Fachhochschule Salzburg

Internet Infrastruktur und Sicherheit
4. Labor Protokoll

vom 04. Dezember 2013

Michael Haslauer
Daniela Pointinger | itsb-m2013

Version 0.1 | 3. Januar 2014

Inhaltsverzeichnis

1 Beschreibung

In der folgenden Übung wird das Neighbour Detection Protocol (NDP) von IPv6 näher untersucht und aktiv durchgeführt. Dabei wird die in Abbildung 1 gezeigte Topologie verwendet.

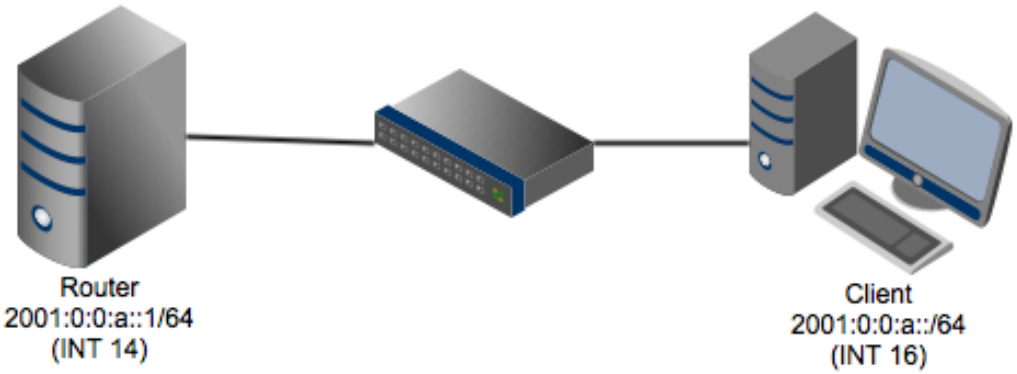

Abbildung 1: Netzwerktopologie der Übung

Ein Ubuntu Rechner fungiert hierbei als eine Art von DHCP Server. Bei IPv6 ist kein DHCP Server mehr notwendig um neuen Clients automatisch eine IP Adresse zuweisen zu können. Allerdings muss auf mindestens einem Rechner der sogenannte Route Advertisement Daemon (radvd) laufen um die Netzwerkkonfiguration im Netz zu verbreiten. Der zweite Rechner ist hierbei nur ein Client der neu ins Netzwerk integriert wird und dabei eine IP Adresse anfordert.

1.1 Konfiguration des radvd

Der Router Advertisement Daemon (radvd) ist ein Service der auf dem Rechner läuft und regelmäßig eine Router Advertisement über das Netzwerk schickt um sich neuen Clients bekannt zu machen. Außerdem reagiert er auf Router Solicitation Nachrichten von Clients. Der radvd muss dabei mit den entsprechenden Parametern konfiguriert werden. Listing 1 zeigt die radvd.conf des Service auf dem Rechner in der Übung.

```
interface eth1
{
        AdvSendAdvert on;
        AdvIntervalOpt on;
        MinRtrAdvInterval 1;
        MaxRtrAdvInterval 4;
        AdvHomeAgentFlag off;
        prefix 2001:0:0:a::/64
        {
                AdvOnLink on;
                AdvAutonomous on;
                AdvRouterAddr on;
        };
};
```

Listing 1: radvd.conf

In der ersten Zeile ist der Name des Interfaces (eth1) angegeben auf dem der Service lauscht. In den weiteren Zeilen kann die Router Advertisement an/aus geschalten werden und deren Verbreitungsintervall konfiguriert werden. Die wichtigste Zeile der Konfiguration ist `prefix`. Hier wird konfiguriert welche Netzinformation verbreitet wird. Im Fall dieser Übung handelt es sich um das Netz 2001:0:0:a::/64. Mittels radvd –C /etc/radvd.conf kann der Service gestartet werden. Der Parameter -C gibt dabei den Ort des Konfigurationsfiles.

