

Internet Infrastruktur und Sicherheit

4. Labor Protokoll

vom 04. Dezember 2013

Michael Haslauer
Daniela Pointinger | itsb-m2013

Version 0.1 | 4. Dezember 2013

Inhaltsverzeichnis

1	Beschreibung	2
1.1	Konfiguration des radvd	2
2	Neighbour Discovery Protocol Ablauf	3
3	Fragen	3
3.1	Welche Nachrichten stehen im Neighbour Discovery Protocol zur Verfügung?	3
3.2	Welche Nachrichten in der IPv4 Welt werden dadurch das NDP IPv6 ersetzt?	4
3.3	Wie funktioniert der Address Autoconfiguration Mechanismus?	4
3.4	Erläutern Sie den Neighbour Unreachability Detection Mechanismus?	4
3.5	Wie wird eine Duplicate Address Detection durchgeführt? Wer ist daran beteiligt?	4
3.6	Welche Sicherheitsrisiken bestehen bei NDP IPv6?	4
3.7	Wie kann die Sicherheit verbessert werden?	4
	Abbildungsverzeichnis	5
	Listings	5

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. Ein Ubuntu Rechner fungiert hierbei als eine Art von DHCP Server. Bei IPv6 ist

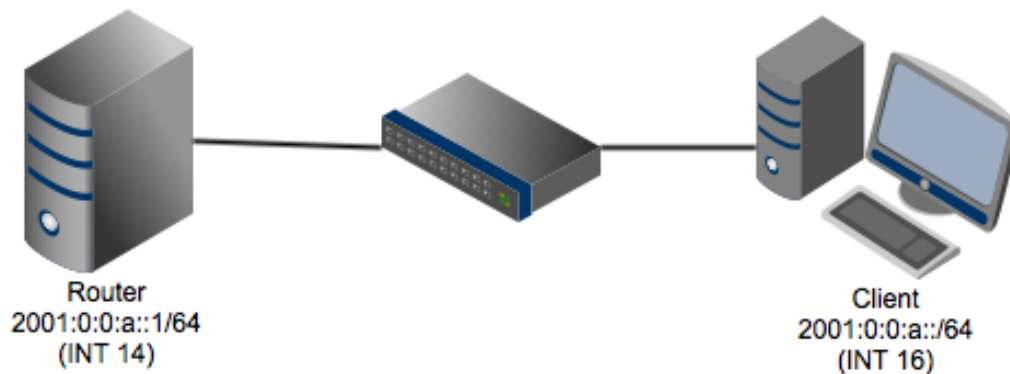


Abbildung 1: Netzwerktopologie der Übung

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 Route 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 geschaltet 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.

TODO: `ifconfig` des Routers einfügen mir Erklärung.

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. Daraufhin sendet der Client eine Neighbor Solicitation an alle Clients im Netzwerk. Sofern kein anderer Rechner mit einer Neighbor Advertisement antwortet, so weiß der ursprüngliche Client, dass diese Adresse frei ist und kann diese ab sofort benutzen.

TODO: Einfügen von Wireshark mitgeschnittenem

Nach erfolgreicher Durchführung des Neighbour Discovery Protocols kann mit dem Befehl `ifconfig` die Konfiguration überprüft werden. Listing 2 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 2: 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.

3 Fragen

3.1 Welche Nachrichten stehen im Neighbour Discovery Protocol zur Verfügung?

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

- Router Solicitation: Mittels 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?

3.3 Wie funktioniert der Address Autoconfiguration Mechanismus?

3.4 Erläutern Sie den Neighbour Unreachability Detection Mechanismus?

3.5 Wie wird eine Duplicate Address Detection durchgeführt? Wer ist daran 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-Infrastruktur 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 annehmen.

Abbildungsverzeichnis

1	Netzwerktopologie der Übung	2
---	---------------------------------------	---

Listings

1	radvd.conf	2
2	IP Konfiguration des Clients	3