DHBW Karlsruhe
Duale Hochschule Baden-Württemberg

Netztechnik I

TINF

Wireshark ARP

Markus Götzl
Dipl.-Inform. (FH)
mail@markusgoetzl.de

http://www.dhbw-karlsruhe.de

Inhalte

Wireshark

- Wireshark Ressourcen
- Mitschitt (Trace) erzeugen
- Trace Analyse
- ARP

Wireshark Ressourcen

- Wireshark Homepage:
  - *http://www.wireshark.org*
- Wireshark Downloads:
  - http://www.wireshark.org/download.html
- Wireshark Dokumentation
  - *http://www.wireshark.org/docs/*

Trace erzeugen

Finden des Netzwerk-Interfaces und des Gateways

```
Themis:~ root# route -n get default
   route to: default
destination: default
       mask: default
    gateway: 192.168.2.1
  interface: en0
```

- Linux: `route`
- Windows: `route print`
- Mac: `route -n get default`

Trace erzeugen

Finden der eigenen MAC-Adresse

```
themis:~ root# ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        inet6 fe80::223:32ff:feda:198c%en0 prefixlen 64 scopeid 0x4
        inet 192.168.2.107 netmask 0xffffff00 broadcast 192.168.2.255
        inet6 2003:6a:6f16:a601:223:32ff:feda:198c prefixlen 64 autoconf
        ether 00:23:32:da:19:8c
        media: autoselect (100baseTX <full-duplex,flow-control>) status: active
        supported media: none autoselect 10baseT/UTP <half-duplex> 10baseT/UTP <
full-duplex> 10baseT/UTP <full-duplex,flow-control> 10baseT/UTP <full-duplex,hw-
loopback> 100baseTX <half-duplex> 100baseTX <full-duplex> 100baseTX <full-duplex
,flow-control> 100baseTX <full-duplex,hw-loopback> 1000baseT <full-duplex> 1000b
aseT <full-duplex,flow-control> 1000baseT <full-duplex,hw-loopback>
```

- Linux: `ifconfig <device>`
- Windows: `ipconfig /all | more`
- Mac: `ifconfig <device>`

Trace erzeugen

“arp” Kommandozeilen-Tool: Anzeigen der aktuellen Einträge im ARP-Cache

```
themis:~ root# arp -a
speedport.ip (192.168.2.1) at 84:9c:a6:19:f6:95 on en0 [ethernet]
mark-14 (192.168.2.104) at 60:36:dd:f4:a9:7f on en0 [ethernet]
cine (192.168.2.143) at 14:da:e9:93:df:23 on en0 [ethernet]
? (192.168.2.255) at ff:ff:ff:ff:ff:ff on en0 [ethernet]
```

