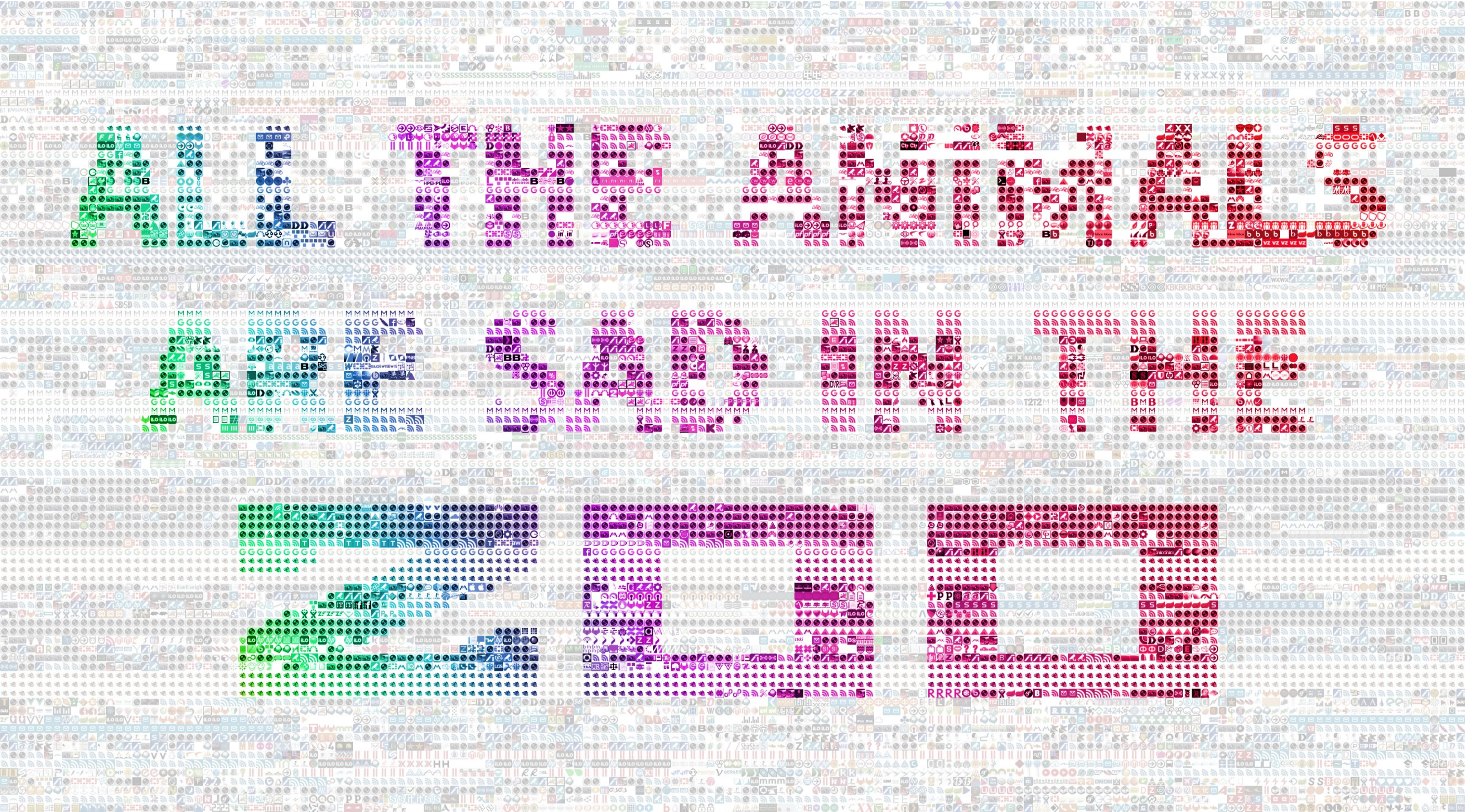


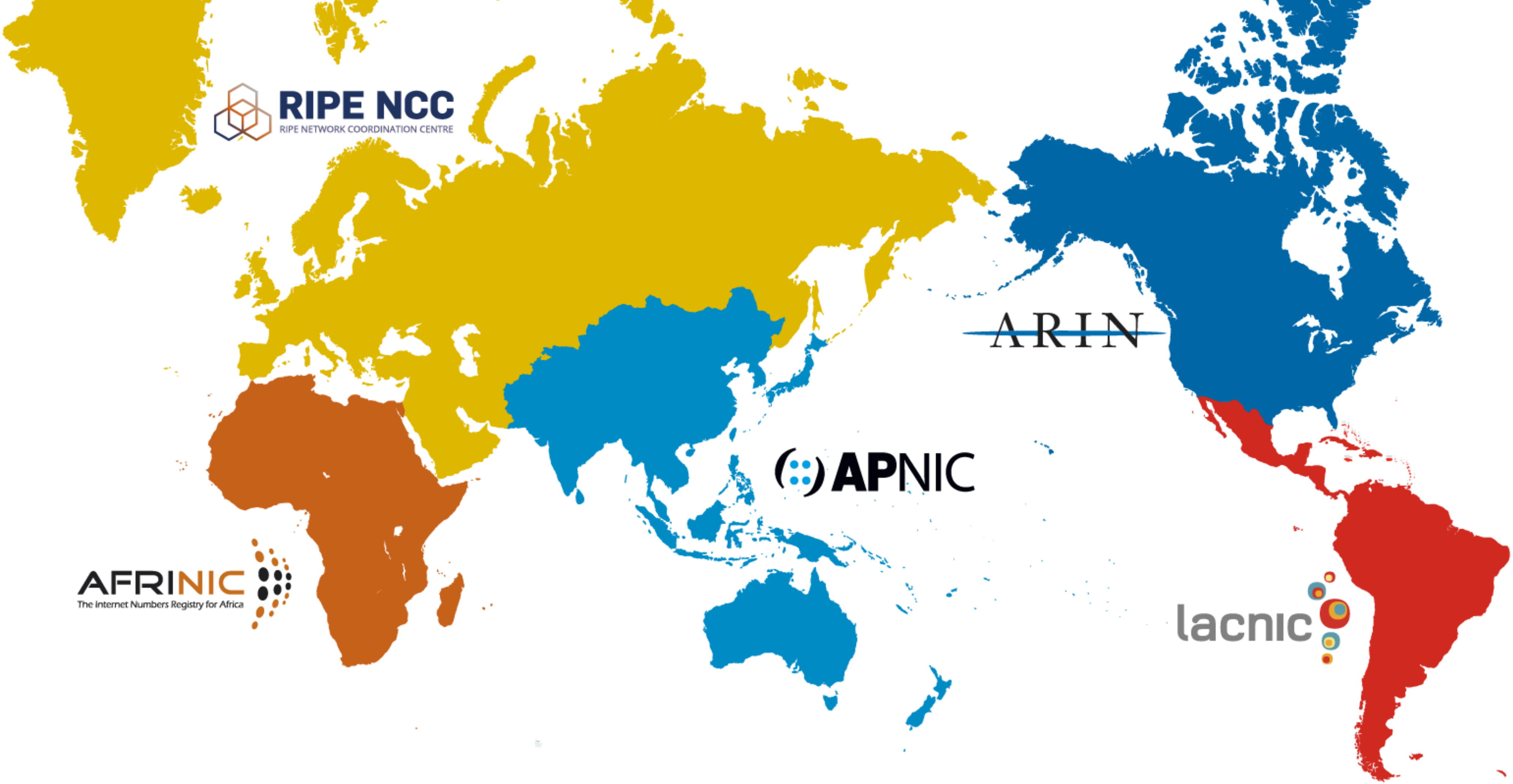
ALL THE ANIMALS ARE SAD IN THE ZOO

https://kirils.org/ https://twitter.com/KirilsSolovjovs

who am I?

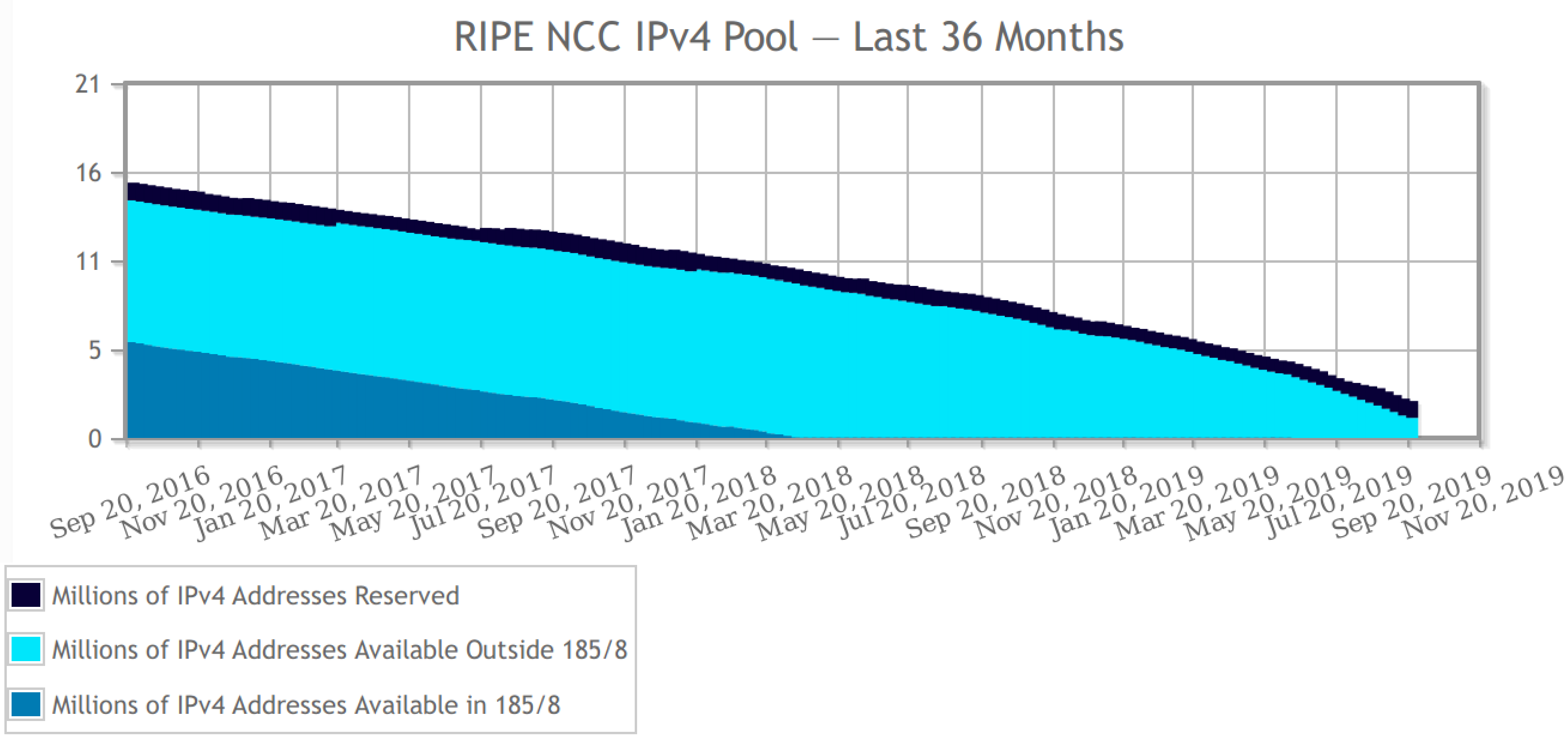
- Lead researcher at Possible Security, Latvia
- Hacking and breaking things
  - Network flow analysis
  - Reverse engineering
  - Social engineering
  - Legal dimension
- https://kirils.org/
- twitter / @KirilsSolovjovs

who manages the zoo?



