Ostbayerische Technische Hochschule Regensburg

K. Spörl

Lösungen zu TCPIP3

3 ROUTINGINFORMATIONEN

- ☑ Wohin sendet der Labor-PC Pakete für Subnetz 192.168.2.0/24 bzw. fd00:0:0:2::/64 ?
  Interface 192.168.1.5
  Interface fd00:0:0:1::5
- ☑ Wohin sendet der IPHost Pakete für Subnetz 192.168.1.0/24 bzw. fd00:0:0:1::/64 ?
  Interface 192.168.2.2
  Interface fd00:0:0:2::2
- ☑ Zu welchem Interface leitet der IPRouter welche Pakete weiter?
  192.168.2.0 -> 192.168.2.2, eth1
  192.168.1.0 -> 192.168.1.5, eth0
  fd00:0:0:2::/64 -> fd00:0:0:2::2, eth1
  fd00:0:0:1::/64 -> fd00:0:0:1::5, eth0

- ☑ Wohin zeigt die Defaultroute am Labor-PC?
  0.0.0.0/0 -> br0 194.95.109.129 oder 130
  ::/0 -> br0 fe80::20c:29ff:fe45:e07c

4 IPv4 ANALYSE MIT WIRESHARK

- ☑ Warum sieht man die ersten beiden Pings nur im Wireshark an VMnet6?
  Weil sie ihr Ziel bereits über VMnet6 finden.

- ☑ Warum wird nur Ping zu 192.168.2.45 auch auf dem Wireshark an VMnet7 angezeigt?
  Weil der Router den Ping weiter leiten muss zum IPHost.

- ☑ Welches Protokoll oberhalb von IP wird für den Ping verwendet. Und welche Kommandos innerhalb dieses Protokolls werden benutzt?
  ICMP Echo Request, Type 8
  ICMP Echo Reply , Type 0

- ☑ Vergleichen Sie die IP-Identifikationen (IP-Header) der Meldungen beim letzten Ping auf beiden Wireshark und finden Sie die korrespondierenden Meldungen! Welche Protokoll-Schichten hat der Router bei der Weiterleitung an den korrespondierenden Meldungen verändert und welche nicht?
  Die gerouteten Meldungen haben die gleiche ID. Es wurde hauptsächlich Datalink verändert.

- ☑ Wurde der IP-Header verändert?
  Nur TTL wurde dekrementiert. Die IP-Adressen wurden NICHT verändert

- ☑ Wurden die MAC-Adressen verändert beim Routing?
  Ja, auf jeder Seite wurden die dortigen MAC-Adressen verwendet.

- ☑ Welche MAC-Adressen waren in welchem Subnetz zu sehen?
  Auf VMnet6 waren die MAC-Adressen vom Labor-PC und eth0 des Routers.
  Auf VMnet7 waren die MAC-Adressen von IPHost und eth1 des Routers.

- ☑ Wozu wird bei IPv4 das ARP Protokoll benötigt?
  Zum Auflösen der MAC-Adressen der unmittelbaren Nachbarn

- ☑ Welche Adresse wird mittels ARP in VMnet6 und welche in VMnet7 gesucht?
  192.168.1.1 und 192.168.1.5 in br6,
  192.168.2.2 und 192.168.2.45 in br7

- ☑ Wo werden die über ARP bezogenen MAC-Adressen später verwendet?
  Bei den Meldungen tauchen sie in den Zieladressen auf.

- ☑ Warum benutzt ARP für den Request eine Ethernet-Broadcast Adresse?
  Weil der Absender die MAC-Zieladresse nicht kennt.

- ☑ Wird die Broadcastmeldung auch auf das andere Netz weiter geleitet?
  Nein, bleibt nur innerhalb des Subnetzes (Broadcast Domain).

- ☑ Welche Protokollkennung hat ICMP im IP-Header?
  01

- ☑ Wie wird die IP-Adresse im IP-Header abgebildet. Das niederwertigste Byte zuerst oder zuletzt?
  Niederwertiges Byte zuletzt.

☑ Sind die IDs im IP-Header absteigend oder aufsteigend?
aufsteigend.

