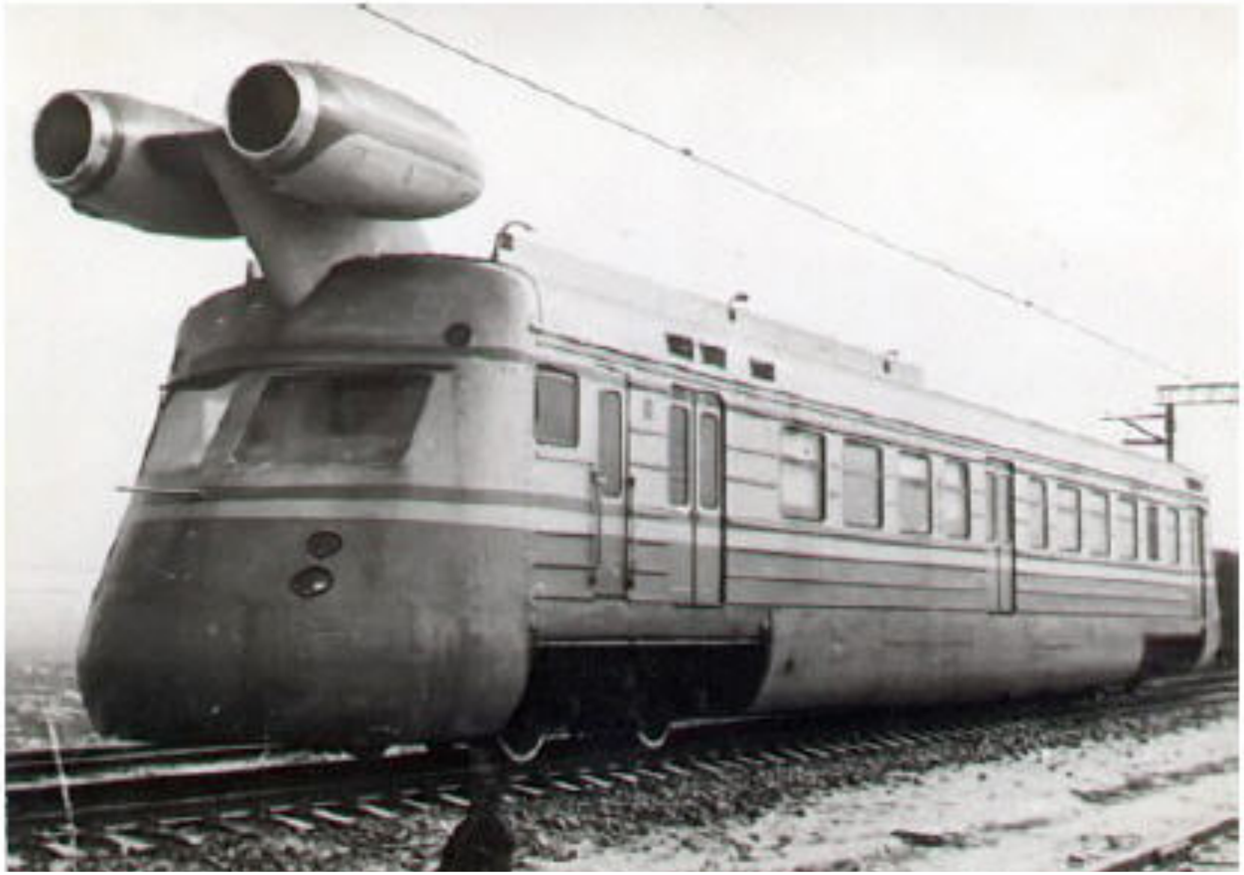


IPv6 – Security Issues

(IPSec does solve everything)

Tomáš Podermański, tpoder@cis.vutbr.cz

IPv6 security

- IPv6 provides better security than IPv4 for applications and networks

- How does IPv6 provide a solution?

  In IPv6, **IPSec** is a major protocol requirement and is one of the factors in ensuring that IPv6 provides better security than IPv4.

  The large address space also prevents networks against **address scanning**.

Source: http://www.ipv6.com/

Scanning

- The huge address space prevents scanning
  - Brute force scanning on a network with prefix /64 would take 28 years until the first active address found. That means 1 mln tests per second and traffic 400Mb/s.
  - RFC 5157 IPv6 - Implications for Network Scanning
  - Privacy extension for Stateless Address Autoconf. (RFC 4941)
- New ways to find active IPv6 addresses
  - DNS, whois, logs, Flow, NI Query (RFC 4620), well known MAC address, existing IPv4 address, transition mechanisms
  - vanHauser – Ministry of Truth (http://www.youtube.com/watch?v=c7hq2q4jQYw)
  - 2000 active addresses were found in 20 seconds !!
- Scanning on the local network
  - Ping FF02::1
  - Information obtained from neighbor cache (or sniffing on FF02::1)

ICMPv6 (RFC 2463)

- Completely differed comparing to IPv4
- IPv6 can not work without ICMPv6
  - Neighbor Discovery (NDP)
  - Stateless Autoconfiguration (RS, RA)
  - Working with multicast groups (MLD)
  - Diagnostics (PING)
  - Signalization
    - Destination Unreachable
    - Time exceeded
    - **Packet to Big**
    - Redirection
  - …

ICMPv6 - Neighbor Discovery

- Neighbor cache spoofing
  - Very similar to ARP spoofing
  - The spoofed address can be kept in the NC longer
- DoS - Duplicate Address Detection (DAD)
  - Nodes usually create own address (EUI 64, Privacy Extensions)
  - (Optimistic) DAD – “sorry, the address is mine, choose another”
- Neighbor Cache Table Overload
  - Big address space (64 bits – 1.8e+19 address)
  - Many records in the NC for non existing clients
- Rouge Router Advertisement
  - I am a router for this network – use me as a default router
  - The real router is not a valid anymore – zero lifetime
- Rouge DHCPv6 Server
  - I am a DHCPv6 sever for this network. Use my options (DNS)

IPv6 Attack Tools

- **Scanners** – Nmap, halfscan6, Scan6, CHScanner
- **Packet forgery** – Scapy6, SendIP, Packit, Spak6
- **DoS Tools** – 6tunneldos, 4to6ddos, Imps6-tools

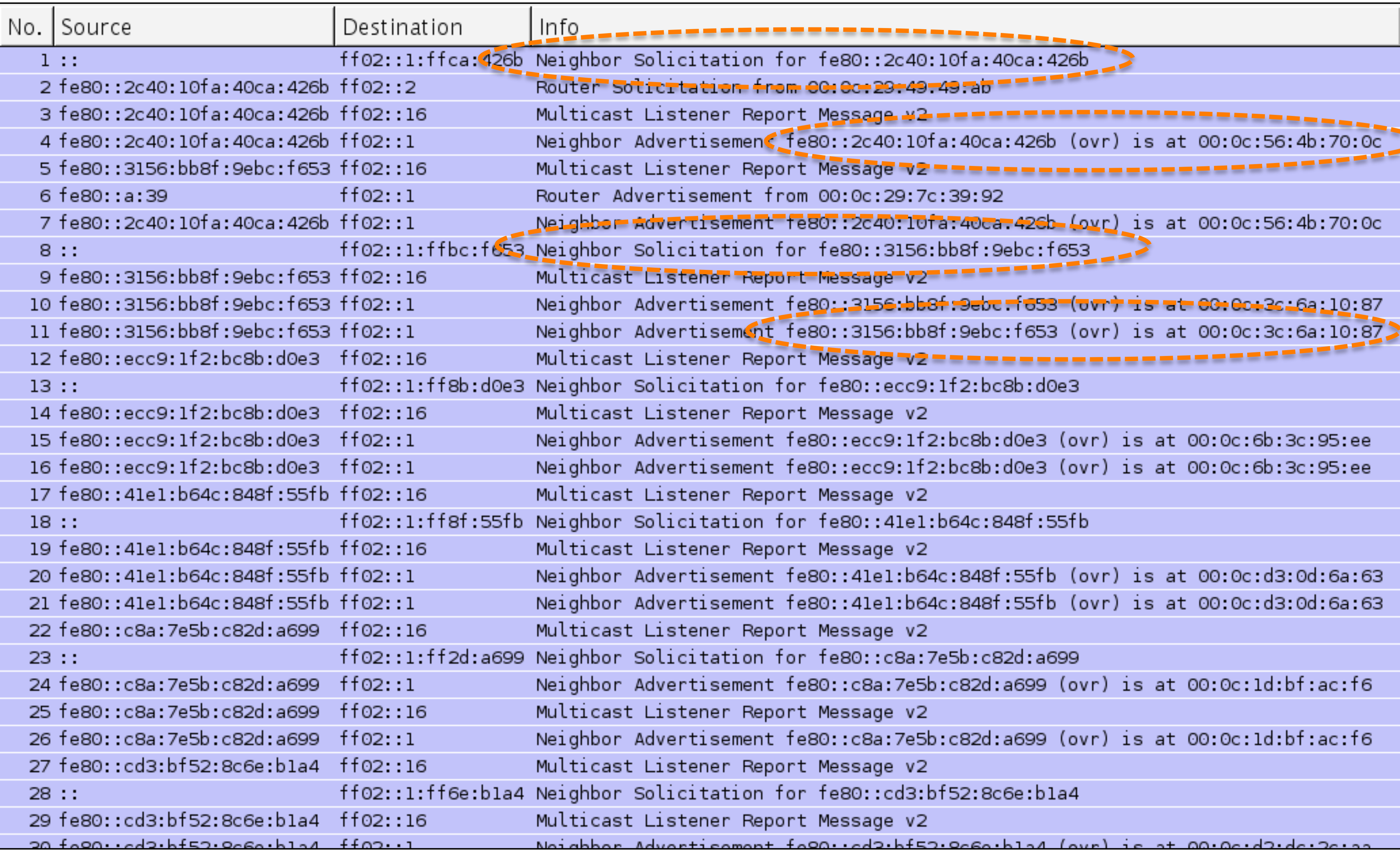
The Hacker's Choice

- **THC IPv6 Attack Toolkit** – parasite6, alive6, fake_router6, redir6, toobig6, detect-new-ip6, dos-new-ip6, fake_mld6, fake_mipv6, fake_advertiser6, smurf6, rsmurf6