RIPE NCC
RIPE NETWORK COORDINATION CENTRE
ARIN
APNIC
AFRINIC
The Internet Numbers Registry for Africa
lacnic

IPv4 exhaustion



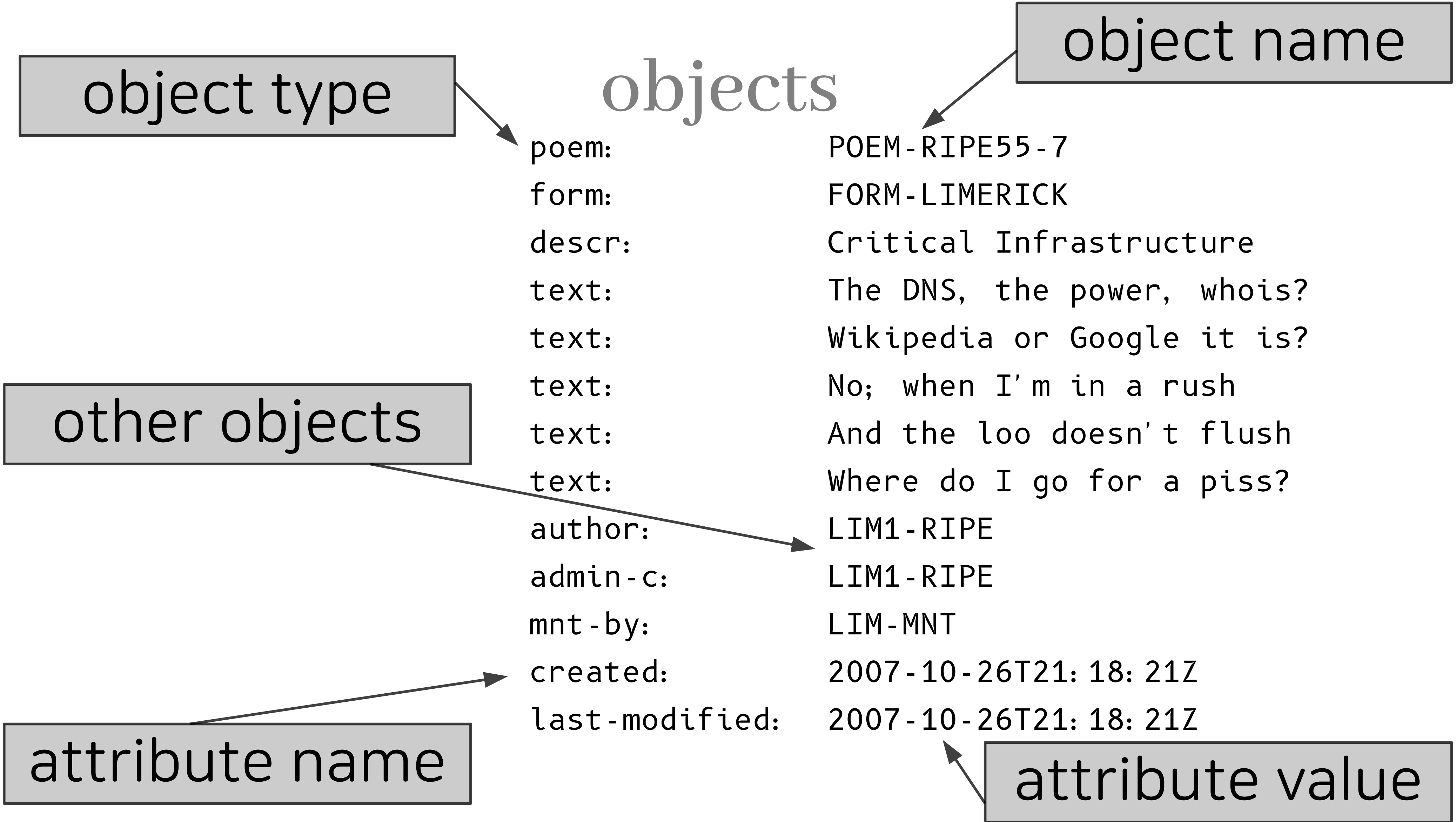
RIPE db

objects

→ attributes

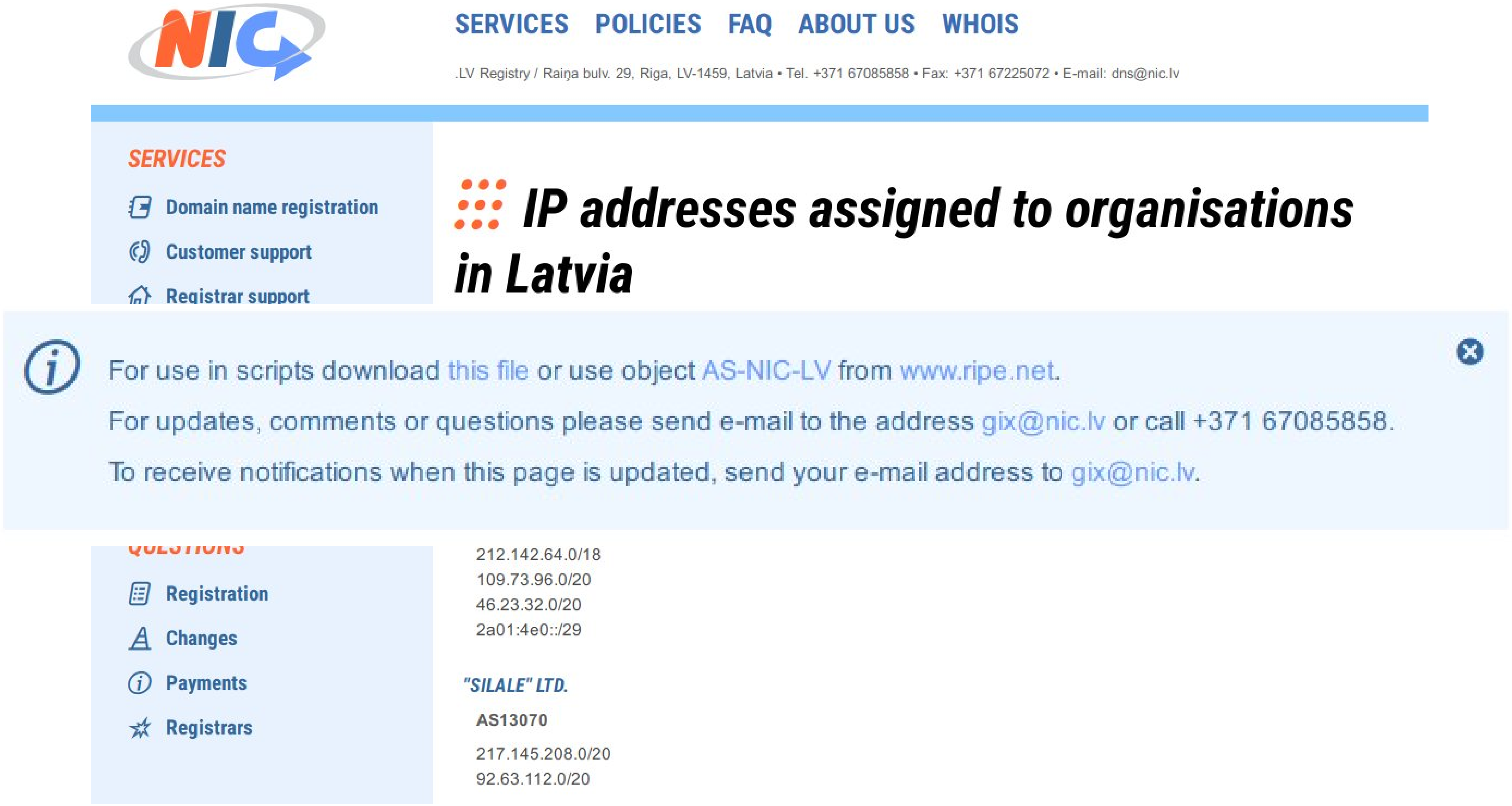
→ other objects

objects



```
poem:             POEM-RIPE55-7
form:             FORM-LIMERICK
descr:            Critical Infrastructure
text:             The DNS, the power, whois?
text:             Wikipedia or Google it is?
text:             No; when I'm in a rush
text:             And the loo doesn't flush
text:             Where do I go for a piss?
author:           LIM1-RIPE
admin-c:          LIM1-RIPE
mnt-by:           LIM-MNT
created:          2007-10-26T21:18:21Z
last-modified:    2007-10-26T21:18:21Z
```

Latvian internet?



.LV Registry / Raiņa bulv. 29, Riga, LV-1459, Latvia • Tel. +371 67085858 • Fax: +371 67225072 • E-mail: dns@nic.lv

IP addresses assigned to organisations in Latvia

For use in scripts download this file or use object AS-NIC-LV from www.ripe.net.

For updates, comments or questions please send e-mail to the address gix@nic.lv or call +371 67085858.

To receive notifications when this page is updated, send your e-mail address to gix@nic.lv.

212.142.64.0/18
109.73.96.0/20
46.23.32.0/20
2a01:4e0::/29

"SILALE" LTD.

AS13070

217.145.208.0/20
92.63.112.0/20

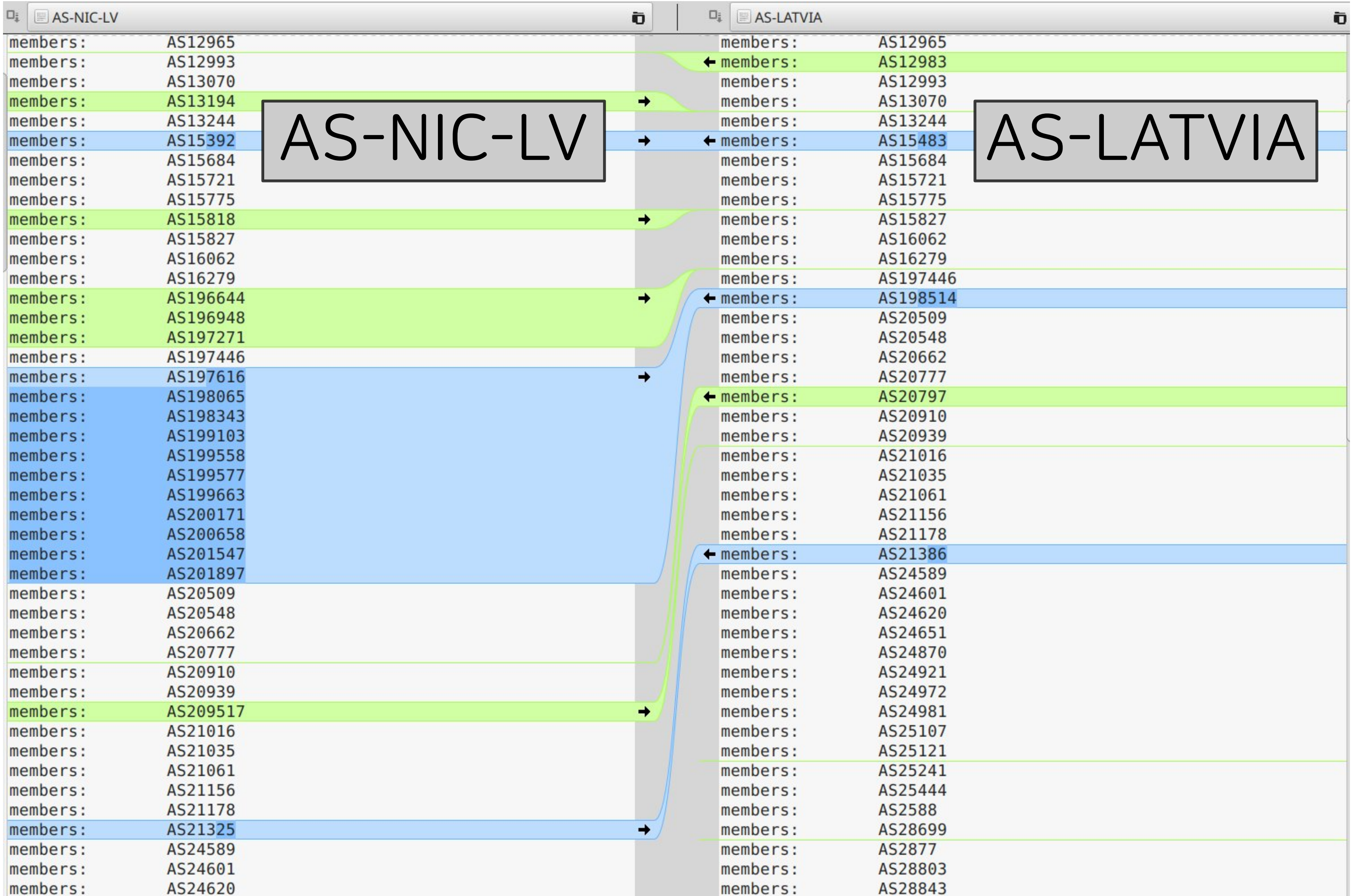
AS-NIC-LV

```
as-set:          AS-NIC-LV
descr:           AS-s of Latvia

admin-c:         NICo3-RIPE
tech-c:          NICo3-RIPE
mnt-by:          lumii-mnt

created:         2010-06-09T07:56:49Z
last-modified:   2019-09-17T10:23:08Z

role:  Network Information Centre of LV
```

AS-s of Latvia

```
as-set:          AS-NIC-LV
descr:           AS-s of Latvia

admin-c:         NICo3-RIPE
tech-c:          NICo3-RIPE
mnt-by:          lumii-mnt

created:         2010-06-09T07:56:49Z
last-modified:   2019-09-17T10:23:08Z

role:  Network Information Centre of LV
```

```
as-set:          AS-LATVIA
descr:           AS-s of Latvia

admin-c:         LN645-RIPE
tech-c:          LN645-RIPE
mnt-by:          AS2588-MNT
mnt-lower:       LTK
created:         2002-09-17T12:15:54Z
last-modified:   2019-02-27T09:38:16Z

role:            Latnet HostMaster
```



AS-NIC-LV

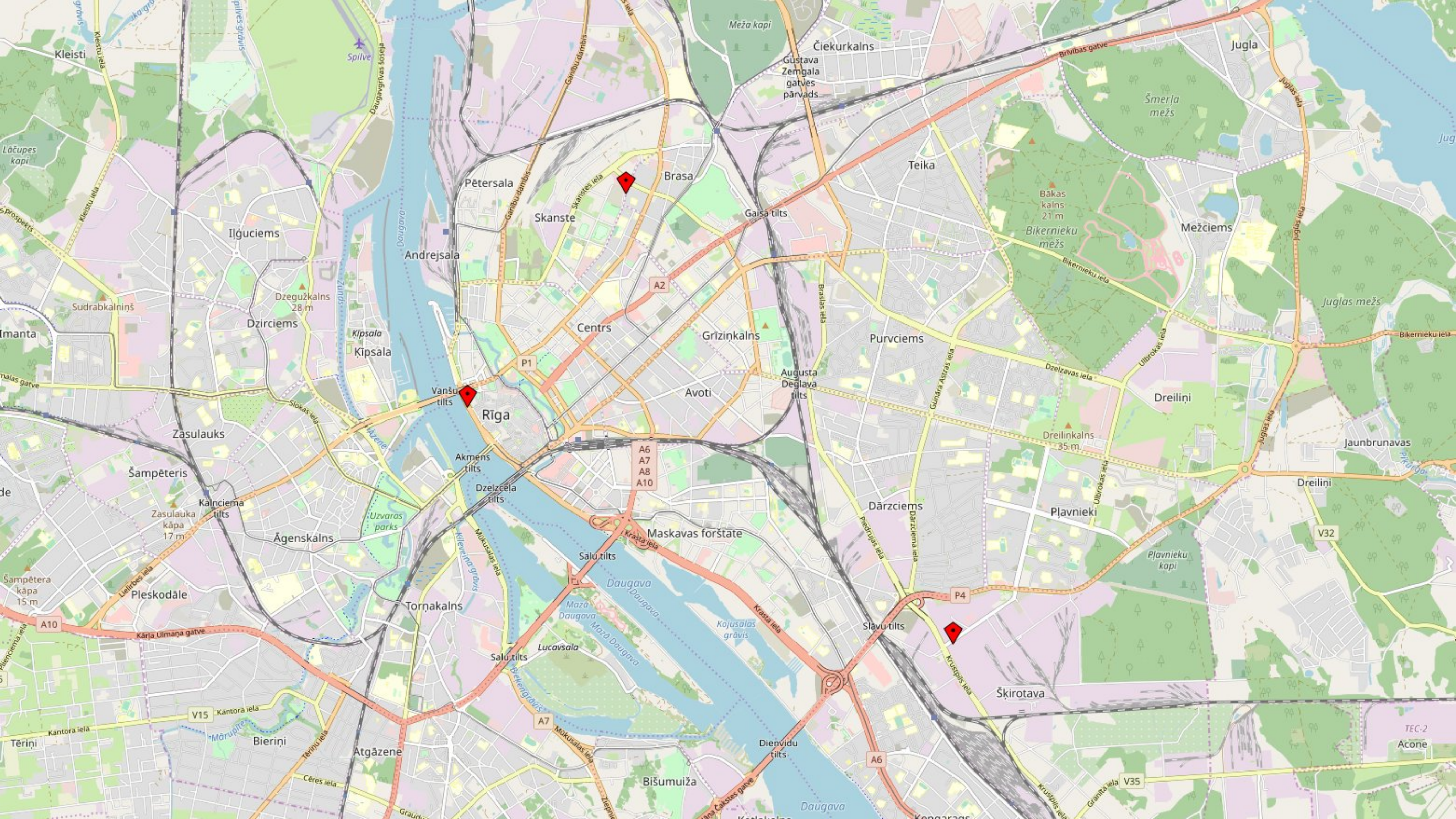
```
members:        AS12965
members:        AS12993
members:        AS13070
members:        AS13194
members:        AS13244
members:        AS15392
members:        AS15684
members:        AS15721
members:        AS15775
members:        AS15818
members:        AS15827
members:        AS16062
members:        AS16279
members:        AS196644
members:        AS196948
members:        AS197271
members:        AS197446
members:        AS197616
members:        AS198065
members:        AS198343
members:        AS199103
members:        AS199558
members:        AS199577
members:        AS199663
members:        AS200171
members:        AS200658
members:        AS201547
members:        AS201897
members:        AS20509
members:        AS20548
members:        AS20662
members:        AS20777
members:        AS20910
members:        AS20939
members:        AS209517
members:        AS21016
members:        AS21035
members:        AS21061
members:        AS21156
members:        AS21178
members:        AS21325
members:        AS24589
members:        AS24601
members:        AS24620
```

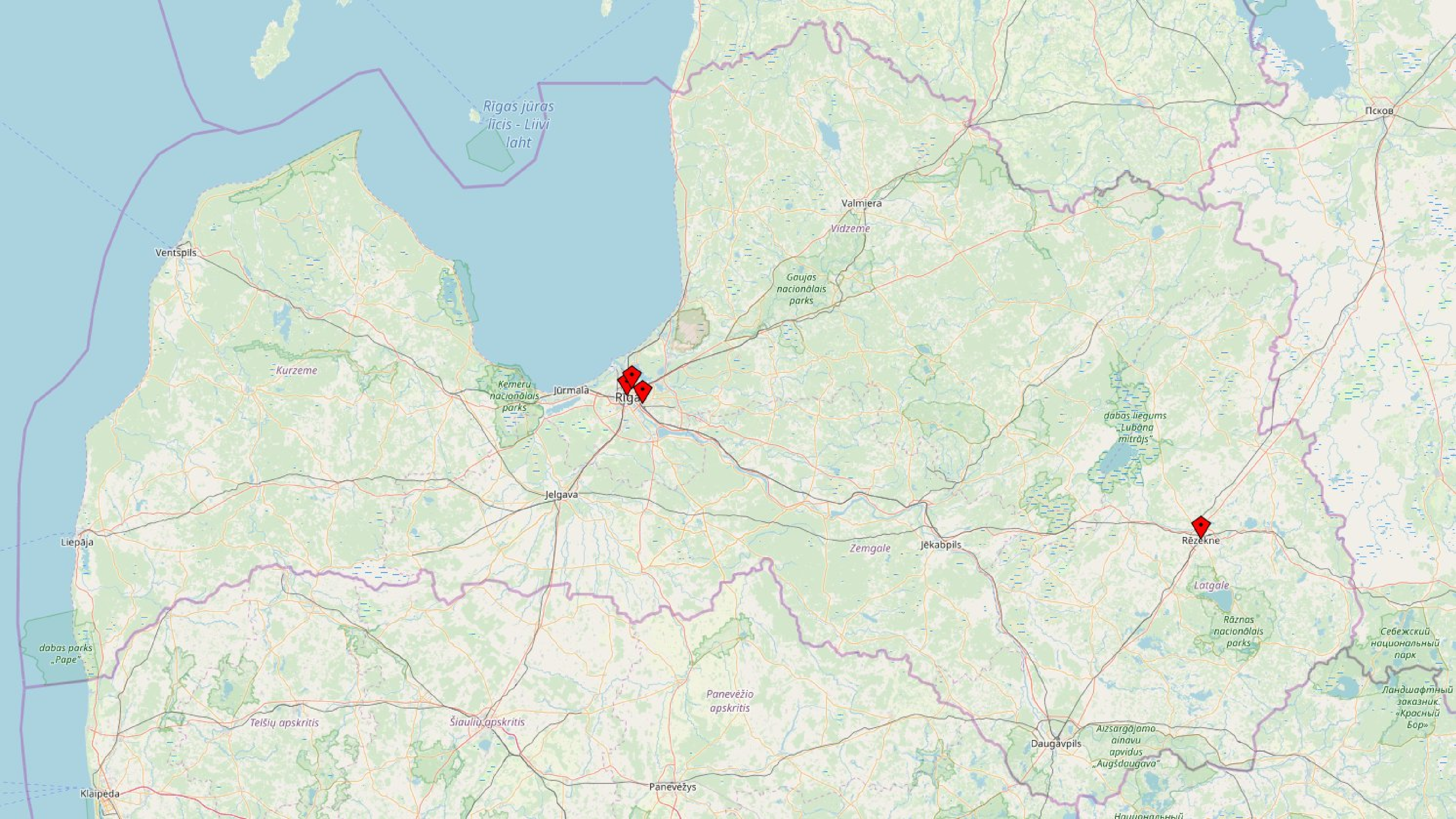
AS-LATVIA

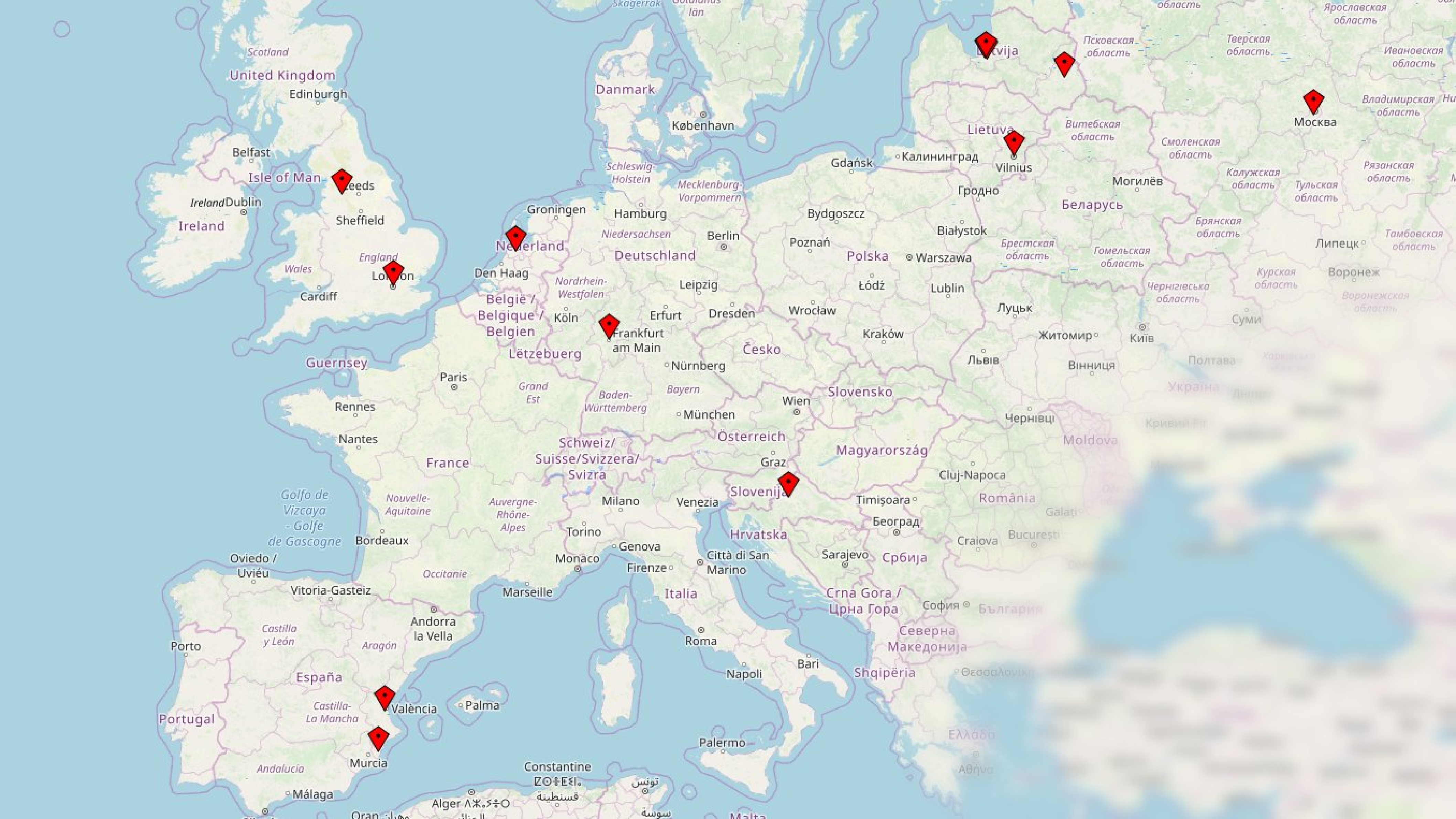
```
members:        AS12965
members:        AS12983
members:        AS12993
members:        AS13070
members:        AS13244
members:        AS15483
members:        AS15684
members:        AS15721
members:        AS15775
members:        AS15827
members:        AS16062
members:        AS16279
members:        AS197446
members:        AS198514
members:        AS20509
members:        AS20548
members:        AS20662
members:        AS20777
members:        AS20797
members:        AS20910
members:        AS20939
members:        AS21016
members:        AS21035
members:        AS21061
members:        AS21156
members:        AS21178
members:        AS21386
members:        AS24589
members:        AS24601
members:        AS24620
members:        AS24651
members:        AS24870
members:        AS24921
members:        AS24972
members:        AS24981
members:        AS25107
members:        AS25121
members:        AS25241
members:        AS25444
members:        AS2588
members:        AS28699
members:        AS2877
members:        AS28803
members:        AS28843
```

geolocation, maybe?

```
inetnum:        212.22.75.0 - 212.22.75.255
netname:        LV-location
geoloc:         56.9519 24.1221
country:        LV
admin-c:        DM16411-RIPE
tech-c:         DM16411-RIPE
status:         ASSIGNED PA
mnt-routes:     CTH-DCMSK
mnt-domains:    CTH-DCMSK
mnt-by:         QUADRONET-MNT
```

