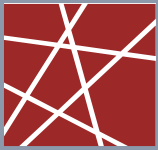




Motivierende Fragen

- ❑ Welche Protokolle gehören zur TCP/IP-Familie ?
- ❑ Welche IP-Dienste gibt es ?
- ❑ Wie ist die Routing-Hierarchie aufgebaut ?
- ❑ Was steckt hinter IPv6 ?
- ❑ Wie lassen sich Internet und Mobilität vereinen ?



Grundlagen: Rechnernetze und Verteilte Systeme

Kapitel 5:

Internet-Protokolle

Internet-Protokolle der Netzwerkschicht

Prof. Dr.-Ing. Georg Carle
Lehrstuhl für Netzarchitekturen und Netzdienste
Technische Universität München
carle@net.in.tum.de
<http://www.net.in.tum.de>





Übersicht

1. Einführung und Motivation
 - Bedeutung, Beispiele
2. Begriffswelt und Standards
 - Dienst, Protokoll, Standardisierung
3. Direktverbindungsnetze
 - Fehlererkennung, Protokolle
 - Ethernet
4. Vermittlung
 - Vermittlungsprinzipien
 - Wegwahlverfahren
5. **Internet-Protokolle**
 - **IP, ARP, DHCP, ICMP**
 - **Routing-Protokolle**
6. Transportprotokolle
 - UDP, TCP
7. Verkehrssteuerung
 - Kriterien, Mechanismen
 - Verkehrssteuerung im Internet
8. Anwendungsorientierte Protokolle und Mechanismen
 - Netzmanagement
 - DNS, SMTP, HTTP
9. Verteilte Systeme
 - Middleware
 - RPC, RMI
 - Web Services
10. Netzsicherheit
 - Kryptographische Mechanismen und Dienste
 - Protokolle mit sicheren Diensten: IPSec etc.
 - Firewalls, Intrusion Detection
11. Nachrichtentechnik
 - Daten, Signal, Medien, Physik
12. Bitübertragungsschicht
 - Codierung
 - Modems



- In diesem Kapitel wollen wir vermitteln
 - TCP/IP-Protokollfamilie
 - Funktionalität von IP-Adressen
 - Zusammenspiel von Protokollen
 - Hierarchie von Routing
 - Funktionalität von IPv6
 - Mobilität im Internet



5.1. Internet-Architektur

5.1.1. Internet-Protokollfamilie

5.1.2. TCP/IP-Protokollfamilie

5.1.3. Zusammenspiel

5.1.4. IP-Adressen

5.1.5. NAT

5.1.6. DHCP

5.1.7. IP-Dienste

5.1.8. Routing-Hierarchie (u.a. OSPF, RIP, BGP, CIDR, IGMP)

5.1.9. ARP

5.1.10. IPv6

5.2. Mobilität im Internet

5.2.1. Terminologie

5.2.2. Beispielnetz



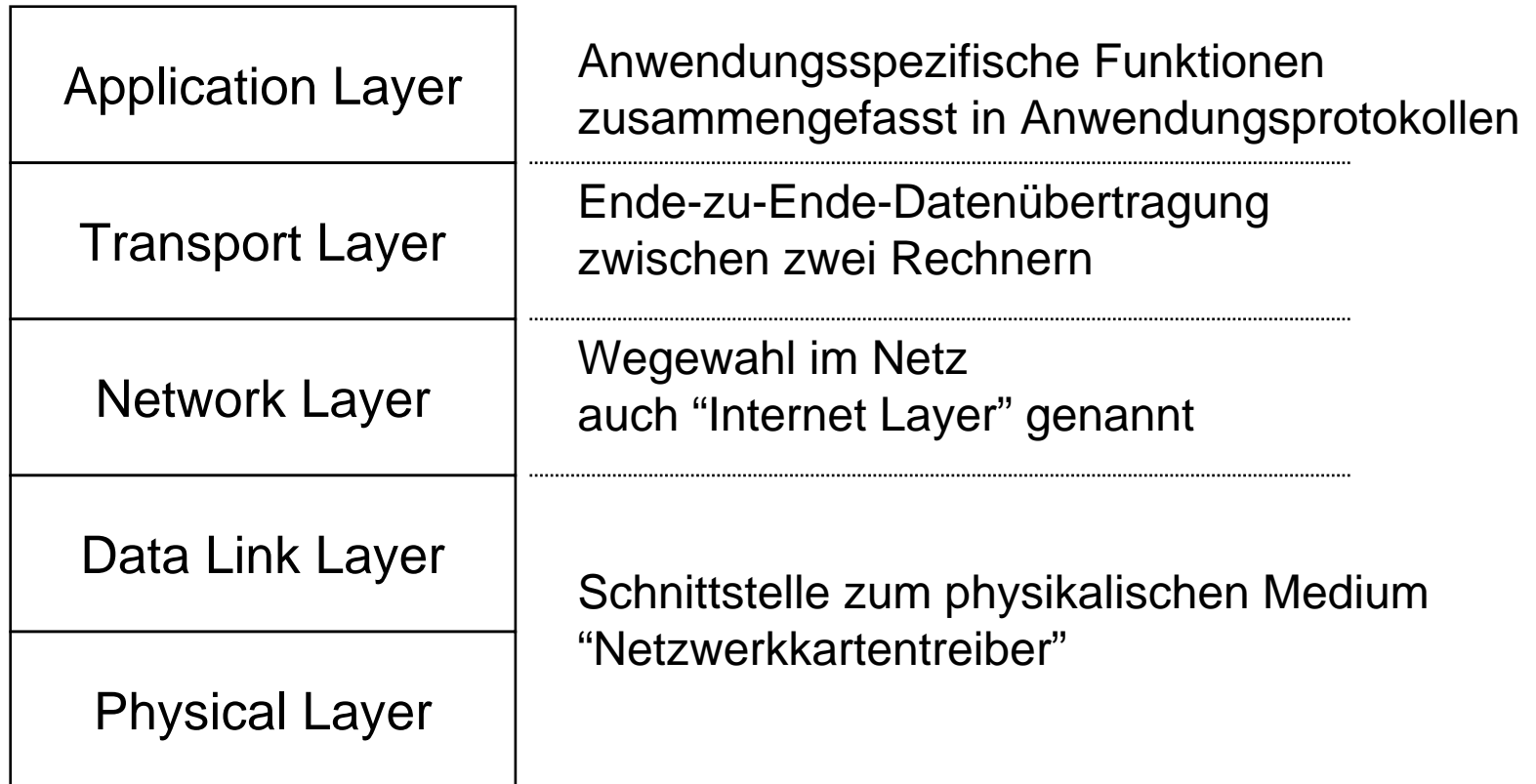
5.1. Internet-Architektur: Merkmale

- Grundlegende Entwurfsprinzipien:
 - Keine Zustandsinformation in den Zwischensystemen halten
⇒ bei Ausfall keine Resynchronisation notwendig
 - Datenstrom-spezifische Information wird in den Endsystemen gespeichert
⇒ Bestandteil des Ende-zu-Ende-Prinzips
 - Trennung der Weiterleitung der Pakete („Forwarding“) vom „Routing“ = Erstellung der Weiterleitungstabellen

- IP-Basiskommunikationsdienst:
 - verbindungslos, unzuverlässig
 - abschnittsweise Weiterleitung, speichervermittelt
 - „Best Effort“-Dienstleistung: so gut wie möglich mit den momentan vorhandenen Ressourcen



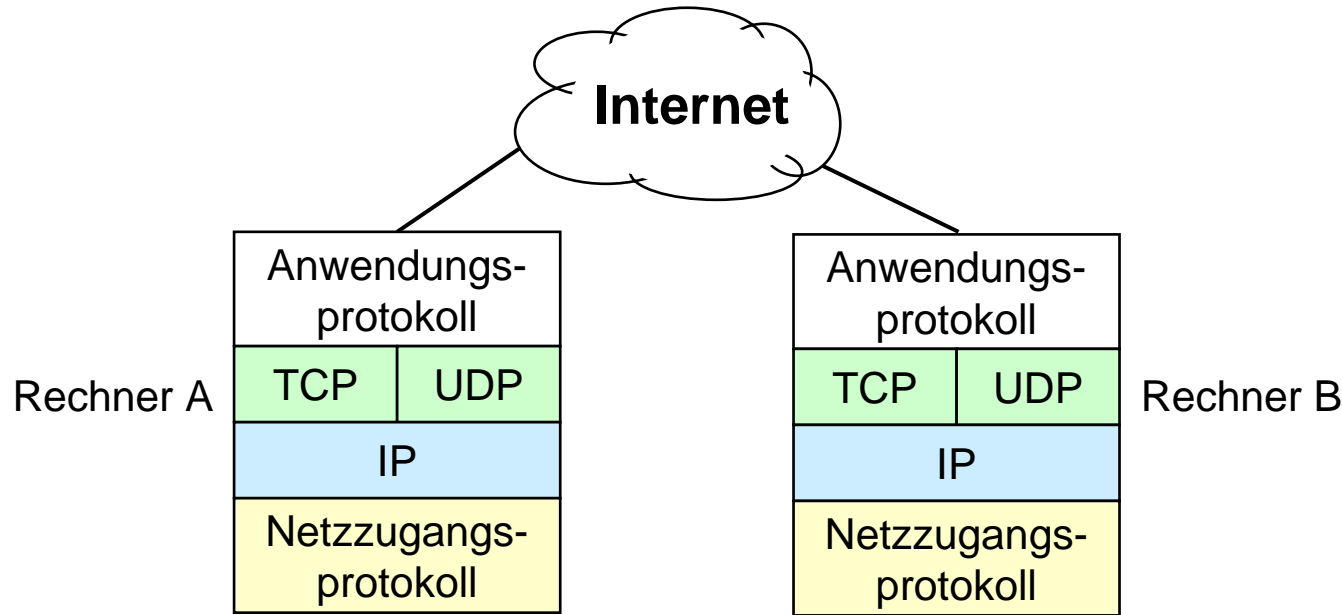
Wiederholung: Die Internet-Protokollhierarchie



- Gegenüber ISO/OSI wurden die drei anwendungsorientierten Schichten zu einer einzigen Schicht zusammengefasst.



