tgm

IT Sicherheit

Netzwerktechnik - Angriffsmethoden

Christoph Roschger, Stefan Zakall

TGM Wien
Höhere Abteilung für Informationstechnologie

Februar, 2022

Wie komme ich zu meiner IP-Adresse?

DHCP?

DHCP – Aufgabe

- Dynamische Vergabe von IP-Adressen/Mask
- Dynamischen Setzen von DNS-Server, Gateway
- Protokollierung vergebener MAC zu IP

DHCP – Aufgabe

- Dynamische Vergabe von IP-Adressen/Mask
- Dynamischen Setzen von DNS-Server, Gateway
- Protokollierung vergebener MAC zu IP

Angriffe:

- Angreifer als Gateway
- Angreifer als DNS-Server

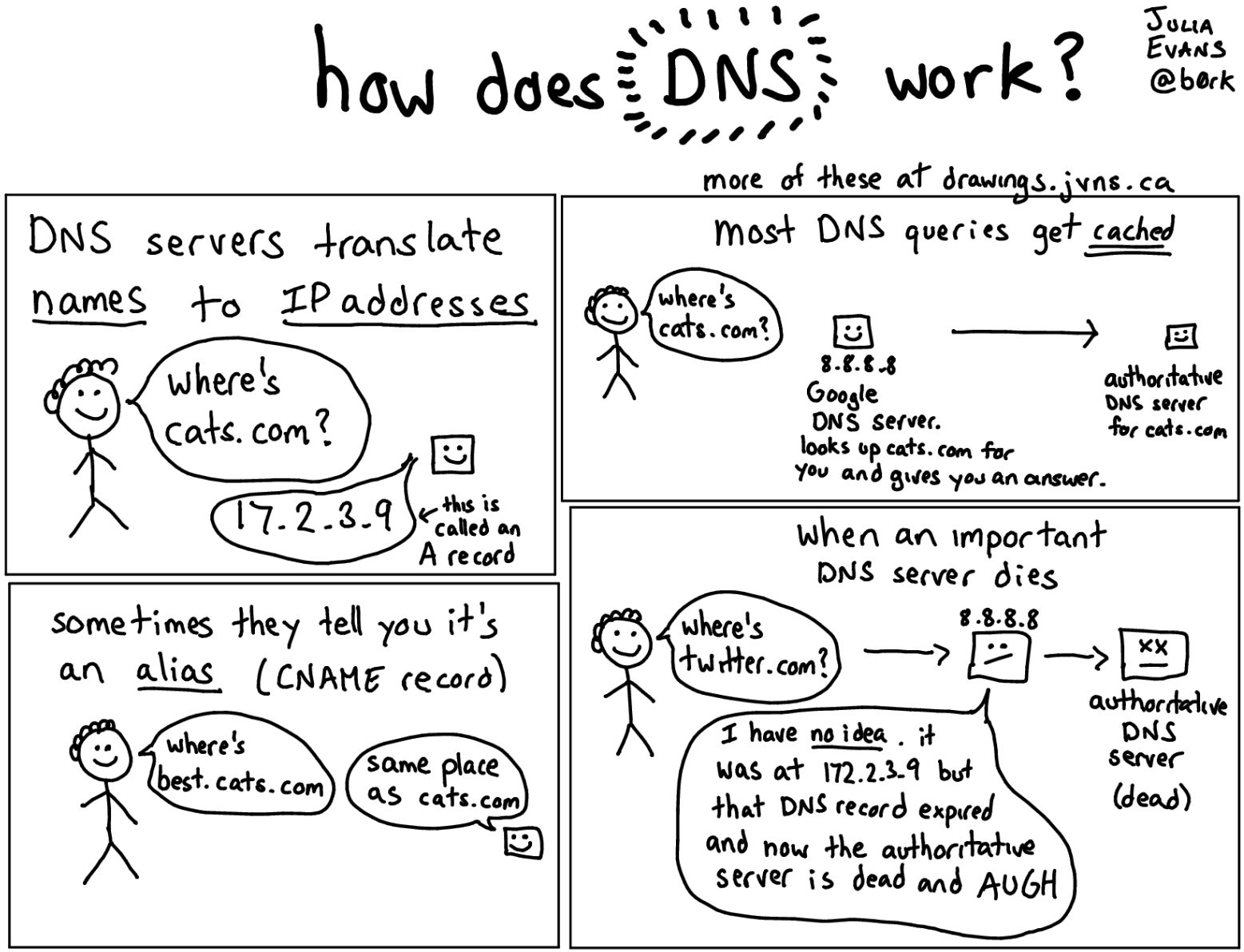
Netzwerktechnik

Dynamic Host Configuration Protocol – DHCP

DNS?

Netzwerktechnik

Protokolle – DNS



Domain Name System

DNS

Übersetzung Namen vs. IP-Adressen

rekursiv Fragt selbst bei anderen Servern nach.

iterativ Gibt andere Serveradressen weiter.

Angriffe:

- DNS Spoofing
- Man-In-The-Middle Attacken
- Phishing
- “Defacement”

Domain Name System

DNS

Übersetzung Namen vs. IP-Adressen

rekursiv Fragt selbst bei anderen Servern nach.

iterativ Gibt andere Serveradressen weiter.

Angriffe:

- DNS Spoofing
- Man-In-The-Middle Attacken
- Phishing
- “Defacement”

Verwandte Protokolle (Windows)

