# TCP/IP Network Security

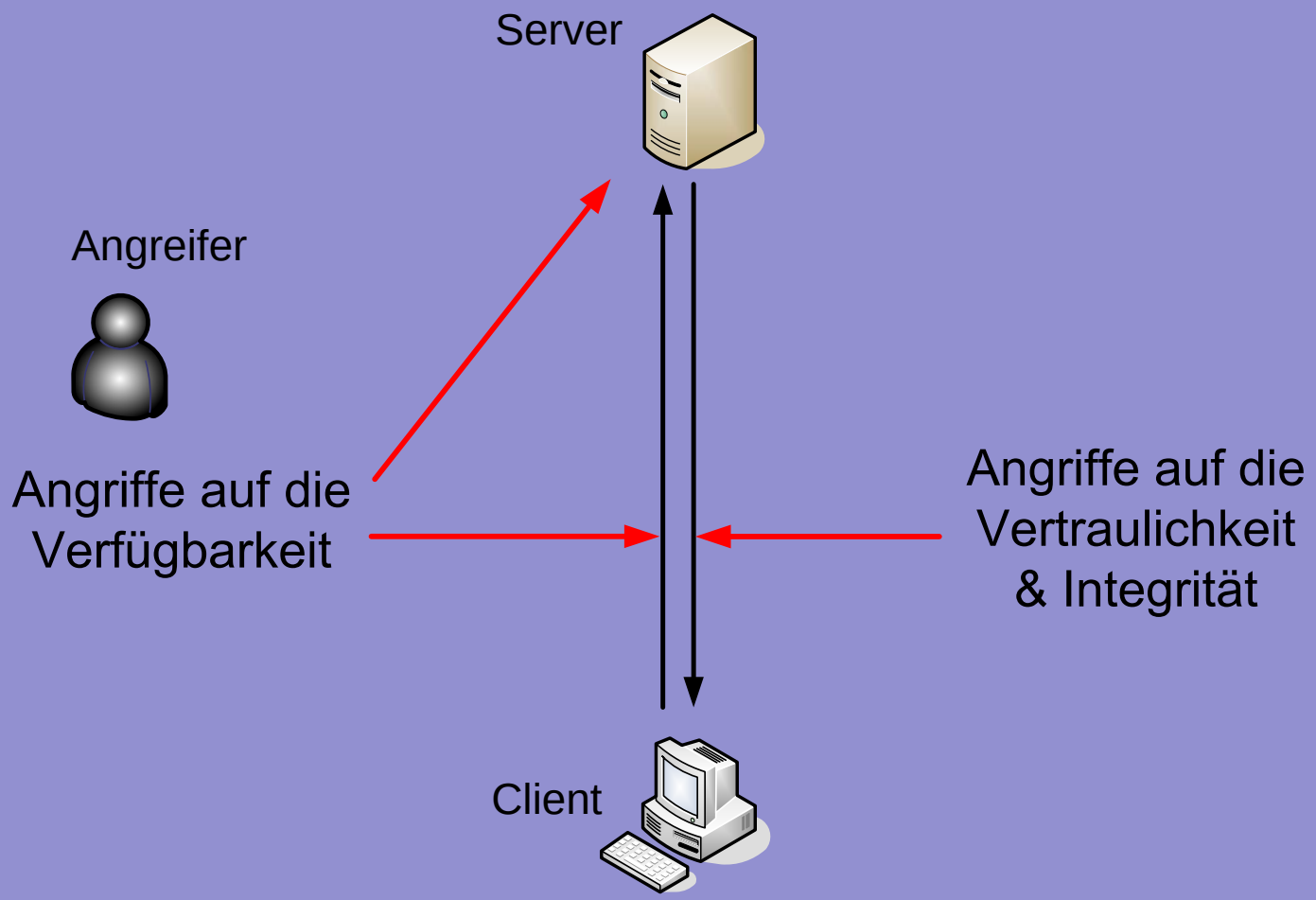
Mag. Lukas Feiler, SSCP
lukas.feiler@lukasfeiler.com
http://www.lukasfeiler.com/lectures_stubenbastei

