Weird Packets in a Weird World

(*Show Me Yourrr Interrrnet!*)

Fernando Gont

SI6 NETWORKS

IPv6 Hackers #2
Prague, Czech Republic. July 21, 2015

What is this talk about?

- Weird packet exchanges found in the wild
- This particular case forwarded from Timo Hilbrink
  - Resulting from discussions in the Slo IPv6 Summit

The culprits

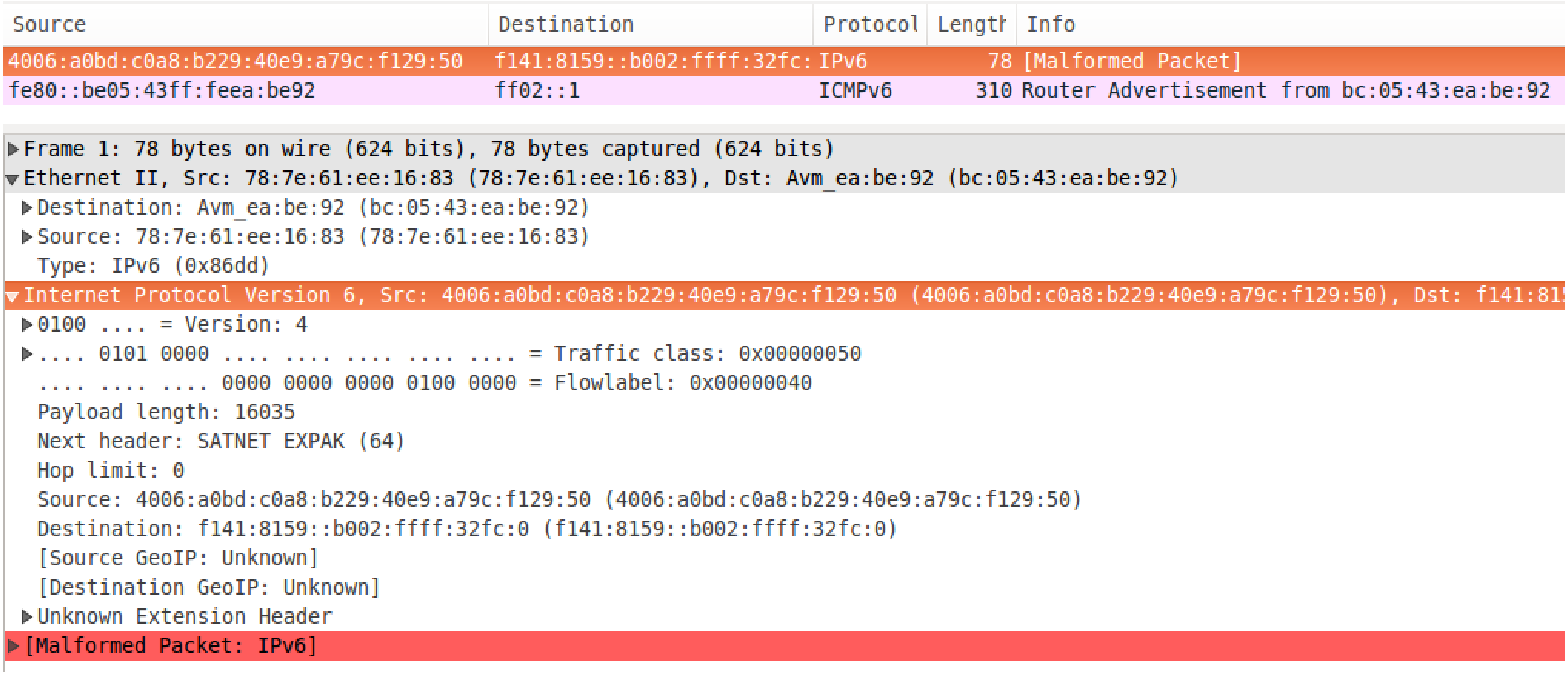
- Apple iOS 8.3
- Fritz!Box CPE

The Crime Scene

```
19:00:02.246726 IP6 truncated-ip6 - 16011 bytes missing!(class 0x50, flowlabel 0x00040,
hlim 0, next-header unknown (64) payload length: 16035)
4006:a0bd:c0a8:b229:40e9:a79c:f129:50 > f141:8159::b002:ffff:32fc:0: ip-proto-64
16035
19:00:02.252529 IP6 (hlim 255, next-header ICMPv6 (58) payload length: 256)
fe80::be05:43ff:feea:be92 > ip6-allnodes: [icmp6 sum ok] ICMP6, router
advertisement, length 256
       hop limit 255, Flags [other stateful], pref high, router lifetime 1800s, reachable time
0s, retrans time 0s
         prefix info option (3), length 32 (4): 4006:a0bd:c0a8:b229::/64, Flags [onlink, auto],
valid time 7200s, pref. time 0s
         prefix info option (3), length 32 (4): 4006:11b:c0a8:b229::/64, Flags [onlink, auto],
valid time 6973s, pref. time 0s
         prefix info option (3), length 32 (4): 4006:3e38:c0a8:b229::/64, Flags [onlink, auto],
valid time 6972s, pref. time 0s
         prefix info option (3), length 32 (4): 2001:980:376d:1::/64, Flags [onlink, auto], valid
time 6603s, pref. time 3600s
         rdnss option (25), length 24 (3):  lifetime 1200s, addr: fd00::be05:43ff:feea:be92
         mtu option (5), length 8 (1):  1500
         unknown option (24), length 8 (1):
         0x0000:  0008 0000 0708
```

So... What happened?

