Systeme II

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

Christian Schindelhauer

Sommersemester 2007

9. Vorlesungswoche

18.06.-22.06.2007

schindel@informatik.uni-freiburg.de

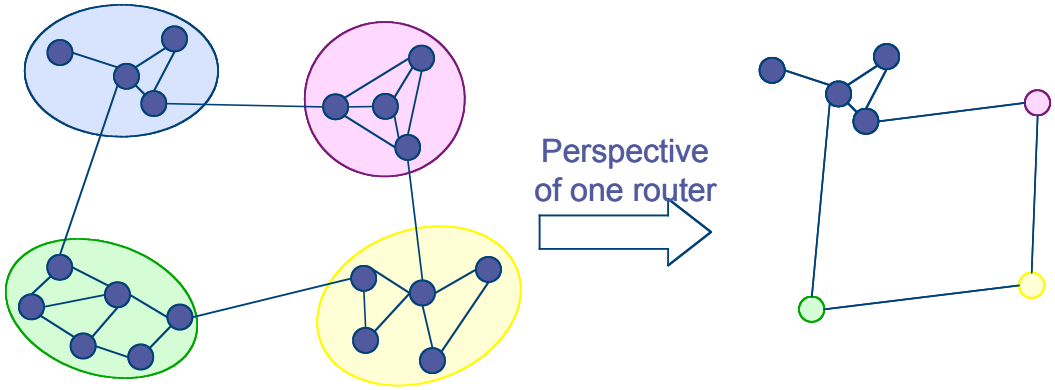
Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

Die Vermittlungsschicht
The Network Layer

Adressierung und Hierarchisches Routing

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

- **Flache (MAC-) Adressen haben keine Struktur-Information**



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

IP-Adressen und Domain Name System

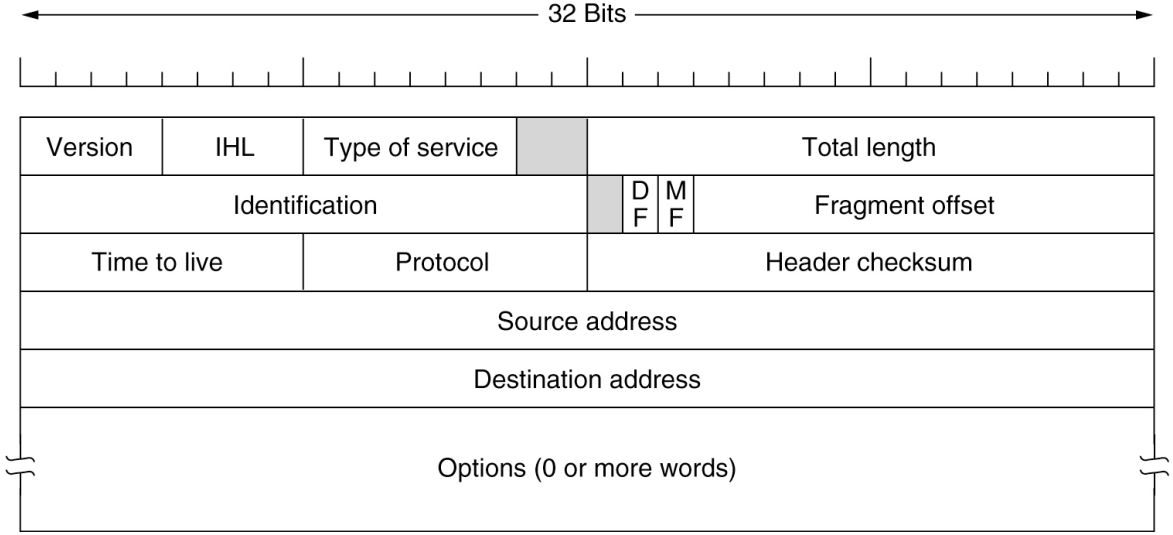
Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **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)