Listing 2 zeigt die IPv6 Adressen des Ubuntu Routers am Interface eth1. Da bei IPv6 einem Interface mehrere Adressen zugewiesen werden können, ist es kein Problem dass dieses Interface mehrere globale Adressen hat. Außer den beiden globalen Adressen (IP: 2001:0:0:a::/64) hat das Interface auch eine Link-Local Adresse (FE80::/64) zugewiesen bekommen.

```
root@U460-15:/home/its# ifconfig
eth1  Link encap:Ethernet  HWaddr 18:a9:05:c3:f6:a1
      inet6 addr: 2001::a:1d8f:ac12:8a54:a9c5/64 Scope:Global
      inet6 addr: 2001::a:1aa9:5ff:fec3:f6a1/64 Scope:Global
      inet6 addr: fe80::1aa9:5ff:fec3:f6a1/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:117 errors:0 dropped:0 overruns:0 frame:0
      TX packets:237 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:31914 (31.9 KB)  TX bytes:48327 (48.3 KB)
      Interrupt:19 Memory:f0400000-f0420000
```

Listing 2: ifconfig des Ubuntu Routers

2 Neighbour Discovery Protocol Ablauf

Um einen neuen Ablauf des Protokolls zu initiieren wird das Interface eth1 des Clients, das mit dem Router verbunden ist, neu hochgefahren. Als erstes wird dabei vom Client eine Router Solicitation Nachricht gesendet um die Konfiguration vom Router zu erhalten. Dieser antwortet mit einer Router Advertisement Nachricht an den Client. Daraufhin baut sich der Client aus den nun bekannten Präfixen aus der Router Advertisement Nachricht und seiner Hardwareadresse des Interfaces eine IP Adresse zusammen. Danach sendet der Client eine Neighbor Solicitation Nachricht (siehe Abbildung 2) an alle Clients im Netzwerk. Sofern kein anderer Rechner mit einer Neighbor Advertisement antwortet, so weis der ursprüngliche Client, dass diese Adresse frei ist und kann diese ab sofort benutzen.

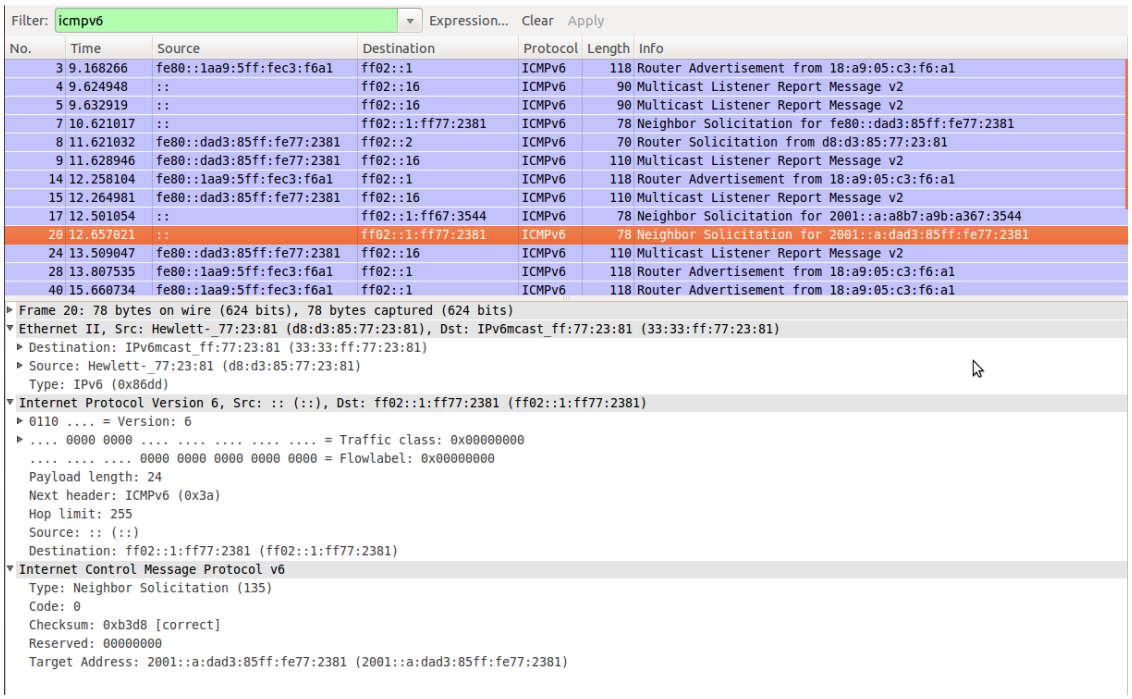

Abbildung 2: Wireshark Neighbor-Solicitation-Nachricht

Listing 3 zeigt den beschriebenen Ablauf im Wireshark Protokoll. Wenn an die IPv6 Adresse `ff02::2` Pakete gesendet werden, erhalten das alle Router im Netzwerk. Bei der Adresse `ff02::1` werden die Daten an alle Hosts im Netzwerk gesendet.

```
No. | Source | Destination | Info
1 | fe80::dad3:85ff:fe77:2381 | ff02::2 | Router Solicitation
2 | fe80::1aa9:05ff:fec3:f6a1 | ff02::1 | Router Advertisement
3 | :: | ff02::1:ff67:3544 | Neighbor Solicitation
4 | :: | ff02::1:ff77:2381 | Neighbor Solicitation
```