# Aspekte der Netzwerk-Sicherheit

-Vertraulichkeit

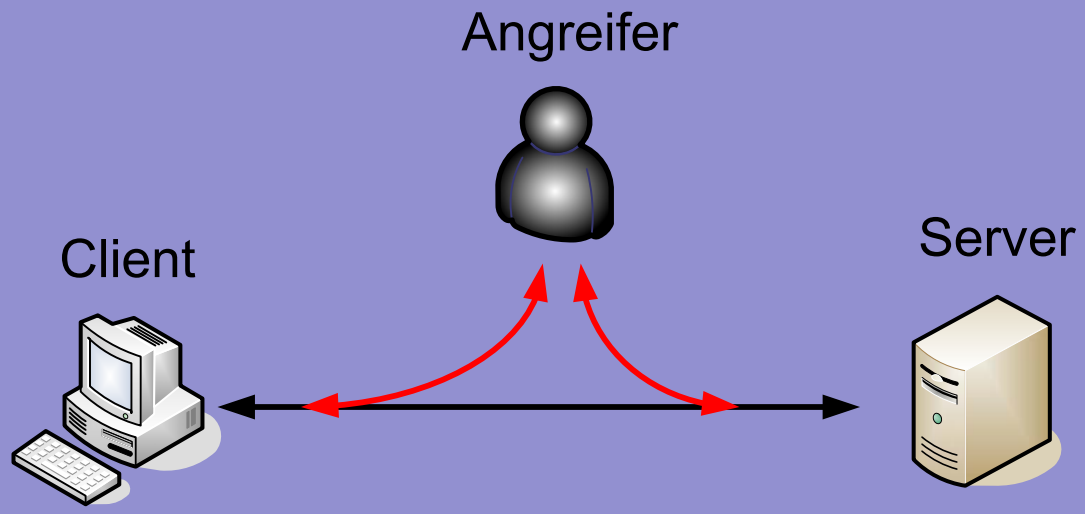
-Verfügbarkeit

-Integrität

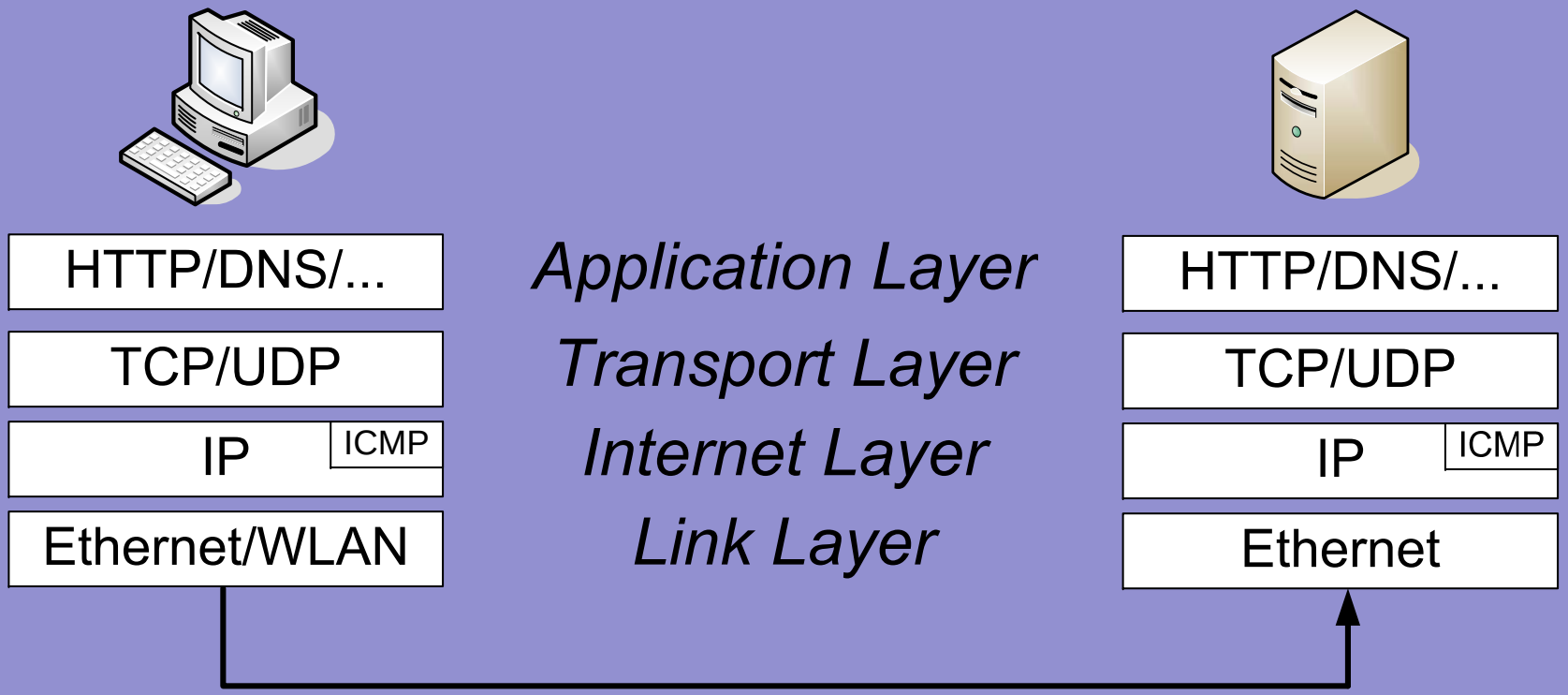



# Angriffe auf die Netzwerksicherheit

- Überbeanspruchung der verfügbaren Ressourcen (Denial of Service = DoS-Attacks)
- Man-in-the-Middle-Attacks (Positionierung zwischen Client und Server)




## Anrten der Angriffe




# Die 4 Network Layers des TCP/IP Modells

*Application Layer*