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



Internet IP Adressen bis 1993

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

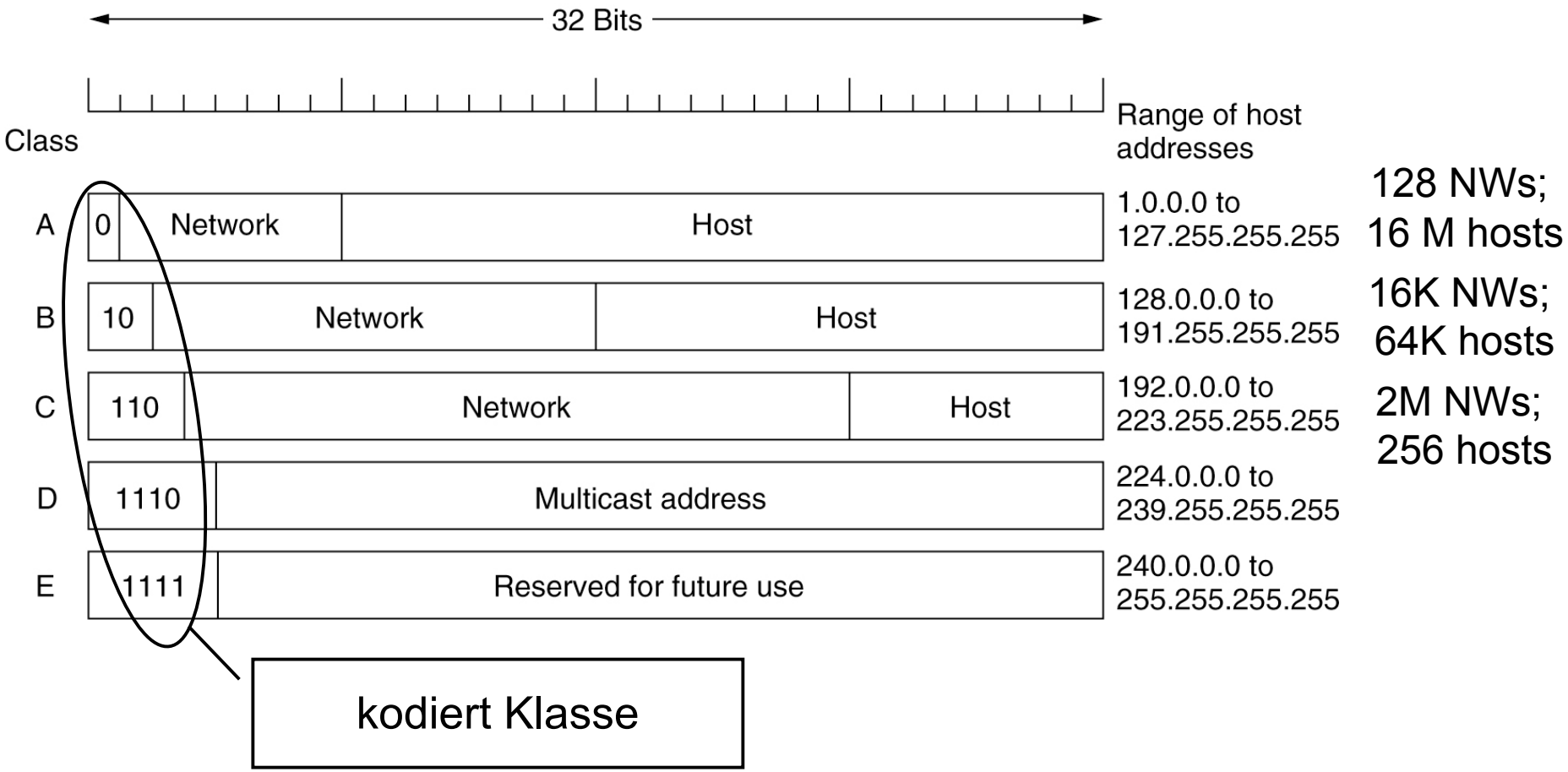
- **IP-Adressen unterscheiden zwei Hierarchien**
  - Netzwerk-Interfaces
  - Netzwerke
    - Verschiedene Netzwerkgrößen
    - Netzwerkklassen:
      - Groß - mittel - klein (Klasse A, B, and C)

- **Eine IP-Adresse hat 32 Bits**
  - Erster Teil: Netzwerkadresse
  - Zweiter Teil: Interface

