) beinhalten
- **Padding** (Füllzeichen): Variable Länge, um die Optionen auf eine Länge von n*32 Bits zu ergänzen

Fragmentierung von IP-Paketen

- Links (Sicherungsschicht) haben eine maximale Begrenzung der Länge einzelner Dateneinheiten (vgl. Zwischenspeicherung/Verarbeitung)
- Größe wird als Maximum Transfer Unit (MTU) bezeichnet
- Maximale Paketlänge bei IP: 65536 Bytes, MTU im LAN typischerweise 1500 Bytes (teilweise erweiterbar auf max. ~9000 Bytes „Jumbo Frames“)
- IP-Pakete müssen an MTU der Links im Netz angepasst werden
  → Aufteilung der IP-Pakete in Fragmente → Fragmentierung

Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

IPv4-Adressen

- 32 Bit Source und Destination Address im IP-Header
  - Typische Darstellung: 4 Bytes (Oktetts) (4x8 Bit), Menschen denken dezimal ;-)

(128+64=192) (168=128+32+8)

192.168.178.1

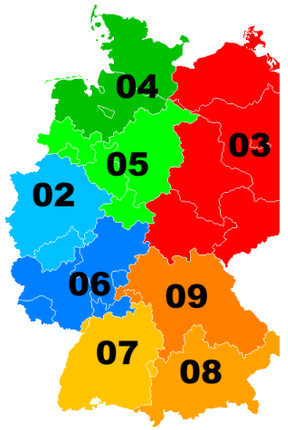
11000000.10101000.10110010.00000001

(223=255-32)

223.128.64.1

11011111.10000000.01000000.00000001

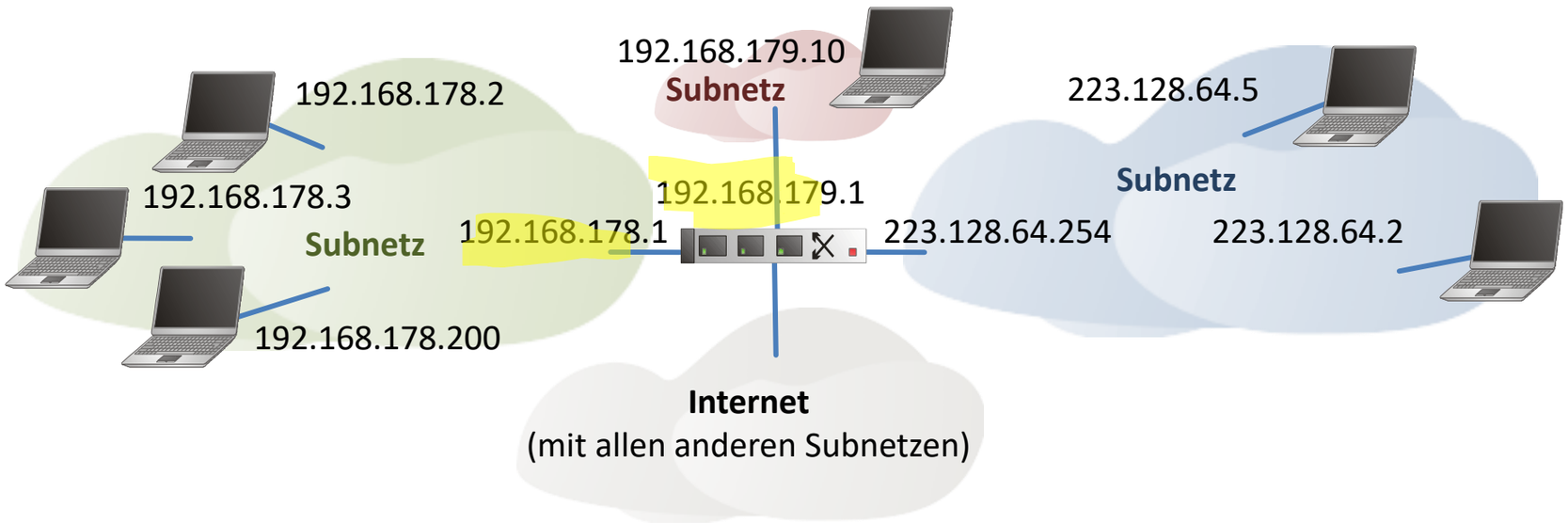
  - Jede Netzwerkschnittstelle am IP-Netz hat mindestens eine IP-Adresse
  - Grundidee: Öffentliche Adressen weltweit eindeutig
- Was genau ist eine Netzwerkschnittstelle?
  - Nächstes Kapitel (z.B. Ethernet, WLAN, …)
- Unterteilung der Bits innerhalb der Adressen:
  - Höherwertige Bits („von links“) identifizieren Netz-Anteil (Netz-ID)
  - Niederwertige Bits („von rechts“) identifizieren Host (Host-ID)
- Wo liegt die Unterteilung? Netz-ID kann als „Vorwahl“ aufgefasst werden
  - Im o.g. Beispiel könnte z.B. 192.168.178 eine „Vorwahl“ bilden, vgl. Vorwahlen beim Telefon hierarchisch 06, 066 (Großraum Fulda), 0661 (Fulda)
  - Unterteilung in „Subnetze“ (Netz-ID), zwischen denen Router vermitteln



Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

IP-Subnetze (vgl. „Vorwahlen“ bzw. genauer: „Präfixe“)

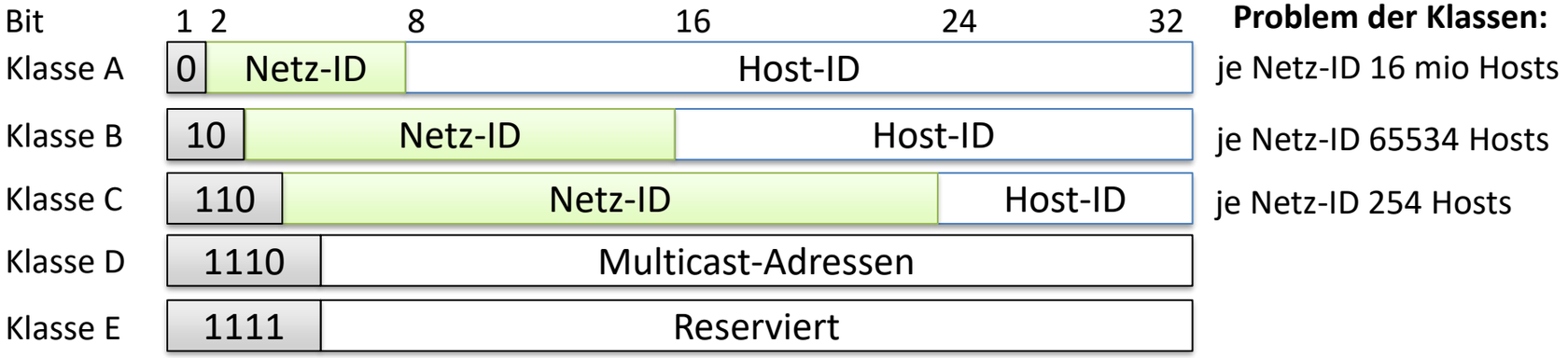
- Subnetz (Teilnetz) umfasst bei IP alle Rechner, die sich direkt erreichen können, ohne über einen Router (als Layer 3-Vermittler) zu gehen
  - Vgl. mit Vorwahl: Alle Telefonanschlüsse, die ohne Vorwahl (im gleichen Ort) erreichbar sind
- Subnetz wird auch als Präfix (Prefix) der IP-Adresse bezeichnet
- **Beispiel:** IP-Netz mit 3 Subnetzen und Internet als „Netz der Netze“ bzw. als Netz aller restlichen Subnetze



Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Wie werden Subnetze festgelegt?

- Bis Mitte 90er war Subnetz durch Klassifizierung der Adresse vorgegeben
- Problem: Großer „Verschnitt“ bzw. „Verschwendung“



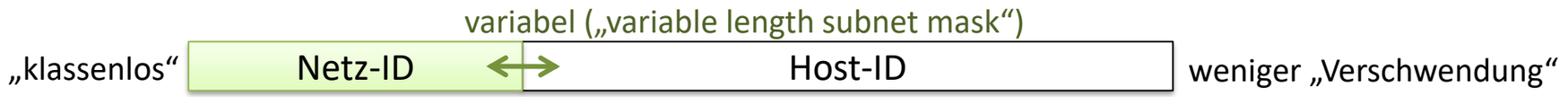
Problem der Klassen:

je Netz-ID 16 mio Hosts

je Netz-ID 65534 Hosts

je Netz-ID 254 Hosts

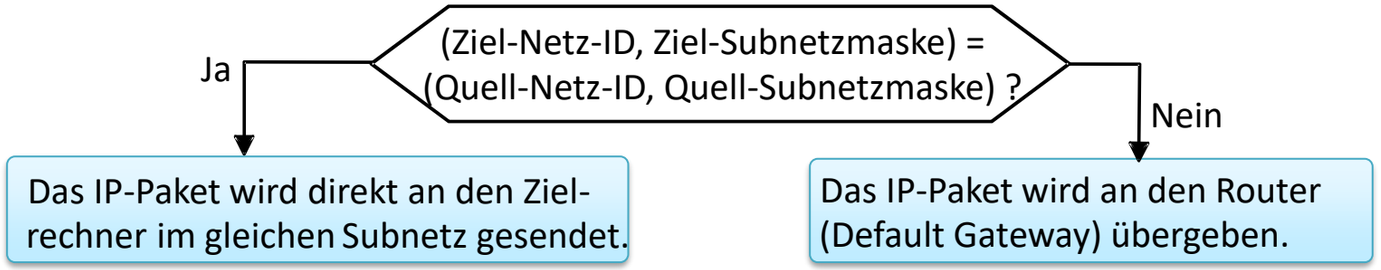
- Heute: Classless Inter-Domain Routing (CIDR), klassenlos, variable Grenze
- Grenze zwischen Netz- und Host-ID wird definiert über Subnetzmaske (Subnet Mask). Die Grenze „trennt Vorwahl von Host-Rufnummer“
- Beispiel: 192.168.178.0/24, 24 Bits Netz-ID, 8 Bits Host-ID (sog. „/24er“)
- Dezimalschreibweise wieder in 4x8 Bit, bei 24 also 255.255.255.0
- Anhand der Subnetzmaske wird entschieden, ob Ziel im lokalen Netz erreichbar ist (vgl. „die gleiche Vorwahl hat“)



Bestimmen des Ziels eines IP-Pakets mit Hilfe der Subnetzmaske

Beim Absenden jedes IP-Pakets muss im Quellrechner festgelegt werden, ob das Paket für einen Zielrechner in demselben Subnetz oder in einem anderen „Remote“-Subnetz bestimmt ist. Falls der Zielrechner sich in einem anderen Subnetz befindet, wird das IP-Paket an einen **Router (häufig als Default Gateway** bezeichnet) im lokalen Netz abgeschickt.

Bestimmen des Ziels eines IP-Pakets vor dem Absenden



Beispiel: Durch eine **logische UND**-Operation aus der Quell-IP-Adresse und der Subnetzmaske wird die **Quell-Subnetz-ID** herausgefiltert:

```
Quell-IP-Adresse:        10010101.00001011.00100000.11000011
Subnetzmaske:           ^11111111.11111111.11100000.00000000     (/19 bzw. 255.255.224.0)
Quell-Subnetz-ID:        10010101.00001011.00100000.00000000
```

Durch eine **logische UND**-Operation aus der Ziel-IP-Adresse und der Subnetzmaske wird die **Ziel-Subnetz-ID** herausgefiltert:

```
Ziel-IP-Adresse:         10010101.00001011.01000000.11000001
Subnetzmaske:           ^11111111.11111111.11100000.00000000
Ziel-Subnetz-ID:         10010101.00001011.01000000.00000000
```

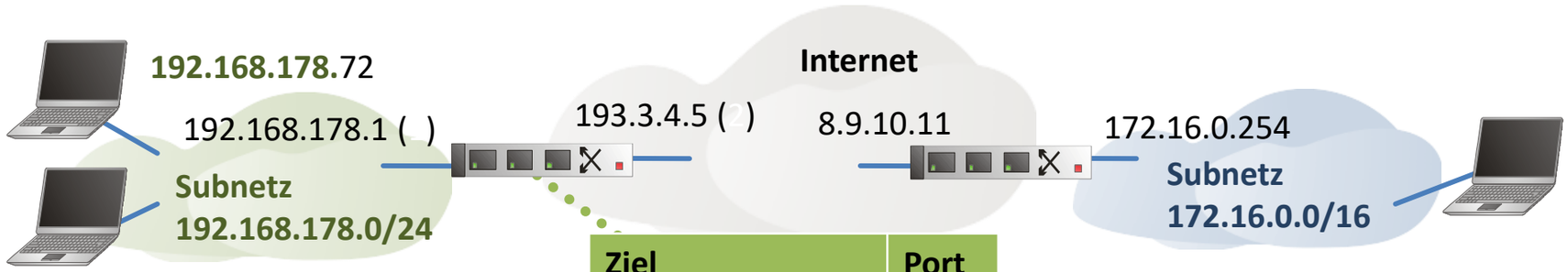
Da Quell-Subnetz-ID und Ziel-Subnetz-ID hier unterschiedlich sind, befindet sich der Zielrechner in einem anderen Subnetz.

Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Quelle: Badach, Skript Kommunikationsnetze

Einsatz von Routern

- Kommunikation innerhalb des Subnetzes erfolgt direkt (Verwendung der Sicherungsschicht, Layer 2 „MAC-Adressen“ → siehe nächstes Kapitel)
- Pakete an Ziele außerhalb des Subnetzes werden im lokalen Netz an Layer 2-Adresse (MAC-Adresse) des lokalen Routers gesendet (Default Gateway)
- Router verwenden Routing-Tabelle für Wegewahl, diese wird manuell oder durch Routing-Algorithmus verwaltet
- Routing durch „Longest Prefix Matching“, d.h. je genauer bzw. länger das passende Präfix (Subnetzmaske) ist, desto geeigneter die Route

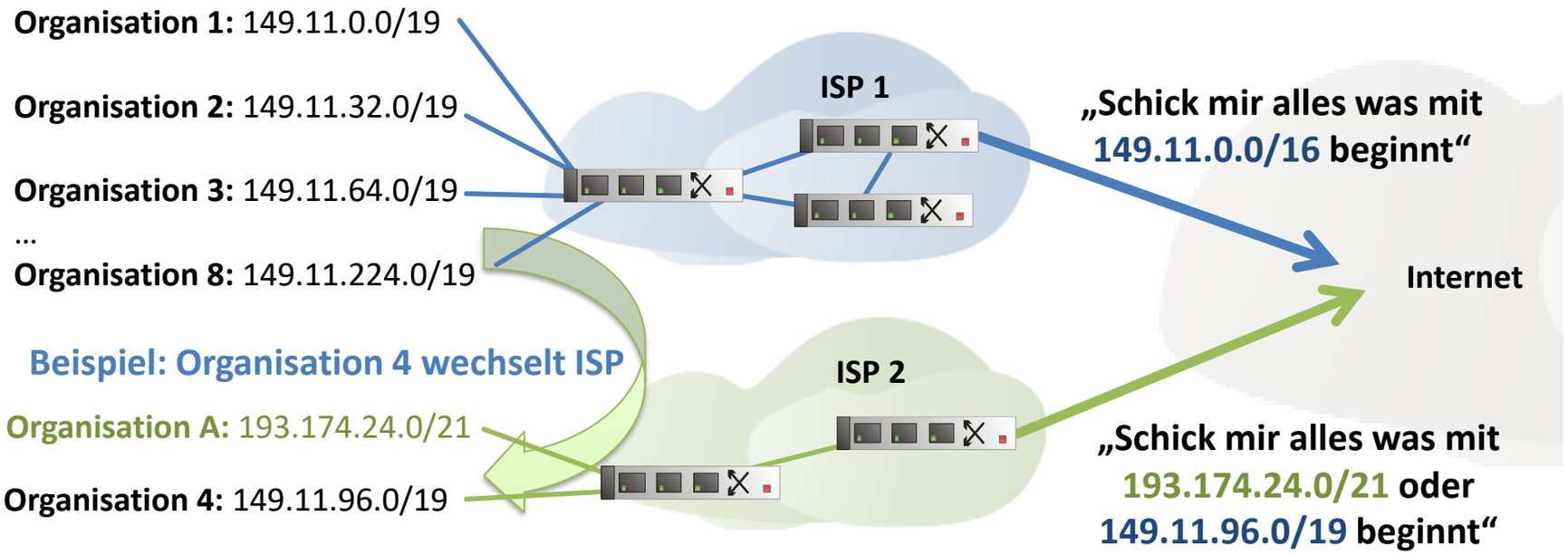


Ziel	Port
192.168.178.0/24	1
alle anderen Ziele	2

Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Route Aggregation durch Longest Prefix Matching

- Öffentliche IP-Adressen von ICANN an Regional Internet Registries (RIR), z.B. RIPE in Europa, diese vergeben an ISPs https://www.ripe.net/manage-ips-and-asns/db
- ISPs vergeben Ihren Kunden „Subnetze“ bzw. Adressbereiche, „Vorwahl“
- Hierarchische Adressierung in CIDR erlaubt Aggregation von Routen
- Route Aggregation möglich durch Zusammenfassung: „Kleinere“ Routingtabellen (~900.000 Einträge derzeit) bgp.potaroo.net/as2.0/bgp-active.html
- Dank Longest Prefix Matching auch Umzug von Subnetzen zwischen ISPs möglich, neuer ISP kann „genauere“ Route anbieten

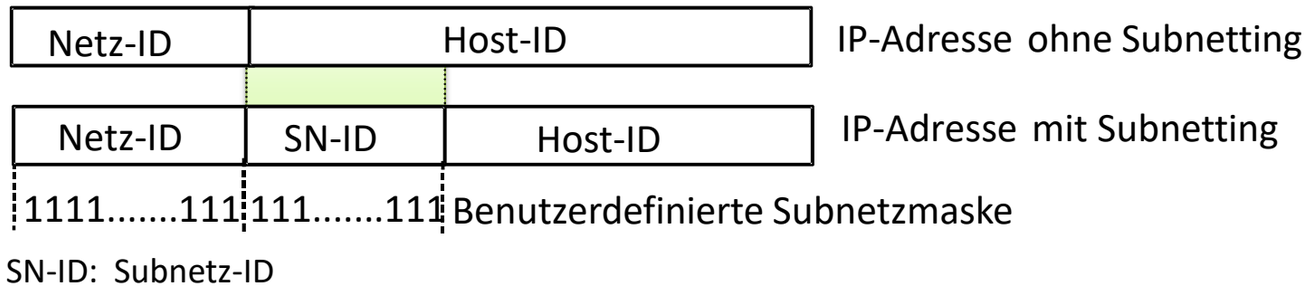


Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Unterteilung von Subnetzen mit Subnetting

Große IP-Netzwerke müssen aus organisatorischen Gründen oft in kleinere **Subnetze** unterteilt werden. Die Bildung dieser Subnetze in einem Netzwerk nach den Anforderungen einer Organisation bezeichnet man als **Subnetting**. Das Subnetting wird bereits in der Planungsphase durchgeführt und erfordert einen sorgfältig definierten **IP-Adressierungsplan**.

