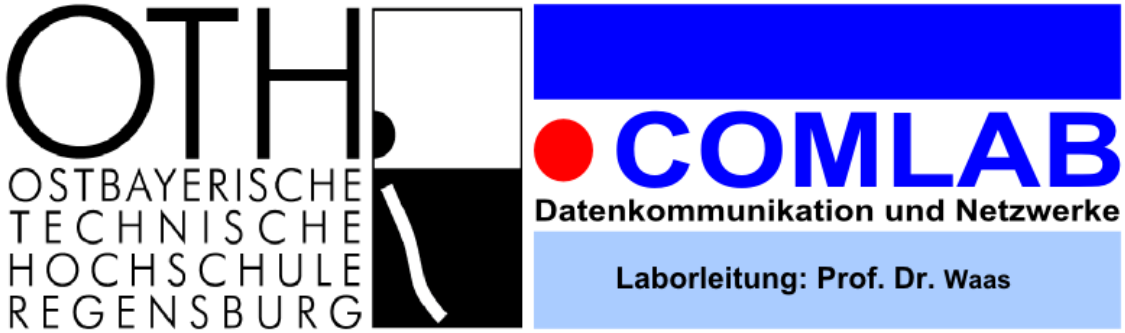

Ostbayerische Technische Hochschule Regensburg

K. Spörl

Lösungen zu TCPIP 2

3 WEITERE FILTER AUF MAC-EBENE

- Filtern Sie alle Frames heraus, die als Zieladresse die Broadcast-Adresse haben (FF:FF:FF:FF:FF:FF). Welche höheren Protokolle verwenden diese Art der Meldungen?
  eth.addr==ff:ff:ff:ff:ff:ff

- Filtern Sie alle Frames heraus, die als Zieladresse eine Multicast Adresse haben (IG-Bit=1). Welche höheren Protokolle verwenden diese Art der Meldungen?
  eth.ig==1 && !eth.addr==ff:ff:ff:ff:ff:ff

- Filtern Sie alle Frames, die IPv4 transportieren.
  eth.type=0x800

- Filtern Sie alle Frames, die IPv6 transportieren.
  eth.type=0x86dd

- Filtern Sie alle Frames heraus, die weder IPv4 noch IPv6 transportieren.
  !eth.type==0x800 && !eth.type==0x86dd

- Filtern Sie alle Frames heraus die vom Type IPv6 sind und an eine Multicast-Adresse gesendet werden. Welche Art von Frames sind das?
  eth.type==0x86dd && eth.ig==1
  DHCPv6 Solicit, Router Adv., Neighbor Discovery, LLMNR

- Filtern Sie alle Frames heraus die kürzer als die minimale Framelänge sind. Die Filterregel dafür beginnt mit frame.len ...
  frame.len<64

- Filtern Sie alle Frames heraus, die größer als die max. Ethernet Framegröße sind.
  frame.len>1518
- Filtern Sie alle Frames heraus, die eine LLC haben. Filterregel: llc
- Filtern Sie alle Frames heraus, die keine LLC haben.
  !llc

  - ☑ Mit welcher anderen Capture-Filterregel könnte man LLC Ethernet Frames noch filtern?
    eth.len<0x600
  - ☑ Welches Bit in der Wireshark Anzeige signalisiert, dass es sich um ein Broad-oder Multicastadresse handelt?
    IG-Bit ist D0 des höchstwertigen Bytes der Zieladresse

5 CAPTURE FILTER

- Filtern Sie nur alle Broadcasts im Adressbereich 194.95.109.128/26. Erstellen Sie dazu selbst den geeigneten Filter.
  broadcast and net 194.95.109.128/26

6 ARP PROTOKOLL

- ☑ Warum sendet der Labor-PC den ARP Request an eine Broadcastadresse.
  Weil er das Ziel nicht kennt.
- ☑ Wie unterscheiden sich die Sender- und Target-Adressfelder bei ARP-Request und ARP-Reply?
  Werden vertauscht.