IP-Klassen bis 1993

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

- **Klassen A, B, and C**
- **D für multicast; E: “reserved”**



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

Umwandlung in MAC-Adressen: ARP

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

- **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

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

Lösung der Adressenknappheit: DHCP

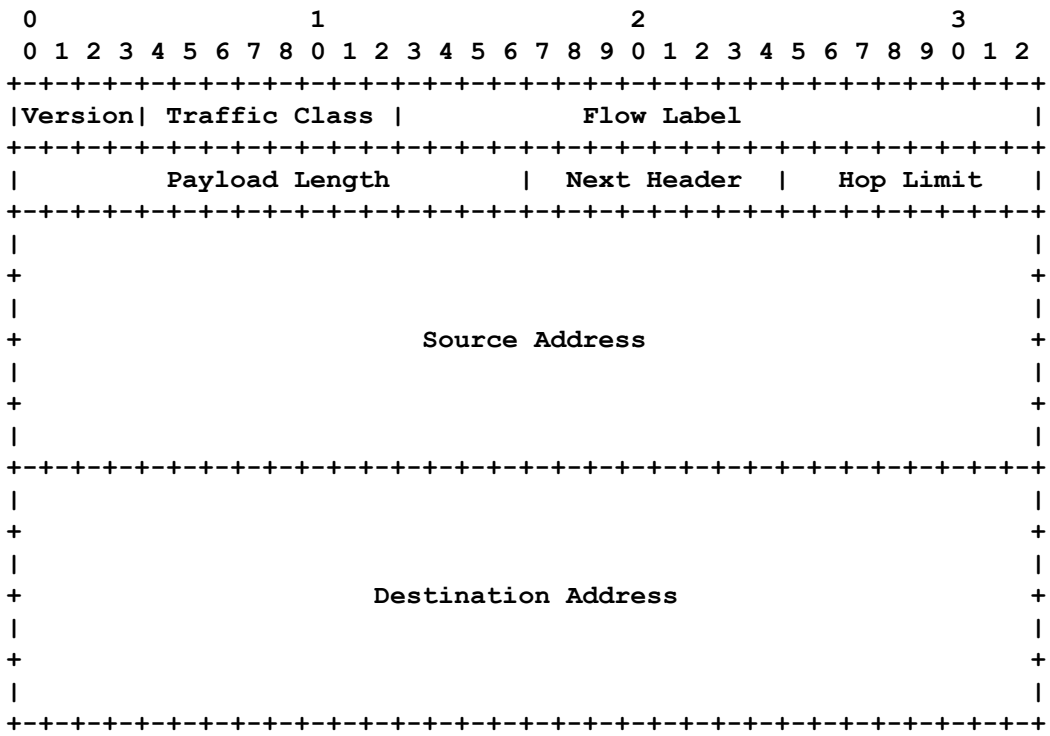
Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **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

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



IPsec (RFC 2401)

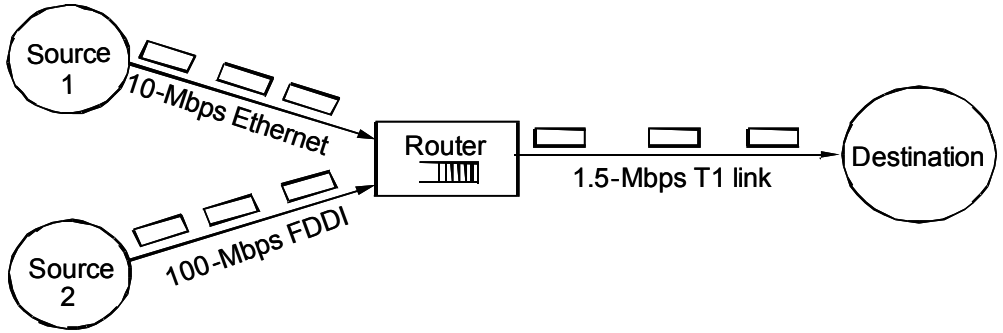
Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Schutz für Replay-Attacken**
- **IKE (Internet Key Exchange) Protokoll**
  - Vereinbarung einer Security Association
    - 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**

