CoNe Freiburg

IIF INSTITUT FÜR INFORMATIK FREIBURG

Systeme II

4. Die Vermittlungsschicht

Christian Schindelhauer
Technische Fakultät
Rechnernetze und Telematik
Albert-Ludwigs-Universität Freiburg

Version 03.06.2014

UNI FREIBURG

CoNe Freiburg

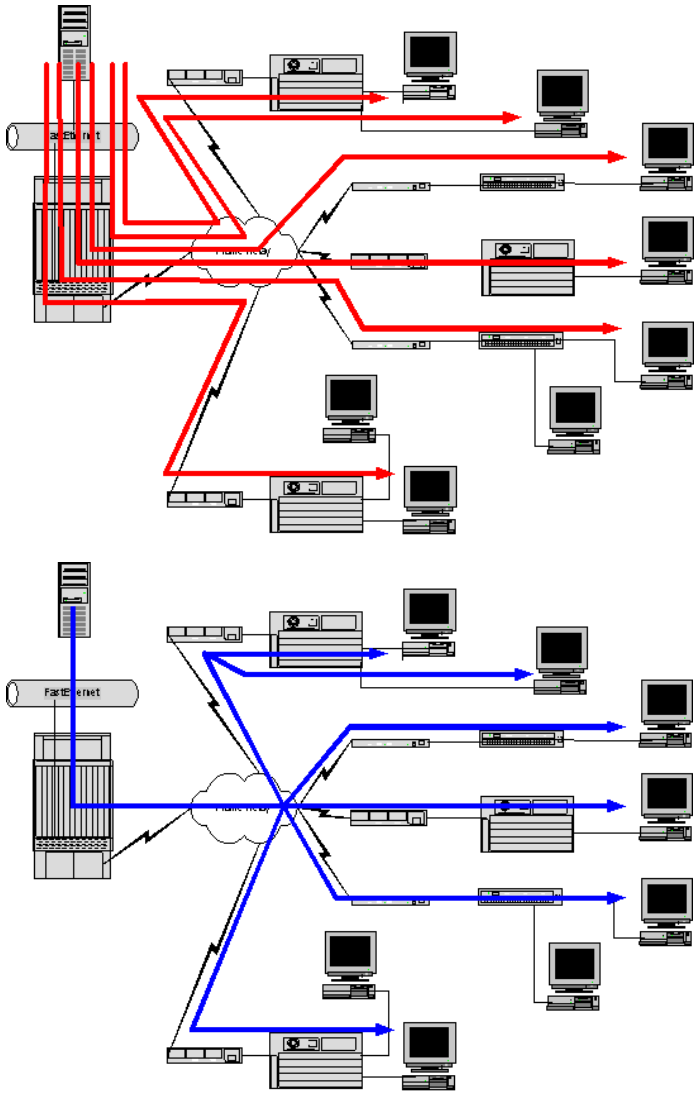
Broadcast & Multicast

- 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