First Packet

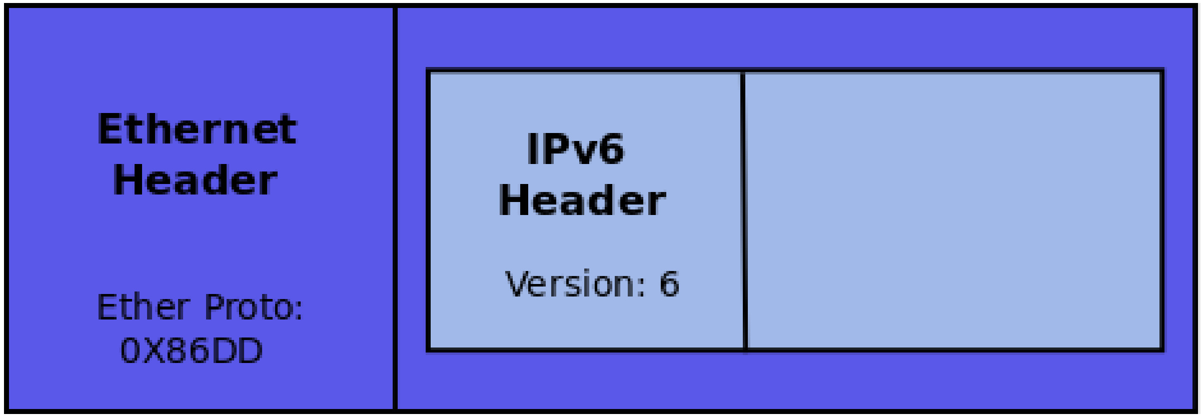


```
Source                                Destination                 Protocol Lengtł Info
4006:a0bd:c0a8:b229:40e9:a79c:f129:50 f141:8159::b002:ffff:32fc: IPv6           78 [Malformed Packet]
fe80::be05:43ff:feea:be92             ff02::1                    ICMPv6        310 Router Advertisement from bc:05:43:ea:be:92
```

```
▶Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
▼Ethernet II, Src: 78:7e:61:ee:16:83 (78:7e:61:ee:16:83), Dst: Avm_ea:be:92 (bc:05:43:ea:be:92)
  ▶Destination: Avm_ea:be:92 (bc:05:43:ea:be:92)
  ▶Source: 78:7e:61:ee:16:83 (78:7e:61:ee:16:83)
   Type: IPv6 (0x86dd)
▼Internet Protocol Version 6, Src: 4006:a0bd:c0a8:b229:40e9:a79c:f129:50 (4006:a0bd:c0a8:b229:40e9:a79c:f129:50), Dst: f141:81
  ▶0100 .... = Version: 4
  ▶.... 0101 0000 .... .... .... .... .... = Traffic class: 0x00000050
   .... .... .... 0000 0000 0000 0100 0000 = Flowlabel: 0x00000040
   Payload length: 16035
   Next header: SATNET EXPAK (64)
   Hop limit: 0
   Source: 4006:a0bd:c0a8:b229:40e9:a79c:f129:50 (4006:a0bd:c0a8:b229:40e9:a79c:f129:50)
   Destination: f141:8159::b002:ffff:32fc:0 (f141:8159::b002:ffff:32fc:0)
   [Source GeoIP: Unknown]
   [Destination GeoIP: Unknown]
  ▶Unknown Extension Header
▶[Malformed Packet: IPv6]
```

IPv6 Version Field

- Identifies the Internet Protocol version number ("6" for IPv6)
- It should match the "Protocol" specified by the underlying link-layer protocol
  - If not, link-layer access controls could be bypassed
- All implementations tested so far properly validate this field.