  http://freeworld.thc.org/

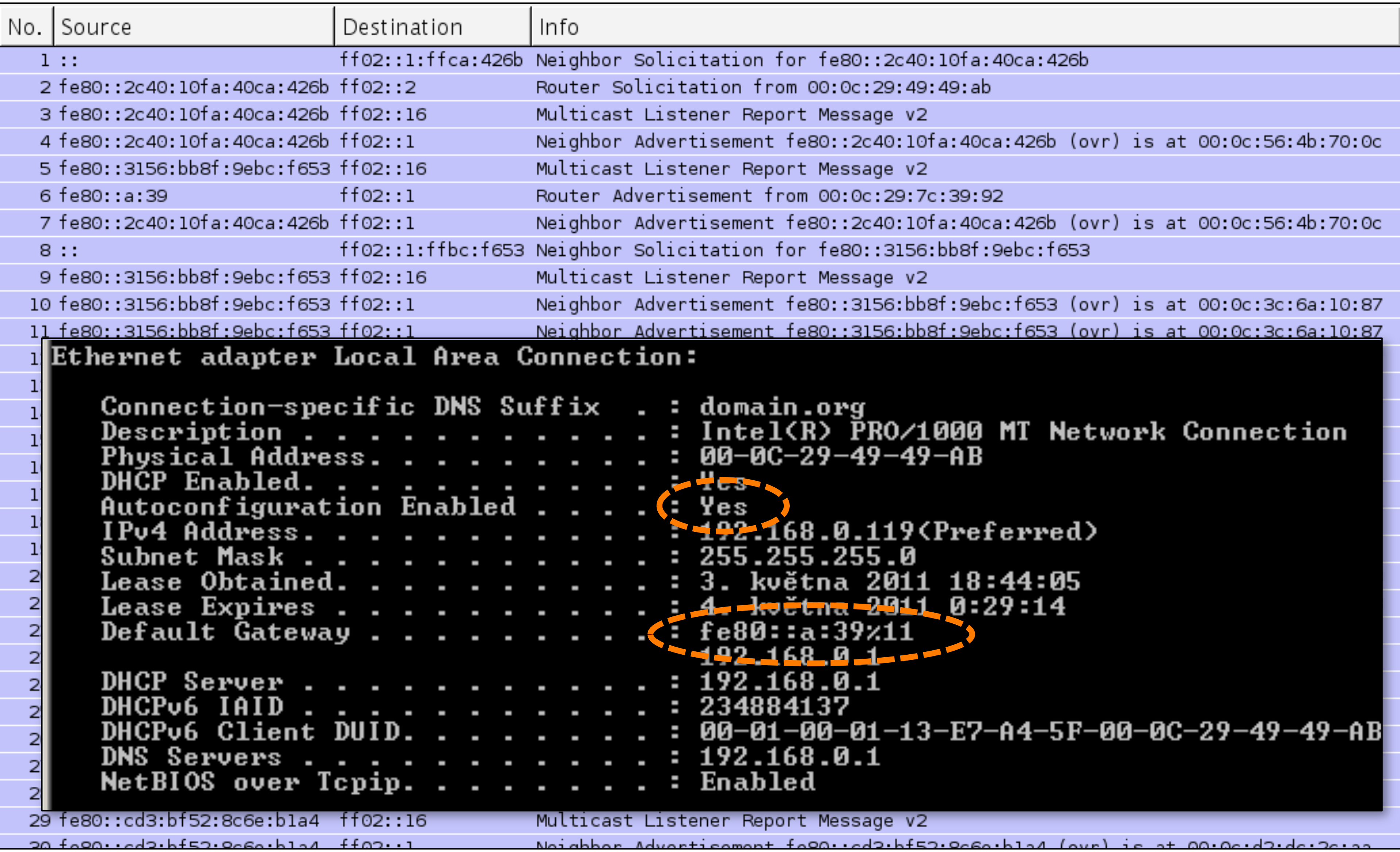
```
# ./dos-new-ipv6 eth0
```

DAD – DoS attack



No.	Source	Destination	Info
1	::	ff02::1:ffca:426b	Neighbor Solicitation for fe80::2c40:10fa:40ca:426b
2	fe80::2c40:10fa:40ca:426b	ff02::2	Router Solicitation from 00:0c:29:49:49:ab
3	fe80::2c40:10fa:40ca:426b	ff02::16	Multicast Listener Report Message v2
4	fe80::2c40:10fa:40ca:426b	ff02::1	Neighbor Advertisement fe80::2c40:10fa:40ca:426b (ovr) is at 00:0c:56:4b:70:0c
5	fe80::3156:bb8f:9ebc:f653	ff02::16	Multicast Listener Report Message v2
6	fe80::a:39	ff02::1	Router Advertisement from 00:0c:29:7c:39:92
7	fe80::2c40:10fa:40ca:426b	ff02::1	Neighbor Advertisement fe80::2c40:10fa:40ca:426b (ovr) is at 00:0c:56:4b:70:0c
8	::	ff02::1:ffbc:f653	Neighbor Solicitation for fe80::3156:bb8f:9ebc:f653
9	fe80::3156:bb8f:9ebc:f653	ff02::16	Multicast Listener Report Message v2
10	fe80::3156:bb8f:9ebc:f653	ff02::1	Neighbor Advertisement fe80::3156:bb8f:9ebc:f653 (ovr) is at 00:0c:3c:6a:10:87
11	fe80::3156:bb8f:9ebc:f653	ff02::1	Neighbor Advertisement fe80::3156:bb8f:9ebc:f653 (ovr) is at 00:0c:3c:6a:10:87
12	fe80::ecc9:1f2:bc8b:d0e3	ff02::16	Multicast Listener Report Message v2
13	::	ff02::1:ff8b:d0e3	Neighbor Solicitation for fe80::ecc9:1f2:bc8b:d0e3
14	fe80::ecc9:1f2:bc8b:d0e3	ff02::16	Multicast Listener Report Message v2
15	fe80::ecc9:1f2:bc8b:d0e3	ff02::1	Neighbor Advertisement fe80::ecc9:1f2:bc8b:d0e3 (ovr) is at 00:0c:6b:3c:95:ee
16	fe80::ecc9:1f2:bc8b:d0e3	ff02::1	Neighbor Advertisement fe80::ecc9:1f2:bc8b:d0e3 (ovr) is at 00:0c:6b:3c:95:ee
17	fe80::41e1:b64c:848f:55fb	ff02::16	Multicast Listener Report Message v2
18	::	ff02::1:ff8f:55fb	Neighbor Solicitation for fe80::41e1:b64c:848f:55fb
19	fe80::41e1:b64c:848f:55fb	ff02::16	Multicast Listener Report Message v2
20	fe80::41e1:b64c:848f:55fb	ff02::1	Neighbor Advertisement fe80::41e1:b64c:848f:55fb (ovr) is at 00:0c:d3:0d:6a:63
21	fe80::41e1:b64c:848f:55fb	ff02::1	Neighbor Advertisement fe80::41e1:b64c:848f:55fb (ovr) is at 00:0c:d3:0d:6a:63
22	fe80::c8a:7e5b:c82d:a699	ff02::16	Multicast Listener Report Message v2
23	::	ff02::1:ff2d:a699	Neighbor Solicitation for fe80::c8a:7e5b:c82d:a699
24	fe80::c8a:7e5b:c82d:a699	ff02::1	Neighbor Advertisement fe80::c8a:7e5b:c82d:a699 (ovr) is at 00:0c:1d:bf:ac:f6
25	fe80::c8a:7e5b:c82d:a699	ff02::16	Multicast Listener Report Message v2
26	fe80::c8a:7e5b:c82d:a699	ff02::1	Neighbor Advertisement fe80::c8a:7e5b:c82d:a699 (ovr) is at 00:0c:1d:bf:ac:f6
27	fe80::cd3:bf52:8c6e:b1a4	ff02::16	Multicast Listener Report Message v2
28	::	ff02::1:ff6e:b1a4	Neighbor Solicitation for fe80::cd3:bf52:8c6e:b1a4
29	fe80::cd3:bf52:8c6e:b1a4	ff02::16	Multicast Listener Report Message v2
30	fe80::cd3:bf52:8c6e:b1a4	ff02::1	Neighbor Advertisement fe80::cd3:bf52:8c6e:b1a4 (ovr) is at 00:0c:d2:dc:2c:aa

