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

NAT und PAT

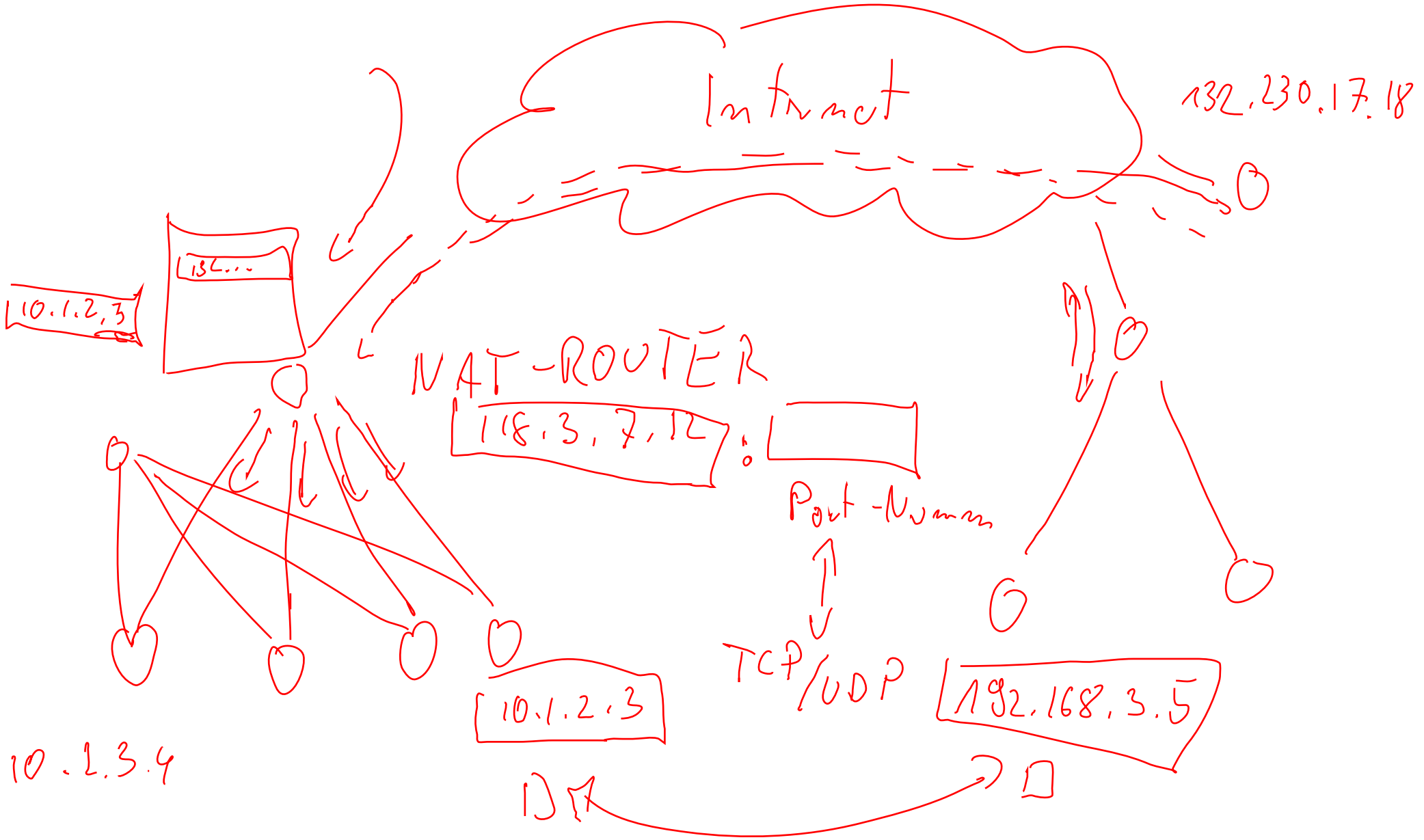
- NAT (Network Address Translation)
- Basic NAT (Static NAT)
  - Jede interne IP wird durch eine externe IP ersetzt
- Hiding NAT = PAT (Port Address Translation) = NAPT (Network Address Port Translation)
  - Das Socket-Paar (IP-Addresse und Port-Nummer) wird umkodiert

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 → DNS
- DHCP (Dynamic Host Configuration Protocol)
  - bringt ähnliche Vorteile

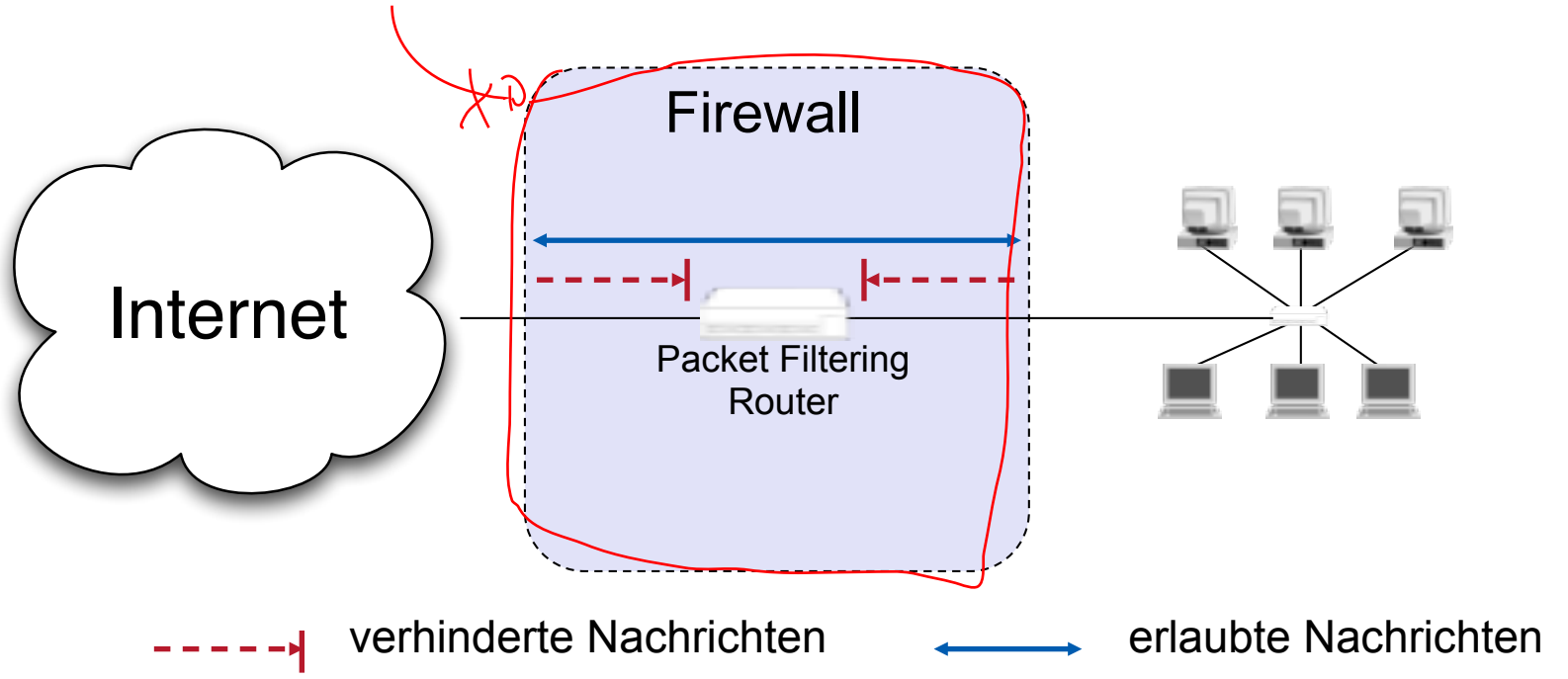
↳ BootP


Internet
132.230.17.18
10.1.2.3
NAT-ROUTER
18.3.7.12 :
Port-Nummer
TCP/UDP
192.168.3.5
10.1.2.3
10.2.3.4

CoNe Freiburg

Firewall-Architektur Einfacher Paketfilter

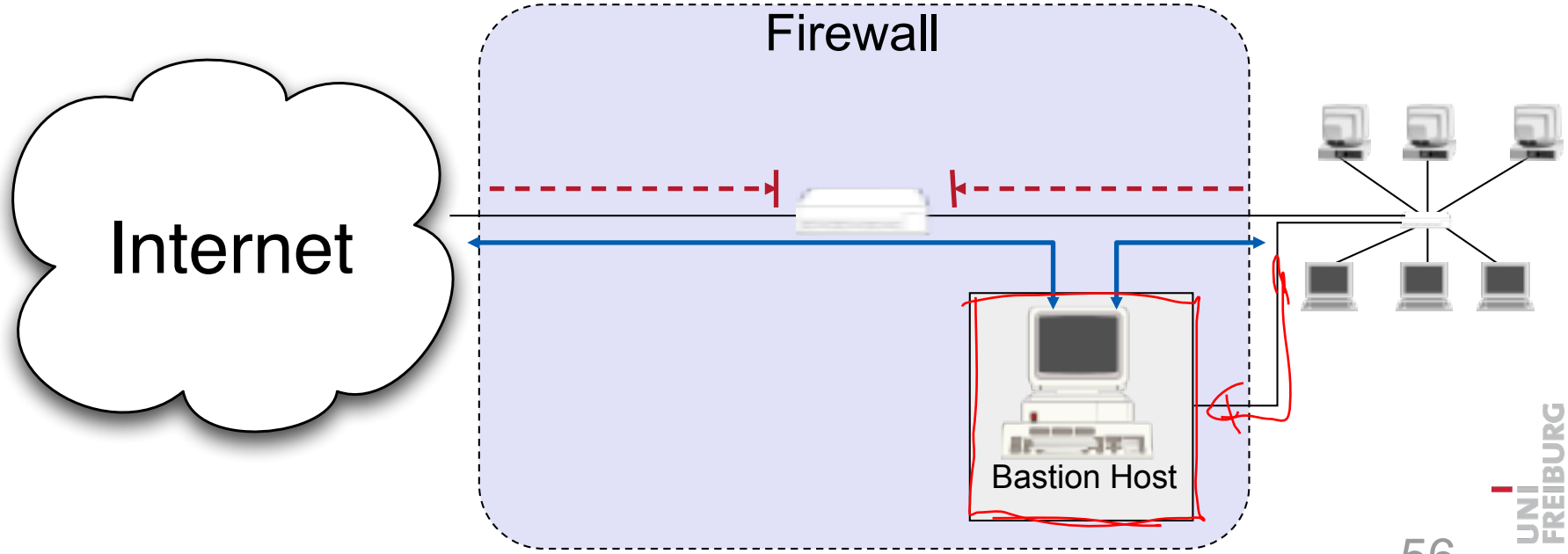
- Realisiert durch
  - Eine Standard-Workstation (e.g. Linux PC) mit zwei Netzwerk-Interfaces und Filter-Software oder
  - Spezielles Router-Gerät mit Filterfähigkeiten