*Transport Layer*

*Internet Layer*

*Link Layer*

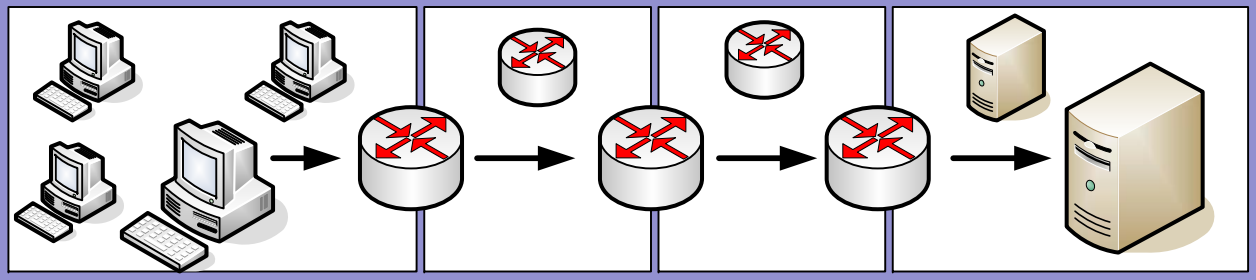
# Sicherheit auf dem Link-Layer

- Netzwerk-Traffic „mithören“
- ARP-Spoofing

# MAC-Adressen

→ Rechner des selben Netzwerks verfügen über eine Verbindung auf dem Link-Layer

→ Identifizierung einzelner Rechner auf dem Link-Layer: MAC-Adressen (nicht IP-Adressen!)
z.B. 02-1C-25-74-D0-98