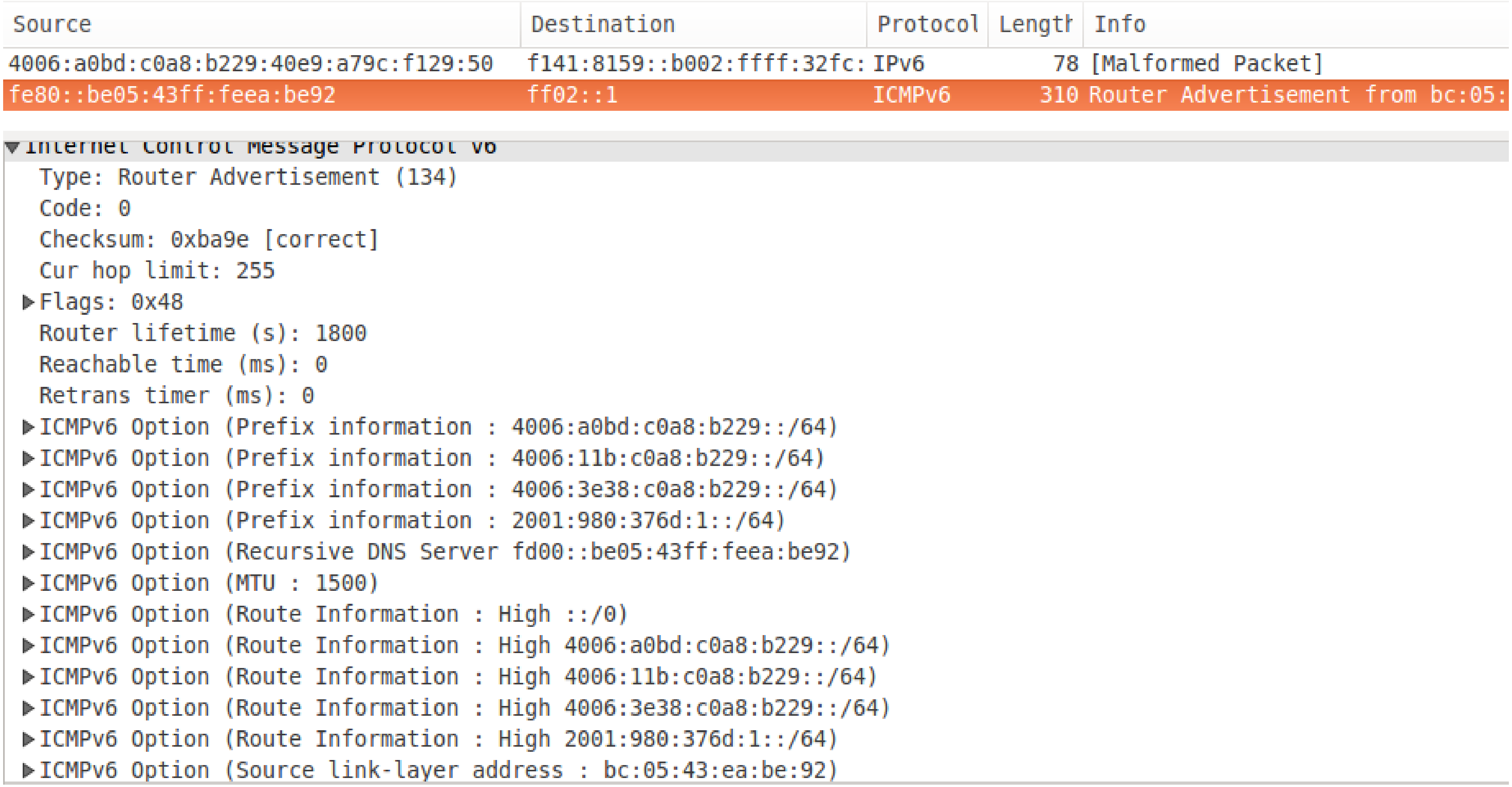


The first packet

- Apple iOS 8.3 sets the IPv6 version field incorrectly
- Fritz!Box CPE does not care about that

You arrrre mental!

Second Packet



```
Source                            Destination                Protocol Length Info
4006:a0bd:c0a8:b229:40e9:a79c:f129:50  f141:8159::b002:ffff:32fc: IPv6     78 [Malformed Packet]
fe80::be05:43ff:feea:be92         ff02::1                    ICMPv6   310 Router Advertisement from bc:05:
```

```
▼Internet Control Message Protocol v6
   Type: Router Advertisement (134)
   Code: 0
   Checksum: 0xba9e [correct]
   Cur hop limit: 255
  ▶Flags: 0x48
   Router lifetime (s): 1800
   Reachable time (ms): 0
   Retrans timer (ms): 0
  ▶ICMPv6 Option (Prefix information : 4006:a0bd:c0a8:b229::/64)
  ▶ICMPv6 Option (Prefix information : 4006:11b:c0a8:b229::/64)
  ▶ICMPv6 Option (Prefix information : 4006:3e38:c0a8:b229::/64)
  ▶ICMPv6 Option (Prefix information : 2001:980:376d:1::/64)
  ▶ICMPv6 Option (Recursive DNS Server fd00::be05:43ff:feea:be92)
  ▶ICMPv6 Option (MTU : 1500)
  ▶ICMPv6 Option (Route Information : High ::/0)
  ▶ICMPv6 Option (Route Information : High 4006:a0bd:c0a8:b229::/64)
  ▶ICMPv6 Option (Route Information : High 4006:11b:c0a8:b229::/64)
  ▶ICMPv6 Option (Route Information : High 4006:3e38:c0a8:b229::/64)
  ▶ICMPv6 Option (Route Information : High 2001:980:376d:1::/64)
  ▶ICMPv6 Option (Source link-layer address : bc:05:43:ea:be:92)
```

The second packet

- A “security feature” in Fritz!Box CPE
- To be removed from their firmware

Questions?

Thanks!

Fernando Gont

fgont@si6networks.com

IPv6 Hackers mailing-list

http://www.si6networks.com/community/

www.si6networks.com