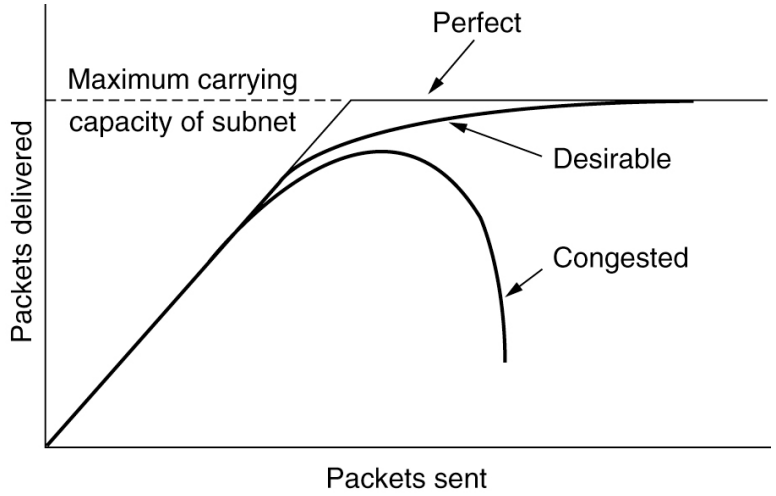
Congestion Control Stauvermeidung

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

- **Jedes Netzwerk hat eine eingeschränkte Übertragungs-Bandbreite**



- **Wenn mehr Daten in das Netzwerk eingeleitet werden, führt das zum**
  - Datenstau (Congestion) oder gar
  - Netzwerkzusammenbruch(***congestive collapse***)



- **Folge: Datepakete werden nicht ausgeliefert**

Schneeballeffekt

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

- **Congestion control soll Schneeballeffekte vermeiden**
  - Netzwerküberlast führt zu Paketverlust (Pufferüberlauf, ...)
  - Paketverlust führt zu Neuversand
  - Neuversand erhöht Netzwerklast
  - Höherer Paketverlust
  - Mehr neu versandte Pakete
  - ...

Anforderungen an Congestion Control

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

- **Effizienz**
  - Verzögerung klein
  - Durchsatz hoch
- **Fairness**
  - Jeder Fluss bekommt einen fairen Anteil
  - Priorisierung möglich
    - gemäß Anwendung
    - und Bedarf

Mittel der Stauvermeidung

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

- **Erhöhung der Kapazität**
  - Aktivierung weiterer Verbindungen, Router
  - Benötigt Zeit und in der Regel den Eingriff der Systemadministration
- **Reservierung und Zugangskontrolle**
  - Verhinderung neuen Verkehrs an der Kapazitätsgrenze
  - Typisch für (Virtual) Circuit Switching

- **Verringerung und Steuerung der Last**
  - (Dezentrale) Verringerung der angeforderten Last bestehender Verbindungen
  - Benötigt Feedback aus dem Netzwerk
  - Typisch für Packet Switching
    - wird in TCP verwendet

Orte und Maße

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

- **Router oder Host-orientiert**
  - Messpunkt (wo wird der Stau bemerkt)
  - Steuerung (wo werden die Entscheidungen gefällt)
  - Aktion (wo werden Maßnahmen ergriffen)
- **Fenster-basiert oder Raten-basiert**
  - Rate: x Bytes pro Sekunde
  - Fenster: siehe Fenstermechanismen in der Sicherungsschicht
    - wird im Internet verwendet

Routeraktion: Paket löschen

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

- **Bei Pufferüberlauf im Router**
  - muss (mindestens) ein Paket gelöscht werden
- **Das zuletzt angekommene Paket löschen (*drop-tail queue*)**
  - Intuition: “Alte” Pakete sind wichtiger als neue (Wein)
    - z.B. für go-back-n-Strategie
- **Ein älteres Paket im Puffer löschen**
  - Intuition: Für Multimedia-Verkehr sind neue Pakete wichtiger als alte (Milch)

Paketverlust erzeugt implizites Feedback

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

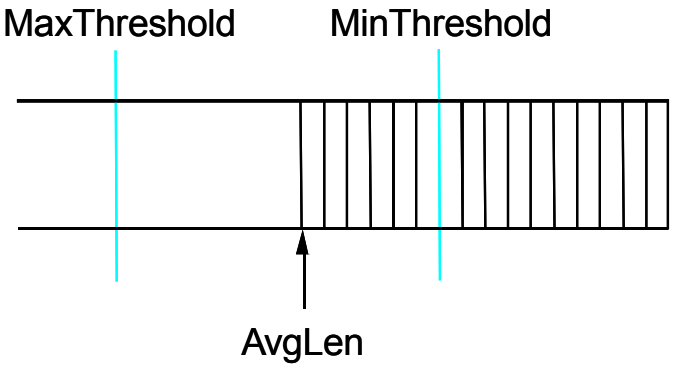
- **Paketverlust durch Pufferüberlauf im Router erzeugt Feedback in der Transportschicht beim Sender durch ausstehende Bestätigungen**
  - Internet
- **Annahme: Paketverlust wird hauptsächlich durch Stau ausgelöst**