5.1.1. Die Internet-Protokollfamilie

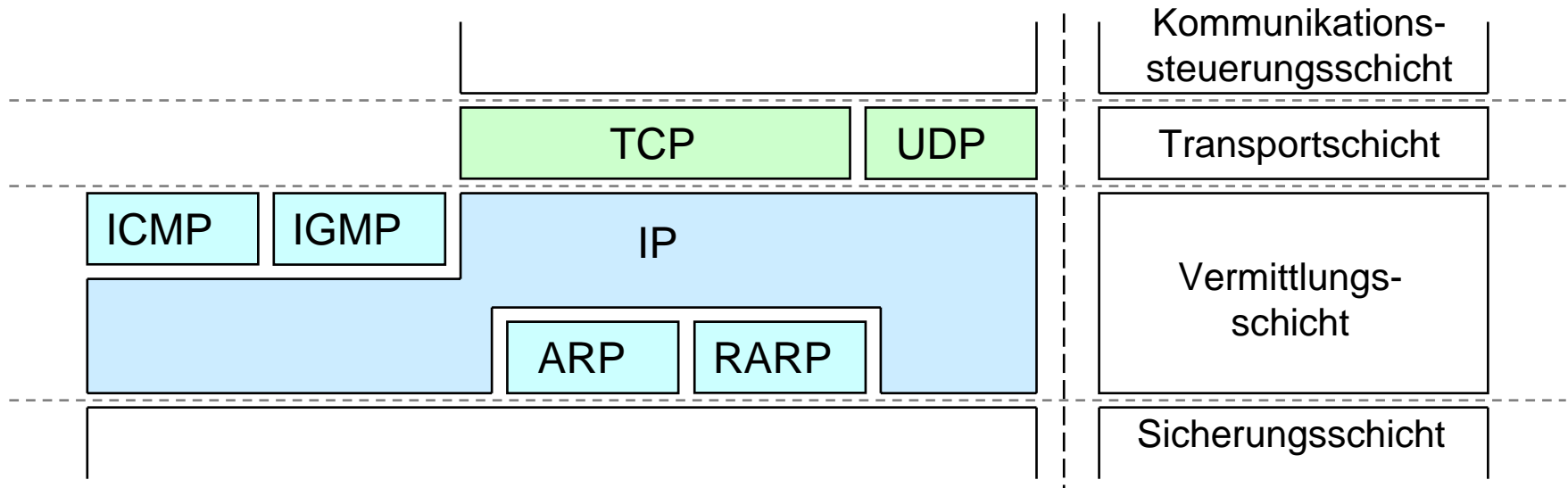


- ❑ **TCP** (Transmission Control Protocol):
 - Zuverlässiges, verbindungsorientiertes Transportprotokoll über unzuverlässigem IP (Internet Protocol).
- ❑ **UDP** (User Datagram Protocol):
 - Verbindungsloses Transportprotokoll, bietet Anwendungsschnittstelle zu IP und Multiplexdienst.
- ❑ Beispiele für **Anwendungsprotokolle**:
 - HTTP: HyperText Transfer Protocol (im WWW benutzt)
 - FTP: File Transfer Protocol
 - Telnet: Protokoll für virtuelle Terminals



5.1.2. Die TCP/IP-Protokollfamilie – Überblick

- ❑ Die Bezeichnung TCP/IP wird häufig als Synonym für die gesamte Protokollfamilie verwendet
- ❑ Einordnung der Internetprotokolle in das ISO/OSI-Referenzmodell:



- ❑ Obwohl die IP-Steuerungsprotokolle ICMP und IGMP den IP-Dienst nutzen, werden sie dennoch der Vermittlungsschicht zugeordnet
- ❑ In den anwendungsbezogenen Schichten 5-7 werden im Internet Protokolle wie z.B. FTP, TELNET oder SMTP eingesetzt (Schichten 5-7 im Internet zusammengefasst zur Anwendungsschicht)



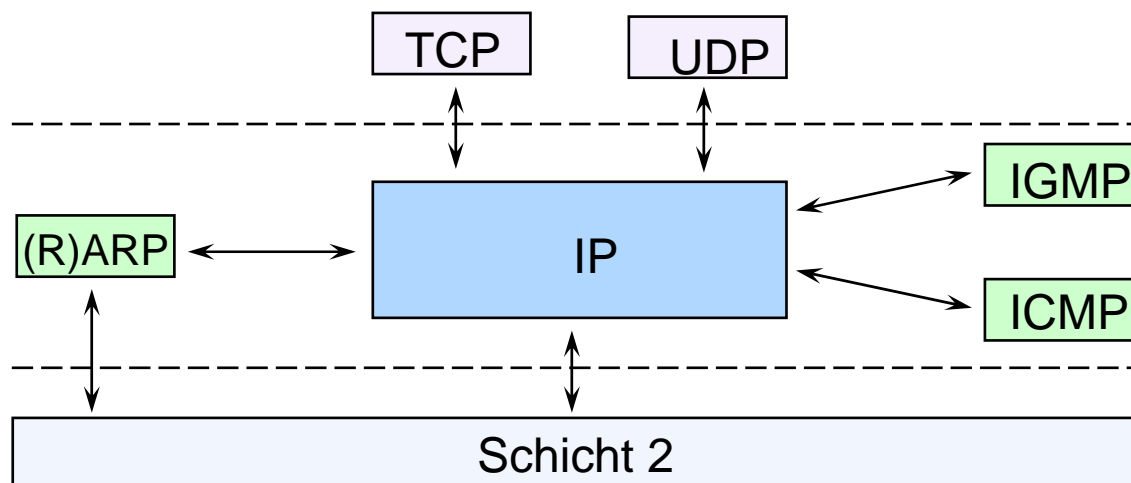
Die TCP/IP-Protokollfamilie: Protokollaufgaben

- TCP (Transmission Control Protocol): Stellt verbindungsorientierten, gesicherten Transportdienst bereit
- UDP (User Datagram Protocol): Stellt verbindungslosen, ungesicherten Transportdienst bereit
- IP (Internet Protocol): Sorgt für Wegewahl und ungesicherte Übertragung von Datagrammen
- ICMP (Internet Control Message Protocol): Unterstützt den Austausch von Steuerungsinformationen innerhalb der Vermittlungsschicht
- IGMP (Internet Group Management Protocol): Unterstützt die Verwaltung von Kommunikationsgruppen
- ARP (Address Resolution Protocol): Unterstützt die Zuordnung von IP-Adressen zu den entsprechenden Adressen der Sicherungsschicht
- RARP (Reverse Address Resolution Protocol): Stellt die Umkehrfunktion von ARP zur Verfügung



5.1.3. Zusammenspiel: IP-Instanz und angrenzende Instanzen

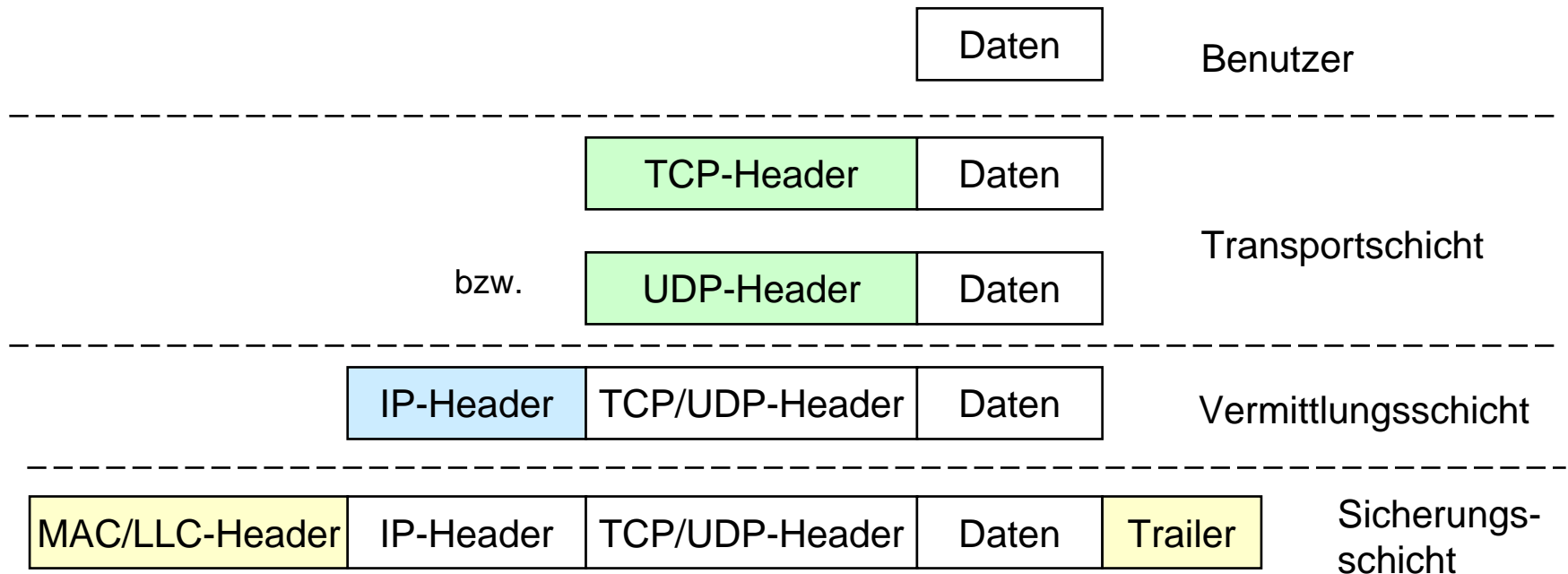
- ❑ Schicht-4-Instanz (TCP- bzw. UDP) übergibt die Daten zusammen mit der IP-Adresse des Empfängers zur Übertragung an die IP-Instanz
- ❑ IP-Instanz beauftragt ARP-Instanz mit Ermittlung der entsprechenden Schicht-2-Adresse
- ❑ IP-Instanz übergibt PDUs zusammen mit der ermittelten Schicht-2-Adresse an die Instanz der Sicherungsschicht
- ❑ IP-Instanz reicht empfangene Daten an TCP- bzw. UDP-Instanzen weiter
- ❑ Probleme während der Übermittlung können den Partnerinstanzen über ICMP mitgeteilt werden
- ❑ Informationen über Gruppenzugehörigkeiten werden mittels IGMP (Internet Group Management Protocol) im Netz verbreitet





Zusammenspiel der Protokollinstanzen: die PDUs

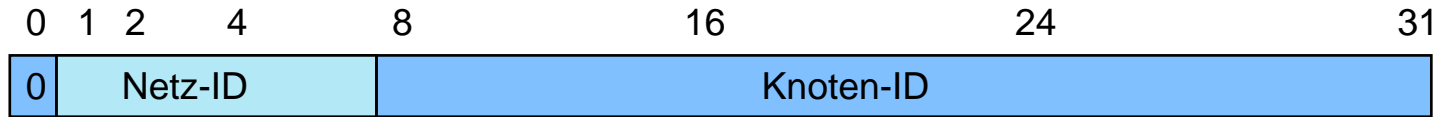
- ❑ IP leitet Datenpakete durch das Netzwerk zum Empfänger
- ❑ TCP/UDP fügen Prozessadressierung (Ports) zu IP hinzu
- ❑ TCP sichert darüberhinaus die Datenübertragung
- ❑ Protokolldateneinheiten (PDUs) werden gekapselt





5.1.4. IP-Adressen / Adressklassen (historisch)

- **Class A** für Netze mit bis zu 16 Mio. Knoten (0.0.0.0 - 127.255.255.255):



- **Class B** für Netze mit bis zu 65.536 Knoten (128.0.0.0 - 191.255.255.255):



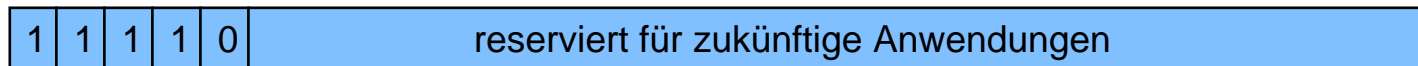
- **Class C** für Netze mit bis zu 256 Knoten (192.0.0.0 - 223.255.255.255):



- **Class D** für Gruppenkommunikation (Multicast) (224.0.0.0 - 239.255.255.255):



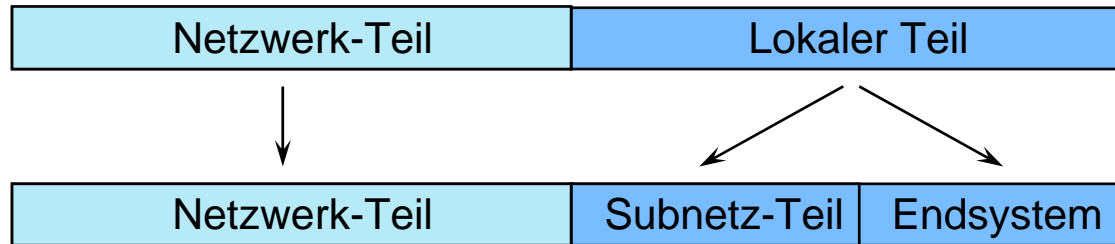
- **Class E**, noch reserviert für zukünftige Anwendungen (240.0.0.0 - 247.255.255.255):





IP-Subnetz-Adressen

- **IP-Adresse** (hier Class B):



- **Subnetzmasken** kennzeichnen den Bereich der IP-Adresse, der das Netzwerk und das Subnetzwerk beschreibt. Dieser Bereich wird dabei durch Einsen („1“) in der binären Form der Subnetzmaske festgestellt. Subnetzmasken haben keine Internet-weite Gültigkeit.

