Bab X - Troubleshooting IPV6

Iljitsch van Beijnum

tcpdump

- Secara umum, aplikasi tcpdump mengintercep paket data dan interface jaringan, kemudian menampilkan isinya, mendekode beberapa protokolnya pada proses.
- dua mekanisme yang digunakan untuk mengintercep dan menampilkan paket: Packet Capture library (pcap library or libpcap) dan Berkeley Packet Filter (BPF).

Tcpdumping ICMPv6

Tcpdump digunakan sebagai monitoring fungsi ICMPv6. termasuk router advertisements dan

```
# tcpdump
tcpdump: listening on eth0
13:33:33.436664 fe80::204:27ff:fefe:249f > ff02::1: icmp6: router advertisement➥
[class 0xe0]

1 packets received by filter
0 packets dropped by kernel
```

- Mendekode Neighbor Discovery

```
# tcpdump -v -s 0 -e
tcpdump: listening on eth0
15:02:27.471601 0:a:95:f5:24:6e 33:33:ff:29:23:b6 ip6 86: host3.example.com > ➥
ff02::1:ff29:23b6: icmp6: neighbor sol: who has host5.example.com(src lladdr: ➥
00:0a:95:f5:24:6e) (len 32, hlim 255)
15:02:27.471708 0:1:2:29:23:b6 0:a:95:f5:24:6e ip6 86: host5.example.com > host3 ➥
.example.com: icmp6: neighbor adv: tgt is host5.example.com(SO)(tgt lladdr: 00:0 ➥
1:02:29:23:b6) (len 32, hlim 255)
```

tcpdumping UDP

```
# tcpdump
tcpdump: listening on eth0
13:12:33.935061 host5.example.com.32782 > ns.example.com.domain:  15025+ AAAA?  ➥
ns.example.com. (32)
13:12:33.948362 host5.example.com.domain > host5.example.com.32782:  15025* 1/2/2  ➥
(148)
```

- Untuk paket DNS, tcpdump menampilkan identifier, tipe, dan nama pada setiap informasi yang diminta. Nilai terakhir dari panjang DNS paket, kecuali panjang IP dan UDP header.

tcpdumping TCP

- Hasil dari tcpdump mendapatkan nilai bit dan decipher ketika menangkap TCP, karena TCP

ripada

```
% sudo tcpdump
tcpdump: WARNING: en0: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on en0, link-type EN10MB (Ethernet), capture size 96 bytes
14:32:35.468540 host3.example.com.58231 > ns.example.com.domain: S 2265400865: ➥
2265400865(0) win 65535 <mss 1440,nop,wscale 0,nop,nop,timestamp 631301731 0>
14:32:35.484974 ns.example.com.domain > host3.example.com.58231: S 3739752857: ➥
3739752857(0) ack 2265400866 win 57344 <mss 1220> [flowlabel 0x6c66e]
14:32:35.485197 host3.example.com.58231 > ns.example.com.domain: . ack 1 win 65535
14:32:35.485722 host3.example.com.58231 > ns.example.com.domain: P 1:35(34) ack 1  ➥
win 65535 45278+[|domain]
14:32:35.503456 ns.example.com.domain > host3.example.com.58231: P 1:151(150) ack  ➥
35 win 58560 45278*[|domain] [flowlabel 0x6c6bd]
14:32:35.507729 host3.example.com.58231 > ns.example.com.domain: F 35:35(0) ack  ➥
151 win 65535
```

Promiscuity

- Tcpdump akan mencoba meletakkan interface ke dalam “promiscuous mode”, jadi dapat menarik semua paket dari kabel daripada hanya satu alamat pada MAC addressnya sendiri. Promiscuous mode, tentunya hanya diaplikasikan pada interfaces yang menggunakan MAC address, seperti Ethernet.

Filter

- Filtre sederhana dapat dilihat pada pengalamatan seperti nomor port, memastikan ditandai oleh identifier protokol. Contoh:

➢ Ip : melihat paket IPv4
➢ Ipv6: melihat paket IPv6
➢ host (alamat _ip) : melihat paket dengan IPv4 atau IPv6
➢ host (nama_domain) : melihat paket dngan nama domain
➢ dll

Konektivitas IPv6

- Ketersediaan alamat dan kesalahan DAD

```
netsh interface ipv6>show address
Querying active state...

Interface 5: Local Area Connection 3

Addr Type  DAD State  Valid Life   Pref. Life   Address
---------  ---------- ------------ ------------ ---------------------------
Temporary  Preferred   6d23h59m39s    23h56m52s 2001:db8:31:2:ff8f:41ae:c9f6:a97
Public     Duplicate  29d23h59m58s  6d23h59m58s 2001:db8:31:2:201:2ff:fe29:23b6
Link       Preferred      infinite     infinite fe80::201:2ff:fe29:23b6
```

- ndp

Ndp digunakan sebagai menampilkan informasi pada neightbor discovery, termasuk router advertisements dan konfigurasi otomatis pada BSD

```
% ndp -an
Neighbor                        Linklayer Address  Netif Expire    St Flgs Prbs
::1                             (incomplete)         lo0 permanent R
2001:1af8:6::20a:95ff:fef5:246e 0:a:95:f5:24:6e      en1 permanent R
fe80::1%lo0                     (incomplete)         lo0 permanent R
fe80::204:27ff:fefe:249f%en1    0:4:27:fe:24:9f      en1 23h57m56s S  R
fe80::20a:95ff:fef5:246e%en1    0:a:95:f5:24:6e      en1 permanent R
```

- Traceroute6

Jika sistem terdapat kedua routing IPv6 dan penggunakan global unicast, dapat menggunakan traceroute6.

```
% netstat -n | more
Active Internet connections
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp6       0      0  2001:db8:31::20a.55858 3ffe:ffff:2310:2.993 ESTABLISHED
tcp4       0      0  192.0.2.6.55672        192.0.2.225.22        ESTABLISHED
tcp6       0      0  2001:db8:31::20a.52731 2001:db8:2:5::2.80    CLOSE_WAIT
udp6       0      0  *.5353                 *.*
udp4       0      0  *.5353                 *.*
```

Memindahkan versi IP

- Ada 4 langkah untuk memindahkan versi IP yaitu:
  - Menggunakan mekanisme aplikasi.
  - Memilih nama DNS hanya IPv4 atau IPv6
  - Menggunakan alamat literal
  - Memodifikasi tabel address policy untuk memberikan protokol yang diinginkan maupun yang tidak diinginkan.

Path MTU Discovery dan Fragmentasi

- Pada IPv4, Path MTU Discovery menyebabkan banyak masalah yang mana digunakan sebagai

```
# ping6 -c 1 www.kame.net
PING www.kame.net(orange.kame.net) 56 data bytes
64 bytes from orange.kame.net: icmp_seq=1 ttl=47 time=345 ms

--- www.kame.net ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 345.453/345.453/345.453/0.000 ms
# ip -6 route get 2001:200:0:8002:203:47ff:fea5:3085
2001:200:0:8002:203:47ff:fea5:3085 via fe80::204:27ff:fefe:249f dev eth0  proto ➥
kernel  src 2001:db8:31:2:201:2ff:fe29:23b6 metric 1024 expires 59sec mtu 1500 ➥
advmss 1440
```