☑ Welcher TTL wird im IP-Header verwendet. Verändert der Router beim Weiterleiten diesen Wert und falls ja, wie und warum?
TTL=128, ja um endlos zirkulierende Pakete zu verhindern.

☑ Wurden die IP-Datenpakete fragmentiert oder nicht?
Nein laut Flagsfeld im IP-Header.

5 IPv6 ANALYSE MIT WIRESHARK

☑ Unterscheidet sich das ICMP von IPv4 mit dem ICMP von IPv6 bezüglich des Ping?
Ja, Kommandocode ist anders. Request=Type 128, Reply-Type 129

☑ Es ist kein ARP Protokoll zu erkennen. Woher weiß der Router die MAC-Adresse des jeweiligen Ziels?
Er benutzt das sog. Neighbor Discovery.

☑ Welches Protokoll wird für die Ermittlung der MAC-Adressen der unmittelbaren Nachbarn bei IPv6 verwendet?
Er benutzt das sog. Neighbor Discovery.

Haben Sie sog. Neighbor Solicitation und Neighbor advertisement Frames aufgezeiochnet? Tauchen darin die gesuchten MAC-Adressen auf?

Achtung: MAC Adresse kann abweichen!
Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: Vmware_c0:00:06 (**00:50:56:c0:00:06**), Dst: IPv6mcast_ff:00:00:05 (33:33:ff:00:00:05)
Destination: IPv6mcast_ff:00:00:05 (33:33:ff:00:00:05)
Source: Vmware_c0:00:06 (00:50:56:c0:00:06)
Type: IPv6 (0x86dd)
Internet Protocol Version 6, Src: fd00:0:0:1::1 (fd00:0:0:1::1), Dst: ff02::1:ff00:5 (ff02::1:ff00:5)
Internet Control Message Protocol v6
Type: 135 (Neighbor solicitation)
Code: 0
Checksum: 0x2a7a [correct]
Reserved: 0 (Should always be zero)
Target: fd00:0:0:1::5 (fd00:0:0:1::5)
ICMPv6 Option (Source link-layer address)
Type: Source link-layer address (1)
Length: 8
Link-layer address: 00:50:56:c0:00:06

Frame 2: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: Vmware_4b:89:c4 (00:0c:29:4b:89:c4), Dst: Vmware_c0:00:06 (00:50:56:c0:00:06)
Destination: Vmware_c0:00:06 (00:50:56:c0:00:06)
Source: Vmware_4b:89:c4 **(00:0c:29:4b:89:c4)**
Type: IPv6 (0x86dd)

Internet Protocol Version 6, Src: fd00:0:0:1::5 (fd00:0:0:1::5), Dst: fd00:0:0:1::1 (fd00:0:0:1::1)
Internet Control Message Protocol v6
Type: 136 (Neighbor advertisement)
Code: 0
Checksum: 0xee76 [correct]
Flags: 0xe0000000
Target: fd00:0:0:1::5 (fd00:0:0:1::5)
ICMPv6 Option (Target link-layer address)
Type: Target link-layer address (2)
Length: 8
Link-layer address: 00:0c:29:4b:89:c4

6 TRACEROUTE

☑ Betrachten Sie das IP-Feld TTL bei der Ausführung des ICMP-Request. Es hat den Wert 1. Was wird der nächste Empfänger damit machen?
IPRouer sendet ICMP Time-to-live-exceeded an Labor-PC (192.168.1.1)

☑ Wer sendet eine Antwort auf die erste ICMP-Request Meldung und wie sieht diese aus? Was bedeutet die Antwort und was kann der Empfänger damit anfangen?
Siehe oben

☑ Was passiert bei der ICMP-Request Meldung mit TTL=2. Wer sendet die Antwort und wie sieht diese aus.
Normales ICMP Reply von IPHost.

7 RECORD ROUTE

☑ Wann erfolgt der erste Eintrag in das Optionsfeld beim ICMP Request und welche Adresse wird eingetragen?
IPRouter trägt 192.168.2.2 ein.

☑ Gibt es auch einen Eintrag in das Optionsfeld beim ICMP Reply?
ja (abhängig von der Implementierung)

☑ Wie unterscheidet sich diese Adresse vom Ergebnis durch tracert?
tracert liefert 192.168.1.5 und RR liefert 192.168.2.2.