- **Maßnahme:**
  - Transport-Protokoll passt Senderate an die neue Situation an

Proaktive Methoden

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

- **Pufferüberlauf deutet auf Netzwerküberlast hin**
- **Idee: Proaktives Feedback = Stauvermeidung (*Congestion avoidance*)**
  - Aktion bereits bei kritischen Anzeigewerten
  - z.B. bei Überschreitung einer Puffergröße
  - z.B. wenn kontinuirlich mehr Verkehr eingeht als ausgeliefert werden kann
  - ...
  - Router ist dann in einem Warn-Zustand



Proactive Aktion: Pakete drosseln (Choke packets)

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

- **Wenn der Router in dem Warnzustand ist:**
  - Sendet er Choke-Pakete (Drossel-Pakete) zum Sender
- **Choke-Pakete fordern den Sender auf die Sende-Rate zu verringern**

- **Problem:**
  - Im kritischen Zustand werden noch mehr Pakete erzeugt
  - Bis zur Reaktion beim Sender vergrößert sich das Problem

Proaktive Aktion: Warnbits

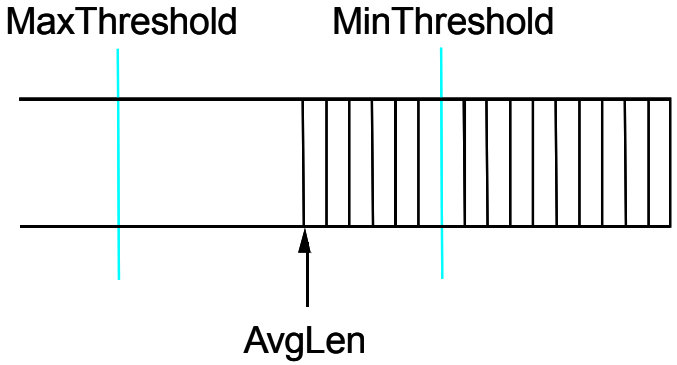
Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

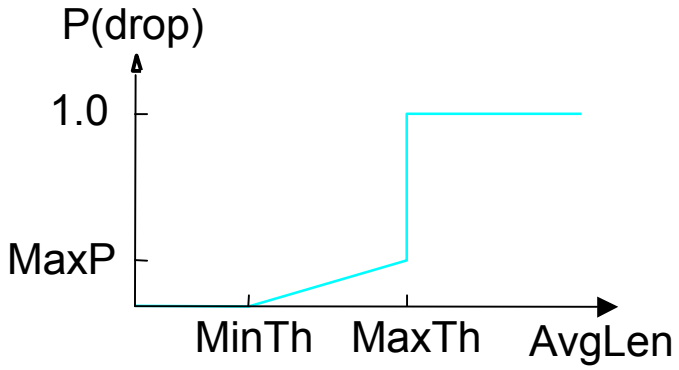
- **Wenn der Router in dem Warnzustand ist:**
  - Sendet er Warn-Bits in allen Paketen zum Ziel-Host
- **Ziel-Host sendet diese Warn-Bits in den Bestätigungs-Bits zurück zum Sender**
  - Quelle erhält Warnung und reduziert Sende-Rate

Proaktive Aktion: Random early detection (RED)

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

- **Verlorene Pakete werden als Indiz aufgefasst**
- **Router löschen Pakete willkürlich im Warnzustand**
- **Löschrate kann mit der Puffer-Größe steigen**





Reaktion des Senders

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

- **Raten-basierte Protokolle**
  - Reduzierung der Sende-Rate
  - Problem: Um wieviel?

- **Fenster-basierte Protokolle:**
  - Verringerung des Congestion-Fensters
  - z.B. mit AIMD (additive increase, multiplicative decrease)