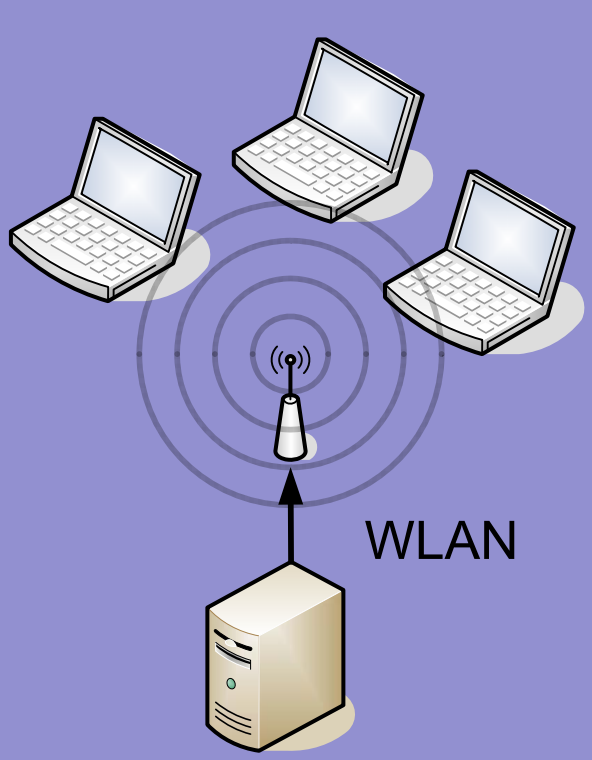


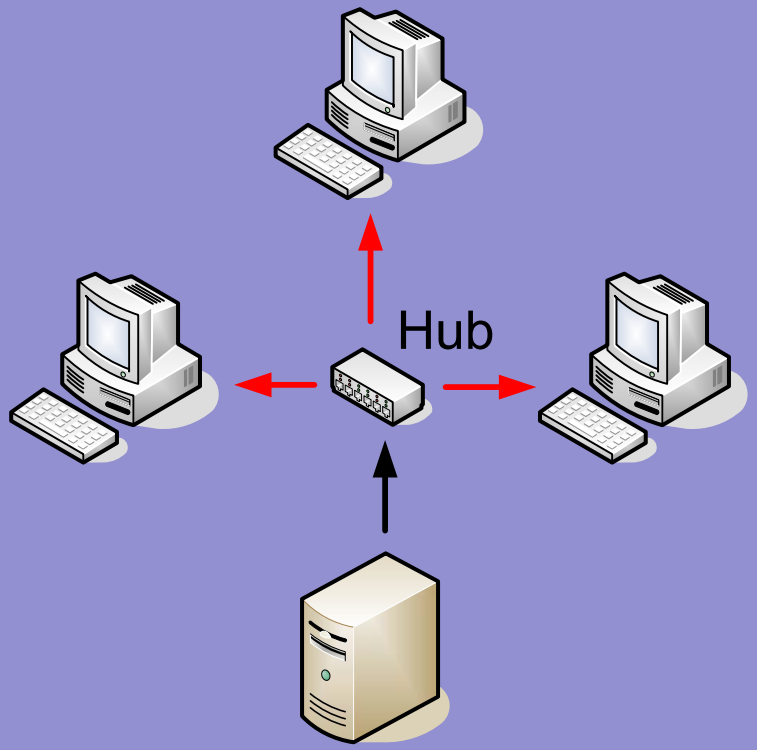
Wie wird ein IP- in eine MAC-Adresse übersetzt?

→ ARP (Address Resultion Protocol) - Funktionsweise:

„Wer hat IP 192.168.1.66?
Bitte send mir deine MAC-Adresse“

Grds werden alle Datenpakete an alle Rechner gesendet, die dann anhand der MAC-Adresse entscheiden, ob sie sie verarbeiten:




# Netzwerk-Traffic „mithören“: Promiscuous mode

# ARP-Spoofing

1) ARP-Request: Wer hat IP 192.168.1.66?
2) ARP-Response: *Falscher* Rechner antwortet mit seiner MAC-Adresse

Gegenmaßnahmen:
- ARP-Spoofing Detection im eigenen Netzwerk
- Statische ARP-Einträge

