Systeme II

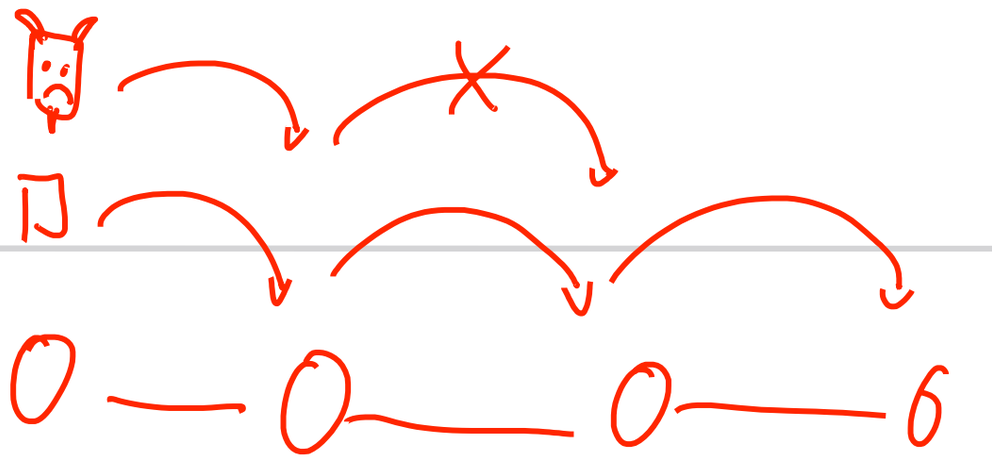
4. Die Vermittlungsschicht

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

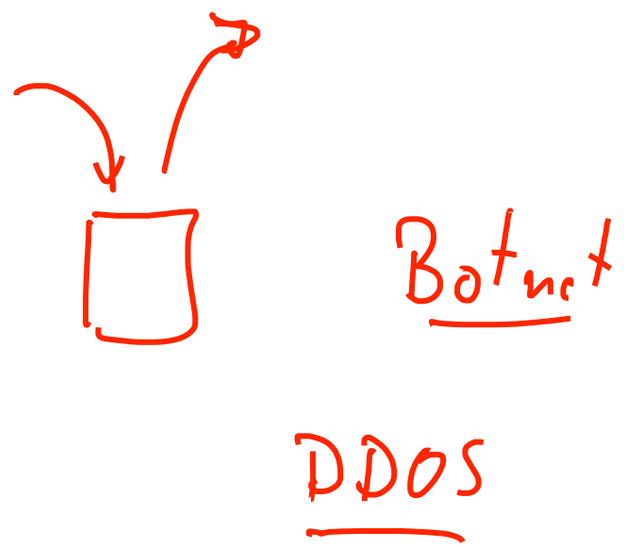
Version 07.06.2016

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)

UNI FREIBURG

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

CoNe Freiburg

Firewalls: Begriffe

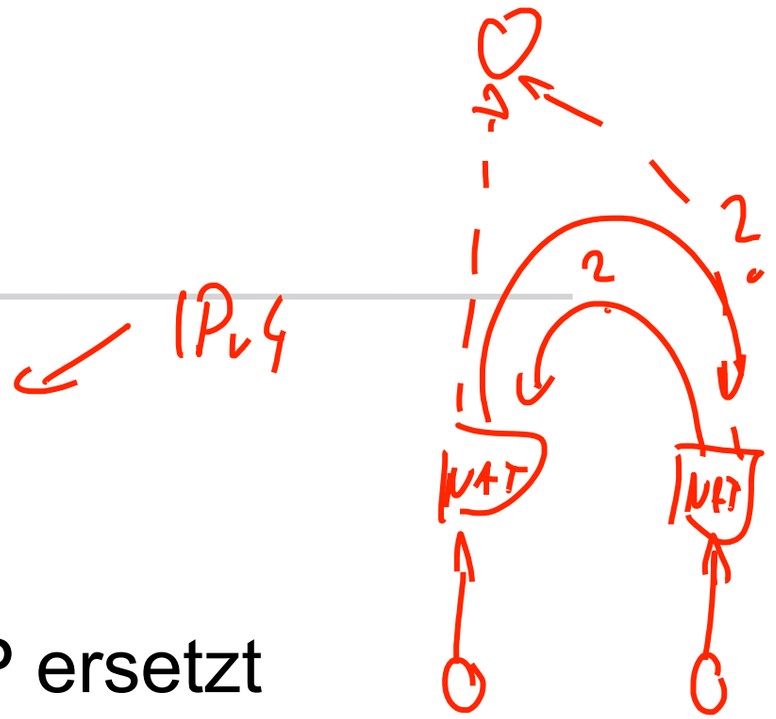
- (Network) Firewall
  - beschränkt den Zugriff auf ein geschütztes Netzwerk aus dem Internet
- Paket-Filter
  - wählen Pakete aus dem Datenfluss in oder aus dem Netzwerk aus
  - Zweck des Eingangsfilter:
    - z.B. Verletzung der Zugriffskontrolle
  - Zweck des Ausgangsfilter:
    - z.B. Trojaner
- 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)

