IPv6: ko se v praksi zalomi, če se stvari ne lotimo pravilno...

Andrej Kobal
LPIC, CCSE+, ACE

Vsebina

predstavitev praktičnih izkušenj

- s samodejno konfiguracijo vozlišč
- z usmerjanjem na IPv6 internetu
- z uporabo NAT64

Samodejna konfiguracija odjemalcev – 1

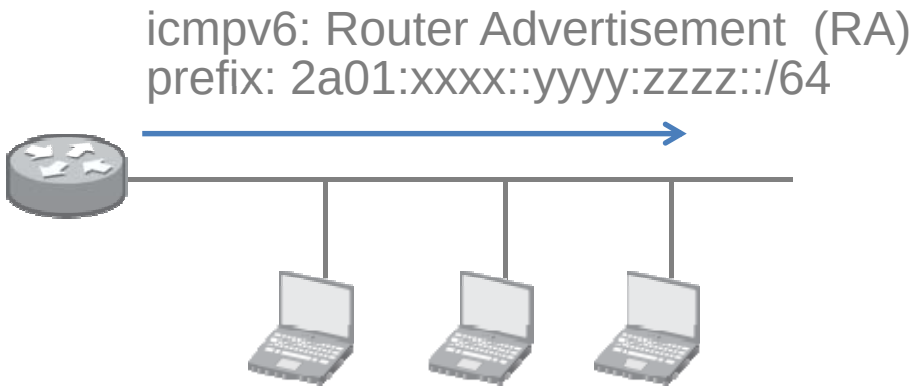
- IPv6 ponuja dve možnosti – SLAAC (RA) in SFAAC (DHCP)
  - včasih je bilo dodeljevanje DNS strežnikov mogoče samo z uporabo SFAAC, danes to ne velja več (RFC-6106)
- sledljivost
  - privzeta konfiguracija Windows odjemalcev predvideva uporabo javnih (public) in začasnih (temporary) naslovov
  - javni naslovi so izračunani neposredno iz MAC naslova (EUI-64), pri začasnih pa se uporabi še algoritem MD5
  - problem – kako naj v lokalnem omrežju sledim odjemalcem, ko pa se njihovi naslovi spreminjajo, v DNS strežnike pa se registrirajo zgolj javni naslovi?
  - rešitev – ukinitev uporabe začasnih naslovov
    - netsh interface ipv6 set global randomizeidentifiers=disabled