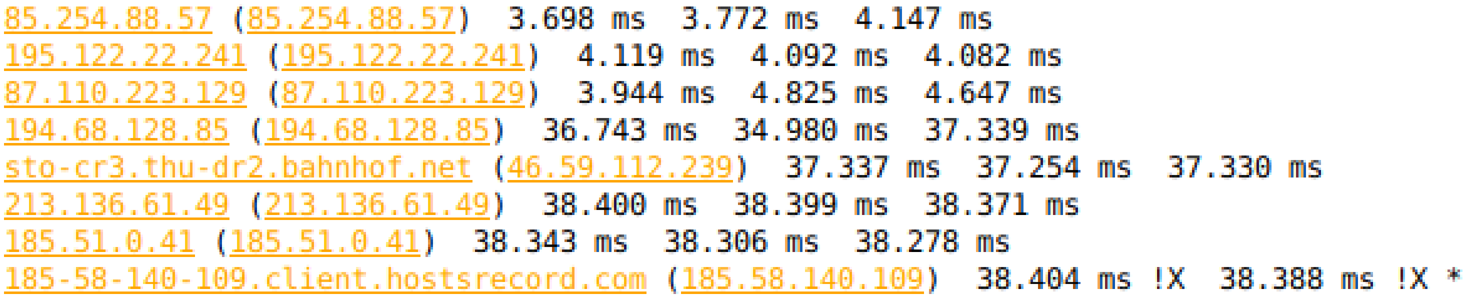

Kleisti
Spilve
Meža kapi
Čiekurkalns
Jugla
Gustava Zemgala gatves pārvads
Brīvības gatve
Šmerļa mežs
Lāčupes kapi
Pētersala
Brasa
Teika
Skanste
Gaisa tilts
Ilģuciems
Andrejsala
Bākas kalns 21 m
Biķernieku mežs
Mežciems
Biķernieku iela
A2
Dzegužkalns 28 m
Sudrabkalniņš
Dzirciems
Juglas mežs
Imanta
Ķīpsala
Centrs
Grīziņkalns
Purvciems
P1
Augusta Deglava tilts
Dzelzavas iela
Dreiliņi
Vanšu tilts
Rīga
Avoti
Zasulauks
Dreiliņkalns 35 m
Jaunbrunavas
Akmens tilts
A6
A7
A8
A10
Šampēteris
Dzelzceļa tilts
Dārzciems
Dreiliņi
Kalnciema tilts
Pļavnieki
Zasulauka kāpa 17 m
Uzvaras parks
Āgenskalns
Maskavas forštate
Krasta iela
V32
Salu tilts
Daugava
Pļavnieku kapi
Šampētera kāpa 15 m
Pleskodāle
Mazā Daugava
P4
Torņakalns
Kojusalas grāvis
Slāvu tilts
A10
Kārļa Ulmaņa gatve
Lucavsala
Salu tilts
Škirotava
Krustpils iela
V15
Kantora iela
A7
TEC-2
Tēriņi
Biķeriņi
Dienvidu tilts
Acone
Atgāzene
A6
V35
Bišumuiža
Cēres iela
Daugava
Ķengarags


Rīgas jūras līcis - Liivi laht
Псков
Valmiera
Vidzeme
Gaujas nacionālais parks
Ventspils
Kurzeme
Ķemeru nacionālais parks
Jūrmala
Rīga
dabas liegums „Lubāna mitrājs"
Jelgava
Liepāja
Jēkabpils
Zemgale
Rēzekne
Latgale
Rāznas nacionālais parks
Себежский национальный парк
dabas parks „Pape"
Ландшафтный заказник «Красный Бор»
Panevėžio apskritis
Telšių apskritis
Šiaulių apskritis
Daugavpils
Aizsargājamo ainavu apvidus „Augšdaugava"
Klaipėda
Panevėžys
Национальный


Skagerrak
Ярославская область
Scotland
United Kingdom
Edinburgh
Latvija
Псковская область
Тверская область
Ивановская область
Danmark
København
Владимирская область
Москва
Lietuva
Витебская область
Смоленская область
Belfast
Isle of Man
Leeds
Ireland
Dublin
Sheffield
Gdańsk
Калининград
Vilnius
Schleswig-Holstein
Mecklenburg-Vorpommern
Гродно
Могилёв
Калужская область
Тульская область
Рязанская область
Беларусь
Groningen
Hamburg
Bydgoszcz
Nederland
Niedersachsen
Berlin
Białystok
Брянская область
Тамбовская область
Липецк
England
Poznań
Brestская область
Гомельская область
Wales
London
Den Haag
Deutschland
Polska
Warszawa
Курская область
Воронеж
Cardiff
Nordrhein-Westfalen
Leipzig
Łódź
Lublin
Чернігівська область
Воронежская область
België / Belgique / Belgien
Köln
Erfurt
Dresden
Wrocław
Луцьк
Суми
Frankfurt am Main
Житомир
Київ
Guernsey
Lëtzebuerg
Česko
Kraków
Львів
Полтава
Paris
Nürnberg
Вінниця
Grand Est
Bayern
Україна
Rennes
Baden-Württemberg
München
Wien
Slovensko
Чернівці
Nantes
Österreich
Moldova
Schweiz/ Suisse/Svizzera/ Svizra
France
Magyarország
Graz
Cluj-Napoca
Golfo de Vizcaya - Golfe de Gascogne
Nouvelle-Aquitaine
Auvergne-Rhône-Alpes
Slovenija
Milano
Venezia
Timișoara
România
Torino
Hrvatska
Београд
Bordeaux
Genova
Craiova
București
Oviedo / Uviéu
Monaco
Città di San Marino
Sarajevo
Србија
Firenze
Occitanie
Vitoria-Gasteiz
Marseille
Italia
Crna Gora / Црна Гора
Софија
България
Andorra la Vella
Castilla y León
Porto
Aragón
Roma
Северна Македонија
España
Napoli
Bari
Shqipëria
Θεσσαλονίκη
Castilla-La Mancha
València
Palma
Portugal
Ελλάδα
Murcia
Palermo
Αθήνα
Andalucía
Constantine
ⵇⵙⵏⵟⵉⵏⵜ
قسنطينة
تونس
Málaga
Alger ⴷⵣⴰⵢⴻⵔ
Oran
Malta

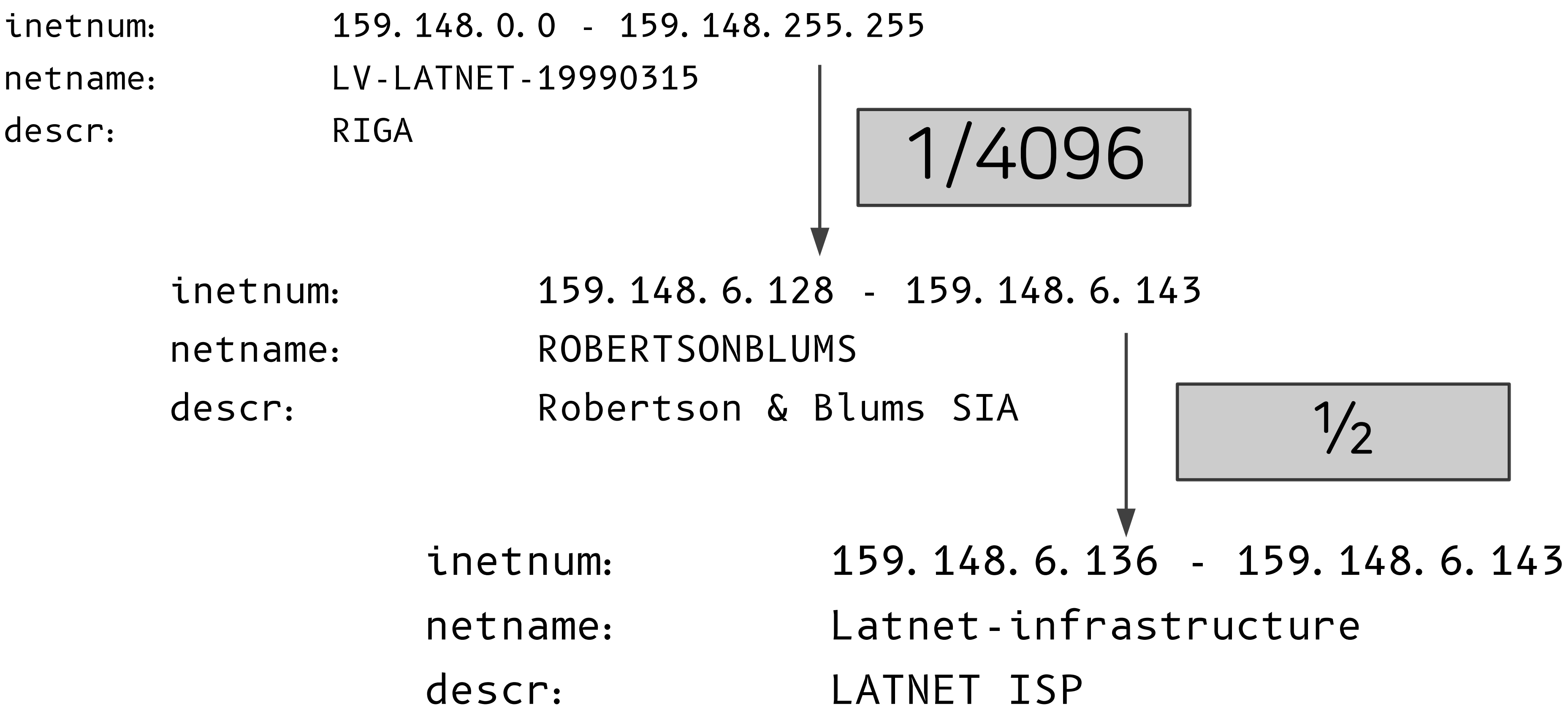
country attribute?

```
inetnum:        185.58.140.109 - 185.58.140.109
netname:        SE-MISSGROUP
descr:          MissDomain Group AB
country:        LV
admin-c:        MGN45-RIPE
tech-c:         MGN45-RIPE
status:         ASSIGNED PA
mnt-by:         MISSGROUP-NCC
created:
last-modified:
```



```
85.254.88.57 (85.254.88.57)  3.698 ms  3.772 ms  4.147 ms
195.122.22.241 (195.122.22.241)  4.119 ms  4.092 ms  4.082 ms
87.110.223.129 (87.110.223.129)  3.944 ms  4.825 ms  4.647 ms
194.68.128.85 (194.68.128.85)  36.743 ms  34.980 ms  37.339 ms
sto-cr3.thu-dr2.bahnhof.net (46.59.112.239)  37.337 ms  37.254 ms  37.330 ms
213.136.61.49 (213.136.61.49)  38.400 ms  38.399 ms  38.371 ms
185.51.0.41 (185.51.0.41)  38.343 ms  38.306 ms  38.278 ms
185-58-140-109.client.hostsrecord.com (185.58.140.109)  38.404 ms !X  38.388 ms !X *
```

RIPE db is a mess...



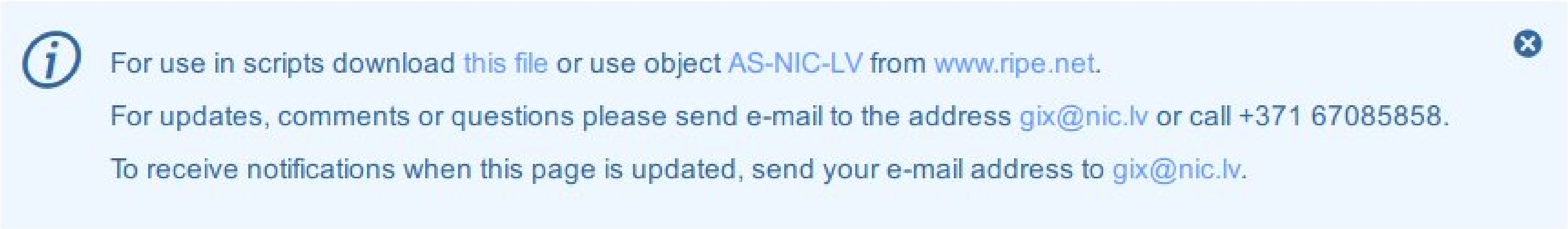
```
inetnum:        159.148.0.0 - 159.148.255.255
netname:        LV-LATNET-19990315
descr:          RIGA
```

1/4096

```
inetnum:        159.148.6.128 - 159.148.6.143
netname:        ROBERTSONBLUMS
descr:          Robertson & Blums SIA
```

½

```
inetnum:        159.148.6.136 - 159.148.6.143
netname:        Latnet-infrastructure
descr:          LATNET ISP
```



For use in scripts download this file or use object AS-NIC-LV from www.ripe.net.

For updates, comments or questions please send e-mail to the address gix@nic.lv or call +371 67085858.