Honey Pot

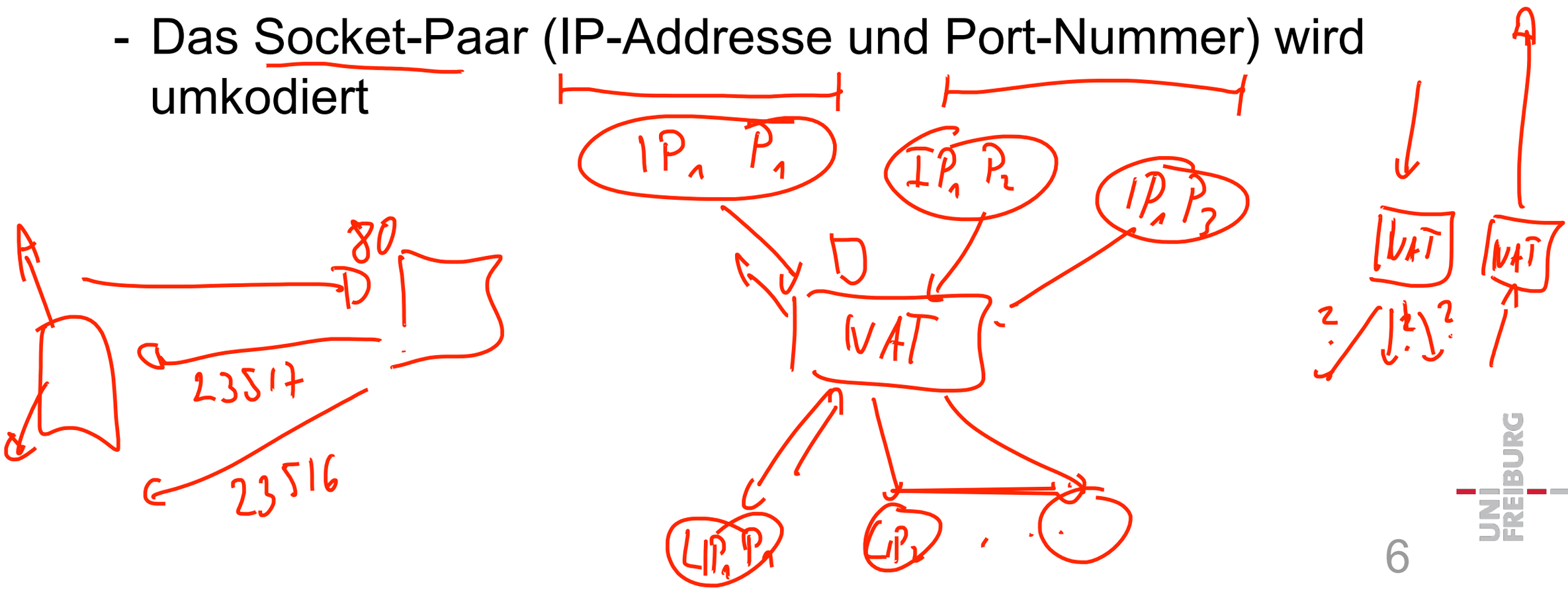
Firewalls: Begriffe

- 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)

NAT und PAT

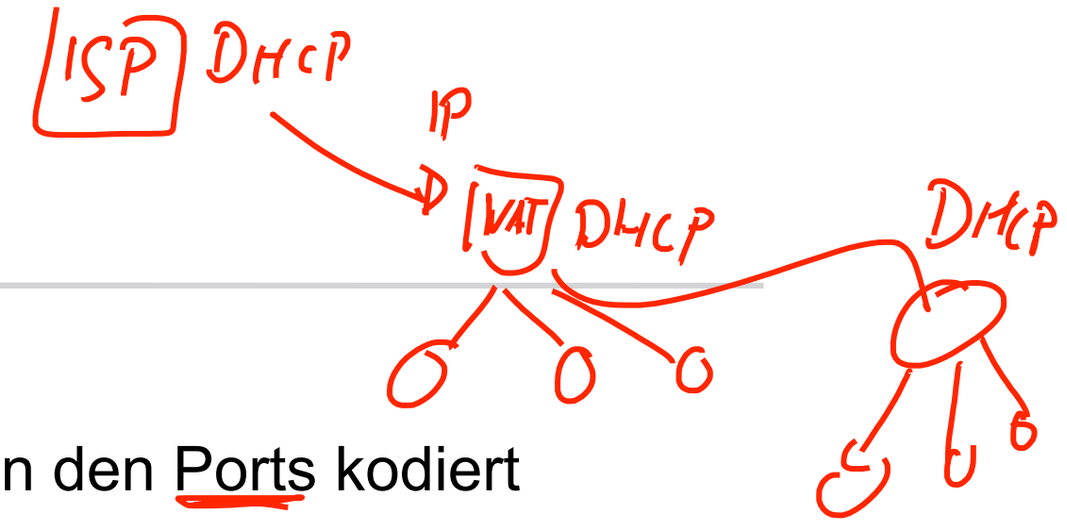


- NAT (Network Address Translation)
- Basic NAT (Static NAT)
  - Jede interne IP wird durch eine externe IP ersetzt
- Hiding NAT = PAT (Port Address Translation) = NAPT (Network Address Port Translation)
  - Das Socket-Paar (IP-Addresse und Port-Nummer) wird umkodiert