Samodejna konfiguracija odjemalcev – 2

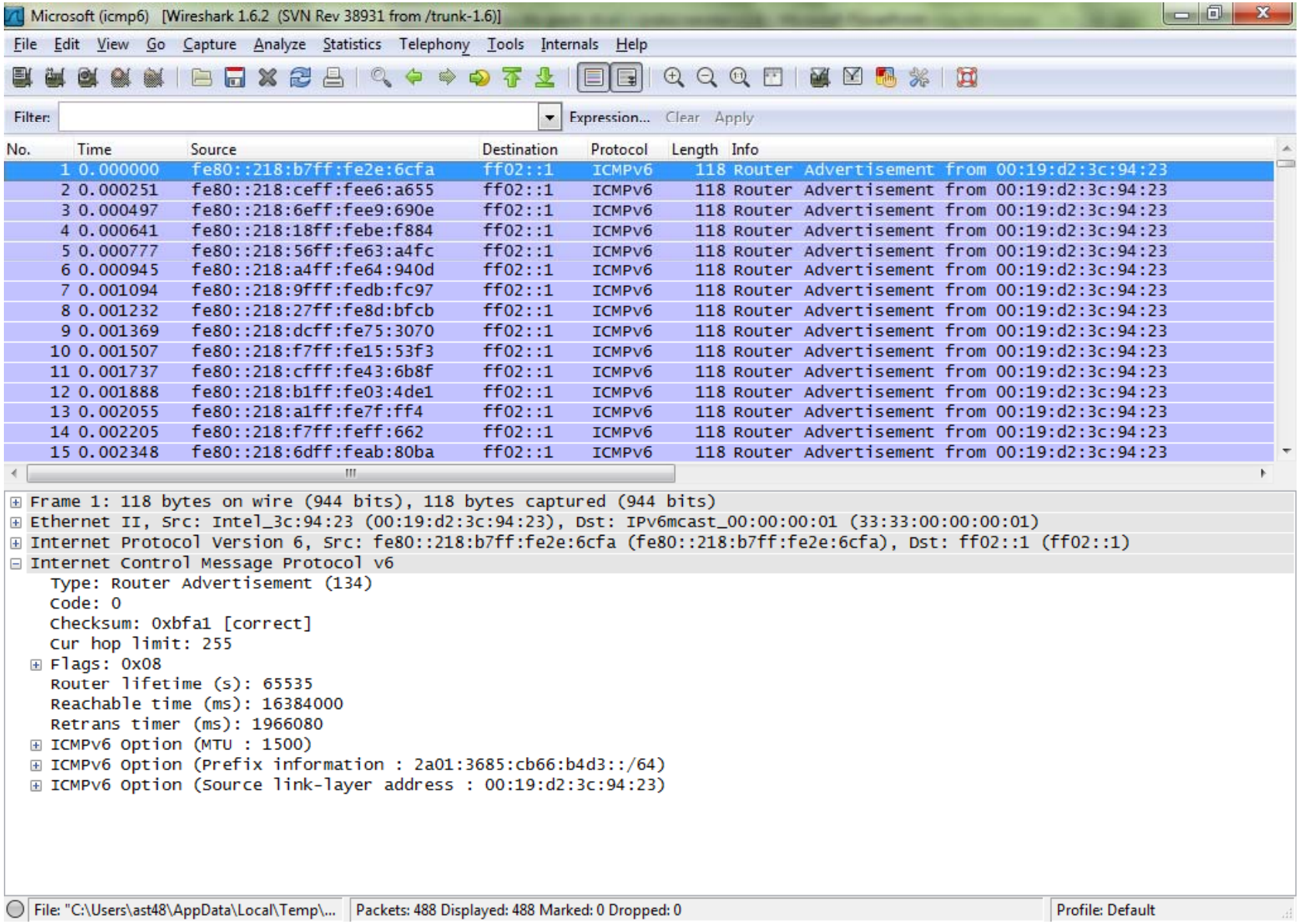
- varnost
  - problem - preusmerjanje prometa v lokalnem omrežju (spoofing) in onemogočanje delovanja s preobremenjevanjem
    - ste že poskusili na Windows odjemalcu vključiti ICS (Internet Connection Sharing)?
  - ozadje – iskanje MAC naslovov in usmerjevalnikov pri IPv6 temelji na uporabi protokola ND (RS/RA/NS/NA)
    - podobno kot pri IPv4 je tudi pri IPv6 mogoče oddati NA (arp-reply) paket brez da bi bil prej oddan NS (arp-request) paket, prav tako ni mogoče preveriti identitete legitimnega vozlišča ali usmerjevalnika
  - rešitev
    - SEcure Neighbor Discovery (SEND, RFC3917)
      - podpora na strani odjemalcev ???
    - omejevanje razširjanja DHCP in RA paketov
      - RA Guard, ND Inspection
      - Port ACL

Samodejna konfiguracija v praksi – 1

- izkoristiti želimo ranljivost v operacijski sistemih Windows (CVE-2010-4669) in preprečiti njihovo delovanje
- kaj potrebujemo?
  - IPv6 omrežje
  - namensko programsko opremo - thc.org/thc-ipv6
    - parasite6 - prevzem identitete sosednjih vozlišč (sleparjenje z NS/NA paketi)
    - fake_router6 – prevzem identitete lokalnega usmerjevalnika (sleparjenje z RA paketi)
    - **flood_router6 – preobremenitev odjemalcev**