CoNe Freiburg

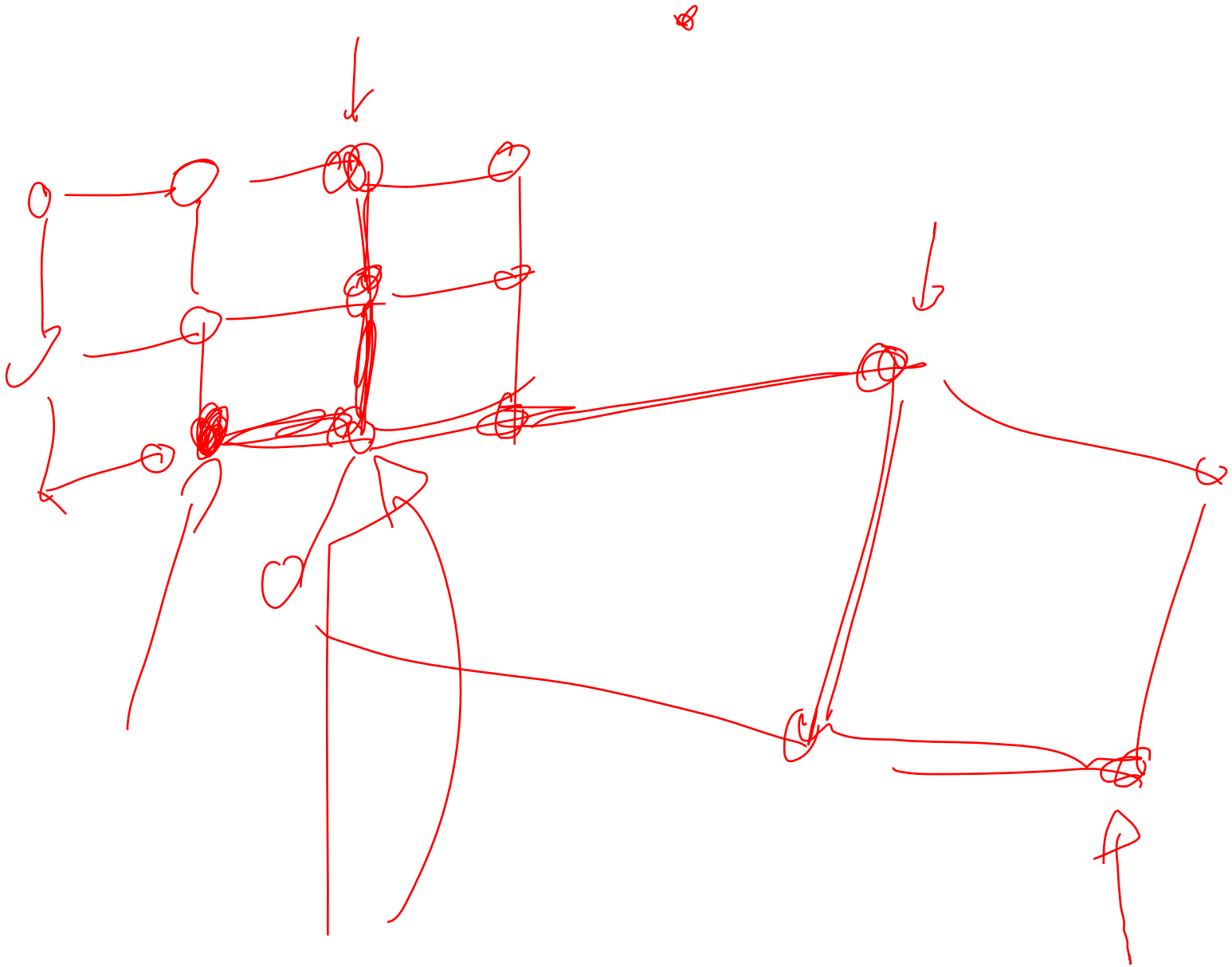
IP Multicast

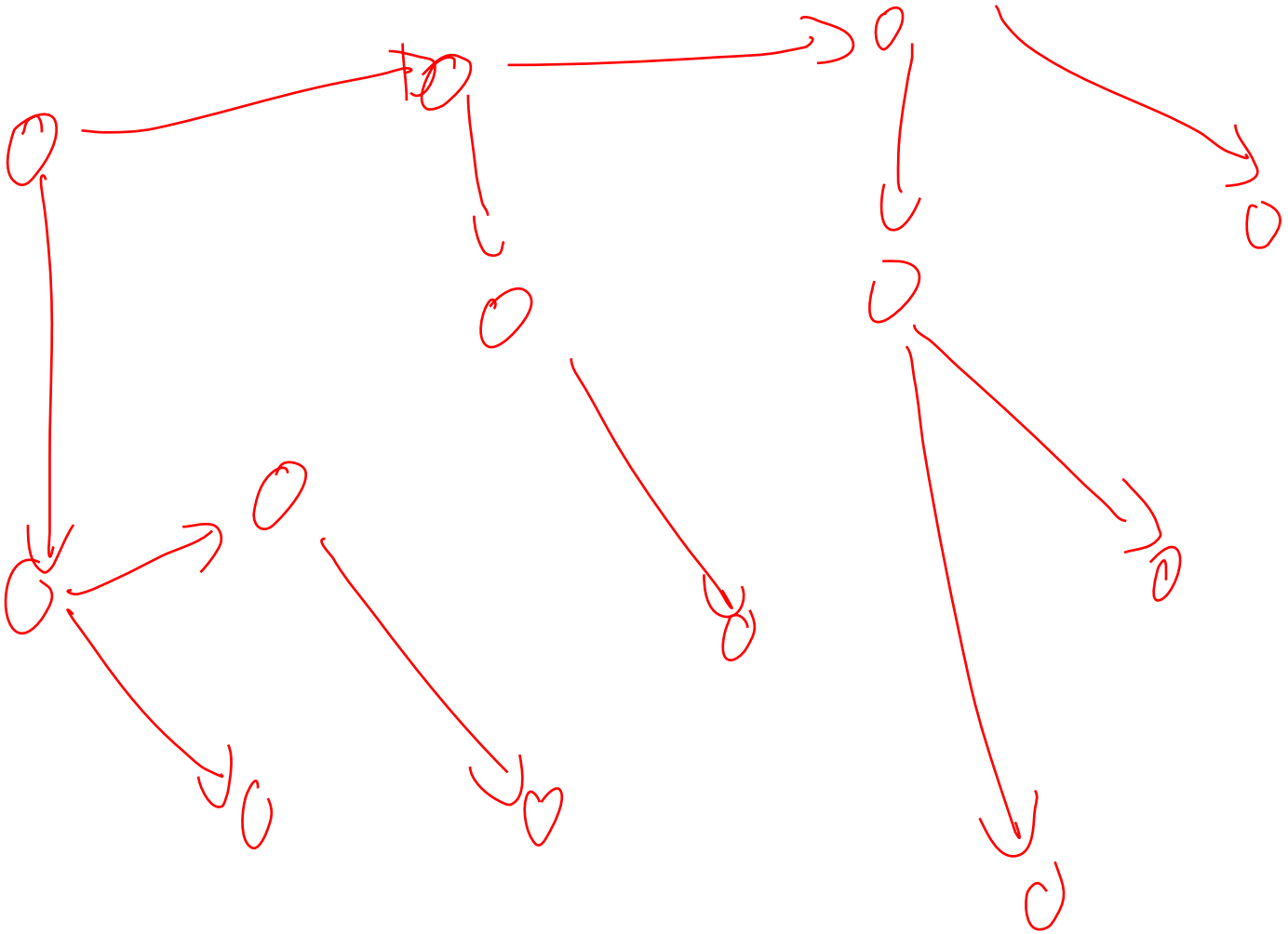
- Motivation
  - Übertragung eines Stroms an viele Empfänger
- Unicast
  - Strom muss mehrfach einzeln übertragen werden
  - Bottleneck am Sender
- Multicast
  - Strom wird über die Router vervielfältigt
  - Kein Bottleneck mehr

