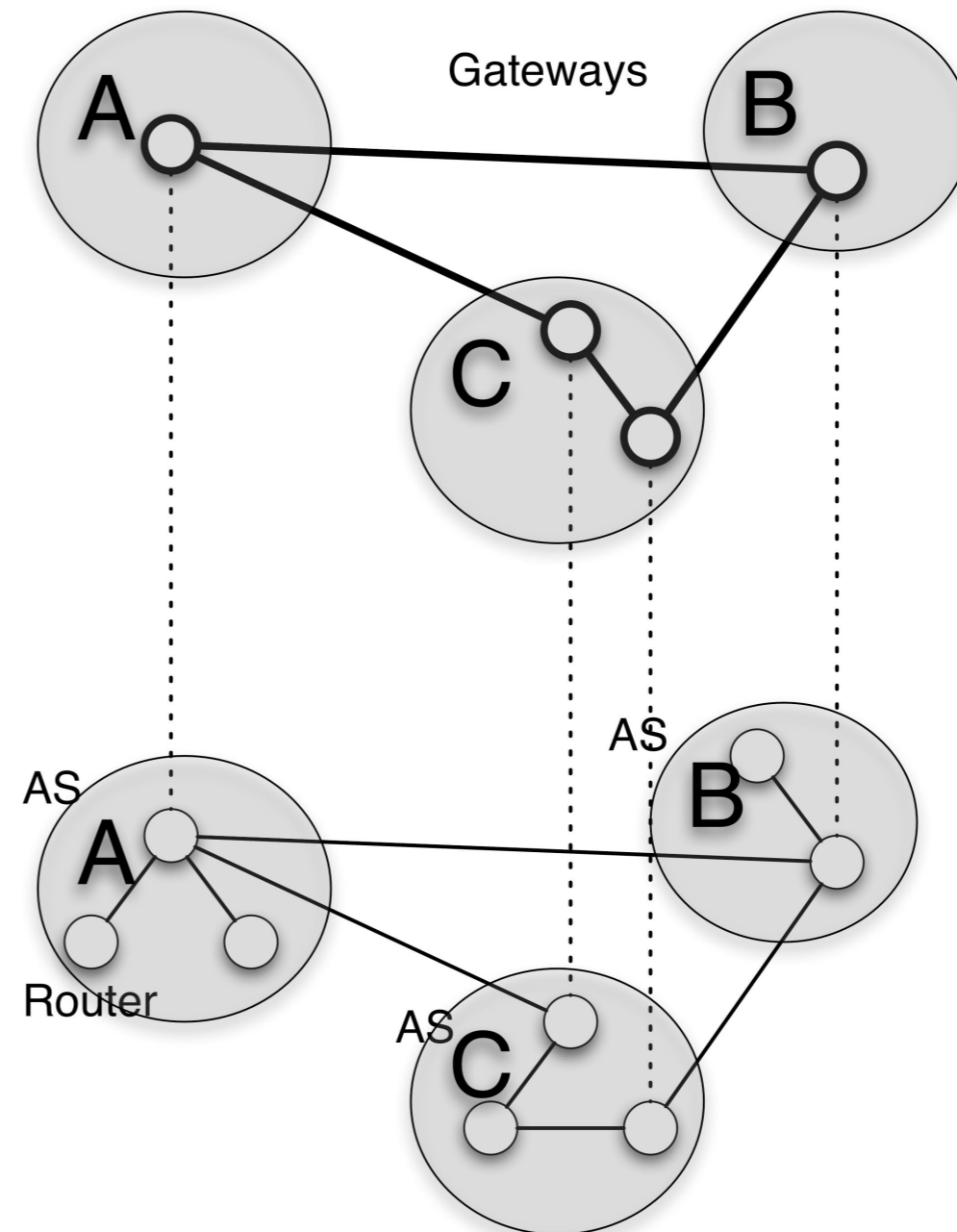


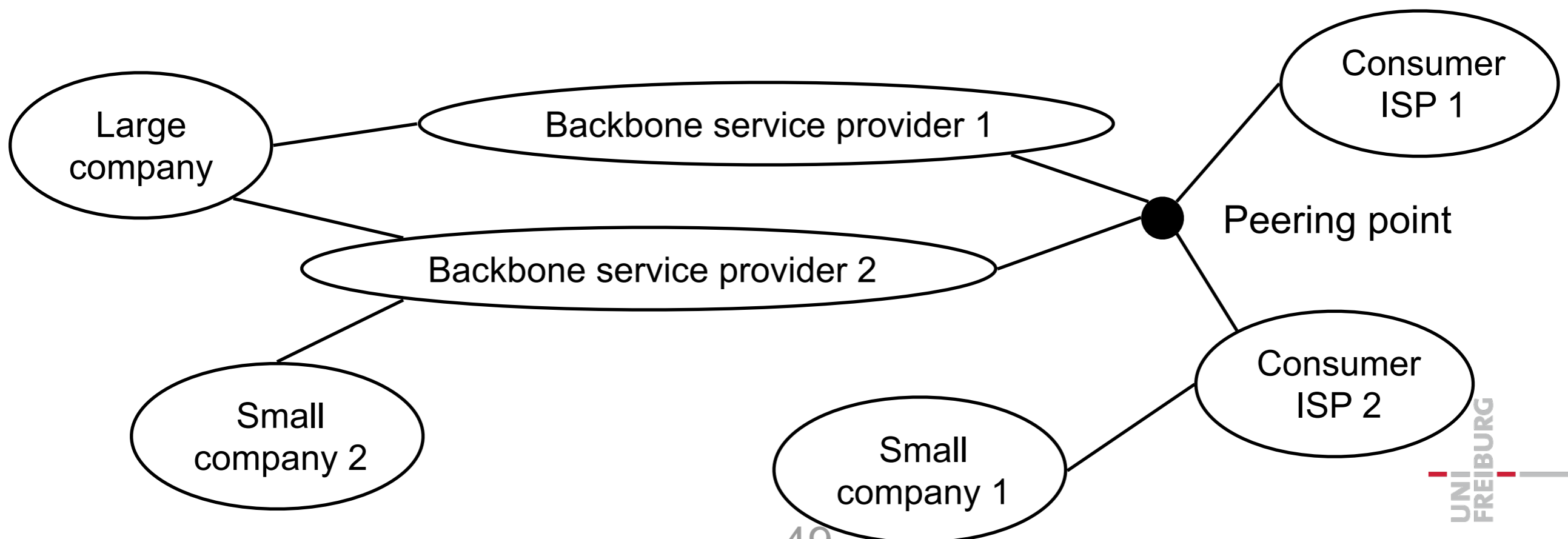
- Link State Router
  - tauschen Information mittels Link State Packets (LSP) aus
  - Jeder verwendet einen eigenen Kürzeste-Wege-Algorithmus zu Anpassung der Routing-Tabelle
- LSP enthält
  - ID des LSP erzeugenden Knotens
  - Kosten dieses Knotens zu jedem direkten Nachbarn
  - Sequenznr. (SEQNO)
  - TTL-Feld für dieses Feld (time to live)
- Verlässliches Fluten (Reliable Flooding)
  - Die aktuellen LSP jedes Knoten werden gespeichert
  - Weiterleitung der LSP zu allen Nachbarn
    - bis auf den Knoten der diese ausgeliefert hat
  - Periodisches Erzeugen neuer LSPs
    - mit steigender SEQNOs
  - Verringern der TTL bei jedem Weiterleiten

- Link State Routing
  - benötigt  $O(g \cdot n)$  Einträge für  $n$  Router mit maximalen Grad  $g$
  - Jeder Knoten muss an jeden anderen seine Informationen senden
- Distance Vector
  - benötigt  $O(g \cdot n)$  Einträge
  - kann Schleifen einrichten
  - Konvergenzzeit steigt mit Netzwerkgröße
- Im Internet gibt es mehr als  $10^7$  Router
  - damit sind diese so genannten flachen Verfahren nicht einsetzbar
- Lösung:
  - Hierarchisches Routing

- Autonomous System (AS)
  - liefert ein zwei Schichten-Modell des Routing im Internet
  - Beispiele für AS:
    - uni-freiburg.de
- Intra-AS-Routing (Interior Gateway Protocol)
  - ist Routing innerhalb der AS
  - z.B. RIP, OSPF, IGRP, ...