Struktur einer IP-Adresse mit Subnetting und benutzerdefinierter Subnetzmaske

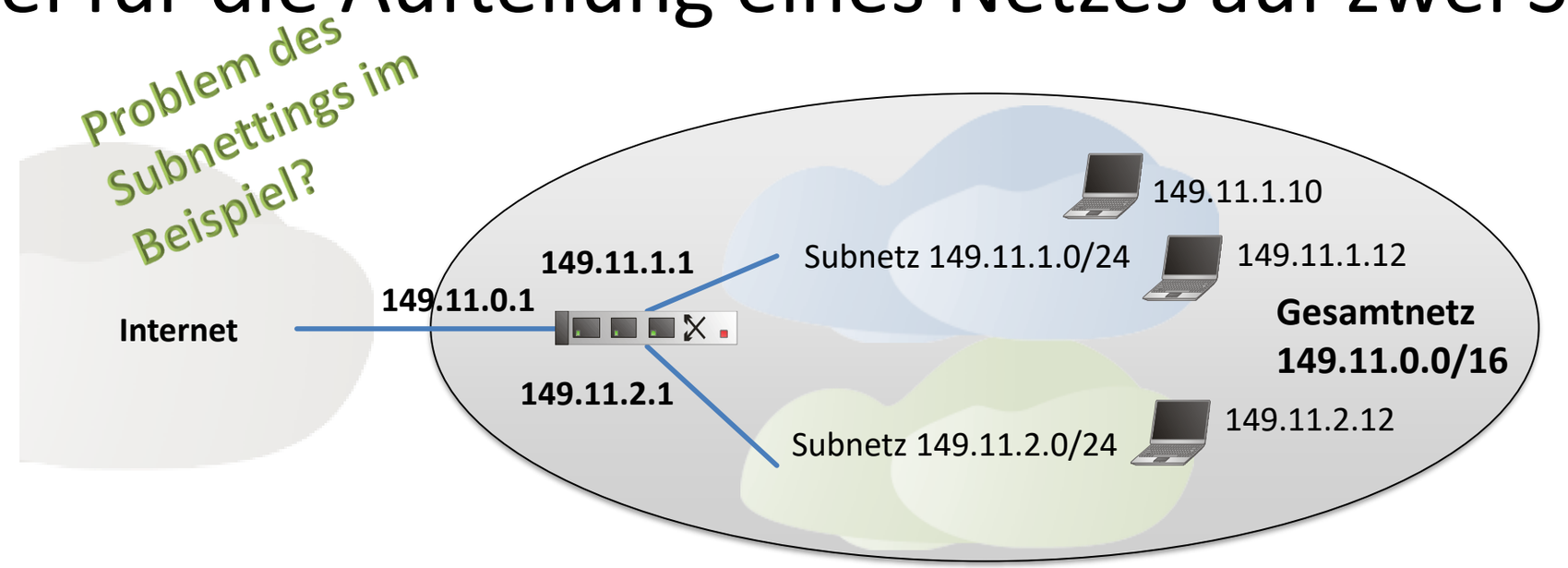


Um ein Netz in Subnetze unterteilen zu können, muss jedes Subnetz eine individuelle Identifikation (ID) verwenden. Diese Identifikation wird geschaffen, indem man aus der Host-ID die ersten Bits für die Subnetz-ID (SN-ID) nimmt und die restlichen Bits weiterhin als Host-ID nutzt. Für die Markierung von Bits aus den Teilen Netz-ID und Subnetz-ID wird die sog. **benutzerdefinierte Subnetzmaske** verwendet. Daher wird ein Subnetz (Subnet) in aller Regel auch als Netz-ID + SN-ID verstanden.

Quelle: Badach, Skript Kommunikationsnetze

Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Beispiel für die Aufteilung eines Netzes auf zwei Subnetze



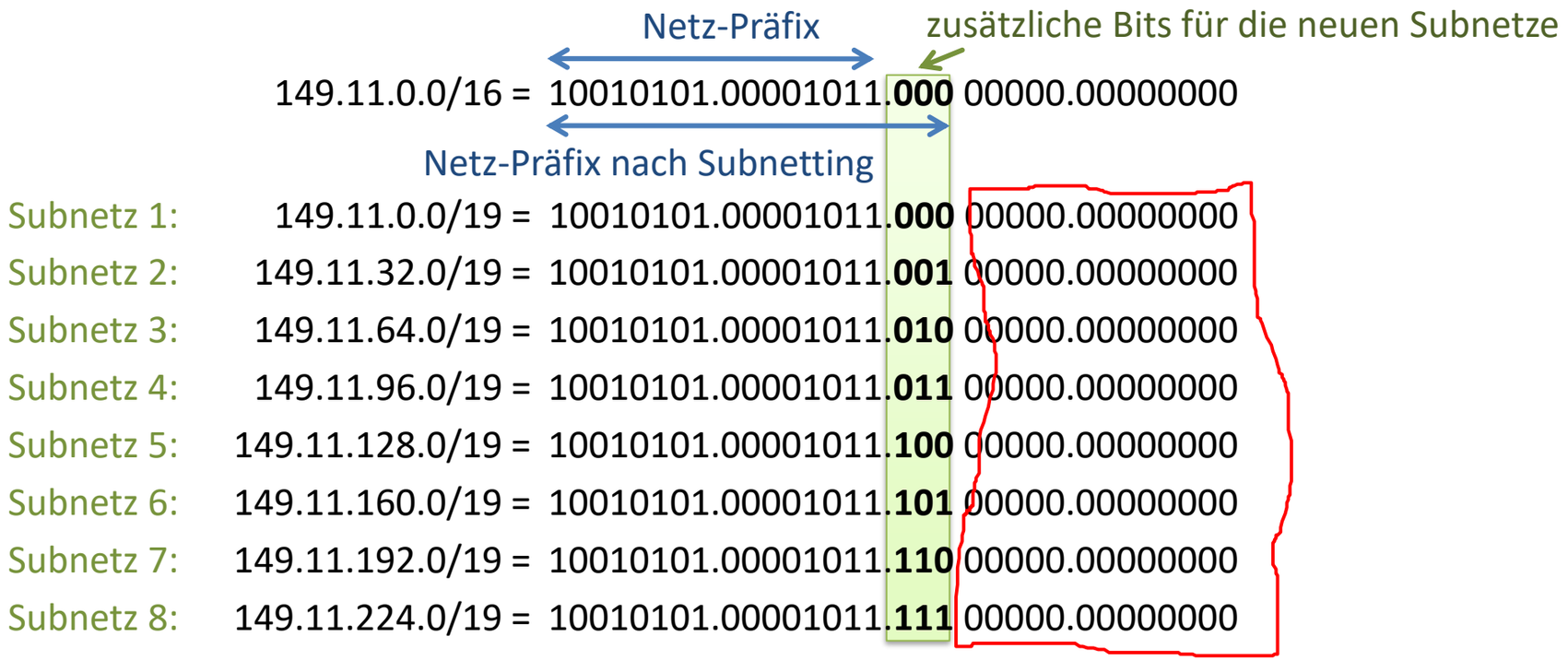
Die zwei über den Router verbundenen Subnetze haben unterschiedliche Netz- bzw. Subnet-IDs, nämlich 149.11.1.0/24 und 149.11.2.0/24. Diese dienen als Präfix im jeweiligen Subnetz.

Vorteile von Subnetzen u.a.:

- Jeder Abteilung (Organisation) kann ein getrenntes Subnetz zugeordnet werden.
- Verschiedene LANs können als unterschiedliche Subnetze definiert und dementsprechend über Router verbunden bzw. getrennt (Sicherheit) werden.
- Die Auslastung des Gesamtnetzes kann reduziert werden, indem man den Verkehr zu den einzelnen Subnetzen einschränkt (Broadcasts nur in einem Subnetz), Eingrenzung von Fehler- und Broadcast-Domäne auf ein Subnetz

Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Beispiel: Einrichtung 8 untergeordneter IP-Subnetze mittels Subnetting

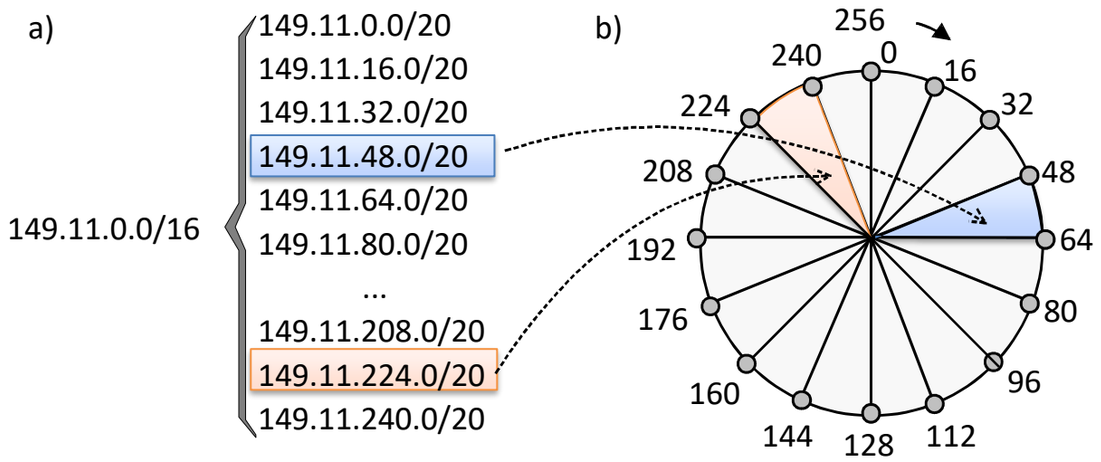


- Ursprünglicher IP-Adressblock 149.11.0.0/16: Jeweils 16 Bit für Netz- und Host-IDs.
- Um 8 zusätzliche Subnetze binär zu nummerieren, sind 3 Bits nötig. Daher wird das Netz-Präfix um 3 Bits erweitert. Die Subnetz-Präfixlänge beträgt somit 19 Bits.
- In jedem Subnetz bleiben 13 Bits für Hosts: $2^{(32-19)}-2 = 8190$ Rechner adressierbar.
- Die zwei Adressen, die abgezogen werden, sind die (erste) (Sub-)Netzadresse (z.B. für Subnetz 2 149.11.32.0) und die (letzte) Broadcast-Adresse zum Versenden von Nachrichten an alle Hosts im Subnetz (bei Subnetz 2 z.B. 149.11.63.255).

Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Weiteres Beispiel für Subnetting

Beispiel: Im Netzwerk mit der IP-Vorwahl **149.11.0.0/16** sollen 14 Subnetze eingerichtet werden. Um die 14 Subnetze binär nummerieren zu können, muss die 16 Bit lange Netzmaske um 4 Bits verlängert werden. Somit ist die Subnetzmaske der neuen Subnetze 20 Bits lang. Daher wird der /16-Adressblock 149.11.0.0/16 auf 16 /20-Adressblöcke aufgeteilt.



Der /16-Adressblock 149.11.0.0/16 wird nun in 16 gleichgroße Bereiche aufgeteilt. Dies könnte man sich wie **eine Torte** vorstellen, die auf gleiche 16 Teile geschnitten wird. Der Umfang dieser Torte beträgt $2^8 = 256$ und sie entspricht dem dritten Oktett bei der Netzmaske mit 16 Bits. Die Länge des Bogens eines „Tortenstücks“ entspricht der Verlängerung der Netzmaske um 4 Bits zur 20 Bits langen Subnetzmaske. Somit ist die Länge des Bogens eines „Tortenstücks“ gleich $2^4 = 16$. Jedes „Tortenstück“ stellt hier einen /20-Adressblock 149.11.**x**.0/20 dar, wobei **x** = 0, 16, 32, ..., 240.

Quelle: Badach, Skript Kommunikationsnetze

Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Spezielle IP-Adressen

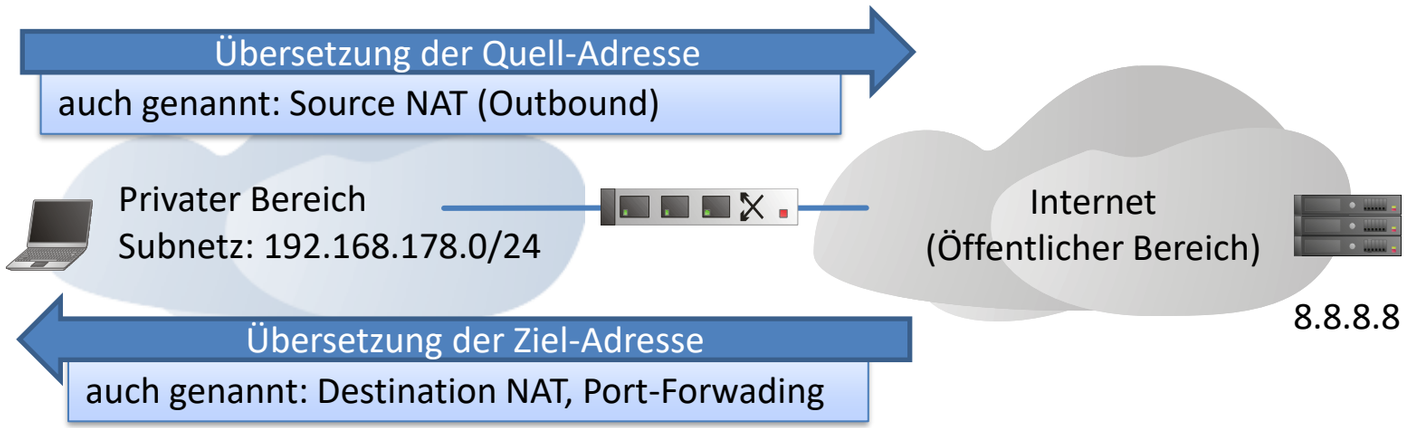
Spezielle IP-Adresse	Bedeutung	Beispiel
Alle Bits 0	als Quelle: Host in diesem Netz, als Ziel: alle Netze (z.B. Default Route)	**0.0.0.0**
Alle Bits 1	Lokaler IP-Broadcast	**255.255.255.255**
Alle Bits der Host-ID 0	Subnetz	192.168.100.**0**
Alle Bits der Host-ID 1	Gerichteter Broadcast	192.168.100.**255**
100.64.0.0/10	Carrier-Grade-NAT	**100.64**.1.1
127.0.0.0/8	Loopback/Local	**127**.0.0.1, 127.0.0.2, …
10.0.0.0/8	Privater IP-Adressbereich Class A	**10**.174.26.117
172.16.0.0/12	Privater IP-Adressbereich Class B	**172.16**.19.1
192.168.0.0/16	Privater IP-Adressbereich Class C	**192.168**.0.1
169.254.0.0/16	Automatische Konfiguration von Rechnern (APIPA)	169.254.1.1
224.0.0.0/4	Multicast (Gruppenadresse)	**224**.0.0.2 (alle Router im Subnetz)
192.0.0.0/24, 240.0.0.0/4	Reserviert	
192.0.2.0/24	Reserviert für Beispieladressen	
192.88.99.0/24	IPv6-Übergang (6to4 anycast)	
198.18.0.0/15	Netzwerktests	

Quelle: IANA

Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Network Address Translation (NAT) Klassifizierung

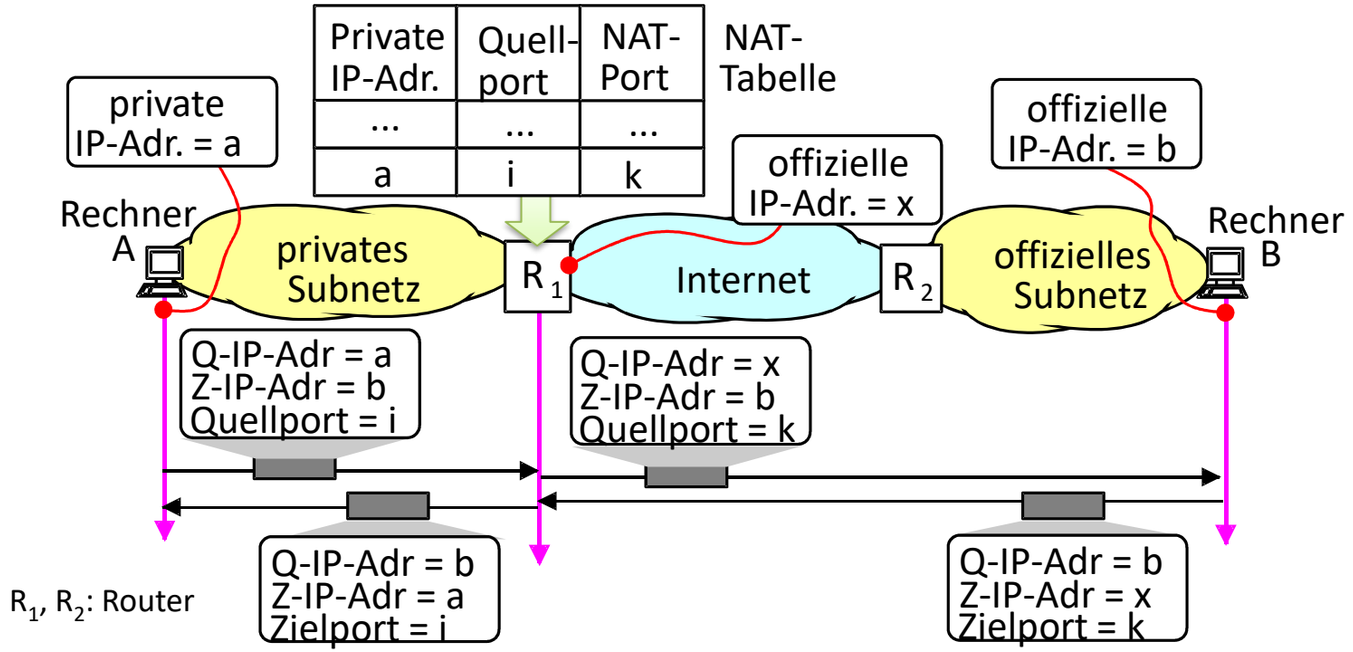
- Als IPv4-Adressen knapp wurden, kam Idee auf, in LANs private, nicht öffentliche Adressen einzusetzen (dies spart öffentliche Adressen).
- Pakete mit privaten IP-Adressen (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) werden im Internet allerdings von jedem ISP verworfen
- Network Address Translation (NAT) wurde daher eingeführt, um zwischen diesen internen, privaten Adressen und externen (öffentlichen bzw. public) IP-Adressen zu übersetzen.
- Hierbei sind mehrere Richtungen der Übersetzung möglich:



- Beispiel: Heimnetz, eine einzige offizielle IP-Adresse vom ISP
- Viele verschiedene Arten von NAT:
  - Basic NAT, Port-based NAT, Full Cone, Port-restricted Cone , Symmetric NAT, …
- Häufigster Fall: Port-restricted Cone NAT, realisiert zusätzliche „Firewall“ Funktion, da private Adressen aus dem Internet nicht erreichbar

Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Grundlegende Funktionsweise von Port-based NAT



Im Beispiel steht dem privaten Subnetz nur eine einzige offizielle IP-Adresse zur Verfügung, über die Tausende von Kommunikationsbeziehungen nach Außen gleichzeitig verlaufen können. Alle privaten IP-Adressen aus dem privaten Bereich werden im Router auf diese einzige IP-Adresse abgebildet.