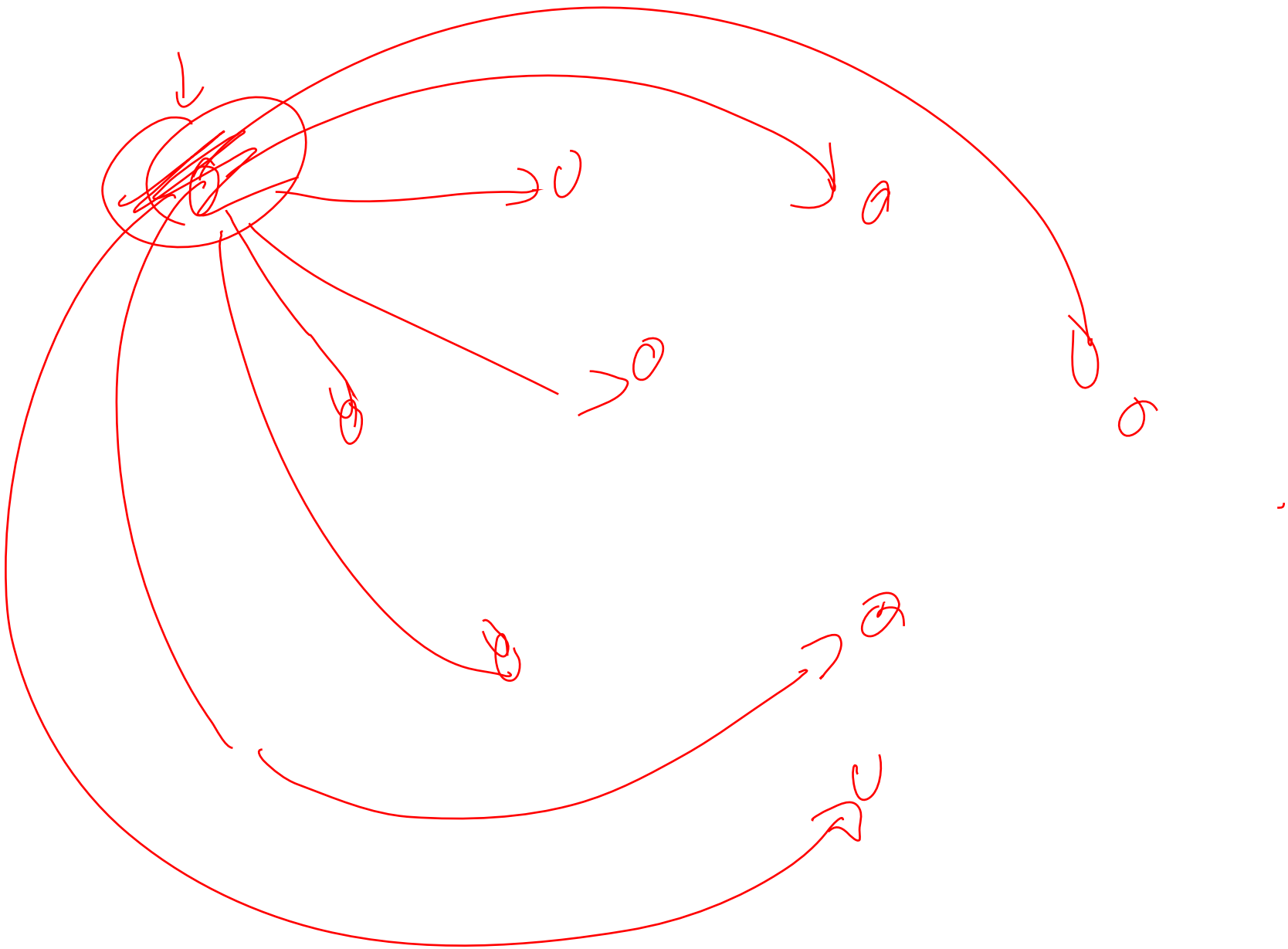


Bilder von Peter J. Welcher

UNI FREIBURG

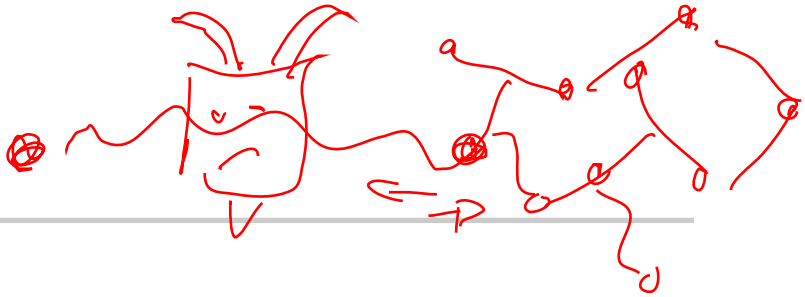

Steiner-Punkt



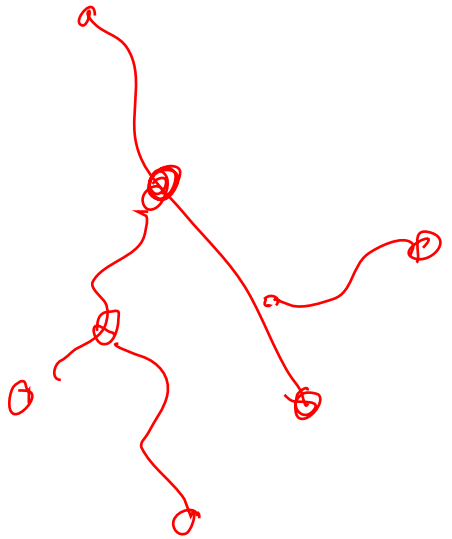


CoNe Freiburg

Funktionsprinzip



- 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



CoNe Freiburg

Routing Protokolle

- 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 Rendevous-Point (RP) in ein-Hop-Entfernung
  - RP muss PIM-SM unterstützen
  - oder Tunneling zu einem Proxy in der Nähe eines RP

CoNe Freiburg

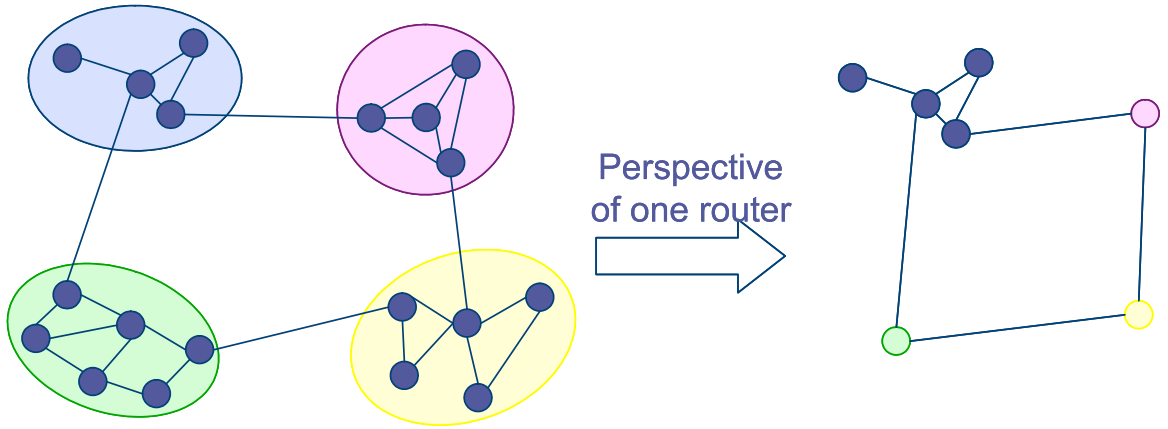
Warum so wenig IP Multicast?

- 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 propertiäre 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!)

