Grundlagen TCP/IP

C3D2 – Chaostreff Dresden

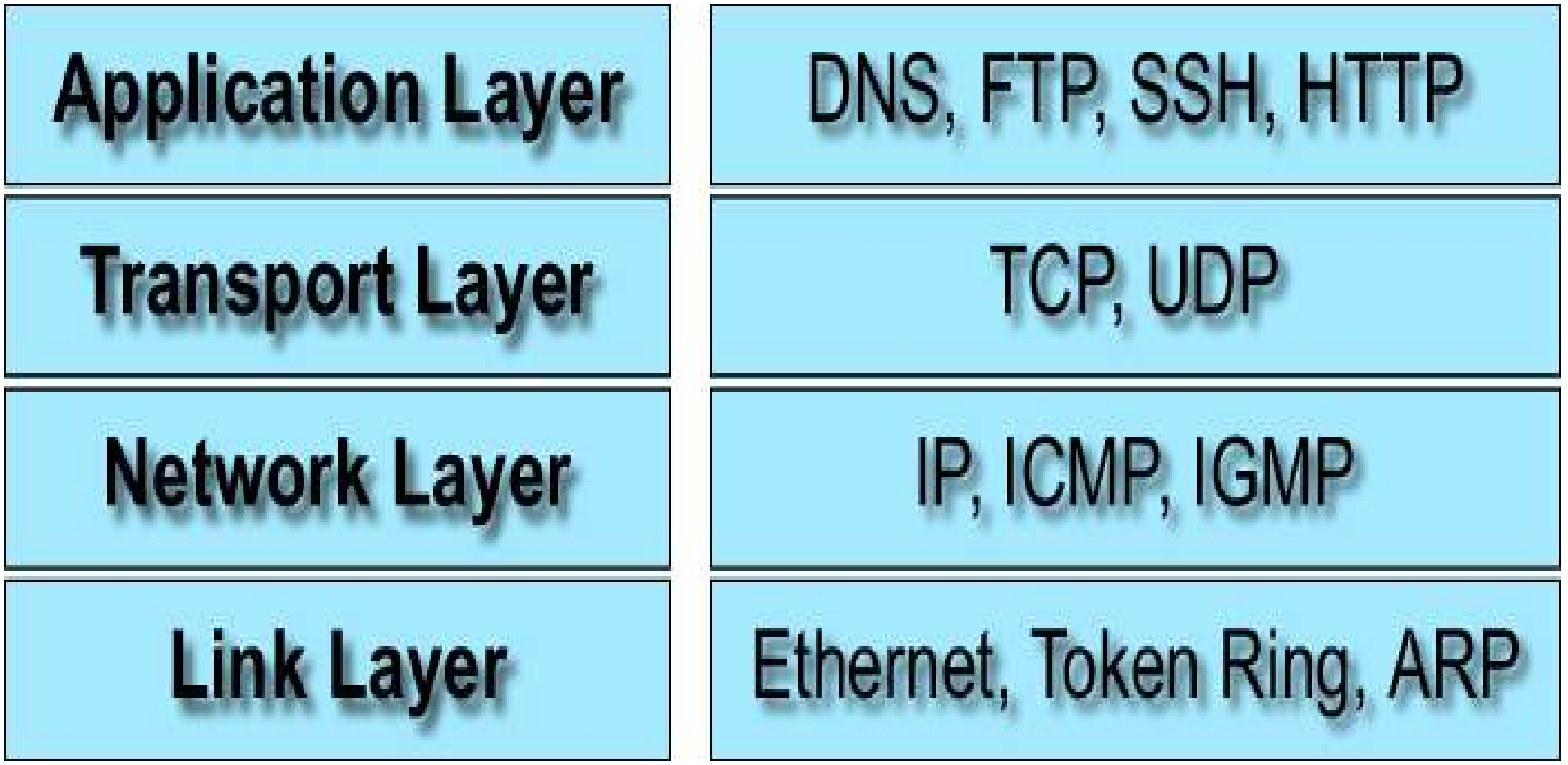
Sven Klemm
sven@elektro-klemm.de

Gliederung

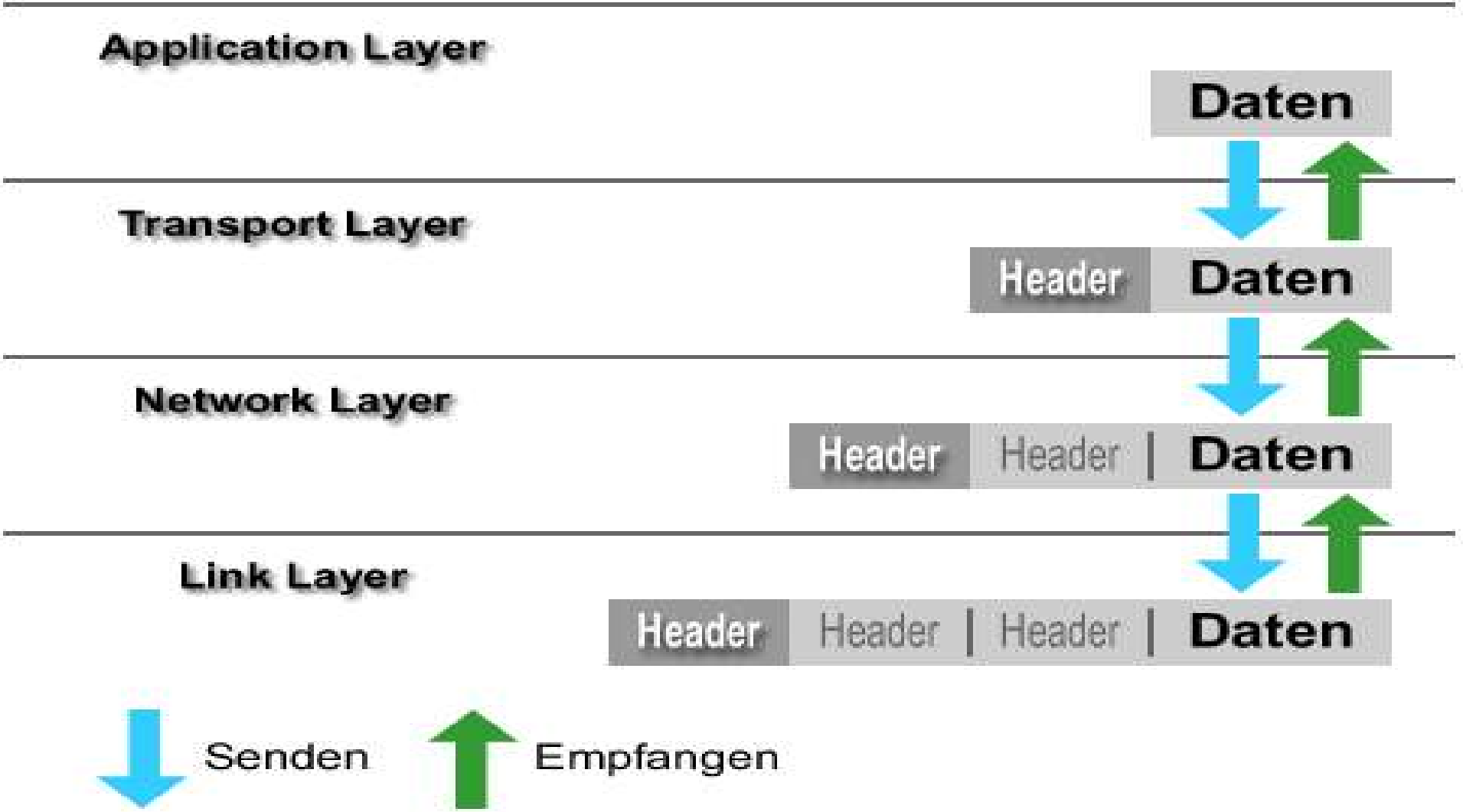
- TCP/IP
  - Schichtenmodell / Kapselung
- ARP
  - Spoofing
  - Relaying
- IP
- ICMP
  - Redirection
- UDP
- TCP