*Application Layer*

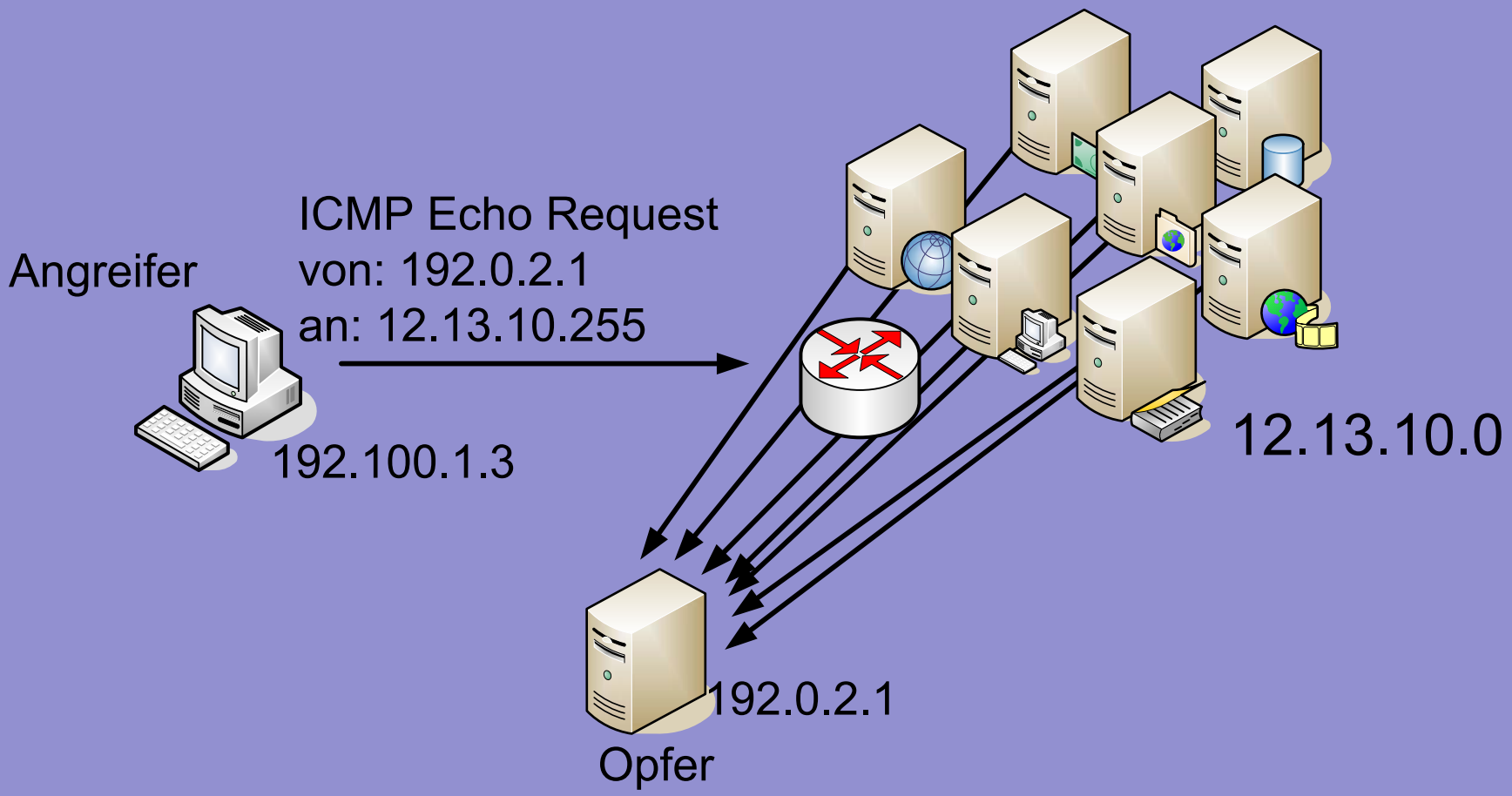
*Transport Layer*

*Internet Layer*

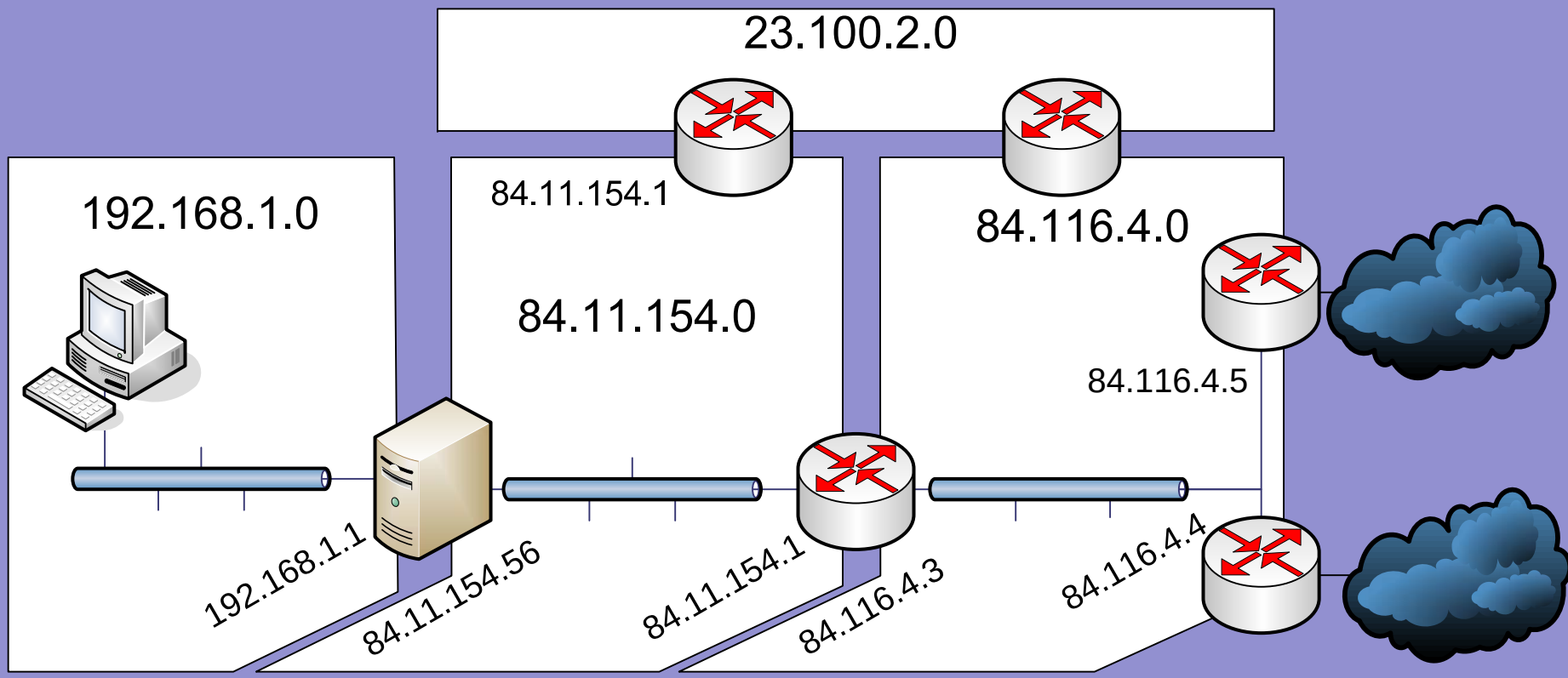
*Link Layer*

# Sicherheit auf dem Internet-Layer

- ICMP Floods
- Routing-basierte Angriffe


Angreifer
ICMP Echo Request
von: 192.0.2.1
an: 12.13.10.255
192.100.1.3
12.13.10.0
192.0.2.1
Opfer

# ICMP Flood


23.100.2.0
84.11.154.1
84.116.4.0
192.168.1.0
84.11.154.0
84.116.4.5
192.168.1.1
84.11.154.56
84.11.154.1
84.116.4.3
84.116.4.4