Samodejna konfiguracija v praksi – 2

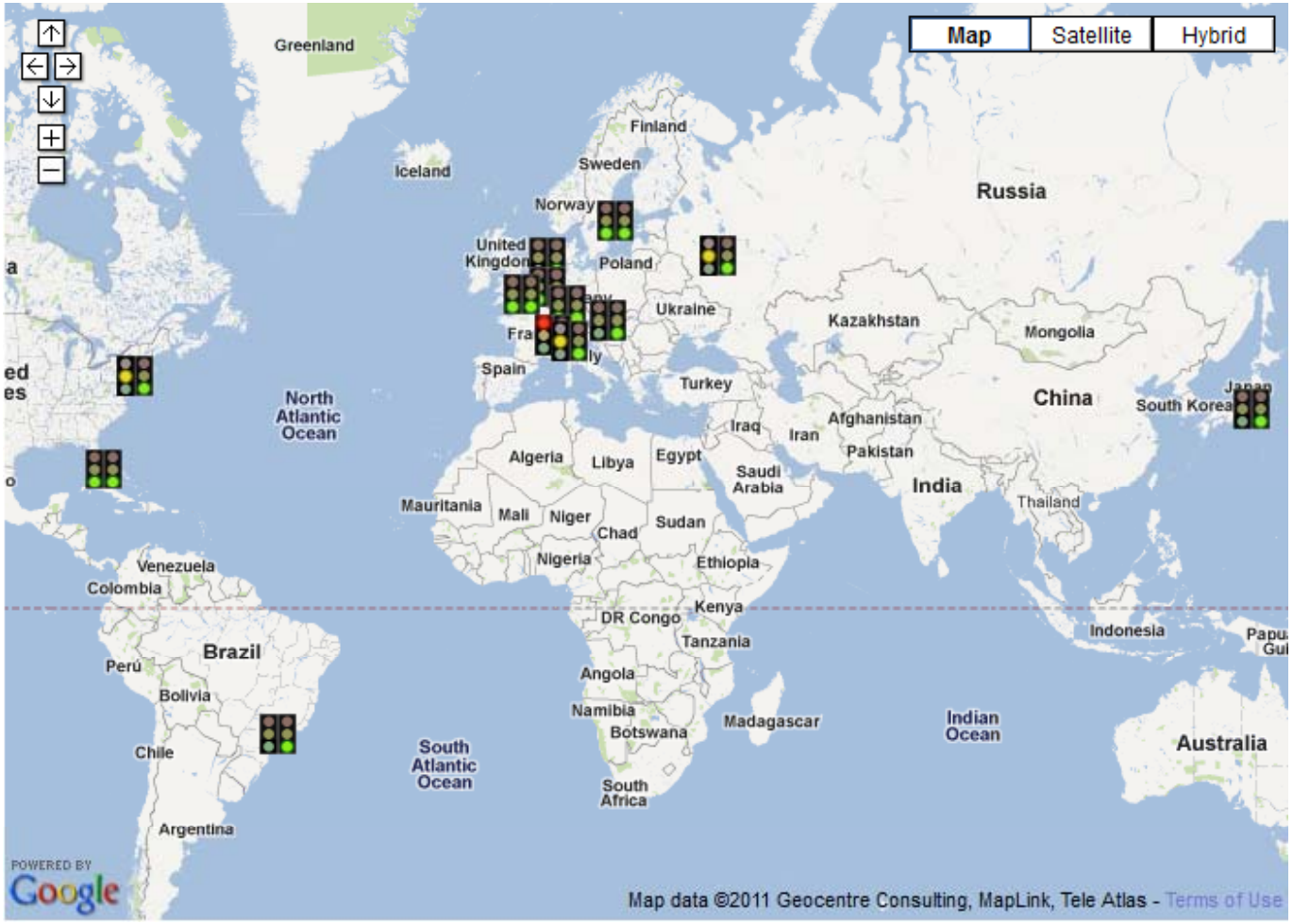


Usmerjanje na IPv6 internetu

- simptom – dostop do support.novell.com (2600:806:310::101) in www.novell.com (2600:806:310::102) ni mogoč
- ozadje – IPv4/IPv6 PI naslovni prostor in redundatni dostop do interneta primarna (Siol – AS5603) in sekundarna (Amis – AS8591)
- analiza – primarni ponudnik dostopa nima poti za 2600:806:310::/48
- rešitev – izmenjava polnih BGP tabel s ponudnikoma dostopa

Usmerjanje na IPv6 internetu v praksi

- http://www.ris.ripe.net/dashboard/2600:806:310::/48



Uporaba NAT64

- simptom – dostop do www6.nil.si iz našega lokalnega omrežja ni mogoč
- analiza – zajem prometa na naši požarni pregradi (CheckPoint) je pokazal nenavadno uporabo fragmentacijskih glav (fragmentacija SYN-ACK paketov)
- kaj vraga se tukaj dogaja? je kriv kakšem FW ali IPS? je kriv kakšen ponudnik dostopa?
  - NE, kriva je uporaba NAT64 in različno tolmačenje RFC6145

  "When the IPv4 sender does not set the DF bit, the translator SHOULD always include an IPv6 Fragment Header to indicate that the sender allows fragmentation. "...