- Inter-AS-Routing (Exterior Gateway Protocol)
  - Übergabepunkte sind Gateways
  - ist vollkommen dezentrales Routing
  - Jeder kann seine Optimierungskriterien vorgeben
  - z.B. EGP (früher), BGP



- Stub-AS
  - Nur eine Verbindung zu anderen AS
- Multihomed AS
  - Verbindungen zu anderen ASen
  - weigert sich aber Verkehr für andere zu befördern
- Transit AS
  - Mehrere Verbindungen
  - Leitet fremde Nachrichten durch (z.B. ISP)



- Distance Vector Algorithmus
  - Distanzmetrik = Hop-Anzahl
- Distanzvektoren
  - werden alle 30s durch Response-Nachricht (advertisement) ausgetauscht
- Für jedes Advertisement
  - Für bis zu 25 Zielnetze werden Routen veröffentlicht per UDP
- Falls kein Advertisement nach 180s empfangen wurde
  - Routen über Nachbarn werden für ungültig erklärt
  - Neue Advertisements werden zu den Nachbarn geschickt
  - Diese antworten auch mit neuen Advertisements
    - falls die Tabellen sich ändern
  - Rückverbindungen werden unterdrückt um Ping-Pong-Schleifen zu verhindern (poison reverse) gegen Count-to-Infinity-Problem
    - Unendliche Distanz = 16 Hops

- “open” = öffentlich verfügbar
- Link-State-Algorithmus
  - LS Paket-Verbreitung
  - Topologie wird in jedem Knoten abgebildet
  - Routenberechnung mit Dijkstras Algorithmus
- OSPF-Advertisment
  - per TCP, erhöht Sicherheit (security)
  - werden in die gesamte AS geflutet
  - Mehrere Wege gleicher Kosten möglich