CoNe Freiburg

NAT und PAT

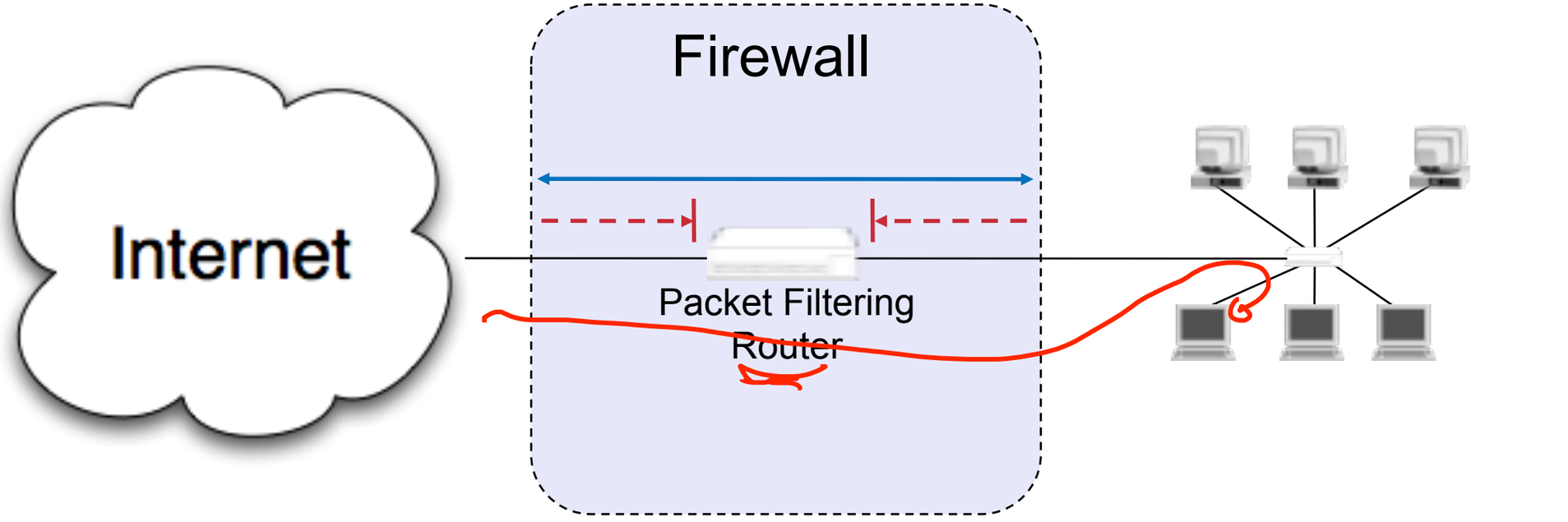


- Verfahren
  - Die verschiedenen lokalen Rechner werden in den Ports kodiert
  - Diese werden im Router an der Verbindung zum WAN dann geeignet kodiert
  - Bei ausgehenden Paketen wird die LAN-IP-Adresse und ein kodierter Port als Quelle angegeben
  - Bei eingehenden Paketen (mit der LAN-IP-Adresse 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
    - NAT nicht üblich für IPv6
  - Lokale Rechner können nicht als Server dienen
- DHCP (Dynamic Host Configuration Protocol)
  - bringt ähnliche Vorteile

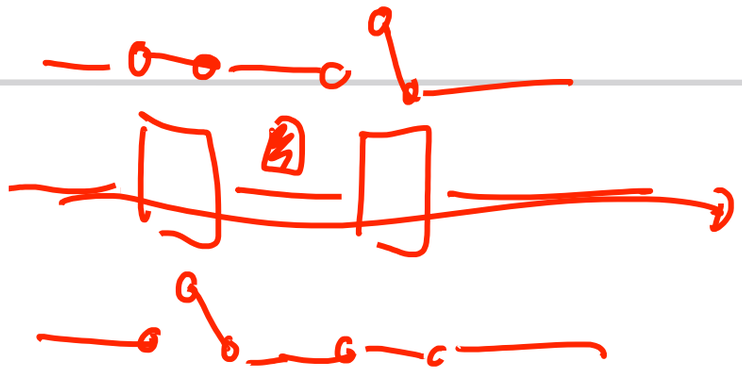
UNI FREIBURG

Firewall-Architektur Einfacher Paketfilter

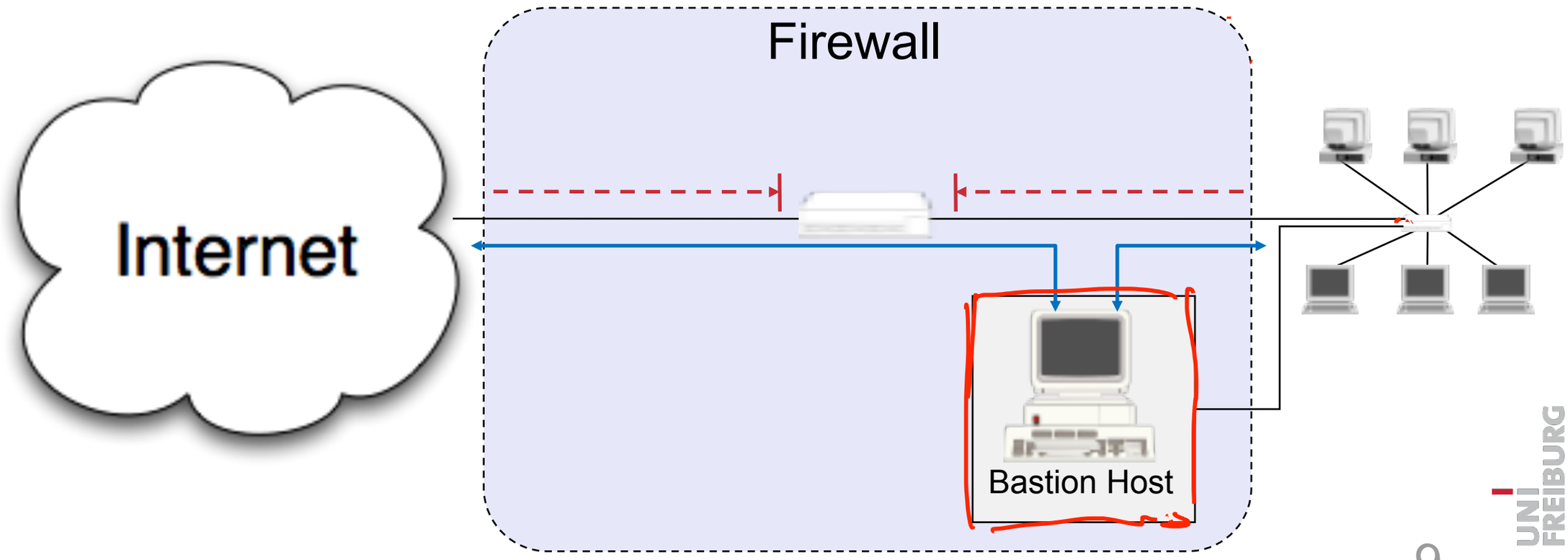
- Realisiert durch
  - Eine Standard-Workstation (e.g. Linux PC) mit zwei Netzwerk-Interfaces und Filter-Software oder
  - Spezielles Router-Gerät mit Filterfähigkeiten