- NetBIOS
- LLMNR

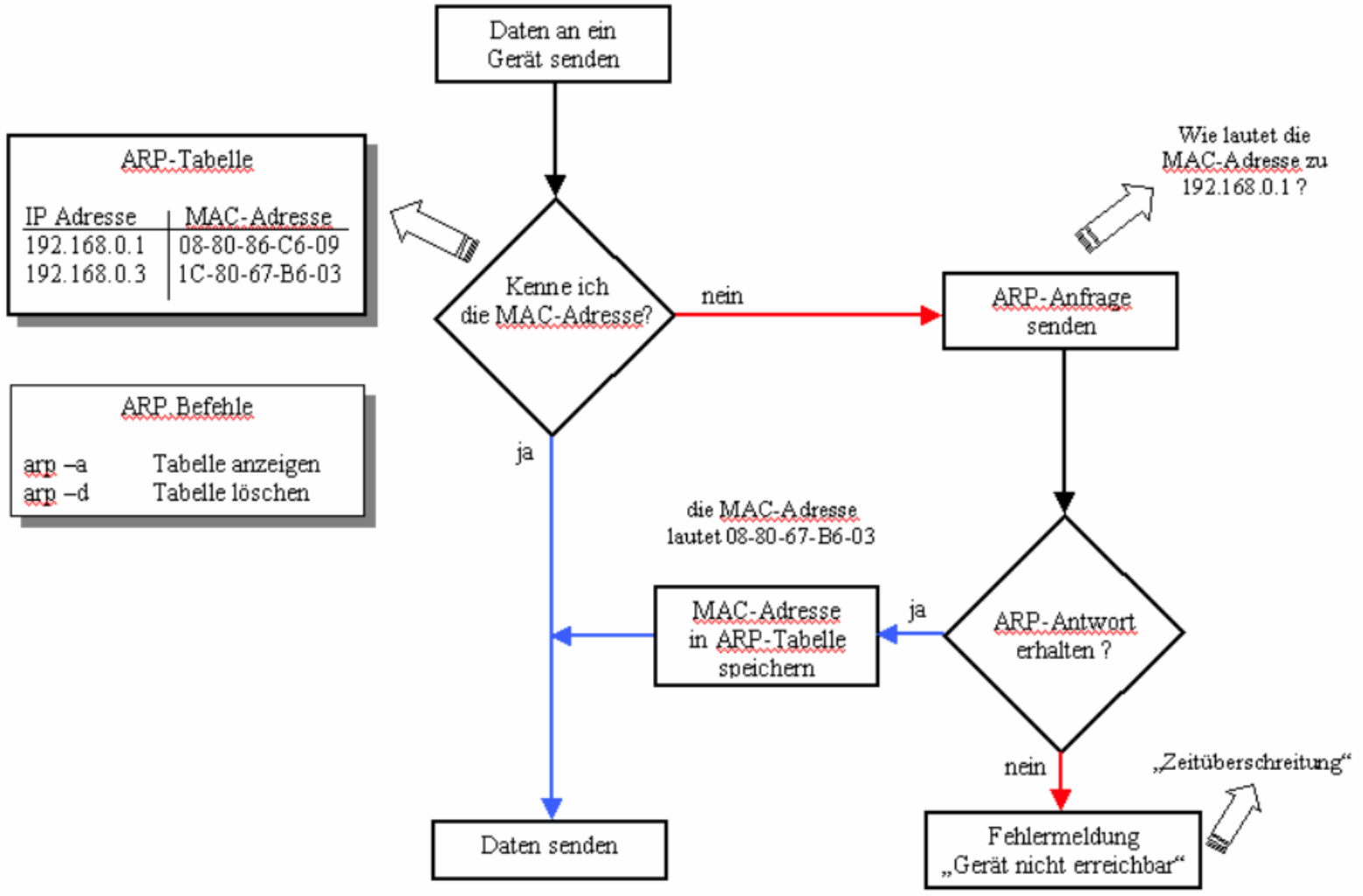
Protokolle

ARP

ARP?

Address Resolution Protocol

ARP



Address Resolution Protocol

ARP