- **Beispiel:**

IP-Adresse:	129.	13.	3.	64
	1000 0001	0000 1101	0000 0011	0100 0000
Subnetzmaske:	255.	255.	255.	0
	1111 1111	1111 1111	1111 1111	0000 0000
Netzwerk:	129.	13.		
Subnetz:			3.	
Endsystem:				64



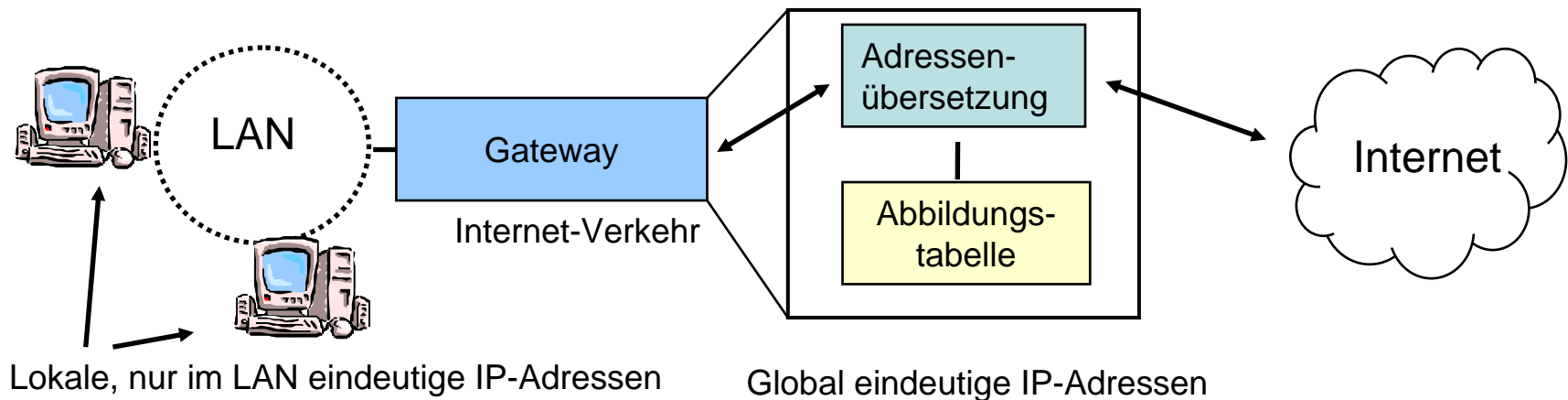
CIDR: Classless Inter-Domain Routing

- Bisher: 3 Adressklassen für Unicast (A, B und C)
 - schlechte Ausnutzung durch ungenutzte Adressen („Verschnitt“)
 - ⇒ Granularität der Netze häufig nicht passend; Anzahl der Netze zu klein
- Beispiel:
 - Kleinbetrieb, der 100 IP-Adressen braucht, beantragt Class-C-Netz
 - 254 Adressen könnten vergeben werden, damit **154 ungenutzte Adressen**
- **CIDR**: Ersetzen der festen Klassen durch **Netzwerk-Präfixe** variabler Länge
 - Bsp.: 129.24.12.0/14 → Die ersten 14 Bits der IP-Adresse werden für die Netzwerk-Identifikation verwendet
- Einsatz in Verbindung mit hierarchischem Routing:
 - Backbone-Router, z.B. an Transatlantik-Link, betrachtet nur z.B. die ersten 13 Bit; dadurch kleine Routing-Tabellen, wenig Rechenaufwand
 - Router eines angeschlossenen Providers z.B. die ersten 15 Bit
 - Router in einem Firmennetz mit 128 Hosts betrachtet die ersten 25 Bit



5.1.5. Network Address Translation/Translator (NAT)

- Nur Rechner, die gerade mit der Außenwelt kommunizieren, benötigen eine global eindeutige Adresse
 - Diese global eindeutige Adresse kann temporär vergeben werden
 - Gateway/Router nimmt transparente Umsetzung zwischen Adressen/Adressbereichen vor
 - Speicherung in Abbildungstabelle
 - keine Änderungen an Endgeräten erforderlich
- ⇒ Identitäten der Hosts werden verborgen





NAT - weitere Eigenschaften

□ **Abbildungsarten:**

- **Statisch:** lokale Adresse \Leftrightarrow globale Adresse
 - z.B. 192.168.39.100 \Leftrightarrow 129.13.41.100
- **Dynamisch:** lokale Adresse \Leftrightarrow globale Adresse aus Adresspool
 - Erzeugen eines „Simple Entry“ in Abbildungstabelle ($IP_{\text{lokal}} \Leftrightarrow IP_{\text{global}}$)
- **Overloading:**
 - Abbildung aller lokalen Adressen auf eine einzige globale Adresse
 - zusätzliches Unterscheidungskriterium: Portnummern
 - Erzeugen eines „Extended Entry“ in Abbildungstabelle
 - Protokoll, ($Port_{\text{lokal}}, IP_Ad_{\text{lokal}}$) \Leftrightarrow ($IP_Ad_{\text{global}}, Port_{\text{global}}$)

Protokoll	lokaler Port	lokale IP-Addr.	globaler Port	globale IP-Addr.	Ziel-IP-Addr.	Ziel-Port
TCP	1024	192.168.1.1	1024	129.133.3.1	207.171.4.4	1234
TCP	1500	192.168.1.2	1500	129.133.3.1	134.100.4.4	80



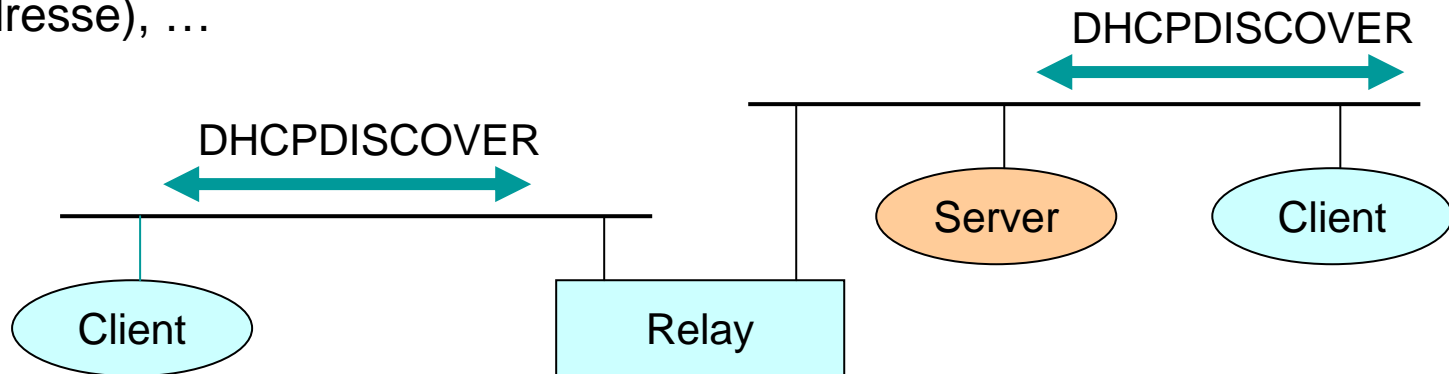
5.1.6. DHCP: Dynamic Host Configuration Protocol

□ Anwendung

- Vereinfachung der Installation und Verwaltung von vernetzten Rechnern
- liefert Rechnern notwendige Informationen über IP-Adresse, DNS-Server-Adresse, Domain-Namen, Subnetz-Masken, Router etc.
- damit weitgehend automatische Integration eines Rechners in das Internet bzw. Intranet

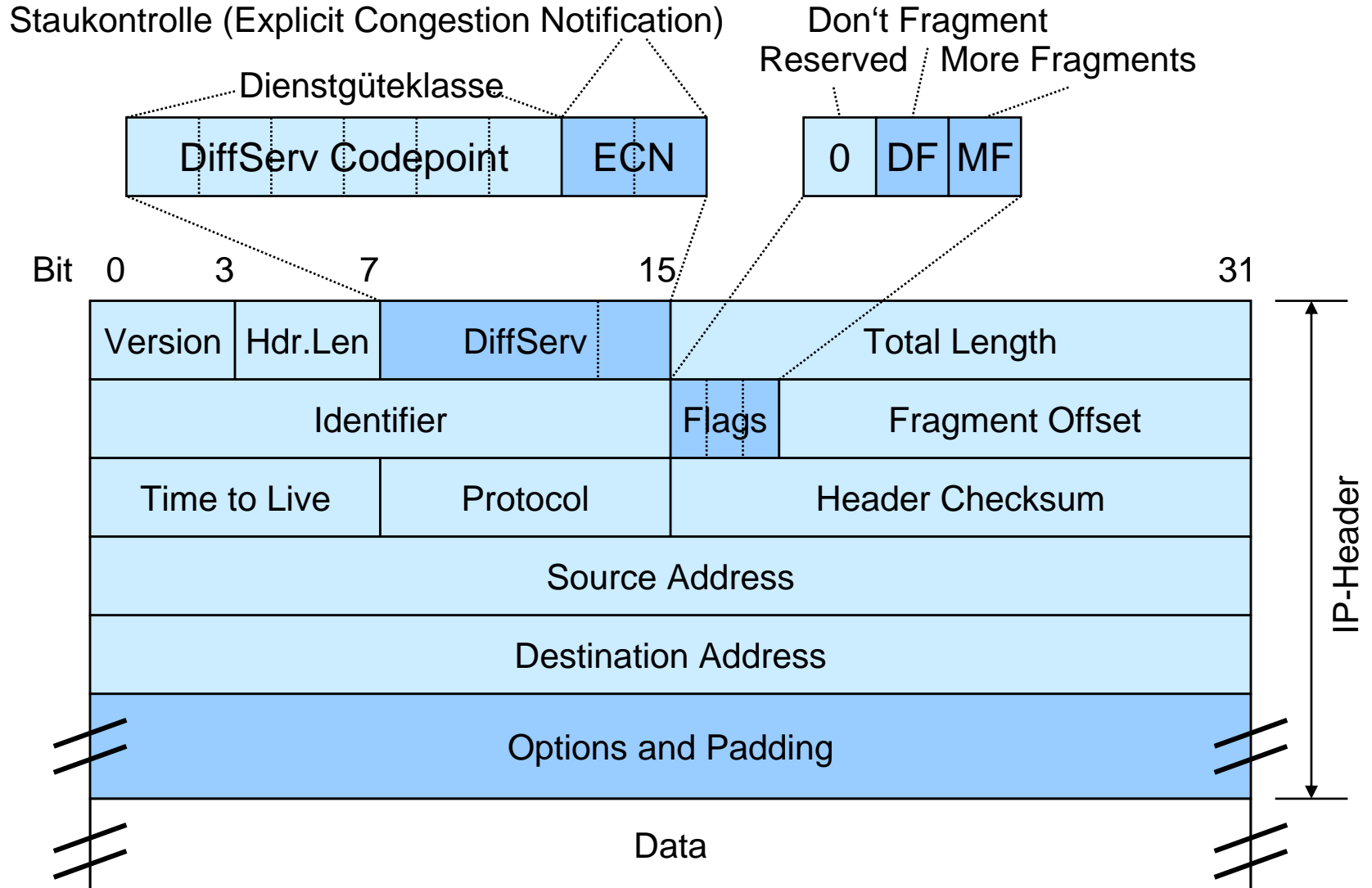
□ Client/Server-Modell

- ein Client sendet via IP-Broadcast eine Anfrage an einen DHCP-Server an UDP Port 67 (unter Umständen über ein DHCP-Relay)
Clientanfragen: DHCPDISCOVER, DHCPREQUEST, DHCPRELEASE, ...
- der Server antwortet (initial via IP-Broadcast) und liefert die angeforderte Konfiguration. Serverantworten: DHCPPOFFER, *DHCPACK* (mit IP-Adresse), ...