Listing 3: Wireshark

Nach erfolgreicher Durchführung des Neighbour Discovery Protocols kann mit dem Befehl `ifconfig` die Konfiguration überprüft werden. Listing 4 zeigt die IP Konfiguration des Clients nach der Durchführung.

```
root@U460-16:/home/its# ifconfig
eth1  Link encap:Ethernet  HWaddr d8:d3:85:77:23:81
      inet6 addr: 2001::a:dad3:85ff:fe77:2381/64 Scope:Global
      inet6 addr: fe80::dad3:85ff:fe77:2381/64 Scope:Link
      inet6 addr: 2001::a:a8b7:a9b:a367:3544/64 Scope:Global
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:849 errors:0 dropped:0 overruns:0 frame:0
      TX packets:428 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:132118 (132.1 KB)  TX bytes:82430 (82.4 KB)
      Interrupt:19 Memory:f0400000-f0420000
```

Listing 4: IP Konfiguration des Clients

Hier erkennt man, dass der Client sich nun die IP Adresse 2001::a:dad3:85ff:fe77:2381/64 mittels Autokonfiguration zugewiesen hat. Diese enthält dabei das vom Router verbreitete

Prefix 2001:0:0:a::/64. Anschließend konnten sich der Router und der Client über diese IPv6 Adressen gegenseitig erreichen. Überprüft wurde das durch einen Ping-Versuch (siehe Listing 5).

```
root: ping6 -I eth1 2001::a:dad3:85ff:fe77:2381
PING 2001::a:dad3:85ff:fe77:2381 from 2001::a:1d8f:ac12:8a54:
   a9c5 eth1: 56 data bytes
64 bytes from 2001::a:dad3:85ff:fe77:2381: icmp_seq=1 ttl=64
   time=0.424 ms
64 bytes from 2001::a:dad3:85ff:fe77:2381: icmp_seq=2 ttl=64
   time=0.191 ms
64 bytes from 2001::a:dad3:85ff:fe77:2381: icmp_seq=3 ttl=64
   time=0.226 ms

--- 2001::a:dad3:85ff:fe77:2381 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.191/0.280/0.424/0.103 ms
```

Listing 5: Ping an Client

3 Fragen

3.1 Welche Nachrichten stehen im Neighbour Discovery Protocol zur Verfügung?

Das NDP nutz ICMPv6 um die Informationen im Netzwerk auszutauschen. Es definiert dabei folgende 5 verschiedene Nachrichten.

- **Router Solicitation:** Mittles dieser Nachricht werden von Clients eine Router Advertisement von allen Routern im Netzwerk angefordert.
- **Router Advertisement:** Damit antworten Router auf Router Solicitation Nachrichten um die IP Konfiguration im Netzwerk zu verteilen. Neben den Antworten auf Router Solicitation Nachrichten senden Router diese Nachricht auch periodisch ins Netzwerk.
- **Neighbor Solicitation:** Damit testen Clients ihre ausgewählten IP Adressen im Netzwerk ob diese auch eindeutig sind oder bereits vergeben. Bekommen Clients keine Antwort auf ihre Neighbor Solicitation Nachricht so nehmen sie ihre Adresse als gültig an.
- **Neighbor Advertisement:** Diese Nachricht wird gesendet falls ein Client bereits die IP Adresse besitzt die ein anderer Client über eine Neighbor Solicitation Nachricht verbreitet. Damit wird dem neuen Client bekannt gemacht, dass er eine andere IP Adresse wählen muss.
- **Redirect:** Mittels einer Redirect Nachricht können Router bessere Routen bekannt geben sofern es einen anderen besseren ersten Hop gibt zu gewissen Zielen.