Übersetzung Namen MAC-Adressen vs. IP-Adressen

Broadcast Anfragen gehen immer ans ganze Netzwerk.

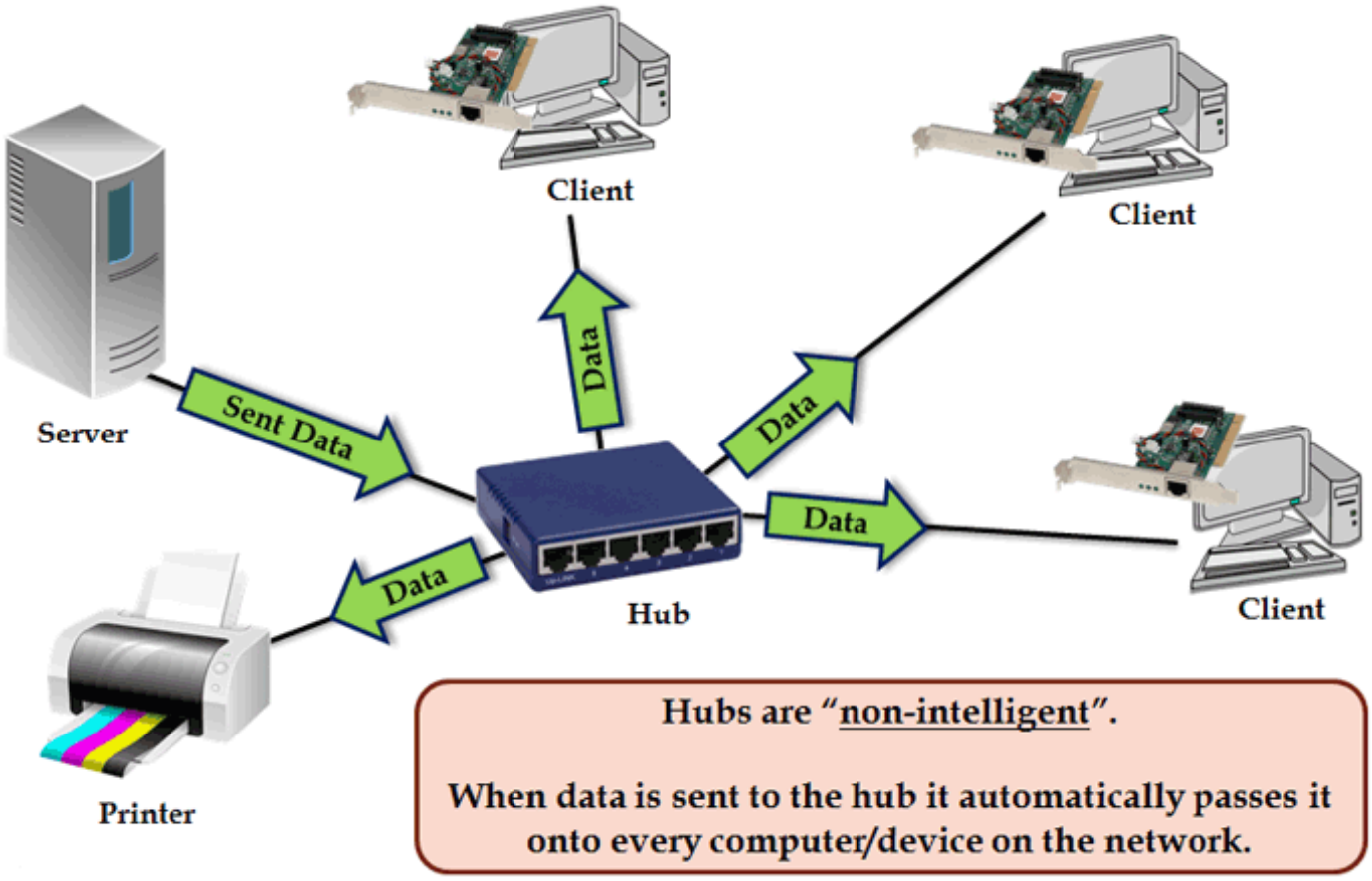
ARP-Cache MAC-Adressen werden gecached (ca. 10min).