To receive notifications when this page is updated, send your e-mail address to gix@nic.lv.

nic.lv/local.net

```
#####DESCR. PART######
##Latvijas Nacionala Biblioteka:www.lnb.lv:AS201547
#5.45.44.0/22
##SIA Latnet Serviss:www.ls.lv:AS2588
#159.148.0.0/16
#85.254.0.0/17
#85.254.128.0/18
#79.135.128.0/19
#176.67.32.0/20
#185.62.196.0/22
##IZZI:www.izzi.lv:AS6851
#194.8.42.0/24
#84.38.128.0/20
##Hansabanka:www.hansabank.lv:AS9091
#194.8.10.0/23
```

```
######ACCT. PART######
159.148.0.0/16
193.41.195.0/24
193.41.33.0/24
193.41.45.0/24
193.68.64.0/19
193.108.29.0/24
193.108.144.0/22
193.108.185.0/24
193.109.211.0/24
193.110.8.0/23
193.110.164.0/23
193.111.244.0/22
195.69.88.0/22
193.178.150.0/23
```

nic.lv/local.net

```
##Hansabanka: www.hansabank.lv: AS9091
#194.8.10.0/23

                                         91.220.0.0/24
                                         91.221.98.0/23


##Eunet (Versija): www.eunet.lv: AS8285
#194.8.5.0/24
                                         194.8.4.0/22
#194.8.6.0/23
```

not in local.net

```
inetnum:  185.61.150.0 -
185.61.150.255
netname:        Makonix
descr:          Makonix SIA
country:        LV
admin-c:        MTC62-RIPE
tech-c:         MTC62-RIPE
status:         ASSIGNED PA
mnt-by:         Makonix
created:        2015-09-14T14:35:02Z
last-modified:  2015-09-14T14:35:02Z
```

```
route:          185.61.150.0/24
descr:          Makonix
origin:         AS52173
mnt-by:         Makonix
created:        2015-02-12T16:11:46Z
last-modified:  2015-02-12T16:11:46Z
source:         RIPE

$ whois AS-NIC-LV|grep AS52173
members:        AS52173
members:        AS52173
```

what is in local.net ??

194.8.12.0/23 is in local.net !

```
inetnum:        0.0.0.0 - 255.255.255.255
netname:        IANA-BLK
descr:          The whole IPv4 address space
country:        EU # Country field is actually all countries in the world and not just EU countries
org:            ORG-IANA1-RIPE
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
status:         ALLOCATED UNSPECIFIED
remarks:        This object represents all IPv4 addresses.
remarks:        If you see this object as a result of a single IP query, it
remarks:        means that the IP address you are querying is currently not
remarks:        assigned to any organisation.
mnt-by:         RIPE-NCC-HM-MNT
mnt-lower:      RIPE-NCC-HM-MNT
```

how large is the zoo?

- RIPE
  - country:lv 2002727
    - 133875 of them not in nic.lv
  - country:lv+ 23040
  - total 2025411

- nic.lv/local.net
  - DESCR. 2211904
  - ACCT. 2212416
    - 260649 of them don’t have country:lv
  - total 2212928

ok, so what to use?

- for historic reasons: local.net ACCT. part
- BGP to be further researched as an option

methodology

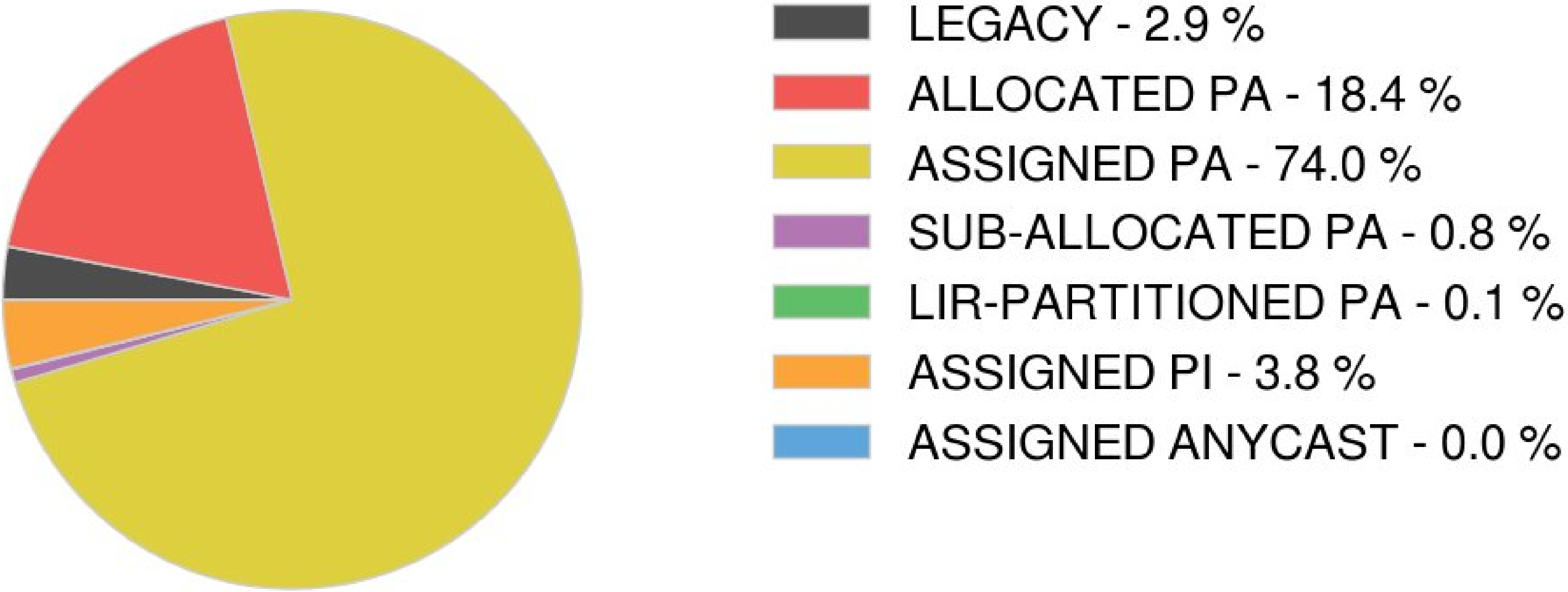
1) choose what to scan
2) choose ports and protocols
3) choose date and time
4) grab banners and web
5) analyse everything*

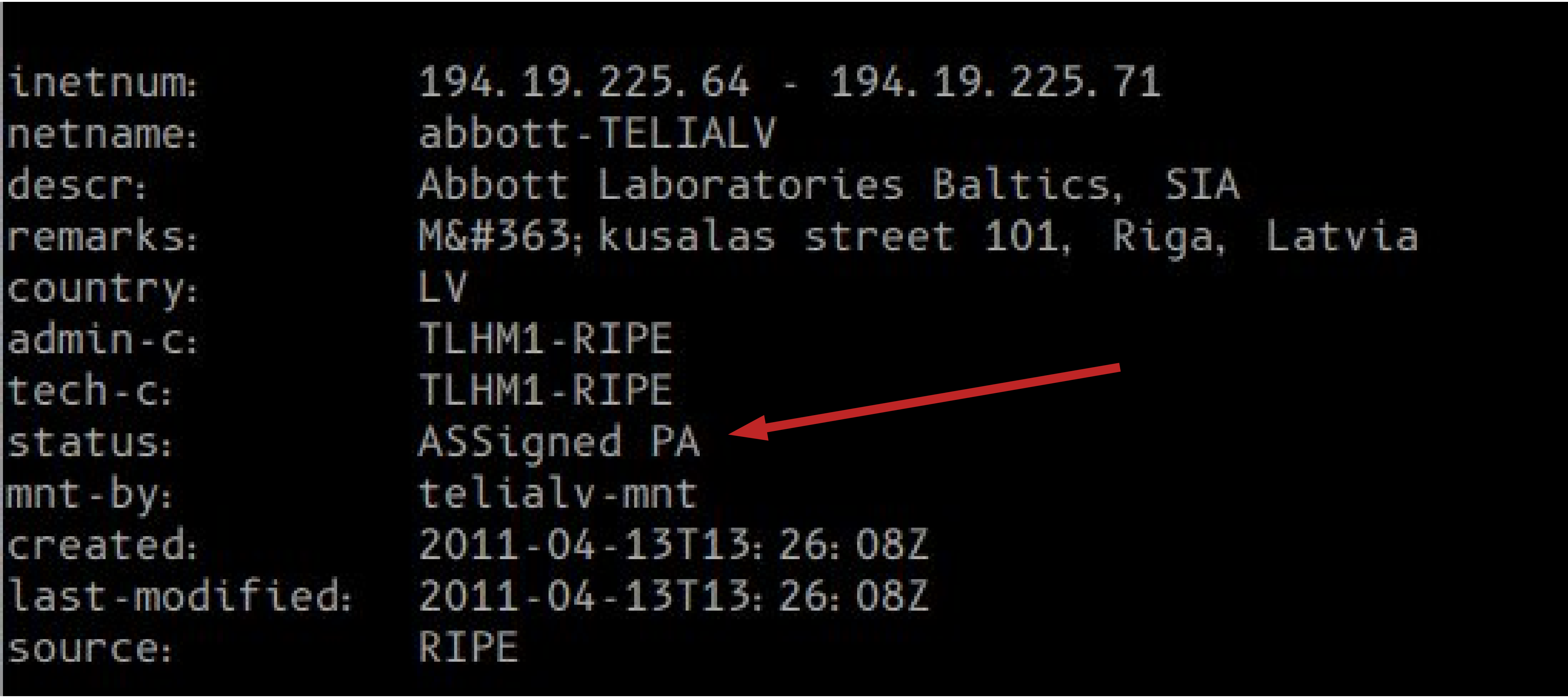
tools

- whois
- masscan
- zmap
- nmap
- parallel
- progress ♥
- bash
- GNU coreutils
- chart ♥

http://eja.lv/3c0

allocation type (status attribute)





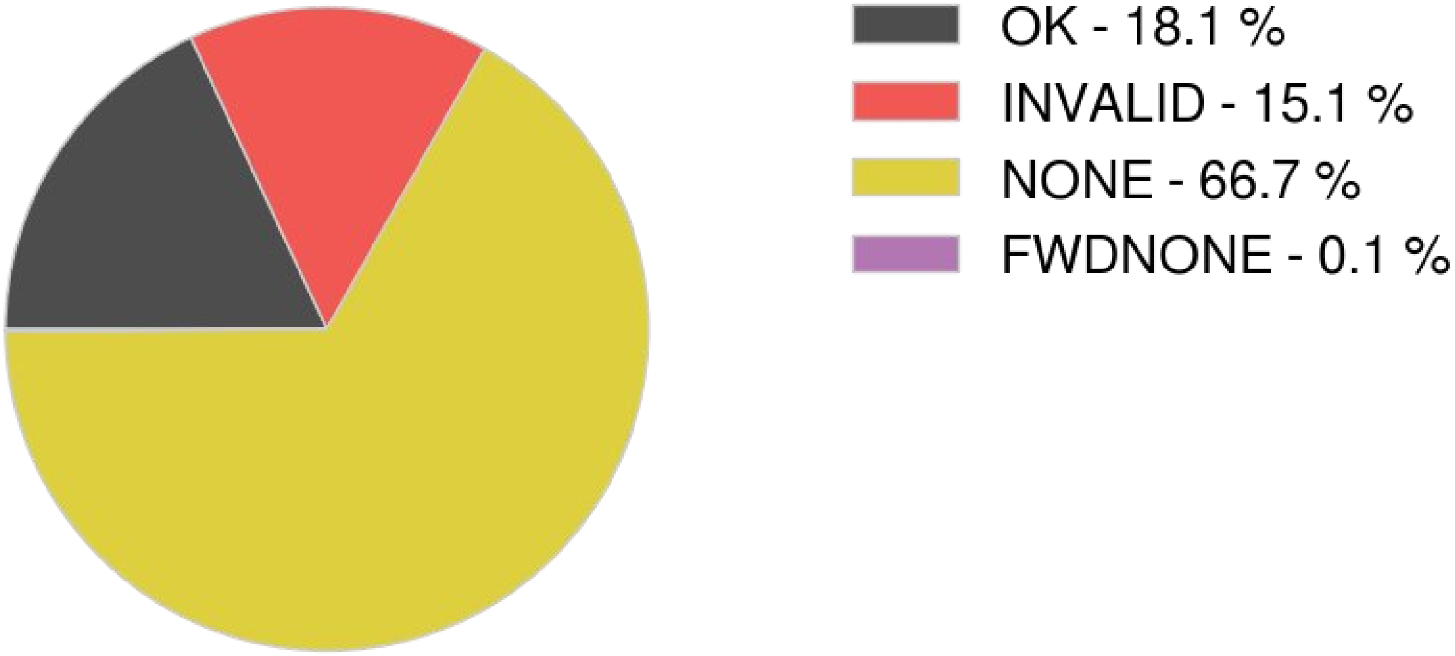
```
inetnum:        194.19.225.64 - 194.19.225.71
netname:        abbott-TELIALV
descr:          Abbott Laboratories Baltics, SIA
remarks:        M&#363;kusalas street 101, Riga, Latvia
country:        LV
admin-c:        TLHM1-RIPE
tech-c:         TLHM1-RIPE
status:         ASSigned PA
mnt-by:         telialv-mnt
created:        2011-04-13T13:26:08Z
last-modified:  2011-04-13T13:26:08Z
source:         RIPE
```