Firewall-Architektur Screened Host



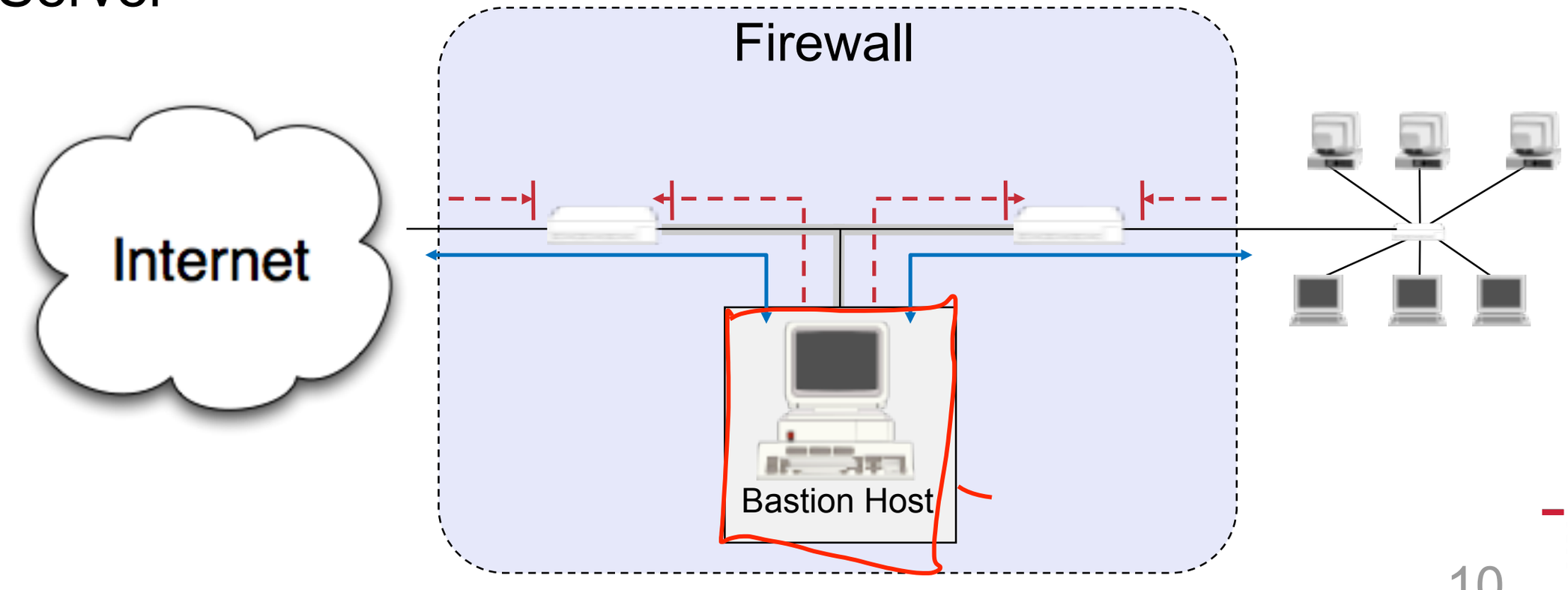
- Screened Host
- Der Paketfilter
  - erlaubt nur Verkehr zwischen Internet und dem Bastion Host und
  - Bastion Host und geschützten Netzwerk
- Der Screened Host bietet sich als Proxy an
  - Der Proxy Host hat die Fähigkeiten selbst Angriffe abzuwehren



CoNe Freiburg

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. [illegible], oder WWW-Server

