Peer-to-Peer-Netzwerke

Albert-Ludwigs-Universität Freiburg
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

Christian Schindelhauer

Sommersemester 2006

5. Vorlesung

10.05.2006

schindel@informatik.uni-freiburg.de

Inhalte

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Kurze Geschichte der Peer-to-Peer-Netzwerke**
- **Das Internet: Unter dem Overlay**
- **Die ersten Peer-to-Peer-Netzwerke**
  - Napster
  - Gnutella
- **Chord**
- **Pastry und Tapestry**
- **Gradoptimierte Netzwerke**
  - Viceroy
  - Distance-Halving
  - Koorde
- **Netzwerke mit Suchbäumen**
  - Skipnet und Skip-Graphs
  - P-Grid
- **Selbstorganisation**
  - Pareto-Netzwerke
  - Zufallsnetzwerke
  - Selbstorganisation
  - Metrikbasierte Netzwerke Sicherheit in Peer-to-Peer-Netzwerken
- **Anonymität**
- **Datenzugriff: Der schnellere Download**
- **Peer-to-Peer-Netzwerke in der Praxis**
  - eDonkey
  - FastTrack
  - Bittorrent
- **Peer-to-Peer-Verkehr**
- **Juristische Situation**

Die Internet-Schichten TCP/IP-Layer

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

Anwendung	Application	Peer-to-Peer-Netzwerke, HTTP (Web), SMTP (E-Mail), ...
Transport	Transport	TCP (Transmission Control Protocol) UDP (User Datagram Protocol)
Vermittlung	Network	IP **(Internet Protocol)** + ICMP **(Internet Control Message Protocol)** + IGMP **(Internet Group Management Protoccol)**
Verbindung	Link	LAN **(z.B. Ethernet, Token Ring etc.)**

IPv4-Adressen

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **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 OSBF verschiedene Netzwerke unter einer ID anbieten
    - Z.B. alle Netzwerke mit Präfix 10010101010* werden über Host X erreicht

Lösungen der Adressknappheit: NAT

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **NAT (Network Address Translation)**

- **Problemstellung**
  - Es gibt zu wenig IP-Adressen für alle Rechner des lokalen Netzwerks
- **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

- **Problem**
  - Rechner im lokalen Netzwerk können nicht direkt angesprochen werden

Lösungen der Adressknappheit: PAT

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Masquerading, PAT (Port Address Translation) oder NAPT (Network Adress Port Translation)**

- **Problemstellung**
  - Es steht für eine LAN mit verschiedenen Rechnern nur eine IP-Adresse zur Verfügung
- **Lösung**
  - 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
- **Probleme:**
  - Lokale Rechner können nicht als Server dienen
  - oder auch nicht als Peer (ohne Zusatzinformation) direkt kontaktiert werden

Lösung der Adressenknappheit: DHCP

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **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 den 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
- **P2P:**
  - DHCP ist gut für die Anynomisierung (wenn der Provider mit spielt)
  - DHCP ist schlecht um Peers wieder auffindbar zu machen

Firewalls

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **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)
- **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
  - Stateful Inspection
    - Beobachtung des Zustands einer Verbindung
- **Firewalls können Peer-to-Peer-Verbindungen gewollt oder ungewollt unterbinden**

IPv6

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

Wozu IPv6:

- **IP-Adressen sind knapp**
  - Zwar gibt es 4 Milliarden in IPv4 (32 Bit)
  - Diese sind aber statisch organisiert in Netzwerk und Rechner-Teil
    - 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

IPsec (RFC 2401)