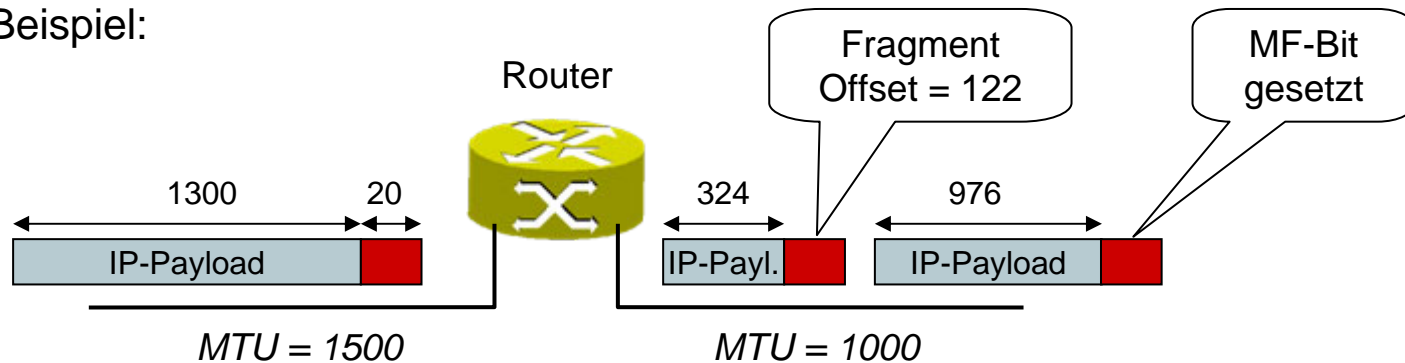
IP Datagramm: Aufbau





IP-Fragmentierung

- Größe eines IP-Pakets durch maximale Rahmengröße auf Schicht 2 begrenzt
 - MTU (Maximum Transport Unit): maximale Nutzdatenlänge in Schicht-2-Rahmen
 - Beispiel IEEE 802.3: MTU = 1500 Byte
- IP-Endsysteme kennen MTU der angeschlossenen Netzwerkadapter
 - Sender passt i.d.R. Paketgröße an lokale MTU an
- IP-Fragmentierung wird notwendig, wenn Paket über einen Link mit kleinerer MTU geroutet wird
 - Fragmentierung der IP-Payload an 8-Byte Grenzen
 - Beispiel:



- Fragmentierung heutzutage durch Path-MTU-Discovery vermieden (→ ICMP)

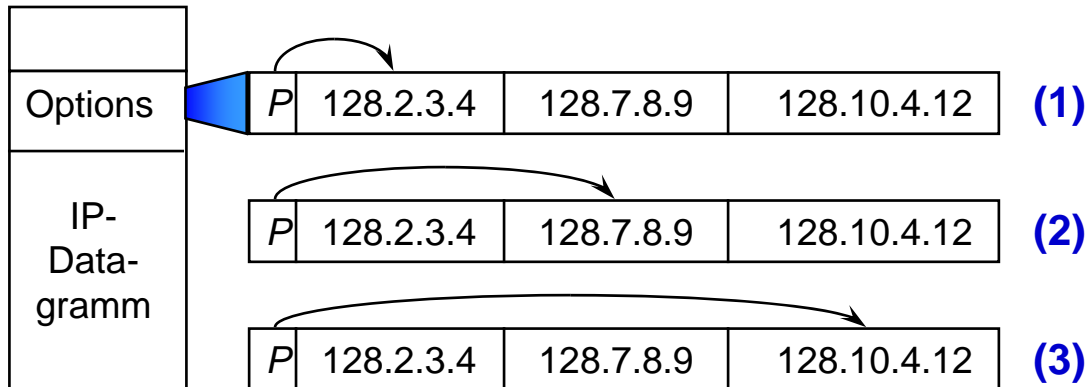
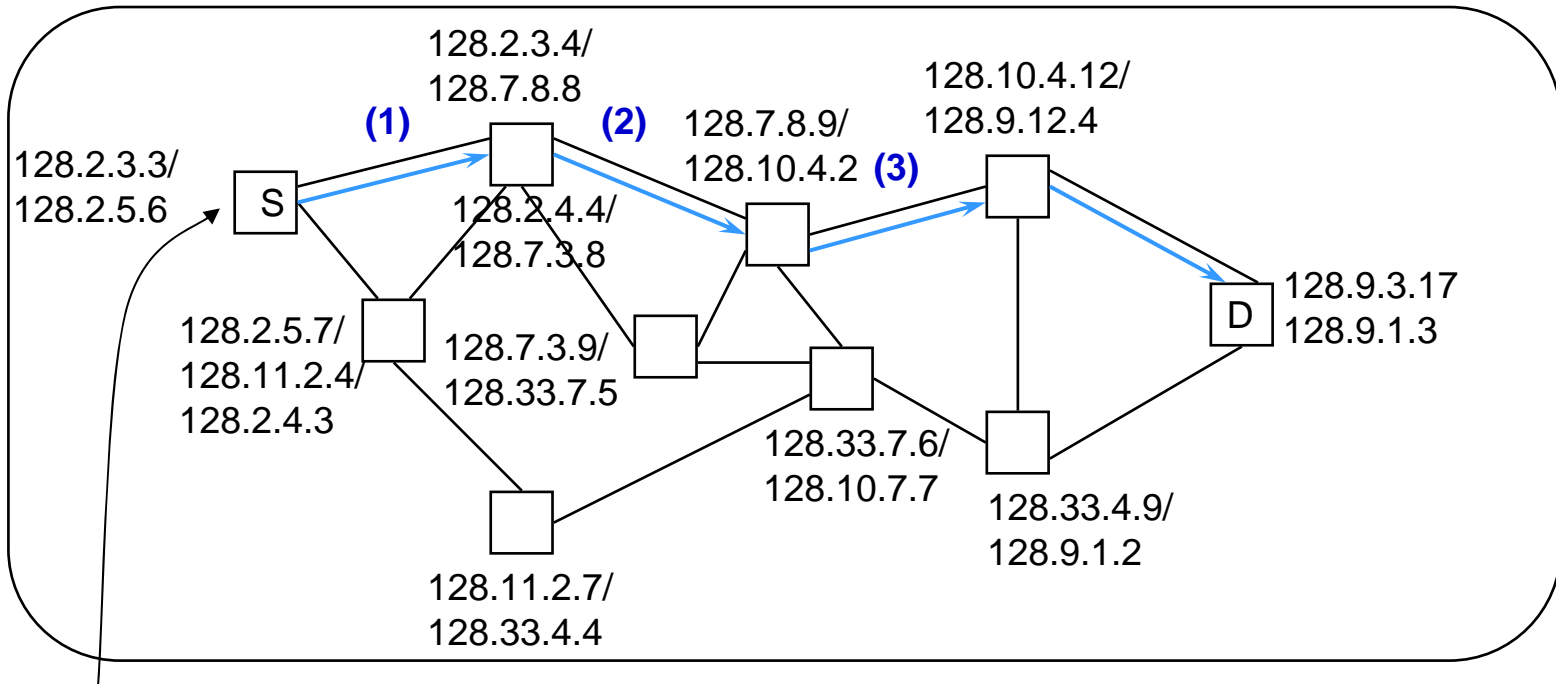


5.1.7. IP-Dienste: Überprüfung des Paketkopfes

- Überprüfungen, die nach dem Empfang eines IP-Datagrammes am Header durchgeführt werden
 - Überprüfung der korrekten Länge des Headers
 - Test der IP-Versionsnummer
 - Überprüfung der korrekten Datagrammlänge
 - Prüfsummenbildung über den IP-Header
 - Überprüfung der Paketlebenszeit
 - Überprüfung der Protokoll-ID
- Bei negativem Resultat eines der oben aufgeführten Tests wird das Paket einfach verworfen und eine Fehlermeldung über ICMP an den Sender des Pakets gesendet



Optionale IP-Dienste: Source Routing – Beispiel



Hinweis:
 Jeder Schnittstelle (Interface) ist eine eigene IP-Adresse zugeordnet. Im Diagramm sind aber nicht alle IP-Adressen aufgeführt.



Optionale IP-Dienste: Zeitstempel

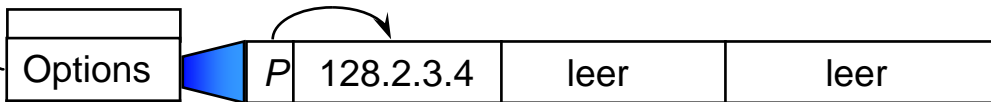
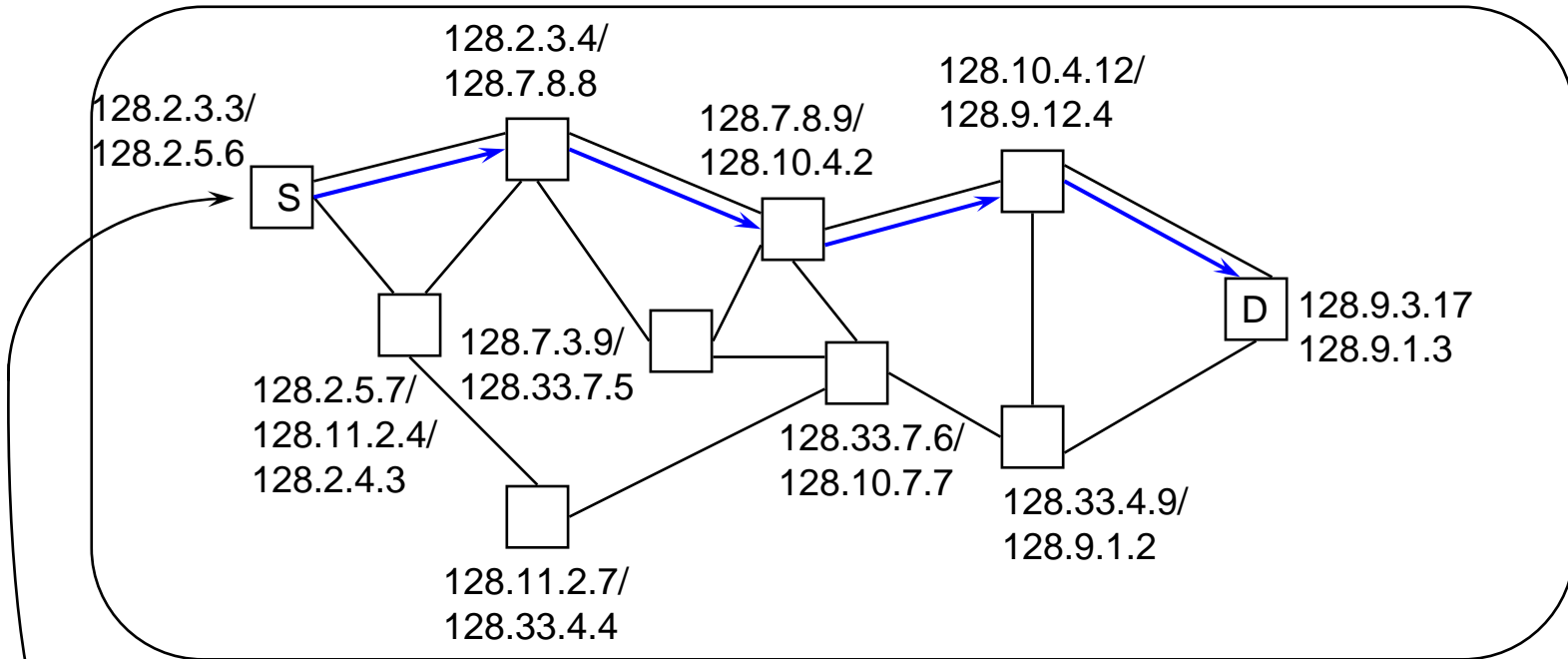
- Jeder Router fügt im Optionsfeld einen Zeitstempel ein, der den Zeitpunkt charakterisiert, zu dem das Paket vom Router bearbeitet wurde.
 - Aussagen über die Belastung der Netzwerke sind möglich
 - Die Effizienz der benutzten Routing-Algorithmen kann abgeschätzt werden

- Dabei existieren folgende Möglichkeiten, die durch ein 4 Bit langes Flag-Feld definiert werden:
 - Flag-Wert = 0: Nur Zeitstempel aufzeichnen, keine Adressen.
 - Flag-Wert = 1: Sowohl Zeitstempel als auch Adressen (Route Recording) aufzeichnen
 - Flag-Wert = 3: Die Adressen sind vom Sender vorgegeben (Source Routing), die adressierten Router tragen nur ihren Zeitstempel ein

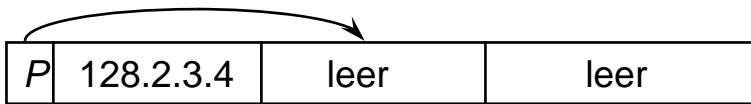


Optionale IP-Dienste: Route Recording

- Im Record-Route-Options-Feld wird der durchlaufene Weg festgehalten



1. Füge eigene Adresse an der durch den Pointer P festgelegten Stelle ein ...



2. ... und erhöhe dann den Pointer P um 4 [byte], so dass er auf das nächste leere Feld in der Liste zeigt



Übersicht: IP-Routing Protokolle

- **IGP** (Interior Gateway Protocol): zur Wegewahl *innerhalb* einer Verwaltungseinheit (Administrative Domain oder Autonomous System)
 - **RIP** (Routing Information Protocol) basierend auf Distance-Vector-Algorithmus (überall verfügbar, aber veraltet)
 - **OSPF** (Open Shortest Path First) basierend auf Link-State-Algorithmus (neuer Standard)
 - **IS-IS** (Intermediate System-Intermediate System), ebenfalls Link-State-Algorithmus, aus der OSI-Welt, teilweise auch im Internet eingesetzt

- **EGP** (Exterior Gateway Protocol): Wegewahl *zwischen* Verwaltungseinheiten, sog. „politische Firewall“
 - EGP (Protokoll gleichen Namens!, veraltet)
 - **BGP** (Border Gateway Protocol, derzeit Version BGP4, RFC 1654)
 - Anwendungen:
 - Verhindern des Durchleitens „fremder“ Pakete durch eigenes Netz, obwohl der Weg kürzer ist
 - politische Restriktionen
 - Firmenpolitik (Firma X will nicht für den Transport der Pakete von Firma Y bezahlen)



Dynamische Wegewahl im Internet

Wegewahl im Internet

Interior Gateway Protocols (IGP)

- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF)

Exterior Gateway Protocols (EGP)

- Exterior Gateway Protocol (EGP) - veraltet
- Border Gateway Protocol (BGP) - aktuell

Autonomes System (AS):

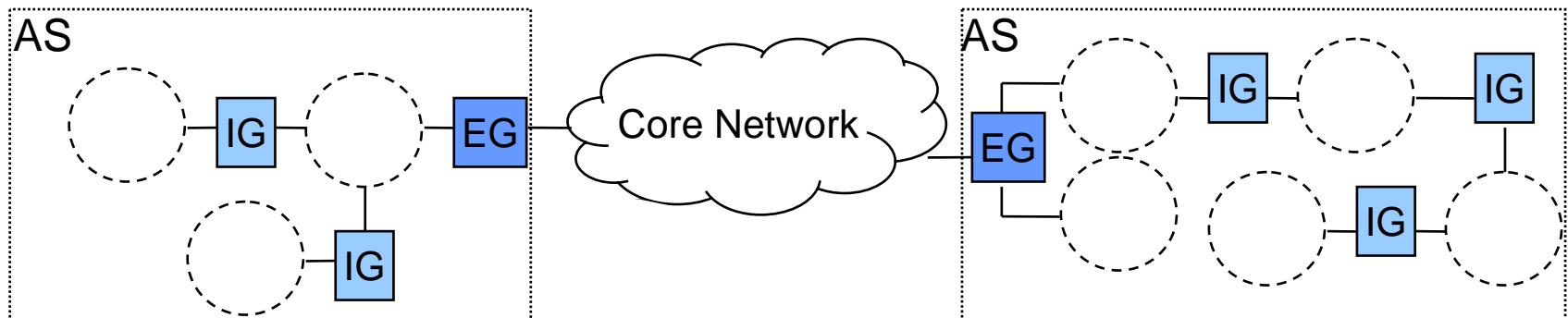
Netz(e) unter einheitlicher Verwaltung

Interior Gateway (IG):

Interner Router eines AS

Exterior Gateway (EG):

Router am Rande eines AS





5.1.8. Routing Hierarchie – Protokolle

□ Intra-Domain-Routing:

- OSPF (Open Shortest Path First)
 - vom IAB empfohlenes Protokoll
 - „Link State“-Verfahren
- RIP (Routing Information Protocol) - früher bzw. heute bei kleinen Netzen
 - wenig robust in komplexeren Netzwerken (Schleifenbildung)
 - langsamer bei Änderungen
 - Distanzvektorverfahren

□ Inter-Domain-Routing:

- BGP (Border Gateway Protocol)
 - Pfad-Vektor-Verfahren
 - BGP Version 4 (BGP4) unterstützt Classless Inter-Domain Routing (CIDR)



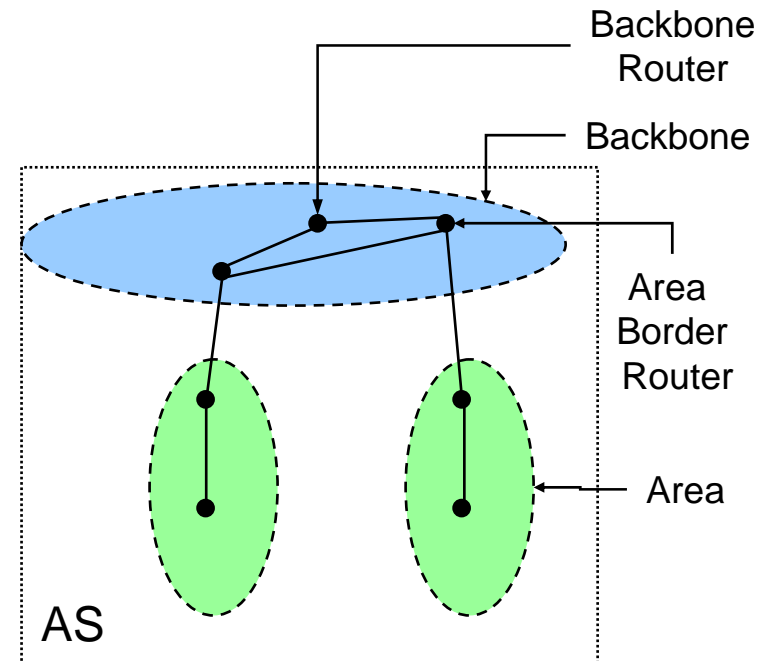
OSPF (Überblick)

□ Grundlage:

- Verbessertes Link State Routing
- Basiert auf der Berechnung eines kürzesten Pfades von der Quelle zum Ziel
- Hierarchische Aufteilung des AS
- Intra-Area-, Inter-Area-, Inter-AS-Verkehr
- Je Area Auswahl eines "Designated Router" (DR) und eines Backup-DR

□ Eigenschaften:

- Unterstützung unterschiedlichster Metriken, z.B. Anzahl Hops, Verzögerung
- Adaptiv (d.h. reagiert auf Topologieänderungen)
- Lastausgleich (Berücksichtigung verschiedener Wege) zum Zielknoten
- Unterstützung hierarchischer (Sub-)Netze
- Unterstützung verschiedener Wege





Intra-Domain-Routing mit OSPF

- ❑ Namensgebung:
 - Open: offener Entwicklungsprozess der IETF
 - SPF: durch Dijkstras Algorithmus kürzeste Pfade in Graph zu finden
Komplexität: $O(n \log n)$, $n = \#Links$
- ❑ Je OSPF-Area nicht mehr als 200 Router empfohlen
- ❑ Jeder Knoten
 - besitzt komplettes Abbild des Netzwerks (Routing-Datenbank) und
 - berechnet selbständig alle Pfade mit SPF-Algorithmus
- ❑ Austausch von geänderten Einträgen durch Fluten (bestätigt)
- ❑ Periodischer Austausch von Einträgen (Link-ID, Version)
→ interessante Einträge werden explizit angefordert
- ❑ Unterstützung mehrerer Metriken und mehrfacher Pfade
- ❑ Externe Routen werden gesondert eingetragen und vermerkt