UNI FREIBURG

Adressierung und Hierarchisches Routing

- Flache (MAC-) Adressen haben keine Strukturinformation



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

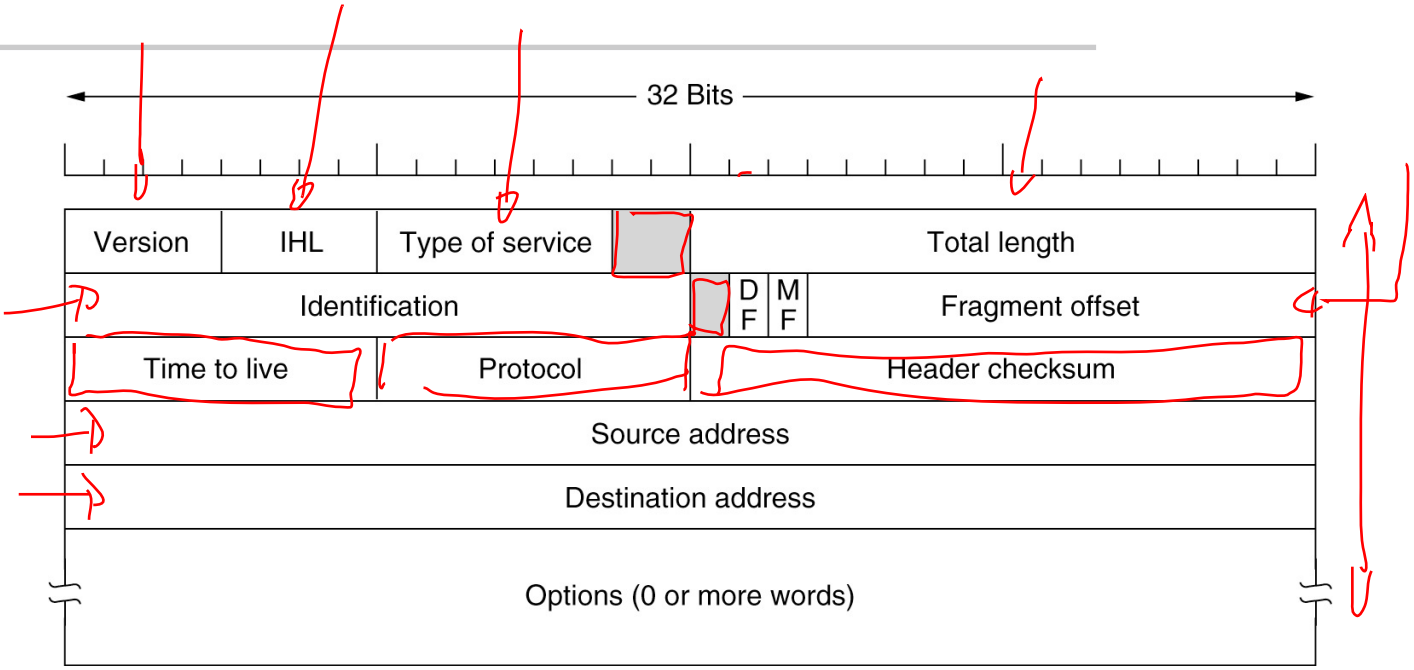
CoNe Freiburg

IP-Adressen und Domain Name System

- 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
  - Optimiere 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