DAD – DoS attack



```
No. Source                     Destination       Info
  1 ::                         ff02::1:ffca:426b Neighbor Solicitation for fe80::2c40:10fa:40ca:426b
  2 fe80::2c40:10fa:40ca:426b  ff02::2           Router Solicitation from 00:0c:29:49:49:ab
  3 fe80::2c40:10fa:40ca:426b  ff02::16          Multicast Listener Report Message v2
  4 fe80::2c40:10fa:40ca:426b  ff02::1           Neighbor Advertisement fe80::2c40:10fa:40ca:426b (ovr) is at 00:0c:56:4b:70:0c
  5 fe80::3156:bb8f:9ebc:f653  ff02::16          Multicast Listener Report Message v2
  6 fe80::a:39                 ff02::1           Router Advertisement from 00:0c:29:7c:39:92
  7 fe80::2c40:10fa:40ca:426b  ff02::1           Neighbor Advertisement fe80::2c40:10fa:40ca:426b (ovr) is at 00:0c:56:4b:70:0c
  8 ::                         ff02::1:ffbc:f653 Neighbor Solicitation for fe80::3156:bb8f:9ebc:f653
  9 fe80::3156:bb8f:9ebc:f653  ff02::16          Multicast Listener Report Message v2
 10 fe80::3156:bb8f:9ebc:f653  ff02::1           Neighbor Advertisement fe80::3156:bb8f:9ebc:f653 (ovr) is at 00:0c:3c:6a:10:87
 11 fe80::3156:bb8f:9ebc:f653  ff02::1           Neighbor Advertisement fe80::3156:bb8f:9ebc:f653 (ovr) is at 00:0c:3c:6a:10:87
 29 fe80::cd3:bf52:8c6e:b1a4   ff02::16          Multicast Listener Report Message v2
 30 fe80::cd3:bf52:8c6e:b1a4   ff02::1           Neighbor Advertisement fe80::cd3:bf52:8c6e:b1a4 (ovr) is at 00:0c:d2:dc:2c:aa
```

```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : domain.org
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-49-49-AB
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.0.119(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 3. května 2011 18:44:05
   Lease Expires . . . . . . . . . . : 4. května 2011 0:29:14
   Default Gateway . . . . . . . . . : fe80::a:39%11
                                       192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 234884137
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-13-E7-A4-5F-00-0C-29-49-49-AB
   DNS Servers . . . . . . . . . . . : 192.168.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

It is not a problem

There are not enough services available on IPv6.
We have plenty of time to solve it and
implement a proper solution.

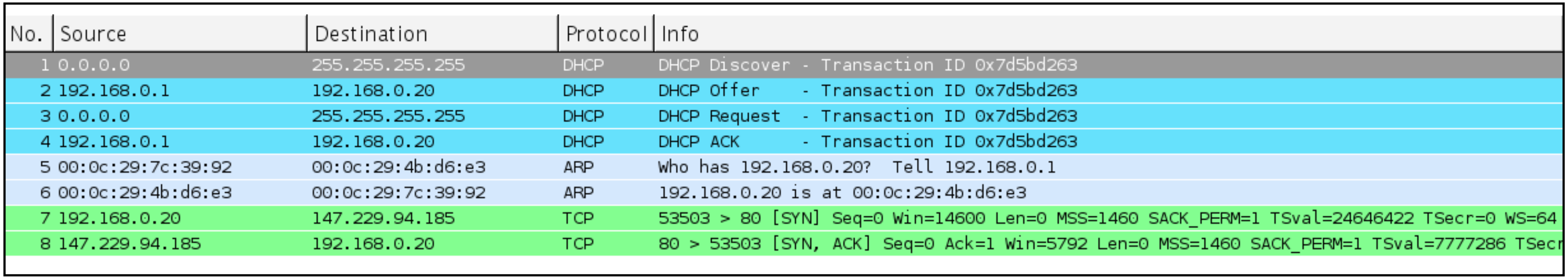
Really ? Do we ?

Autoconfiguration – SLAAC, DHCPv6

- SLAAC **does not contain addresses of DNS servers**
  - Obtain via another protocol (DHCPv4, DHCPv6)
  - Anycast address for recursive DNS servers
  - New option in RA (RFC 6106) – lack of implementation
- DHCP was not planned for IPv6
  - The first RFC 3315 (2003)
  - Coexistence with SLAAC (flags M,O)
  - **Does not contain the address of a default router**
- We have to use both mechanisms in IPv6-only networks
- Different platforms support different techniques
  - Windows Vista/7 – SLAAC + DHCPv6
  - MAC OS, iOS - SLAAC only
  - Linux, BSD, … – depends on distribution

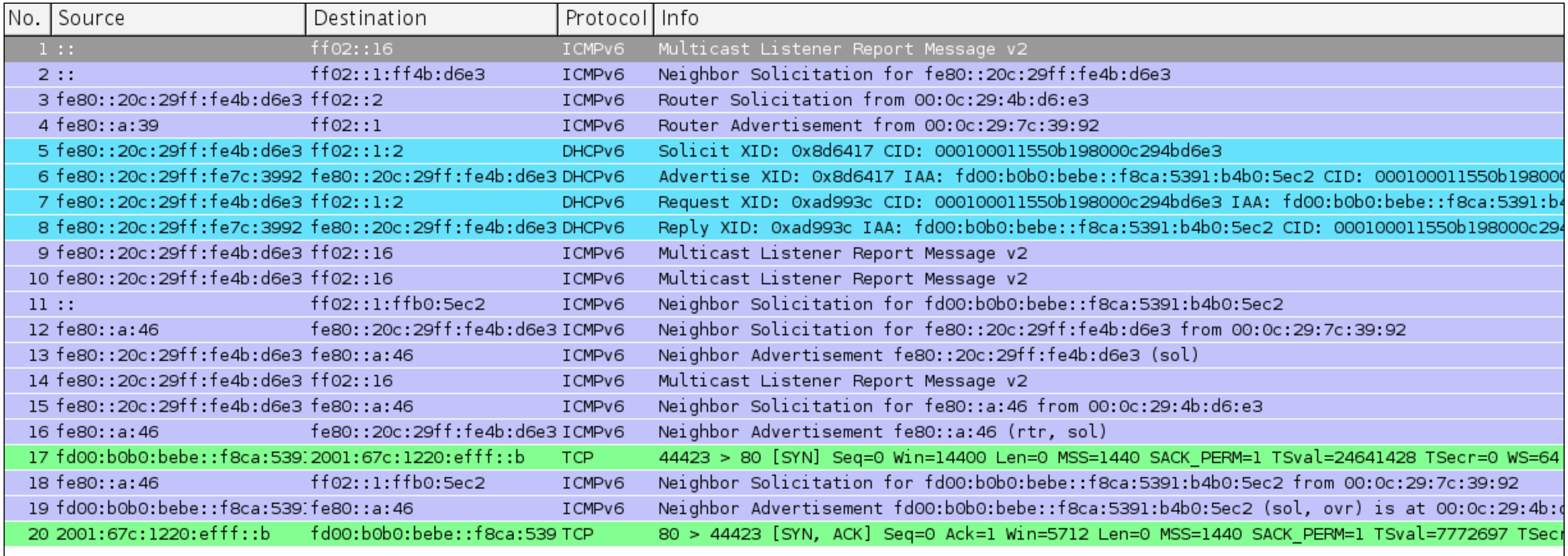
Autoconfiguration IPv4 x IPv6

- IPv4 – DHCP, ARP



No.	Source	Destination	Protocol	Info
1	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x7d5bd263
2	192.168.0.1	192.168.0.20	DHCP	DHCP Offer - Transaction ID 0x7d5bd263
3	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x7d5bd263
4	192.168.0.1	192.168.0.20	DHCP	DHCP ACK - Transaction ID 0x7d5bd263
5	00:0c:29:7c:39:92	00:0c:29:4b:d6:e3	ARP	Who has 192.168.0.20? Tell 192.168.0.1
6	00:0c:29:4b:d6:e3	00:0c:29:7c:39:92	ARP	192.168.0.20 is at 00:0c:29:4b:d6:e3
7	192.168.0.20	147.229.94.185	TCP	53503 > 80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=24646422 TSecr=0 WS=64
8	147.229.94.185	192.168.0.20	TCP	80 > 53503 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=7777286 TSecr

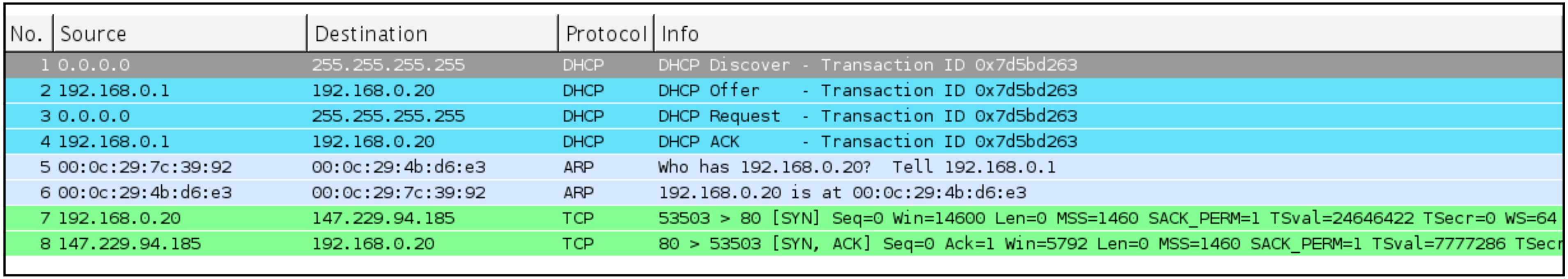
- IPv6 – DAD, RS/RA, DHCPv6, MLDv2, ND



No.	Source	Destination	Protocol	Info
1	::	ff02::16	ICMPv6	Multicast Listener Report Message v2
2	::	ff02::1:ff4b:d6e3	ICMPv6	Neighbor Solicitation for fe80::20c:29ff:fe4b:d6e3
3	fe80::20c:29ff:fe4b:d6e3	ff02::2	ICMPv6	Router Solicitation from 00:0c:29:4b:d6:e3
4	fe80::a:39	ff02::1	ICMPv6	Router Advertisement from 00:0c:29:7c:39:92
5	fe80::20c:29ff:fe4b:d6e3	ff02::1:2	DHCPv6	Solicit XID: 0x8d6417 CID: 000100011550b198000c294bd6e3
6	fe80::20c:29ff:fe7c:3992	fe80::20c:29ff:fe4b:d6e3	DHCPv6	Advertise XID: 0x8d6417 IAA: fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 CID: 000100011550b19800
7	fe80::20c:29ff:fe4b:d6e3	ff02::1:2	DHCPv6	Request XID: 0xad993c CID: 000100011550b198000c294bd6e3 IAA: fd00:b0b0:bebe::f8ca:5391:b
8	fe80::20c:29ff:fe7c:3992	fe80::20c:29ff:fe4b:d6e3	DHCPv6	Reply XID: 0xad993c IAA: fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 CID: 000100011550b198000c29
9	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
10	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
11	::	ff02::1:ffb0:5ec2	ICMPv6	Neighbor Solicitation for fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2
12	fe80::a:46	fe80::20c:29ff:fe4b:d6e3	ICMPv6	Neighbor Solicitation for fe80::20c:29ff:fe4b:d6e3 from 00:0c:29:7c:39:92
13	fe80::20c:29ff:fe4b:d6e3	fe80::a:46	ICMPv6	Neighbor Advertisement fe80::20c:29ff:fe4b:d6e3 (sol)
14	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
15	fe80::20c:29ff:fe4b:d6e3	fe80::a:46	ICMPv6	Neighbor Solicitation for fe80::a:46 from 00:0c:29:4b:d6:e3
16	fe80::a:46	fe80::20c:29ff:fe4b:d6e3	ICMPv6	Neighbor Advertisement fe80::a:46 (rtr, sol)
17	fd00:b0b0:bebe::f8ca:539	2001:67c:1220:efff::b	TCP	44423 > 80 [SYN] Seq=0 Win=14400 Len=0 MSS=1440 SACK_PERM=1 TSval=24641428 TSecr=0 WS=64
18	fe80::a:46	ff02::1:ffb0:5ec2	ICMPv6	Neighbor Solicitation for fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 from 00:0c:29:7c:39:92
19	fd00:b0b0:bebe::f8ca:539	fe80::a:46	ICMPv6	Neighbor Advertisement fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 (sol, ovr) is at 00:0c:29:4b:
20	2001:67c:1220:efff::b	fd00:b0b0:bebe::f8ca:539	TCP	80 > 44423 [SYN, ACK] Seq=0 Ack=1 Win=5712 Len=0 MSS=1440 SACK_PERM=1 TSval=7772697 TSecr

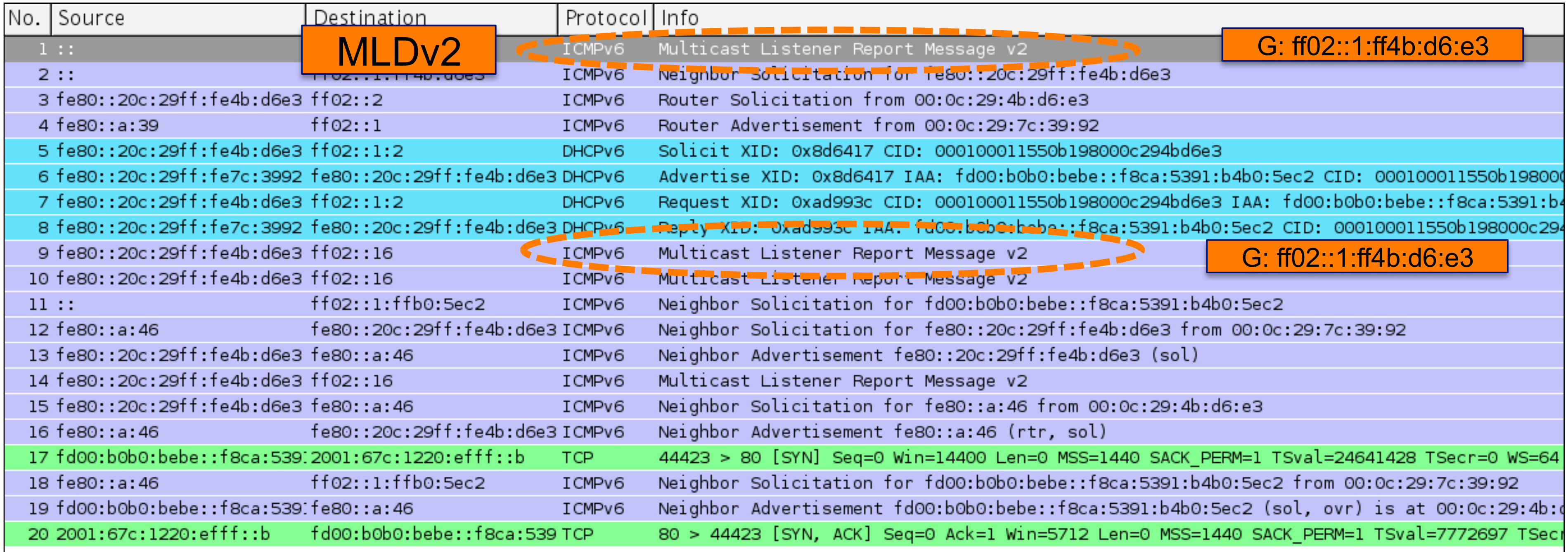
Autoconfiguration IPv4 x IPv6

- IPv4 – DHCP, ARP



No.	Source	Destination	Protocol	Info
1	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x7d5bd263
2	192.168.0.1	192.168.0.20	DHCP	DHCP Offer - Transaction ID 0x7d5bd263
3	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x7d5bd263
4	192.168.0.1	192.168.0.20	DHCP	DHCP ACK - Transaction ID 0x7d5bd263