dns PTR

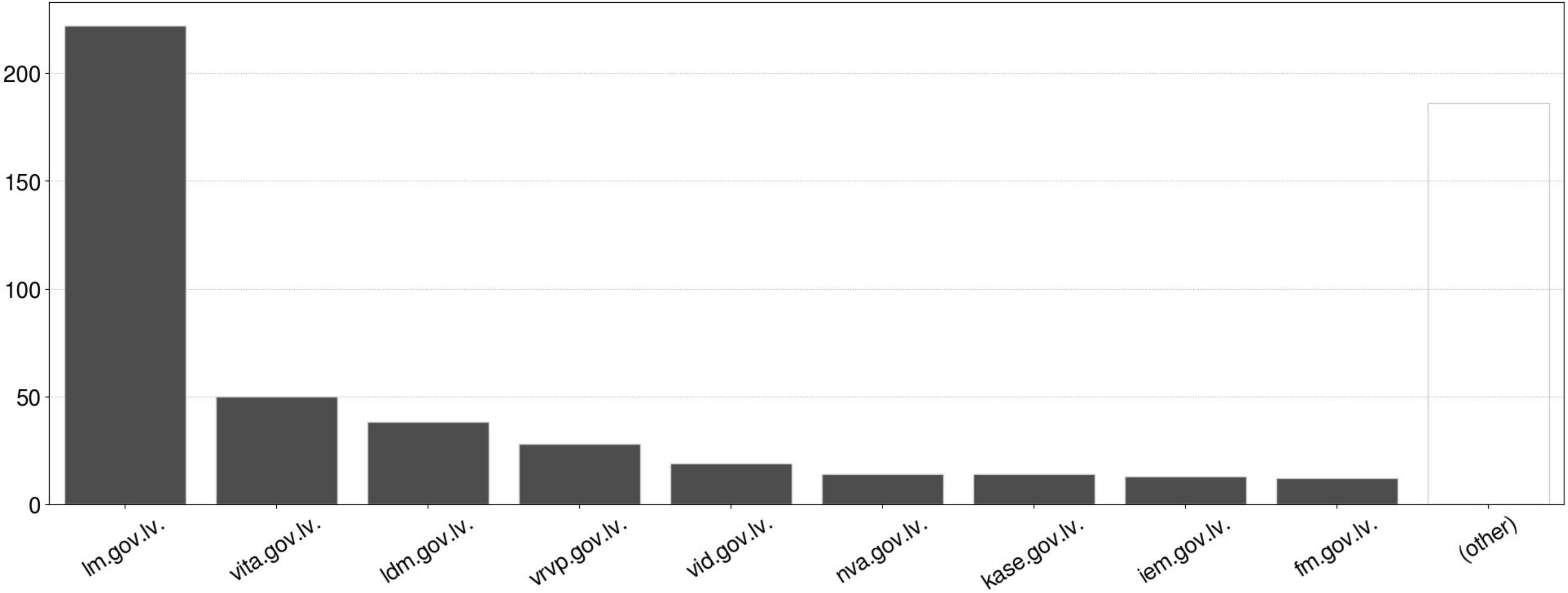
```
$ host 194.19.240.152
152.240.19.194.in-addr.arpa domain
name pointer
beidziet.piesavinaaties.adresi.
telia.lv.240.19.194.in-addr.arpa.
```

→ “stop appropriating the address”

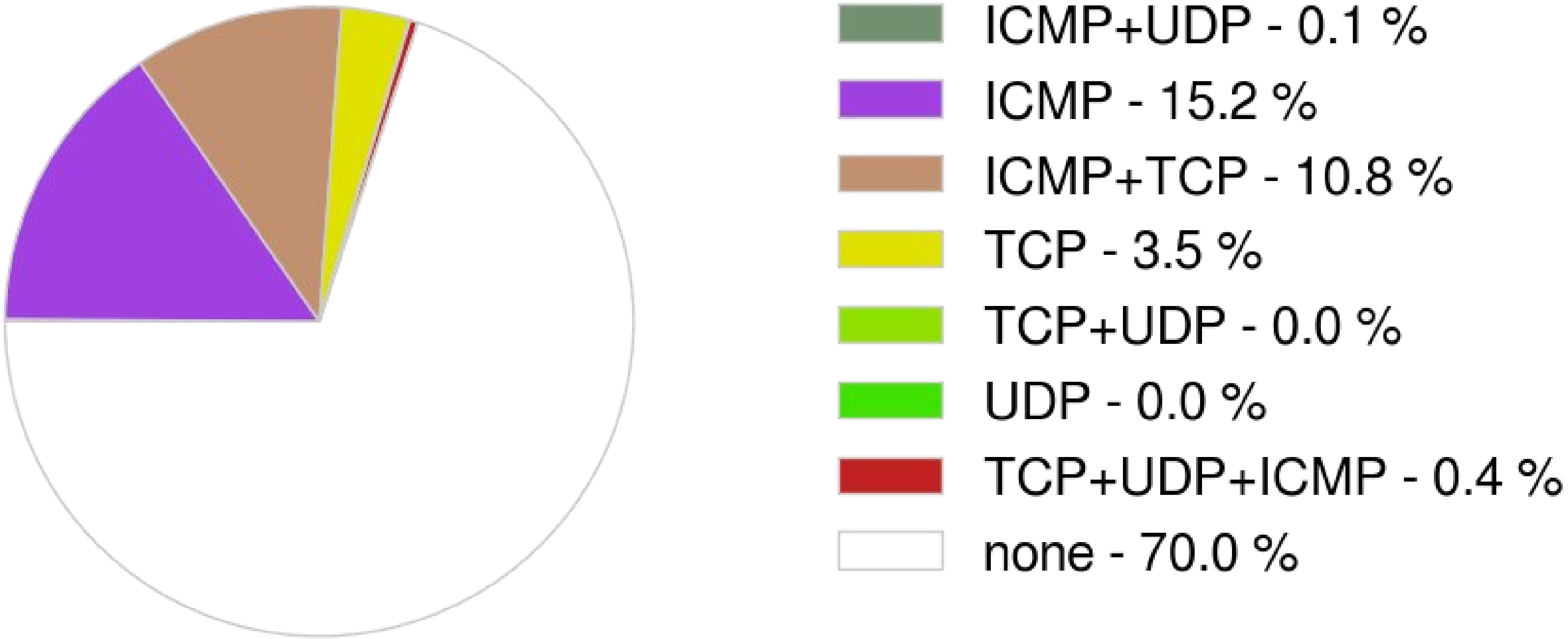
dns PTR



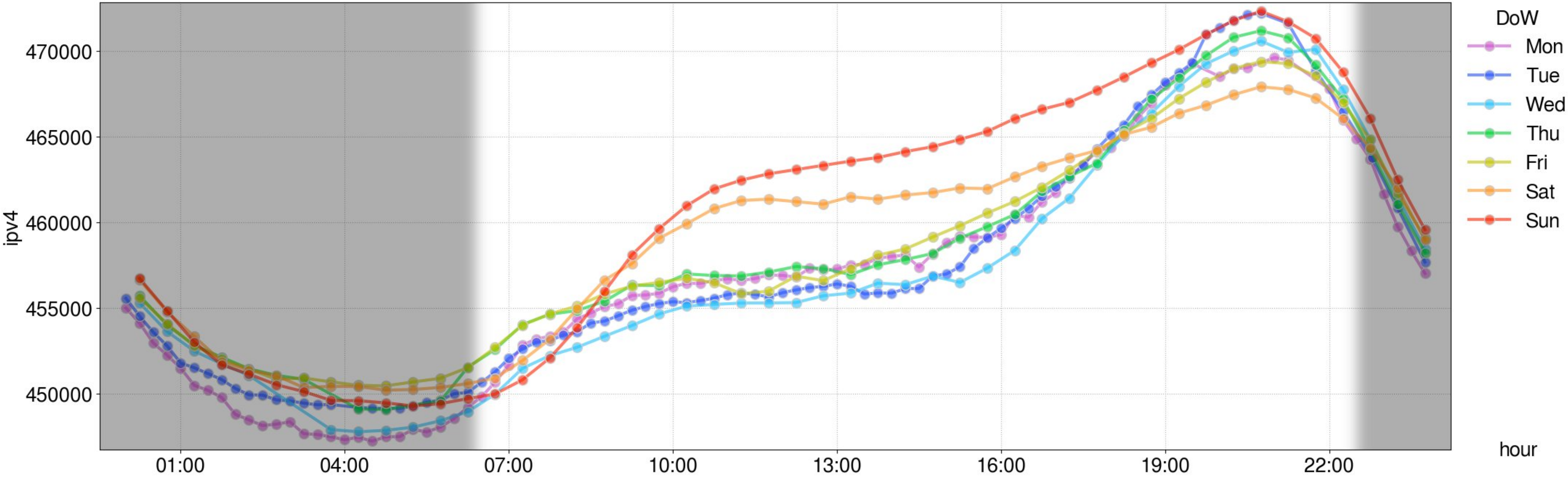
invalid PTR records (2^{nd} lvl @gov.lv)