- Für große Netzwerke zwei Ebenen:
  - Lokales Gebiet und Rückgrat (backbone)
    - Lokal: Link-state advertisement
    - Jeder Knoten berechnet nur in Richtung zu den Netzen in anderen lokalen Gebieten
- Local Area Border Router:
  - Fassen die Distanzen in das eigene lokale Gebiet zusammen
  - Bieten diese den anderen Area Border Routern an (per Advertisement)
- Backbone Routers
  - verwenden OSPF beschränkt auf das Rückgrat (backbone)
- Boundary Routers:
  - verbinden zu anderen AS

# Intra-AS: IGRP (Interior Gateway Routing Protocol)

---

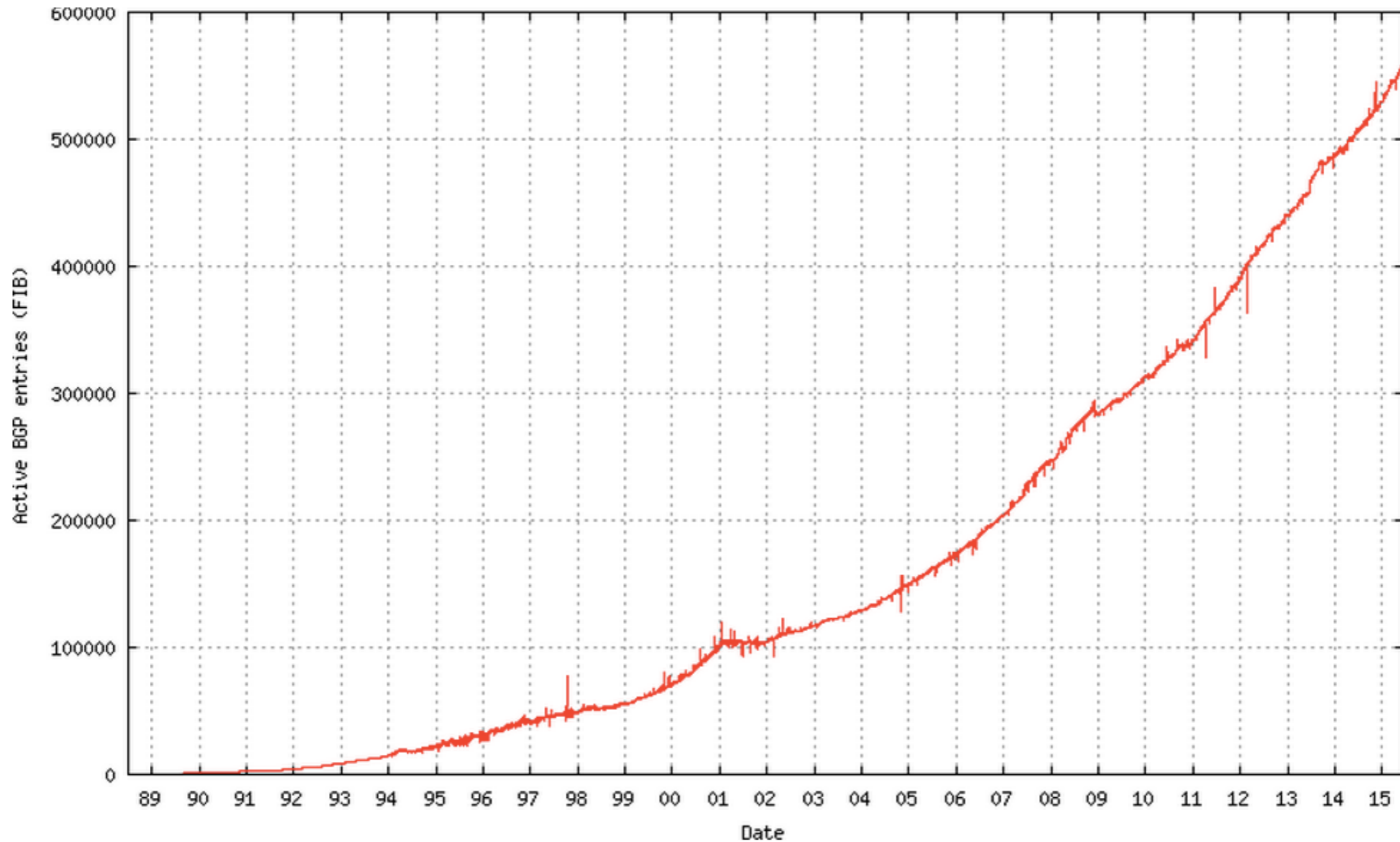
- CISCO-Protokoll, Nachfolger von RIP (1980er)
- Distance-Vector-Protokoll, wie RIP
  - Hold Down Counter
    - weggefallene Verbindungen werden eine zeitlang noch angeboten, werden dann entfernt
  - Split Horizon
    - Advertisements werden nicht auf dem angebotenen Pfad weitergegeben
  - Poison Reverse
    - weggefallene Verbindungen werden sofort mit Entfernung „unendlich“ (100) allen Nachbarn angeboten
- Verschiedene Kostenmetriken
  - Delay, Bandwidth, Reliability, Load etc.
- Verwendet TCP für den Austausch von Routing Updates