- Linux: `arp -a`
- Windows: `arp -a`
- Mac: `arp -a`

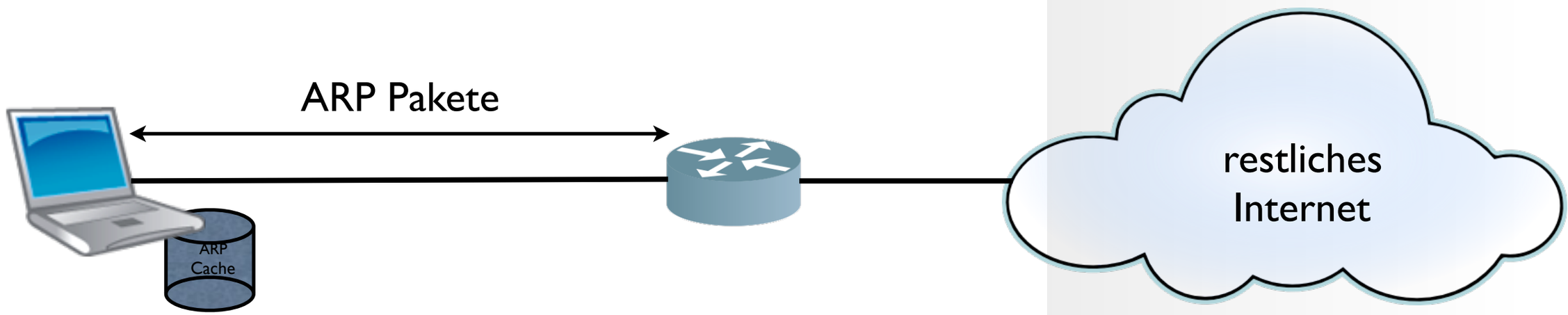
Trace erzeugen

“arp” Kommandozeilen-Tool: Einen Eintrag aus dem ARP-Cache löschen bzw. den gesamten ARP-Cache löschen

```
themis:~ root# arp -d -a
192.168.2.1 (192.168.2.1) deleted
192.168.2.104 (192.168.2.104) deleted
192.168.2.143 (192.168.2.143) deleted
192.168.2.255 (192.168.2.255) deleted
themis:~ root# arp -a
```