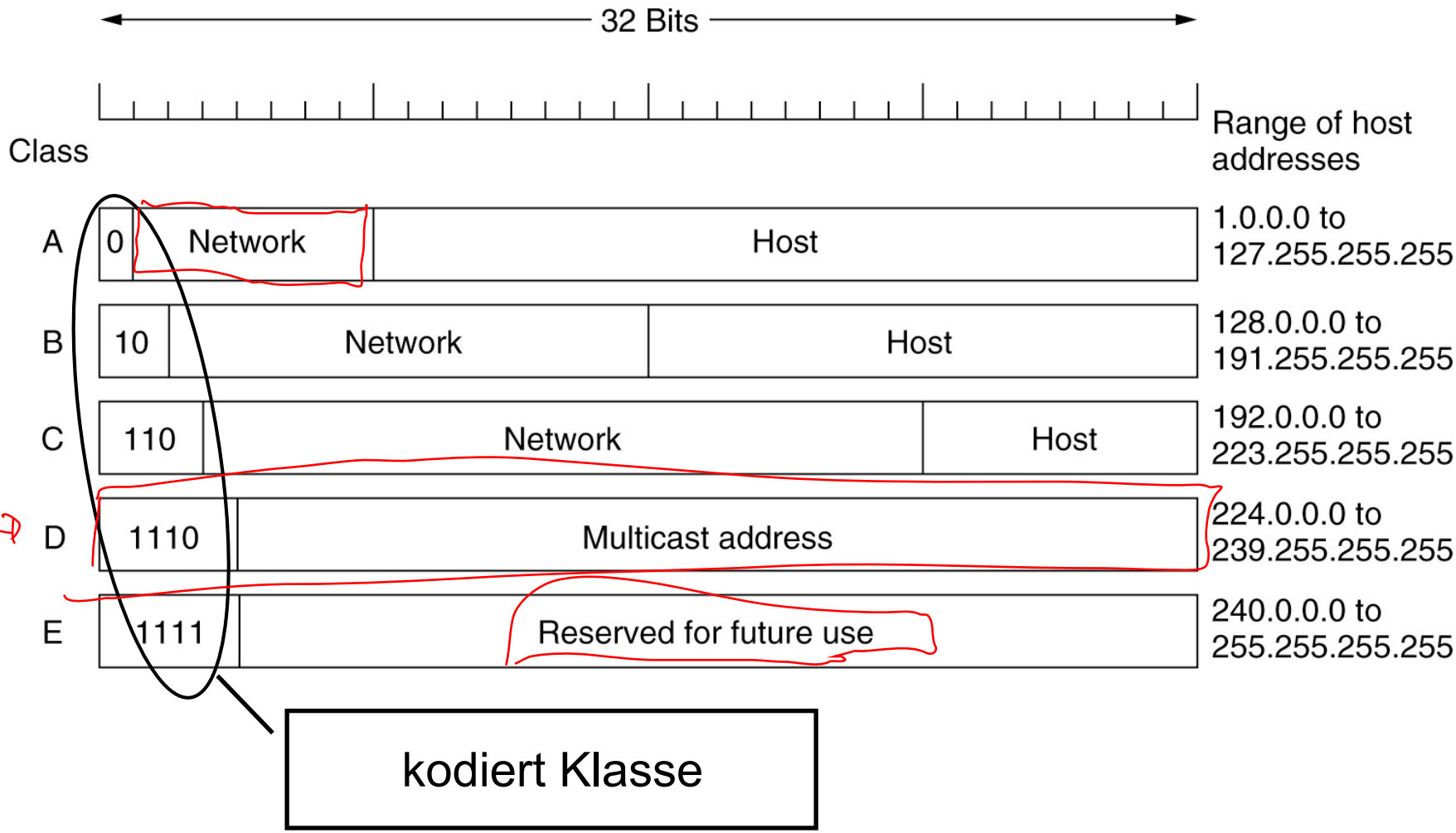
CoNe Freiburg

Internet IP Adressen bis 1993 ← alt!!

- 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”