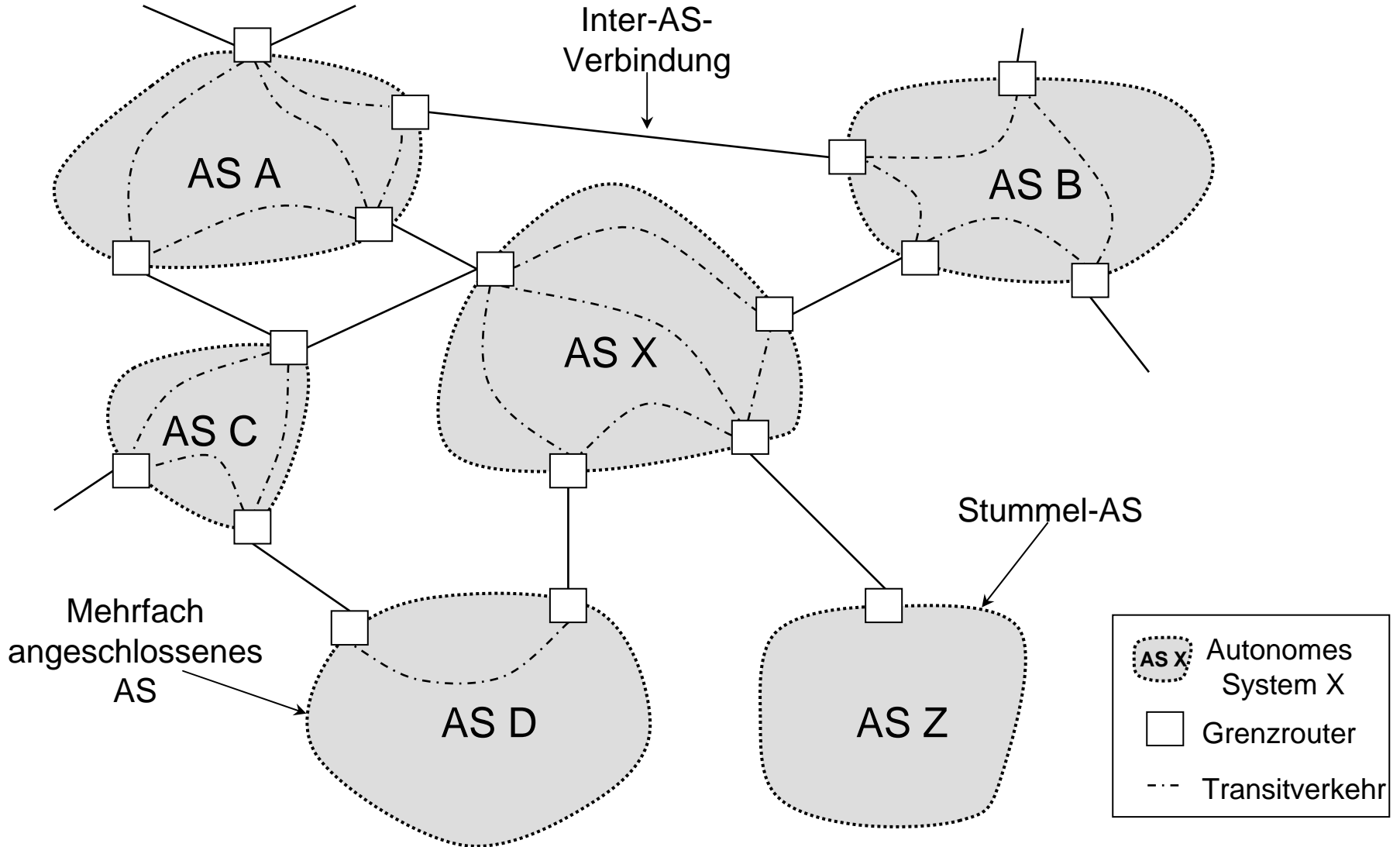


Autonome Systeme im Internet

- ❑ **Autonomes System (AS):** Zusammenhängende Menge von Routern und Netzwerken unter derselben Administration
- ❑ Änderungen innerhalb des Systems sollen verborgen bleiben
- ❑ Betreiber möchte i.A. interne Struktur nicht bekannt geben
- ❑ Innerhalb eines AS sind auch unterschiedliche Intra-Domain-Routing-Protokolle möglich (RIP, OSPF)
- ❑ Jedes AS erhält eine eindeutige AS-Nummer (16 Bit)
- ❑ Derzeit > 14000 Autonome Systeme, davon
 - ~ 80% Stub/Origin only-AS
 - ~ 19% Mixed-AS
 - ~ 1% Transit-AS
 - Details siehe u.a.: <http://bgp.potaroo.net/> (bgp table growth)



Internet-Architektur: Autonome Systeme





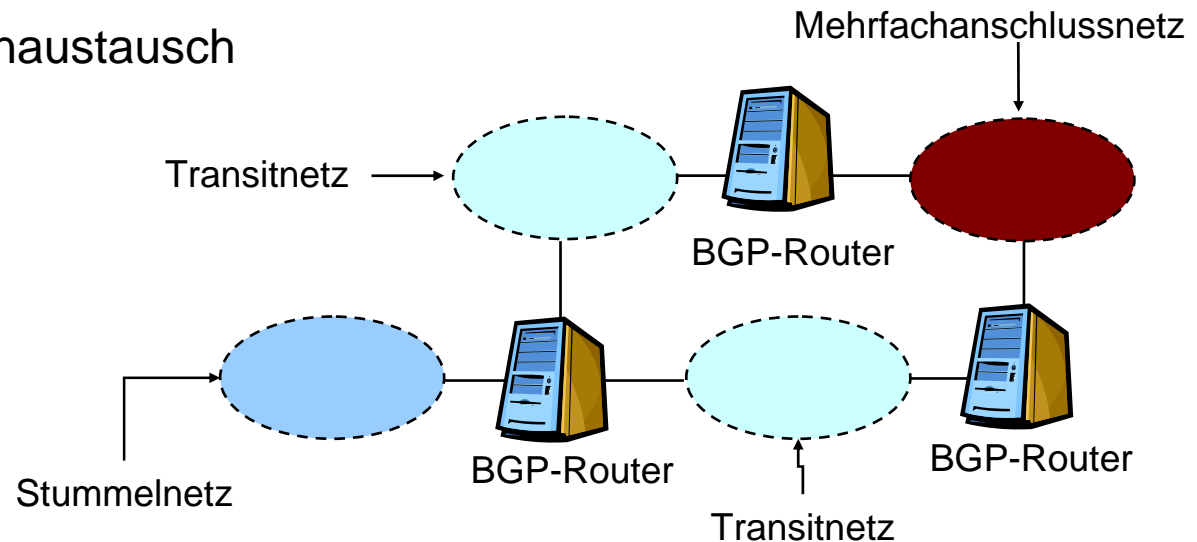
BGP (Überblick)

□ Aufgabe:

- Wegewahl zwischen autonomen Systemen (AS) unter Berücksichtigung besonderer politischer, wirtschaftlicher oder sicherheitsbezogener Regeln (Policies).

□ Grundlage:

- Distance Vector Routing
- Exakter Pfad zum Zielknoten wird gespeichert
- BGP-Router tauschen komplette Pfade aus (→ Path Vector Routing)
- Routing innerhalb der AS wird nicht betrachtet
- TCP zum Datenaustausch





Inter-Domain-Routing mit BGP

- ❑ Welche Netzwerke sind über die Nachbardomänen erreichbar?
- ❑ Protokoll zum Austausch dieser Informationen: BGP-4 [RFC 1771]
- ❑ Unterstützung von Classless Interdomain Routing (CIDR)
- ❑ Berücksichtigung politischer Entscheidungen (Routing policies) möglich, daher Angabe kompletter Pfade (Schleifenfreiheit):

Dest. Net.	Next-Hop	Pfad
141.3.0.0/16	195.221.222.254	5409 1275 553

- ❑ Austausch der Routing-Tabellen bzw. der Änderungen erfolgt über TCP-Verbindungen
- ❑ Größe der Routingtabelle: derzeit bis zu 140000 Einträge
- ❑ Import von Routen des Intra-Domain-Routing-Protokolls



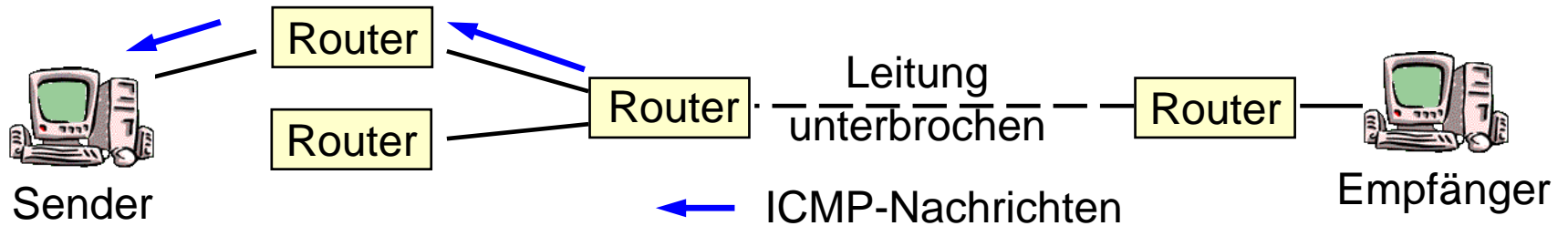
Zusammenspiel: OSPF ↔ BGP

- ❑ Innerhalb eines AS muss jeder Router zu jedem Netzwerk-Präfix eine Route kennen
- ❑ Die Border-Router im Backbone-Bereich importieren und exportieren Routen zwischen BGP und OSPF
- ❑ Jeder Border-Router stellt mit jedem anderen Border-Router des AS eine interne BGP-Verbindung her
- ❑ Einfacher Fall: nur ein Router stellt die Verbindung zu externen Systemen her (Stub-Area) → Default-Route eintragen
- ❑ Weiterer Fall: Default-Route mit zusätzlichen expliziten Angaben
- ❑ Mehrere Router mit externer Verbindung:
komplette Routing-Tabelle mit sämtlichen Zielnetzwerk-Präfixen notwendig (in OSPF importierte externe Routen)



Steuerung von IP: ICMP

- ❑ IP ist nur für den (unzuverlässigen) Datenaustausch zuständig.
- ❑ Für Fehlerfälle oder Testzwecke wird ICMP (Internet Control Message Protocol) verwendet.



Nachrichtentypen, Beispiele:

- ❑ *Destination Unreachable*: Ziel nicht erreichbar.
- ❑ *Time Exceeded*: Time-to-Live-Feld eines Pakets ist abgelaufen.
- ❑ *Echo Request / Reply*: Echo Reply wird angefordert ("ping").
- ❑ *Timestamp Request / Reply*: Ähnlich Echo Request. Zusätzlich Zeitstempel mit Ankunftszeit der Anfrage/Sendezeit der Antwort.



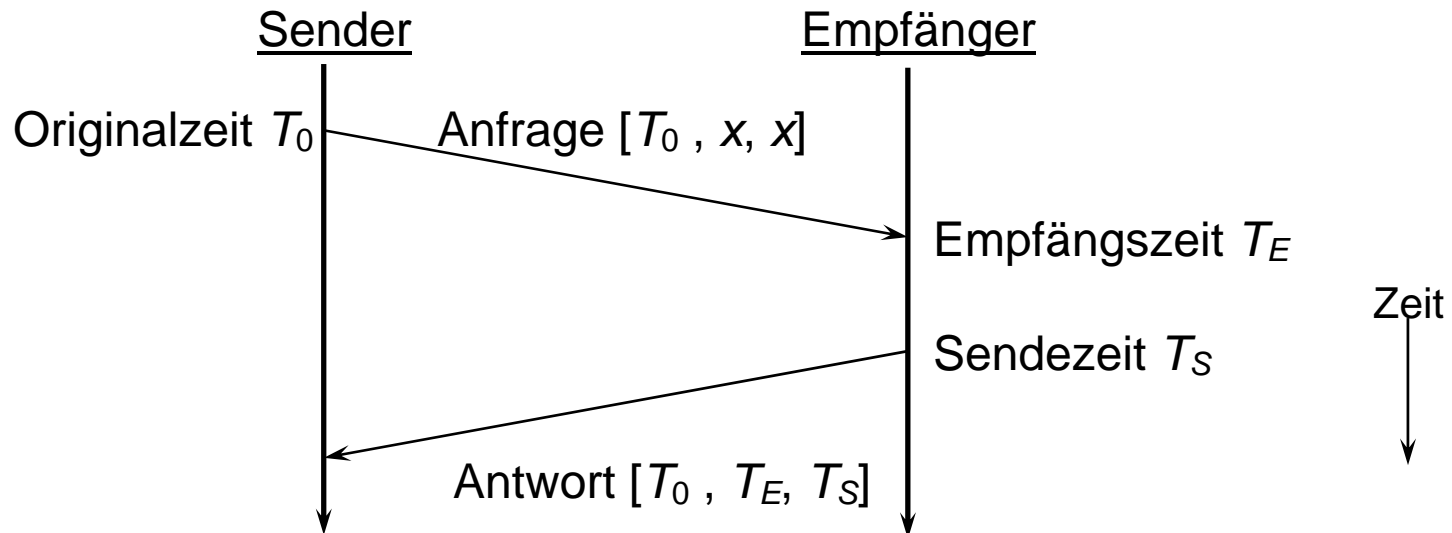
ICMP: Fehlermeldungen

- ❑ **Zieladresse nicht erreichbar** (destination unreachable):
Ein Datenpaket konnte (z.B. wegen einer unterbrochenen Leitung oder eines ausgefallenen Routers) nicht zugestellt werden.
- ❑ **Zeit abgelaufen** (time exceeded):
Datenpaket wurde wegen Ablauf seiner Lebenszeit von einem Router verworfen.
- ❑ **Falscher Parameter** (parameter problem):
Datenpaket wurde wegen eines unzulässigen Wertes im IP-Paketkopf verworfen.
- ❑ **Quellendämpfung** (source quench):
Ein überlastetes Kommunikationssystem fordert den Sender auf, die Übertragungsrate zu senken.
- ❑ **Umleiten** (redirect):
Ein Datenpaket sollte besser über einen anderen Router gesendet werden.
→ Die Fehlermeldungen enthalten jeweils ein Feld zur genauen Angabe der Fehlerursache (z.B. „Netzwerk nicht erreichbar“ oder „Endsystem nicht erreichbar“ für die Meldung „Zieladresse nicht erreichbar“)



ICMP: Statusanfragen

- ❑ **Echo und Echoantwort** (echo and echo reply): Dient der Überprüfung der Aktivität von Kommunikationssystemen. Der Empfänger einer Echo-Anfrage sendet in der Echo-Antwort die erhaltenen Daten an den Kommunikationspartner zurück.
- ❑ **Zeitstempel und Zeitstempelantwort** (timestamp and timestamp reply): Dient der Bestimmung von Paketumlaufzeiten. Die Meldungen umfassen mehrere Felder zur Aufnahme von Zeitstempeln, anhand derer die Paketbearbeitungszeiten beim Empfänger und die Verzögerung im Netzwerk bestimmt werden können.