3.2 Welche Nachrichten in der IPv4 Welt werden dadurch das NDP IPv6 ersetzt?

Das NDP von IPv6 ersetzt mit seinen verfügbaren Nachrichten das Address Resolution Protocol (ARP) von IPv4. Dabei verwaltet jeder Client eigene Address-Caches bei dem zu jeder IPv6-Adresse eine Link-Layer Adresse steht. Die Link-Layer Adressen von Clients werden dabei über Neighbor-Solicitation-Nachrichten erfragt.

3.3 Wie funktioniert der Address Autoconfiguration Mechanismus?

Als allererstes konfiguriert sich der Client eine Link-local-Adresse die er aus dem Prefix FE80 und seinem Interface Indentifier zusammenbaut. Danach generiert der Client die Solicited-Node Multicast Adresse und sendet eine Neighbor Solicitation Nachricht an die Solicited-Node Multicast Adresse. Sofern kein Client antwortet ist diese Adresse nicht vergeben und kann vom ursprünglichen Client verwendet werden. Ist dieser Fall eingetreten sendet der Client anschließend eine Router Solicitation Nachricht an alle Router (FE02::2) um die Netzwerkinformationen zu erhalten. Mit den Informationen aus der Router Advertisement Nachricht kann sich der Client nun eine Global Unicast Adresse konfigurieren und ist nun bereit im Internet zu kommunizieren.

3.4 Erläutern Sie den Neighbour Unreachability Detection Mechanismus?

Der Neighbour Unreachability Detection Mechanismus ist Teil des Neighbour Discovery Protocols und wird verwendet um die Adress-Caches der Clients auf dem neuesten Stand zu halten. Sofern regelmäßig mit einem Client kommuniziert wird ist die Neighbour Unreachability Detection nicht notwendig. Überschreitet ein Eintrag im Adress-Cache allerdings seinen Gültigkeitszeitraum ohne das eine Kommunikation stattgefunden hat, so wird überprüft ob der Client noch verfügbar ist. Zuerst wird versucht die Erreichbarkeit des anderen Clients mittels normaler Kommunikation zu bestätigen. Antwortet dieser nicht so wird anschließend eine Neighbor-Solicitation-Nachricht für diesen Client versendet. Erhält der Client wieder keine Antwort so wird der Kommunikationspartner aus dem Adress-Cache entfernt.

3.5 Wie wird eine Duplicate Address Detection durchgeführt? Wer ist daran beteiligt?

Die Duplicate Address Detection ist Teil des Neighbor Discovery Protocols und wird bei der Address Autoconfiguration verwendet. Während der Address Autokonfiguration muss der Client überprüfen ob die von ihm gewählte Adresse noch frei ist. Dazu sendet er eine Neighbor Solicitation Nachricht an die vorher generierte Solicited-Node Multicast Adresse. Antwortet ihm daraufhin ein anderer Client mit einer Neighbor Advertisement Nachricht auf der All-Nodes Multicast Adresse so ist diese Adresse bereits vergeben und es muss eine manuelle Konfiguration vorgenommen werden. Erhält der Client hingegen keine Antwort so gilt die gewählte Adresse als nicht vergeben und kann vom Client verwendet werden. An der Duplicate Address Detection sind somit alle Clients am selben Link beteiligt.

3.6 Welche Sicherheitsrisiken bestehen bei NDP IPv6?

Wie beim DHCP-Spoofing können Clients im Netzwerk nicht kontrollieren von wem die Informationen gesendet werden und ob diese korrekt sind oder verfälscht. Ein Angreifer kann sich demnach, sofern er sich bereits im Netzwerk befindet, als Router ausgeben und gefälschte IP Konfigurationen im Netzwerk verbreiten. Außerdem kann ein Angreifer feststellen welche IP Adressen im Netzwerk bereits verwendet sind und auch auf Neighbor Solicitation Nachrichten mit gefälschten Neighbor Advertisement antworten.

3.7 Wie kann die Sicherheit verbessert werden?

Für das NDP gibt es eine Erweiterung namens SEND (SEcure Neighbor Discovery). Dieses erweitert das NDP um einen Sicherheitsmechanismus der auf Zertifikaten und einer Public-Key-Infrastrutur basiert. Dabei dürfen nur mehr Router eine Konfiguration im Netzwerk verbreiten die sich über ein Zertifikat ausweisen können. Dieses Zertifikat wird dabei von den Clients überprüft bevor sie die Konfiguration annehmem.

Abbildungsverzeichnis

Listings