5	00:0c:29:7c:39:92	00:0c:29:4b:d6:e3	ARP	Who has 192.168.0.20? Tell 192.168.0.1
6	00:0c:29:4b:d6:e3	00:0c:29:7c:39:92	ARP	192.168.0.20 is at 00:0c:29:4b:d6:e3
7	192.168.0.20	147.229.94.185	TCP	53503 > 80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=24646422 TSecr=0 WS=64
8	147.229.94.185	192.168.0.20	TCP	80 > 53503 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=7777286 TSecr

- IPv6 – DAD, RS/RA, DHCPv6, MLDv2, ND



MLDv2

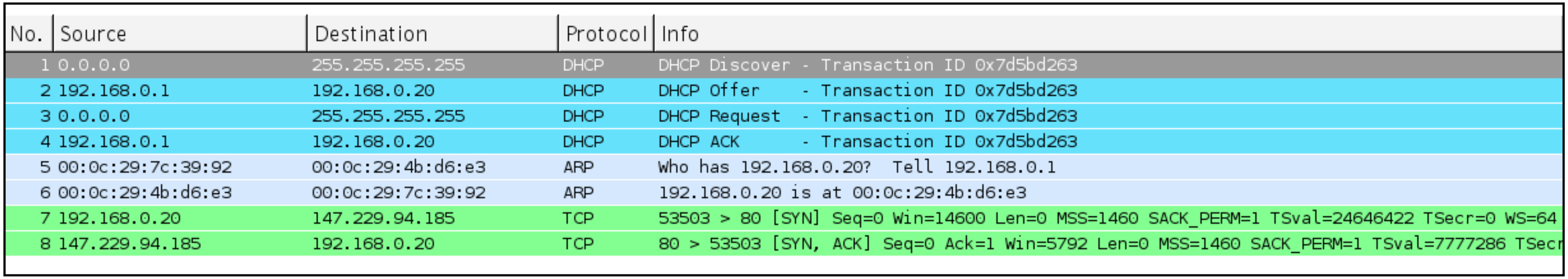
G: ff02::1:ff4b:d6:e3

G: ff02::1:ff4b:d6:e3

No.	Source	Destination	Protocol	Info
1	::		ICMPv6	Multicast Listener Report Message v2
2	::	ff02::1:ff4b:d6e3	ICMPv6	Neighbor Solicitation for fe80::20c:29ff:fe4b:d6e3
3	fe80::20c:29ff:fe4b:d6e3	ff02::2	ICMPv6	Router Solicitation from 00:0c:29:4b:d6:e3
4	fe80::a:39	ff02::1	ICMPv6	Router Advertisement from 00:0c:29:7c:39:92
5	fe80::20c:29ff:fe4b:d6e3	ff02::1:2	DHCPv6	Solicit XID: 0x8d6417 CID: 000100011550b198000c294bd6e3
6	fe80::20c:29ff:fe7c:3992	fe80::20c:29ff:fe4b:d6e3	DHCPv6	Advertise XID: 0x8d6417 IAA: fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 CID: 000100011550b19800
7	fe80::20c:29ff:fe4b:d6e3	ff02::1:2	DHCPv6	Request XID: 0xad993c CID: 000100011550b198000c294bd6e3 IAA: fd00:b0b0:bebe::f8ca:5391:b4
8	fe80::20c:29ff:fe7c:3992	fe80::20c:29ff:fe4b:d6e3	DHCPv6	Reply XID: 0xad993c IAA: fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 CID: 000100011550b198000c294
9	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
10	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
11	::	ff02::1:ffb0:5ec2	ICMPv6	Neighbor Solicitation for fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2
12	fe80::a:46	fe80::20c:29ff:fe4b:d6e3	ICMPv6	Neighbor Solicitation for fe80::20c:29ff:fe4b:d6e3 from 00:0c:29:7c:39:92
13	fe80::20c:29ff:fe4b:d6e3	fe80::a:46	ICMPv6	Neighbor Advertisement fe80::20c:29ff:fe4b:d6e3 (sol)
14	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
15	fe80::20c:29ff:fe4b:d6e3	fe80::a:46	ICMPv6	Neighbor Solicitation for fe80::a:46 from 00:0c:29:4b:d6:e3
16	fe80::a:46	fe80::20c:29ff:fe4b:d6e3	ICMPv6	Neighbor Advertisement fe80::a:46 (rtr, sol)
17	fd00:b0b0:bebe::f8ca:539	2001:67c:1220:efff::b	TCP	44423 > 80 [SYN] Seq=0 Win=14400 Len=0 MSS=1440 SACK_PERM=1 TSval=24641428 TSecr=0 WS=64
18	fe80::a:46	ff02::1:ffb0:5ec2	ICMPv6	Neighbor Solicitation for fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 from 00:0c:29:7c:39:92
19	fd00:b0b0:bebe::f8ca:539	fe80::a:46	ICMPv6	Neighbor Advertisement fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 (sol, ovr) is at 00:0c:29:4b:d
20	2001:67c:1220:efff::b	fd00:b0b0:bebe::f8ca:539	TCP	80 > 44423 [SYN, ACK] Seq=0 Ack=1 Win=5712 Len=0 MSS=1440 SACK_PERM=1 TSval=7772697 TSecr

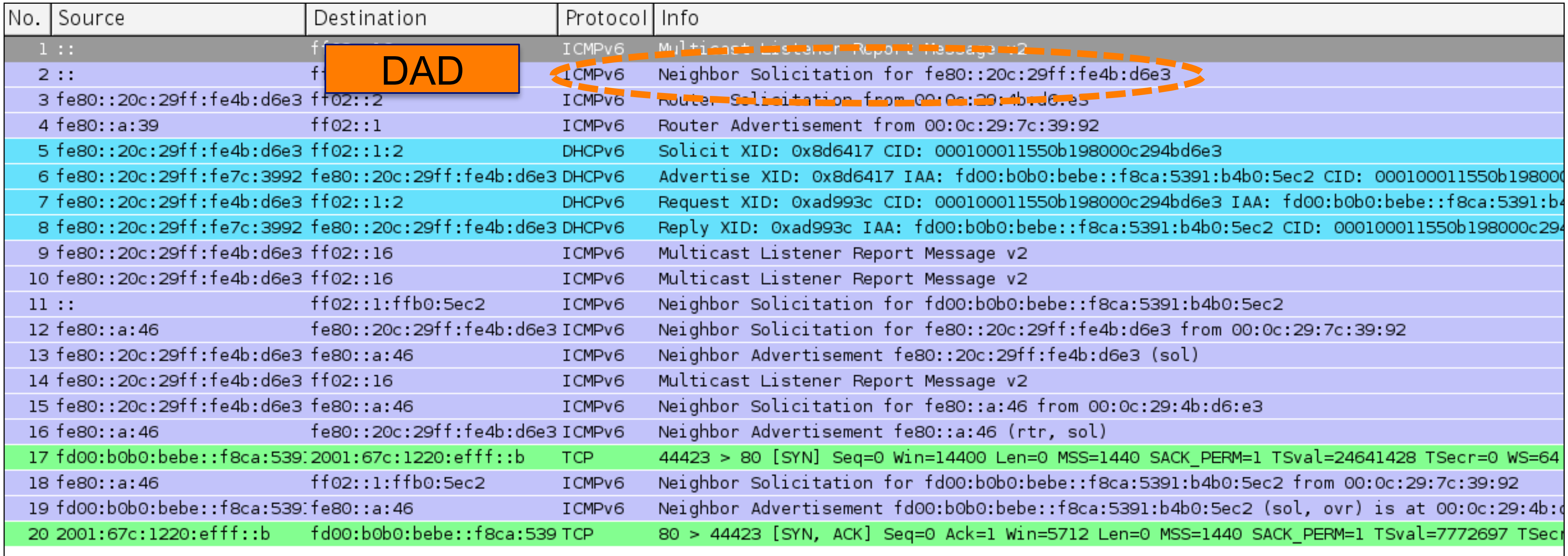
Autoconfiguration IPv4 x IPv6

- IPv4 – DHCP, ARP



No.	Source	Destination	Protocol	Info
1	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x7d5bd263
2	192.168.0.1	192.168.0.20	DHCP	DHCP Offer - Transaction ID 0x7d5bd263
3	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x7d5bd263
4	192.168.0.1	192.168.0.20	DHCP	DHCP ACK - Transaction ID 0x7d5bd263
5	00:0c:29:7c:39:92	00:0c:29:4b:d6:e3	ARP	Who has 192.168.0.20? Tell 192.168.0.1
6	00:0c:29:4b:d6:e3	00:0c:29:7c:39:92	ARP	192.168.0.20 is at 00:0c:29:4b:d6:e3
7	192.168.0.20	147.229.94.185	TCP	53503 > 80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=24646422 TSecr=0 WS=64
8	147.229.94.185	192.168.0.20	TCP	80 > 53503 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=7777286 TSecr

- IPv6 – DAD, RS/RA, DHCPv6, MLDv2, ND

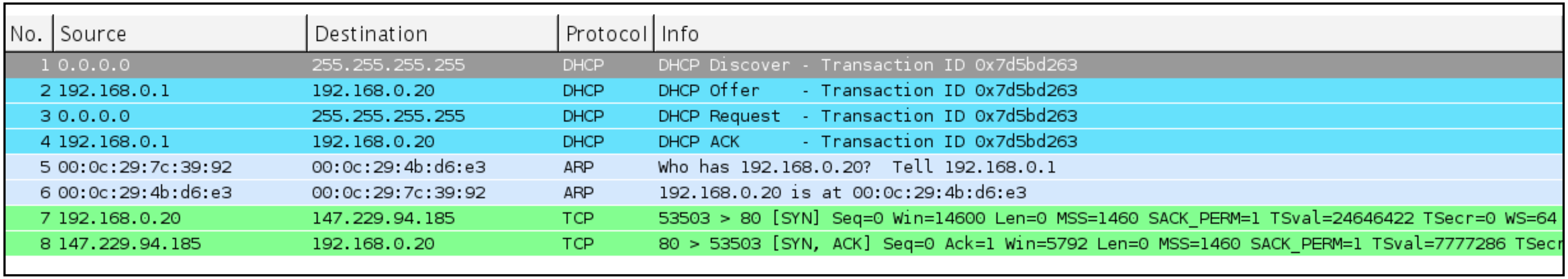


DAD

No.	Source	Destination	Protocol	Info
1	::	ff02::16	ICMPv6	Multicast Listener Report Message v2
2	::	f[illegible]	ICMPv6	Neighbor Solicitation for fe80::20c:29ff:fe4b:d6e3
3	fe80::20c:29ff:fe4b:d6e3	ff02::2	ICMPv6	Router Solicitation from 00:0c:29:4b:d6:e3
4	fe80::a:39	ff02::1	ICMPv6	Router Advertisement from 00:0c:29:7c:39:92
5	fe80::20c:29ff:fe4b:d6e3	ff02::1:2	DHCPv6	Solicit XID: 0x8d6417 CID: 000100011550b198000c294bd6e3
6	fe80::20c:29ff:fe7c:3992	fe80::20c:29ff:fe4b:d6e3	DHCPv6	Advertise XID: 0x8d6417 IAA: fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 CID: 000100011550b19800
7	fe80::20c:29ff:fe4b:d6e3	ff02::1:2	DHCPv6	Request XID: 0xad993c CID: 000100011550b198000c294bd6e3 IAA: fd00:b0b0:bebe::f8ca:5391:b4
8	fe80::20c:29ff:fe7c:3992	fe80::20c:29ff:fe4b:d6e3	DHCPv6	Reply XID: 0xad993c IAA: fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 CID: 000100011550b198000c29
9	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
10	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
11	::	ff02::1:ffb0:5ec2	ICMPv6	Neighbor Solicitation for fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2
12	fe80::a:46	fe80::20c:29ff:fe4b:d6e3	ICMPv6	Neighbor Solicitation for fe80::20c:29ff:fe4b:d6e3 from 00:0c:29:7c:39:92
13	fe80::20c:29ff:fe4b:d6e3	fe80::a:46	ICMPv6	Neighbor Advertisement fe80::20c:29ff:fe4b:d6e3 (sol)
14	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
15	fe80::20c:29ff:fe4b:d6e3	fe80::a:46	ICMPv6	Neighbor Solicitation for fe80::a:46 from 00:0c:29:4b:d6:e3
16	fe80::a:46	fe80::20c:29ff:fe4b:d6e3	ICMPv6	Neighbor Advertisement fe80::a:46 (rtr, sol)
17	fd00:b0b0:bebe::f8ca:539	2001:67c:1220:efff::b	TCP	44423 > 80 [SYN] Seq=0 Win=14400 Len=0 MSS=1440 SACK_PERM=1 TSval=24641428 TSecr=0 WS=64
18	fe80::a:46	ff02::1:ffb0:5ec2	ICMPv6	Neighbor Solicitation for fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 from 00:0c:29:7c:39:92
19	fd00:b0b0:bebe::f8ca:539	fe80::a:46	ICMPv6	Neighbor Advertisement fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 (sol, ovr) is at 00:0c:29:4b:
20	2001:67c:1220:efff::b	fd00:b0b0:bebe::f8ca:539	TCP	80 > 44423 [SYN, ACK] Seq=0 Ack=1 Win=5712 Len=0 MSS=1440 SACK_PERM=1 TSval=7772697 TSecr

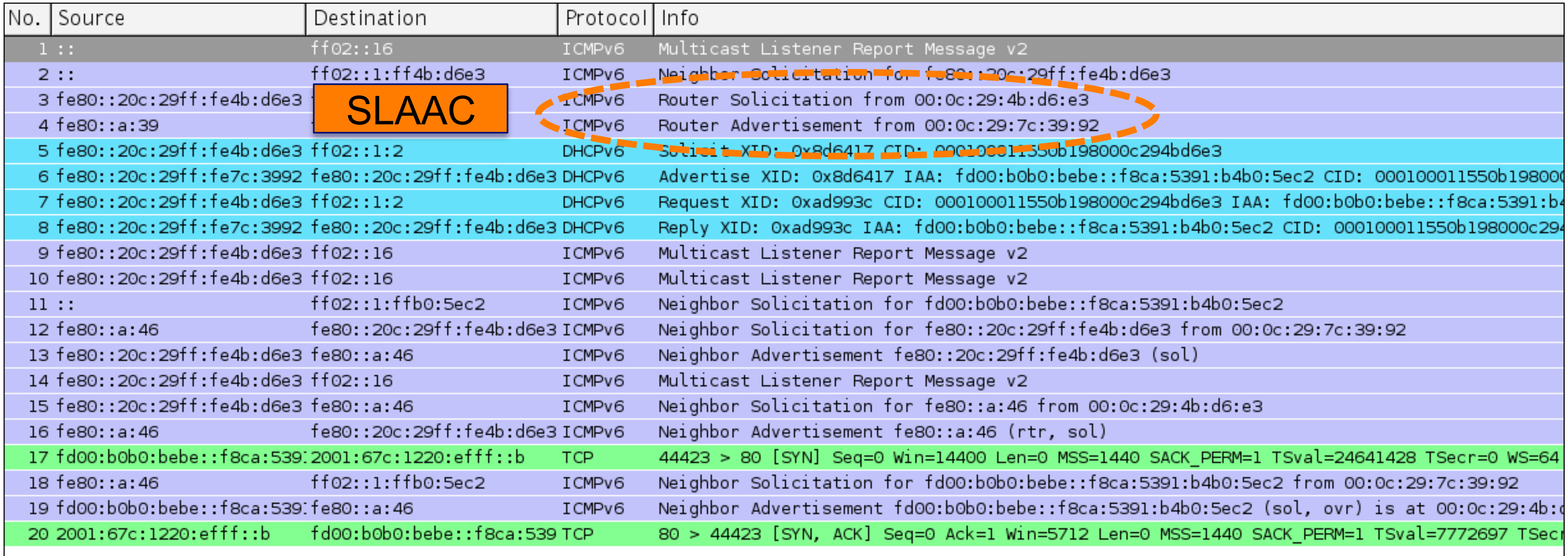
Autoconfiguration IPv4 x IPv6

- IPv4 – DHCP, ARP



No.	Source	Destination	Protocol	Info
1	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x7d5bd263
2	192.168.0.1	192.168.0.20	DHCP	DHCP Offer - Transaction ID 0x7d5bd263
3	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x7d5bd263
4	192.168.0.1	192.168.0.20	DHCP	DHCP ACK - Transaction ID 0x7d5bd263
5	00:0c:29:7c:39:92	00:0c:29:4b:d6:e3	ARP	Who has 192.168.0.20? Tell 192.168.0.1
6	00:0c:29:4b:d6:e3	00:0c:29:7c:39:92	ARP	192.168.0.20 is at 00:0c:29:4b:d6:e3