CoNe Freiburg

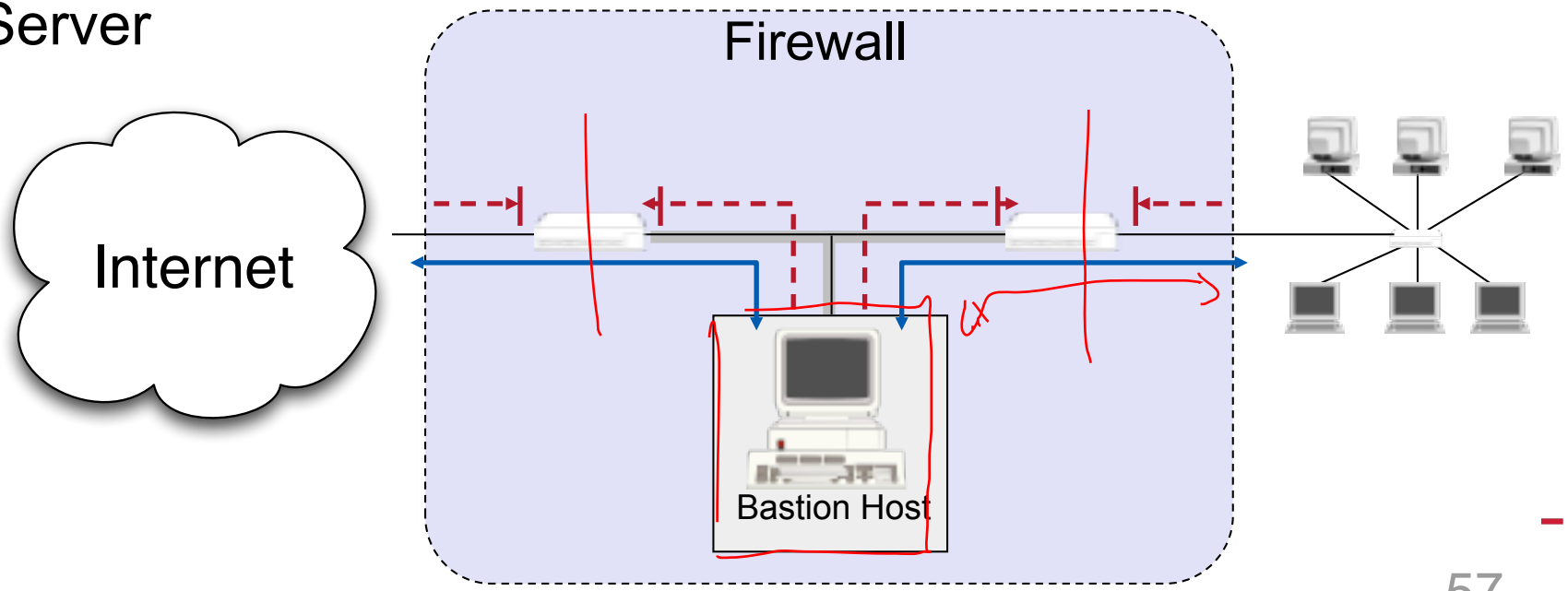
Firewall-Architektur Screened Host

- Screened Host
- Der Paketfilter
  - erlaubt nur Verkehr zwischen Internet und dem Bastion Host und
  - Bastion Host und geschützten Netzwerk
- Der Screened Host bietet sich als Proxy an
  - Der Proxy Host hat die Fähigkeiten selbst Angriffe abzuwehren



Firewall-Architektur Screened Subnet

- Perimeter network zwischen Paketfiltern
- Der innere Paketfilter schützt das innere Netzwerk, falls das Perimeter-Network in Schwierigkeiten kommt
  - Ein gehackter Bastion Host kann so das Netzwerk nicht ausspionieren
- Perimeter Netzwerke sind besonders geeignet für die Bereitstellung öffentlicher Dienste, z.B. FTP, oder WWW-Server