- Inter-AS-Routing ist schwierig...
  - Organisationen können Durchleitung von Nachrichten verweigern
  - Politische Anforderungen
    - Weiterleitung durch andere Länder?
  - Routing-Metriken der verschiedenen autonomen Systeme sind oftmals unvergleichbar
    - Wegeoptimierung unmöglich!
    - Inter-AS-Routing versucht wenigstens Erreichbarkeit der Knoten zu ermöglichen
  - Größe: momentan müssen Inter-Domain-Router mehr als 500.000 Einträge verwalten

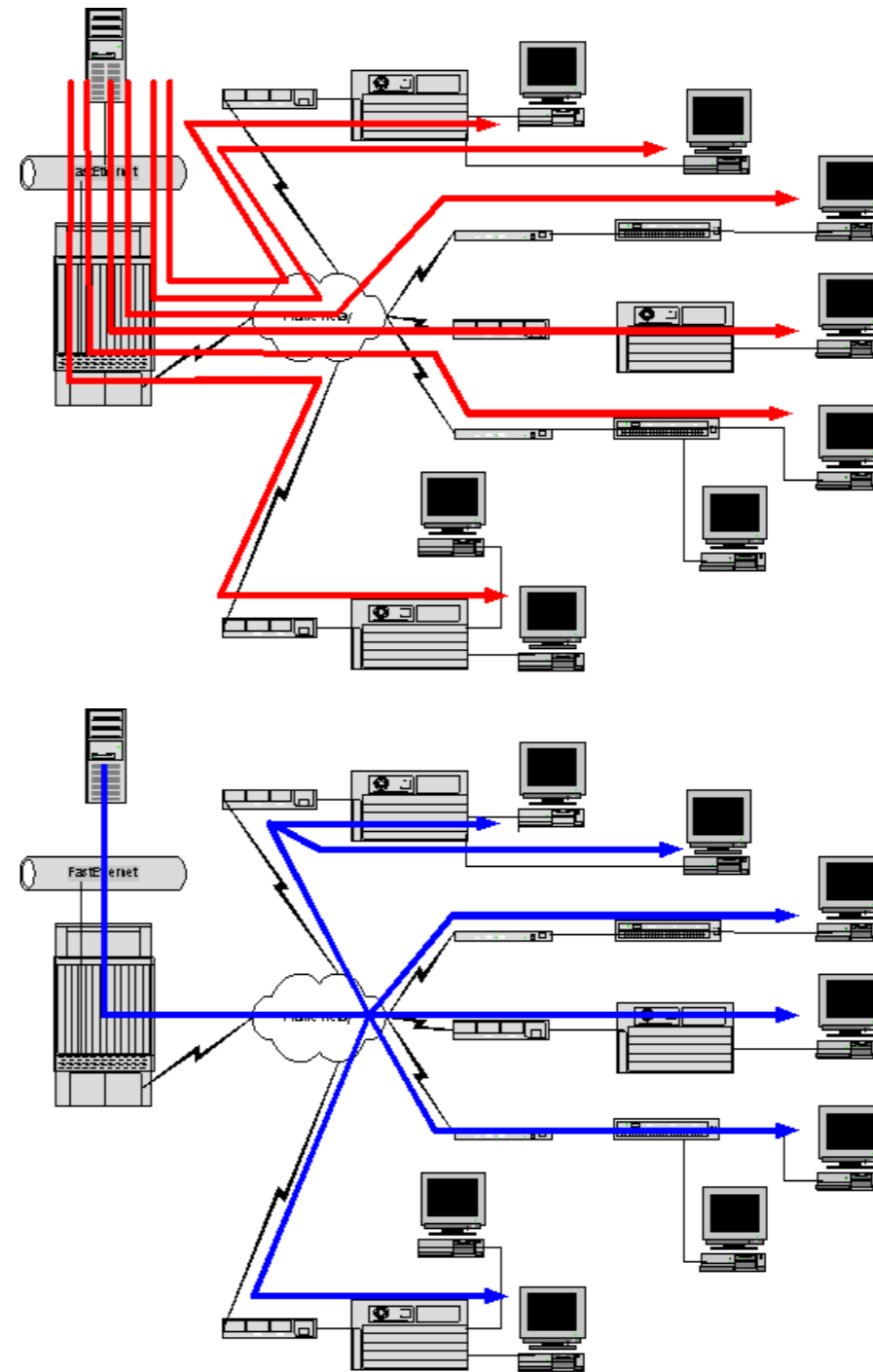
- Ist faktisch der Standard
- Path-Vector-Protocol
  - ähnlich wie Distance Vector Protocol
    - es werden aber ganze Pfade zum Ziel gespeichert
  - jeder Border Gateway teilt all seinen Nachbarn (peers) den gesamten Pfad (Folge von ASen) zum Ziel mit (advertisement) (per TCP)
- Falls Gateway X den Pfad zum Peer-Gateway W sendet
  - dann kann W den Pfad wählen oder auch nicht
  - Optimierungskriterien:
    - Kosten, Politik, etc.
  - Falls W den Pfad von X wählt, dann publiziert er
    - $\text{Path}(W,Z) = (W, \text{Path}(X,Z))$
- Anmerkung
  - X kann den eingehenden Verkehr kontrollieren durch Senden von Advertisements
  - Sehr kompliziertes Protokoll