7	192.168.0.20	147.229.94.185	TCP	53503 > 80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=24646422 TSecr=0 WS=64
8	147.229.94.185	192.168.0.20	TCP	80 > 53503 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=7777286 TSecr

- IPv6 – DAD, RS/RA, DHCPv6, MLDv2, ND

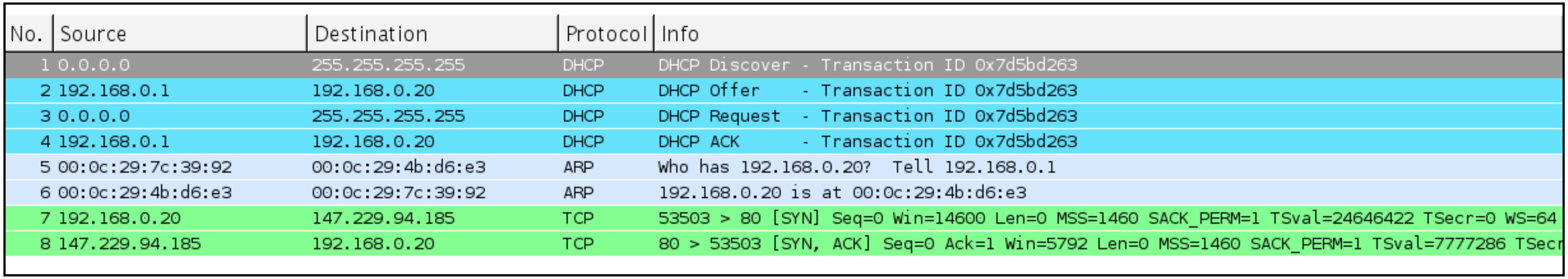


SLAAC

No.	Source	Destination	Protocol	Info
1	::	ff02::16	ICMPv6	Multicast Listener Report Message v2
2	::	ff02::1:ff4b:d6e3	ICMPv6	Neighbor Solicitation for fe80::20c:29ff:fe4b:d6e3
3	fe80::20c:29ff:fe4b:d6e3		ICMPv6	Router Solicitation from 00:0c:29:4b:d6:e3
4	fe80::a:39		ICMPv6	Router Advertisement from 00:0c:29:7c:39:92
5	fe80::20c:29ff:fe4b:d6e3	ff02::1:2	DHCPv6	Solicit XID: 0x8d6417 CID: 000100011550b198000c294bd6e3
6	fe80::20c:29ff:fe7c:3992	fe80::20c:29ff:fe4b:d6e3	DHCPv6	Advertise XID: 0x8d6417 IAA: fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 CID: 000100011550b19800
7	fe80::20c:29ff:fe4b:d6e3	ff02::1:2	DHCPv6	Request XID: 0xad993c CID: 000100011550b198000c294bd6e3 IAA: fd00:b0b0:bebe::f8ca:5391:b4
8	fe80::20c:29ff:fe7c:3992	fe80::20c:29ff:fe4b:d6e3	DHCPv6	Reply XID: 0xad993c IAA: fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 CID: 000100011550b198000c29
9	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
10	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
11	::	ff02::1:ffb0:5ec2	ICMPv6	Neighbor Solicitation for fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2
12	fe80::a:46	fe80::20c:29ff:fe4b:d6e3	ICMPv6	Neighbor Solicitation for fe80::20c:29ff:fe4b:d6e3 from 00:0c:29:7c:39:92
13	fe80::20c:29ff:fe4b:d6e3	fe80::a:46	ICMPv6	Neighbor Advertisement fe80::20c:29ff:fe4b:d6e3 (sol)
14	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
15	fe80::20c:29ff:fe4b:d6e3	fe80::a:46	ICMPv6	Neighbor Solicitation for fe80::a:46 from 00:0c:29:4b:d6:e3
16	fe80::a:46	fe80::20c:29ff:fe4b:d6e3	ICMPv6	Neighbor Advertisement fe80::a:46 (rtr, sol)
17	fd00:b0b0:bebe::f8ca:539	2001:67c:1220:efff::b	TCP	44423 > 80 [SYN] Seq=0 Win=14400 Len=0 MSS=1440 SACK_PERM=1 TSval=24641428 TSecr=0 WS=64
18	fe80::a:46	ff02::1:ffb0:5ec2	ICMPv6	Neighbor Solicitation for fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 from 00:0c:29:7c:39:92
19	fd00:b0b0:bebe::f8ca:539	fe80::a:46	ICMPv6	Neighbor Advertisement fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 (sol, ovr) is at 00:0c:29:4b:
20	2001:67c:1220:efff::b	fd00:b0b0:bebe::f8ca:539	TCP	80 > 44423 [SYN, ACK] Seq=0 Ack=1 Win=5712 Len=0 MSS=1440 SACK_PERM=1 TSval=7772697 TSecr

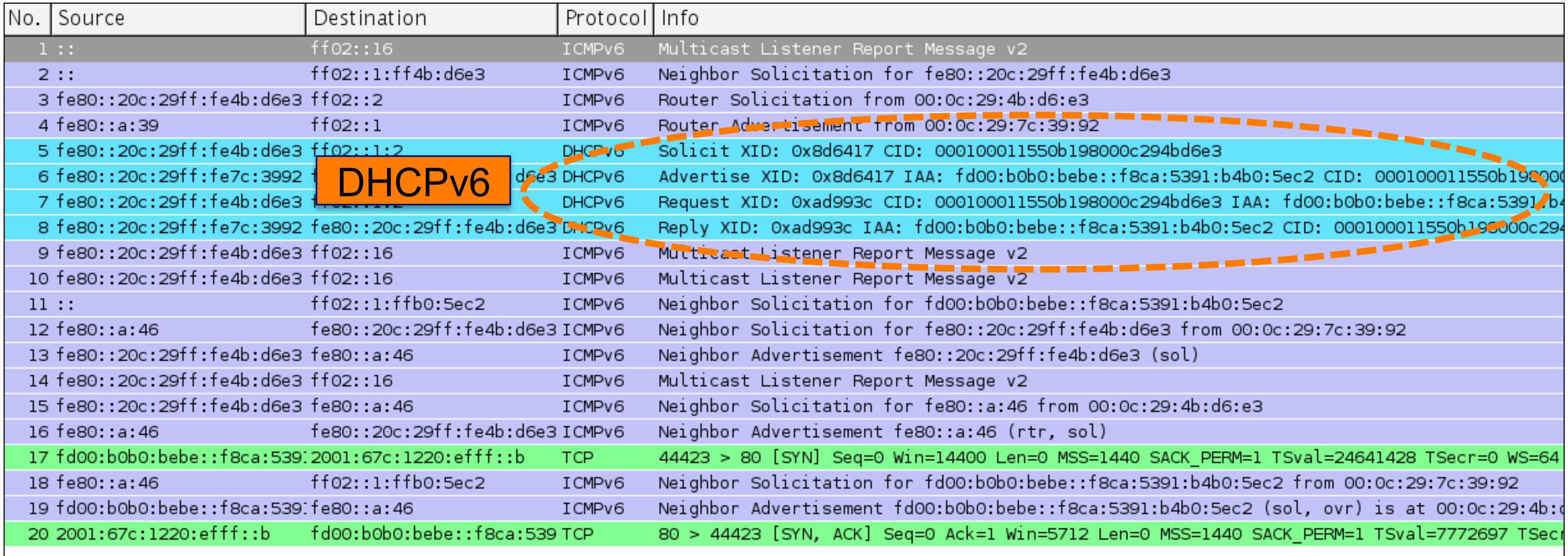
Autoconfiguration IPv4 x IPv6

- IPv4 – DHCP, ARP



No.	Source	Destination	Protocol	Info
1	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x7d5bd263
2	192.168.0.1	192.168.0.20	DHCP	DHCP Offer - Transaction ID 0x7d5bd263
3	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x7d5bd263
4	192.168.0.1	192.168.0.20	DHCP	DHCP ACK - Transaction ID 0x7d5bd263
5	00:0c:29:7c:39:92	00:0c:29:4b:d6:e3	ARP	Who has 192.168.0.20? Tell 192.168.0.1
6	00:0c:29:4b:d6:e3	00:0c:29:7c:39:92	ARP	192.168.0.20 is at 00:0c:29:4b:d6:e3
7	192.168.0.20	147.229.94.185	TCP	53503 > 80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=24646422 TSecr=0 WS=64
8	147.229.94.185	192.168.0.20	TCP	80 > 53503 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=7777286 TSecr

- IPv6 – DAD, RS/RA, DHCPv6, MLDv2, ND

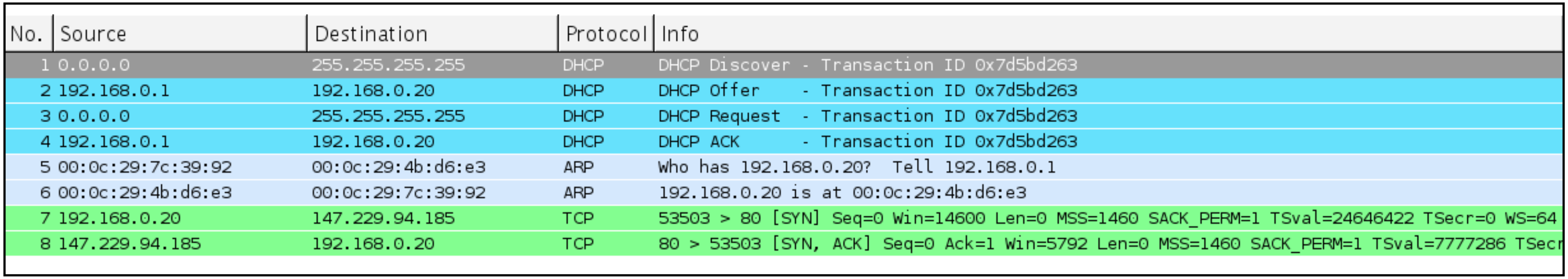


DHCPv6

No.	Source	Destination	Protocol	Info
1	::	ff02::16	ICMPv6	Multicast Listener Report Message v2
2	::	ff02::1:ff4b:d6e3	ICMPv6	Neighbor Solicitation for fe80::20c:29ff:fe4b:d6e3
3	fe80::20c:29ff:fe4b:d6e3	ff02::2	ICMPv6	Router Solicitation from 00:0c:29:4b:d6:e3
4	fe80::a:39	ff02::1	ICMPv6	Router Advertisement from 00:0c:29:7c:39:92
5	fe80::20c:29ff:fe4b:d6e3	ff02::1:2	DHCPv6	Solicit XID: 0x8d6417 CID: 000100011550b198000c294bd6e3
6	fe80::20c:29ff:fe7c:3992	fe80::20c:29ff:fe4b:d6e3	DHCPv6	Advertise XID: 0x8d6417 IAA: fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 CID: 000100011550b198000
7	fe80::20c:29ff:fe4b:d6e3	ff02::1:2	DHCPv6	Request XID: 0xad993c CID: 000100011550b198000c294bd6e3 IAA: fd00:b0b0:bebe::f8ca:5391:b4
8	fe80::20c:29ff:fe7c:3992	fe80::20c:29ff:fe4b:d6e3	DHCPv6	Reply XID: 0xad993c IAA: fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 CID: 000100011550b198000c294
9	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
10	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
11	::	ff02::1:ffb0:5ec2	ICMPv6	Neighbor Solicitation for fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2
12	fe80::a:46	fe80::20c:29ff:fe4b:d6e3	ICMPv6	Neighbor Solicitation for fe80::20c:29ff:fe4b:d6e3 from 00:0c:29:7c:39:92
13	fe80::20c:29ff:fe4b:d6e3	fe80::a:46	ICMPv6	Neighbor Advertisement fe80::20c:29ff:fe4b:d6e3 (sol)
14	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
15	fe80::20c:29ff:fe4b:d6e3	fe80::a:46	ICMPv6	Neighbor Solicitation for fe80::a:46 from 00:0c:29:4b:d6:e3
16	fe80::a:46	fe80::20c:29ff:fe4b:d6e3	ICMPv6	Neighbor Advertisement fe80::a:46 (rtr, sol)
17	fd00:b0b0:bebe::f8ca:539	2001:67c:1220:efff::b	TCP	44423 > 80 [SYN] Seq=0 Win=14400 Len=0 MSS=1440 SACK_PERM=1 TSval=24641428 TSecr=0 WS=64
18	fe80::a:46	ff02::1:ffb0:5ec2	ICMPv6	Neighbor Solicitation for fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 from 00:0c:29:7c:39:92
19	fd00:b0b0:bebe::f8ca:539	fe80::a:46	ICMPv6	Neighbor Advertisement fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 (sol, ovr) is at 00:0c:29:4b:
20	2001:67c:1220:efff::b	fd00:b0b0:bebe::f8ca:539	TCP	80 > 44423 [SYN, ACK] Seq=0 Ack=1 Win=5712 Len=0 MSS=1440 SACK_PERM=1 TSval=7772697 TSecr

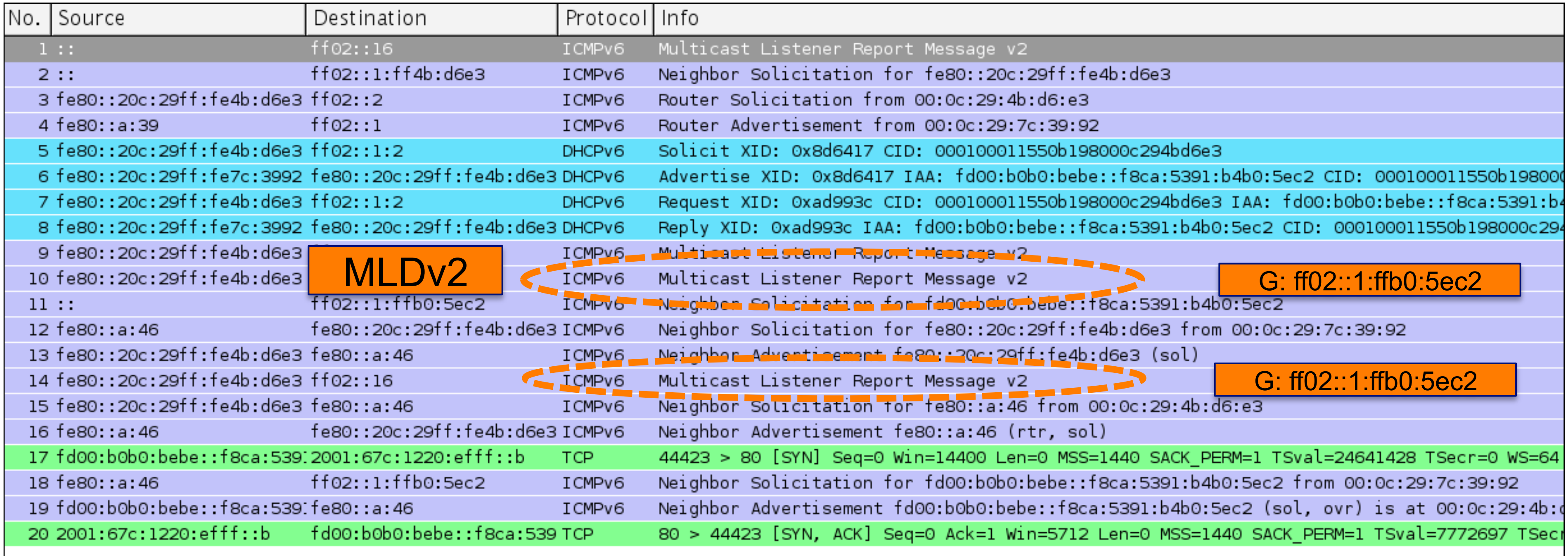
Autoconfiguration IPv4 x IPv6

- IPv4 – DHCP, ARP



No.	Source	Destination	Protocol	Info
1	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x7d5bd263
2	192.168.0.1	192.168.0.20	DHCP	DHCP Offer - Transaction ID 0x7d5bd263
3	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x7d5bd263
4	192.168.0.1	192.168.0.20	DHCP	DHCP ACK - Transaction ID 0x7d5bd263
5	00:0c:29:7c:39:92	00:0c:29:4b:d6:e3	ARP	Who has 192.168.0.20? Tell 192.168.0.1
6	00:0c:29:4b:d6:e3	00:0c:29:7c:39:92	ARP	192.168.0.20 is at 00:0c:29:4b:d6:e3
7	192.168.0.20	147.229.94.185	TCP	53503 > 80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=24646422 TSecr=0 WS=64
8	147.229.94.185	192.168.0.20	TCP	80 > 53503 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=7777286 TSecr

- IPv6 – DAD, RS/RA, DHCPv6, MLDv2, ND



