Netzwerke, Teil 1: Werkzeuge

Handout zum Vortrag im CCC Freiburg

Balrog

2026-10-06

Befehle je Betriebssystem

Aufgabe	Linux	macOS	Windows
Adressen anzeigen	`ip -br addr`	`ifconfig`	`ipconfig /all`
MAC-Adressen	`ip -br link`	`ifconfig en0 ether`	`getmac /v`
ARP-Cache (IPv4)	`ip -4 neigh`	`arp -an`	`arp -a`
Nachbarn (IPv6)	`ip -6 neigh`	`ndp -an`	`netsh interface ipv6 show neighbors`
Routing-Tabelle	`ip route`	`netstat -rn`	`route print`
Erreichbarkeit	`ping 10.23.42.1`	`ping 10.23.42.1`	`ping 10.23.42.1`
Weg zum Ziel	`traceroute`, `mtr`	`traceroute`	`tracert`
DNS-Abfrage	`dig cccfr.de`	`dig cccfr.de`	`Resolve-DnsName cccfr.de`
Offene Ports	`ss -tulpn`	`lsof -nP -iTCP -sTCP:LISTEN`	`netstat -ano`
Mitschnitt im Terminal	`sudo tcpdump -ni eth0 -e`	`sudo tcpdump -ni en0 -e`	`pktmon` oder Wireshark

Die Schnittstellennamen weichen ab: unter Linux z. B. `eth0`, `enp3s0` oder `wlan0`, unter macOS meist `en0` (WLAN oder Kabel), unter Windows Namen wie „Ethernet" oder „WLAN". `ip`, `ss` und `tcpdump` sind unter Linux fast immer vorinstalliert; `mtr` und `dig` meist als eigene Pakete (`mtr`, `dnsutils` bzw. `bind-tools`).

Wireshark

Download: wireshark.org. Unter Linux aus der Paketverwaltung; damit man ohne root mitschneiden darf, den eigenen Benutzer in die Gruppe `wireshark` aufnehmen und neu anmelden.

Fenster

- **Oben:** Paketliste, ein Frame pro Zeile.
- **Mitte:** der ausgewählte Frame, Schicht für Schicht aufklappbar. Von oben nach unten gelesen ist das die Kapselung.
- **Unten bzw. rechts:** die rohen Bytes. Ein Klick auf ein Feld in der Mitte markiert die zugehörigen Bytes.

Anzeigefilter

Kommen in die Filterzeile über der Paketliste und lassen sich während des Mitschnitts ändern.

Filter	zeigt
`eth.dst == ff:ff:ff:ff:ff:ff`	alle Broadcasts
`eth.addr == d0:ea:11:dc:66:b5`	alles von oder zu einer MAC
`vlan`	Frames mit VLAN-Tag
`arp`	ARP-Anfragen und -Antworten
`icmp or icmpv6`	Ping und Fehlermeldungen
`dns`	Namensauflösung
`dhcp`	Adressvergabe (IPv4)
`tcp.port == 443`	HTTPS
`not (mdns or ssdp or llmnr)`	blendet häufiges Hintergrundrauschen aus

Filter lassen sich mit `and`, `or`, `not` und Klammern kombinieren. Ist die Filterzeile grün, stimmt die Syntax.

Mitschnittfilter

Werden **vor** dem Start eingetragen und entscheiden, was überhaupt gespeichert wird. Sie haben eine andere Syntax (BPF, wie bei `tcpdump`):

Filter	speichert
`arp`	nur ARP
`host 10.23.42.1`	nur Verkehr von und zu dieser Adresse
`not port 22`	alles außer SSH (nützlich, wenn man per SSH auf dem Gerät ist)
`ether broadcast`	nur Broadcasts

`eth.dst == …` ist ein Anzeigefilter und funktioniert als Mitschnittfilter nicht.

Mitschneiden

Im eigenen Netz und an eigenen Geräten ist Mitschneiden in Ordnung. In fremden Netzen nur mit Erlaubnis der Betreiber; Mitschnitte enthalten Namen, Adressen und manchmal Passwörter.

An einem Switch sieht man nur den eigenen Verkehr sowie Broadcasts und Multicasts. Um den Verkehr anderer Geräte zu sehen, braucht man einen Spiegelport am Switch.

Übungen

1. **Eigene MAC.** Finde die MAC-Adresse deines Laptops (Kabel und WLAN) und deines Handys. Welche ist lokal vergeben? Prüfe die zweite Hex-Ziffer.
2. **Hersteller.** Schlage die ersten drei Byte deiner Laptop-MAC nach, z. B. auf maclookup.app. Passt der Hersteller zur Netzwerkkarte?
3. **Broadcasts zählen.** Schneide fünf Minuten lang im Club-Netz mit, Anzeigefilter `eth.dst == ff:ff:ff:ff:ff:ff`. Welche Protokolle tauchen auf? Unter *Statistiken → Protokollhierarchie* gibt es eine Übersicht.
4. **Nachbarn finden.** Filtere auf `mndp` bzw. `lldp`. Welche Switches melden sich, mit welchem Namen und Modell?

5. **ARP beobachten.** Leere den ARP-Cache, starte den Mitschnitt mit Filter `arp` und pinge den Router an. Wer fragt, wer antwortet, und an welche MAC-Adresse geht die Antwort?

ARP-Cache leeren: macOS `sudo arp -a -d`, Linux `sudo ip neigh flush all`, Windows als Administrator `arp -d *`.

Zum Weiterlesen

- Julia Evans, *Networking! ACK!* Kurzes Comic-Heft, guter Einstieg. wizardzines.com
- James F. Kurose, Keith W. Ross, *Computer Networking: A Top-Down Approach*. Lehrbuch, beginnt bei der Anwendung und arbeitet sich nach unten.
- W. Richard Stevens, Kevin R. Fall, *TCP/IP Illustrated, Volume 1: The Protocols*, 2. Auflage 2011. Erklärt jedes Protokoll an echten Mitschnitten, das Nachschlagewerk schlechthin. Die 1. Auflage (1994) von Stevens allein ist sprachlich die schönere, kennt aber kaum IPv6.
- Andrew S. Tanenbaum, *Computernetzwerke*. Das deutschsprachige Standardwerk, geht von unten nach oben.
- Chris Sanders, *Practical Packet Analysis*. Wireshark an echten Fehlerbildern.
- Wireshark-Beispielmitschnitte: wiki.wireshark.org/SampleCaptures