- ☑ Sehen Sie auch einen ARP Request für 194.95.104.1?
  Nein, weil die Adresse in einem andern Subnetz liegt. Daher geht alles für diese Adresse zum Router
- ☑ Und aus welchem Grund?
  s.o.
- ☑ Sind beide IP-Adressen im selben Subnetz?
  s.o.
- ☑ Wohin wird der Ping Request eigentlich gesendet. Gleichen Sie die Adresse aus Wireshark mit dem aktuellen ARP-Cache des Labor-PCs ab?
  MAC-Adresse des Router 194.95.109.129 oder 130, je nach Routingtabelle.
- ☑ Wer verbirgt sich hinter dieser Adresse 194.95.109.129 bzw. 130
  Der Router

☑ Sind unter den aufgezeichneten ARP-Request Frames auch welche aus anderen Subnetzen? Warum ist das so?
Nein. ARP Request bleiben nur im eigenen Subnetz

☑ Wie weit breitet sich eine Broadcast-Meldung in einem Ethernet Segment aus? Wo ist die Grenze?
Nur im eigenen Subnetz (Broadcast Domain)

7 MESSUNGEN MIT IPv6

☑ Betrachten Sie einen ICMPv6 Router advertisement Frame. Welche Zieladresse hat er auf Datalink und IPv6 Ebene.
33:33:00:00:00:01
ff02::1

☑ Wie erfolgt die Abbildung der IPv6 Multicastadresse auf eine Ethernet Multicastadresse?
33:33: < last sig. 32 Bit der IPv6 Adresse>

☑ Finden Sie die Neighbor Discovery Frames für den oben "angepingten" host.
Falls Sie keine aufgezeichnet haben, löschen Sie wieder den Neighbor-Cache und wiederholen Sie den ping.

- Welche MAC-Adresse ist beim Neighbor Solicitation im ICMPv6-Header als Link-Layer-Adresse angegeben?
  Suchender Host
- Welche MAC-Adresse ist beim Neighbor Advertisement im ICMP-Header als Link-Layer-Adresse angegeben?
  Gesuchter Host
- Achtung: MAC Adresse kann abweichen!

  Frame 11 (86 bytes on wire, 86 bytes captured)
  Ethernet II, Src: Dell_b9:5b:02 (00:1e:4f:b9:5b:02), Dst: IPv6mcast_ff:f3:b1:67 (33:33:ff:f3:b1:67)
  Internet Protocol Version 6
  Internet Control Message Protocol v6
  Type: 135 (Neighbor solicitation)
  Code: 0
  Checksum: 0xd1cb [correct]
  Target: 2001:638:a01:109:20c:29ff:fef3:b167 (2001:638:a01:3f09:20c:29ff:fef3:b167)
  ICMPv6 Option (Source link-layer address)
  Type: Source link-layer address (1)
  Length: 8
  Link-layer address: 00:1e:4f:b9:5b:02

  Frame 12 (86 bytes on wire, 86 bytes captured)
  Ethernet II, Src: Vmware_f3:b1:67 (00:0c:29:f3:b1:67), Dst: Dell_b9:5b:02 (00:1e:4f:b9:5b:02)
  Internet Protocol Version 6
  Internet Control Message Protocol v6

Type: 136 (Neighbor advertisement)
Code: 0
Checksum: 0xe1f3 [correct]
Flags: 0x60000000
Target: 2001:638:a01:3f09:20c:29ff:fef3:b167
(2001:638:a01:109:20c:29ff:fef3:b167)
ICMPv6 Option (Target link-layer address)
Type: Target link-layer address (2)
Length: 8
Link-layer address: 00:0c:29:f3:b1:67

☑ Vergleichen Sie die mit Wireshark gefundene Adresse für den o.g. Host mit dem Ergebnis aus dem Neighbor-Cache.