No.	Source	Destination	Protocol	Info
1	::	ff02::16	ICMPv6	Multicast Listener Report Message v2
2	::	ff02::1:ff4b:d6e3	ICMPv6	Neighbor Solicitation for fe80::20c:29ff:fe4b:d6e3
3	fe80::20c:29ff:fe4b:d6e3	ff02::2	ICMPv6	Router Solicitation from 00:0c:29:4b:d6:e3
4	fe80::a:39	ff02::1	ICMPv6	Router Advertisement from 00:0c:29:7c:39:92
5	fe80::20c:29ff:fe4b:d6e3	ff02::1:2	DHCPv6	Solicit XID: 0x8d6417 CID: 000100011550b198000c294bd6e3
6	fe80::20c:29ff:fe7c:3992	fe80::20c:29ff:fe4b:d6e3	DHCPv6	Advertise XID: 0x8d6417 IAA: fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 CID: 000100011550b19800
7	fe80::20c:29ff:fe4b:d6e3	ff02::1:2	DHCPv6	Request XID: 0xad993c CID: 000100011550b198000c294bd6e3 IAA: fd00:b0b0:bebe::f8ca:5391:b
8	fe80::20c:29ff:fe7c:3992	fe80::20c:29ff:fe4b:d6e3	DHCPv6	Reply XID: 0xad993c IAA: fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 CID: 000100011550b198000c29
9	fe80::20c:29ff:fe4b:d6e3	[illegible]	ICMPv6	Multicast Listener Report Message v2
10	fe80::20c:29ff:fe4b:d6e3	[illegible]	ICMPv6	Multicast Listener Report Message v2
11	::	ff02::1:ffb0:5ec2	ICMPv6	Neighbor Solicitation for fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2
12	fe80::a:46	fe80::20c:29ff:fe4b:d6e3	ICMPv6	Neighbor Solicitation for fe80::20c:29ff:fe4b:d6e3 from 00:0c:29:7c:39:92
13	fe80::20c:29ff:fe4b:d6e3	fe80::a:46	ICMPv6	Neighbor Advertisement fe80::20c:29ff:fe4b:d6e3 (sol)
14	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
15	fe80::20c:29ff:fe4b:d6e3	fe80::a:46	ICMPv6	Neighbor Solicitation for fe80::a:46 from 00:0c:29:4b:d6:e3
16	fe80::a:46	fe80::20c:29ff:fe4b:d6e3	ICMPv6	Neighbor Advertisement fe80::a:46 (rtr, sol)
17	fd00:b0b0:bebe::f8ca:539	2001:67c:1220:efff::b	TCP	44423 > 80 [SYN] Seq=0 Win=14400 Len=0 MSS=1440 SACK_PERM=1 TSval=24641428 TSecr=0 WS=64
18	fe80::a:46	ff02::1:ffb0:5ec2	ICMPv6	Neighbor Solicitation for fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 from 00:0c:29:7c:39:92
19	fd00:b0b0:bebe::f8ca:539	fe80::a:46	ICMPv6	Neighbor Advertisement fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 (sol, ovr) is at 00:0c:29:4b:
20	2001:67c:1220:efff::b	fd00:b0b0:bebe::f8ca:539	TCP	80 > 44423 [SYN, ACK] Seq=0 Ack=1 Win=5712 Len=0 MSS=1440 SACK_PERM=1 TSval=7772697 TSecr

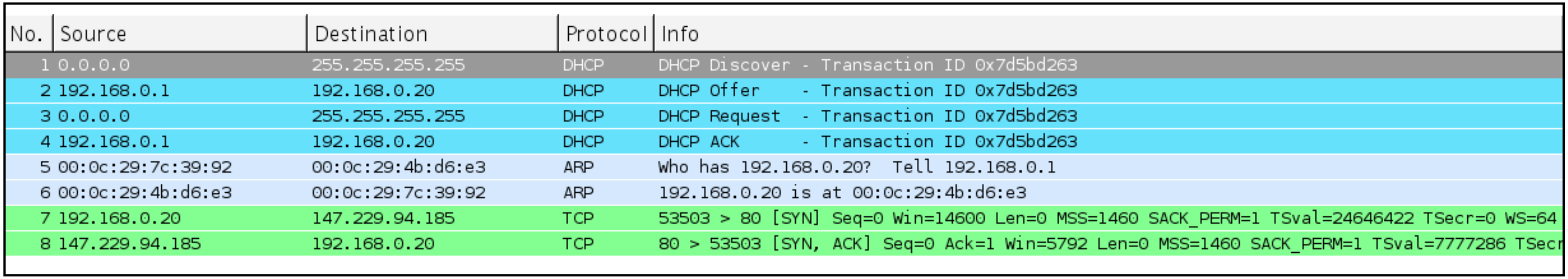
MLDv2

G: ff02::1:ffb0:5ec2

G: ff02::1:ffb0:5ec2

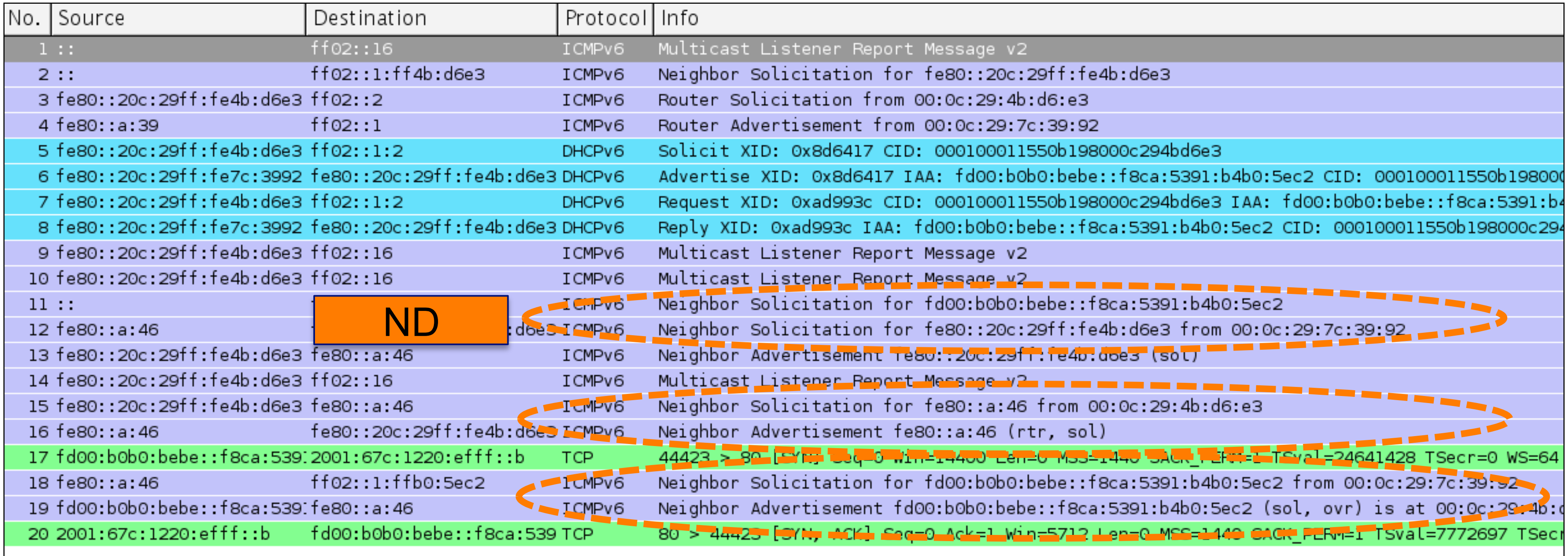
Autoconfiguration IPv4 x IPv6

- IPv4 – DHCP, ARP



No.	Source	Destination	Protocol	Info
1	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x7d5bd263
2	192.168.0.1	192.168.0.20	DHCP	DHCP Offer - Transaction ID 0x7d5bd263
3	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x7d5bd263
4	192.168.0.1	192.168.0.20	DHCP	DHCP ACK - Transaction ID 0x7d5bd263
5	00:0c:29:7c:39:92	00:0c:29:4b:d6:e3	ARP	Who has 192.168.0.20? Tell 192.168.0.1
6	00:0c:29:4b:d6:e3	00:0c:29:7c:39:92	ARP	192.168.0.20 is at 00:0c:29:4b:d6:e3
7	192.168.0.20	147.229.94.185	TCP	53503 > 80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=24646422 TSecr=0 WS=64
8	147.229.94.185	192.168.0.20	TCP	80 > 53503 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=7777286 TSecr

- IPv6 – DAD, RS/RA, DHCPv6, MLDv2, ND

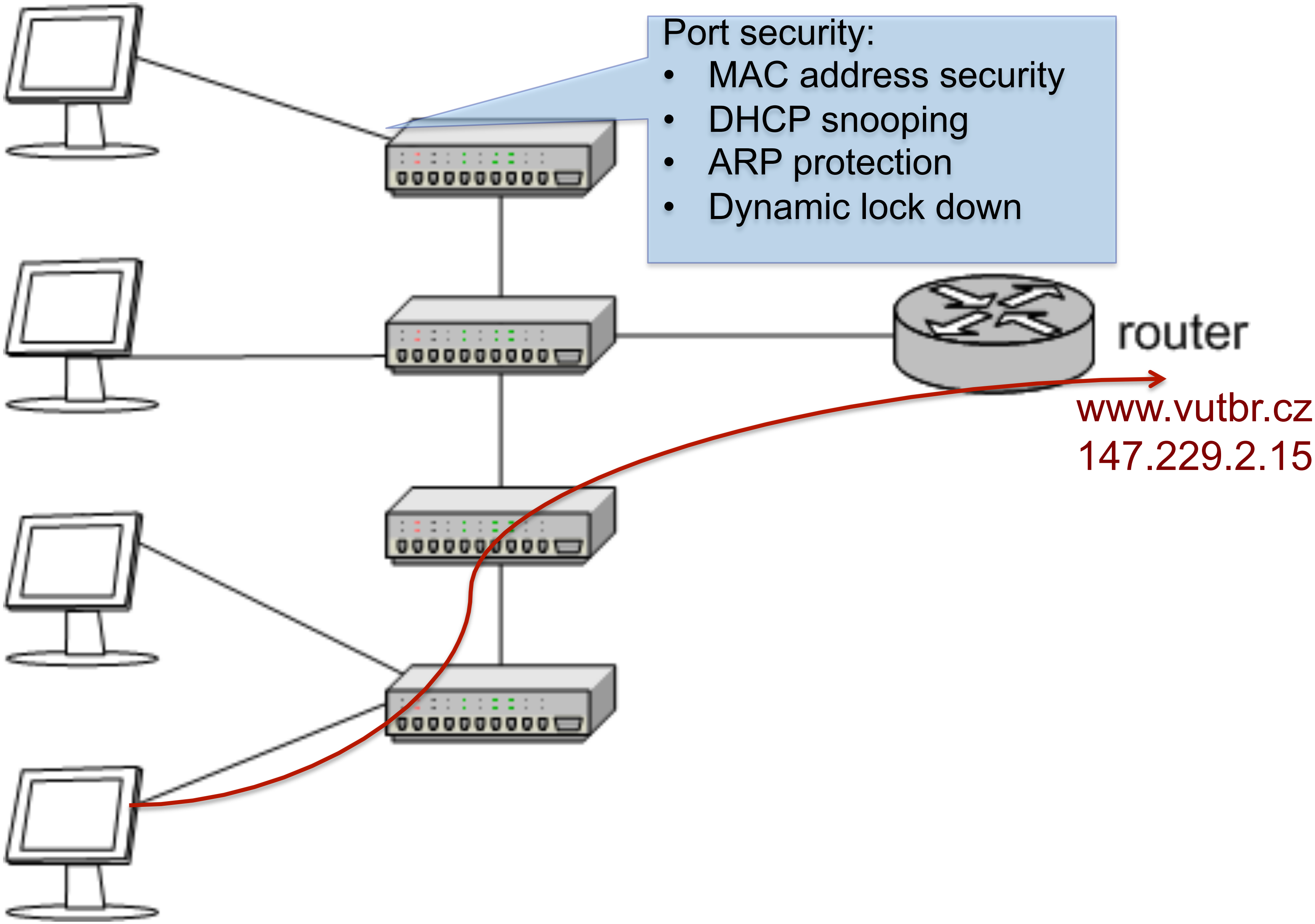


No.	Source	Destination	Protocol	Info
1	::	ff02::16	ICMPv6	Multicast Listener Report Message v2
2	::	ff02::1:ff4b:d6e3	ICMPv6	Neighbor Solicitation for fe80::20c:29ff:fe4b:d6e3
3	fe80::20c:29ff:fe4b:d6e3	ff02::2	ICMPv6	Router Solicitation from 00:0c:29:4b:d6:e3
4	fe80::a:39	ff02::1	ICMPv6	Router Advertisement from 00:0c:29:7c:39:92
5	fe80::20c:29ff:fe4b:d6e3	ff02::1:2	DHCPv6	Solicit XID: 0x8d6417 CID: 000100011550b198000c294bd6e3
6	fe80::20c:29ff:fe7c:3992	fe80::20c:29ff:fe4b:d6e3	DHCPv6	Advertise XID: 0x8d6417 IAA: fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 CID: 000100011550b19800
7	fe80::20c:29ff:fe4b:d6e3	ff02::1:2	DHCPv6	Request XID: 0xad993c CID: 000100011550b198000c294bd6e3 IAA: fd00:b0b0:bebe::f8ca:5391:b4
8	fe80::20c:29ff:fe7c:3992	fe80::20c:29ff:fe4b:d6e3	DHCPv6	Reply XID: 0xad993c IAA: fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 CID: 000100011550b198000c29
9	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
10	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
11	::	f[illegible]	ICMPv6	Neighbor Solicitation for fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2
12	fe80::a:46	f[illegible]:d6e3	ICMPv6	Neighbor Solicitation for fe80::20c:29ff:fe4b:d6e3 from 00:0c:29:7c:39:92
13	fe80::20c:29ff:fe4b:d6e3	fe80::a:46	ICMPv6	Neighbor Advertisement fe80::20c:29ff:fe4b:d6e3 (sol)
14	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
15	fe80::20c:29ff:fe4b:d6e3	fe80::a:46	ICMPv6	Neighbor Solicitation for fe80::a:46 from 00:0c:29:4b:d6:e3
16	fe80::a:46	fe80::20c:29ff:fe4b:d6e3	ICMPv6	Neighbor Advertisement fe80::a:46 (rtr, sol)
17	fd00:b0b0:bebe::f8ca:539	2001:67c:1220:efff::b	TCP	44423 > 80 [SYN] Seq=0 Win=14400 Len=0 MSS=1440 SACK_PERM=1 TSval=24641428 TSecr=0 WS=64
18	fe80::a:46	ff02::1:ffb0:5ec2	ICMPv6	Neighbor Solicitation for fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 from 00:0c:29:7c:39:92
19	fd00:b0b0:bebe::f8ca:539	fe80::a:46	ICMPv6	Neighbor Advertisement fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 (sol, ovr) is at 00:0c:29:4b:d
20	2001:67c:1220:efff::b	fd00:b0b0:bebe::f8ca:539	TCP	80 > 44423 [SYN, ACK] Seq=0 Ack=1 Win=5712 Len=0 MSS=1440 SACK_PERM=1 TSval=7772697 TSecr

IPv4 and IPv6 in a network

- More than 50% of PC supports dualstack
  - Most of them use autoconfiguration (SLAAC) to get IP address (MS Vista/7, Linux, Mac OS, iOS, BSD*)
  - IPv6 is preferred protocol by default
- Steps to make an attack:
  - Setup attacker’s IP to act as a RA sender
  - Prepare a DHCPv6 server on the attacker's PC; as DNS servers provide attacker’s addresses
  - Modify the behavior of DNS server to return A or AAAA records for www.google.com, www.yahoo.com, etc. to your attacker’s address
  - Transparent proxy service allows attacker to modify content of webpages

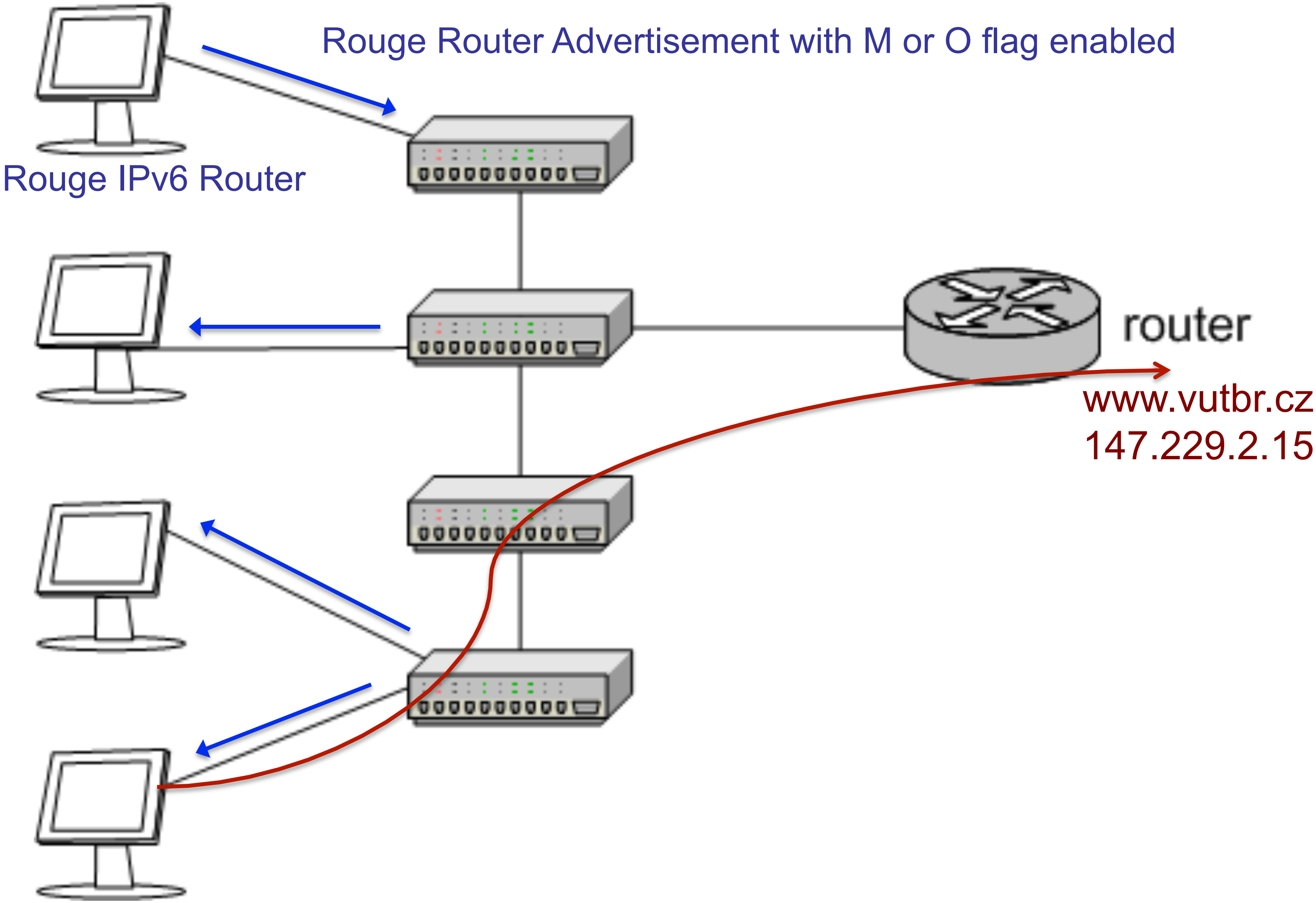
Extension headers



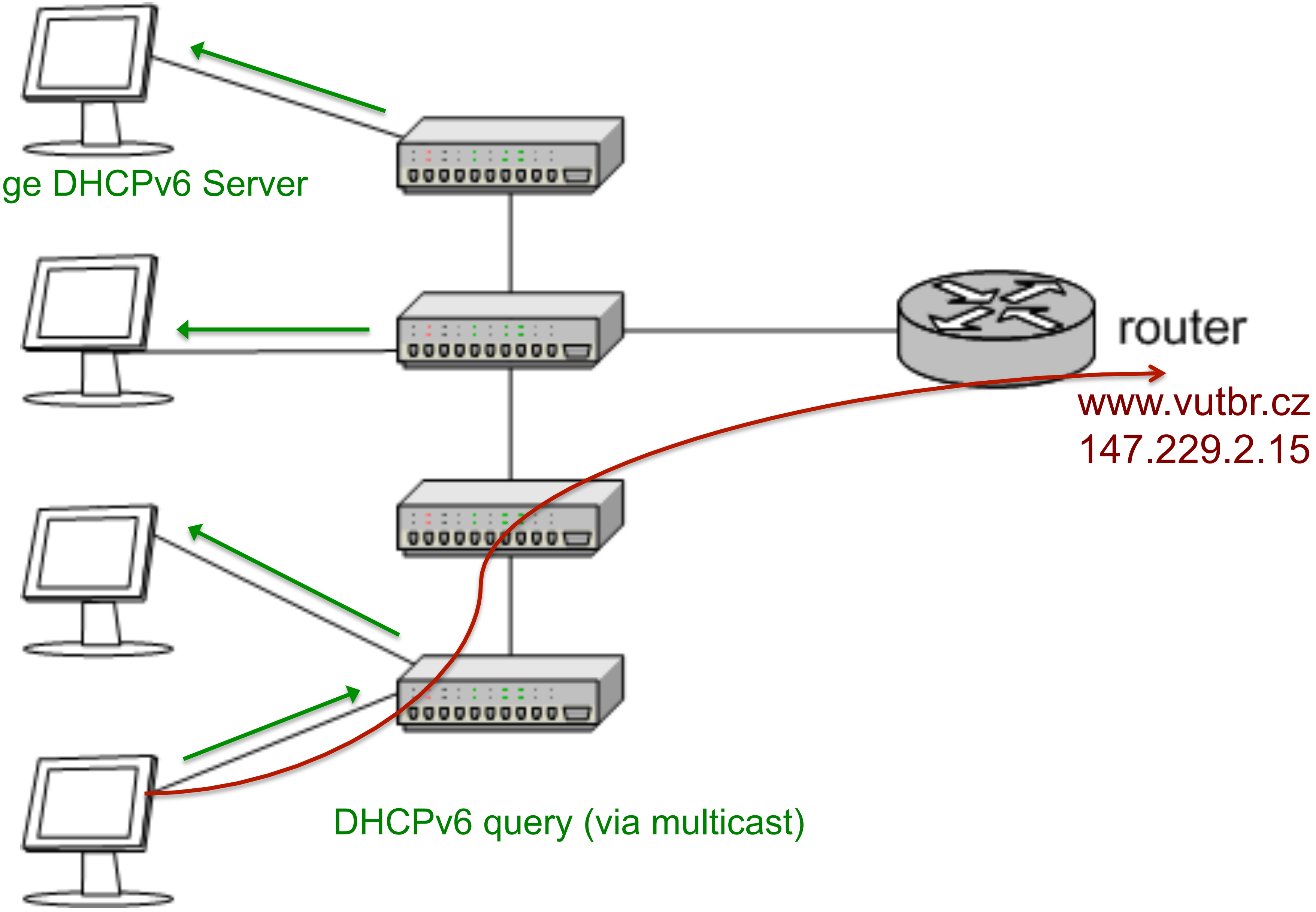
Port security:

- MAC address security
- DHCP snooping
- ARP protection
- Dynamic lock down

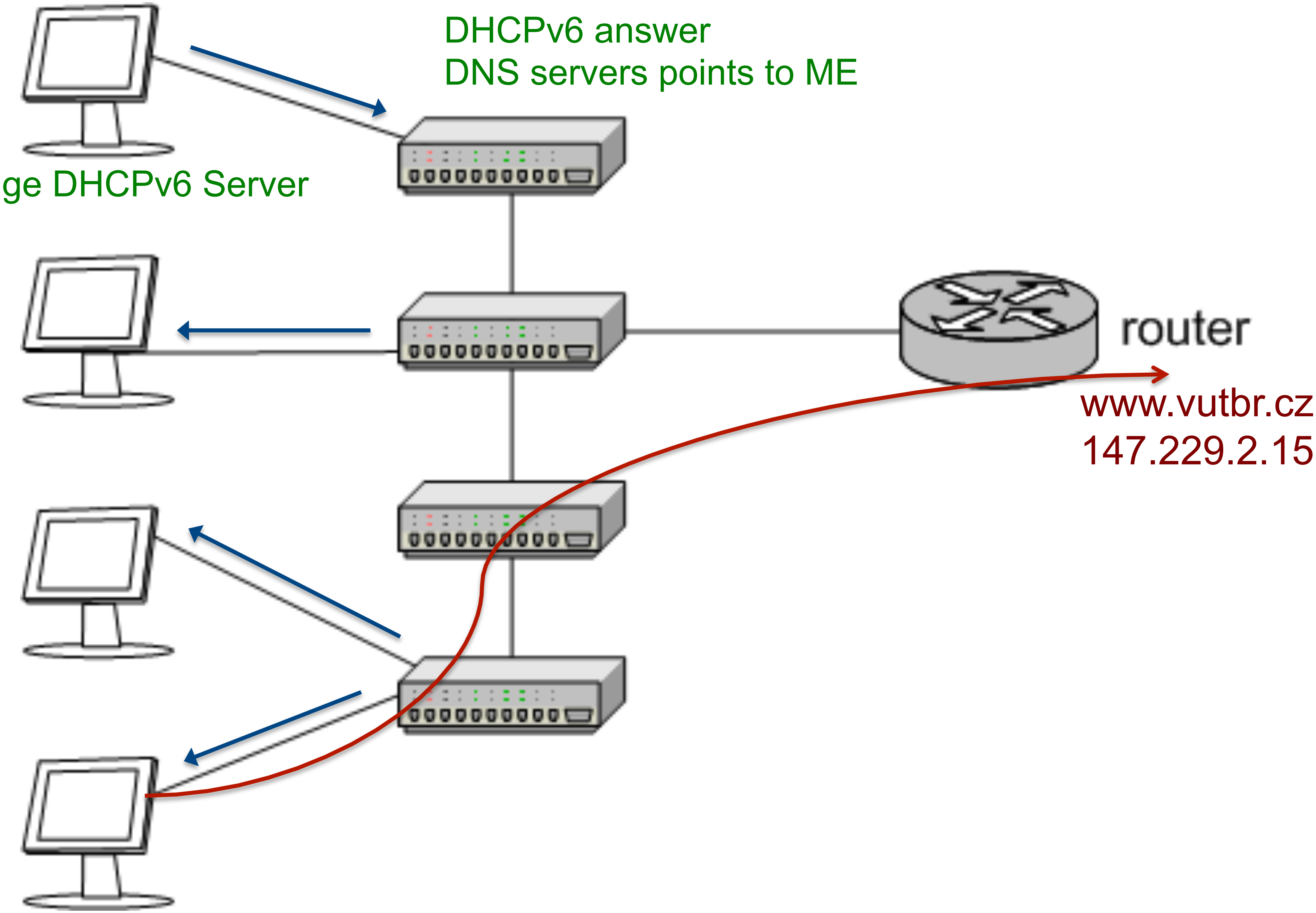
Extension headers



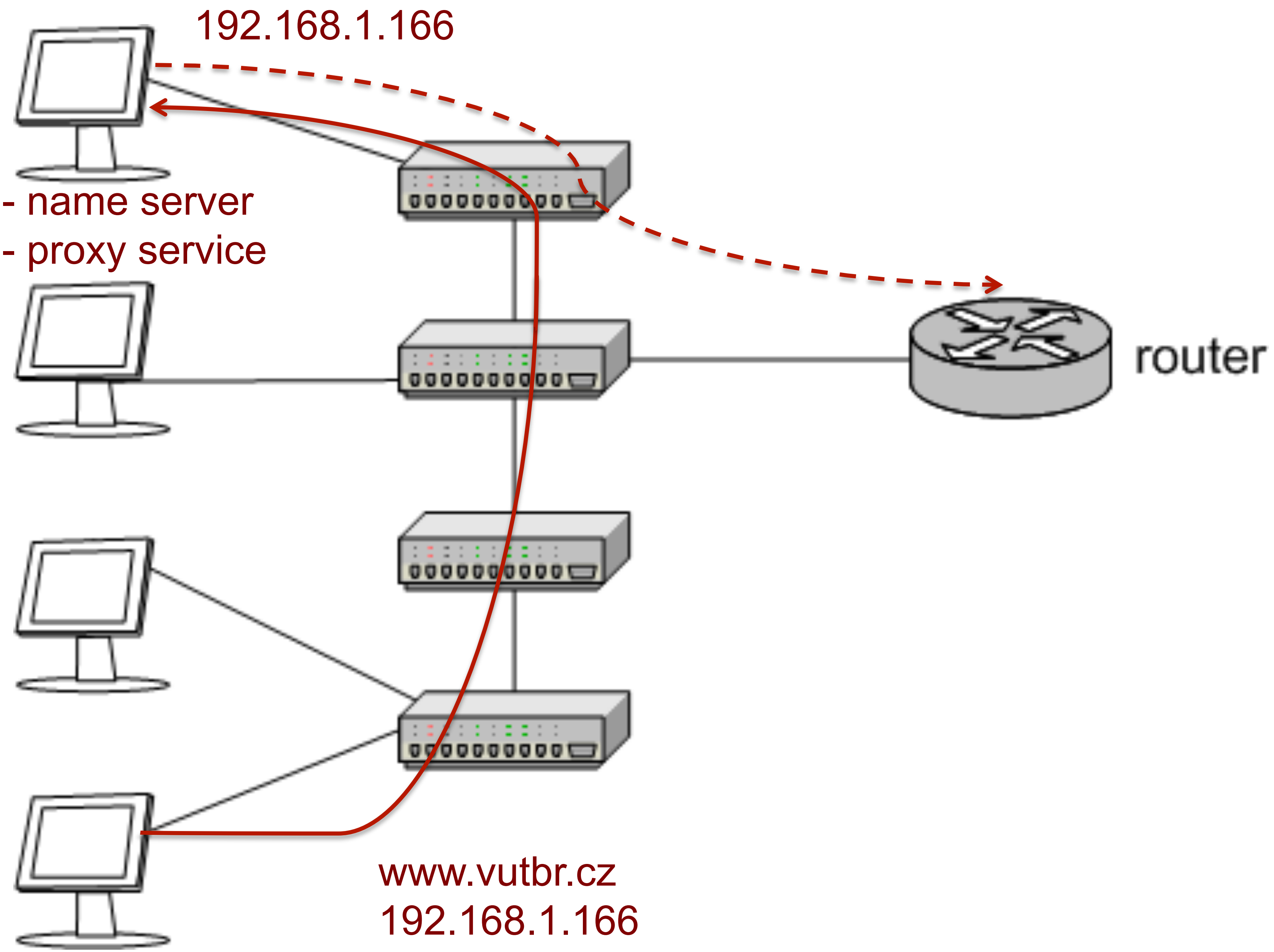
Extension headers



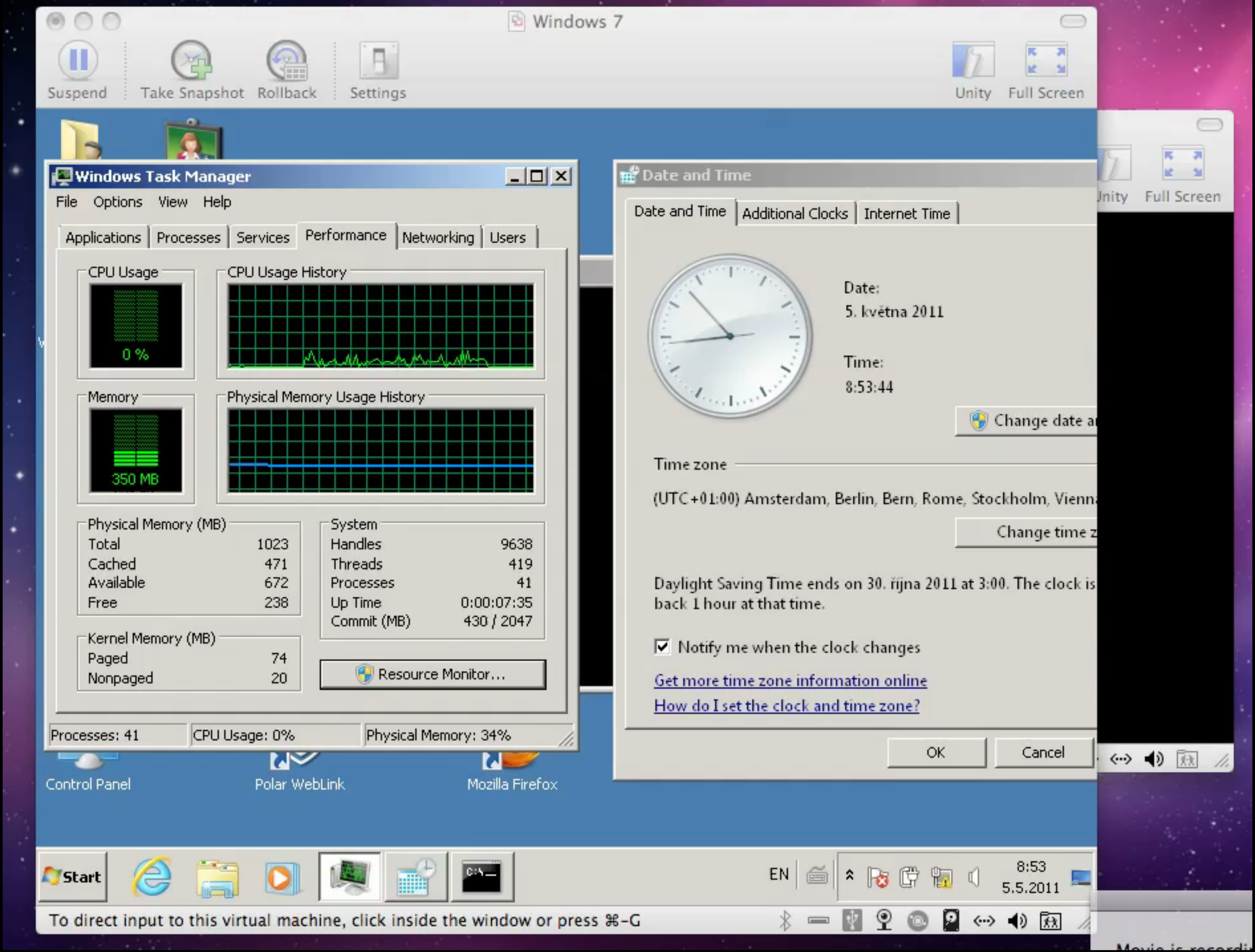
Extension headers



Extension headers