# IP Routing

*Application Layer*

*Transport Layer*

*Internet Layer*

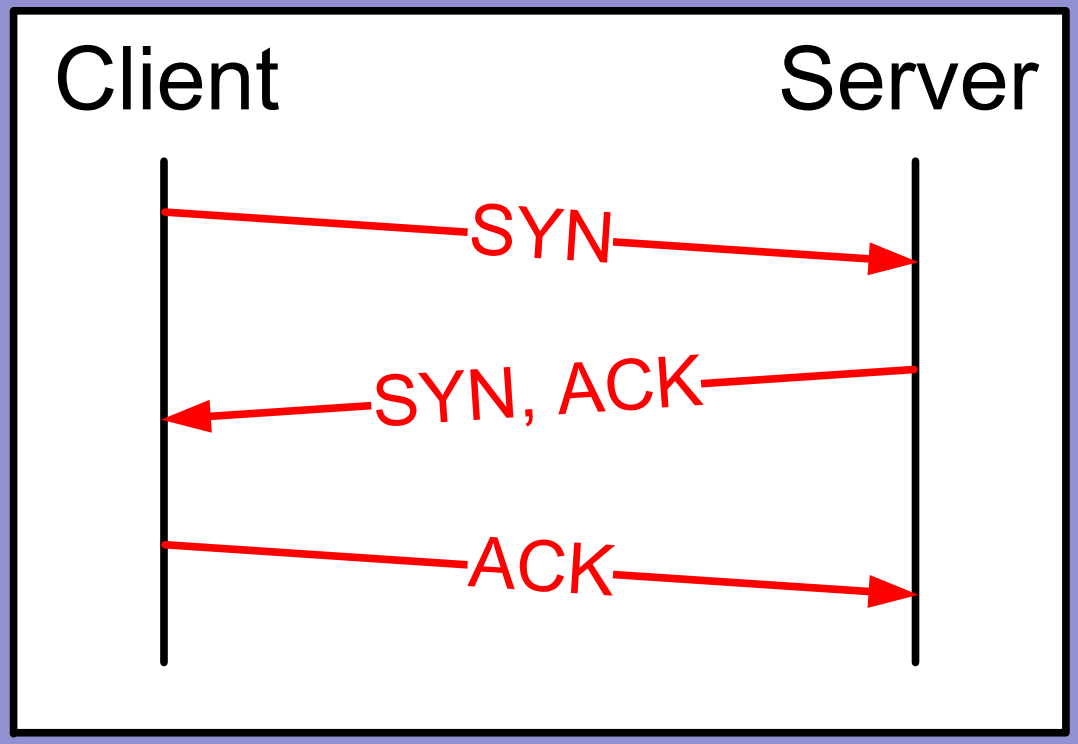
*Link Layer*

# Sicherheit auf dem Transport-Layer

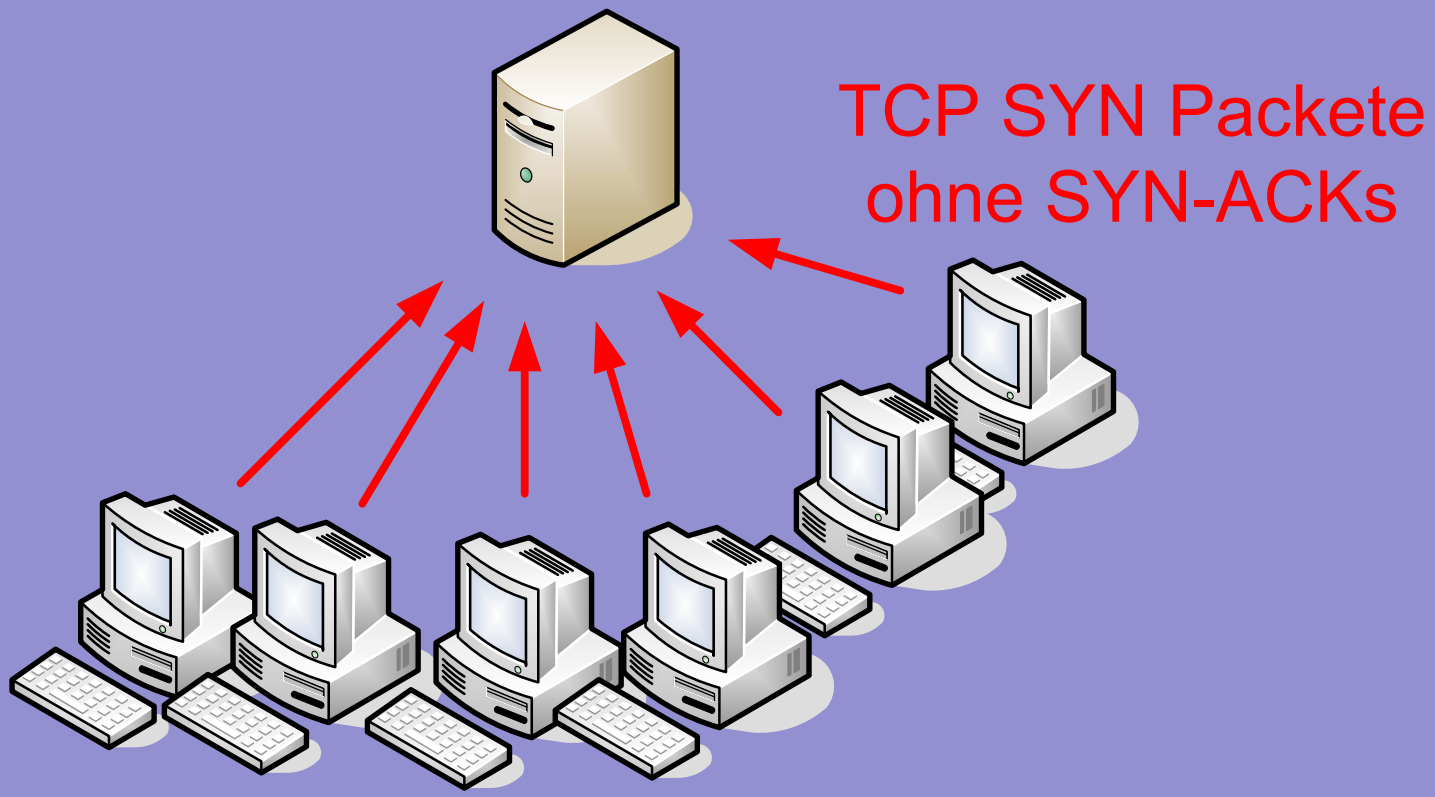
- TCP & UDP Basics
- TCP SYN Flooding

# Transmission Control Protocol (TCP) vs. User Datagram Protocol (UDP)

| | TCP | UDP |
|---|---|---|
| Verbindungsorientiert | + | - |
| Zuverlässig | + | - |
| ununterbrochener Datenstrom für Application-Layer-Protokolle | + | - |
| Einfachheit & Performance | - | + |