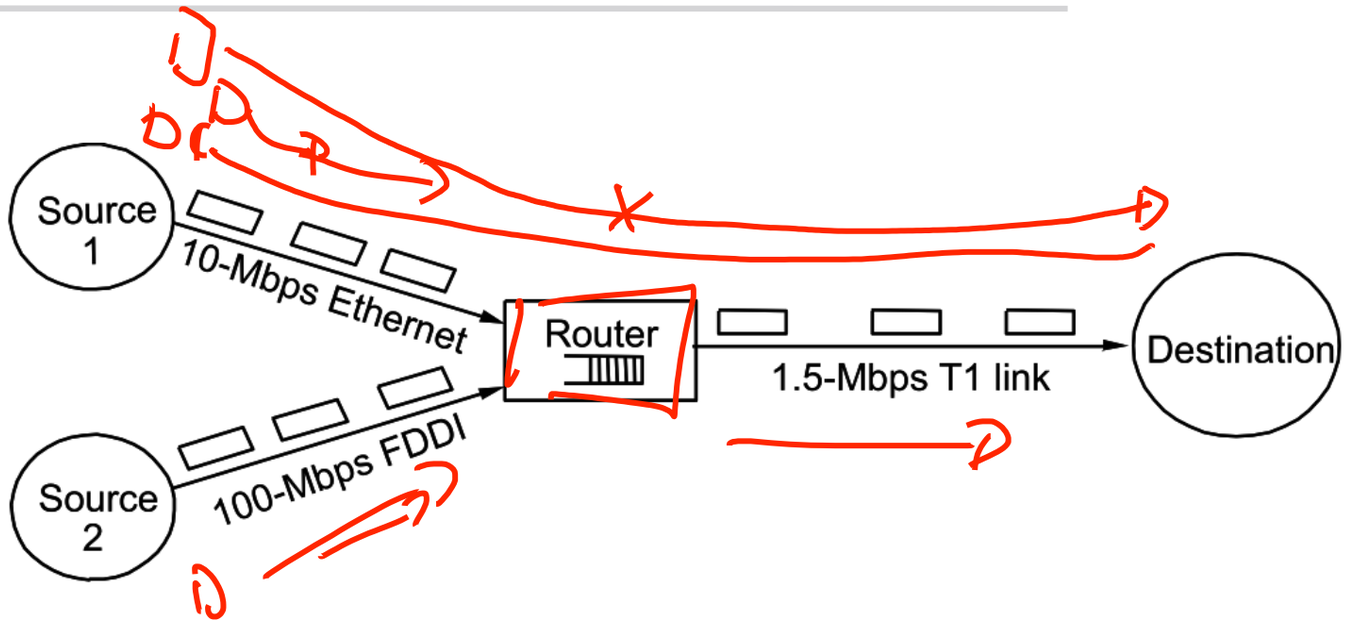


Firewall und Paketfilter

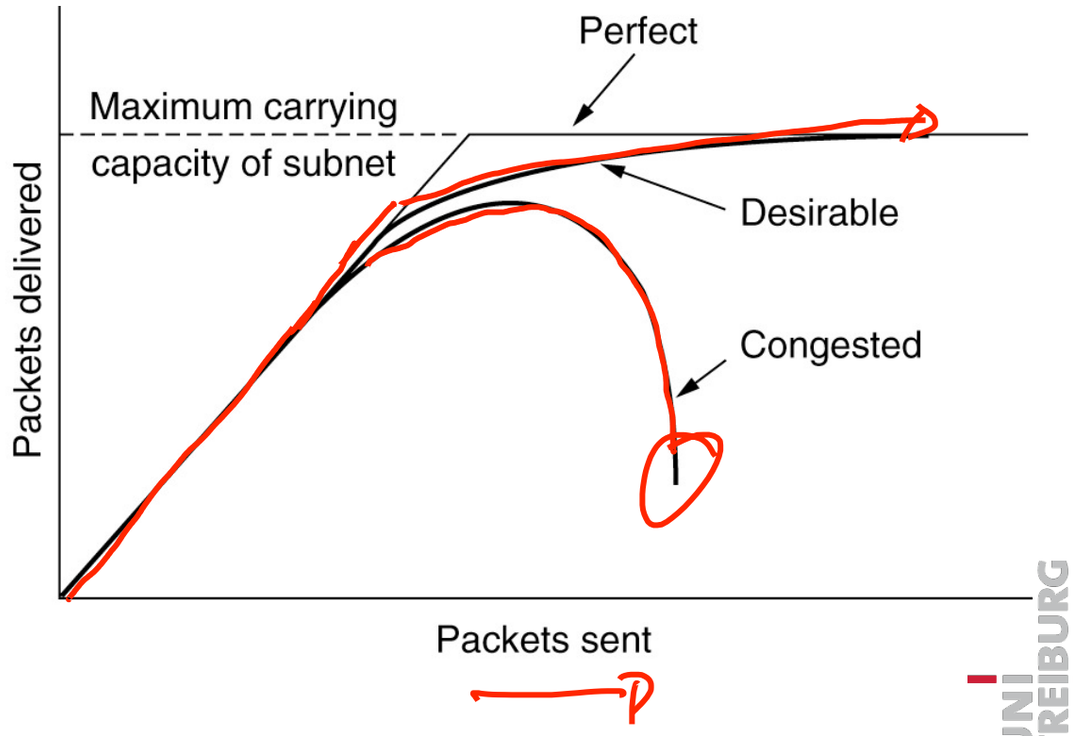
- Fähigkeiten von Paketfilter
  - Erkennung von Typ möglich (Demultiplexing-Information)
- Verkehrskontrolle durch
  - Source IP Address
  - Destination IP Address
  - Transport protocol
  - Source/destination application port
- Grenzen von Paketfiltern (und Firewalls)
  - Tunnel-Algorithmen sind aber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

Congestion Control
Stauvermeidung

- 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

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

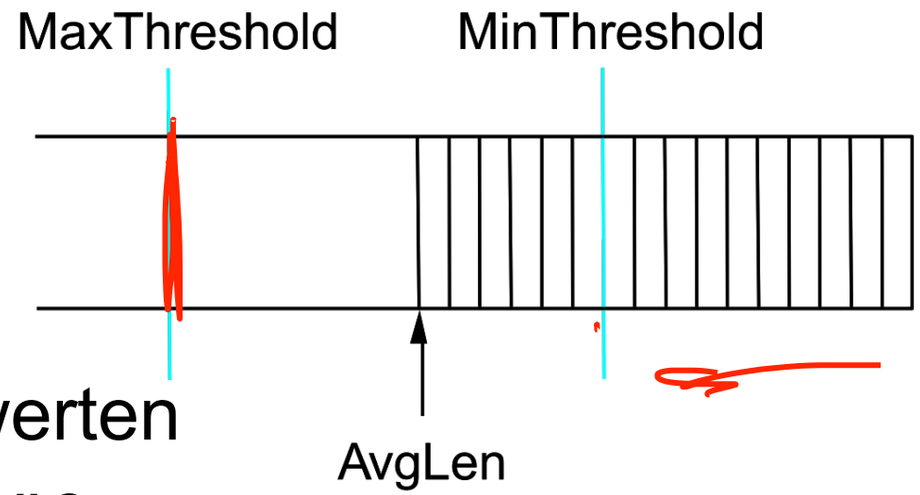
Paketverlust erzeugt implizites Feedback

- 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

Proaktive Methoden

Random Early Detect.

- 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 kontinuierlich mehr Verkehr eingeht als ausgeliefert werden kann
- ...
- Router ist dann in einem Warn-Zustand