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

Die Transportschicht

Dienste der Transport-Schicht

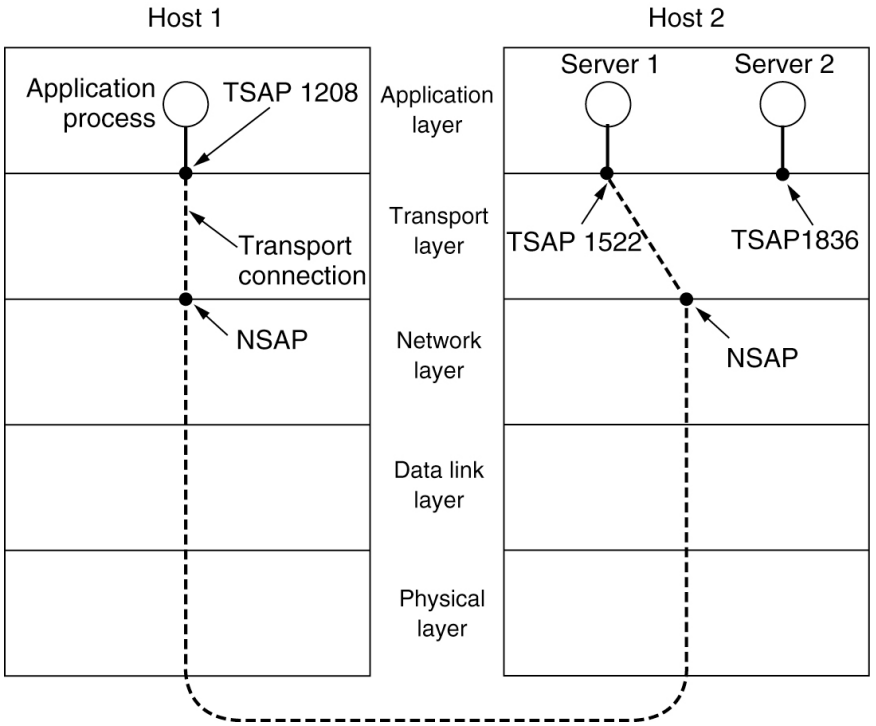
Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Verbindungslos oder Verbindungsorientert**
  - Beachte: Sitzungsschicht im ISO/OSI-Protokoll
- **Verlässlich oder Unverlässlich**
  - Best effort oder Quality of Service
  - Fehlerkontrolle
- **Mit oder ohne Congestion Control**
- **Möglichkeit verschiedener Punkt-zu-Punktverbindungen**
  - Stichwort: Demultiplexen
- **Interaktionsmodelle**
  - Byte-Strom, Nachrichten, „Remote Procedure Call“

Multiplex in der Transportschicht

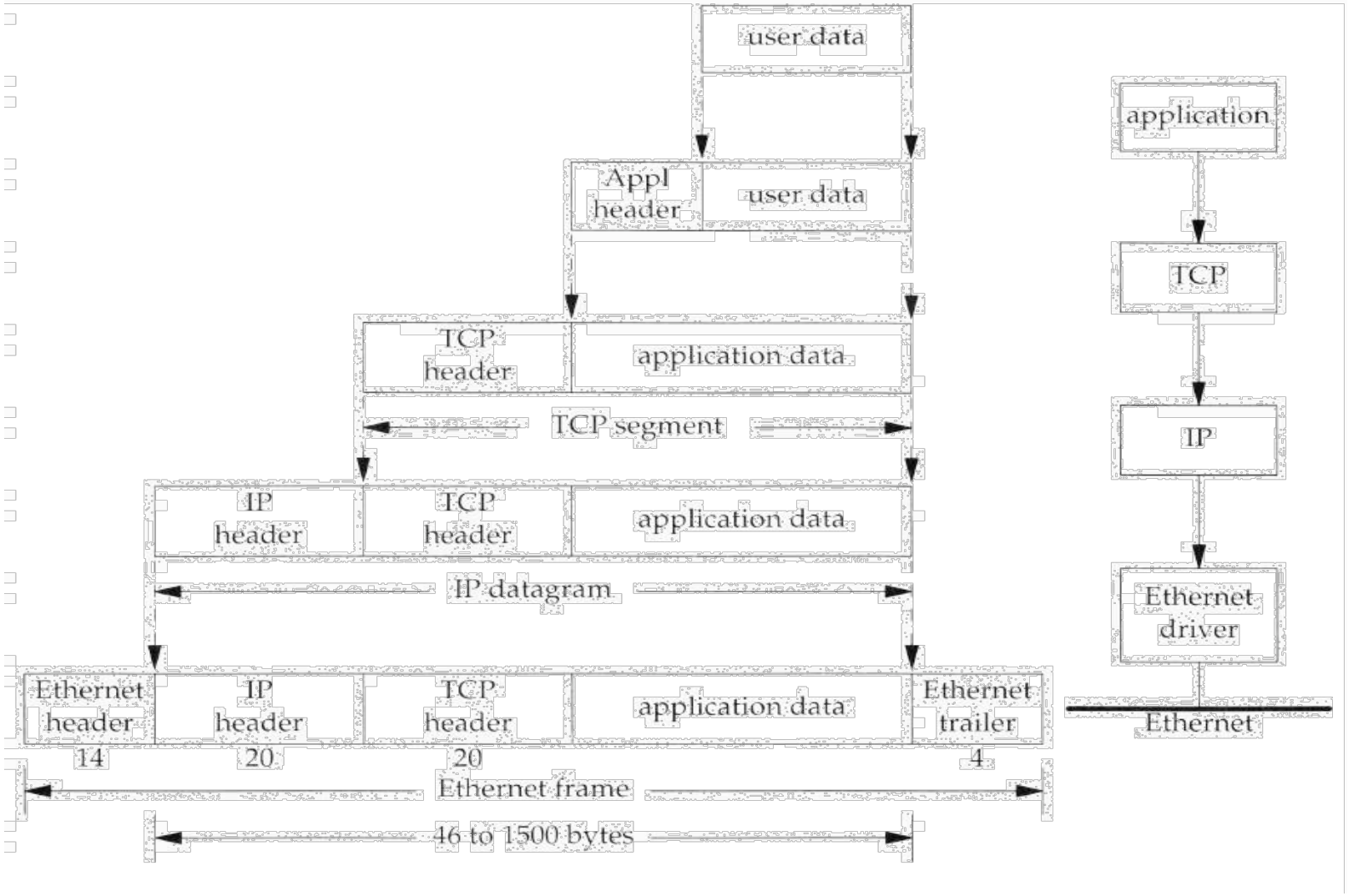
Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Die Netzwerkschicht leitet Daten an die Transportschicht unkontrolliert weiter**
- **Die Transportschicht muss sie den verschiedenen Anwendungen zuordnen:**
  - z.B. Web, Mail, FTP, ssh, ...
  - In TCP/UDP durch Port-Nummern
  - z.B. Port 80 für Web-Server