Kommuniziert Rechner A mit dem Internet, wird für das Quell-Socket a,i ein neues Quell-Socket x,k am Router reserviert und in der NAT Tabelle eingetragen. Die Zuordnung erhält einen Timeout. Antworten, die an x,k adressiert werden, übersetzt der Router 1 beim Eintreffen in das Ziel-Socket a,i.

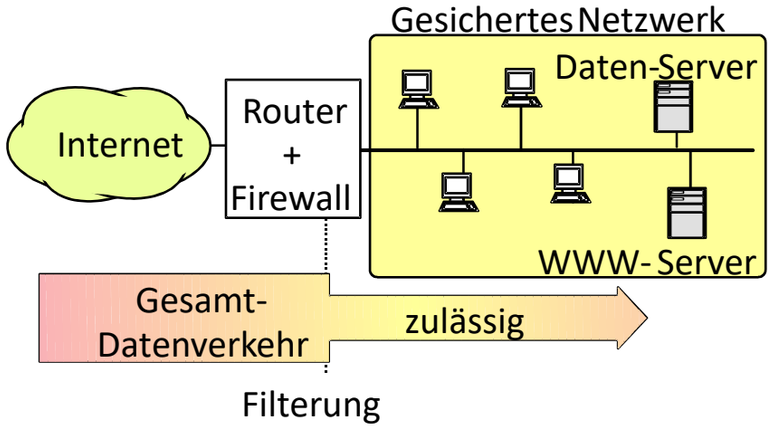
In der Regel akzeptiert der Router nur dann die Antwort des externen Rechners X, wenn zuvor eine, Anfrage gesendet wurde. Dies realisiert einen Schutz („Firewall“) für die Rechner im privaten Subnetz vor Zugriffen (und Angriffen). Wird stattdessen ein Port-Forwarding eingesetzt, sind auch direkt Anfragen von außen ohne vorherige Anfrage des internen Rechners erlaubt (z.B. Server hinter NAT).

Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Quelle: Badach, Skript Kommunikationsnetze

Firewalls

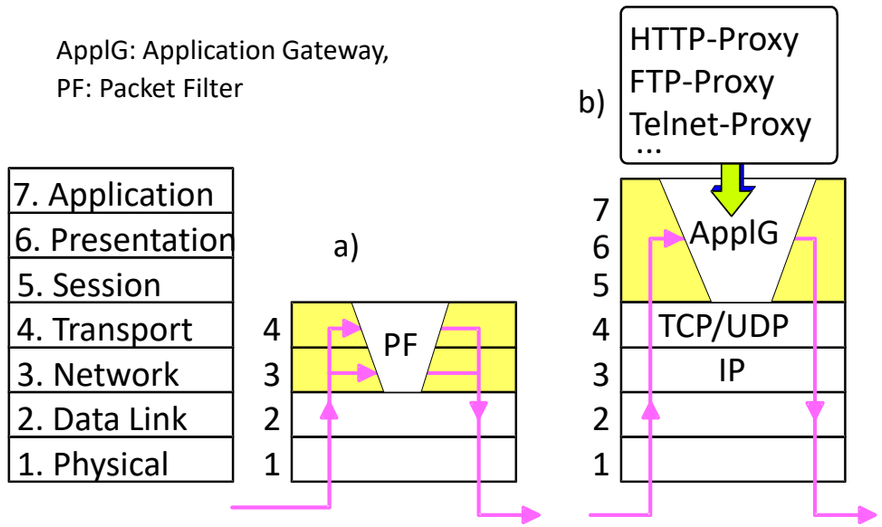
Der Begriff **Firewall** kommt aus der Architektur und kann als eine Art **Brandschutzmauer** angesehen werden. Eine Firewall hat daher die Aufgabe, das eigene Netzwerk gegen Eindringlinge bzw. Angriffe aus dem Internet zu schützen.



Im Allgemeinen gibt es zwei grundlegende Firewall Komponenten:

- **Packet Filter** (z.B. mit Stateful Packet Inspection) und
- **Application Gateway** (Vermittler auf der Anwendungsschicht – Layer 7).

Eine Firewall als Packet Filter analysiert und kontrolliert die Pakete innerhalb der Schichten 3 und 4. Die Daten oberhalb der Transportschicht werden in der Regel vom Packet Filter nicht analysiert.



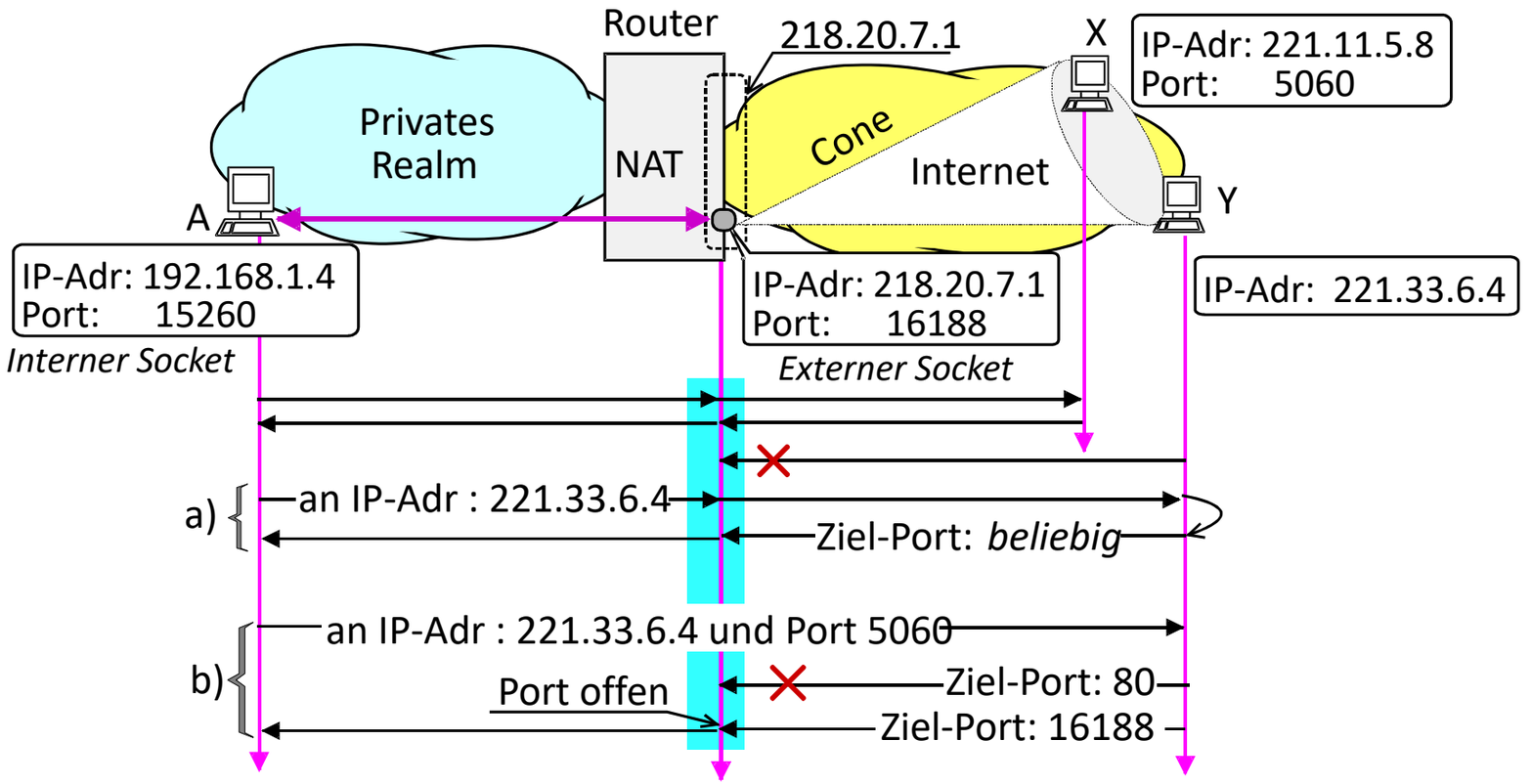
Eine Firewall als **Application Gateway** analysiert und kontrolliert die Daten innerhalb der Schichten 5, 6 und 7, d.h. auf dem Application Level. Application Gateway bilden die Funktion eines **Proxy (deutsch: Stellvertreter)**. Der Proxy trennt in diesem Fall das geschützte Netzwerk von der „Außenwelt“ sowohl logisch als auch physikalisch.

Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Quelle: Badach, Skript Kommunikationsnetze

Prinzip von Port-restricted Cone NAT

Bei NAT mit einer **Firewall-Funktion**, bei der der externe Socket von der Ziel-IP-Adresse unabhängig ist, kann es sich handeln um: a) **Restricted Cone NAT** bzw. b) **Port-restricted Cone NAT**.



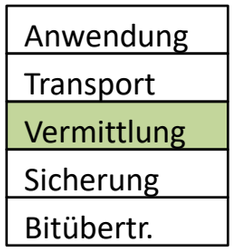
Bei **Port-restricted Cone NAT** können nur IP-Pakete von einem Port eines bestimmten Rechners am Internet in ein privates Realm weitergeleitet werden. Ein Paket von dem Port *j* im externen Rechner X wird nur dann nicht blockiert und an den internen Socket im Rechner A weitergeleitet, falls bereits zuvor ein IP-Paket vom Rechner A an den Port *j* im Rechner X abgeschickt wurde. Daher werden bei Port Restricted Cone NAT nur die IP-Pakete von einem vorher „kontaktierten“ Socket nicht blockiert und Antworten entsprechend zum internen Socket im privaten Realm weitergeleitet.

Quelle: Badach, Skript Kommunikationsnetze

Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Grenzen von NAT

- Ports können max. 16 Bit umfassen
  - Z.B. bei UDP also „nur“ ~65000 „Verbindungen“ über eine IP nach außen
- NAT verletzt sog. „end-to-end“ Internet Design Principle
  - Router sollte nur Layer 3 betrachten und keine Zustände speichern (Fehlertoleranz etc.)
- Problem: NAT Traversal
  - Um Server im privaten Netz von außen erreichbar zu machen: Port-Forwarding (wird allerdings statisch konfiguriert)
  - NAT bildet daher Herausforderung für Anwendungen im LAN, die bei Bedarf von außen erreichbar sein müssen
  - Universal Plug and Play (UPNP): Anwendungen im LAN können Port nach innen bei Bedarf öffnen
  - Bei großer Zahl von externen Anfragen von außen UPNP zu aufwändig, z.B. bei Peer-to-Peer (P2P) Anwendungen (Skype, BitTorrent, …)
  - Lösungen: Externes Relay, NAT-Traversal-Techniken → Lehrveranstaltung Multimedia-Kommunikation
- Bessere Lösung für Adressknappheit bei IPv4: IPv6!



Ziele für IP Version 6 (IPv6)

Vergrößerung des IP-Adressraums, da IPv4-Adressen zur Neige gehen…

IPv6-Adressen haben eine Länge von 128 Bits (4 mal so lang im Vergleich zu IPv4-Adressen). Den öffentlichen IPv4-Adressen entsprechen bei IPv6 die globalen Unicast-Adressen. Sie werden jedoch nun so strukturiert, dass sie der „Lokation“ eines Netzes auf der Erdkugel entsprechen. Unique Local Unicast Adressen bei IPv6 entsprechen den privaten IPv4-Adressen. Außerdem: Direkte Unterstützung von Multicasting.

Verbesserung der Header-Struktur

Die Struktur des Headers im IPv6-Paket wurde gegenüber dem Header im IPv4-Paket wesentlich verbessert. Es wurde eine stärkere Unterteilung zwischen notwendigen Angaben und optionalen Angaben vorgenommen. Keine Checksum und Fragmentierung im Netz mehr, entlastet Router.

Unterstützung einer Autokonfiguration

Die Installation eines Rechners am Netzwerk mit IPv6 soll weitgehend nach dem Prinzip **Plug-and-Play** erfolgen. Hierfür wurden ICMP zu ICMPv6 erweitert, DHCP zu DHCPv6 und statt ARP das Neighbor Discovery Protocol (NDP) eingeführt.

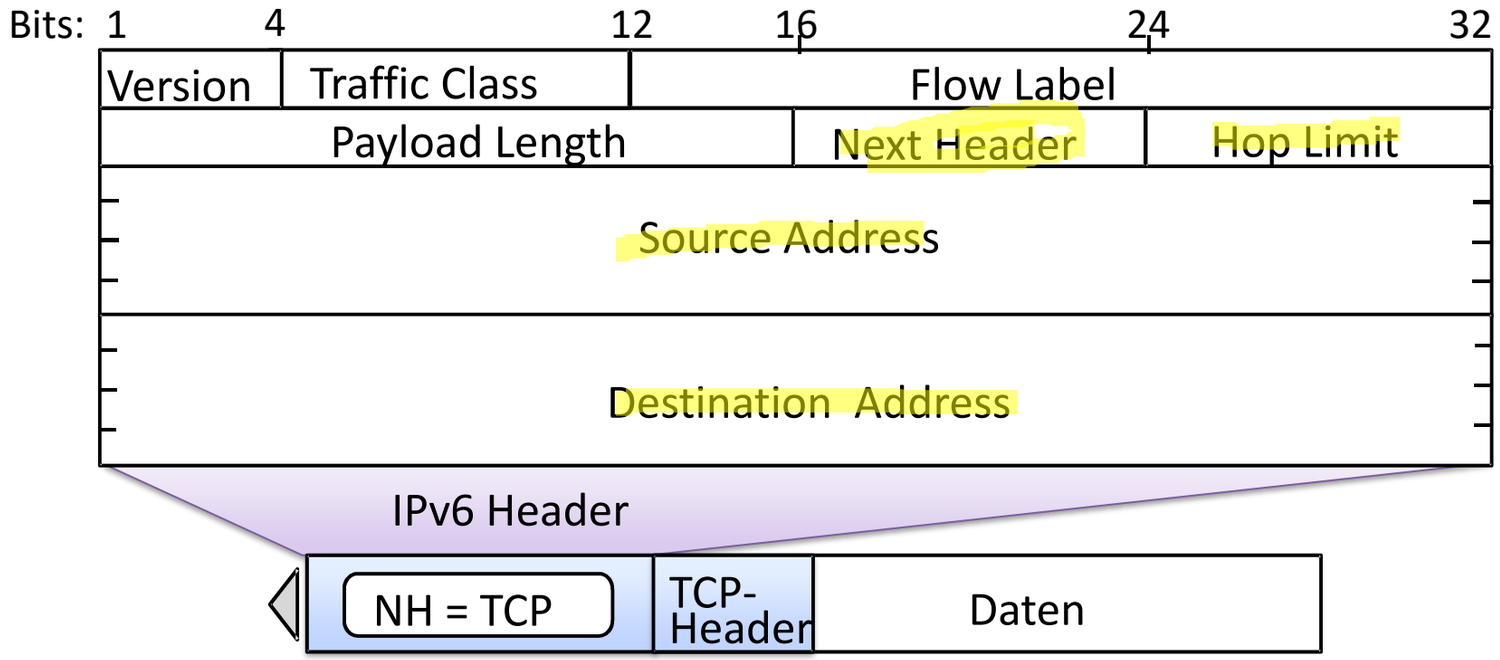
Verbesserung der Sicherheit

Hierfür wurden folgende zwei Extension Header vorgesehen: **Encapsulation Security Payload** und **Authentication Header**. Diese beiden Extension Header können auch beim IPv4 eingesetzt werden. Dies hat zur Entstehung von **IPsec** (*IP Security*) geführt.

Quelle: Badach, Skript Kommunikationsnetze

Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Header-Struktur bei IPv6 (RFC 2460 – aus dem Jahr 1998 ;-))



NH: Next Header

Der IPv6-Header stellt eine deutliche Vereinfachung und Erweiterung gegenüber dem IPv4 dar.