# BGP-Routing Tabellengröße 1989-2015



- Broadcast routing
  - Ein Paket soll (in Kopie) an alle ausgeliefert werden
  - Lösungen:
    - Fluten des Netzwerks
    - Besser: Konstruktion eines minimalen Spannbaums
- Multicast routing
  - Ein Paket soll an eine gegebene Teilmenge der Knoten ausgeliefert werden (in Kopie)
  - Lösung:
    - Optimal: Steiner Baum Problem (bis heute nicht lösbar)
    - Andere (nicht-optimale) Baum-konstruktionen

- Motivation
  - Übertragung eines Stroms an viele Empfänger
- Unicast
  - Strom muss mehrfach einzeln übertragen werden
  - Bottleneck am Sender
- Multicast
  - Strom wird über die Router vervielfältigt
  - Kein Bottleneck mehr



- IPv4 Multicast-Adressen
  - in der Klasse D (außerhalb des CIDR - Classless Interdomain Routings)
  - 224.0.0.0 - 239.255.255.255
  - in IPv6 mit Präfix FF
- Hosts melden sich per IGMP bei der Adresse an
  - IGMP = Internet Group Management Protocol
  - Nach der Anmeldung wird der Multicast-Tree aktualisiert
- Source sendet an die Multicast-Adresse
  - Router duplizieren die Nachrichten an den Routern
  - und verteilen sie in die Bäume
- Angemeldete Hosts erhalten diese Nachrichten
  - bis zu einem Time-Out
  - oder bis sie sich abmelden
- Achtung:
  - Kein TCP, nur UDP
  - Viele Router lehnen die Beförderung von Multicast-Nachrichten ab
    - Lösung: Tunneln

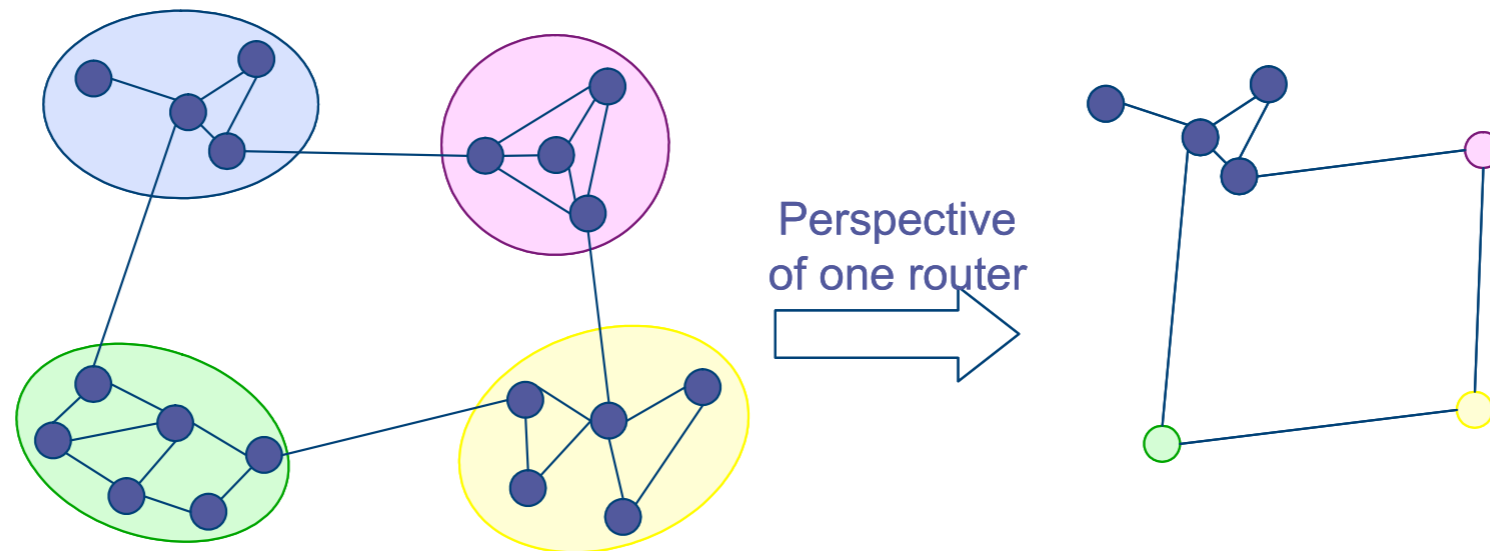
- Distance Vector Multicast Routing Protocol (DVMRP)
  - jahrelang eingesetzt in MBONE (insbesondere in Freiburg)
  - Eigene Routing-Tabelle für Multicast
- Protocol Independent Multicast (PIM)
  - im Sparse Mode (PIM-SM)
  - aktueller Standard
  - beschneidet den Multicast Baum
  - benutzt Unicast-Routing-Tabellen
  - ist damit weitestgehend protokollunabhängig
- Voraussetzung PIM-SM:
  - benötigt Rendezvous-Point (RP) in ein-Hop-Entfernung
  - RP muss PIM-SM unterstützen
  - oder Tunneling zu einem Proxy in der Nähe eines RP