ARP Spoofing

- Senden falscher Antworten an ARP Anfragen
- Angriff auf ARP Cache des Opfers
- $\rightarrow$ DoS-Attacken
- $\rightarrow$ Man-in-the-Middle Attacken

Netzwerkgeräte

Hub



Probleme:

- Kollisionen
- Vertraulichkeit?

Netzwerkgeräte

Switch

- Vermittlung zwischen Rechnern im gleichen Netz
- Mapping MAC $\mapsto$ Port
- Zustellung nur an jeweiligen Port
- Häufiges Angriffsziel

Netzwerkgeräte

Switch

- Vermittlung zwischen Rechnern im gleichen Netz
- Mapping MAC $\mapsto$ Port
- Zustellung nur an jeweiligen Port
- Häufiges Angriffsziel
- Frage: Fail-Open oder Fail-Close?

Netzwerkgeräte

Router

- Vermittelt zwischen verschiedenen Netzwerken
- Verwendung von Routing-Tabellen
- Angriffe:
  - BGP Hijacking `https://therecord.media/klayswap-crypto-users-lose-funds-after-bgp-hijack/`
  - DDoS Angriffe
  - Man-in-the-Middle Angriffe

Netzwerkgeräte

Security

Firewall

Filtern von Paketen nach verschiedenen Kriterien

- Src, Dest - Port
- Deep Packet Inspection: Anderen Kriterien

Netzwerkgeräte

Security

Firewall

Filtern von Paketen nach verschiedenen Kriterien

- Src, Dest - Port
- Deep Packet Inspection: Anderen Kriterien

Intrusion Detection System

Erkennen von Angriffen im Netzwerk

- Protokollieren von verdächtigem Traffic
- Software: https://zeek.org/

Netzwerkgeräte

Security

Firewall

Filtern von Paketen nach verschiedenen Kriterien

- Src, Dest - Port
- Deep Packet Inspection: Anderen Kriterien

Intrusion Detection System

Erkennen von Angriffen im Netzwerk

- Protokollieren von verdächtigem Traffic
- Software: https://zeek.org/

Intrusion Prevention System

Blockieren von verdächtigen Paketen

- Meist regelbasiert
- Software: https://www.snort.org/