Um **Quality of Service** (QoS) zu unterstützen, ermöglicht das Feld **Traffic Class** dem Absender seinen Paketen eine Priorität zu vergeben. Hop Limit übernimmt die Funktion der Time to Live in IPv4.

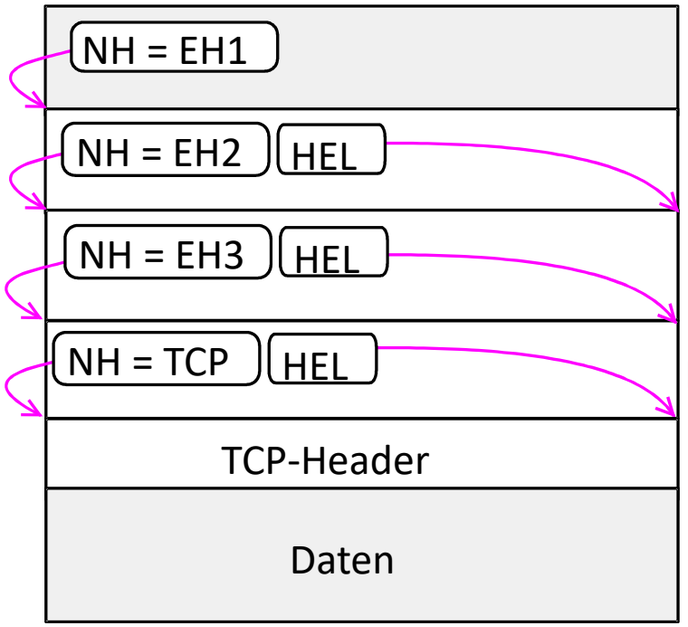
Flow Label stellt die zufällig gewählte Identifikationsnummer einer virtuellen Ende-zu-Ende-Verbindung (z.B. TCP-Verbindung) dar. Diese Angabe kann genutzt werden, um Pakete zu kennzeichnen, die eine besondere Behandlung im Übermittlungsnetz benötigen.

Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Quelle: Badach, Skript Kommunikationsnetze

Erweiterungs-Header (Next Header)

Prinzip der Erweiterung des IPv6-Headers



Beispiele für Extension Header:

- Routing
- Fragment (Fragmentierung nur noch an Quelle erlaubt, keine Fragmentierung im Netz mehr)
- Hop-by-Hop, Mobility, Security (AH/ESP)…

EH: Extension Header, NH: Next Header, HEL: Hdr Ext Len = Header Extension Length

Das Feld **Next Header** im IPv6-Header nimmt eine zentrale Rolle bei der Strukturierung der IPv6-Pakete ein. Next Header weist darauf hin, welche Daten direkt nach dem IPv6-Header folgen.

Hierbei sind zwei Fälle zu unterscheiden, entweder folgt direkt ein TCP- bzw. UDP-Header mit den dazugehörigen Daten oder es folgt zuerst ein weiterer **Erweiterungs-Header**, der wiederum ein Feld Next Header enthält.

Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Quelle: Badach, Skript Kommunikationsnetze

Adressstruktur von IPv6

Beim IPv6 unterscheidet man zwischen folgenden Kategorien von Adressen:

- **Unicast-Adressen**,
- **Multicast-Adressen (im Vergleich zu IPv4: kein Broadcast mehr unterstützt)** und
- **Anycast-Adressen**.

Die IPv6-Adressen haben dabei folgende Form:
X:X:X:X:X:X:X:X
wobei jedes X einen 16-Bit-Block in hexadezimaler Schreibweise darstellt.

Eine IPv6-Adresse kann also folgendermaßen aussehen:
ADCF:0005:0000:0000:0000:0000:0600:FEDC

Führende Nullen können weggelassen werden. Es ist erlaubt, z.B. 0 statt 0000, 5 statt 0005, 600 statt 0600 zu schreiben. Dadurch lässt sich die bereits erwähnte Adresse nun in einer *kompakten Form* wie folgt darstellen:
ADCF:5:0:0:0:0:600:FEDC

Ebenso können mehrere aufeinanderfolgende **16-Bit-Null-Werte** unterdrückt und durch **„::“** abgekürzt werden. Eine korrekte Schreibweise für die eben gezeigte Adresse wäre damit auch:
ADCF:5::600:FEDC

Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Quelle: Badach, Skript Kommunikationsnetze

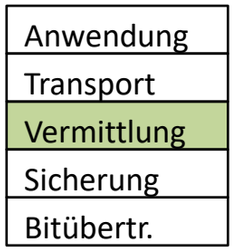
Aufteilung des IPv6-Adressraums

Typen von IPv6-Adressen und zugehörige Präfixe

IPv6-Präfix	Verwendung
::/128	Reserviert für „Unspecified Address“
::1/128	Reserviert für Loopback Address
::/96	IPv4-compatible IPv6 Address (veraltet)
::ffff:0:0/96	IPv4-mapped Address
64:ff9b::/96	Mapping von IPv4 nach IPv6 nach RFC6052
2000::/3	Global Unicast
2001::/32	TEREDO (IPv6-Migration)
2002::/16	6to4 (IPv6-Migration)
fc00::/7	Unique Local Adresses (vgl. private IPv4-Adressen)
fe80::/10	Linked-Scoped Unicast Adresses
ff00::/8	Multicast

https://www.ripe.net/participate/member-support/lir-basics/ipv6_reference_card.pdf

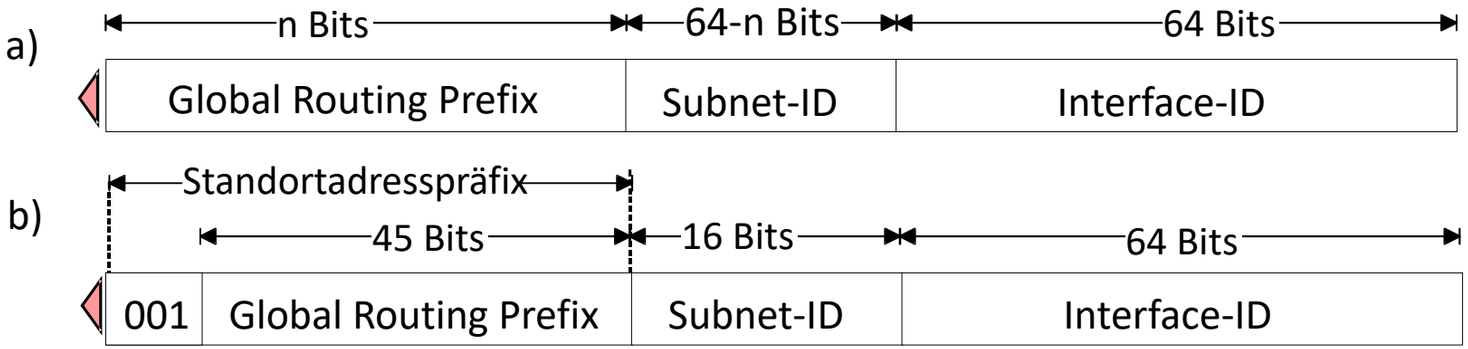
Die Aufteilung des IPv6-Adressraums wird von der **IANA** (*Internet Assigned Numbers Authority*) koordiniert, siehe http://www.iana.org/assignments/ipv6-address-space



Global Unicast-Adressen bei IPv6

Diese IPv6-Adressen haben das Präfix **001** (binär) bzw. **2000::/3** (hexadezimal). Das Adresspräfix für alle momentan öffentlich zugewiesenen globalen IPv6-Adressen lautet daher 2000::/3.

Aufbau von globalen Unicast-Adressen:
a) allgemeine Struktur (nach RFC 3587), b) Adressen mit Präfix 2000::/3



Global Routing Prefix (**GRP**) kann hierarchisch strukturiert werden und wird verwendet, um die Route zu einer bestimmten Organisation anzugeben.

Als **Subnet-ID** wird die Identifikation eines Subnetzes innerhalb einer Organisation angegeben. Subnet-ID kann weiter strukturiert werden, um eine Subnetz-Hierarchie innerhalb eines physikalisch großen Netzes adressieren zu können, sodass man daher von ***privater Struktur*** sprechen kann.

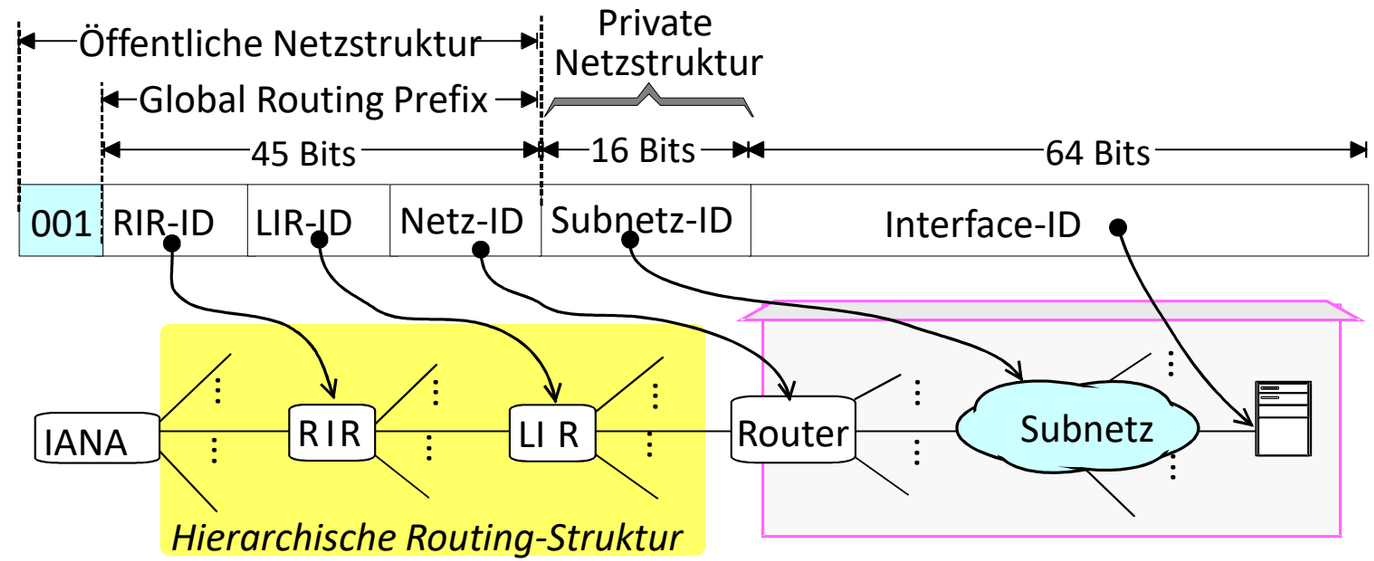
Interface-ID dient als Identifikator eines physikalischen Interfaces in einem Rechner, Router etc. Da die Interface-ID (zunächst war hier die komplette MAC-Adresse gedacht) einen Rechner eindeutig identifiziert und so ein Tracking erlaubt, wurden **Privacy Extensions** eingeführt. Hierbei erhält der Rechner zusätzlich eine zweite zufällig gewürfelte temporäre IPv6-Unicast-Adresse, die regelmäßig gewechselt und für ausgehende Verbindungen genutzt wird.

Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Quelle: Badach, Skript Kommunikationsnetze

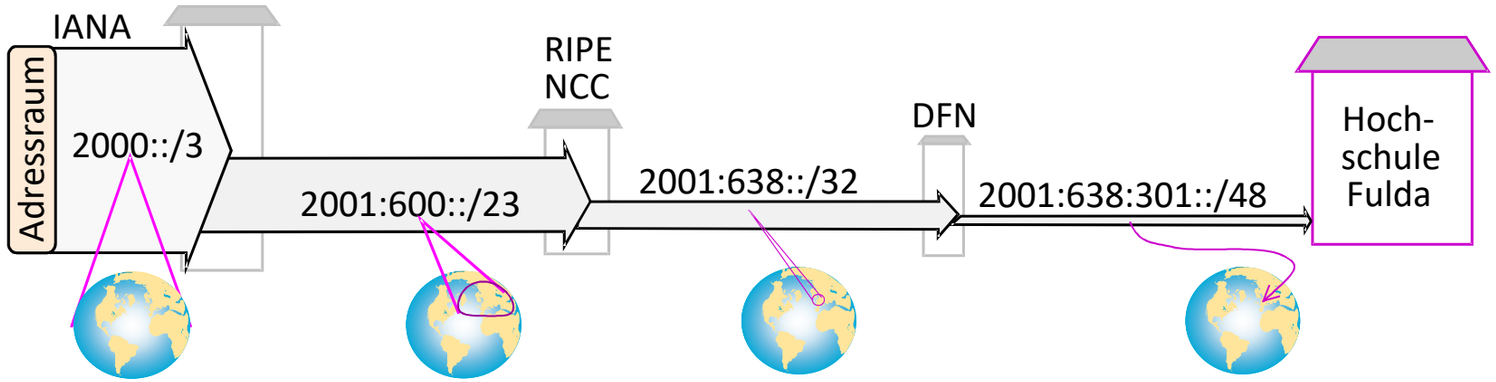
Unicast-Adressen bei IPv6

Prinzip der Strukturierung des Global Routing Prefix (GRP)



RIR: Regional Internet Registry, LIR: Local Internet Registry

Beispiel für die Aggregation von Routen mit Hilfe von GRP



Quelle: Badach, Skript Kommunikationsnetze

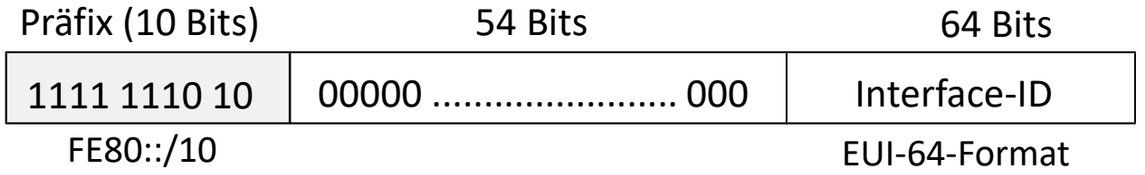
Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Unicast-Adressen von lokaler Bedeutung

Bei IPv6 werden folgende zwei Arten von Unicast-Adressen definiert, die lokale Bedeutung haben:

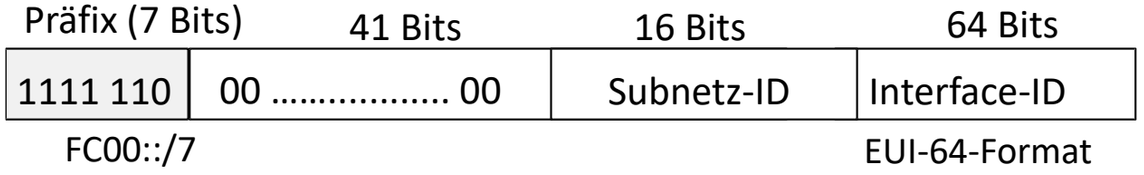
- **Link Local Address** und
- **Unique Local Address (früher als Site Local Adress bezeichnet)**

Struktur von Link Local Addresses



Bei **Link Local-Addressen** - kurz **LLA** genannt - handelt es sich um eine unstrukturierte Adresse mit dem Präfix **FE80::/10**. Da LLA keine Identifikation von Subnetzen enthalten, können sie nur innerhalb „isolierter“ IPv6-Subnetze, die man auch als **Links** bezeichnet, verwendet werden. Da die LLA nur pro Link eindeutig sind, wird vom Betriebssystem häufig eine Interface-ID mit % angehängt (z.B. %4, %eth1). Die LLA werden von Routern nicht weitergeleitet, sodass die Pakete mit LLA nicht ins Internet geschickt werden können. Werden u.a. für IPv6 Auto Configuration/Neighbor Discovery verwendet.

Struktur von Unique Local Addressen



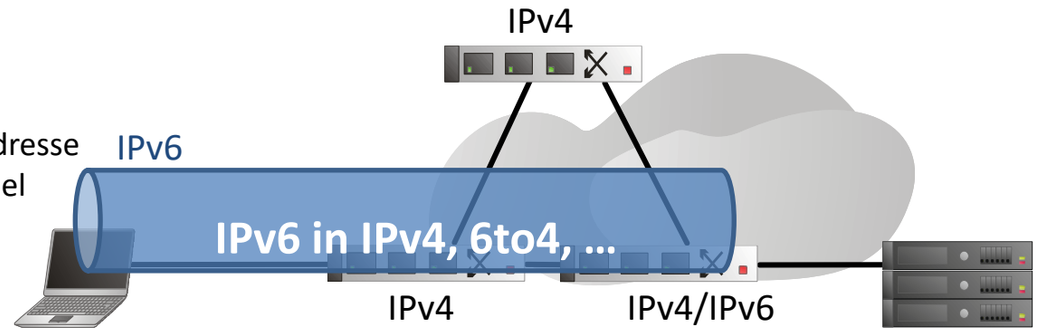
Unique Local Adressen (ULA) entsprechen den privaten Adressen in IPv4 (vgl. z.B. 192.168.0.0/16). Sie werden im Internet nicht geroutet, können aber z.B. innerhalb eines Unternehmens verteilt werden. Dabei folgen z.B. auf das Präfix „FC“ oder „FD“ 41 Bits einer eindeutig gewählten Site-ID und schließlich eine Subnetz- und Interface-ID.

Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Quelle: Badach, Skript Kommunikationsnetze

Migrationsszenarien

Dual Stack mit Tunnel

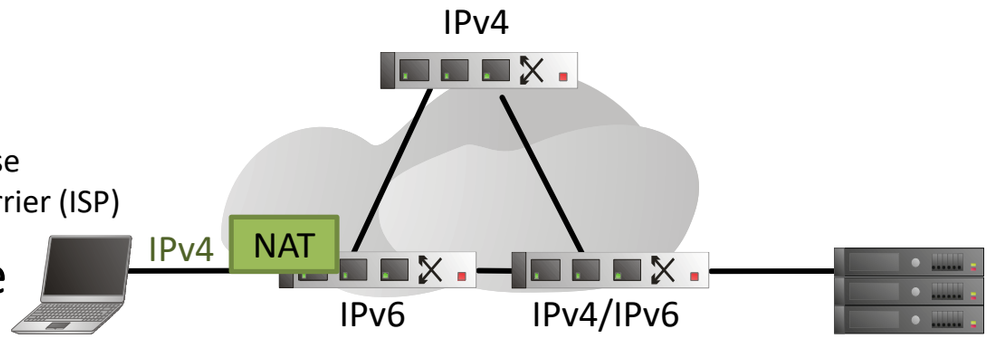


- Öffentliche IPv4-Adresse

Dual Stack

- öffentliche IPv4-Adresse
- öffentliche IPv6-Adresse

Dual Stack Lite



- Öffentliche IPv6-Adresse sog. „Carrier-Grade-NAT“
- Viele Kunden teilen sich gemeinsam eine öffentliche IPv4-Adresse, die beim Carrier geNATet wird
- Kein Zugriff auf Administration der NAT, daher auch kein Port-Forwarding an IPs im privaten Subnetz etc.

Dual Stack

- öffentliche IPv4-Adresse
- öffentliche IPv6-Adresse

Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Automatische Vergabe von IPv6-Adressen (NDP/DHCPv6)

- Neighbor Discovery Protocol (NDP) ersetzt ARP bei IPv6
  - NDP verwendet ICMPv6 für automatische Entdeckung von „Nachbarn“ im IPv6-Netz
  - Automatische Konfiguration von IPv6-Clients (Stateless Address Auto Configuration SLAAC)
    - Jeder IPv6-Router sendet zyklisch Router Advertisement als Multicast, Clients senden Router Solicitation
    - Ermöglicht Erkennung von Routern (Default Gateways) im Netz inkl. Präfix und Adressvergabe (kein DHCP erforderlich)
    - Jeder IPv6-Client hat immer bereits eine Link Local Adress (aus FE80::/10), erhält durch NDP zusätzliche globale (oder zumindest Unique Local) Adresse
    - Duplicate Address Detection (DAD) verhindert, dass gleiche Adresse mehrfach im Netz verwendet wird
    - Unterstützung von „Privacy Extension“ ermöglicht, dass eine zusätzliche globale Adresse (für ausgehende Verbindung) zufällig gewählt wird und für den gleichen Rechner nach Ablauf wechselt
- DHCPv6
  - Optional kann DHCPv6 verwendet werden, um alle Parameter der Clients automatisch zu vergeben (IPv6-Adresse sowie DNS-Server, Zeit-Server (NTP), …)
- Zusätzlich Kombination aus SLAAC für IPv6-Adressvergabe und DHCPv6 für alle weiteren Parameter (DNS-Server etc.) möglich

Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Migration zu IPv6… Problem „thin waist of IP“ (IP-Sanduhr)

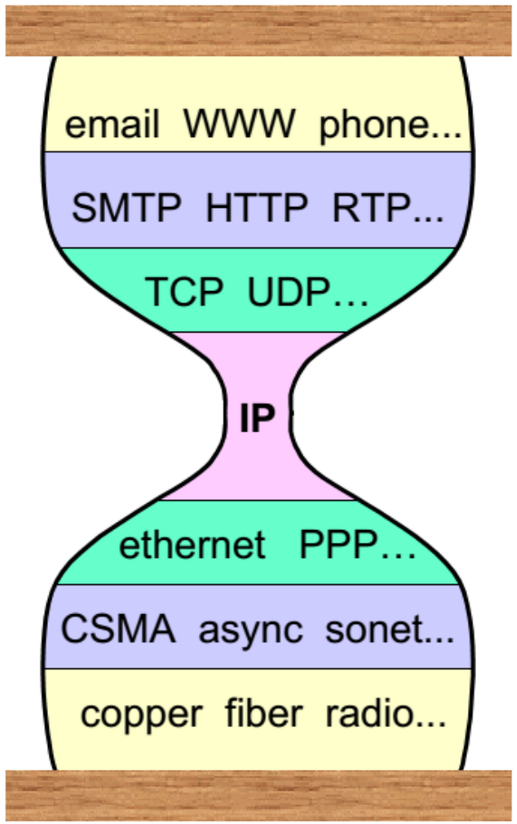
…seit Ende der 90er redet man schon von IPv6… Relevanz hängt stark von dessen Verbreitung ab… solange die meisten Sites per IPv4 erreichbar sind bleibt Relevanz gering… aber IPv4-Adressen sind nun wirklich knapp… ;-)

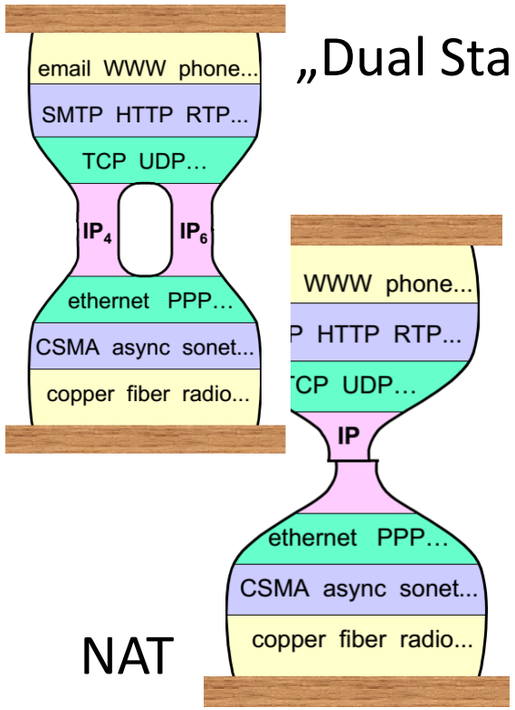
Missing Link: Neuer 'Protokollkrieg' – Streit um New IP und erneuertes Internet (Heise 4/2020)

IP ist schwer austauschbar, da es Austauschbarkeit auf höheren und niedrigeren Schichten erlaubt…

„all over IP“, „IP over all“

…vergleiche im Gegenzug Änderung an Web-Anwendungen in letzten Jahrzehnten…





„Dual Stack“

NAT

Quelle: Steve Deering, Cisco, IETF 51, 2001

Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Verbreitung von IPv6

- Google: ~43% in 5/2023 aller Client-Zugriffe IPv6 (~25% in 2019)
  - https://www.google.de/ipv6/statistics.html
- NIST: 33% aller US-Regierungsnetze IPv6-fähig (Quelle: Kurose/Ross – Computernetzwerke 2016)

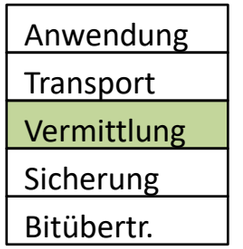
Verbreitung nimmt in Mobilfunknetzen und z.B. bei Kabelnetzbetreibern zu (IPv6 only)…

- RIPE-72 Streit um letzte IPv4-Adressen (Heise 5/2016)
- Das war's mit IPv4-Adressen in Europa (Heise 1/2020)

- RIPE-73 IPv6 verbreitet sich doch (10/2016)
- RIPE-73 Bundesregierung fordert mehr IPv6-Adressen (Heise 10/2016)

Bedarf wird wohl noch steigen? ;)

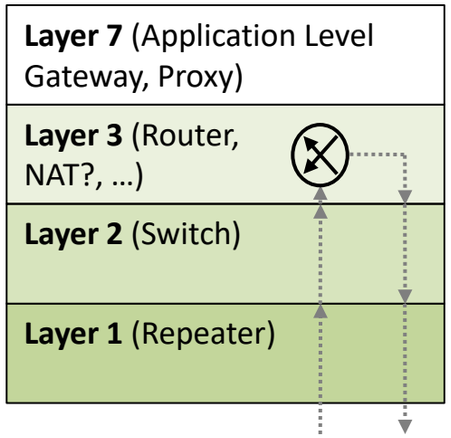
- IT-Markt unter Corona-Druck: Weniger Smartphones & PCs, mehr Server & Router (Heise 4/2020)
- #heiseshow: IPv6 setzt sich langsam durch – die wichtigsten Fragen (Heise 4/2022)
- Angst vor Zensur: China wirbt im "Protokollkrieg" auf ITU-Ebene für IPv6+ (Heise 6/2022)

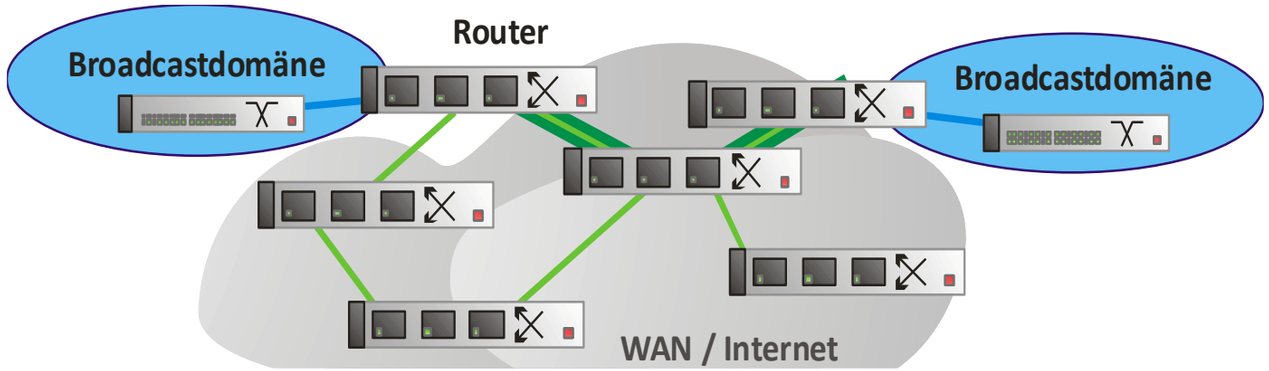


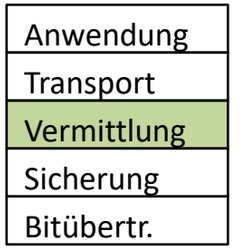
Aufgaben von Routern und Routing-Algorithmen

- Anforderungen an die Paketvermittlung im WAN, z.B. >100km
  - Anpassung an Übertragungsmedien, Synchronisation
  - Zusätzliche Latenz (Verarbeitung, Übertragung, Ausbreitung)
  - Puffer an Eingangs-/Ausgangsport, erneut zusätzliche Latenz
  - Im LAN bzw. Subnetz funktioniert Broadcast, im WAN Katastrophe!, Trennung von Broadcast-Domänen über Router (logische IP-Subnetze)
- Aufgaben von Routern
  - Routing: hop-by-hop, anhand Ziel-Adresse, Verwendung von Routing-Algorithmen, z.B. für Ermittlung „shortest path“
  - Forwarding: Weiterleitung von Paketen zwischen Ein- und Ausgangsports

Zwischensysteme auf den Layern:

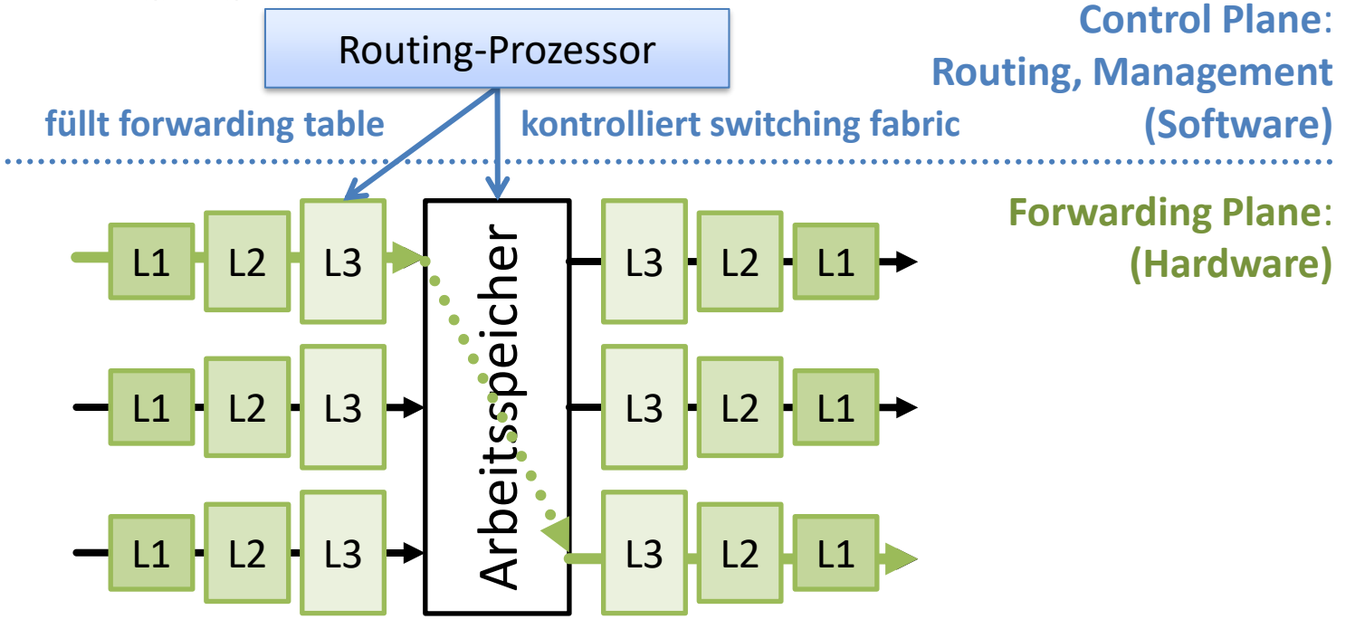






Forwarding: Packet Switching Fabrics

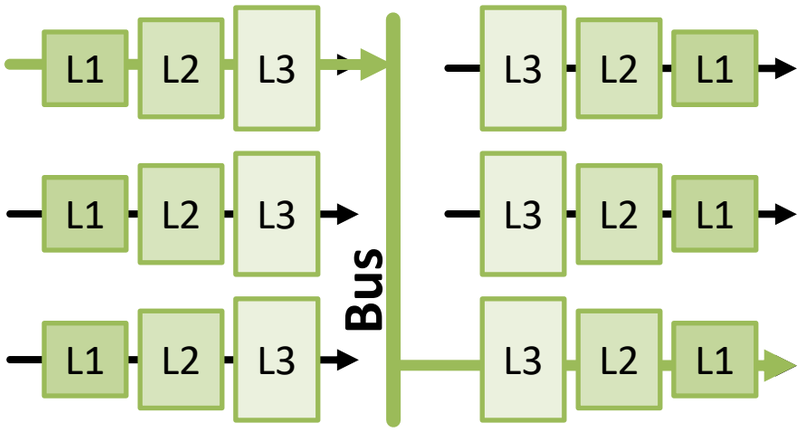
- Forwarding in Vermittlern technisch unterschiedlich realisierbar
- Was befindet sich in einem Router: CPU, RAM, Bus, spezielle Switching-Chips (ASICs, …)
- Einfachster Fall für Realisierung des Switchings
  - Empfangen der Bits auf Layer 1 (L1) am Eingangsport
  - Sicherung der Übertragung (L2)
  - Bearbeitung der Pakete (L3), Auswahl des Ausgangsports anhand analysiertem Paket, ggf. Pufferung, Ziel: Weiterleitung in „line speed“
  - Kopieren des Pakets zum Ausgangsport über Arbeitsspeicherbereich

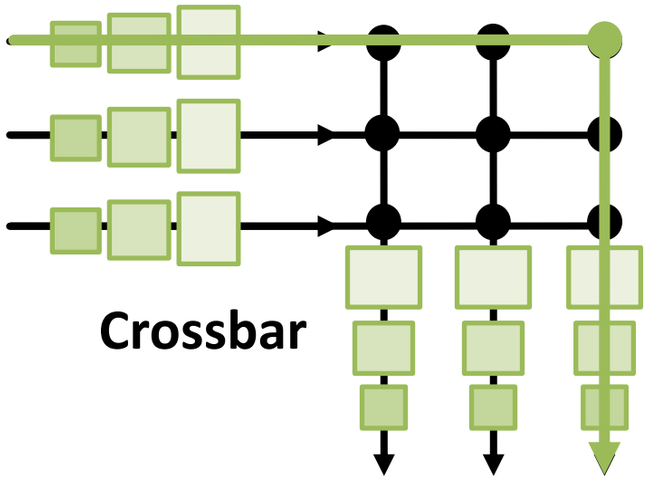


Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Forwarding: Packet Switching Fabrics

- Gemeinsamer Bus für Eingangs- und Ausgangsports, kein Kopieren der Pakete im RAM, typische Realisierung in aktuellen Routern und Switches
- Hohe „kpps“ (kilo packets/s), „line rate“, z.B. ~400ns/Frame
- Bus in aller Regel so ausgelegt, dass alle Portpaare gleichzeitig kommunizieren können („non-blocking“, „full-duplex“)
- Im Bereich Data Center (Rechenzentren): Crossbar
  - Forwarding mehrerer Pakete gleichzeitig, Limit primär nur noch Puffer am Ausgangsport





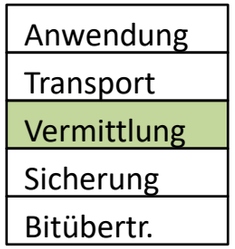
Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Routing: Statisch versus dynamisch

- Statisches Routing: Sinnvoll, wenn sich (optimale) Routen fast nie ändern. Beispiel für eine Routing/Forwarding-Tabelle:

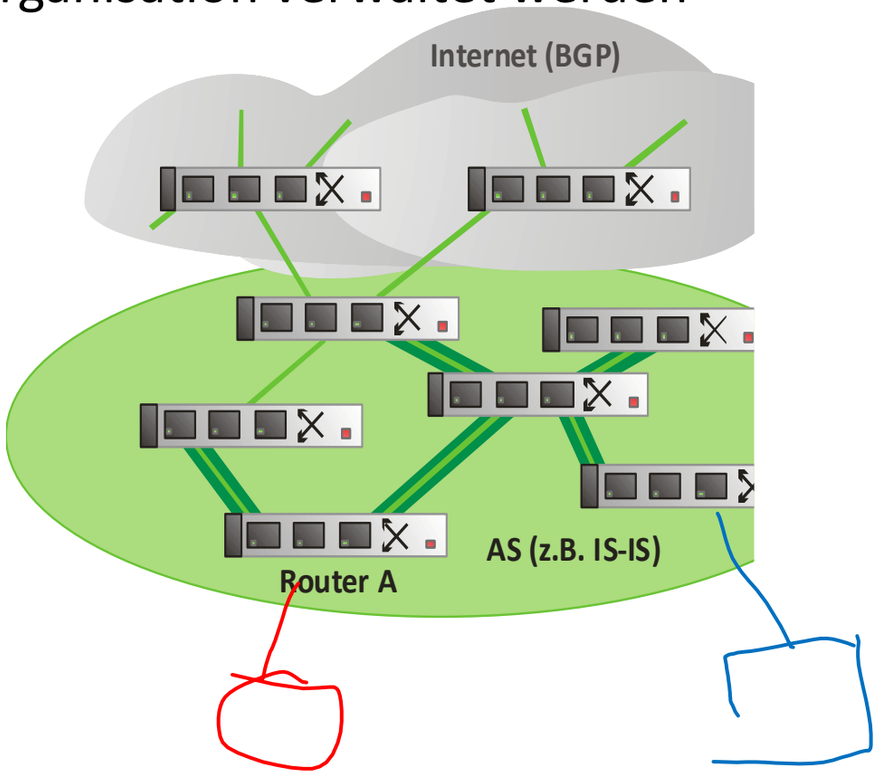
Destination	Gateway	Mask	Interface
0.0.0.0	192.168.178.1	0.0.0.0	eth0
192.168.178.0	*	255.255.255.0	eth0
10.4.1.0	*	255.255.255.0	eth1
10.5.0.0192.168.178.2	255.255.0.0	eth0	

- Dynamisches Routing: Wenn sich Kosten/Links im Netz häufig ändern, ermöglicht schnelle Reaktion auf Auslastung/Zustand des Gesamtnetzes, Verwendung von Routing-Protokollen:
  - Distanz-Vektor (sowie Distanz-Pfad)
    - Router kennt Nachbar-Router und Link-Kosten
    - Iterativer Austausch von Nachbar-Routern über Netz (auch von Fehlern!)
    - Nachrichtenaustausch nur zwischen Nachbarn, dafür hohe Konvergenzzeit
    - Routing-Schleifen möglich (z.B. Problem „Count to infinity“)
  - Link-State Routing-Protokolle
    - Alle Router kennen komplette Topologie und deren Zustand („Link State“: Link up/down, Verzögerung, Auslastung, Kosten/Gebühren, …)
    - Hohes Nachrichtenaufkommen im Gesamtnetz, dafür geringere Konvergenzzeit
    - Routing-Fehler durch oszillierende Routen möglich
    - Fehlerhafte Link-Kosten haben im Gegensatz zu Distanz-Vektor nur lokale Auswirkung



Hierarchisches Routing im Internet

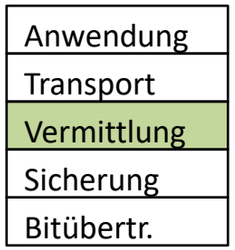
- Administrative Autonomie in Netzen in Bezug auf Routing
- Regionen im Internet: Autonomous System (AS)
  - Verbund aller Subnetze, die von einheitlicher Organisation verwaltet werden
- Intra-AS Routing
  - Innerhalb eines autonomen Systems
  - Routing-Protokolle: Z.B. OSPF, IS-IS
  - Häufig ausgerichtet auf „link state“
- Inter-AS Routing
  - Über mehrere AS, bildet das Internet
  - Routing-Protokoll: BGP
  - Ausfallsichere Pfade, „distance vector“



Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Warum Intra- und Inter-AS-Routing?

- Scale:
  - Hierarchisches Routing verringert Größe der Routing-Tabellen, geringerer Traffic für „Routing Updates“
- Policy:
  - Inter-AS: Admin wünscht Kontrolle darüber, wer welchen Traffic durch sein AS lässt, wie dieser geroutet wird
  - Intra-AS: Einzelne Domain, daher keine Policy-Entscheidungen erforderlich
- Performance:
  - Intra-AS: Kann sich auf Performance konzentrieren
  - Inter-AS: Policy ggf. wichtiger als Performance
- Einblick in Internet Routing: http://www.routeviews.org/, https://stat.ripe.net/ …



Beispiel: Hochschule Fulda

- Wie ist die Hochschule im Internet adressierbar?
- Teil von Autonomous System (AS) 680, gehört: DFN - Verein zur Förderung eines Deutschen Forschungsnetzes e.V. …unser „Internet Provider“ ;)
- Ihre aktuelle IP-Adresse (aus Netz der Hochschule aufrufen): https://stat.ripe.net/widget/whats-my-ip
- „Unsere Vorwahl“ in AS 680: Präfix 193.174.0.0**/15**

```
IP-Adresse (dezimal):   193     .174     .0       .0        (Netz-Adresse)
IP-Adresse (binär):     11000001 10101110 00000000 00000000 (32 Bit, 4 Bytes)
Subnetzmaske (binär):   11111111 11111110 00000000 00000000 (/15 „Einsen“)
Subnetzmaske (dezimal): 255     .254     .0       .0
```

- Mögliche Adressen: 32 Bit (Länge IPv4 Adresse) – **15 Bit (Subnetzmaske)** = 17 Bit (für Hosts) (2^17)**-2** = 131070 Adressen …Hochschule Fulda hat also 131070 öffentliche IP-Adressen? ;-) Leider nein… ;-) Präfix 193.174.0.0/15 wird vom DFN-Verein an mehrere angeschlossene Einrichtungen verteilt und weiter aufgeteilt (Subnetting)
- WHOIS Eintrag zur IP-Adresse ergibt: Adresse gehört zum Bereich 193.174.24.0-193.174.31.255 (193.174.24.0/21) (Hochschule Fulda)

Beispiel: Hochschule Fulda – Subnetting

```
IP-Adresse (dezimal):    193      .174      .24       .0
IP-Adresse (binär):      11000001 10101110 00011000 00000000
Subnetzmaske (binär):    11111111 11111111 11111000 00000000 (/21 „Einsen“)
Subnetzmaske (dezimal): 255      .255      .248      .0
```

- Weitere Unterteilung im Fachbereich AI:
  - NetLab 193 .174 .24 .192/27
    11000001 10101110 00011000 11000000
  - WI-Labor Studentische Projekte 193.174.29.0/27
  - WI-Labor 193.174.29.32/27
  - AI-Mitarbeiter 193.174.24.32/27
  - AI-Server 193.174.26.0/26
  - …

In welchem Netz liegt die Adresse von mmnet.informatik.hs-fulda.de 193.174.29.26? ;)

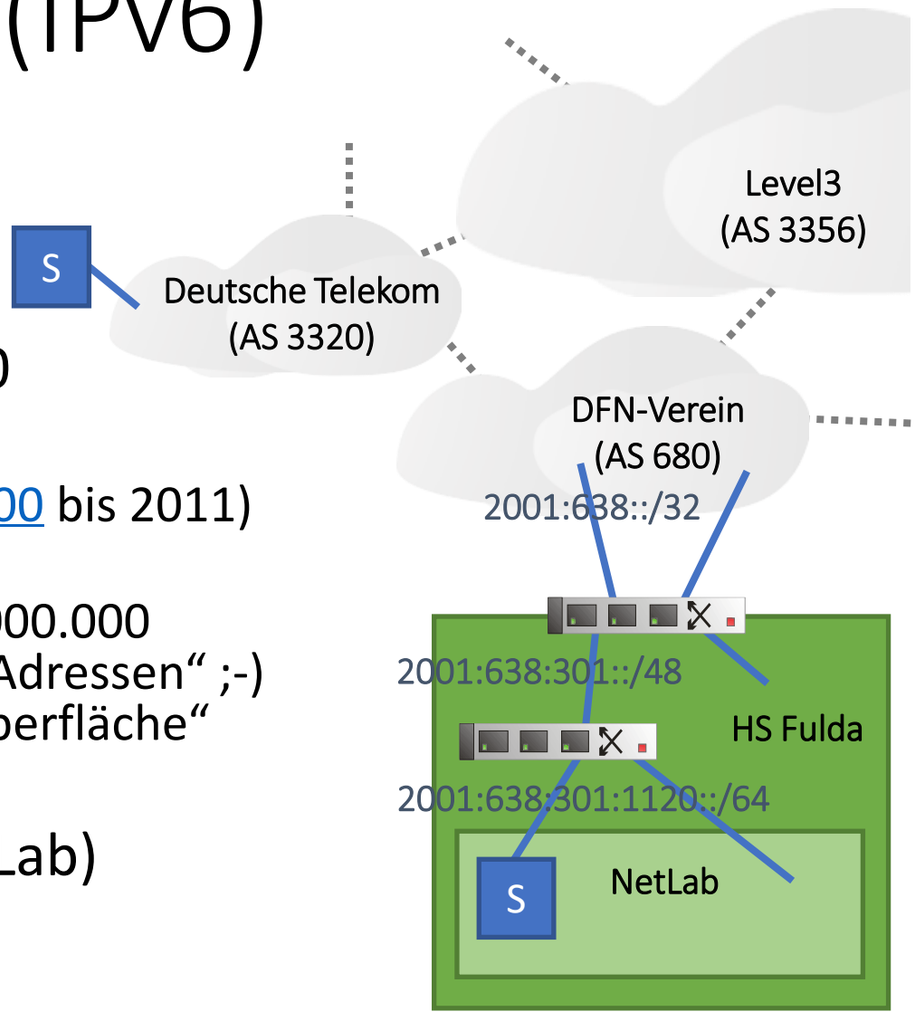
Wie viele Hosts passen in AI-Server? Wie viele ins NetLab?

Beispiel: Hochschule Fulda – „Unser AS“

- 193.174.0.0/15 ist unser „Heimat“-Präfix in AS 680
  - Eins von derzeit ~290 IPv4-Präfixen in AS 680 (Link kopieren und in Browser einfügen zum Öffnen)
  - Eins von derzeit ~1.000.000 IPv4-Präfixen weltweit (<20.000 in 1994)
  - ~3 Milliarden weltweit erreichbare IP-Adressen
  - ~75.000 AS weltweit
- Weltweit wissen alle Internet Core Router über welchen Nachbar-Router sie 193.174.0.0/15 erreichen (über welchen AS Pfad)
- Wie muss man sich die Vernetzung der AS untereinander vorstellen?
  - Wie kommt unser Client aus dem NetLab zum AS der Telekom?
  - vgl. „traceroute www.telekom.de“
  - Anbindung des Deutschen Forschungsnetzes AS 680 (BGP Peers, X-WiN 3/2019, 2022)
  - Änderungen gemäß BGPlay an AS 680
- Wie groß muss man sich diese Anzahl von AS vorstellen?
  - http://www.caida.org/home/

Internet Protocol Version 6 (IPv6)

- IPv6 als „Paralleluniversum“ zu IPv4, separate IPv6-Präfixe in den AS
- **2001:638**::/32 ist unser „Heimat“-Präfix in AS 680
  - Eins von derzeit ~10 IPv6-Präfixen in AS 680
  - Eins von derzeit ~200000 IPv6-Präfixen weltweit (<5000 bis 2011)
  - 128 Bit IPv6-Adressen… 340.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000 Adressen, „für jeden Erdbewohner Milliarden von IP-Adressen“ ;-) „600 Billiarden Adressen pro Quadratmillimeter Erdoberfläche“ …noch… ;-)
- HS-Fulda IPv6-Präfix (nutzbar aus WLAN und NetLab) **2001:638:301**::/48
- NetLab IPv6 Prefix **2001:638:301:1120**::/64



Intra-AS-Routing-Protokolle

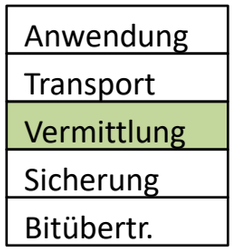
(auch genannt: Interior Gateway Protocol - IGP)

- Routing Information Protocol (RIP)
  - Distanz-Vektor-Protokoll, langsame Konvergenz, Routing-Schleifen möglich, nur noch selten verwendet
- Open Shortest Path First (OSPF)
  - Offener Standard, gängigstes Protokoll für Intra-AS-Routing
  - „link state“ Algorithmus
  - IPv6-Support mit OSPFv3
- Intermediate System to Intermediate System (IS-IS)
  - Vergleichbar mit OSPF, jedoch weniger komplex, „link state“
  - Teilweise beliebt, z.B. für neue interne Routing-Lösungen in Data Centern / ISPs, offener Standard
  - Ursprünglich in OSI für Routing entwickelt, unterstützt daher verschiedene Layer-3-Protokolle (z.B. IPv4, IPv6)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
  - Bis vor Kurzem proprietäres Routing-Protokoll der Fa. Cisco
  - Mischung aus „link state“ und „distance vector“ Algorithmus

Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

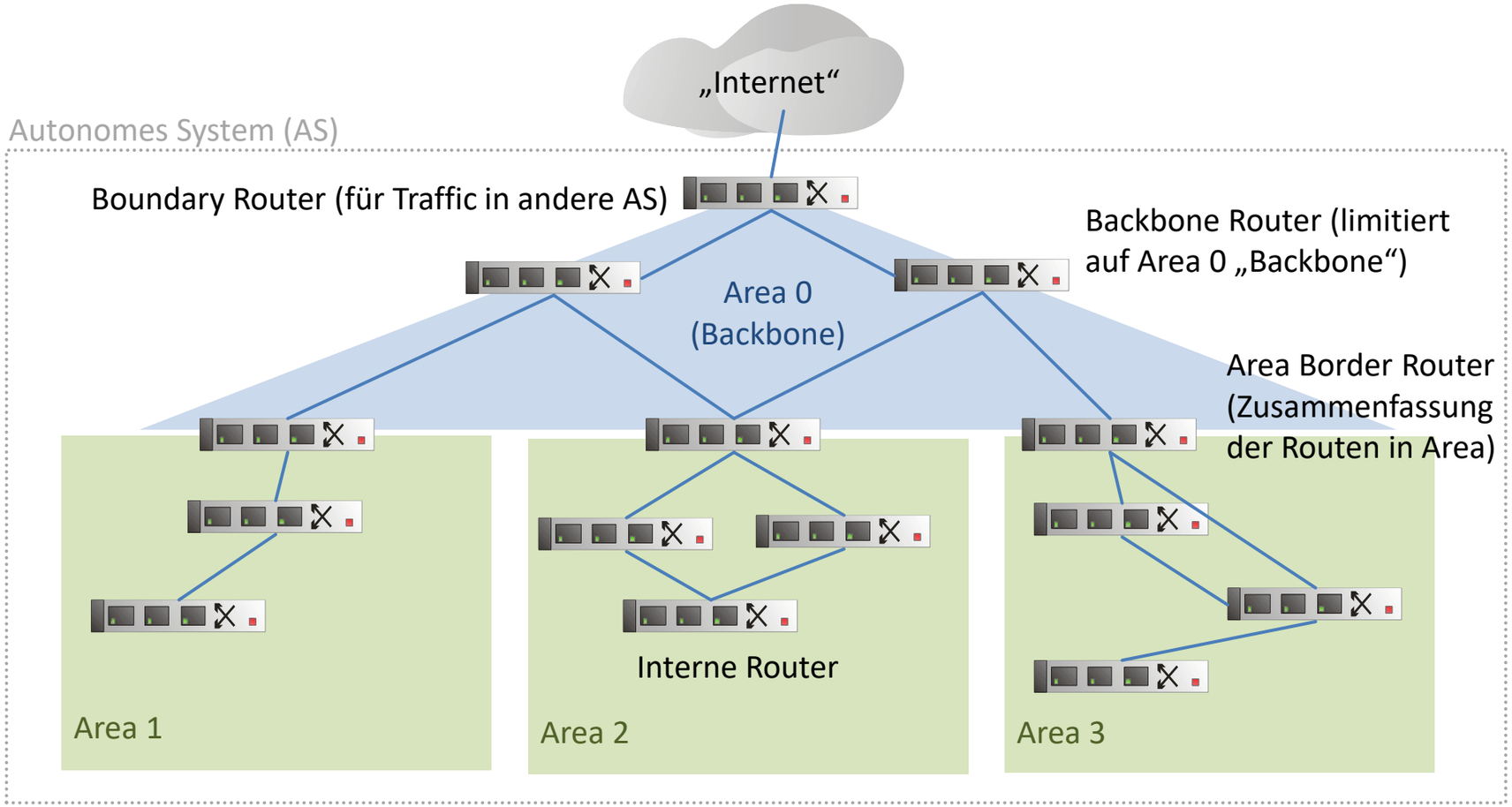
Open Shortest Path First (OSPF)

- Freiverfügbarer Standard (RFC 2328)
  - Praktisch von allen Netzwerkherstellern implementiert
  - Sehr große Verbreitung
- „link state“ Algorithmus
  - Berechnung der Routen basierend auf Dijkstra-Algorithmus (Visualisierung)
  - Jeder Knoten kennt gesamte Topologie und damit „shortest path tree“
- Verteilung von „link state“ Paketen durch das gesamte Netz
  - Verwendet direkt IP (ohne zusätzlichen TCP-/UDP-Overhead)
- Vorteile von OSPF gegenüber RIP
  - Sicherheit: OSPF-Pakete können Authentifizierung beinhalten
  - Lastverteilung über Pfade mit gleichen Kosten
  - „Quality of Service“ in Kosten abbildbar: Z.B. Links mit hoher Latenz, …
  - Integrierter Support für Multicast-Routing
  - Hierarchisches OSPF-Routing für große Domains



Hierarchisches OSPF

- Zwei Hierarchieebenen: Local Area, Backbone
  - Versand von „link state advertisements“ nur innerhalb der Area