# Warum so wenig IP Multicast?

- Trotz erfolgreichen Einsatz
  - in Video-Übertragung von IETF-Meetings
  - MBONE (Multicast Backbone)
- gibt es wenig ISP welche IP Multicast in den Routern unterstützen
- Zusätzlicher Wartungsaufwand
  - Schwierig zu konfigurieren
  - Verschiedene Protokolle
- Gefahr von Denial-of-Service-Attacken
  - Implikationen größer als bei Unicast
- Transport-Protokoll
  - Nur UDP einsetzbar
  - Zuverlässige Protokolle
    - Vorwärtsfehlerkorrektur
    - Oder proprietäre Protokolle in den Routern (z.B. CISCO)
- Marktsituation
  - Endkunden fragen kaum Multicast nach (benutzen lieber P2P-Netzwerke)
  - Wegen einzelner Dateien und weniger Abnehmer erscheint ein Multicast wenig erstrebenswert (Adressenknappheit!)



- Flache (MAC-) Adressen haben keine Strukturinformation



- Hierarchische Adressen
  - Routing wird vereinfacht wenn Adressen hierarchische Routing-Struktur abbilden
  - $\text{Group-ID}_n:\text{Group-ID}_{n-1}:\dots:\text{Group-ID}_1:\text{Device-ID}$

- IP-Adressen

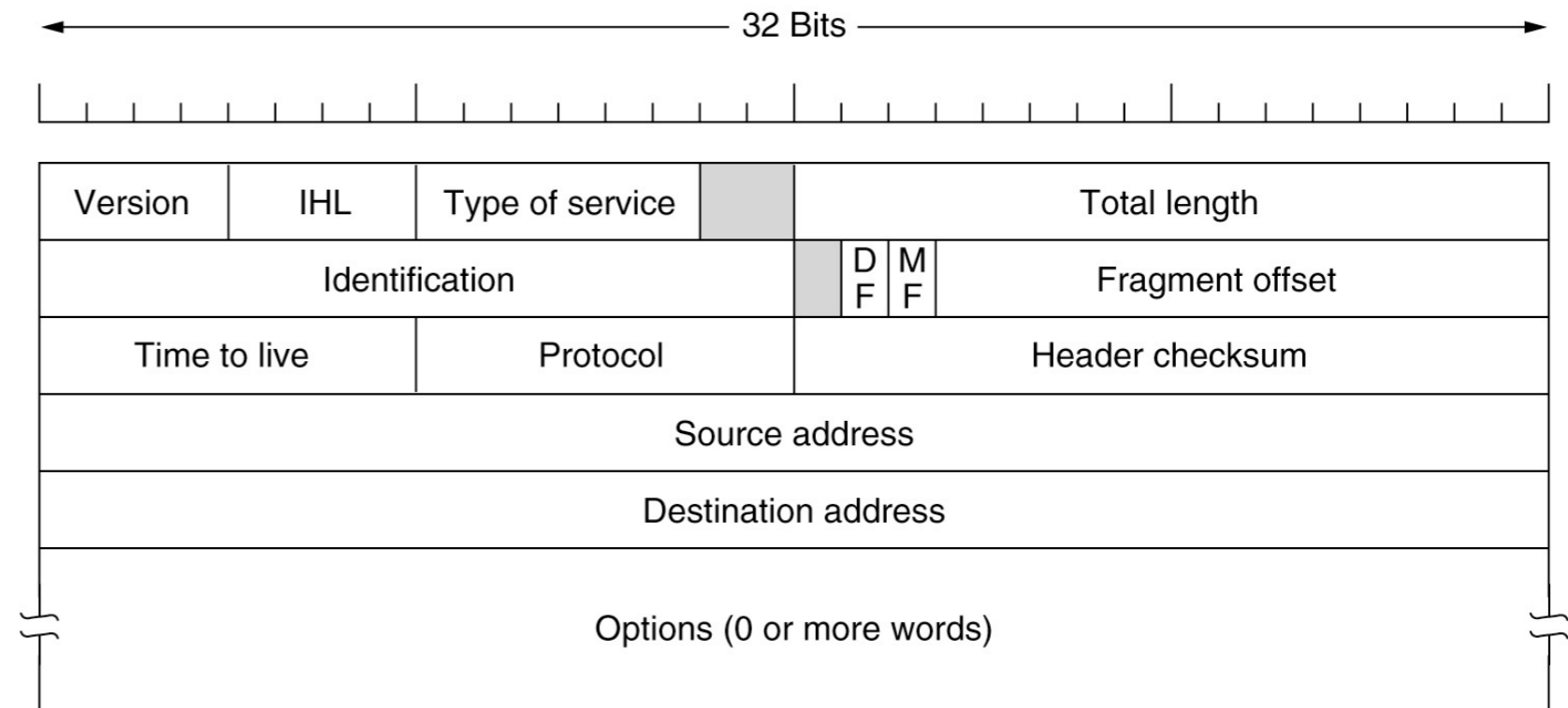
- Jedes Interface in einem Netzwerk hat weltweit eindeutige IP-Adresse
- 32 Bits unterteilt in Net-ID und Host-ID
- Net-ID vergeben durch Internet Network Information Center
- Host-ID durch lokale Netzwerkadministration