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

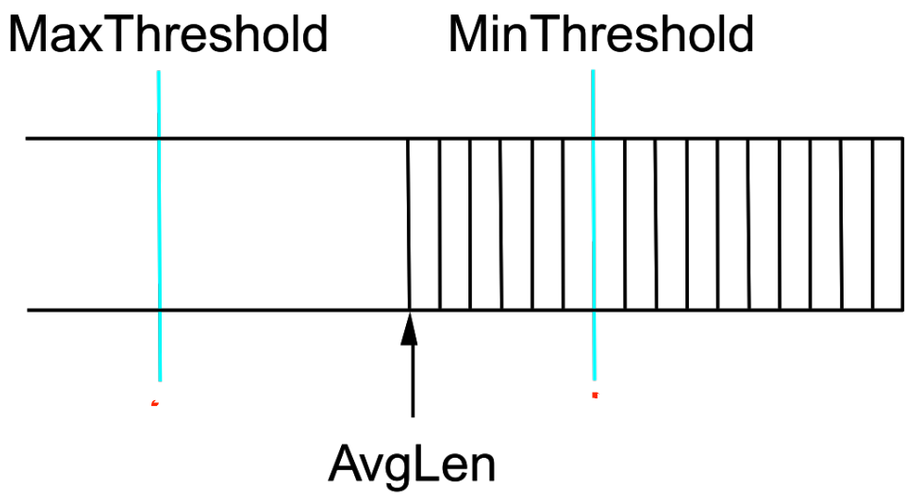
Proaktive Aktion: Warnbits

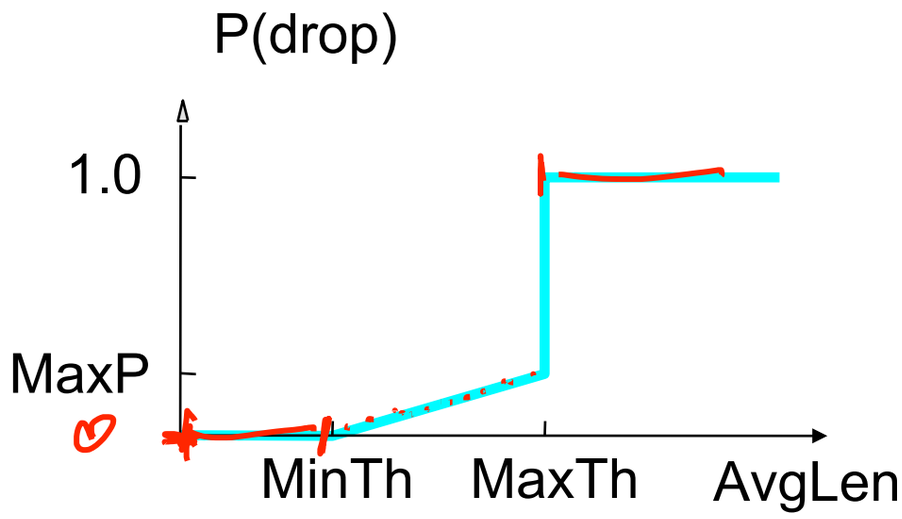
- Wenn der Router in dem Warnzustand ist:
  - Sendet er Warn-Bits in allen Paketen zum Ziel-Host

- Ziel-Host sendet diese Warn-Bits in den Bestätigungs-Bits zurück zum Sender
  - Quelle erhält Warnung und reduziert Sende-Rate

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

5. Die Transportschicht

Christian Schindelhauer
Technische Fakultät
Rechnernetze und Telematik
Albert-Ludwigs-Universität Freiburg
Version 15.06.2016

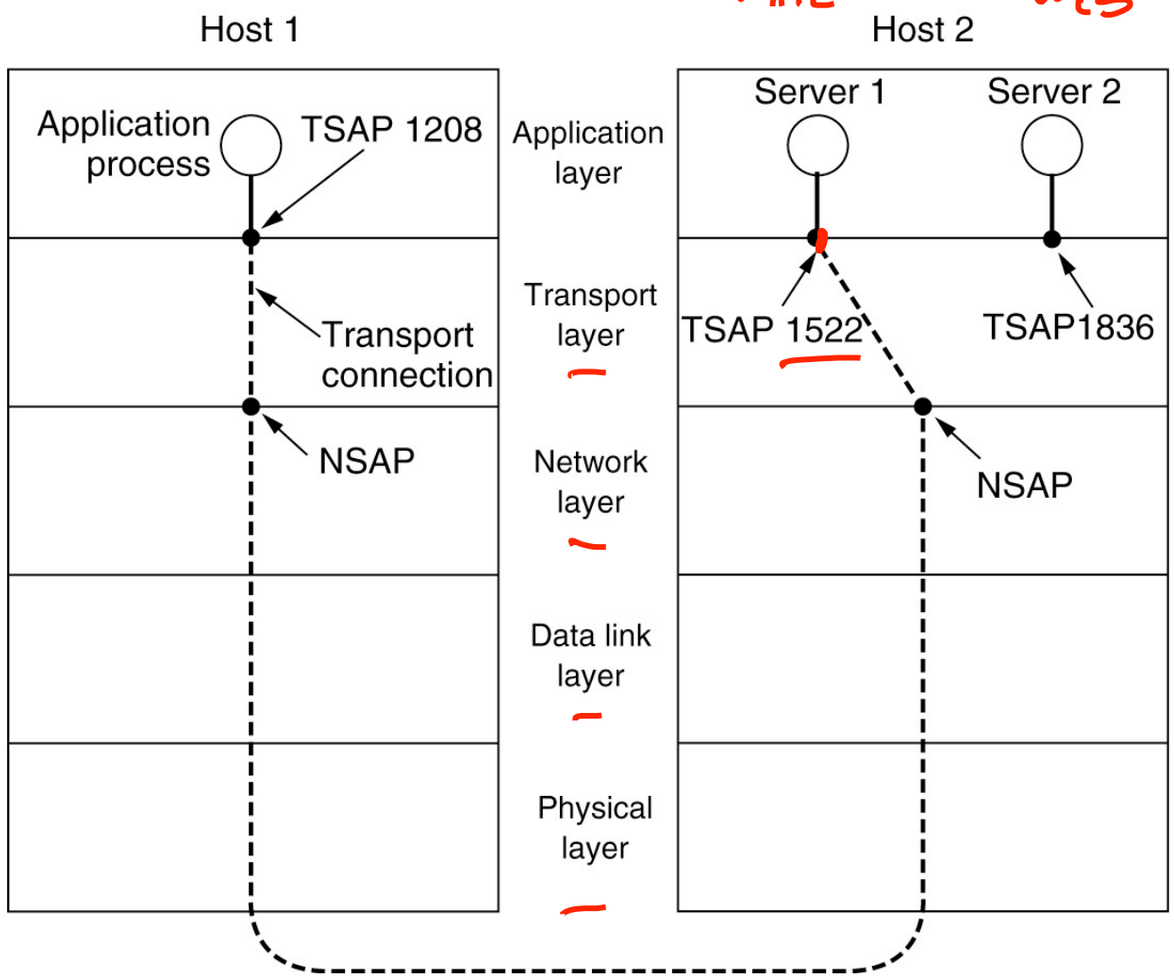
UNI FREIBURG

Dienste der Transportschicht

- Verbindungslos oder Verbindungsorientert
  - Beachte: Sitzungsschicht im ISO/OSI-Protokoll
- Zuverlässig oder unzuverlässig
  - 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“