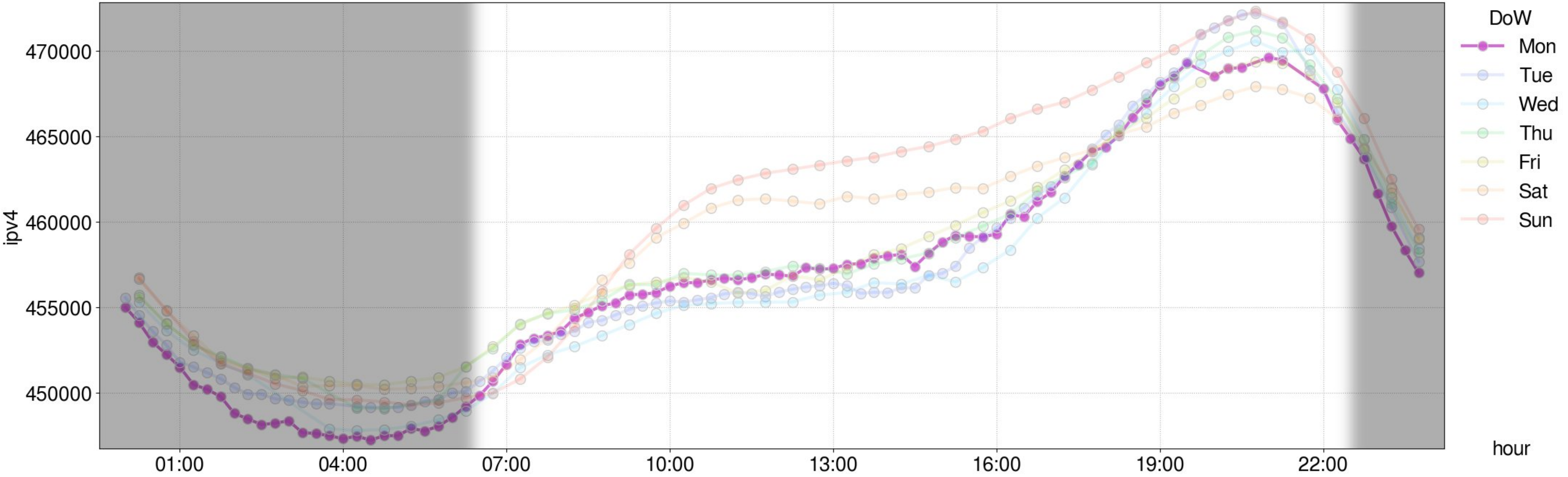
overall host response



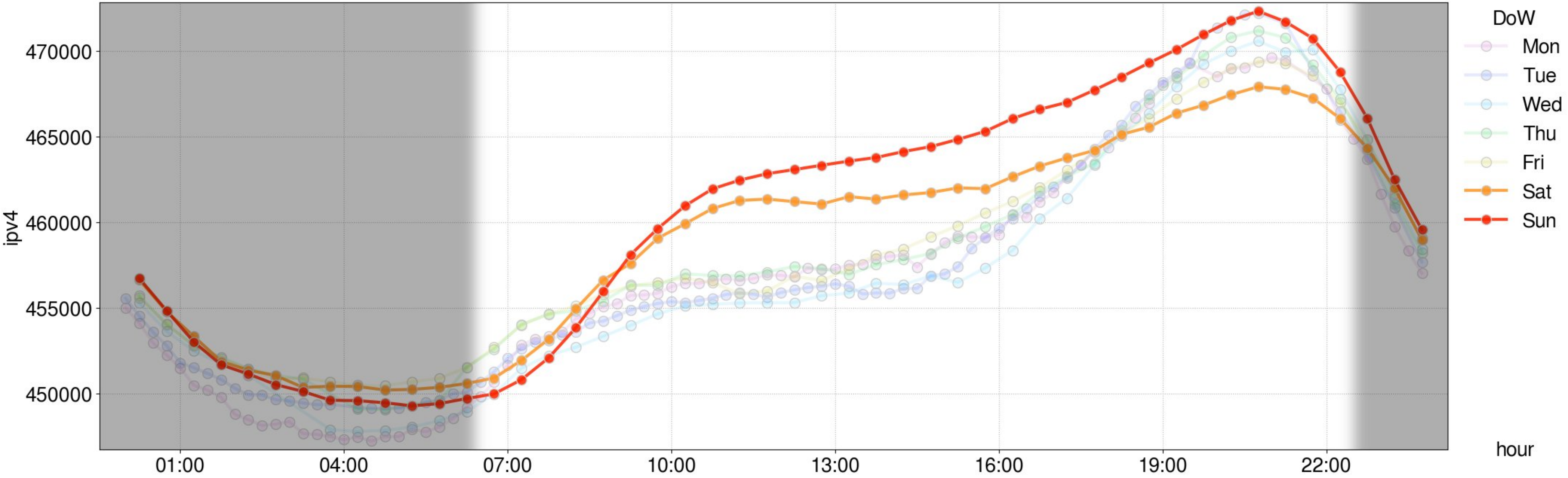
icmp probe responses



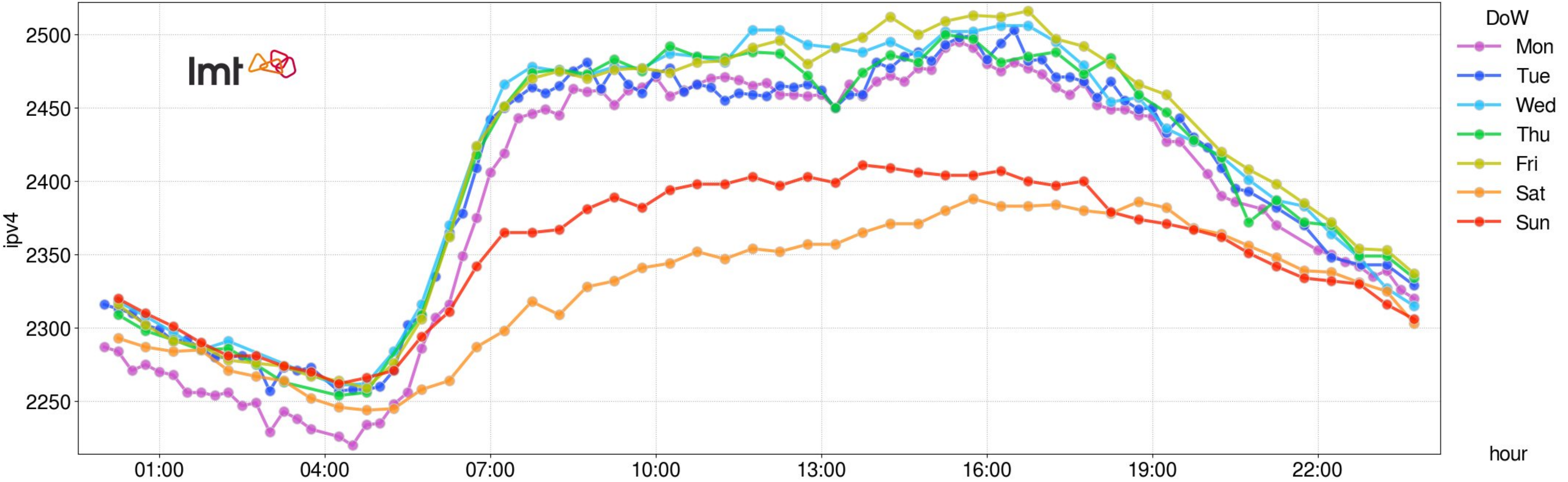
icmp probe responses



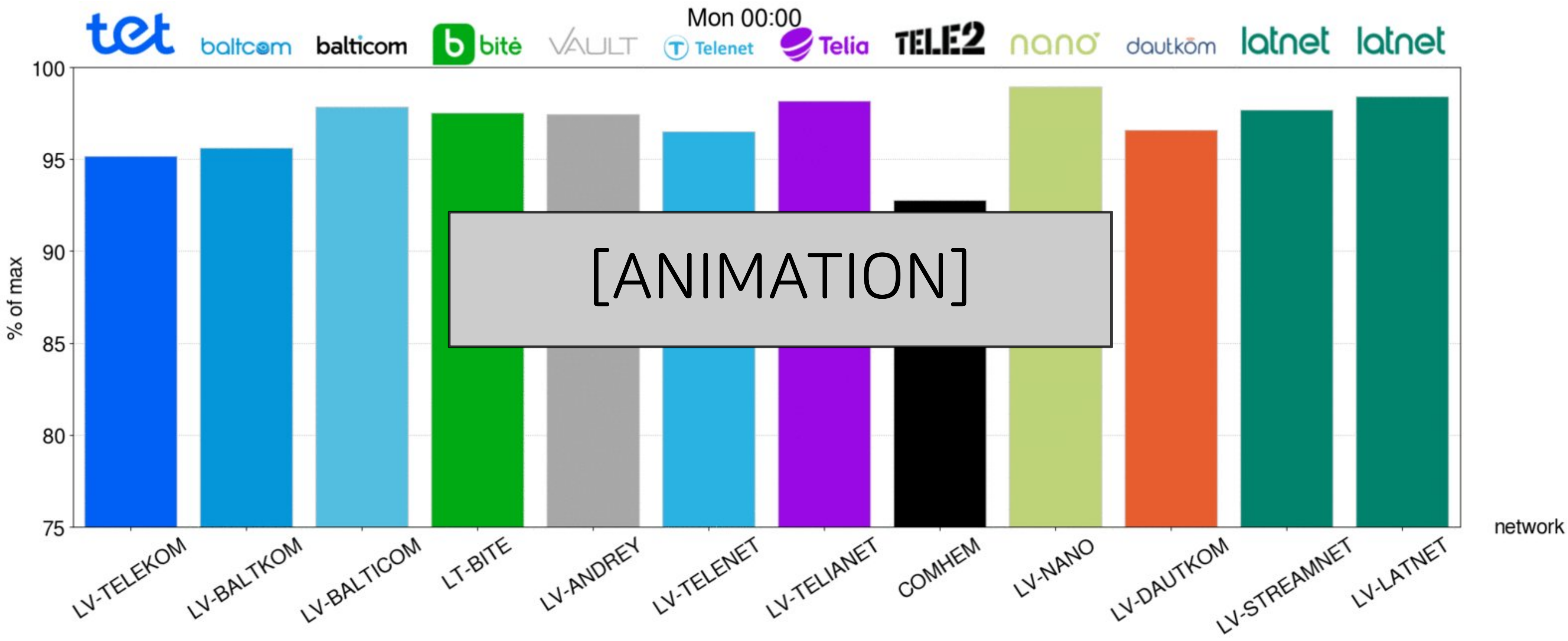
icmp probe responses



mobile users (icmp)

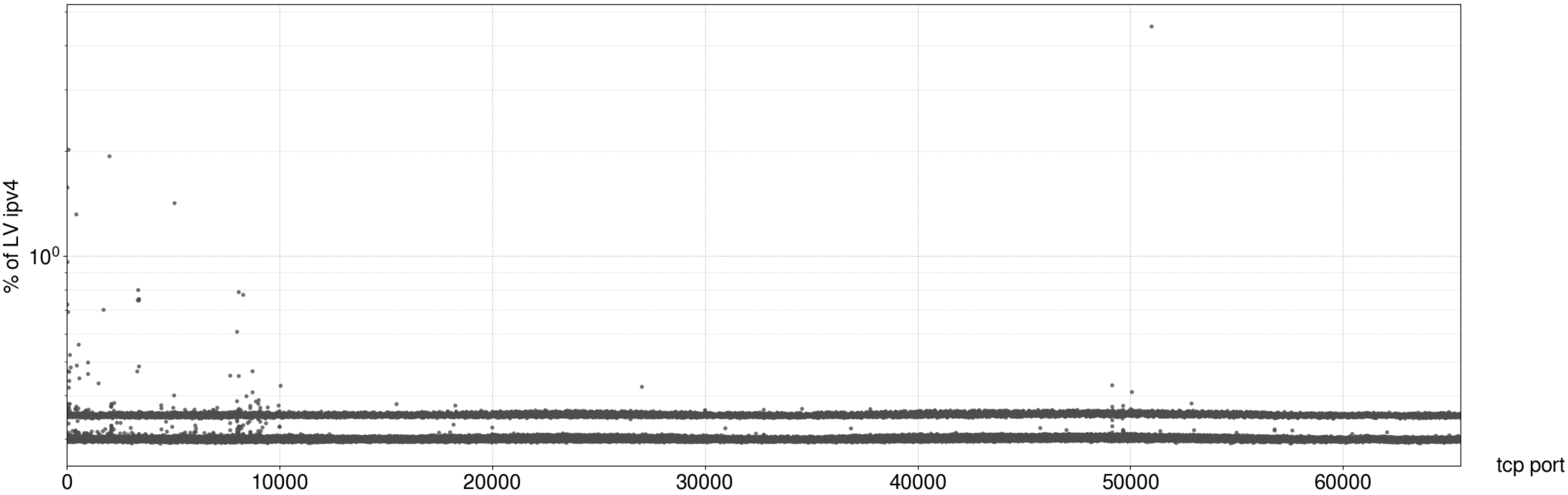


icmp reachability dynamic per isp

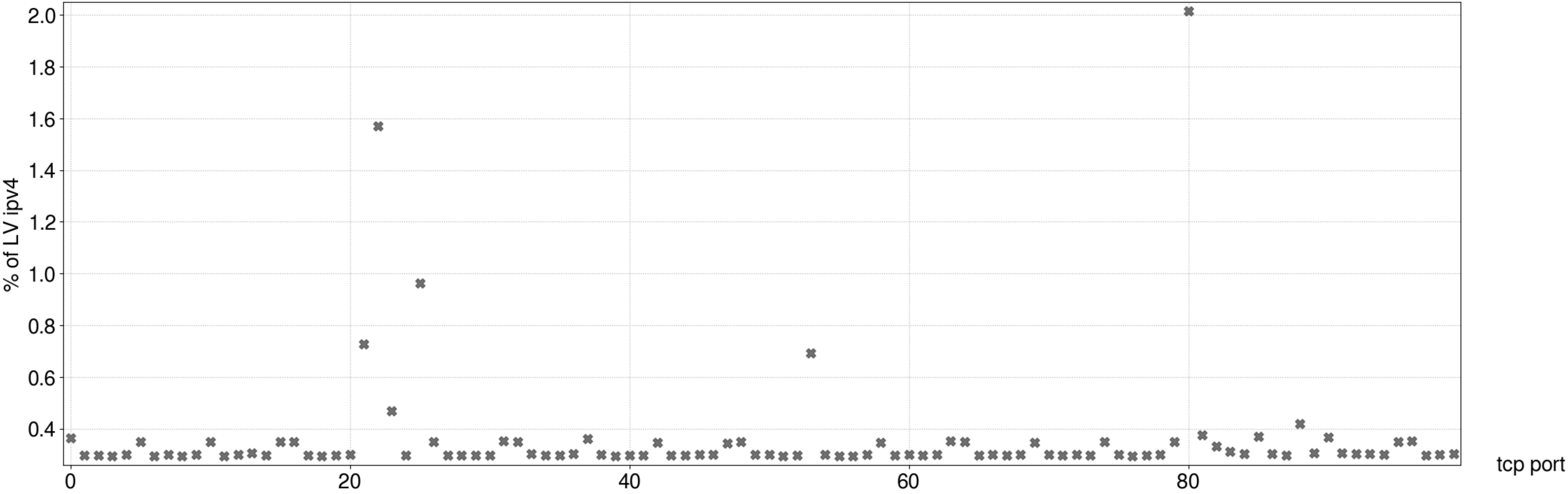


[ANIMATION]