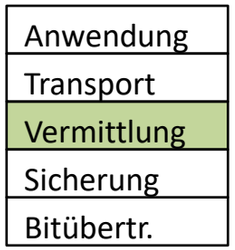


Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

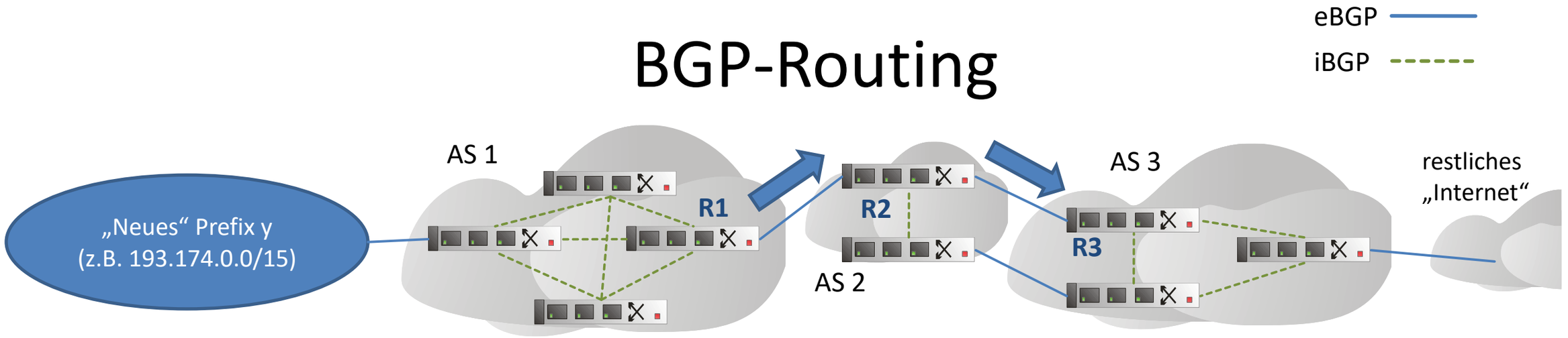
Inter-AS-Routing

(auch genannt: Exterior Gateway Protocol - EGP)

- Border Gateway Protocol (BGP) – RFC 4271
  - „hält im Prinzip das Internet zusammen“
  - External BGP (eBGP) verteilt Erreichbarkeit von AS unter benachbarten Routern weltweit
  - Internal BGP (iBGP) verteilt Erreichbarkeit von externen Zielen innerhalb des AS
- Aufgabe BGP: Optimale Routen im Internet
  - „path vector“ (vgl. distance vector, Bellman-Ford-Algorithmus, Visualisierung)
  - Basierend auf Erreichbarkeit (Präferenz auf „shortest path“) und Policy (z.B. „Verkehr von x nie über AS y leiten“…)
  - Bekanntmachung neuer „Pfade“/Präfixe etc.
  - Angebot des Routings an Präfix über AS, inkl. Zusammenfassung der Präfixe (Route Aggregation)
- BGP Sessions zwischen Routern („peers“)
  - Semi-permanente TCP-Sitzungen



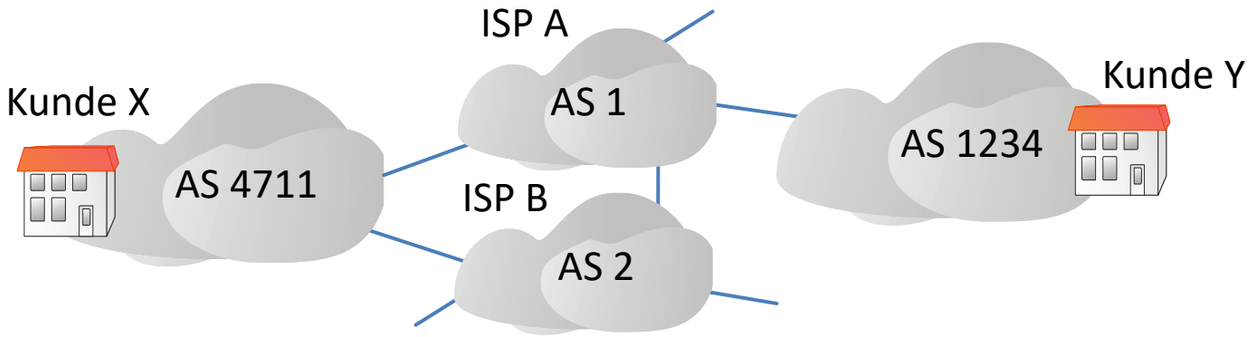
BGP-Routing



- Beispiel:
  - R1 teilt R2 neuen Pfad zu einem Präfix y mit, R2 macht dies per iBGP in AS2 bekannt
  - R2 fügt AS2 in Pfad zu y hinzu und sendet Bekanntmachung an R3 usw.
  - Alle Router tragen neues Präfix in Routing-Tabelle ein
- Inhalt der Bekanntmachung (Advertisement)
  - Präfix + Attribute (AS-Path + Next-Hop) = „Route“
  - AS-PATH: AS, über die das Präfix erhalten wurde
  - **NEXT-HOP**: IP-Adresse des nächsten Routers der zum Präfix führt
- Beispiel-Nachricht an R3: y AS2 AS1 **R2**
- Mehrere Routen zum Ziel-AS möglich, Auswahl anhand:
  - Policy, shortest AS-PATH, closest NEXT-HOP („hot potato routing“) …

Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Beispiel für Bedarf nach Policy-based Routing



- Kunde X ist über mehrere ISPs an das Internet angebunden („multi-homed“), Ausfallsicherheit
- Kunde X könnte Verkehr von AS1 nach AS2 über sich umleiten
  - Daher würden in der Realität ISP A und B die Route Advertisements von AS 4711 filtern (löschen)
- ISP A und B können durch Verbindung untereinander auch Verkehr von AS 1234 nach AS 4711 gemeinsam durchleiten
  - Ggf. wollen sie dies aber aus wirtschaftlichen (Kostenverrechnung) oder politischen (Vertrauen ISP A in ISP B?, z.B. in unterschiedlichen Ländern) Gründen nicht… → Policy

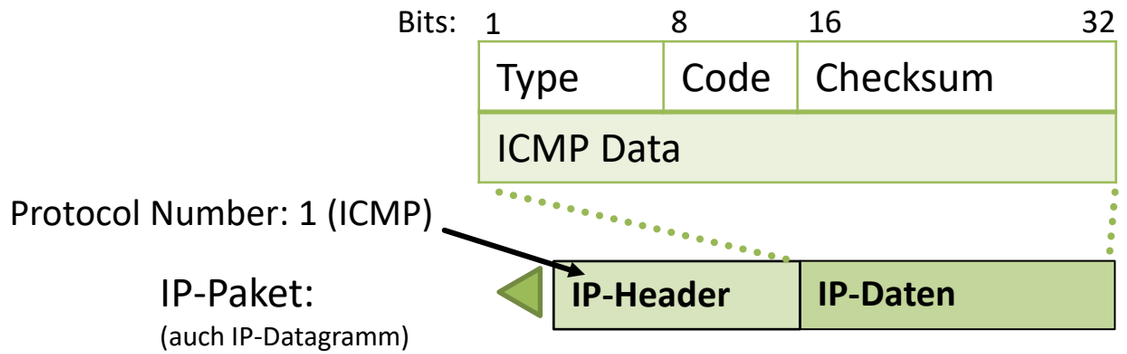
– Mehr Details zu BGP z.B. in „BGP for all“ …siehe dort auch „Campus Network Design & Ops“ ;-)
  – BGP bildet die Basis für Routing im Internet und zunehmend auch im Data Center (vgl. Leaf-Spine)

Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Aufgaben des Internet Control Message Protocol (ICMP)

Wird von Hosts und Routern z.B. verwendet für:
Unterstützung der Diagnose: Hilfsprogramme **ping** , **tracert** (bzw. **traceroute**)
Unterstützung der Aufzeichnung von Zeitmarken (*Timestamps*)
Verwaltung von Routing-Tabellen, ...

Aufbau von ICMP-Nachrichten



Die einzelnen Angaben im ICMP-Header lauten:
Type dient als Unterscheidung der Bedeutung von einzelnen ICMP-Nachrichten.
Code: Eine weitere Unterteilung der Bedeutung der Nachricht innerhalb eines Typs.

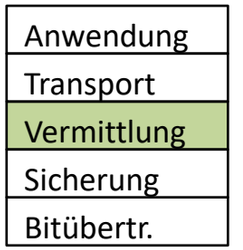
Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Quelle: Badach, Skript Kommunikationsnetze

Beispiele für ICMP-Nachrichtentypen

Typ	Code	Bedeutung
0	0	echo reply (Echo-Antwort „ping“)
3	0	destination network unreachable
3	1	destination host unreachable
3	2	destination port unreachable
3	6	destination network unknown
3	7	destination host unknown
8	0	echo request (Echo-Anfrage „ping“)
9	0	Route Advertisement
10	0	Router Discovery
11	0	TTL expired
12	0	Bad IP Header

- Liste ist nur ein Auszug, weitere Nachrichten z.B. bei ICMPv6 für „packet to big“ (als Ersatz für fehlende Unterstützung von Fragmentierung)



Traceroute mit ICMP

```
C:\Windows\system32>tracert www.kit.edu

Routenverfolgung zu www.kit.edu [129.13.40.10]
über maximal 30 Hops:

  1    <1 ms    <1 ms    <1 ms  fritz.box [192.168.78.254]
  2     9 ms    10 ms     7 ms  10.145.192.1
  3     9 ms    14 ms     8 ms  7411a-mx960-01-ae12-1010.kzl.unity-media.net [81.21
  4                              .69.107.1
  5                              .69.107.1
  6                              .69.107.2
  7    10 ms    12 ms    12 ms  de-fra04a-rc1-ae7.fra.unity-media.net [81.210.129.2
  8    11 ms    19 ms    14 ms  84.116.133.97
  9    11 ms    11 ms    13 ms  Frankfurt-DECIX-1-10GE-0-1-0-3.belwue.net [80.81.19
 10    16 ms    13 ms    15 ms  Karlsruhe-RZ-1-10GE-0-3-0-2.belwue.net [129.143.57.
 11                              .143.166.142]
 12                              .52.249.236]
 13    14 ms    14 ms    14 ms  tf-v1388-rbbch1.scc.kit.edu [141.52.249.241]
 14    14 ms    19 ms    12 ms  www.kit.edu [129.13.40.10]
```

TTL=3, führt zu: 3. Router auf der Strecke schickt ICMP-Antwort: „TTL expired“

TTL=10, 10. Router auf der Strecke schickt ICMP-Antwort: „TTL expired“

```
                                My traceroute  [v0.85]
cardassia (0.0.0.0)                                                    Th
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                                        Packets
Host                                                 Loss%   Snt   Last
1. AS???    fritz.box                                 0.0%   119    4.1
2. AS???    10.145.192.1                              0.0%   119    9.0
3. AS20825  7411a-mx960-01-ae12-1010.kzl.unity-media.net  0.0%   119    7.0
4. AS20825  7411a-mx960-02-ae0.kzl.unity-media.net    0.0%   119   12.8
    [MPLS: Lbl 500282 Exp 0 S 1 TTL 1]
5. AS20825  7111a-mx960-02-ae2.fra.unity-media.net    0.8%   119   11.7
    [MPLS: Lbl 583544 Exp 0 S 1 TTL 1]
6. AS20825  7111a-mx960-01-ae0.fra.unity-media.net   29.7%   119   11.0
    [MPLS: Lbl 301088 Exp 0 S 1 TTL 1]
7. AS20825  de-fra04a-rc1-ae7.fra.unity-media.net    17.9%   118  165.3
    [MPLS: Lbl 466434 Exp 0 S 1 TTL 1]
8. AS6830   84.116.133.66                            23.7%   118  164.8
```

Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

```
C:\Windows\system32>tracert www.kit.edu

Routenverfolgung zu www.kit.edu [129.13.40.10]
über maximal 30 Hops:

  1    <1 ms    <1 ms    <1 ms  fritz.box [192.168.78.254]
  2     9 ms    10 ms     7 ms  10.145.192.1
  3     9 ms    14 ms     8 ms  7411a-mx960-01-ae12-1010.kzl.unity-media.net [81.21
  4    10 ms     8 ms     8 ms  7411a-mx960-02-ae0.kzl.unity-media.net [80.69.107.1
  5     9 ms    10 ms    11 ms  7111a-mx960-02-ae2.fra.unity-media.net [80.69.107.1
  6     *        *       12 ms  7111a-mx960-01-ae0.fra.unity-media.net [80.69.107.2
  7    10 ms    12 ms    12 ms  de-fra04a-rc1-ae7.fra.unity-media.net [81.210.129.2
  8    11 ms    19 ms    14 ms  84.116.133.97
  9    11 ms    11 ms    13 ms  Frankfurt-DECIX-1-10GE-0-1-0-3.belwue.net [80.81.19
 10    16 ms    13 ms    15 ms  Karlsruhe-RZ-1-10GE-0-3-0-2.belwue.net [129.143.57.
 11    14 ms    13 ms    14 ms  KIT-Karlsruhe-RZ-1.belwue.net [129.143.166.142]
 12    15 ms    13 ms    14 ms  tr-v1001-fwkitcn1.scc.kit.edu [141.52.249.236]
 13    14 ms    14 ms    14 ms  tr-v1388-rbbcn1.scc.kit.edu [141.52.249.241]
 14    14 ms    19 ms    12 ms  www.kit.edu [129.13.40.10]
```

```
C:\Users\flex>tracert www.kit.edu

Routenverfolgung zu www.kit.edu [129.13.40.10]
über maximal 30 Hops:

  1    <1 ms    <1 ms    <1 ms  fritz.box [192.168.78.254]
  2     *        *        *     Zeitüberschreitung der Anforderung.
  3    10 ms     8 ms     9 ms  7411A-MX960-01-ae12-1010.kzl.unity-media.net [81.210.139.128]
  4    11 ms    11 ms    18 ms  de-kzl02a-rd02-ae0-0.aorta.net [84.116.196.242]
  5    13 ms    12 ms    10 ms  de-fra01b-rc1-ae42-0.aorta.net [84.116.196.246]
  6    11 ms    10 ms    11 ms  de-fra01b-ri1-ae0-0.aorta.net [84.116.134.6]
  7    12 ms    11 ms    19 ms  Frankfurt-DECIX-1-100GE-0-0-0-5.belwue.net [80.81.192.175]
  8    22 ms    14 ms    12 ms  kar-rz-a99-hu0-2-0-0.belwue.net [129.143.60.114]
  9    21 ms    15 ms    15 ms  kit-cs-1.belwue.net [193.197.63.7]
 10    14 ms    13 ms    13 ms  tr-v1001-fwkit.scc.kit.edu [141.52.249.238]
 11    15 ms    14 ms    15 ms  tr-v1388-rbbcn1.scc.kit.edu [141.52.249.243]
 12    14 ms    22 ms    19 ms  www.kit.edu [129.13.40.10]
```

```
C:\Users\flex>tracert www.kit.edu

Routenverfolgung zu www.kit.edu [2a00:1398:b::8d03:8006]
über maximal 30 Hops:

  1     4 ms     3 ms     4 ms  2a02:908:1b1c:7860:2e91:abff:fe96:794a
  2    15 ms    12 ms    13 ms  de-kzl02a-cr01-ca1.kzl.unity-media.net [2a02:908:1b00:1::1]
  3    12 ms    11 ms    10 ms  7411a-mx960-02-ae12-2010.kzl.unity-media.net [2a02:908:0:364::1]
  4    13 ms    15 ms    24 ms  de-fra01b-rc2-lo0-0.v6.aorta.net [2001:730:2d00::5474:8065]
  5     *       15 ms    13 ms  cr-fra2-be6.x-win.dfn.de [2001:638:c:a2c9::1]
  6    29 ms    26 ms    18 ms  kr-fzk85-1.x-win.dfn.de [2001:638:c:a00d::2]
  7    17 ms    13 ms    16 ms  rcn-border-3-eth53-1.scc.kit.edu [2a00:1398:e:76::]
  8    16 ms    17 ms    16 ms  fwcn-1-eth2-28-2.scc.kit.edu [2a00:1398:e:9c::1]
  9    18 ms    17 ms    23 ms  rcn-0449-l-10-2-eth1-49-2.scc.kit.edu [2a00:1398:e:94::]
 10    18 ms    19 ms    25 ms  defgw-v1212.scc.kit.edu [2a00:1398:4::1]
 11    27 ms    19 ms    13 ms  scc-web-0028.scc.kit.edu [2a00:1398:b::8d03:8006]
```

```
                                  My traceroute  [v0.85]
cardassia (0.0.0.0)                                                    Th
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                                        Packets
Host                                                    Loss%   Snt   Last
1. AS???   fritz.box                                     0.0%   119    4.1
2. AS???   10.145.192.1                                  0.0%   119    9.0
3. AS20825 7411a-mx960-01-ae12-1010.kzl.unity-media.net  0.0%   119    7.0
4. AS20825 7411a-mx960-02-ae0.kzl.unity-media.net        0.0%   119   12.8
   [MPLS: Lbl 500282 Exp 0 S 1 TTL 1]
5. AS20825 7111a-mx960-02-ae2.fra.unity-media.net        0.8%   119   11.7
   [MPLS: Lbl 583544 Exp 0 S 1 TTL 1]
6. AS20825 7111a-mx960-01-ae0.fra.unity-media.net       29.7%   119   11.0
   [MPLS: Lbl 301088 Exp 0 S 1 TTL 1]
7. AS20825 de-fra04a-rc1-ae7.fra.unity-media.net        17.9%   118  165.3
   [MPLS: Lbl 466434 Exp 0 S 1 TTL 1]
8. AS6830  84.116.133.66                                23.7%   118  164.8
```

```
cardassia (192.168.78.252)                          2019-06-25T23:08:53+0200
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                          Packets                 Pings
 Host                                     Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. AS???    fritz.box                    99.2%   121    0.4   0.4   0.4   0.4   0.0
 2. ???
 3. AS6830   7411A-MX960-01-ae12-101       0.0%   121   10.6  11.1   8.0  20.1   2.7
 4. AS6830   de-kzl02a-rd02-ae0-0.ao       0.0%   121   11.0  12.9   9.9  26.4   3.2
    [MPLS: Lbl 317274 Exp 0 S 1 TTL 1]
 5. AS6830   de-fra01b-rc1-ae42-0.ao       0.0%   121   10.1  13.1   9.4  27.8   3.4
    [MPLS: Lbl 300948 Exp 0 S 1 TTL 1]
 6. AS6830   de-fra01b-ri1-ae0-0.aor       0.0%   121   28.3  13.3   9.0  42.4   5.1
 7. AS???    Frankfurt-DECIX-1-100GE       0.0%   121   18.5  12.8   9.5  24.9   2.9
 8. AS553    kar-rz-a99-hu0-2-0-0.be       0.0%   121   21.8  16.1  12.2  64.9   5.9
 9. AS553    kit-cs-1.belwue.net           0.0%   120   14.1  14.4  11.6  32.2   3.1
10. AS34878  tr-v1001-fwkit.scc.kit.        0.0%   120   21.5  15.4  12.0  29.3   3.5
11. AS680    tr-v1388-rbbcs2.scc.kit        0.0%   120   14.7  19.0  11.3  75.7  10.8
12. AS34878  www.kit.edu                    0.0%   120   13.2  14.0  10.7  26.9   3.1
```