- Domain Name System (DNS)

- Ersetzt IP-Adressen wie z.B. 132.230.167.230 durch Namen wie z.B. falcon.informatik.uni-freiburg.de und umgekehrt
- Verteilte robuste Datenbank

# IPv4-Header (RFC 791)

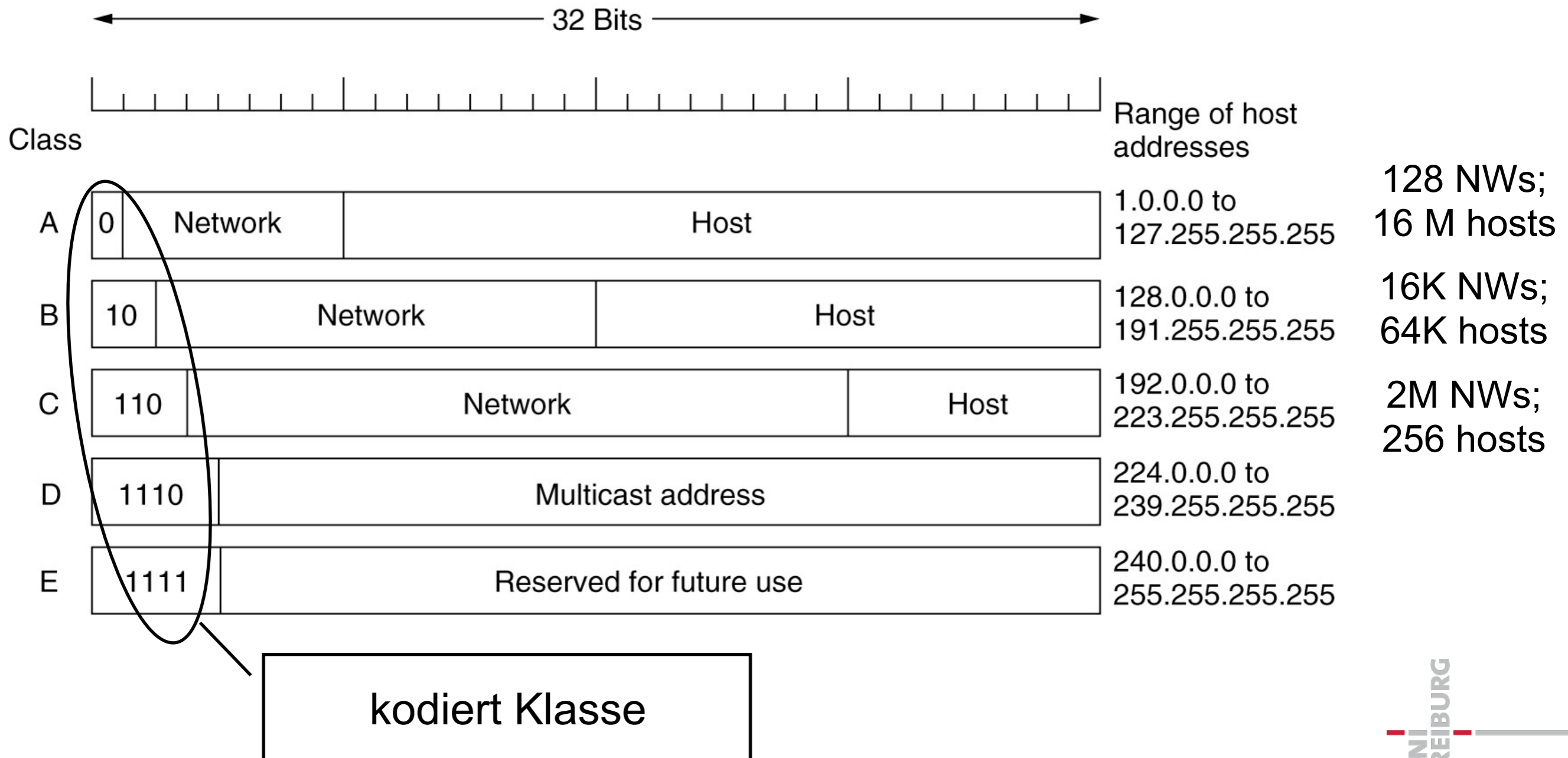
- Version: 4 = IPv4
- IHL: IP Headerlänge
  - in 32 Bit-Wörtern (>5)
- Type of Service
  - Optimierte delay, throughput, reliability, monetary cost
- Checksum (nur für IP-Header)
- Source and destination IP-address
- Protocol, identifiziert passendes Protokoll
  - Z.B. TCP, UDP, ICMP, IGMP
- Time to Live:
  - maximale Anzahl Hops