```
# ./flood_router6 eth0
```



CPU Usage: 0 %

Memory: 350 MB

Physical Memory (MB)
Total 1023
Cached 471
Available 672
Free 238

Kernel Memory (MB)
Paged 74
Nonpaged 20

System
Handles 9638
Threads 419
Processes 41
Up Time 0:00:07:35
Commit (MB) 430 / 2047

Processes: 41 | CPU Usage: 0% | Physical Memory: 34%

Date:
5. května 2011

Time:
8:53:44

Time zone

(UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienn

Daylight Saving Time ends on 30. října 2011 at 3:00. The clock is
back 1 hour at that time.

☑ Notify me when the clock changes

Get more time zone information online

How do I set the clock and time zone?

8:53
5.5.2011

To direct input to this virtual machine, click inside the window or press ⌘-G

It is not a problem!

IPv4 has very similar issues related to autoconfiguration. There is no difference between IPv6 and IPv4.

Really ? Isn’t there ?

Autoconfiguration – IPv4

- IPv4 autoconfiguration = DHCP
- Protection mechanisms on L2 devices
  - **DHCP snooping**
    - Blocking DHCP responses on access ports
    - Prevents against fake DHCP servers
  - **Dynamic ARP protection**
    - MAC-IP address database based on DHCP leases
    - Checking content of ARP packets on client access port
    - Prevents against ARP spoofing
  - **Dynamic lock down**
    - The MAC-IP database is used for inspection of client source MAC and IP address.
    - Prevents against source address spoofing

Possible solutions for IPv6

- SeND (RFC 3971, March 2005)
  - Based on cryptography CGA keys
  - Requires PKI infrastructure
  - Can not work with
    - Manually configured, EUI 64 and Privacy Extension addresses
- RA-Guard (RFC 6105, February 2011)
  - Dropping fake RA messages on access port (RA Snooping)
  - Cooperation with SeND (send proxy) – learning mode
- SAVI (draft-ietf-savi-*, divided into more drafts)
  - Complex solution solving
    - Rouge RA, DHCPv4 an DHCPv6

These solutions have not been widely implementation yet.

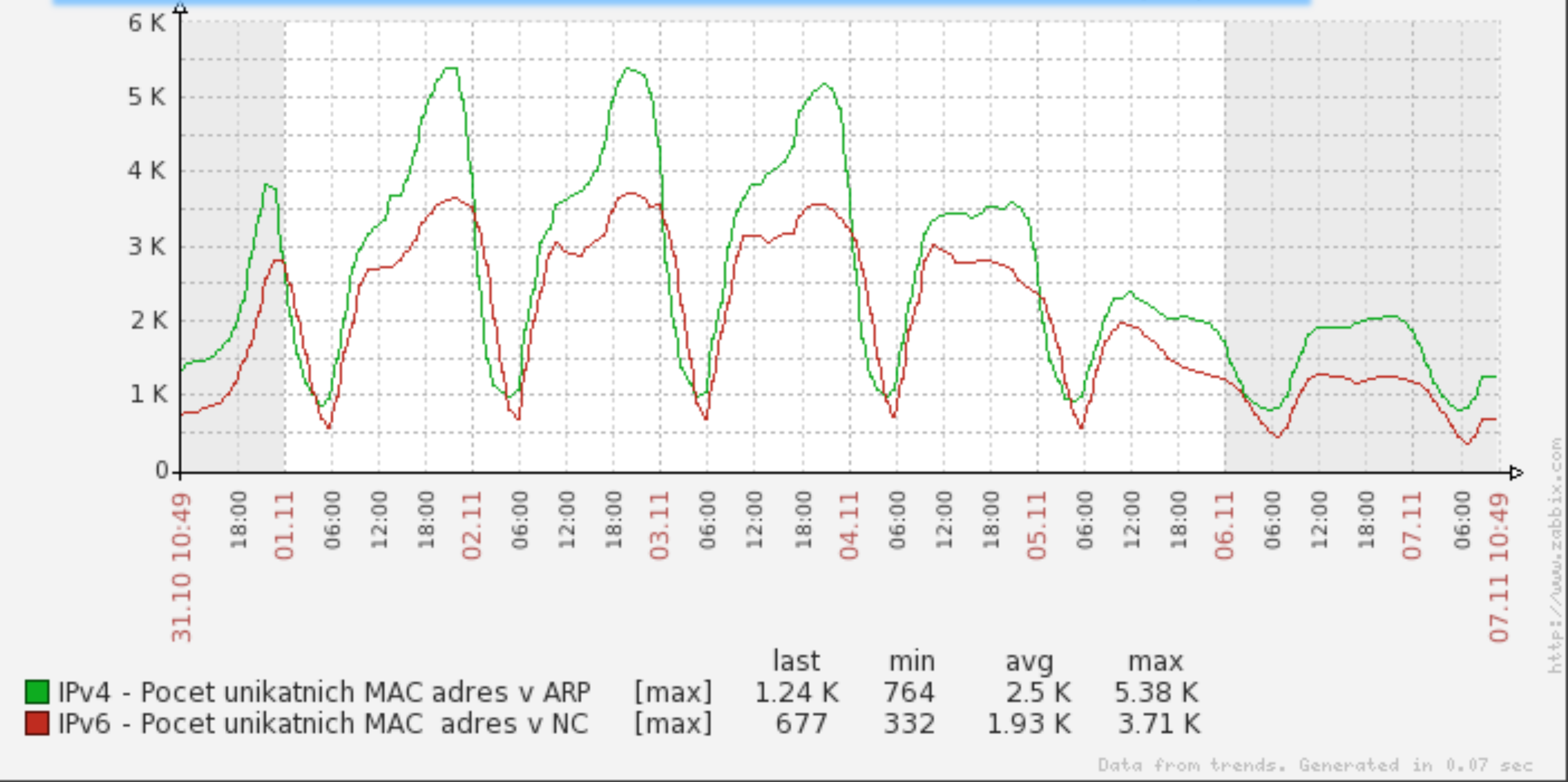
Either is not possible to buy a device supporting any kind of this protection or implementations are available on devices that are more expensive.

But things going to be better:

Cisco Catalyst 2960 (new models)

H3C (HP) 4800

Number of MAC addresses in NC and ARP table



		last	min	avg	max
🟩 IPv4 - Pocet unikatnich MAC adres v ARP	[max]	1.24 K	764	2.5 K	5.38 K
🟥 IPv6 - Pocet unikatnich MAC adres v NC	[max]	677	332	1.93 K	3.71 K

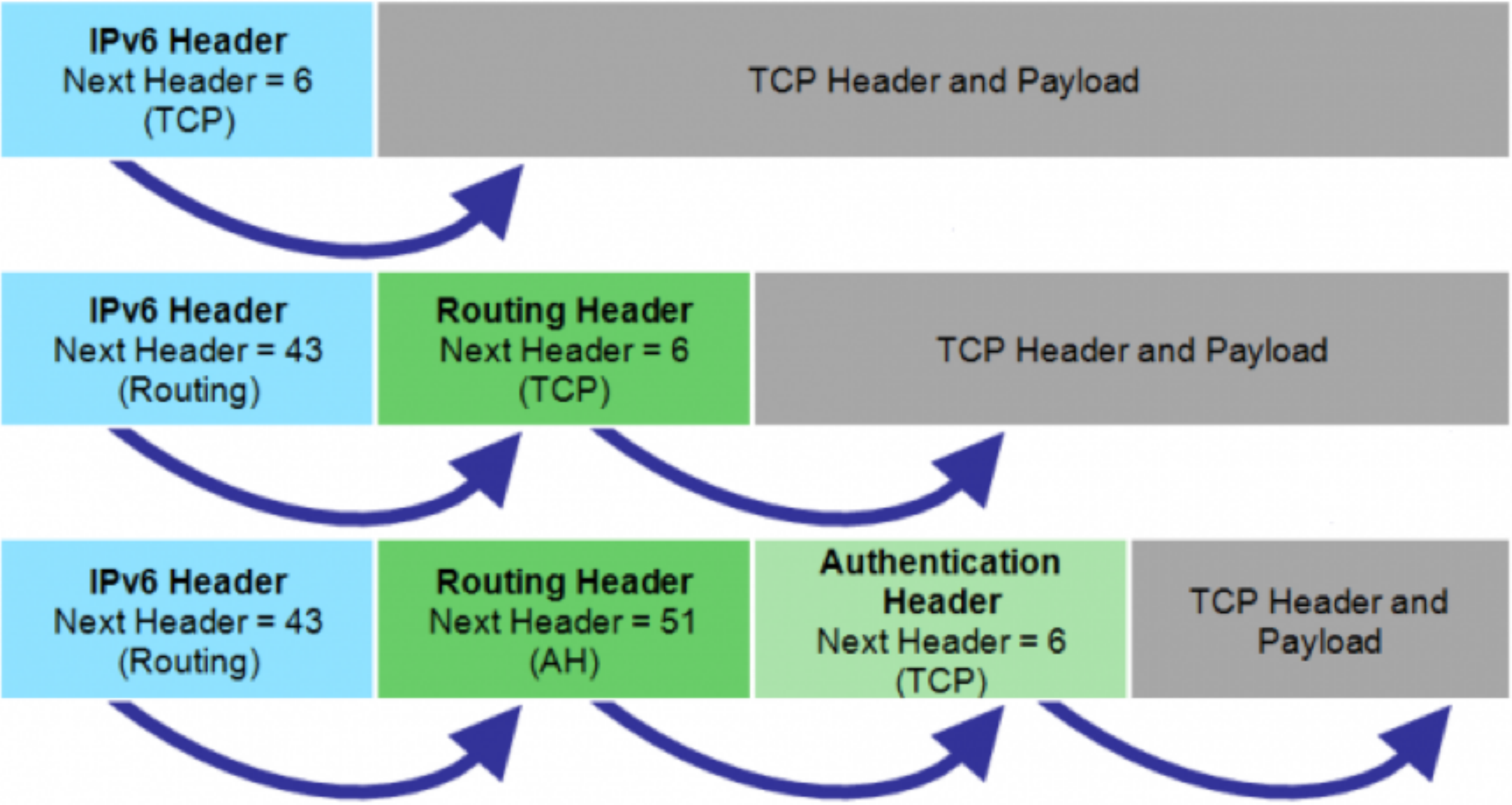
Data from trends. Generated in 0.07 sec

How to mitigate impact of those attacs

- Setup an native connectivity into network
- Prefix monitoring and sending alerts
  - ramond - http://ramond.sourceforge.net/
  - rafixd - http://www.kame.net/
  - ndpmon - http://ndpmon.sourceforge.net/
  - scapy6 - http://hg.natisbad.org/scapy6/
- Blocking unwanted traffic on access ports
  - Taken from:http://www.cesnet.cz/ipv6/wg/p/1006-detekce-routeru.pdf

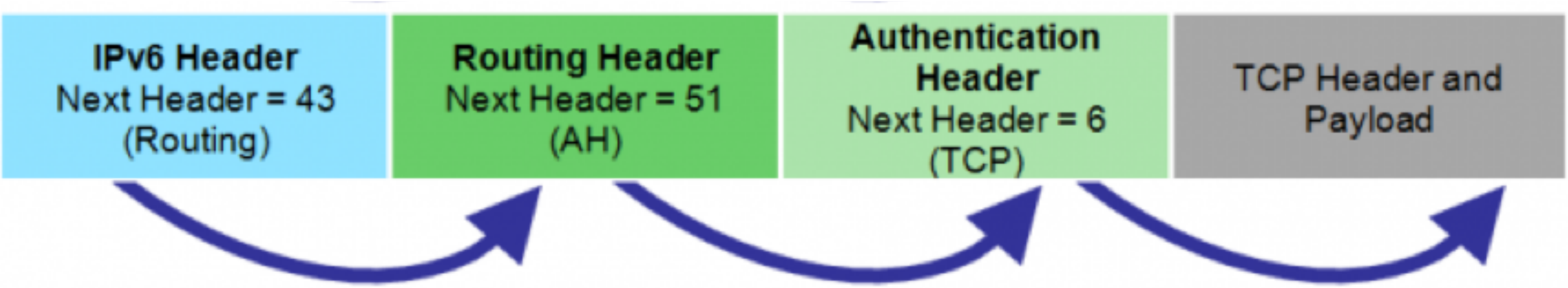
```
ipv6 access-list block-ra-dhcp
     10 deny icmp any any 134 0
     20 deny udp any eq 547 fe80::/64 eq 546
     30 permit ipv6 any any
     exit
interface 1-44
ipv6 access-group block-ra-dhcp in
```

Extension headers



Extension headers

- Mechanism allows to add new features into IPv6
- Chain of headers
  - Protocol:
    - TCP, UDP, ICMPv6, OSPFv3, EIGRP, PIM-SM, …, NULL
  - Extension header:
    - ESP, AH, Hop-by-Hop, Destination, Routing, Fragmentation
- Experimental headers
- Required order



Extension headers

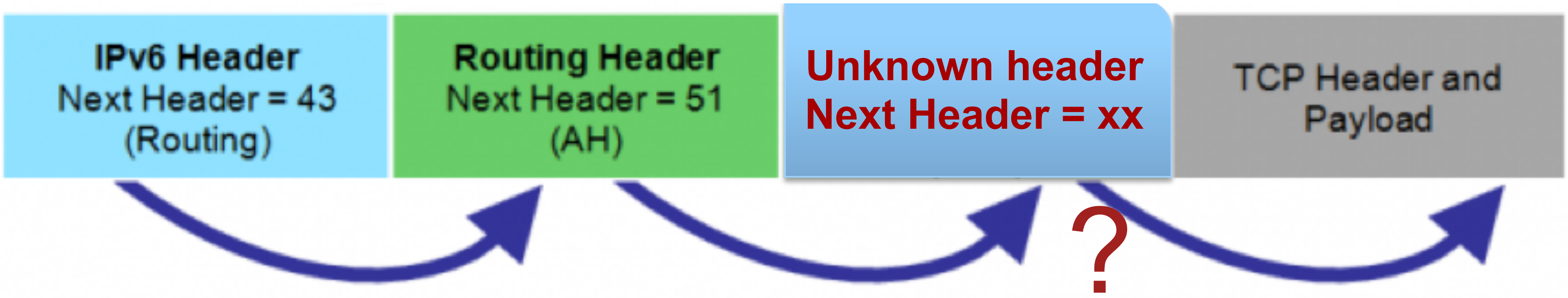
- Routing header (RH0, deprecated by RFC 5095)
- Fragmentation (VRF)
- Extension header manipulation (reorder, long chains of headers)
  - Poor possibility of filtration
  - (do not)try *isic6* – generator of random headers
    - http://isic.sourceforge.net/