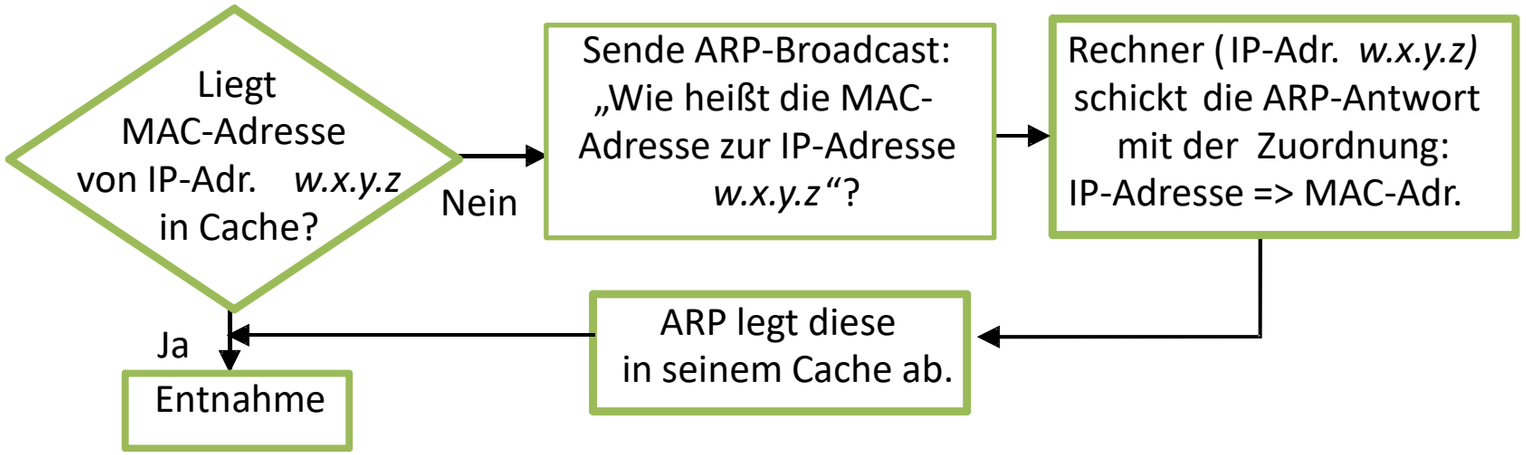
```
                                  My traceroute  [v0.93]
cardassia (2a02:908:1b1c:7860:6a05:caff:fe14:717b)                2022-05-28T23:43:47+0200
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                          Packets                 Pings
 Host                                     Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. AS3209   fritz.box                     0.0%    47    0.9   1.3   0.7   2.6   0.4
 2. AS3209   de-kzl02a-cr01-ca1.kzl.unity-media.net  0.0%    47   13.7   9.8   7.3  13.7   1.4
 3. AS3209   7411a-mx960-02-ae12-2010.kzl.unity-medi  0.0%    46    9.1  10.3   7.4  18.8   2.2
 4. AS6830   de-fra01b-rc2-lo0-0.v6.aorta.net       0.0%    46   20.0  12.3   9.2  22.6   2.7
    [MPLS: Lbl 959663 TC 0 S 0 TTL 1]
    [MPLS: Lbl 2 TC 0 S 1 TTL 1]
 5. AS680    cr-fra2-be6.x-win.dfn.de              8.7%    46   13.6  11.3   9.3  17.1   1.6
 6. AS680    kr-fzk85-1.x-win.dfn.de               0.0%    46   12.9  12.4  10.5  15.6   1.1
 7. AS34878  rcn-border-3-eth53-1.scc.kit.edu      0.0%    46   10.4  12.8  10.4  15.4   1.2
 8. AS34878  fwcn-1-eth2-28-2.scc.kit.edu          0.0%    46   11.7  13.0  11.1  15.9   1.1
 9. AS34878  rcn-0449-l-10-2-eth1-49-2.scc.kit.edu 0.0%    46   15.1  13.9  11.9  17.9   1.2
10. AS34878  defgw-v1212.scc.kit.edu               0.0%    46   13.7  14.8  12.5  23.1   2.1
11. AS34878  scc-web-0028.scc.kit.edu              0.0%    46   11.9  12.7  10.6  21.9   1.9
```

Aufgabe des Address Resolution Protocol (ARP)

Soll ein IP-Paket an ein Endsystem am LAN gesendet werden, wird das Paket in einen MAC-Frame eingebettet. Im Header des MAC-Frames ist eine entsprechende MAC-Adresse des Zielsystems enthalten. Um die zur IP-Adresse des Endsystems passende MAC-Adresse zu ermitteln, muss eine Tabelle mit den Zuordnungen **IP-Adresse => MAC-Adresse** in jedem LAN-Endsystem vorhanden sein.

Diese Zuordnungen werden mit ARP realisiert. ARP ist ein Hilfsprotokoll zur Ermittlung einer physikalischen Adresse (**MAC-Adresse**) für IP, d.h. es ist für die Zuordnung von MAC-Adressen zu IP-Adressen verantwortlich.

Unterstützung der Adressierung mit Hilfe des Protokolls ARP innerhalb eines Subnetzes



ARP legt eine dynamisch organisierte **Adressermittlungs-Tabelle** mit IP-Adressen und den zugehörigen MAC-Adressen an. Oft wird diese Tabelle auch **ARP-Cache** genannt.

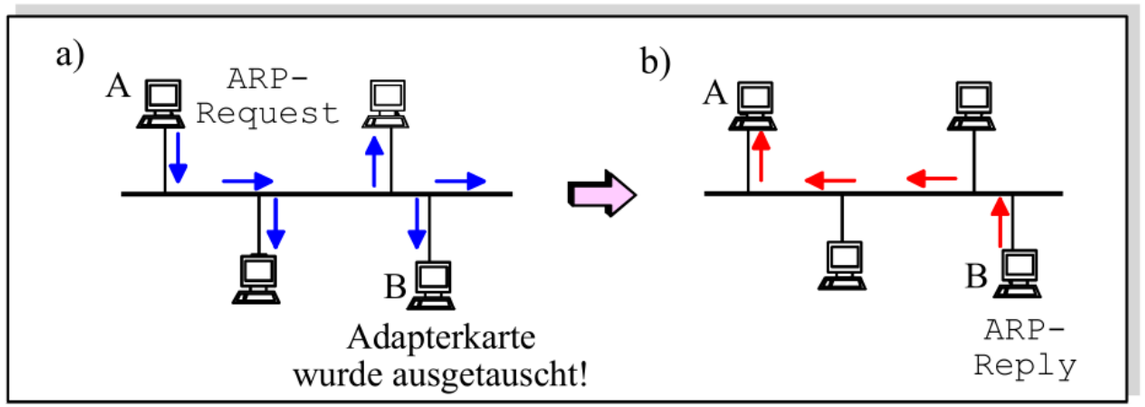
In manchen Implementierungen wird **ein Zeitlimit** (*time-out*) für Einträge im ARP-Cache gesetzt. Falls der Eintrag innerhalb dieses Zeitraums (bei Windows ab Vista zwischen 15 und 45 Sekunden) nicht verwendet wird, wird er gelöscht. Einige Systeme arbeiten wiederum mit einem zeitgesteuerten Aktualisierungsprinzip. Hierbei wird in festen Zeitabständen ein erneuter ARP-Request gesendet, um den Cache zu aktualisieren.

Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Quelle: Badach, Skript Kommunikationsnetze

Unterstützung der Adressierung mit ARP-Hilfe

a) Broadcast-Nachricht ARP-Request, b) Antwort ARP-Reply



Wenn der TCP/IP-Stack die Anforderung erhält, ein Paket an eine IP-Adresse im gleichen Subnetz (!) zu senden, sucht er zuerst im ARP-Cache nach der korrespondierenden MAC-Adresse. Falls kein Eintrag vorhanden ist, wird versucht, mit Hilfe von ARP die gesuchte MAC-Adresse zu ermitteln. Hierfür wird ein ARP-Request als **MAC-Broadcast** verschickt. In dieser Nachricht werden die restlichen Endsysteme in demselben Subnetz gebeten, die gesuchte Adresszuordnung IP-Adresse => MAC-Adresse mitzuteilen. Das Endsystem mit der Adresse schickt seine Antwort als **ARP-Reply** (MAC-Unicast) mit der gesuchten Zuordnung zurück. Anschließend wird dieses Paar vom ARP in seinem Cache abgelegt.

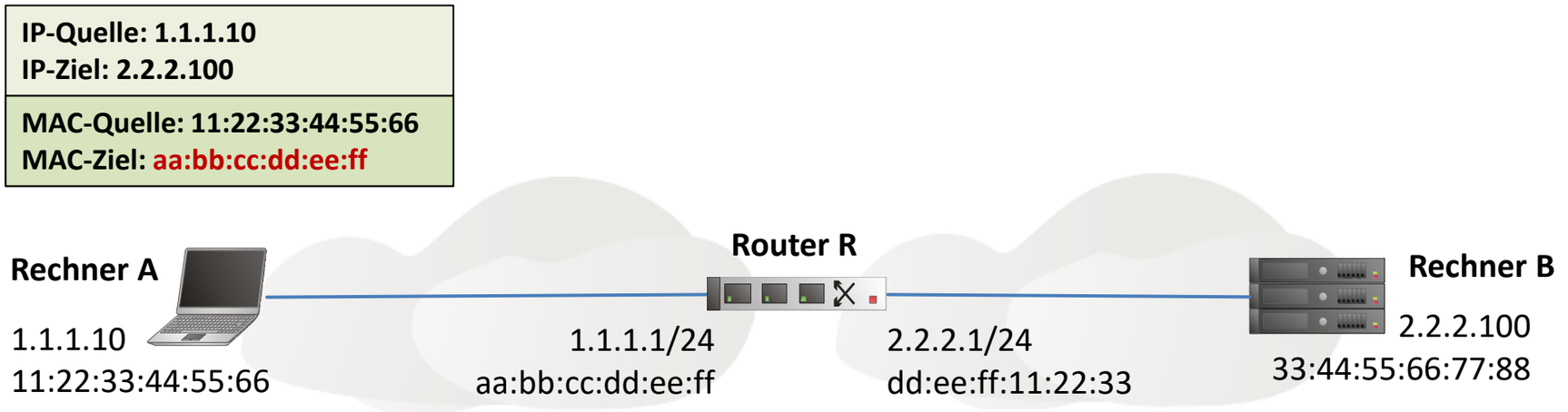
Damit nicht bei jeder Übertragung erneut Anforderungen (ARP-Request) gesendet werden müssen, kopiert auch das Endsystem B, das auf den ARP-Request antwortet, die Zuordnung der IP- und MAC-Adresse des ARP-Request-Absenders (Endsystem A) in seinen eigenen ARP-Cache. Bei einer eventuellen Übertragung in Gegenrichtung (von B zu A) ist es daher nicht mehr nötig, eine ARP-Anforderung in umgekehrter Richtung zu senden, da die MAC-Adresse der IP-Adresse, der gerade geantwortet wurde, bereits bekannt ist.

Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Quelle: Badach, Skript Kommunikationsnetze

Verwendung von ARP bei der Übermittlung zwischen Subnetzen

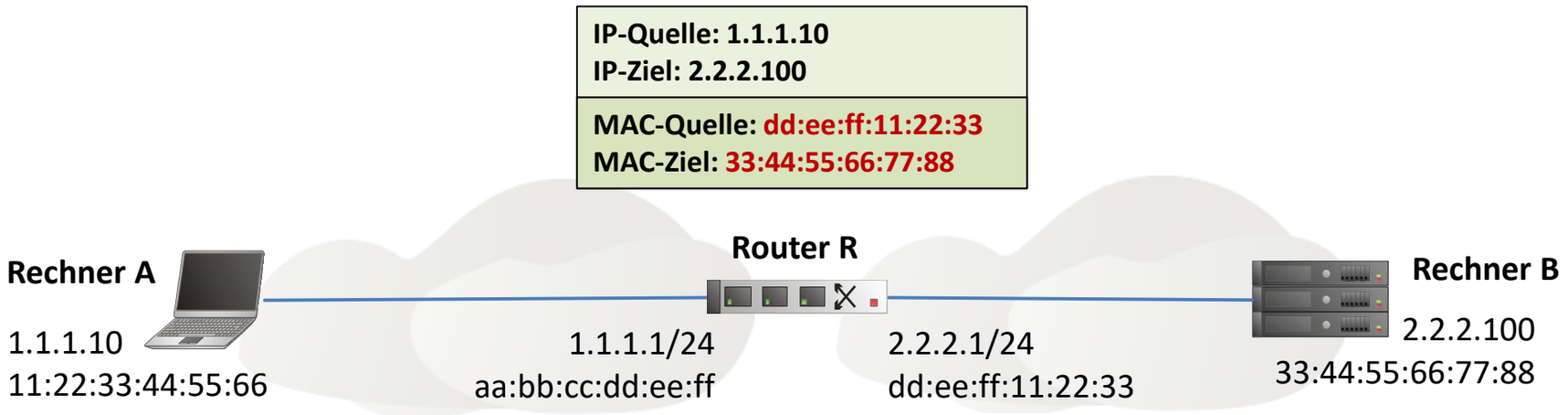
- Rechner A in Subnetz 1 möchte mit Rechner B in Subnetz 2 über Router R kommunizieren.
- Rechner A kennt IP-Adresse von Rechner B (Woher?)
- Rechner A kennt IP-Adresse von Router R (Woher?)
- Rechner A kann MAC-Adresse von R ermitteln (Wie?)
- Rechner A erzeugt IP-Paket, ermittelt MAC-Adresse von Default Gateway R, erzeugt MAC-Frame und sendet es an Router R…



Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

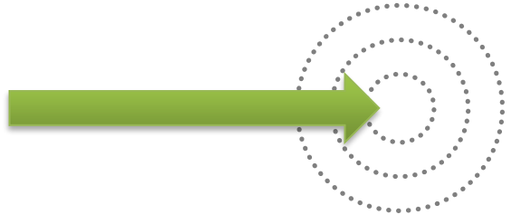
Verwendung von ARP bei der Übermittlung zwischen Subnetzen

- Router R nimmt IP-Paket an
- Router R erkennt, dass Rechner B in seinem Subnetz 2.2.2.0/24 liegt
- Router R ermittelt MAC-Adresse von Rechner B und erzeugt neues MAC-Frame
- IP-Paket und IP-Adressen bleiben gleich
- Beispiel für die Kombination der Aufgaben von Layer 2 und 3 bei der Kommunikation im IP-Subnetz und darüber hinaus



Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Lernzielkontrolle



Ziel: Verstehen, wie die Vermittlungsschicht funktioniert…

- Welche Anforderungen werden an Protokolle auf der Vermittlungsschicht gestellt?
- Was ist das Internet?
- Wie wird gewährleistet, dass Pakete im Internet nicht unendlich zirkulieren?
- Woraus besteht eine IP-Adresse und wie wird ein IP-Subnetz definiert?
- Welche Vorteile bietet das Classless Inter-Domain Routing?
- Wie kann erkannt werden, ob die Ziel-IP-Adresse im gleichen Subnetz ist?
  - Was passiert, wenn die Adresse im gleichen Subnetz ist?
  - Was passiert, wenn sie in einem fremden Subnetz liegt?
- Welche Vorteile bietet das Longest Prefix Matching für das Routing?
- Wie kann das Subnetz 176.16.128.0/17 in fünf neue Subnetze unterteilt werden?
- Erläutern Sie die Verwendung von Ports und privaten IP-Adressen bei NAT.
- Welche Vorteile bietet IPv6? Wie erfolgt die Migration von IPv4 nach IPv6?
- Wie wird die Privatsphäre bei der Verwendung von IPv6 geschützt?
- Welche Aufgaben übernehmen Forwarding und Control Plane bei Routern?
- Was unterscheidet statisches/dynamisches Routing? Welche Typen kennen Sie?
- Welche Vorteile hat OSPF?
- Wie werden bei BGP Prefixes für das Routing im Internet ausgetauscht?
- Warum ist bei BGP ein Policy-based Routing wichtig?
- Welche Funktionen übernimmt das Hilfsprotokoll ICMP?
- Wofür wird ARP benötigt?

Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.

Zusatzaufgaben

„hands-on experience“

- Als praktische Übung zu diesem Kapitel sollten Sie auf einem Rechner zu Hause oder in der Hochschule:
  - Kontrollieren Sie mit dem Befehl „arp -a“, welche ARP-Einträge ihr Rechner kennt.
  - Welche Einträge hat die Routing-Tabelle Ihres Rechners? (unter Windows: „route print“)
  - Starten Sie ein traceroute nach www.stanford.edu. Können Sie ermitteln, an welchem Router Ihre Pakete über den Atlantik übertragen werden?
- Bitte bringen Sie die Ergebnisse mit zur nächsten Veranstaltung!

Anwendung
Transport
Vermittlung
Sicherung
Bitübertr.