- IP-Adressen unterscheiden zwei Hierarchien
  - Netzwerk-Interfaces
  - Netzwerke
    - Verschiedene Netzwerkgrößen
    - Netzwerkklassen:
      - Groß - mittel - klein  
(Klasse A, B, and C)
- Eine IP-Adresse hat 32 Bits
  - Erster Teil: Netzwerkadresse
  - Zweiter Teil: Interface

# IP-Klassen bis 1993

- Klassen A, B, and C
- D für multicast; E: "reserved"



- Bis 1993 (heutzutage veraltet)
  - 5 Klassen gekennzeichnet durch Präfix
  - Dann Subnetzpräfix fester Länge und Host-ID (Geräteteil)
- Seit 1993
  - Classless Inter-Domain-Routing (CIDR)
  - Die Netzwerk-Adresse und die Host-ID (Geräteteil) werden variabel durch die Netzwerkmaske aufgeteilt.
  - Z.B.:
    - Die Netzwerkmaske 11111111.11111111.11111111.00000000
    - Besagt, dass die IP-Adresse
      - 10000100. 11100110. 10010110. 11110011
      - Aus dem Netzwerk 10000100. 11100110. 10010110
      - den Host 11110011 bezeichnet
- Route aggregation
  - Die Routing-Protokolle BGP, RIP v2 und OSPF können verschiedene Netzwerke unter einer ID anbieten
    - Z.B. alle Netzwerke mit Präfix 10010101010\* werden über Host X erreicht

- Address Resolution Protocol (ARP)
- Umwandlung: IP-Adresse in MAC-Adresse
  - Broadcast im LAN, um nach Rechner mit passender IP-Adresse zu fragen
  - Knoten antwortet mit MAC-Adresse
  - Router kann dann das Paket dorthin ausliefern
- IPv6:
  - Funktionalität durch Neighbor Discovery Protocol (NDP)
  - Informationen werden per ICMPv6 ausgetauscht

- Wozu IPv6:
- Freie IPv4-Adressen sind seit 31.01.2011 nicht mehr vorhanden
  - Zwar gibt es 4 Milliarden in IPv4 (32 Bit)
  - Diese sind aber statisch organisiert in Netzwerk- und Host-ID
    - Adressen für Funktelefone, Kühlschränke, Autos, Tastaturen, etc...
- Autokonfiguration
  - DHCP, Mobile IP, Umnummerierung
- Neue Dienste
  - Sicherheit (IPSec)
  - Qualitätssicherung (QoS)
  - Multicast
- Vereinfachungen für Router
  - keine IP-Prüfsummen
  - Keine Partitionierung von IP-Paketen



- DHCP (Dynamic Host Configuration Protocol)
  - Manuelle Zuordnung (Bindung an die MAC-Adresse, z.B. für Server)
  - Automatische Zuordnung (feste Zuordnung, nicht voreingestellt)
  - Dynamische Zuordnung (Neuvergabe möglich)
- Einbindung neuer Rechner ohne Konfiguration
  - Rechner „holt“ sich die IP-Adresse von einem DHCP-Server
  - Dieser weist dem Rechner die IP-Adressen dynamisch zu
  - Nachdem der Rechner das Netzwerk verlässt, kann die IP-Adresse wieder vergeben werden
  - Bei dynamischer Zuordnung, müssen IP-Adressen auch „aufgefrischt“ werden
  - Versucht ein Rechner eine alte IP-Adresse zu verwenden,
    - die abgelaufen ist oder
    - schon neu vergeben ist
  - Dann werden entsprechende Anfragen zurückgewiesen
  - Problem: Stehlen von IP-Adressen

# IPv6-Header (RFC 2460)

- Version: 6 = IPv6
- Traffic Class
  - Für QoS (Prioritätsvergabe)
- Flow Label
  - Für QoS oder Echtzeitanwendungen
- Payload Length
  - Größe des Rests des IP-Pakets (Datagramms)
- Next Header (wie bei IPv4: protocol)
  - Z.B. ICMP, IGMP, TCP, EGP, UDP, Multiplexing, ...
- Hop Limit (Time to Live)
  - maximale Anzahl Hops
- Source Address & Destination Address:
  - 128 Bit IPv6-Adresse,  
z.B. 2822:0000:0000:0000:0000:0005:EBD2:7008