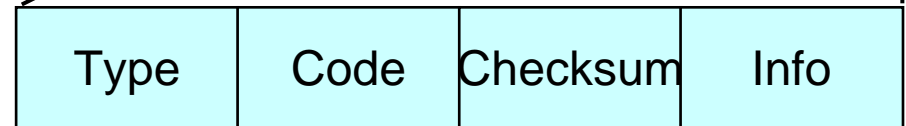
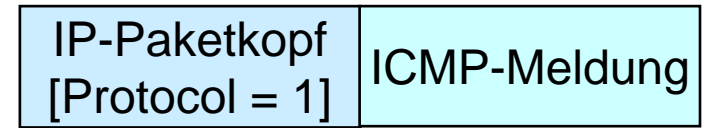




ICMP: Paketformat

□ Übertragung der ICMP-Meldungen

- ICMP-Meldungen werden im Datenteil von IP-Paketen übertragen und durch den Wert „1“ im Protocol-Feld des IP-Paketkopfes kenntlich gemacht.



□ Format der ICMP-Meldungen

- Type: Typ der Meldung (z.B. Type = 3 entspricht „Zieladresse nicht erreichbar“)
- Code: Genaue Beschreibung der Meldung (z.B. „Netzwerk nicht erreichbar“)
- Checksum: Prüfsumme über die gesamte ICMP-Meldung
- Der Inhalt des Info-Teils ist abhängig vom Typ der ICMP-Meldung (z.B. Felder für Zeitstempel bei Meldung „Zeitstempel und Zeitstempelantwort“)
- ICMP „Packet too big“ Nachricht: enthält Typ = 2, Code = 0, Checksum, MTU-size, gefolgt von Original-Paket (max. 576 byte)



5.1.9. ARP: Address Resolution Protocol

❑ **Problem:**

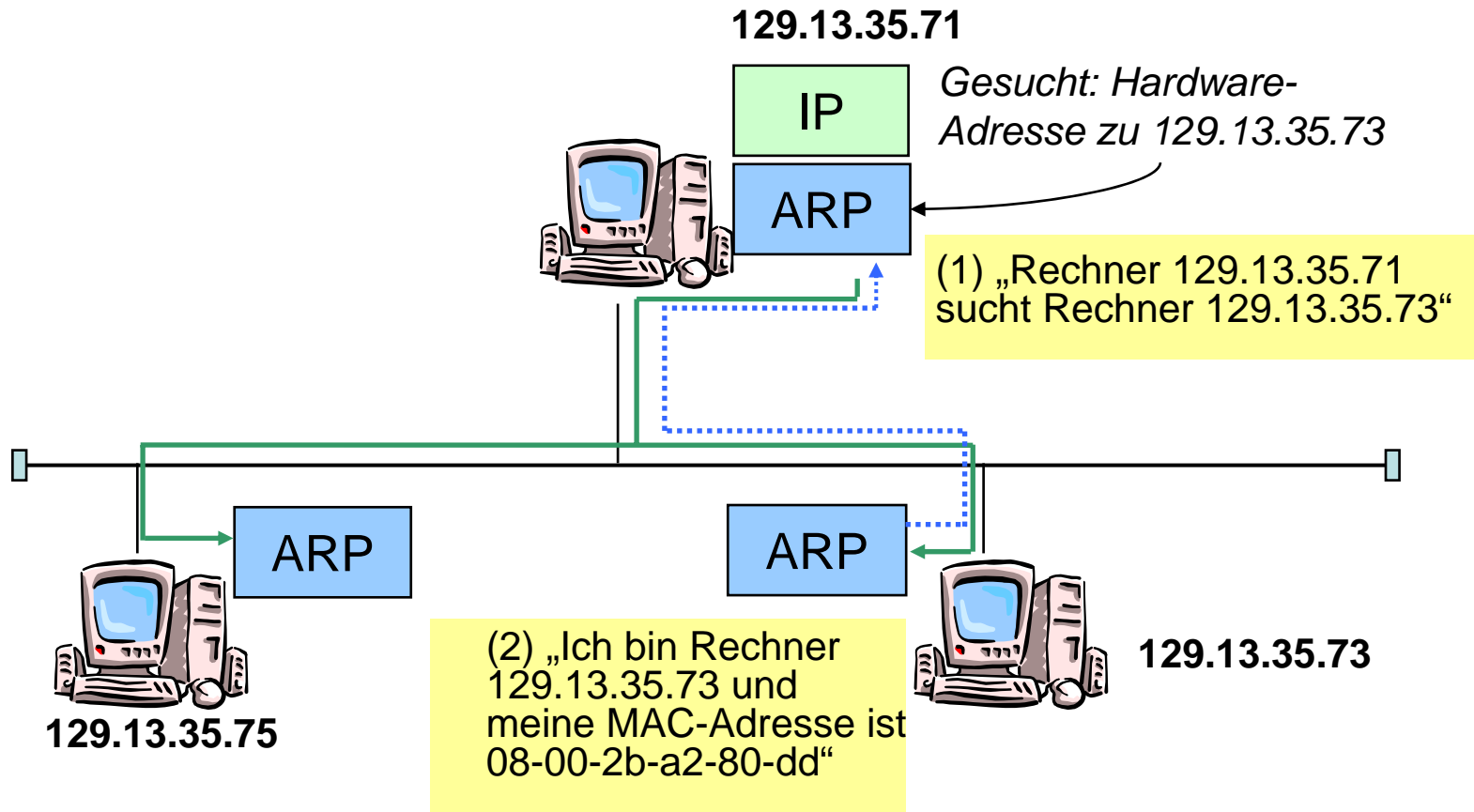
- Abbildung der Internet-Adresse eines Rechners auf die physikalische Adresse der Station (MAC-Adresse = Adresse der Adapterkarte)

❑ **Lösungsalternativen:**

- Unterhalten einer Abbildungstabelle in jedem Rechner.
 - Unterhalten einer Abbildungstabelle in einem Server, der die Anfragen der Kommunikationssysteme beantwortet.
 - Dynamische Abbildung der Adressen durch Senden einer entsprechenden Anfrage an alle Rechner im LAN (Broadcast-Anfrage)
-
- ❑ Bei den beiden erstgenannten Methoden müssen die Abbildungstabellen bei jeder Änderung manuell abgeglichen werden.
 - ❑ Ein Verfahren zur dynamischen Abbildung der Adressen ist durch das Address Resolution Protocol (ARP) festgelegt.



ARP – Beispiel



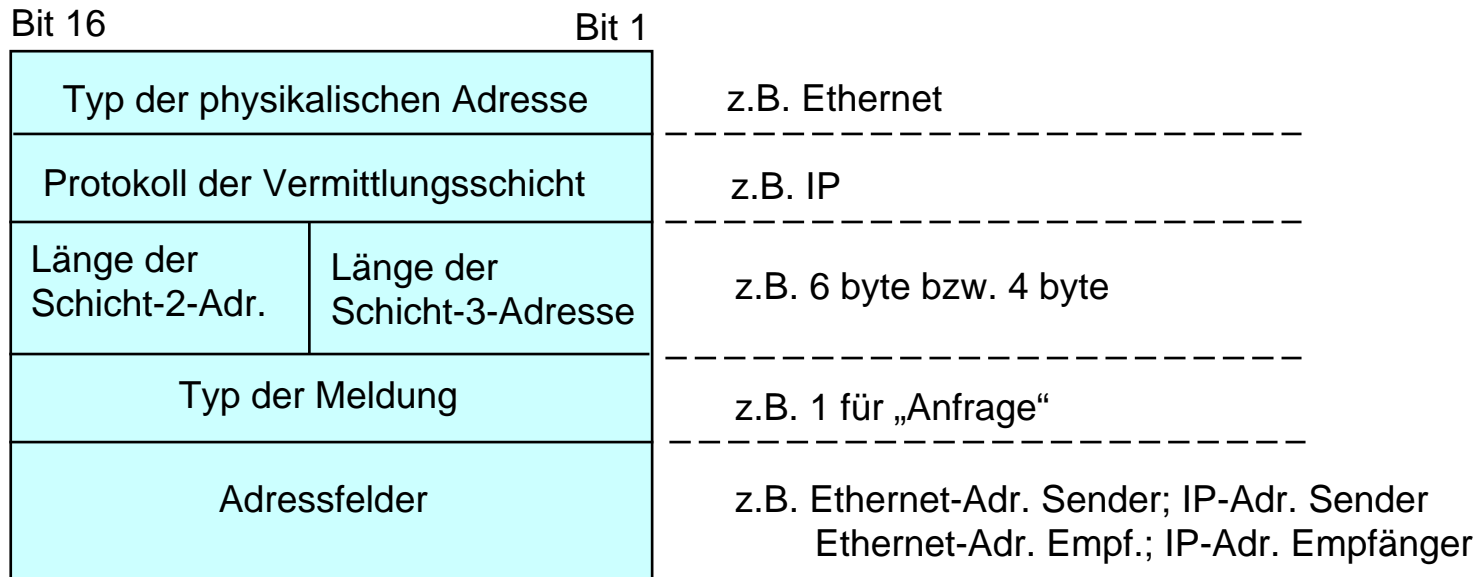
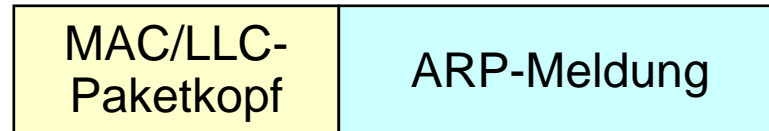
Sicherheitslücke?



ARP: Paketformat

- ❑ Übertragung der ARP-Meldungen
- ❑ Eine ARP-Meldung wird im Datenteil eines Paketes der Sicherungsschicht übertragen.

- ❑ Format der ARP-Meldungen:



Länge und Aufbau der Adressfelder sind vom Typ der Adressen abhängig



Reverse Address Resolution Protocol (RARP)

□ Aufgabe:

- Umsetzen MAC-Adresse \Rightarrow IP-Adresse.
- Wichtig z.B. für plattenlose Workstations, die von einem Dateiserver booten. Dazu müssen sie ihre IP-Adresse wissen, welche die Station allerdings beim Einschalten noch nicht kennt.