Uporaba NAT64 – podrobneje

- uporaba DF=0 v fazi vzpostavitve TCP seje na www.nil.si ...

(tos 0x0, ttl 64, id 44934, offset 0, flags [DF], proto: TCP (6), length: 60) 91.220.107.100.45371 > 193.110.145.36.http: S, cksum 0x7fa6 (correct), 3394961667:3394961667(0) win 5840 <mss 1460,sackOK,timestamp 1940500101 0,nop,wscale 7>

(tos 0x0, ttl 122, id 16421, offset 0, **flags [none]**, proto: TCP (6), length: 44) **193.110.145.36**.http > 91.220.107.100.45371: S, cksum 0x8bea (correct), 3636242822:3636242822(0) ack 3394961668 win 64240 <mss 1360>

(tos 0x0, ttl 64, id 44935, offset 0, flags [DF], proto: TCP (6), length: 40) 91.220.107.100.45371 > 193.110.145.36.http: ., cksum 0x8764 (correct), 1:1(0) ack 1 win 5840

(tos 0x0, ttl 64, id 44936, offset 0, flags [DF], proto: TCP (6), length: 157) 91.220.107.100.45371 > 193.110.145.36.http: P, cksum 0xc776 (correct), 1:118(117) ack 1 win 5840

(tos 0x0, ttl 122, id 16424, offset 0, **flags [DF]**, proto: TCP (6), length: 310) **193.110.145.36**.http > 91.220.107.100.45371: P, cksum 0xc4c5 (correct), 1:271(270) ack 118 win 64123

(tos 0x0, ttl 64, id 44937, offset 0, flags [DF], proto: TCP (6), length: 40) 91.220.107.100.45371 > 193.110.145.36.http: ., cksum 0x8391 (correct), 118:118(0) ack 271 win 6432

(tos 0x0, ttl 122, id 16425, offset 0, **flags [DF]**, proto: TCP (6), length: 1400) **193.110.145.36**.http > 91.220.107.100.45371: ., cksum 0x3696 (correct), 271:1631(1360) ack 118 win 64123

(tos 0x0, ttl 64, id 44938, offset 0, flags [DF], proto: TCP (6), length: 40) 91.220.107.100.45371 > 193.110.145.36.http: ., cksum 0x7231 (correct), 118:118(0) ack 1631 win 9520

Uporaba NAT64 – podrobneje

- ... pomeni fragmentacijo SYN-ACK paketa v primeru www6.nil.si

2001:67c:2014::100.37129 > 2001:67c:58:e01::1.http: S 389912685:389912685(0) win 32752 <mss 16376,sackOK,timestamp 3564800031 0,nop,wscale 7>

2001:67c:58:e01::1 > 2001:67c:2014::100: **frag (0|24)** http > 37129: S 3261309035:3261309035(0) ack 389912686 win 64240 <mss 1360>

2001:67c:2014::100.37129 > 2001:67c:58:e01::1.http: . ack 1 win 32752

2001:67c:2014::100.37129 > 2001:67c:58:e01::1.http: P 1:117(116) ack 1 win 32752

2001:67c:58:e01::1.http > 2001:67c:2014::100.37129: P 1:271(270) ack 117 win 64124

Uporaba NAT64

- trenutna rešitev – spreminjanje vrednosti DF (0->1)
- zaželena rešitev – konfiguracijska opcija na NAT64 prevajalniku (RFC6145)

  "The translator MAY provide a configuration function that allows the translator not to include the Fragment Header for the non-fragmented IPv6 packets."

- nauk – nove mrežne tehnologije velja uvajati premišljeno, sodelovanje med različnimi akterji je ključnega pomena (Astec/ Nil + Amis + Arnes)

?
?
?
?
?
?
?
?
?

Astec d. o. o.
Stegne 31

W: www.astec.si
T: +386 1 2008300
F: +386 1 2008310

andrej.kobal@astec.si