CoNe Freiburg

Firewall und Paketfilter

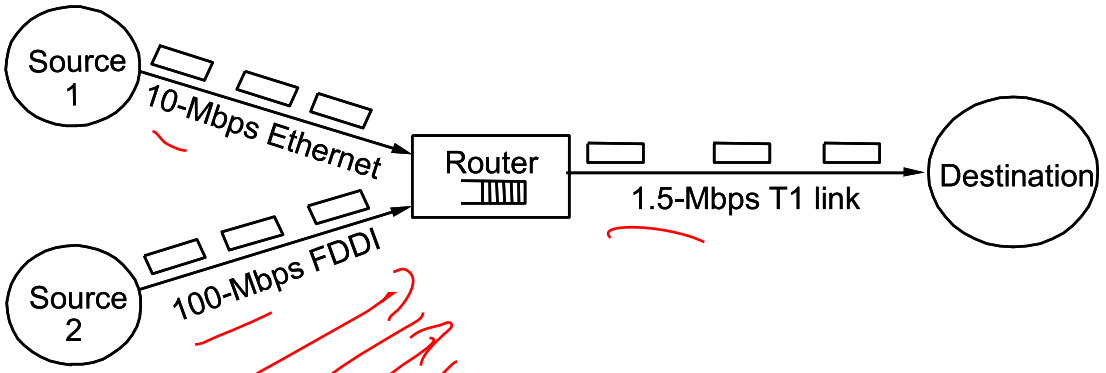
- Fähigkeiten von Paketfilter
  - Erkennung von Typ möglich (Demultiplexing-Information)
- Verkehrskontrolle durch
  - Source IP Address
  - Destination IP Address
  - Transport protocol
  - Source/destination application port
- Grenzen von Paketfiltern (und Firewalls)
  - Tunnel-Algorithmen sind aber mitunter nicht erkennbar
  - Möglich ist aber auch Eindringen über andere Verbindungen
    - z.B. Laptops, UMTS, GSM, Memory Sticks

CoNe Freiburg

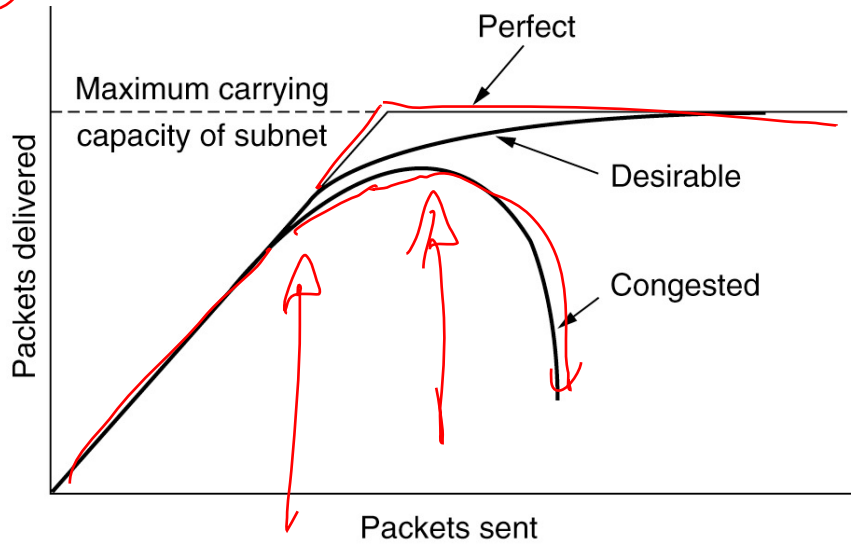
Congestion Control Stauvermeidung

→ Transport

- 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: Datenpakete werden nicht ausgeliefert

CoNe Freiburg

Schneeballeffekt

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

CoNe Freiburg

Anforderungen an Congestion Control

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

CoNe Freiburg

Mittel der Stauvermeidung

- 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

CoNe Freiburg

Orte und Maße

- 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

CoNe Freiburg

Routeraktion: Paket löschen

- 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)

CoNe Freiburg

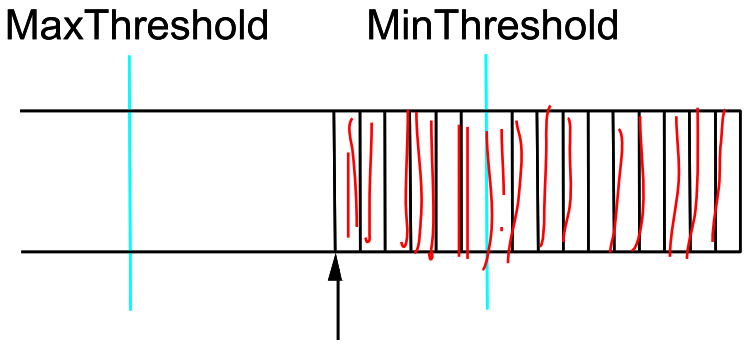
Paketverlust erzeugt implizites Feedback