- Linux: `arp -d <ip gateway>`
- Windows: `arp -d`
- Mac: `arp -d -a`

Umgebung von ARP



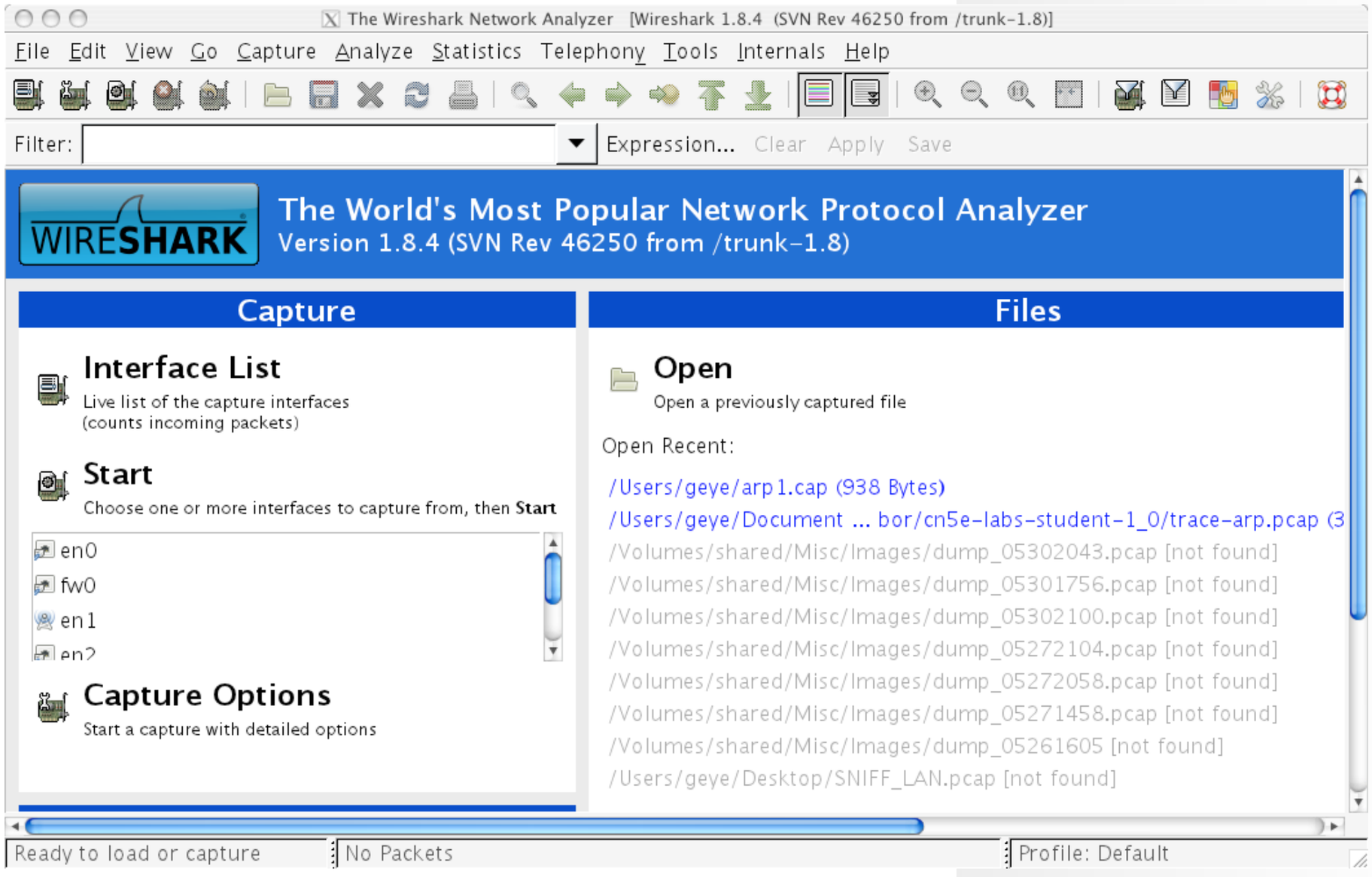
lokale IP - MAC Adressen Zuordnung

lokaler Rechner

lokaler Router
(default gateway)