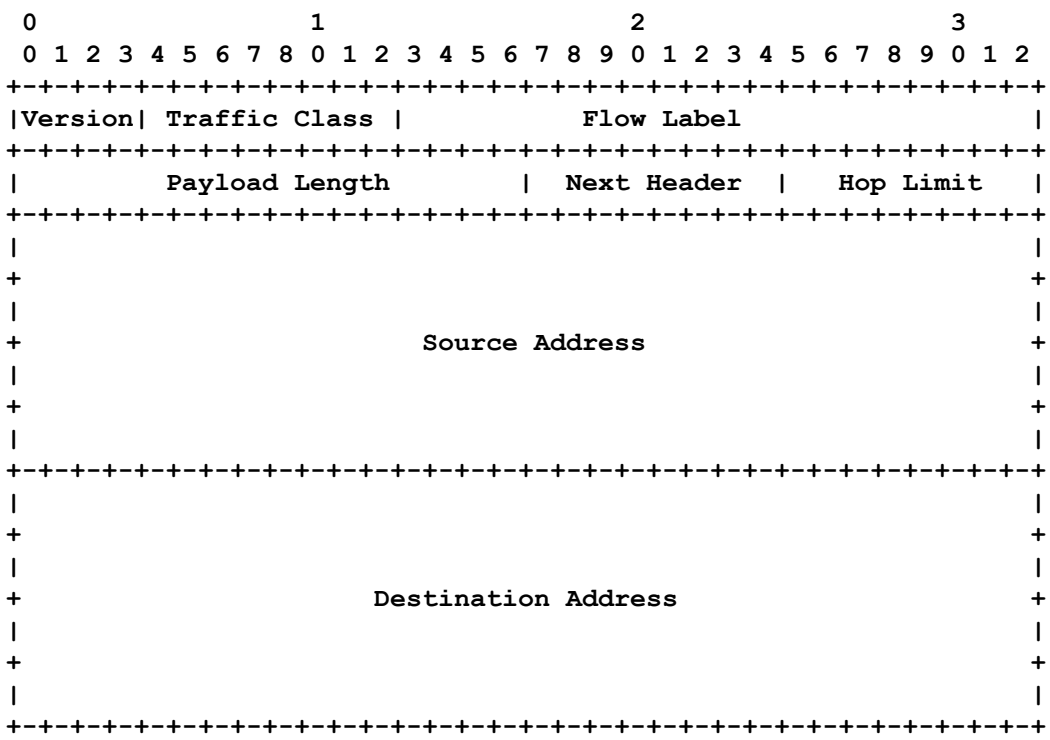
Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Schutz für Replay-Attacken**
- **IKE (Internet Key Exchange) Protokoll**
  - Vereinbarung einer Security Association
    - Idientifikation, Festlegung von Schlüsseln, Netzwerke, Erneuerungszeiträume für Authentffizierung und IPsec Schlüssel
  - Erzeugung einer SA im Schnellmodus (Nach Etablieriung)
- **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**

IPv6-Header (RFC 2460)

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

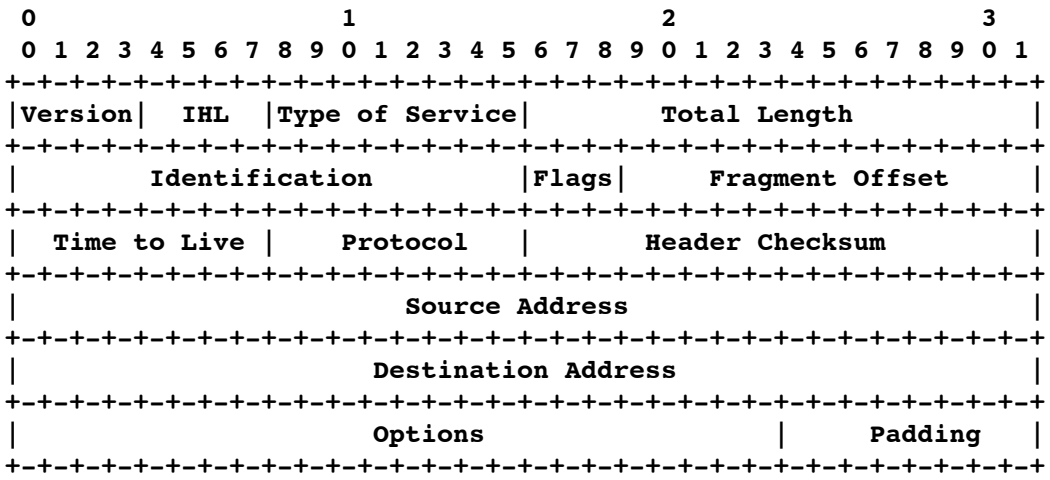
- **Version: 6 = IPv6**
- **Traffic Class**
  - Für QoS (Prioritätsvergabe)
- **Flow Label**
  - Für QoS oder Echtzeitanwendungen
- **Payload Length**
  - Größe des Rests des IP-Pakets (Datagramms)
- **Next Header (wie bei IPv4: protocol)**
  - Z.B. ICMP, IGMP, TCP, EGP, UDP, Multiplexing, ...
- **Hop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



IPv4-Header (RFC 791)

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Version: 4 = IPv4**
- **IHL: Headerlänge**
  - in 32 Bit-Wörter (>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



Zusammenfassung Internet als Underlay

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **IP: Vermittlungsschicht**
  - NAT, PAT, DHCP und Firewalls be- oder verhindern direkte Peer-to-Peer-Verbindungen
    - Rechner erhalten andere Adressen
  - IPv6
    - löst das IP-Adress-Problem nachhaltig
    - setzt sich wegen der Rückportierungen von DHCP, IPsec und Multicast nach IPv4 nur langsam oder gar nicht durch
  - IPsec ermöglicht den unkontrollierten direkten Download
- **TCP: Transportschicht**
  - UDP ist unzuverlässig, aber schnell
  - TCP ist zuverlässig mit Overhead
  - Eigene Protokolle können mit UDP implementiert werden
    - Aber Fairness und Effizienz können gefährdet werden
- **Ein gutes Peer-to-Peer-Netzwerks muss das alles berücksichtigen**

Ende der 5. Vorlesung

Peer-to-Peer-Netzwerke

Christian Schindelhauer

schindel@informatik.uni-freiburg.de

Albert-Ludwigs-Universität Freiburg
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer