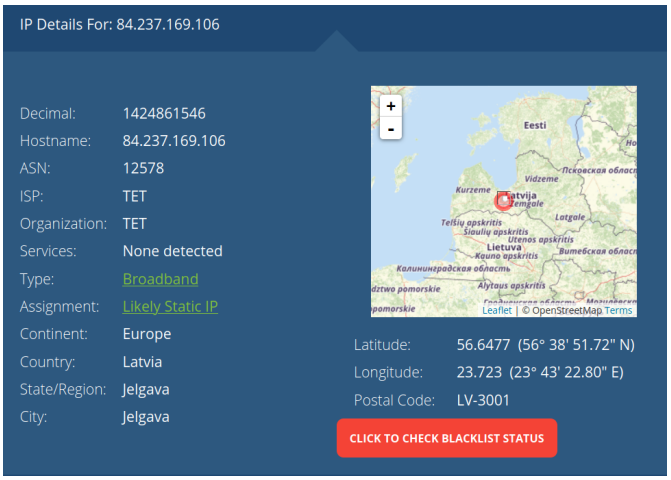
Pēteris Račinskis
pr20015

Mājas darbs 2: BGP tabulas

Uzdevums A

1. *Savas IP adreses ieraksta atrašana*

Ja mērķis ir vienkārši sasniegt rezultātu, šo uzdevumu var atrisināt triijos soļos: ierakstot interneta meklētājā “what’s my ip”, atrodot rezultātu ar detalizētu informāciju un tabulā atrodot subnet, kurā ietilpst adrese.



1. att. Apkopots rezultāts - IP adrese un ASN - kādā internetā pieejamā pakalpojumā.

```
[peter@peter-laptop-old:~/Downloads/bgp2021]$ cat ipv4bgp2021apnic.txt | grep ' 84.237' | grep 12578
*  84.237.128.0/17  202.12.28.1                          0 4777 2516 3257 12578 i
*  84.237.235.0/24  202.12.28.1                          0 4777 2516 3257 12578 44698 i
[peter@peter-laptop-old:~/Downloads/bgp2021]$
```

2. Ieraksta atrašana pēc IP adreses un ASN. Palikuši tikai divi ieraksti, un pēc subnet mask redzams, ka autora adrese pieder pirmajam.

Ja šī metode nav pieņemama un nepieciešams noskaidrot, kā tieši šī informācija ir iegūta, IP adresi un ASN iespējams noteikt no komandrindas. Tā kā autora dators atrodas lokālajā tīklā zem pakalpojuma sniedzējam piederoša maršrutizatora, nekādas informācijas par publisko tīkla adresi pašā datorā nav - jāaptaujā ārējs serveris. Ir dažādi serveri, kas uz dažādiem pieprasījumiem dažādos protokolos atbildēs ar klienta IP adresi:

```
[peter@peter-laptop-old:~/Downloads/bgp2021]$ curl ipinfo.io/ip && echo ''
84.237.169.106
[peter@peter-laptop-old:~/Downloads/bgp2021]$ dig +short myip.opendns.com @resolver1.opendns.com
84.237.169.106
[peter@peter-laptop-old:~/Downloads/bgp2021]$
```

3. att. Divas metodes savas publiskās IP adreses noteikšanai no komandrindas - HTTP un DNS lookup pieprasījumi.

Kad noteikta IP adrese, jāaptaujā kāda datubāze, kurā ir tai atbilstošie reģistrācijas dati.

```
[peter@peter-laptop-old:~/Downloads/bgp2021]$ telnet whois.apnic.net 43
Trying 139.162.237.51...
Connected to whois.apnic.net.
Escape character is '^]'.
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

84.237.169.106
% Information related to '84.0.0.0 - 84.255.255.255'

% No abuse contact registered for 84.0.0.0 - 84.255.255.255

inetnum:        84.0.0.0 - 84.255.255.255
netname:        RIPE-CIDR-BLOCK
descr:          Not allocated by APNIC
remarks:        ------------------------------------------------
remarks:
remarks:        Important:
remarks:
remarks:        Details of networks in this range are not registered
remarks:        in the APNIC Whois Database.
remarks:
remarks:        Please search the RIPE Whois Database, which contains
remarks:        details of IP addresses allocated in Europe, the
remarks:        Middle East, and northern Africa:
remarks:
remarks:        website:      http://www.ripe.net/perl/whois
remarks:        command line: whois.ripe.net
remarks:
```

4. att. Aptaujājot whois.apnic.net, vaicātājs tiek nosūtīts uz whois.ripe.net.

```
[peter@peter-laptop-old:~]$ telnet whois.ripe.net 43
Trying 193.0.6.135...
Connected to whois.ripe.net.
Escape character is '^]'.
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

84.237.169.106
% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '84.237.128.0 - 84.237.191.255'
```

5 . att. Datu bāze uzreiz atrod atbilstošo subnet.

```
% Information related to '84.237.128.0/17AS12578'

route:          84.237.128.0/17
descr:          LATTELEKOM
origin:         AS12578
mnt-by:         LTK
created:        2004-07-27T09:33:12Z
last-modified:  2004-07-27T09:33:12Z
source:         RIPE
```

6. att. Kā arī iekļauj informāciju par ASN.

```
[peter@peter-laptop-old:~/Downloads/bgp2021]$ cat ipv4bgp2021apnic.txt | grep 84.237.128.0/17
*   84.237.128.0/17  202.12.28.1                          0 4777 2516 3257 12578 i
[peter@peter-laptop-old:~/Downloads/bgp2021]$
```

7. att. Ar ko pietiek, lai uzreiz atrastu ierakstu BGP tabulā.

2. AS ar lielāko ierakstu skaitu

Nākamais uzdevums ir atrast AS ar vislielāko ierakstu skaitu tabulā. Tas nenozīmē lielāko AS pieejamo IP adrešu skaita ziņā, jo netiek ņemti vērā masku garumi - pirmajās vietās ir tās AS, kam izdalīts lielāks skaits atsevišķu apakštīklu, neatkarīgi no to izmēriem. Turklāt iespējams, ka lielākām organizācijām ir vairākas AS. Lai šo skaitu iegūtu, izmantots vienkāršs Python skripts, kas:

- nolasa katru tabulas rindu;
- nosaka, vai tajā ir subnet IP adrese;
- nosaka, vai tajā ir īzvēlētais ceļš (marķēts ar *>);
- salgabā aktuālo IP un ceļu, kad atrasts izvēlētais ceļš, vispirms noņemot duplikātus (kas rodas, ja tiek izmantots BGP path padding un ieraksts var tikt daudzas reizes atkārtots).

No iegūtā saraksta pēc tam var aprēķināt populārākos ASN un garākos ceļus. Saskaitot ASN un sašķirojot dilstošā secībā iegūst pirmo izdrukas pusi, populārākos ASN:

```
[peter@peter-laptop-old:~/DT2_MD2/bgp2021]$ ./ascount.py ipv4bgp2021apnic.txt
Most common ASNs:
ASN: 8151       Count: 8396
ASN: 47331      Count: 7751
ASN: 12479      Count: 6368
ASN: 7545       Count: 5709
ASN: 16509      Count: 4872
ASN: 4538       Count: 4838
ASN: 11492      Count: 4752
ASN: 7155       Count: 4030
ASN: 22773      Count: 3903
ASN: 9808       Count: 3757
```

8. att. Visbiežākie AS ieraksti tabulā.

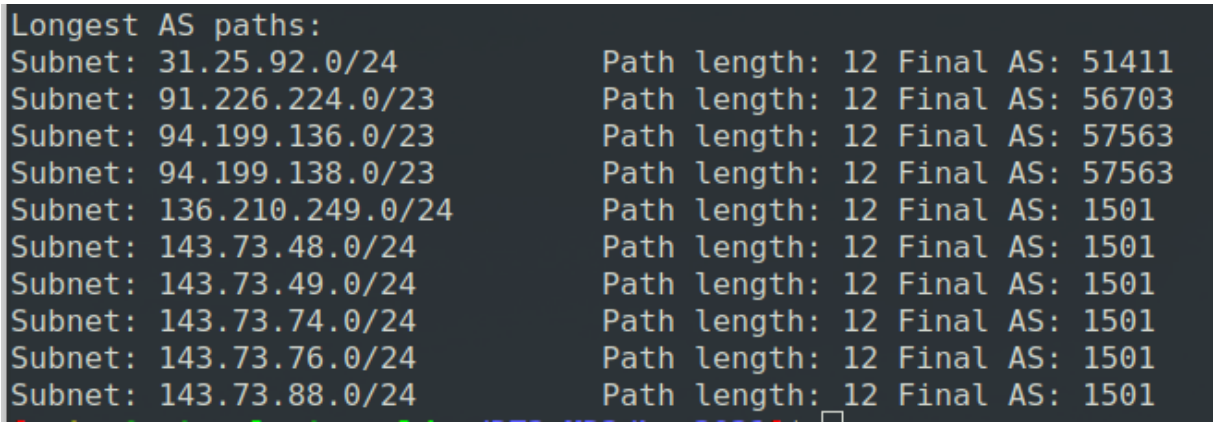
Pārbaudot whois datubāzē, noteikts:

- AS8151: Uninet, ISP Meksikā (lacnic).
- AS47331: Türk Telekom, ISP Turcijā (ripe).
- AS12479: Orange Espagne, ISP Spānijā (ripe).

Mazliet pārsteidzoši, ka pirmajā trijniekā nav nevienas labi zināmas starptautiskas organizācijas, taču paskatoties nedaudz zemāk sarakstā var atrast tādas AS kā 16509 (pieder Amazon), 7155 (ViaSat backbone).

3. Subneti ar lielāko tranzīta AS skaitu

Izmantojot to pašu skriptu, iespējams iegūt arī garākos ceļus. Tā kā duplikāti izņemti jau saraksta veidošanas procesā, pietiek to sašķirot pēc ceļā esošo unikālo ASN garuma:



9. att. 10 no "tālākajiem" tīkliem.

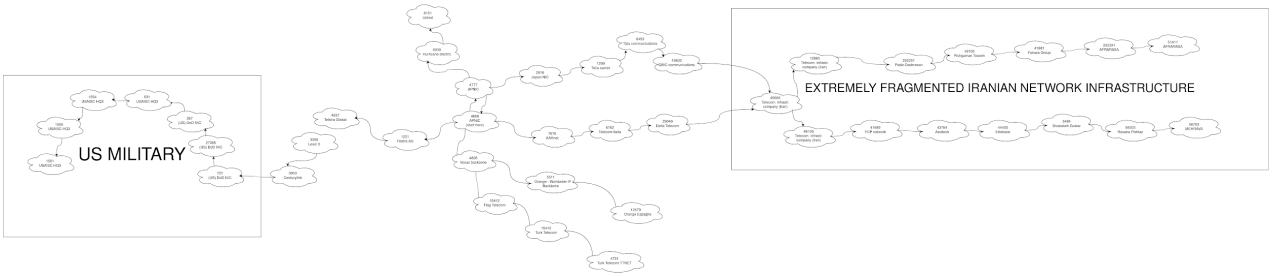
Tā kā visu garumi ir vienādi, nejauši izvēlēti tīkli ir:

- 136.210.249.0/24:
  - Subnet: 136.210.0.0/16, US Army Information Systems Command HQ 3. Izdalīts atsevišķi jo 136.210.0.0 sasniedzams caur AS1555 (priekšpēdējo soli); visticamāk kaut kāda atsevišķa struktūrvienība. Šajā pašā AS atrodami diezgan daudzi citi subneti, droši vien visas kaut kādas vienības un instalācijas dislocētas Fort Huachuca garnizonā Arizonas štatā.
  - AS: AS1501, USAIC HQ3 (arin)
- 91.226.224.0/23:
  - Subnet: tas pats, Mehr Ava Gostar Parsian Information Engineering Co.,ltd (Irāna, ISP?)
  - AS: AS56703, tas pats īpašnieks (ripe)
- 31.25.92.0/24:
  - Subnet: Parsis-Net, iespējams vēl kāds Irānas ISP - taču informāciju sīkāk nevar atrast.
  - AS: AS51411, Toos-Ashena PJSC, ISP/web hosting Irānā (ripe).

Interesanti novērot, ka ASV bāzētām AS ir zemāki kārtas skaitļi, piešķirti senāk.

4. Grafisks attēls

Pilns attēls pielikumā.



10. att. IPv4 AS maršrutu grafisks attēlojums. Interesantas paralēles starp ASV militāro un Irānas it kā civilo tīkla infrastruktūru.

Uzdevums B

1. AS ar lielāko subnet skaitu, garākie tranzīta ceļi

Nedaudz "satīrot" ipv6 tabulu, lai iegūtu tādu pašu formātu, iespējams ar minimālām izmaiņām to pašu skriptu izmantot arī uzdevumam ar ipv6. Tātad analoģiski:

```
[peter@peter-laptop-old:~/DT2_MD2/bgp2021]$ ./ascount.py c_ipv6.txt
Total number of unique final AS: 21693
Most common ASNs:
ASN: 11172      Count: 2889
ASN: 17622      Count: 2112
ASN: 45609      Count: 2081
ASN: 16509      Count: 1543
ASN: 12479      Count: 1492
ASN: 9808       Count: 1430
ASN: 45271      Count: 1369
ASN: 28573      Count: 1232
ASN: 22773      Count: 1225
ASN: 7552       Count: 1159
```

11. att. Biežākie gala ASN.

```
Longest AS paths:
Subnet: 2a07:e440::/29          Path length: 9  Final AS: 59441
Subnet: 2a0b:b400::/29          Path length: 9  Final AS: 207141
Subnet: 2406:5880::/32          Path length: 8  Final AS: 58844
Subnet: 2406:8080::/32          Path length: 8  Final AS: 58844
Subnet: 2406:8b80::/32          Path length: 8  Final AS: 58844
Subnet: 2600:c800::/32          Path length: 8  Final AS: 6079
Subnet: 2600:c806::/32          Path length: 8  Final AS: 6079
Subnet: 2605:6f40::/32          Path length: 8  Final AS: 6079
Subnet: 2606:bc0::/32           Path length: 8  Final AS: 6079
Subnet: 2801:15:7000::/48       Path length: 8  Final AS: 269867
```

12. att. Garākie tranzīta ceļi ipv6 bgp tabulā.

ASN:

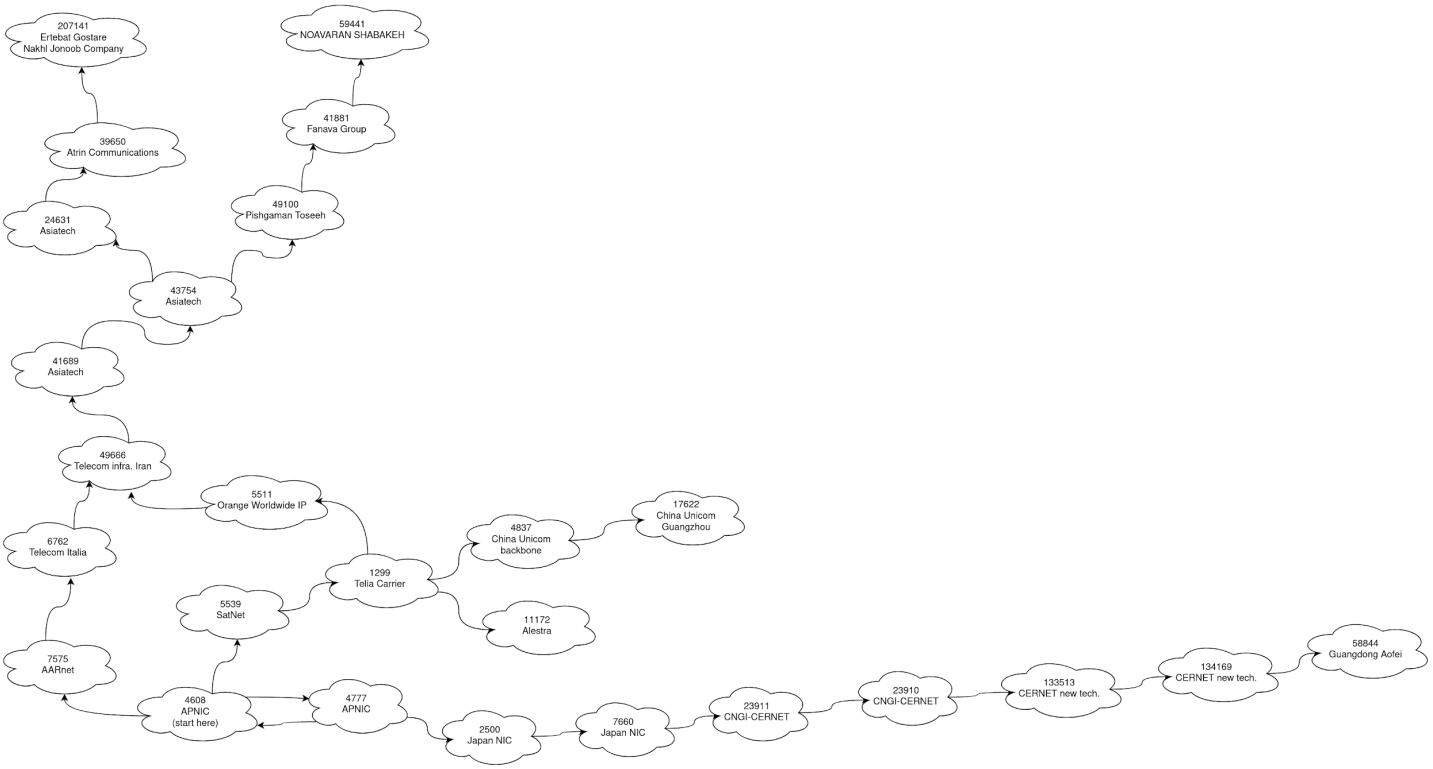
- AS11172: Alestra, ISP Meksikā (lacnic);
- AS17622: China Unicom Guangzhou network, ISP Ķīnā (apnic);
- AS45609: Bharti Airtel Ltd., autonomā sistēma GPRS pakalpojumiem - mobilais ISP Indijā (apnic).

Tālākie subneti:

- 2a07:e440::/29: NOAVARAN SHABAKEH SABZ MEHREGAN (Ltd.) - droši vien ISP vai cita veida IT firma Irānā, bet par Irānas firmām principā informācijas maz. AS59441 (ripe);
- 2a0b:b400::/29: Ertebat Gostare Nakhl Jonoob Company PJSC, atkal Irānā - grūti spriest, kas tas tieši ir. AS207141 (ripe);
- 2406:5880::/32: Guangdong Aofei Data Technology Co Ltd, hostinga pakalpojumu sniedzējs Ķīnā. AS58844 (apnic).

2. Grafisks attēls

Pilns attēls pieejams pielikumā.



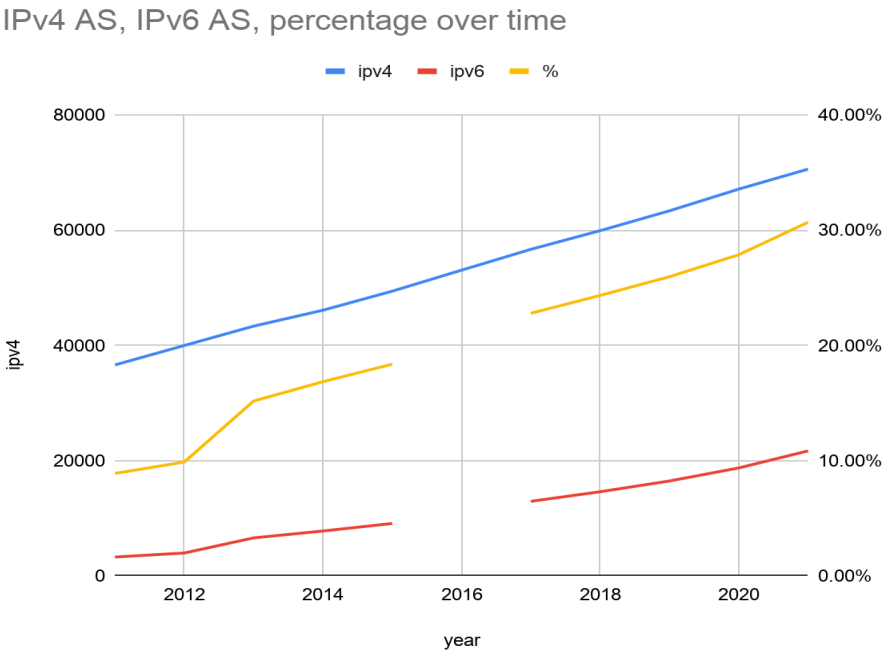
13. att. IPv6 AS maršruta attēls

3. Aptuvens ipv4-ipv6 atbalstošo AS skaita salīdzinājums

Lai varētu veikt nopietnu pētījumu par izdalīto IP adrešu skaitu un dažādo AS sniegto atbalstu IPv6 izmantošanai, ar BGP tabulās pieejamajiem datiem nevar pat

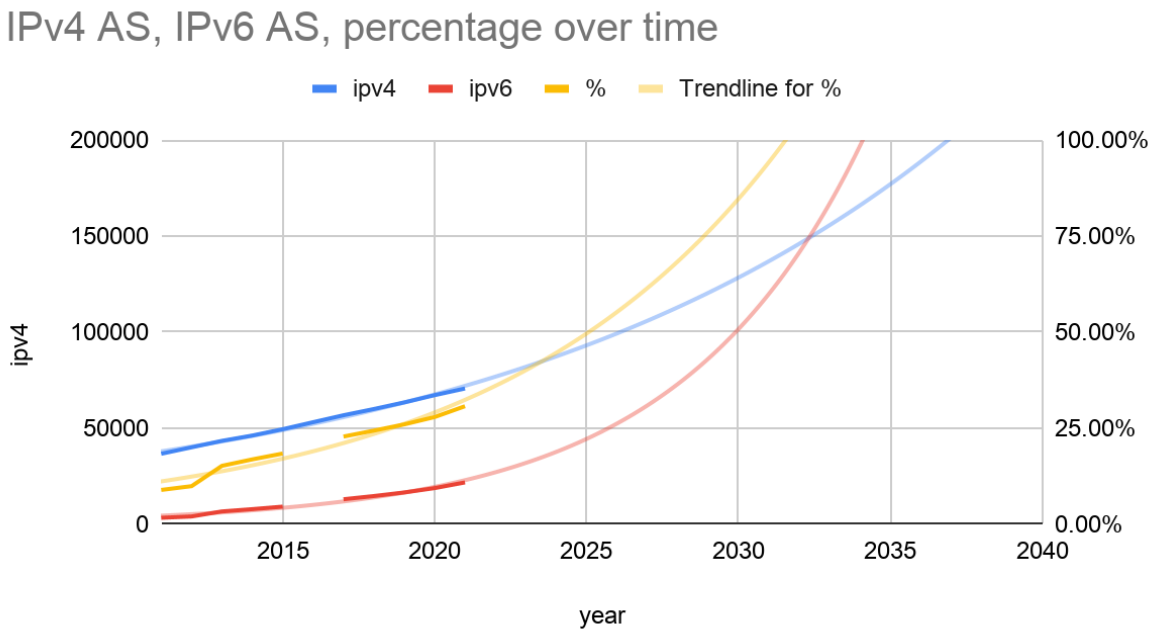
sākt. Taču var gūt ļoti aptuvenu, orientējošu priekštatu par relatīvo AS skaitu katrā sistēmā, vienkārši salīdzinot unikālo ASN skaitu katrā tabulā. Var izmantot jau iepriekš sagatavoto skriptu, un pieņemt, ka AS atbalsta IPv6, ja vismaz viens subnet ir norādīts kā tai iekšējs (t.i., pēdējais maršrutā). Protams, nekāda robustā metodoloģija tā nav, taču pēc autora domām ar to pietiek ātriem "salvetes" aprēķiniem. Iegūtie dati apkopoti pielikumā iekļautajā "results.txt" failā.

Jāņem vērā, ka netiek pievērsta nekāda uzmanība tam, vai AS apkalpo gan IPv4, gan IPv6 tīklus, tiek vienkārši izteikts IPv6 apkalpojošo AS skaits relatīvi IPv4 apkalpojošo AS skaitam.



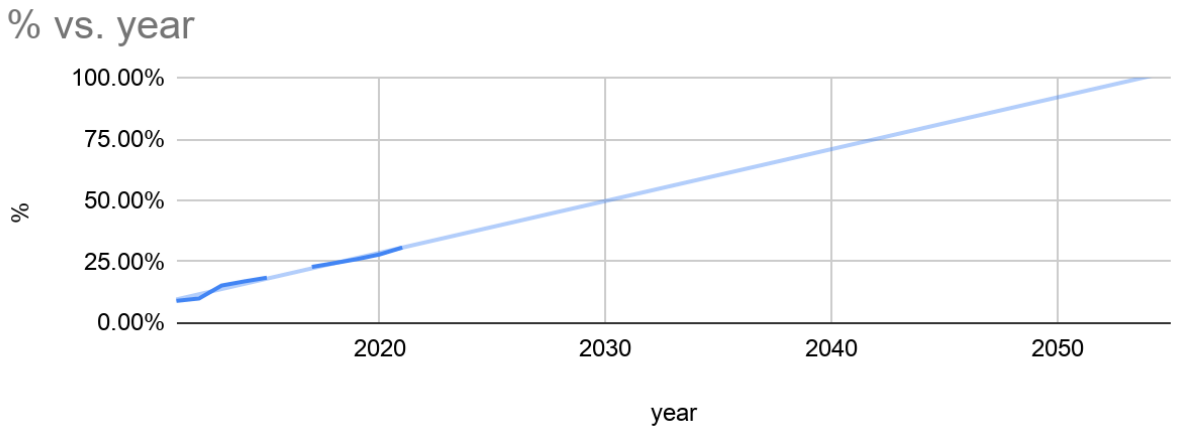
14. att. IPv4, IPv6 subnet atbalstošo AS skaits, relatīvs salīdzinājums.

Autors neuzskata, ka no šādiem ļoti neprecīzā veidā iegūtiem datiem par īsu laika periodu ir liela jēga mēģināt ekstrapolēt kādus nākotnes rezultātus. Tīri intereses pēc ļaujot Google Sheets ekstrapolatoram (kas gan primāri paredzēts vizuāli izskatīgu efektu zīmēšanai) iezīmēt eksponenciālas izaugsmes līknes gan absolūtajiem skaitļiem, gan to attiecībai, izskatās, ka IPv6 atbalstošo AS skaitam vajadzētu apsteigt IPv4 atbalstošās ap 2030-2035 gadu:



15. att. Optimistiska ekstrapolācija no maz ticamiem datiem.

Taču lineāri ekstrapolējot attiecību, 100% varētu sasniegt ap 2055 gadu:



16. att. Pesimistiska ekstrapolācija no maz ticamiem datiem.

Autors netic šiem rezultātiem, taču ja secinājums jāizdara, tad attiecīgi apsteigšanas brīdis varētu būt periodā starp 2030. un 2060. gadu.