Datenkapselung

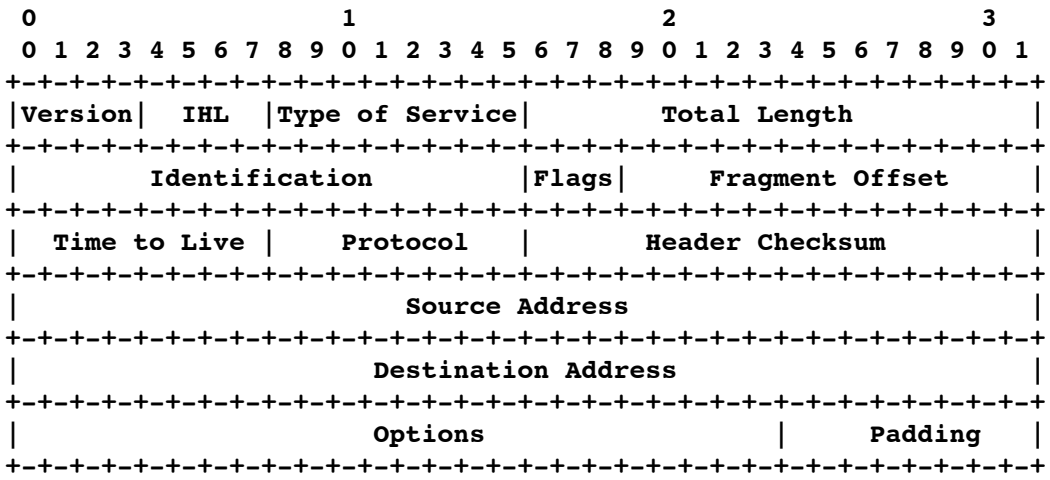
Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer



IP-Header (RFC 791)