# TCP Verbindungsaufbau




# TCP SYN Flood

*Application Layer*

*Transport Layer*

*Internet Layer*

*Link Layer*

# Sicherheit auf dem Application-Layer

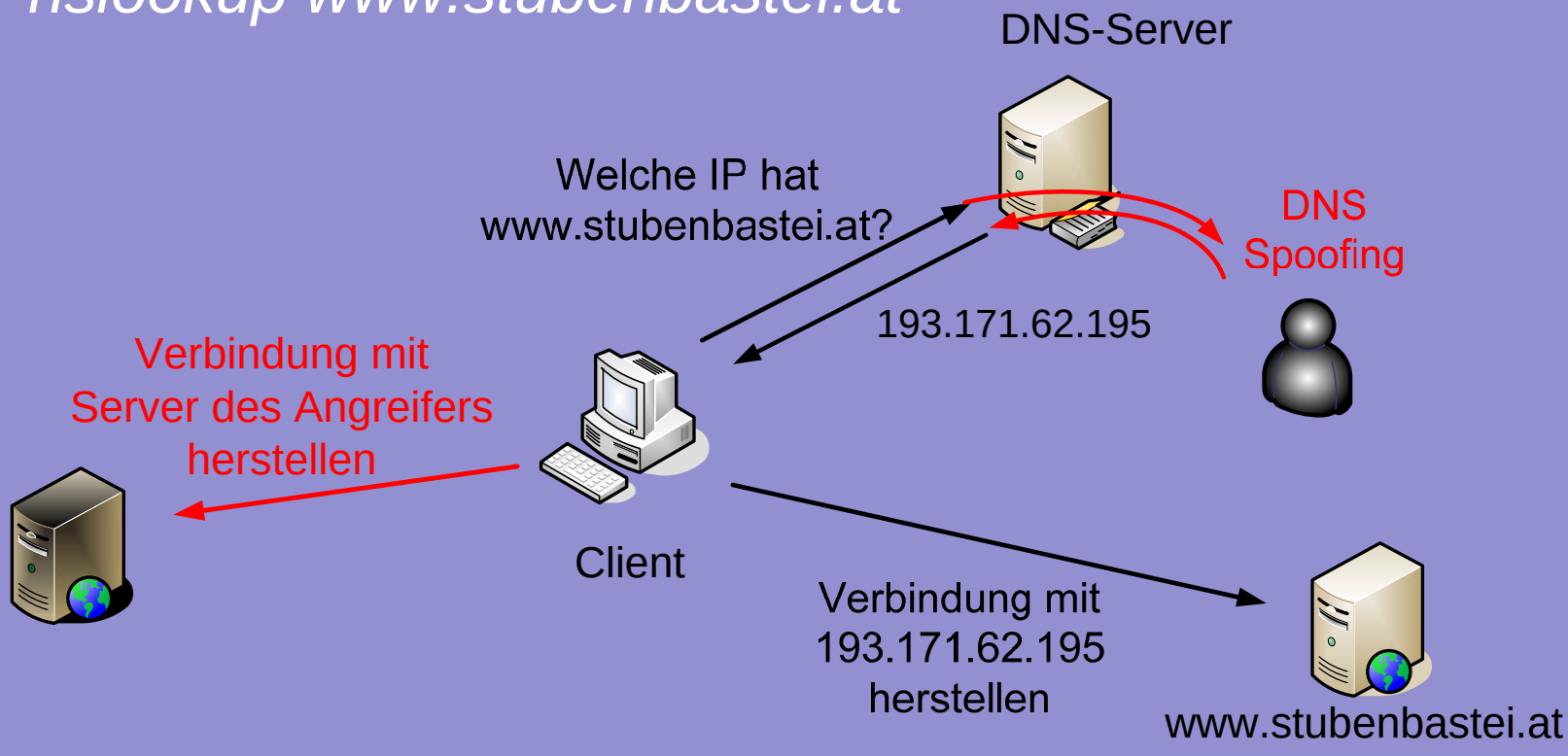
Application Layer Protokolle: z.B. HTTP, SMTP, DNS

→ DNS Spoofing

DNS – Domain Name System

→ Dient vor allem dazu Domain-Namen (z.B. www.example.com) in IP-Adressen zu übersetzen

*nslookup www.stubenbastei.at*



lukas.feiler@lukasfeiler.com

http://www.lukasfeiler.com/lectures_stubenbastei

Danke für die Aufmerksamkeit