128 NWs; 16 M hosts

16K NWs; 64K hosts

2M NWs; 256 hosts

CoNe Freiburg

IPv4-Adressen

- 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

CoNe Freiburg

Umwandlung in MAC-Adressen: ARP

- 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

CoNe Freiburg

IPv6

- 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

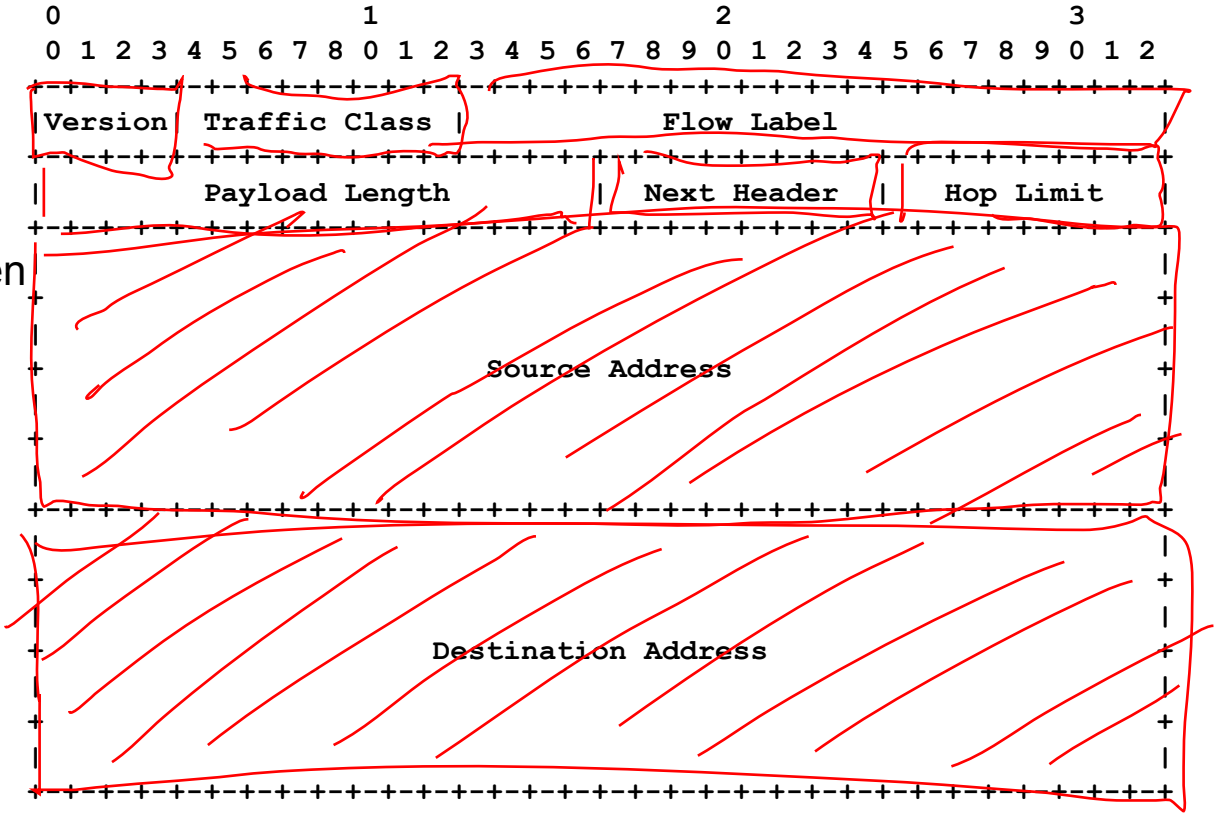
CoNe Freiburg

Lösung der Adressenknappheit: DHCP

- 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



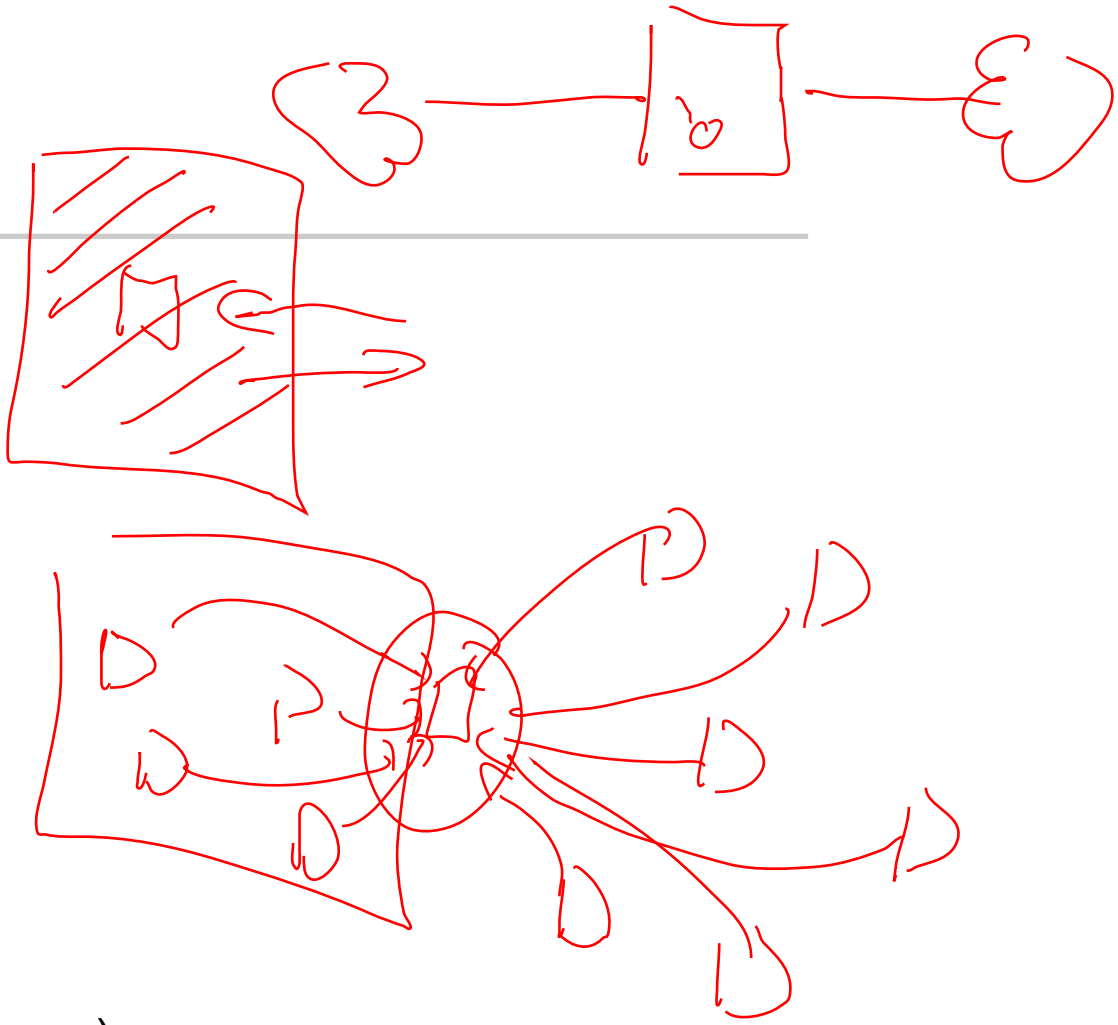
CoNe Freiburg

IPsec (RFC 2401)

- Schutz vor Replay-Attacken
- IKE (Internet Key Exchange) Protokoll
  - Vereinbarung einer Security Association
    - Identifikation, Festlegung von Schlüsseln, Netzwerke, Erneuerungszeiträume für Authentifizierung und IPsec Schlüssel
  - Erzeugung einer SA im Schnellmodus (nach Etablierung)
- Encapsulating Security Payload (ESP)
  - IP-Kopf unverschlüsselt, Nutzdaten verschlüsselt, mit Authentifizierung
- IPsec im Transportmodus (für direkte Verbindungen)
  - IPsec Header zwischen IP-Header und Nutzdaten
  - Überprüfung in den IP-Routern (dort muss IPsec vorhanden sein)
- IPsec im Tunnelmodus (falls mindestens ein Router dazwischen ist)
  - Das komplette IP-Paket wird verschlüsselt und mit dem IPsec-Header in einen neuen IP-Header verpackt
  - Nur an den Enden muss IPsec vorhanden sein.
- IPsec ist Bestandteil von IPv6
- Rückportierungen nach IPv4 existieren