- 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

CoNe Freiburg

Proaktive Methoden

- Pufferüberlauf deutet auf Netzwerküberlast hin
- Idee: Proaktives Feedback = Stauvermeidung (Congestion avoidance)



RED

  - Aktion bereits bei kritischen Anzeigewerten
  - z.B. bei Überschreitung einer Puffergröße
  - z.B. wenn kontinuierlich mehr Verkehr eingeht als ausgeliefert werden kann
  - ...
  - Router ist dann in einem Warn-Zustand

CoNe Freiburg

Proactive Aktion: Pakete drosseln (Choke packets)

- 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

CoNe Freiburg

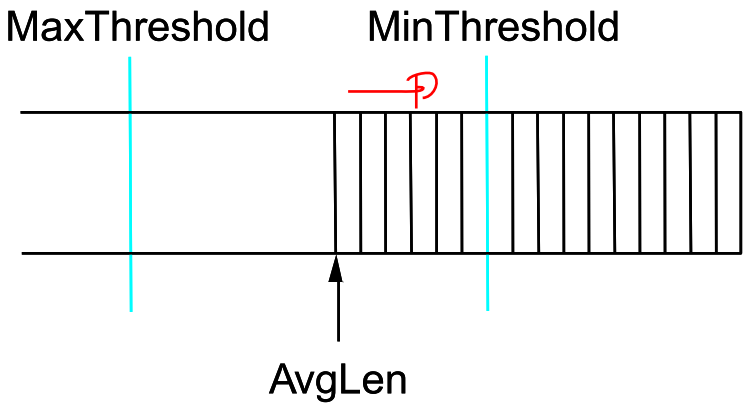
Proaktive Aktion: Warnbits

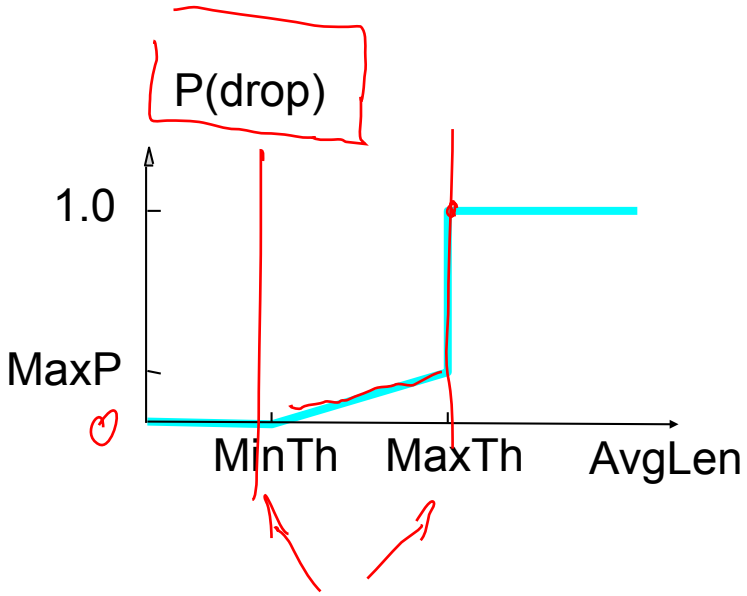
- Wenn der Router in dem Warnzustand ist:
  - Sendet er Warn-Bits in allen Paketen zum Ziel-Host
- Ziel-Host sendet diese Warn-Bits in den Bestätigungs-Bits zurück zum Sender
  - Quelle erhält Warnung und reduziert Sende-Rate

CoNe Freiburg

Proaktive Aktion: Random early detection (RED)

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





CoNe Freiburg

Reaktion des Senders

- 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)

CoNe Freiburg

IIF INSTITUT FÜR INFORMATIK FREIBURG

Systeme II

4. Die Vermittlungsschicht

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

UNI FREIBURG