Schichtenmodell

Protokolle der Schichten



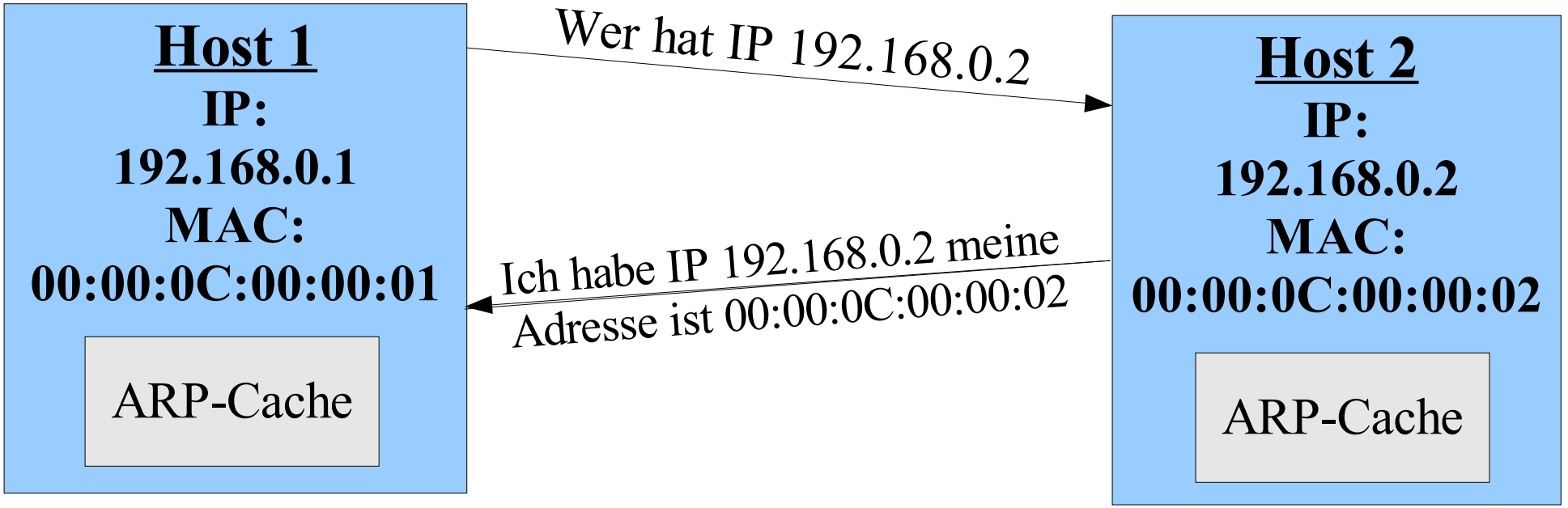
Kapselung


Application Layer
Daten
Transport Layer
Header
Daten
Network Layer
Header
Header
Daten
Link Layer
Header
Header
Header
Daten
Senden
Empfangen

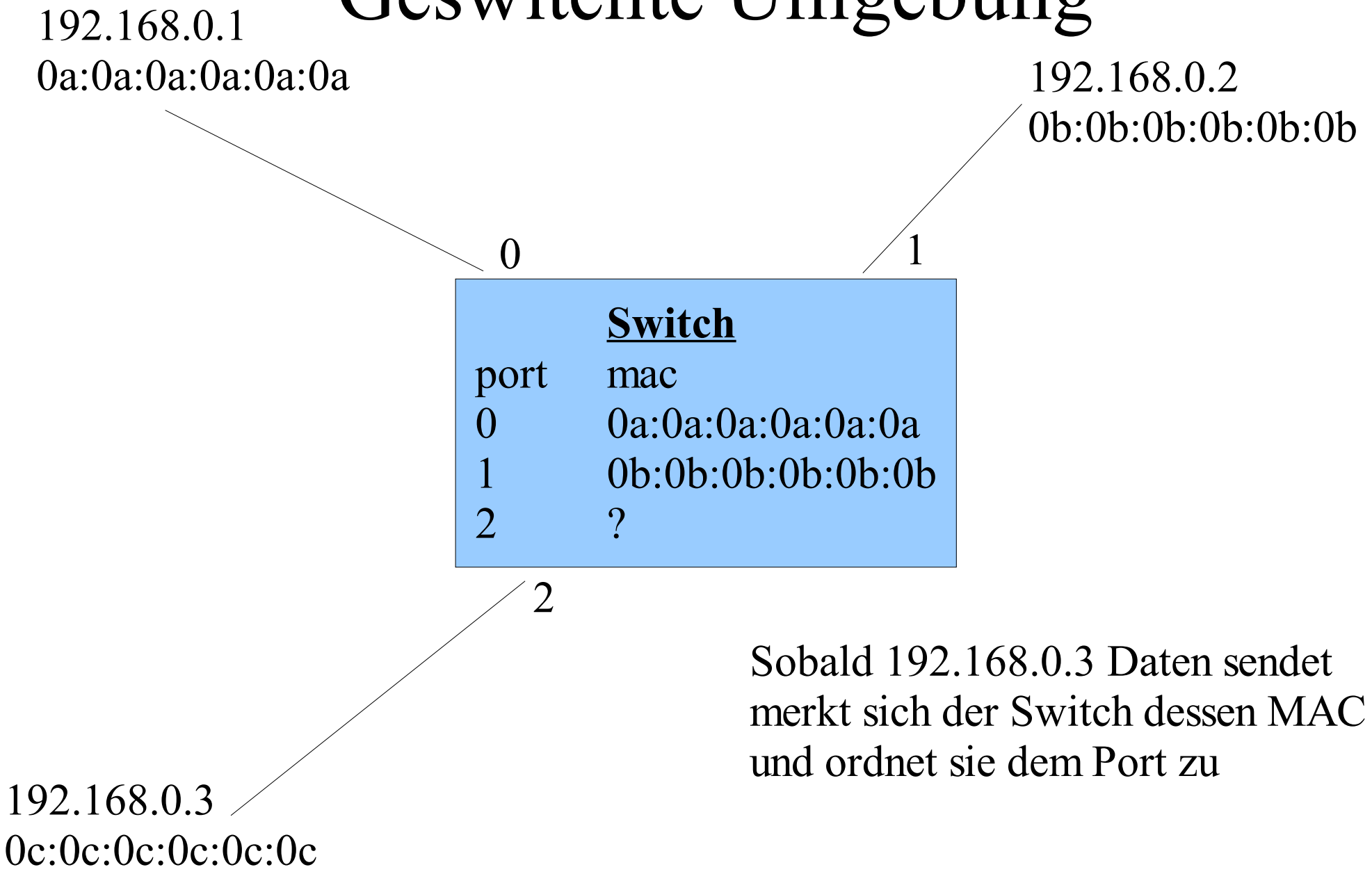
ARP – Address Resolution Protocol

- Auflösung von IP-Adressen in Hardwareadressen
- Identifizierung der Netzwerkadapter über MAC-Adressen (Media Acess Control)
- Ethernet-Adressen (48 Bit) sind weltweit eindeutig in der Hardware gespeichert
- ARP-Anfrage: Broadcast
- ARP-Antwort: Unicast

ARP


Host 1
IP:
192.168.0.1
MAC:
00:00:0C:00:00:01
ARP-Cache
Wer hat IP 192.168.0.2
Ich habe IP 192.168.0.2 meine
Adresse ist 00:00:0C:00:00:02
Host 2
IP:
192.168.0.2
MAC:
00:00:0C:00:00:02
ARP-Cache

Geswitchte Umgebung

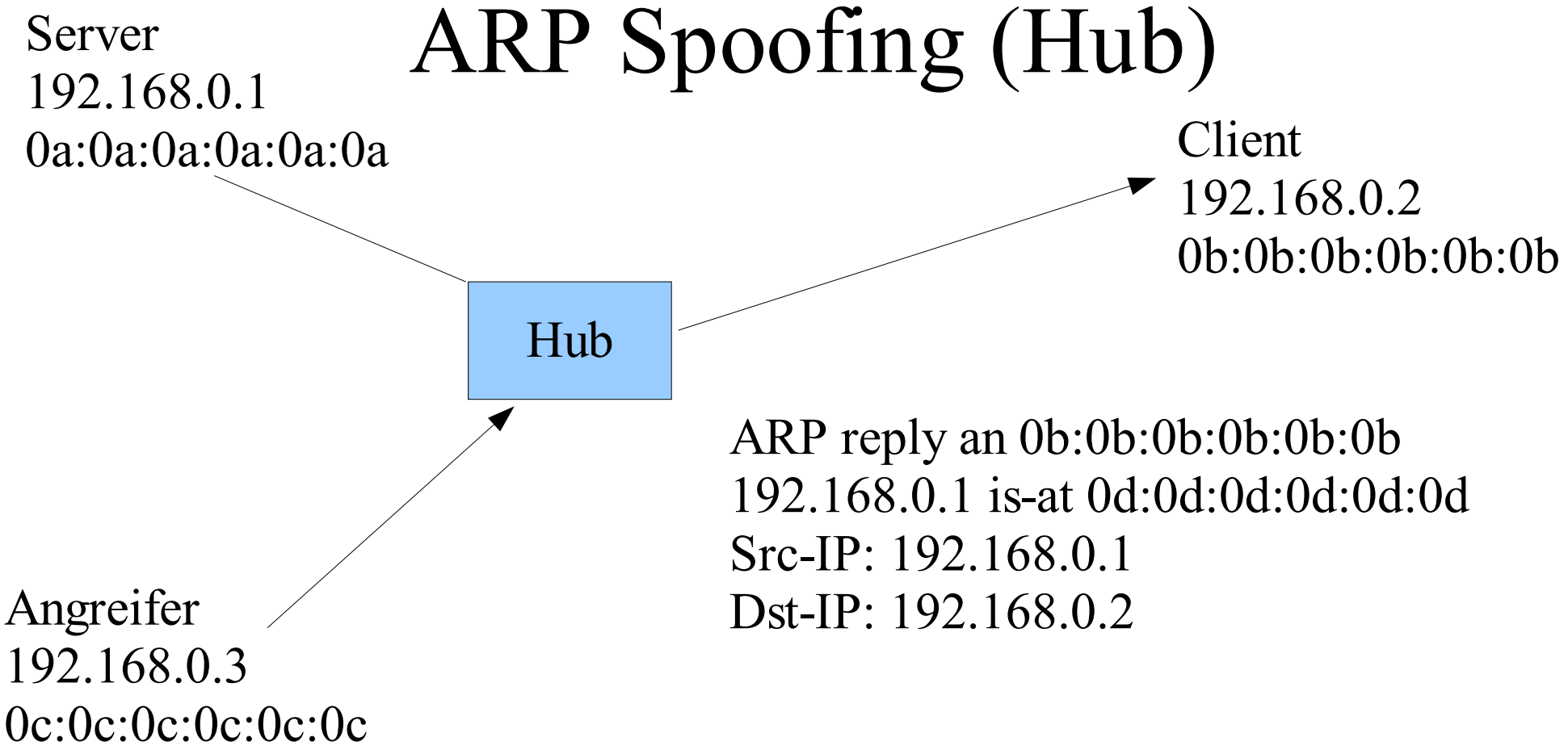


Sobald 192.168.0.3 Daten sendet merkt sich der Switch dessen MAC und ordnet sie dem Port zu

ARP Spoofing

- Übernahme einer strategisch wichtigen Position
- Stören einer bestehenden Verbindung
- z.B.: - arpspoof
  - spak
  - packit
  - hunt

ARP Spoofing (Hub)



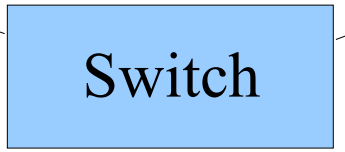
<u>Angreifer will Client vom Server abklemmen</u>

- 192.168.0.3 generiert gefälschte ARP-Antwort
- 192.168.0.2 ändert den Eintrag für 192.168.0.1 in seinem ARP-Cache

ARP-Relaying

Server
192.168.0.1
0a:0a:0a:0a:0a:0a

Client
192.168.0.2
0b:0b:0b:0b:0b:0b



ARP reply an 0a:0a:0a:0a:0a:0a
192.168.0.2 is-at 0c:0c:0c:0c:0c:0c
Src-IP: 192.168.0.2
Dst-IP: 192.168.0.1

ARP reply an 0b:0b:0b:0b:0b:0b
192.168.0.1 is-at 0c:0c:0c:0c:0c:0c
Src-IP: 192.168.0.1
Dst-IP: 192.168.0.2

Angreifer
192.168.0.3
0c:0c:0c:0c:0c:0c

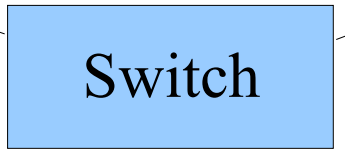
<u>Angreifer will Pakete über sich umleiten</u>

- Alle Pakete kommen bei 192.168.0.3 an
- 192.168.0.3 muß Pakete weitervermitteln

ARP-Relaying 2

Server
192.168.0.1
0a:0a:0a:0a:0a:0a

Client
192.168.0.2
0b:0b:0b:0b:0b:0b



ARP reply an 0a:0a:0a:0a:0a:0a
192.168.0.2 is-at 0d:0d:0d:0d:0d:0d
Src-IP: 192.168.0.2
Dst-IP: 192.168.0.1

ARP reply an 0b:0b:0b:0b:0b:0b
192.168.0.1 is-at 0e:0e:0e:0e:0e:0e
Src-IP: 192.168.0.1
Dst-IP: 192.168.0.2

Angreifer
192.168.0.3
0c:0c:0c:0c:0c:0c

<u>Angreifer will Client und Server voneinander isolieren</u>

- Switch leitet Frames für Pakete mit unbekannter MAC an alle Ports weiter
- Das Paket wird überall verworfen

IP – Internet Protocol

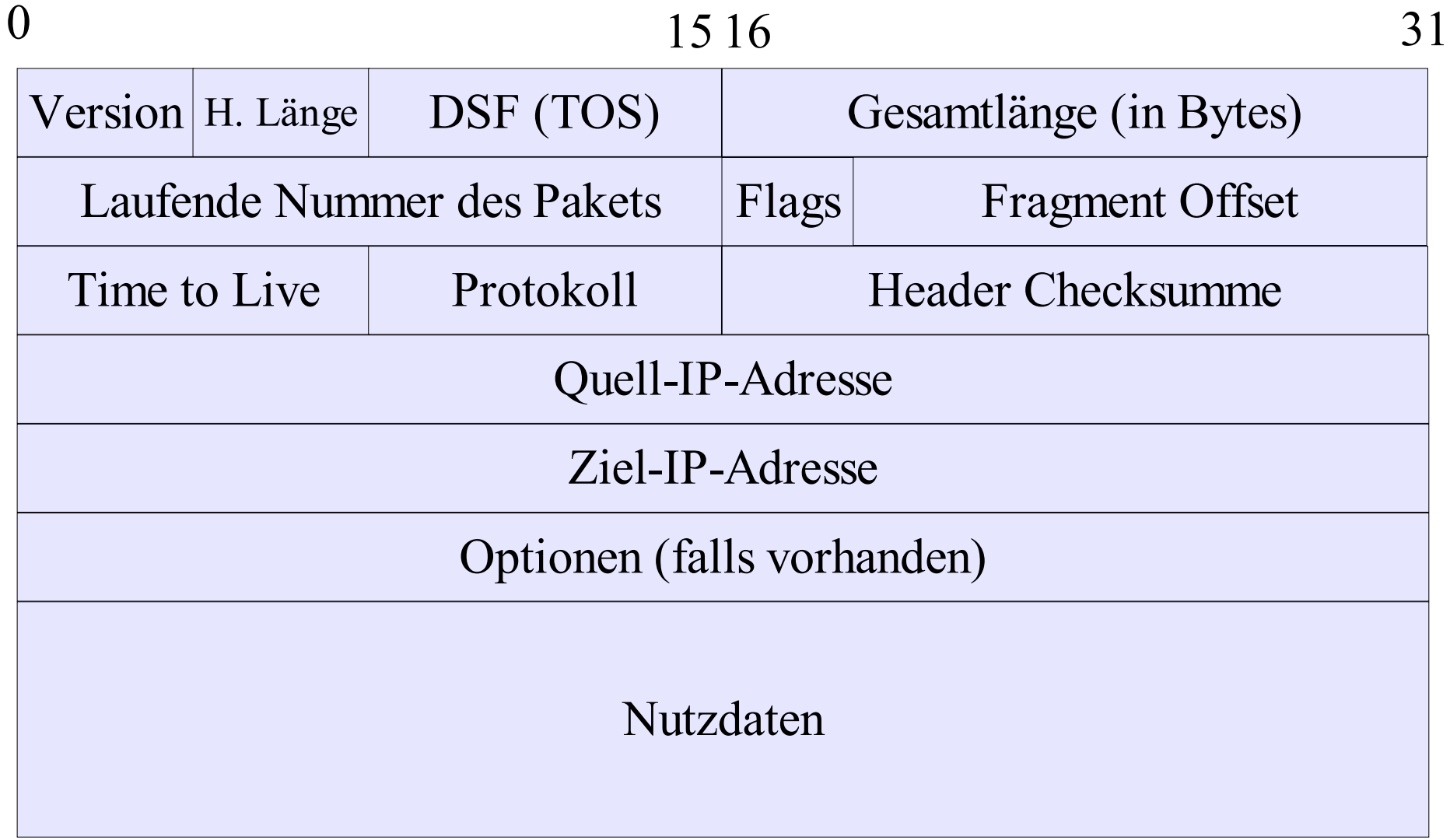
- Paketvermittelnd
- Verbindungslos
- Ungesichert
- „best effort“, keine Garantie
- Fragmentierung zu großer Pakete

Adressierung

- 32-Bit-Adressen
- IP-Adresse besteht aus Netz-ID und Host-ID
- Subnetz-Maske kennzeichnet die Netz-ID einer IP-Adresse

IP-Adresse:	192.168. 0.1		
Subnetz-Maske:	255.255.255.0		
Netz-ID:	192.168.0.0	=	192.168.0.0/24
Host-ID:	0.0.0.1		

IP - Paketaufbau



IP Routing

Wenn Paket nicht für lokales Interface:

- Durchsuchen der Routing-Tabelle:
  1. nach der Ziel-IP-Adresse
  2. nach der Netz-ID der Ziel-Adresse
  3. nach Defaultrouter
- Eintragen der MAC-Adresse des Routers als Ziel-MAC im Ethernet-Frame

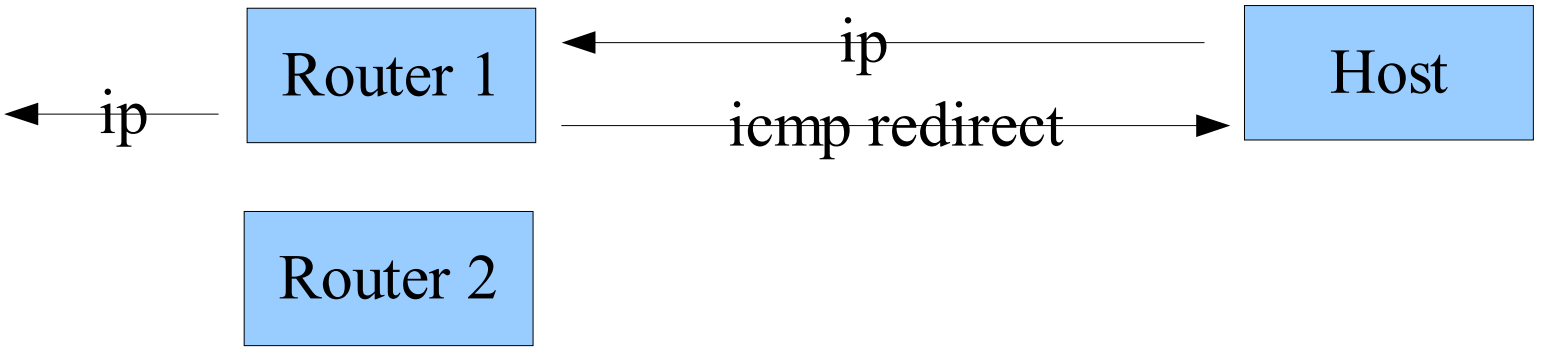
ICMP – Internet Control Message Protocol

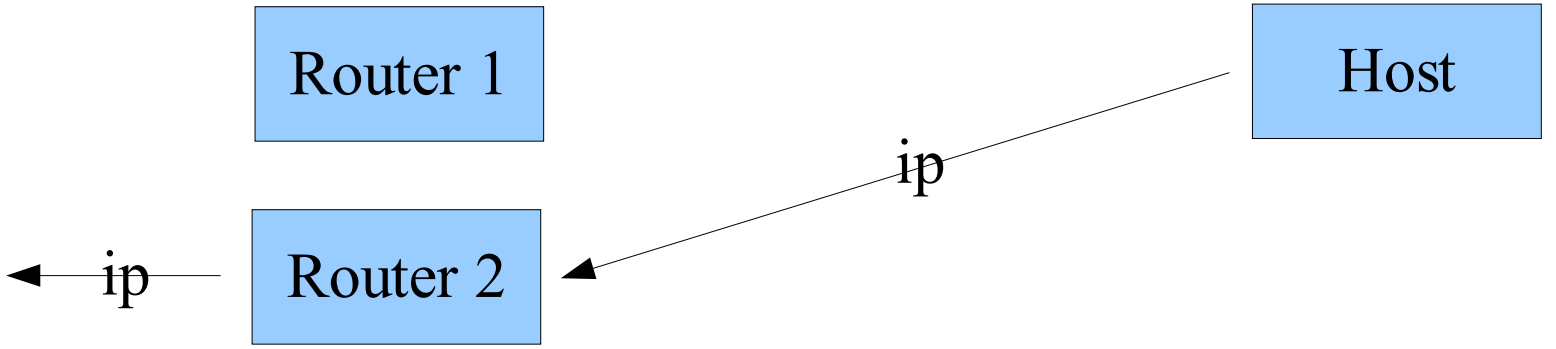
- Für Status- und Fehlermeldungen
- Versand erfolgt in IP-Paket
- z.B.:
  - Destination unreachable
  - Source quench
  - Redirect
  - Timestamp
  - Echo request/reply (ping)

ICMP Redirection

- Nachricht von Routern an Hosts, das Pakete für ein bestimmtes Ziel besser über einen anderen Router verschickt werden sollen
- Host ändert daraufhin seine Routingtabelle
- Die Routen verfallen nicht (im Gegensatz zu ARP-Cache)
- Nur Hosts die keine Router sind nehmen ICMP-redirects an

ICMP Redirection

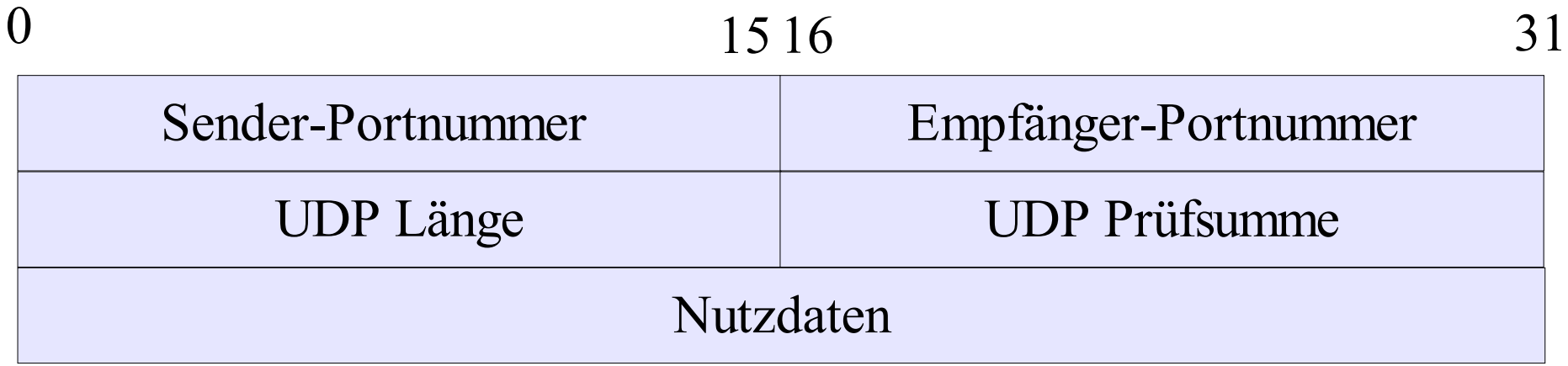




UDP – User Datagram Protocol

- Verbindunglos
- ungesichert
- Für Multicast geeignet
- Relativ simpel
- DNS, TFTP, SNMP

UDP-Paketaufbau



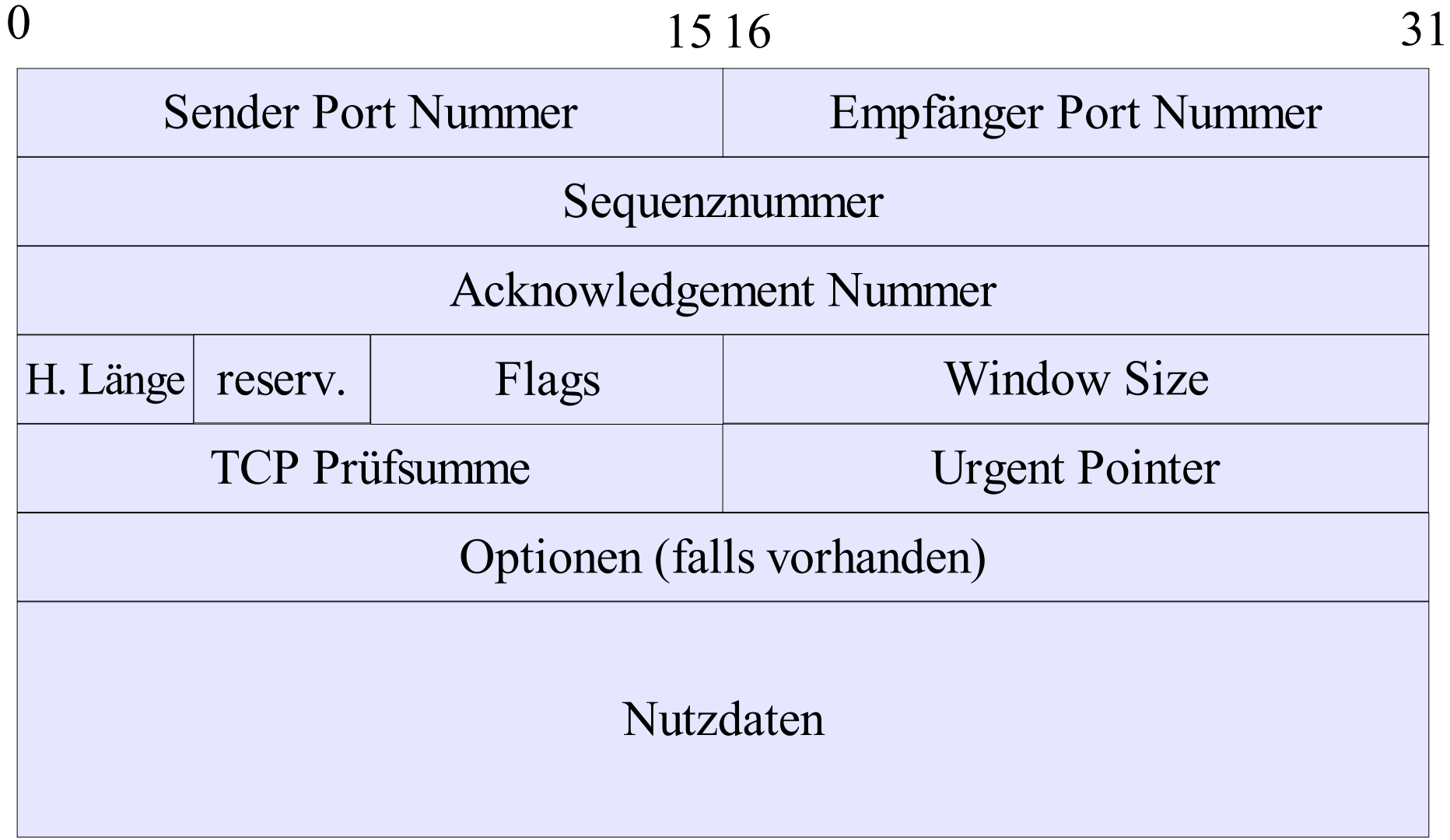
DNS-Spoofing

- Fälschen von Antworten auf eine DNS-Abfrage
- die richtige Antwort vom DNS-Server kommt auch aber meist zu spät
- z.B. mit dnsspoof (bei dsniff enthalten)

TCP – Transmission Control Protocol

- Verbindungsorientiert
- Gesichert
- Kein Multicast
- Komplexer als UDP
- Vermeidung von Überlastung

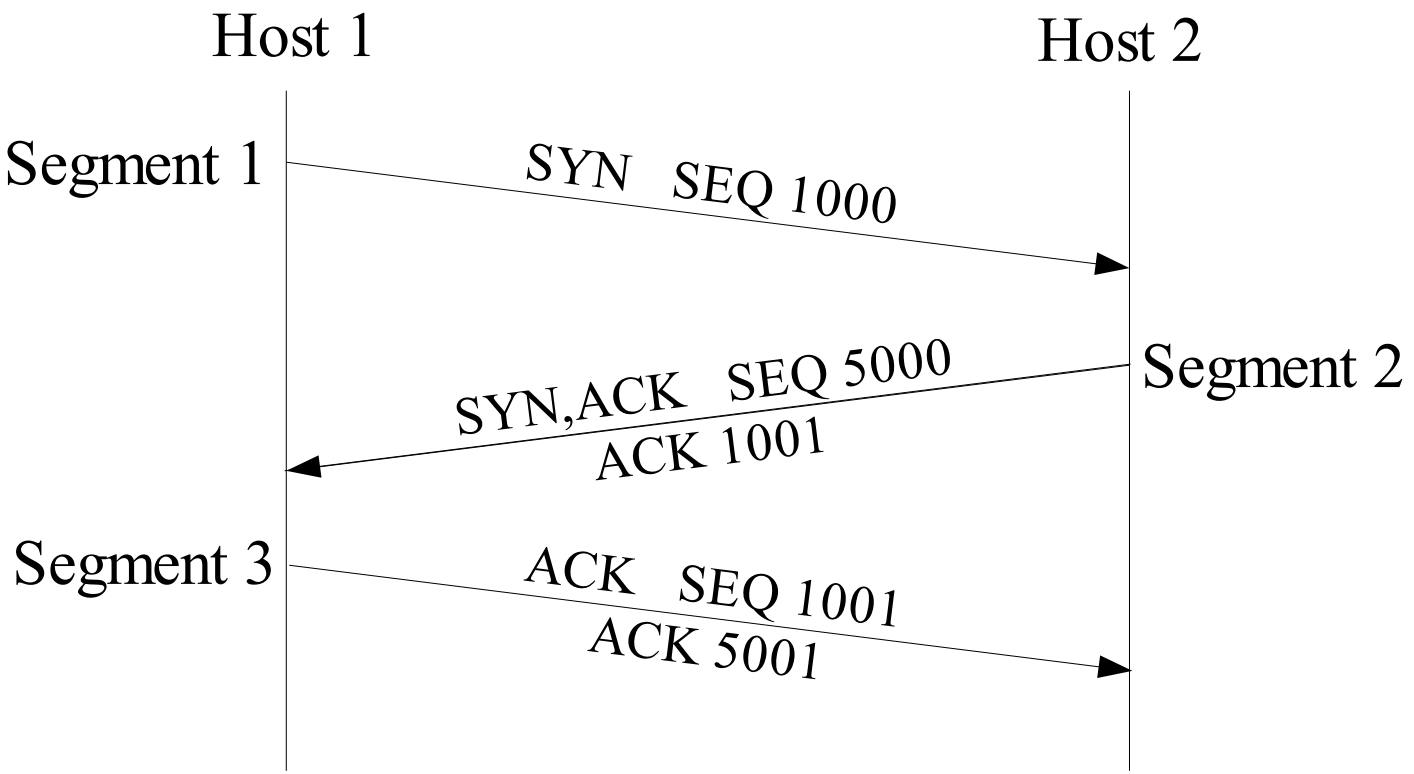
TCP - Paketaufbau



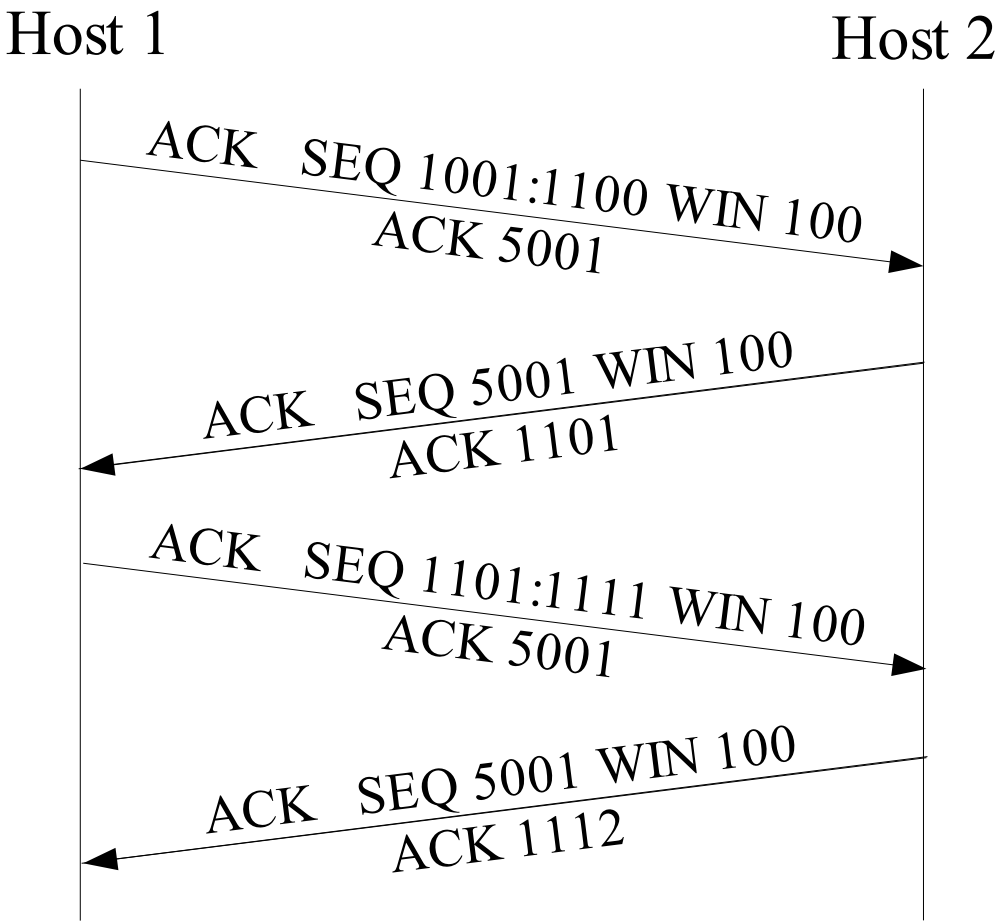
TCP Flags

- CWR: Congestion Window Reduced
- ECE: Explicit Congestion Notification-Echo
- URG: Urgent Pointer ist gültig
- ACK: Acknowledgement Number ist gültig
- PSH: Empfänger soll sofort verarbeiten
- RST: Reset der Verbindung
- SYN: Synchronisiere Sequenznummern (Verbindungsaufbau)
- FIN: keine weiteren Daten zu senden (Verbindungsabbau)

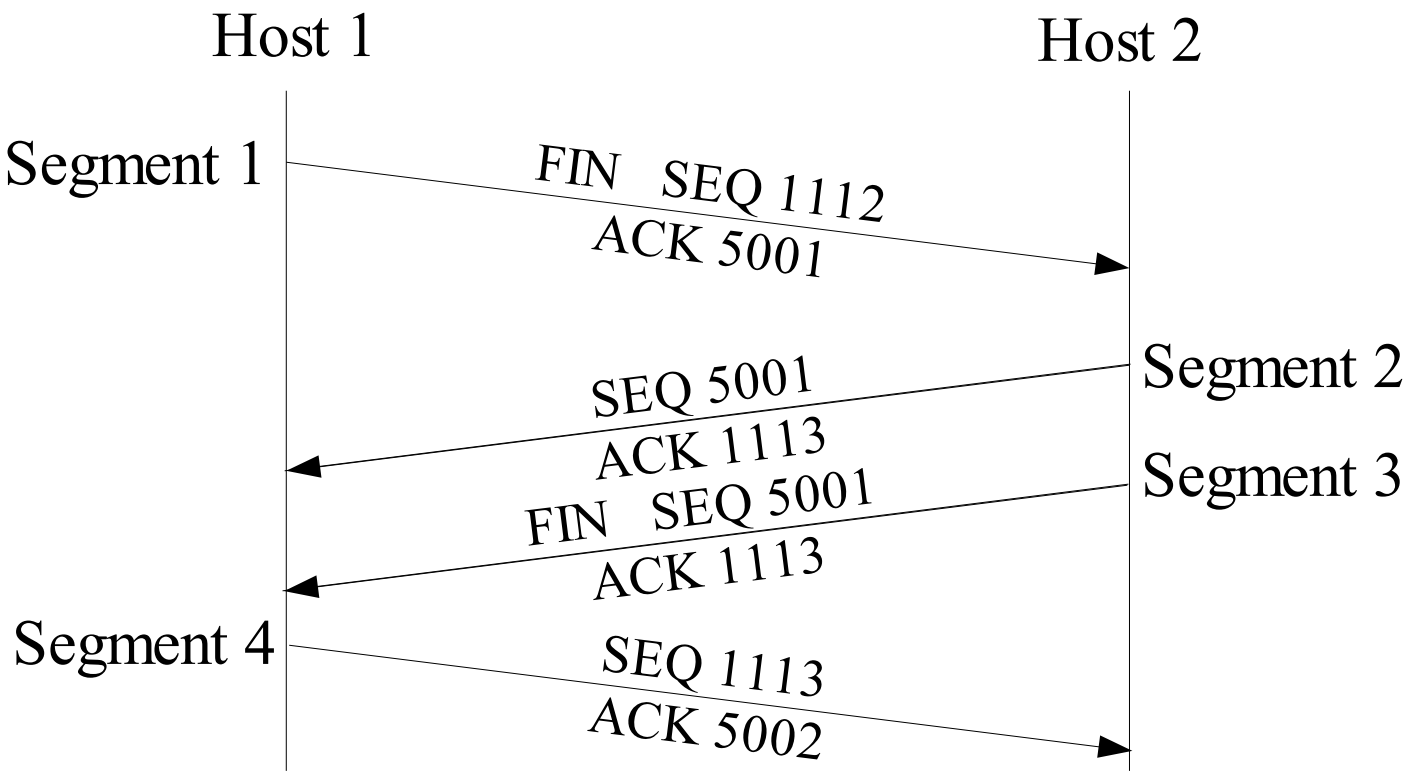
Verbindungsaufbau
Three-way Handshake



TCP Window size



TCP Verbindungsabbau



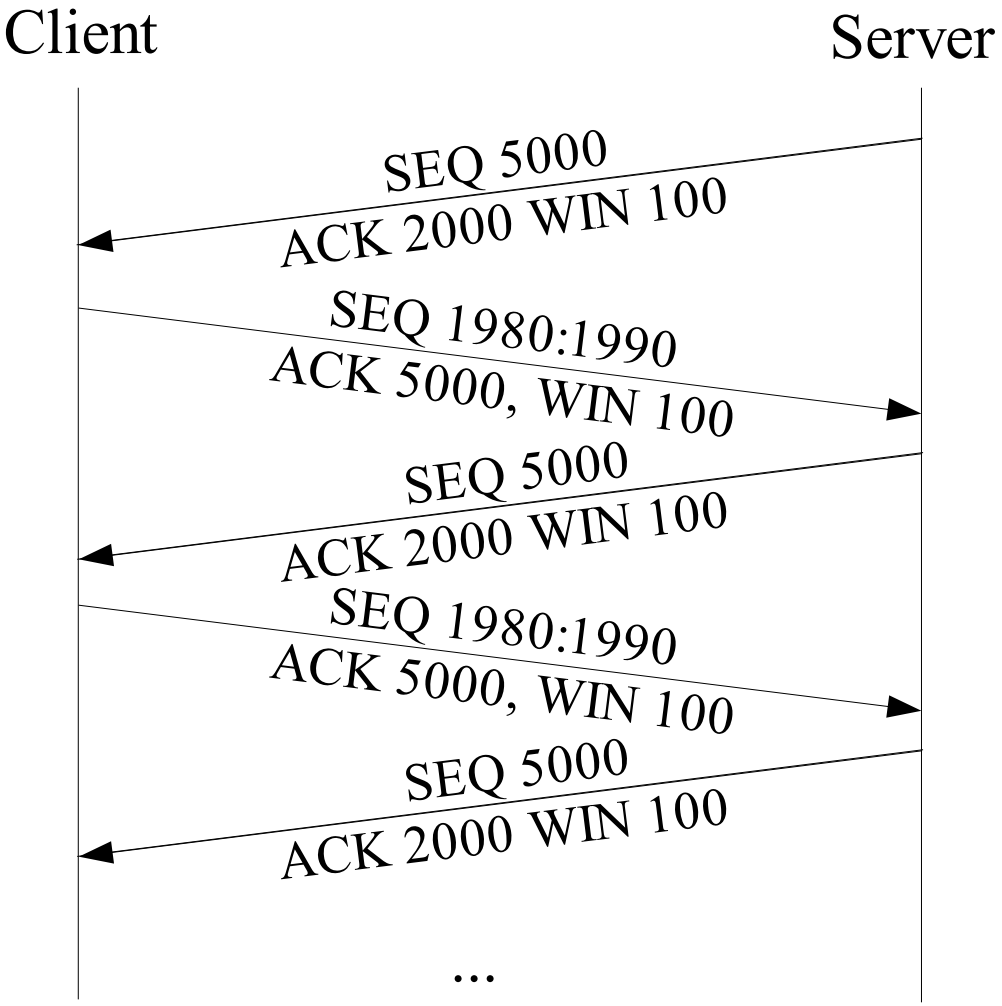
TCP Desynchronized State

- Sequenznummer des Server != ACK des Client
- Sequenznummer des Client != ACK des Server

- Paket wird verworfen wenn:
  - Sequenznr. > ACK + Window Size
  - Sequenznr. < ACK

ACK mit der erwarteten Sequenznummer wird gesendet

TCP Desynchronized State ACK Storm



Übernahme einer Telnet-Session

- Belauschen der Kommunikation um die Sequenznummern zu erhalten
- Abhängen des Client
- mit Paketgenerator Paket erzeugen, dessen Sequenznummer dem letzten ACK des Servers entspricht und dessen ACK dem letzten ACK des Client entspricht

Quellen

- W. Richard Stevens, TCP/IP Illustrated, Volume 1
- Erich Stein, Taschenbuch Rechnernetze und Internet
- Craig Hunt, TCP/IP Network Administration
- RFC 2474, 3168
- http://waptune24.de/krecher/19c3-hijackersguide.pdf
- http://hamburg.ccc.de/bildungswerk/archiv/tcpip_v5/index.html