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

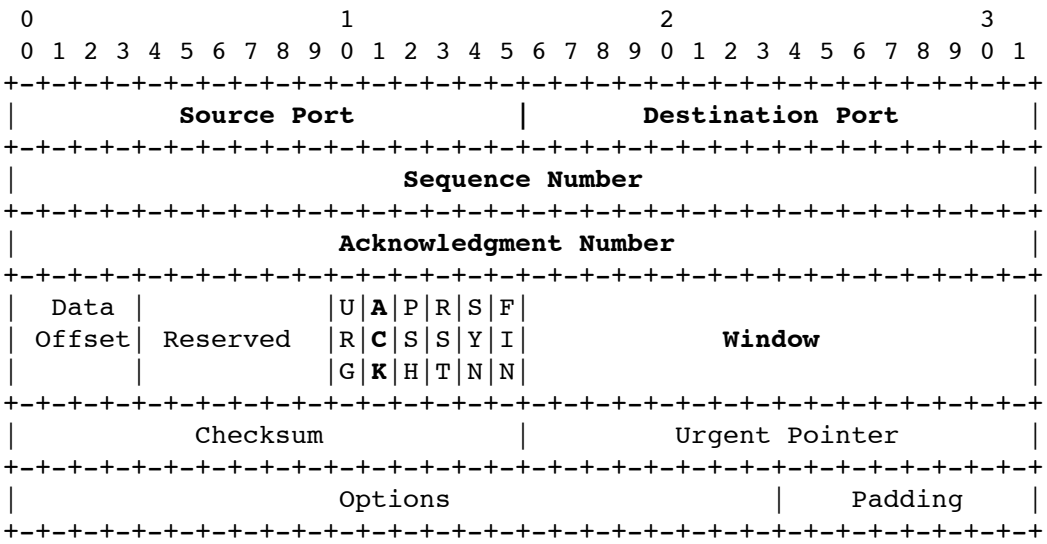
- **Version: 4 = IPv4**
- **IHL: Headerlänge**
  - in 32 Bit-Wörter (>5)
- **Type of Service**
  - Optimiere delay, throughput, reliability, monetary cost
- **Checksum (nur für IP-Header)**
- **Source and destination IP-address**
- **Protocol, identifiziert passendes Protokoll**
  - Z.B. TCP, UDP, ICMP,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



TCP-Header

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

- **Sequenznummer**
  - Nummer des ersten Bytes im Segment
  - Jedes Datenbyte ist nummeriert modulo 2^{32}
- **Bestätigungsnummer**
  - Aktiviert durch ACK-Flag
  - Nummer des nächsten noch nicht bearbeiteten Datenbytes
    - = letzte Sequenznummer + letzte Datenmenge
- **Sonstiges:**
  - Port-Adressen
    - Für parallele TCP-Verbindungen
    - Ziel-Port-Nr.
    - Absender-Port
  - Headerlänge
    - data offset
  - Prüfsumme
    - Für Header und Daten



Transportschicht (transport layer)

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

- **TCP (transmission control protocol)**
  - Erzeugt zuverlässigen Datenfluß zwischen zwei Rechnern
  - Unterteilt Datenströme aus Anwendungsschicht in Pakete
  - Gegenseite schickt Empfangsbestätigungen (Acknowledgments)
- **UDP (user datagram protocol)**
  - Einfacher unzuverlässiger Dienst zum Versand von einzelnen Päckchen
  - Wandelt Eingabe in ein Datagramm um
  - Anwendungsschicht bestimmt Paketgröße
- **Versand durch Netzwerkschicht**
- **Kein Routing: End-to-End-Protokolle**

TCP (I)

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

- **TCP ist ein verbindungsorientierter, zuverlässiger Dienst für bidirektionale Byteströme**

- **TCP ist verbindungsorientiert**
  - Zwei Parteien identifiziert durch Socket: IP-Adresse und Port (TCP-Verbindung eindeutig identifiziert durch Socketpaar)
  - Kein Broadcast oder Multicast
  - Verbindungsaufbau und Ende notwendig
  - Solange Verbindung nicht (ordentlich) beendet, ist Verbindung noch aktiv

TCP (II)

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

- **TCP ist ein verbindungsorientierter, zuverlässiger Dienst für bidirektionale Byteströme**

- **TCP ist zuverlässig**
  - Jedes Datenpaket wird bestätigt (acknowledgment)
  - Erneutes Senden von unbestätigten Datenpakete
  - Checksum für TCP-Header und Daten
  - TCP nummeriert Pakete und sortiert beim Empfänger
  - Löscht duplizierte Pakete

TCP (III)

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

- **TCP ist ein verbindungsorientierter, zuverlässiger Dienst für bidirektionale Byteströme**

- **TCP ist ein Dienst für bidirektionale Byteströme**
  - Daten sind zwei gegenläufige Folgen aus einzelnen Bytes (=8 Bits)
  - Inhalt wird nicht interpretiert
  - Zeitverhalten der Datenfolgen kann verändert werden
  - Versucht zeitnahe Auslieferung jedes einzelnen Datenbytes
  - Versucht Übertragungsmedium effizient zu nutzen
    - = wenig Pakete

Ende der 9. Vorlesungswoche

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

Systeme II

Christian Schindelhauer
schindel@informatik.uni-freiburg.de