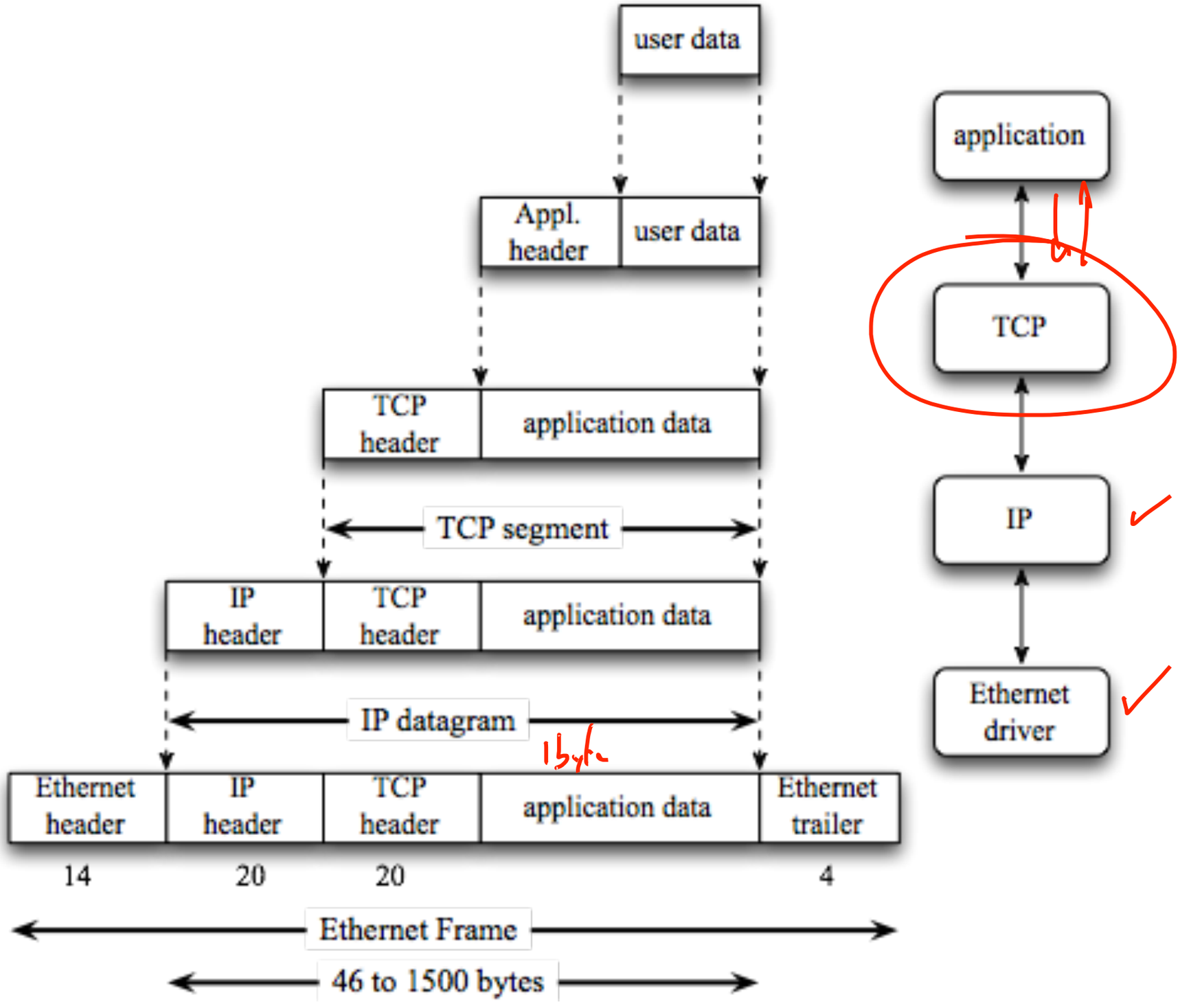
Multiplex in der Transportschicht

- 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



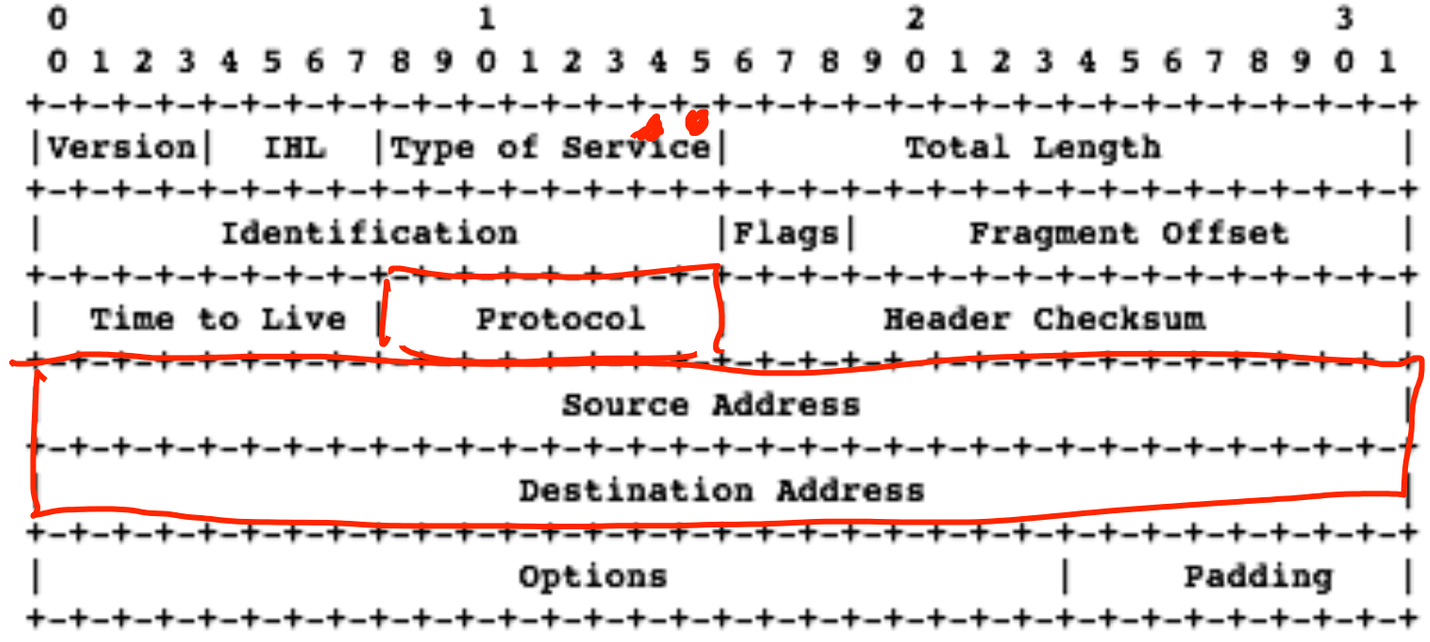
CoNe Freiburg

Datenkapselung



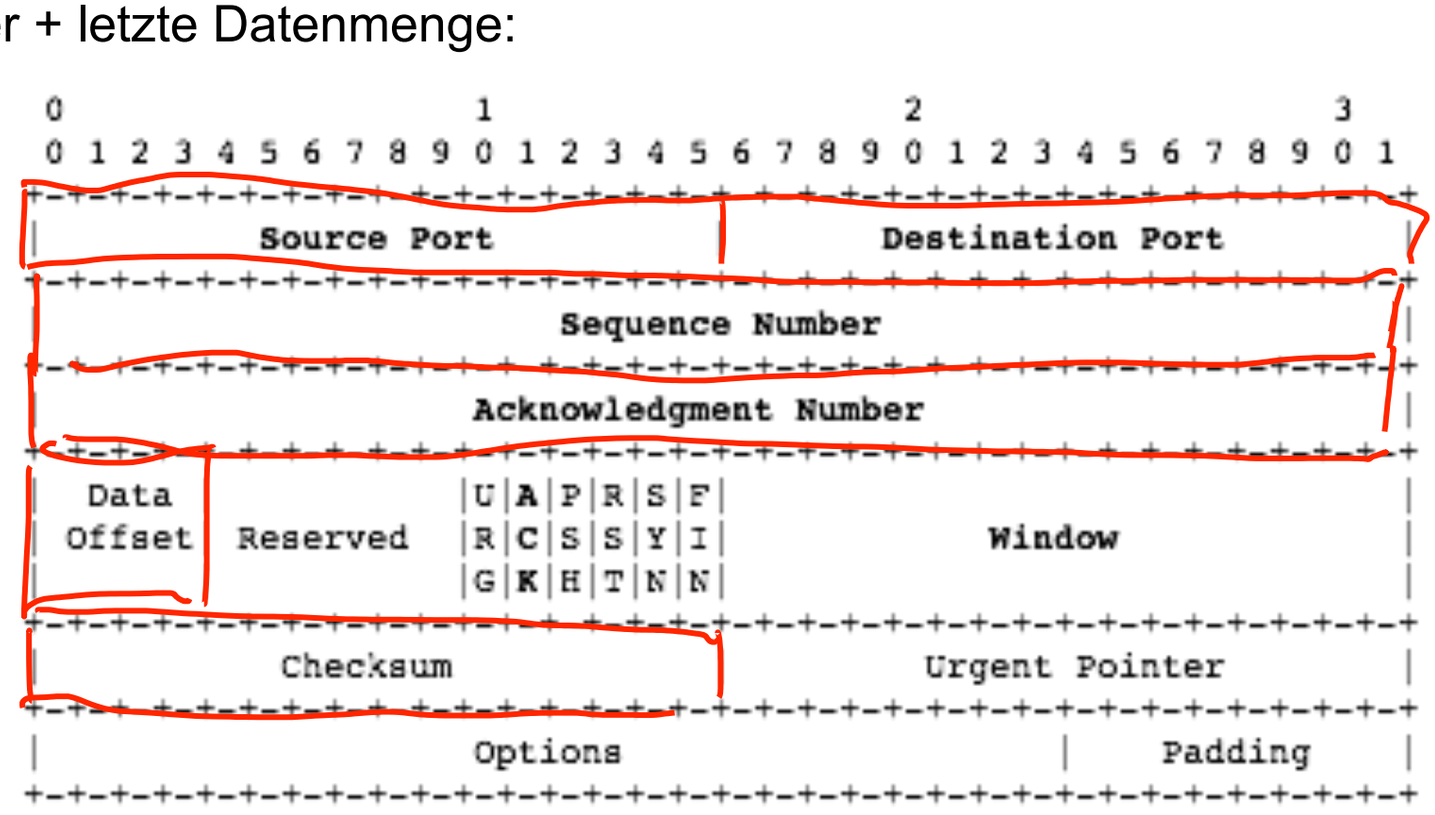
IP-Header (RFC 791)

- 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

- 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:
- Port-Adressen
  - Für parallele TCP-Verbindungen
  - Ziel-Port-Nr.
  - Absender-Port
- Headerlänge
  - data offset
- Prüfsumme
  - Für Header und Daten



CoNe Freiburg

Transportschicht (transport layer)

- 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