CoNe Freiburg

Firewalls



- Typen von Firewalls
  - Host-Firewall
  - Netzwerk-Firewall
- Netzwerk-Firewall
  - unterscheidet
    - Externes Netz
      (Internet - feindselig)
    - Internes Netz
      (LAN - vertrauenswürdig)
    - Demilitarisierte Zone
      (vom externen Netz erreichbare Server)
- Host-Firewall
  - z.B. Personal Firewall
  - kontrolliert den gesamten Datenverkehr eines Rechners
  - Schutz vor Attacken von außerhalb und von innen (Trojanern)

Firewalls - Methoden

- Paketfilter
  - Sperren von Ports oder IP-Adressen
  - Content-Filter
  - Filtern von SPAM-Mails, Viren, ActiveX oder JavaScript aus HTML-Seiten
- Proxy
  - Transparente (extern sichtbare) Hosts
  - Kanalisierung der Kommunikation und möglicher Attacken auf gesicherte Rechner
- NAT, PAT
  - Network Address Translation
  - Port Address Translation
- Bastion Host
- Proxy

→ Honey pots

CoNe Freiburg

Firewalls: Begriffe

- (Network) Firewall
  - beschränkt den Zugriff auf ein geschütztes Netzwerk aus dem Internet
- Paket-Filter
  - wählen Pakete aus dem Datenfluss in oder aus dem Netzwerk aus
  - Zweck des Eingangsfilter:
    - z.B. Verletzung der Zugriffskontrolle
  - Zweck des Ausgangsfilter:
    - z.B. Trojaner
- Bastion Host
  - ist ein Rechner an der Peripherie, der besonderen Gefahren ausgesetzt ist
  - und daher besonders geschützt ist
- Dual-homed host
  - Normaler Rechner mit zwei Interfaces (verbindet zwei Netzwerke)

CoNe Freiburg

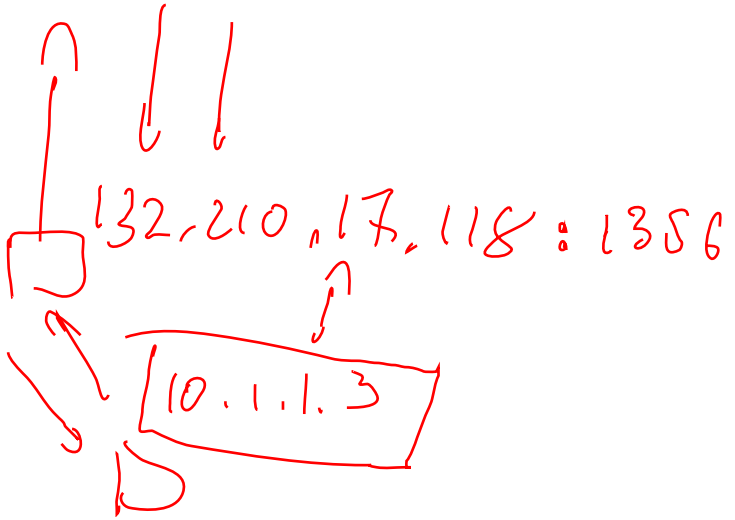
Firewalls: Begriffe

- Proxy (Stellvertreter)
  - Spezieller Rechner, über den Anfragen umgeleitet werden
  - Anfragen und Antworten werden über den Proxy geleitet
  - Vorteil
    - Nur dort müssen Abwehrmaßnahmen getroffen werden
- Perimeter Network:
  - Ein Teilnetzwerk, das zwischen gesicherter und ungesichter Zone eine zusätzliche Schutzschicht bietet
  - Synonym demilitarisierte Zone (DMZ)

CoNe Freiburg

NAT und PAT

- NAT (Network Address Translation)
- Basic NAT (Static NAT)
  - Jede interne IP wird durch eine externe IP ersetzt
- Hiding NAT = PAT (Port Address Translation) = NAPT (Network Address Port Translation)
  - Das Socket-Paar (IP-Addresse und Port-Nummer) wird umkodiert



UNI FREIBURG

CoNe Freiburg

NAT und PAT

- Verfahren
  - Die verschiedenen lokalen Rechner werden in den Ports kodiert
  - Diese werden im Router an der Verbindung zum WAN dann geeignet kodiert
  - Bei ausgehenden Paketen wird die LAN-IP-Adresse und ein kodierter Port als Quelle angegeben
  - Bei eingehenden Paketen (mit der LAN-IP-Adresse als Ziel), kann dann aus dem kodierten Port der lokale Rechner und der passende Port aus einer Tabelle zurückgerechnet werden
- Sicherheitsvorteile
  - Rechner im lokalen Netzwerk können nicht direkt angesprochen werden
  - Löst auch das Problem knapper IPv4-Adressen
  - Lokale Rechner können nicht als Server dienen
- DHCP (Dynamic Host Configuration Protocol)
  - bringt ähnliche Vorteile