```
# ./isic6 -s 2001:2:3:4::1  -d 2001:a:b::1
```

Extension headers or protocol ?

- What happen when a new protocol or header appears ?
  - Expect that header is a protocol an stop processing
    - Drop packet
  - Expect that header is extension header and try to guess next header – process until known header is found

```
config-ipv6-acl# deny ipv6 any any log undetermined transport
```



IPv6 Header
Next Header = 43
(Routing)

Routing Header
Next Header = 51
(AH)

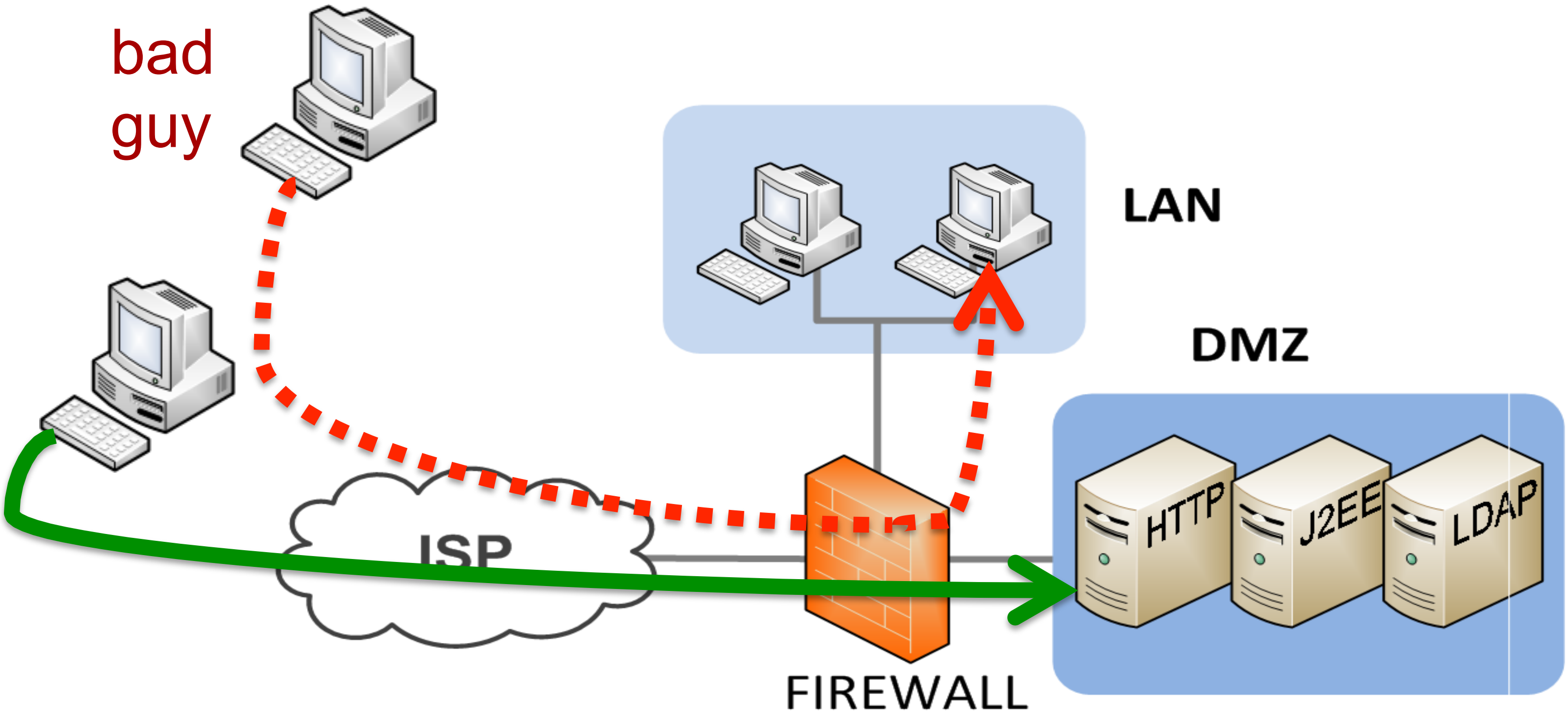
Unknown header
Next Header = xx

TCP Header and
Payload

?

What about IPSec

- IPSec is mandatory in IPv6, encrypts and authenticate communication -> hides content of a communication
- FW, IDS/IPS can not inspect traffic, probes are “blind”
- IPSec traffic should be blocked on the firewall and allowed only for selected addresses or sessions.



Implementation Vulnerabilities in IPv6 so far

- IPv6 was meant to be easy to process and easy to implement.
- Programmers have learned their lessons with IPv4.

Hey, then what can probably go wrong?

Taken from: http://freeworld.thc.org/papers.php

Implementation Vulnerabilities in IPv6 so far

- Microsoft Internet Connection Firewall IPv6 Traffic Blocking Vulnerabilityn Microsoft Windows 2000/XP/2003 IPv6 ICMP Flood Denial Of Service Vulnerability
- Ethereal OSI Dissector Buffer Overflow
- Vulnerabilityn SGI IRIX Snoop Unspecified
- Vulnerabilityn SGI IRIX Snoop Unspecified
- Vulnerabilityn SGI IRIX IPv6 InetD Port Scan
- Denial Of Service Vulnerabilityn Apache Web
- Server FTP Proxy IPv6 Denial Of Service
- Vulnerabilityn Sun Solaris IPv6 Packet Denial of Service Vulnerability
- Multiple Vendor HTTP Server IPv6 Socket IPv4 MappedAddress

Implementation Vulnerabilities in IPv6 so far

- Cisco IOS IPv6 Processing Arbitrary Code Execution Vulnerabilityn Cisco IOS IPv6 Processing Arbitrary Code Execution Vulnerability
- Linux Kernel IPv6 Unspecified Denial of Service Vulnerabilityn HP Jetdirect 635n IPv6/IPsec
- Print Server IKE Exchange Denial Of Service Vulnerabilityn
- 6Tunnel Connection Close State Denial of Service Vulnerability
- HP-UX DCE Client IPv6 Denial of Service Vulnerability
- Multiple Vendor IPv4-IPv6 Transition Address SpoofingVulnerability
- ZMailer SMTP IPv6 HELO Resolved Hostname Buffer Overflow Vulnerability
- Linux Kernel IPv6 FlowLable Denial Of Service Vulnerability
- Linux Kernel IP6_Input_Finish Remote Denial Of Service Vulnerability

Implementation Vulnerabilities in IPv6 so far

- Linux Kernel IP6_Input_Finish Remote Denial Of Service Vulnerability
- Sun Solaris 10 Malformed IPv6 Packets Denial of Service Vulnerability
- Sun Solaris Malformed IPv6 Packets Remote Denial of Service Vulnerability
- Windows Vista Torredo Filter Bypass
- Linux Kernel IPv6 Seqfile Handling Local Denial of Service Vulnerability
- Linux Kernel Multiple IPv6 Packet Filtering Bypass Vulnerabilities
- Cisco IOS IPv6 Source Routing Remote Memory Corruption Vulnerability

Implementation Vulnerabilities in IPv6 so far

- Linux Kernel IPv6_SockGlue.c NULL Pointer Dereference Vulnerability
- Multiple: IPv6 Protocol Type 0 Route Header Denial of Service Vulnerability
- Linux Kernel Netfilter nf_conntrack IPv6 Packet Reassembly Rule Bypass Vulnerability
- Sun Solaris Remote IPv6 IPSec Packet Denial of Service Vulnerability
- Linux Kernel IPv6 Hop-By-Hop Header Remote Denial of Service Vulnerability
- KAME Project IPv6 IPComp Header Denial Of Service Vulnerability
- OpenBSD IPv6 Routing Headers Remote Denial of Service Vulnerability

Implementation Vulnerabilities in IPv6 so far

- Linux Kernel IPv6_Getsockopt_Sticky Memory Leak Information Disclosure Vulnerability
- Linux Kernel IPv6 TCP Sockets Local Denial of Service Vulnerability
- Juniper Networks JUNOS IPv6 Packet Processing Remote Denial of Service VulnerabilityCisco IOS Dual-stack Router IPv6 Denial Of Service Vulnerability
- Multiple Platform IPv6 Address Publication Denial of Service Vulnerabilities
- Microsoft IPv6 TCPIP Loopback LAND Denial of Service Vulnerability
- Handling Vulnerabilityn BSD ICMPV6 Handling
- Routines Remote Denial Of Service Vulnerability

Implementation Vulnerabilities in IPv6 so far

Vulnerability data from June 2008

47 bugs
some multi operating systems
many silently fixed

Taken from: http://freeworld.thc.org/papers.php

Conclusion

- IPv6 have all security issues that IPv4, also have
  - DDoS, Address spoofing, (RH0), Fragmentation, …
- Some attacks are more difficult to perform
  - Scanning
  - Better network filtration
- Some are easier to perform
  - RA, DHCPv6 spoofing, …
  - ICMPv6 – more complex, needs more attention to secure
  - Header reorder, overflow, …
  - Lack of knowledge how to secure the network
- Transition techniques are a new way to perform attacks
  - Avoiding firewalls, probes, IDS, IPS
  - Address behind NAT can be accessible from anywhere
- IPSec is NOT complex solution to solve security issues

What we can do about it ?

- Start using IPv6 immediately
  - We have been waiting for perfect IPv6 more than 15 years - it does not work
  - Until IPv6 is used we will not discover any problem
- Prefer native IPv6 connectivity (anywhere you can)
  - It is a final solution for future (IPv4 will be switched off later)
  - Native IPv6 is more secure than unattended tunneled traffic !
- Ask vendors and creators of standards to fix problems
  - More requests escalate troubles on the vendor side
  - Standardization of IPv6 is not enclosed process. Anyone can contribute or comment the standards
- Stop pretending that IPv6 do not have any troubles
  - IPv6 have got many problems
  - Problems can not be solved by covering them
  - Unreliable information led to broken trust amongst users. The naked truth is always better than the best dressed lie