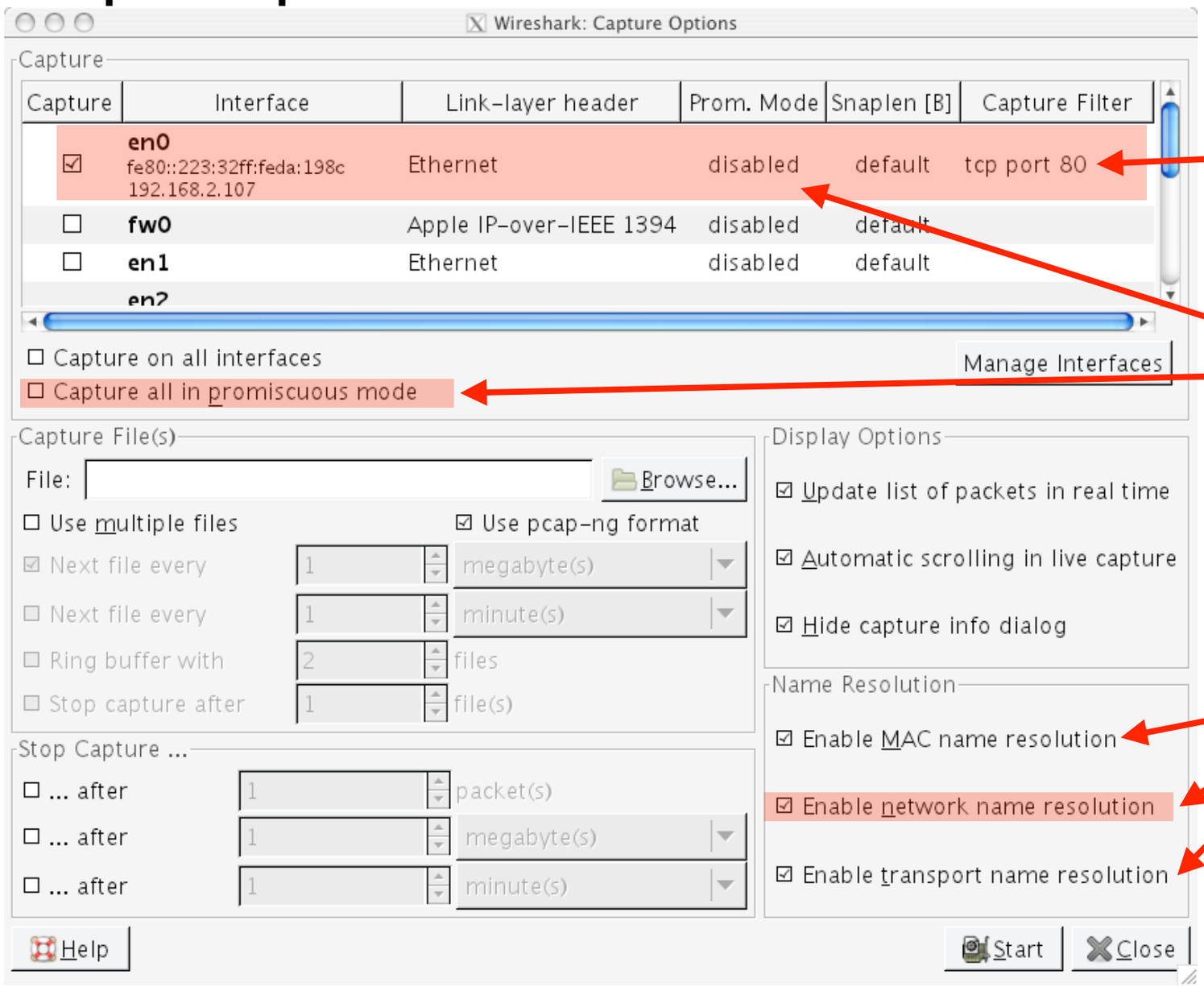
Trace erzeugen

Wireshark starten



Trace erzeugen

Capture Options



Capture Filter: "Vorfiltern" des Mitschnittes. Leer -> keine Filterung.

Nur Verkehr, der für dieses Gerät bestimmt ist.

Namensauflösung

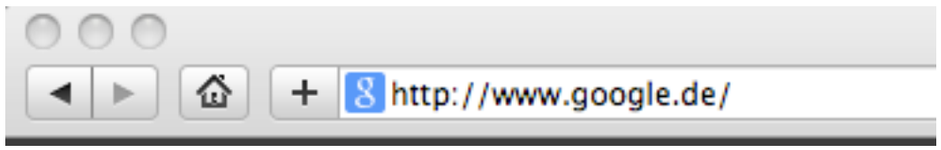
Trace erzeugen

1. Starten Sie den Mitschnitt (Capture Filter: “arp”) - löschen Sie den den Eintrag des “Default Gateways” aus Ihrem ARP-Cache bzw. löschen Sie den gesamten ARP-Cache und rufen Sie über Ihren Browser eine externe Internet-Seite auf (z.B. www.google.de)

(a)

```
themis:~ root# arp -d -a
192.168.2.1 (192.168.2.1) deleted
192.168.2.104 (192.168.2.104) deleted
192.168.2.143 (192.168.2.143) deleted
192.168.2.255 (192.168.2.255) deleted
themis:~ root# arp -a
```

(b)



Trace erzeugen

2. Beschreiben Sie warum es in den Aufgabenteilen 1a und 1b (Vorbereitungen) notwendig war den ARP-Cache zu löschen sowie im Browser eine externe Internet-Seite auf zurufen.

3. Setzen Sie einen “Display Filter” um nur ARP Pakete von und zu Ihrem Rechner zu sehen.

```
eth.addr==<MAC-Adresse>

(z.B.: eth.addr==00:23:32:da:19:8c)
```

Trace erzeugen

4. Finden Sie den *ARP Request.*

   I. Ethernet Block:

      (a) Nennen Sie den Quell- und die Zieladressen des Ethernet-Frames?

      (b) Welchen Wert hat das Ethernet “Type”-Feld?

   II. ARP Block:

      (a) Welcher “Opcode” wird verwendet?

      (b) Welche MAC bzw. IP Adresse hat der Sender?

      (c) Welche MAC bzw. IP Adresse hat der Empfänger?

      (d) Welche Adressen in welcher Größe werden ausgetauscht?

Trace erzeugen

5. Finden Sie den *ARP Reply.*

   I. Ethernet Block:

      (a) Nennen Sie den Quell- und die Zieladressen des Ethernet-Frames?

      (b) Welchen Wert hat das Ethernet “Type”-Feld?

   II. ARP Block:

      (a) Welcher “Opcode” wird verwendet?

      (b) Welche MAC bzw. IP Adresse hat der Sender?

      (c) Welche MAC bzw. IP Adresse hat der Empfänger?

      (d) Welche Adressen in welcher Größe werden ausgetauscht?