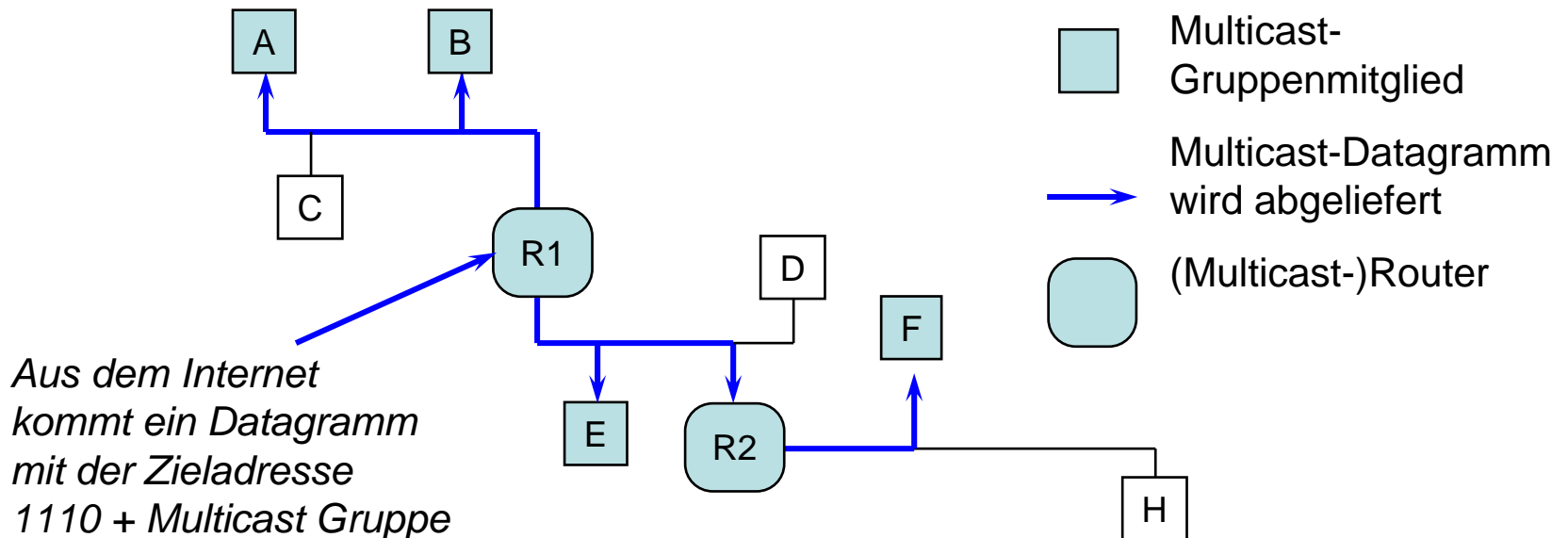
□ Vorgehensweise:

- Station schickt einen Rundruf ins lokale Netz unter Angabe der eigenen MAC-Adresse, die durch die Hardware vorgegeben ist.
- RARP-Server sieht die Anfrage und bestimmt anhand einer Konfigurationsdatei die zugehörige IP-Adresse.
- RARP-Server schickt die IP-Adresse in einer RARP-Antwort an die anfragende Station zurück.



IP-Multicast

- ❑ Ein einzelnes IP-Datagramm wird an mehr als eine Station adressiert.
- ❑ Multicast-Verwaltung erfolgt über das IGMP (Internet Group Management Protocol).
- ❑ Es muss eine Class D-Adresse verwendet werden.
 - Die ersten vier Bits des Adressfelds im Kopfes entsprechen 1110.
 - Danach folgt die 28 bit lange ID der Gruppe.
- ❑ Beispiel:



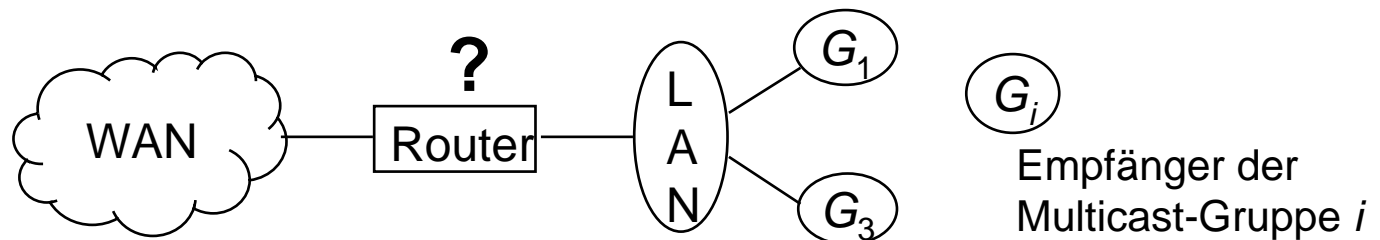


IGMP: Internet Group Management Protocol

❑ Problem:

- Wie erkennt ein Router, dass Multicast-Nachrichten bestimmter Gruppen von ihm weitergeleitet werden müssen?

❑ Beispiel:



- Nachrichten der Gruppen 1 und 3 müssen vom Router in das angeschlossene LAN weitergeleitet werden, wohingegen Nachrichten anderer Gruppen das LAN nicht erreichen sollten.

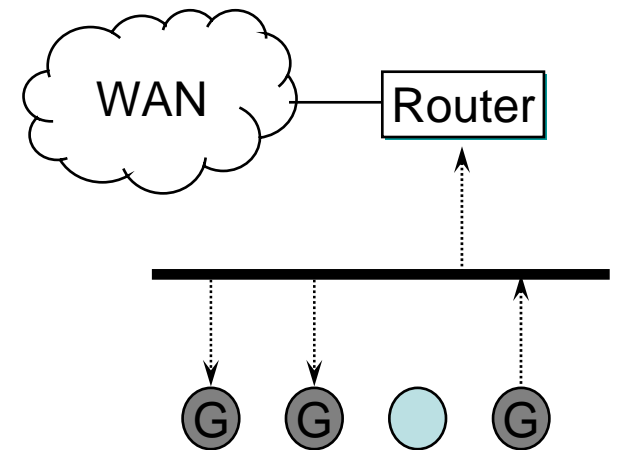
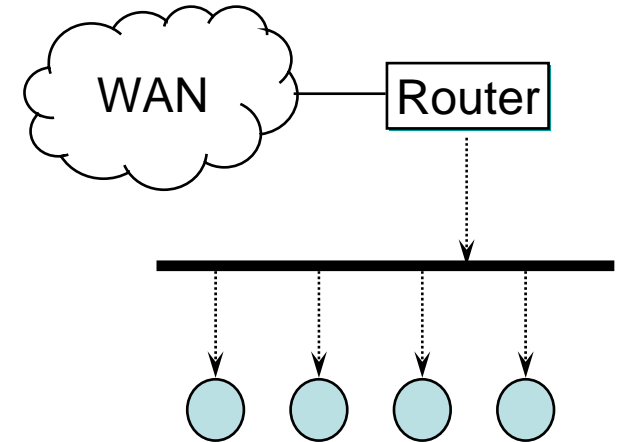
❑ Lösungen:

- Manuelle Eingabe von Gruppenzugehörigkeiten in der Router-konfiguration \Rightarrow hoher Verwaltungsaufwand bei dynamischen Gruppen.
- Selbstständiges Erlernen der Gruppenzugehörigkeiten durch den Austausch entsprechender Information \Rightarrow ein solches Verfahren wird durch das **Internet Group Management Protocol (IGMP)** beschrieben.



IGMP: Protokollablauf I

1. Der Router sendet periodisch Gruppenzugehörigkeitsanfragen an alle Rechner des LAN (via Broadcast). Durch Setzen der „Time To Live“ (TTL) auf 1 wird die Anfrage nur im LAN verbreitet.
2. Nach Erhalt einer Anfrage startet jeder Rechner für jede Gruppe, welcher er angehört, einen Zeitgeber. Dieser wird mit einem Zufallswert initialisiert. Nach Ablauf des Zeitgebers sendet der Host eine Antwort bzgl. der Gruppenzugehörigkeit an alle Gruppenmitglieder im LAN (Gruppenadresse, TTL=1). Multicast-Router erhalten alle IP-Multicast-Nachrichten.





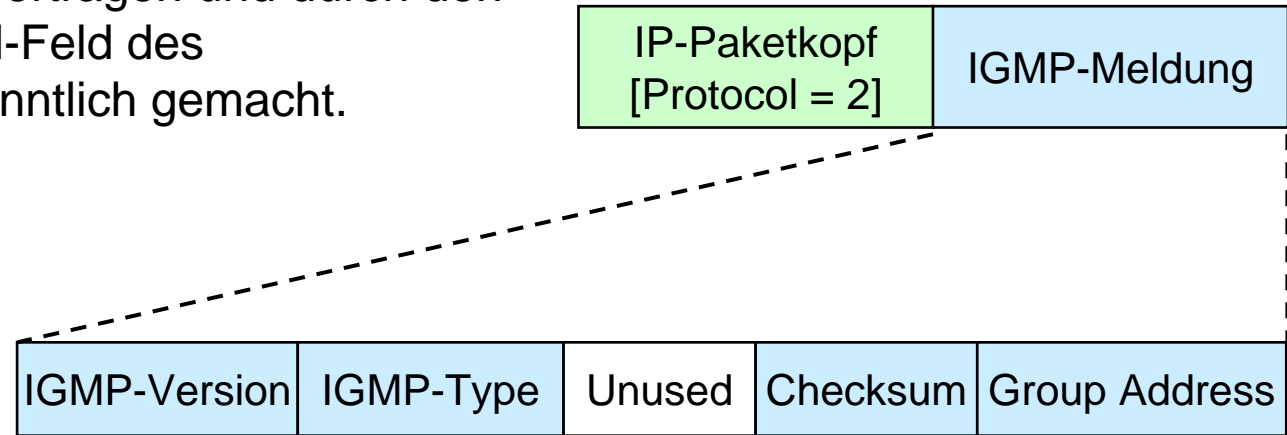
IGMP: Protokollablauf II

3. Weitere Gruppenmitglieder erhalten die Antwort und stoppen den entsprechenden Zeitgeber. Dadurch werden redundante Antworten vermieden.
4. Der Router erhält alle Antworten und aktualisiert seine Routingtabelle entsprechend. Erhält ein Router nach mehrmaliger Anfrage keine Antwort bzgl. einer bestimmten Gruppe, so wird ihr Eintrag aus der Routingtabelle gelöscht.
 - è Tritt ein Rechner einer Gruppe bei, so sendet er sofort eine entsprechende Mitteilung an alle Router im LAN. Aus Gründen der Fehlertoleranz wird die Mitteilung wiederholt gesendet.



IGMP: Paketformat

- ❑ Übertragung der IGMP-Meldungen
- ❑ IGMP-Meldungen werden im Datenteil von IP-Paketen übertragen und durch den Wert 2 im Protocol-Feld des IP-Paketkopfes kenntlich gemacht.



- ❑ Format der IGMP-Meldungen
 - IGMP-Version: Versionsnummer des eingesetzten IGMP-Protokolls.
 - IGMP-Type: Typ der Meldung (z.B. 1 = Anfrage, 0 = Antwort).
 - Unused: Wird nicht genutzt (immer zu 0 gesetzt).
 - Checksum: Prüfsumme über die gesamte IGMP-Meldung.
 - Group Address: Wird bei einer Anfrage auf 0 gesetzt, bei einer Antwort enthält das Feld die Adresse derjenigen Gruppe, auf welche sich die Meldung bezieht.