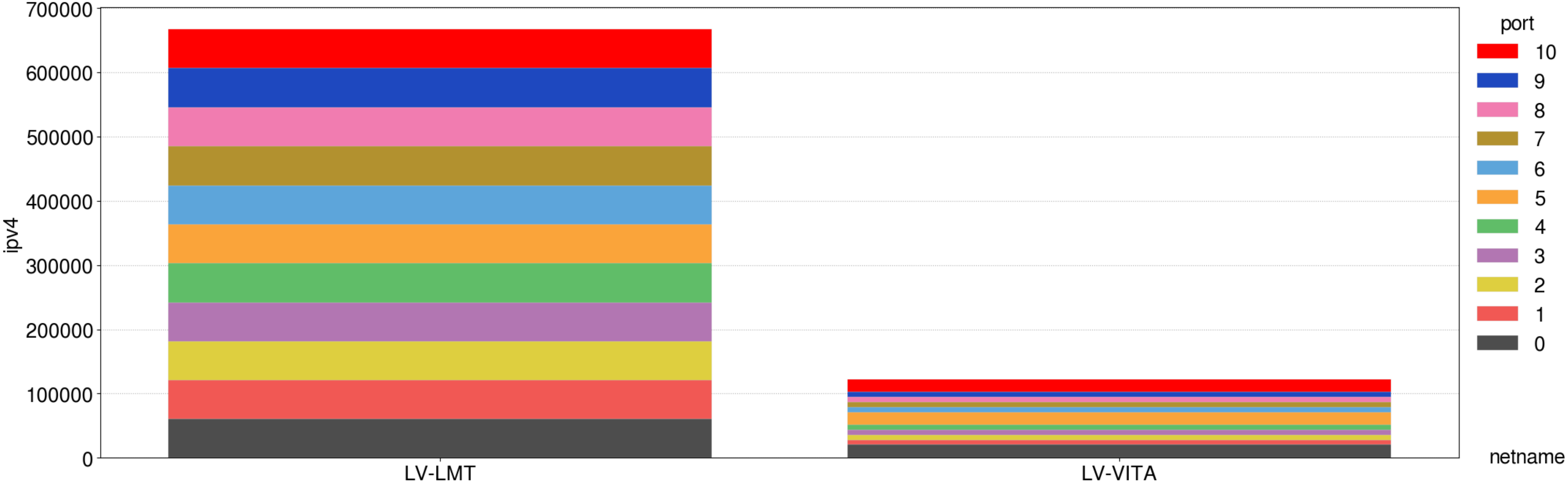
tcp port responses: all



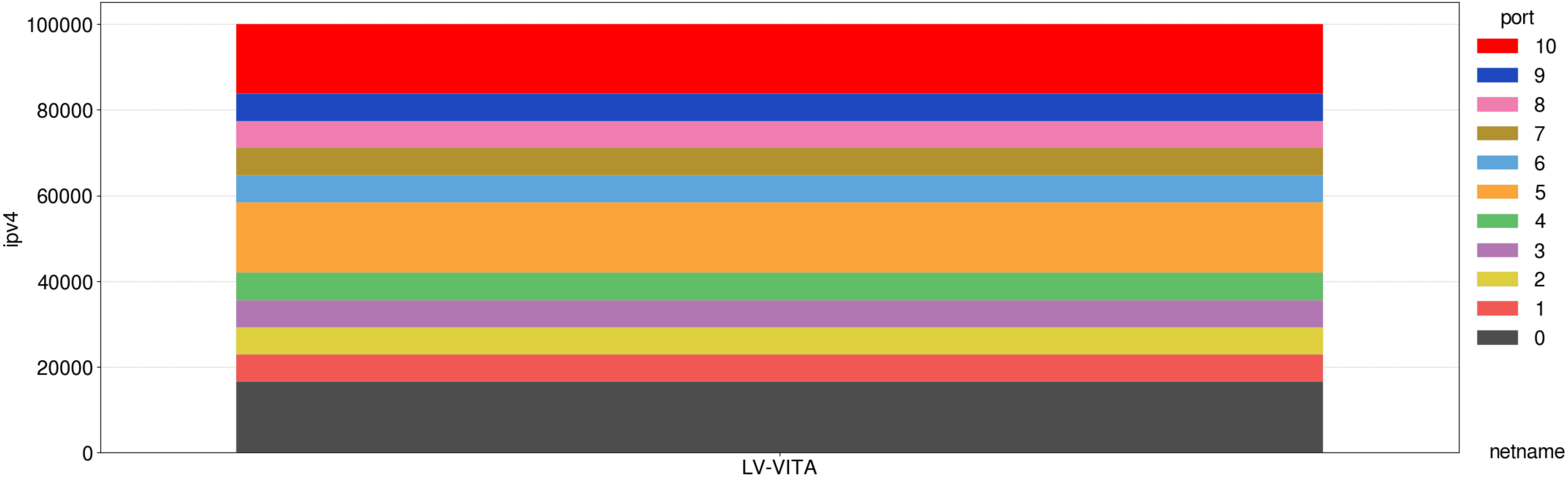
tcp port responses: low ports



oh!

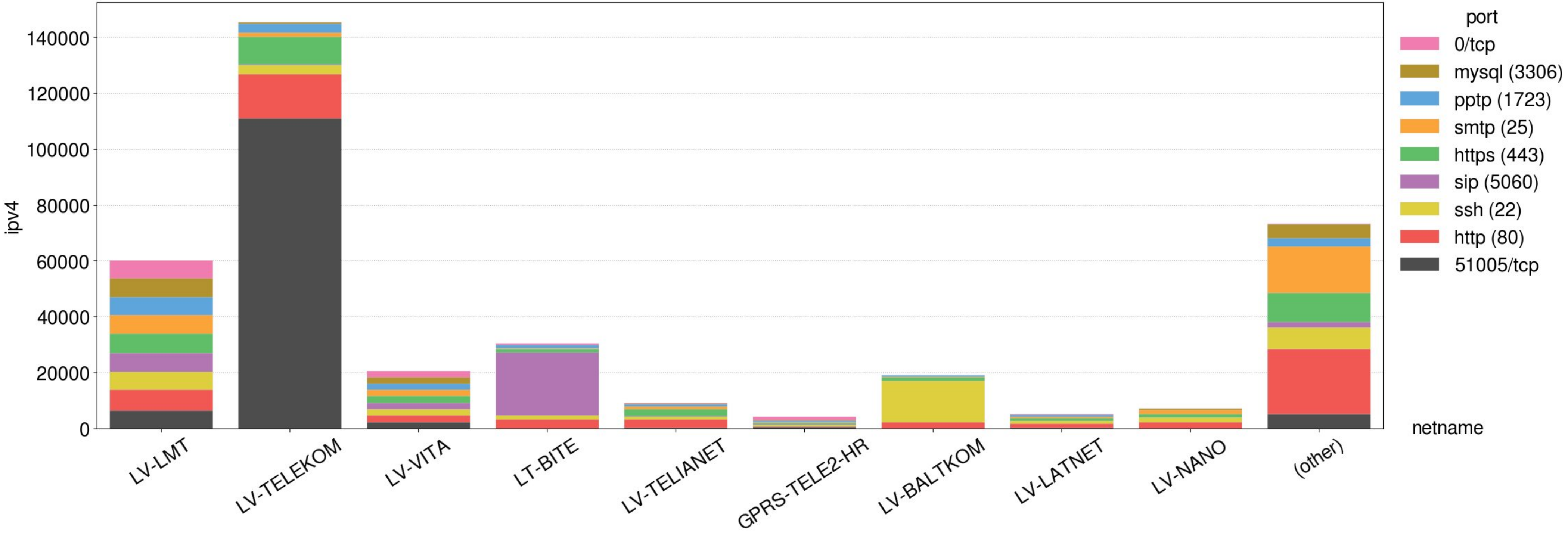

port
10
9
8
7
6
5
4
3
2
1
0
ipv4
700000
600000
500000
400000
300000
200000
100000
0
LV-LMT
LV-VITA
netname

oooooooh...

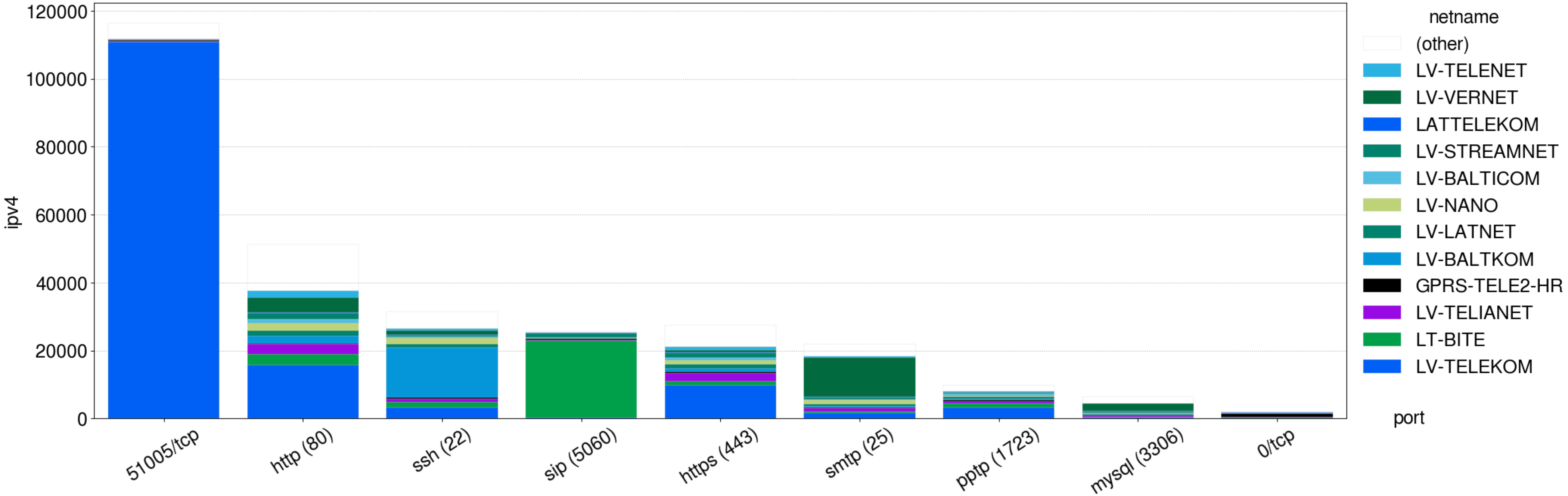


100000
80000
60000
40000
20000
0
ipv4
LV-VITA
port
10
9
8
7
6
5
4
3
2
1
0
netname

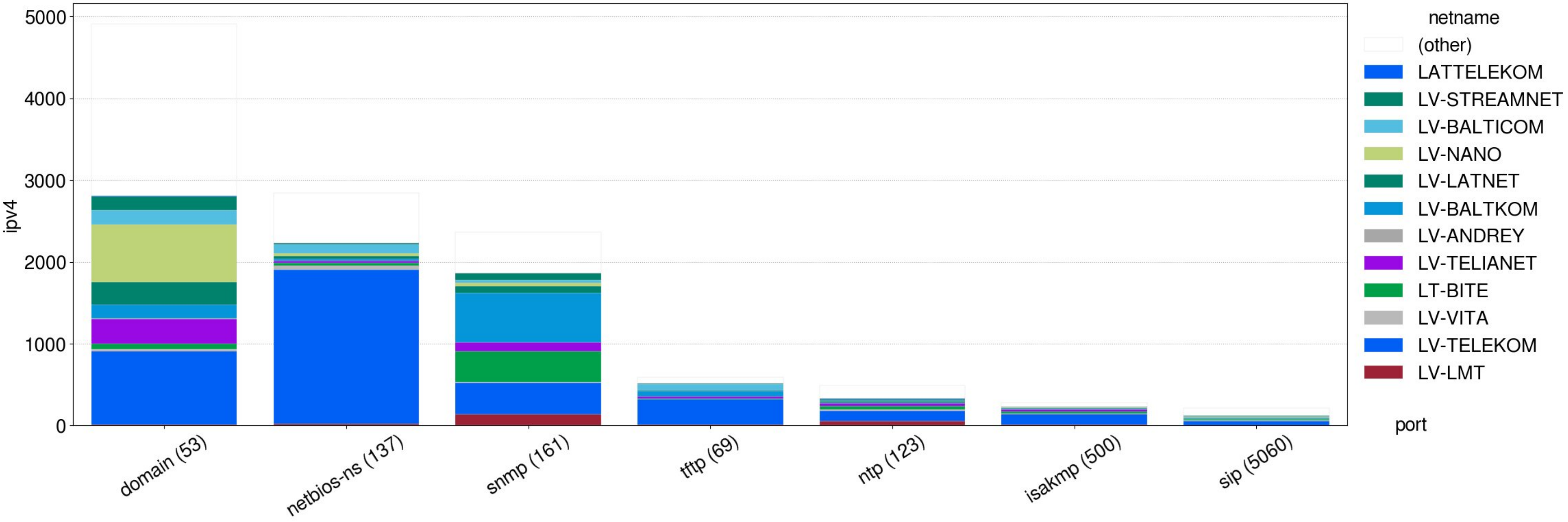
select tcp ports in top isps



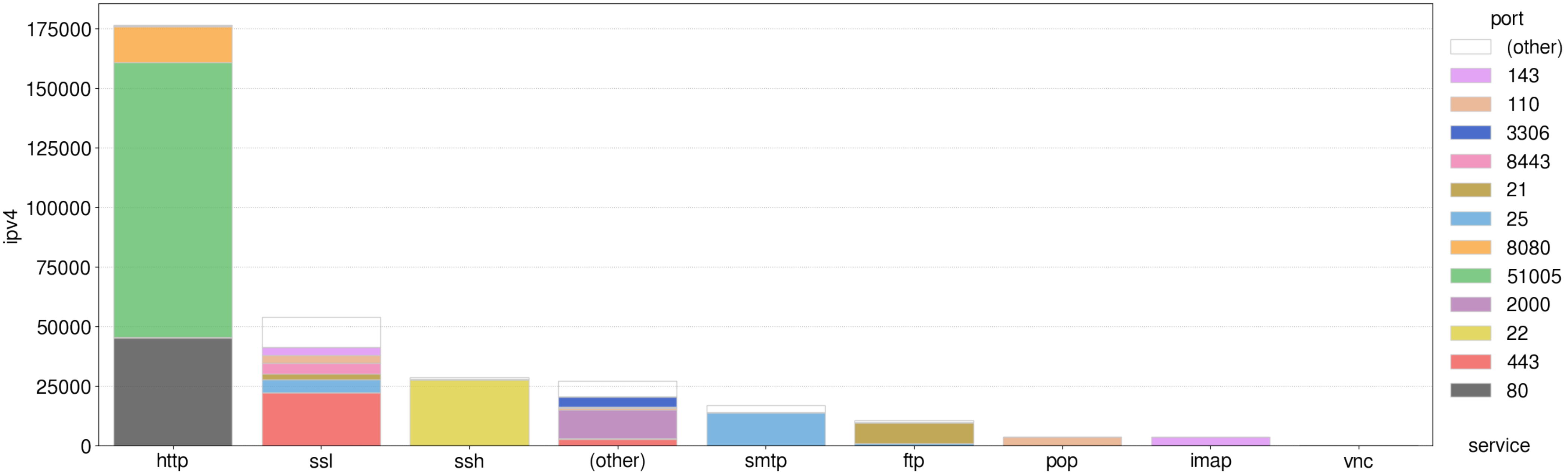
top isp per port

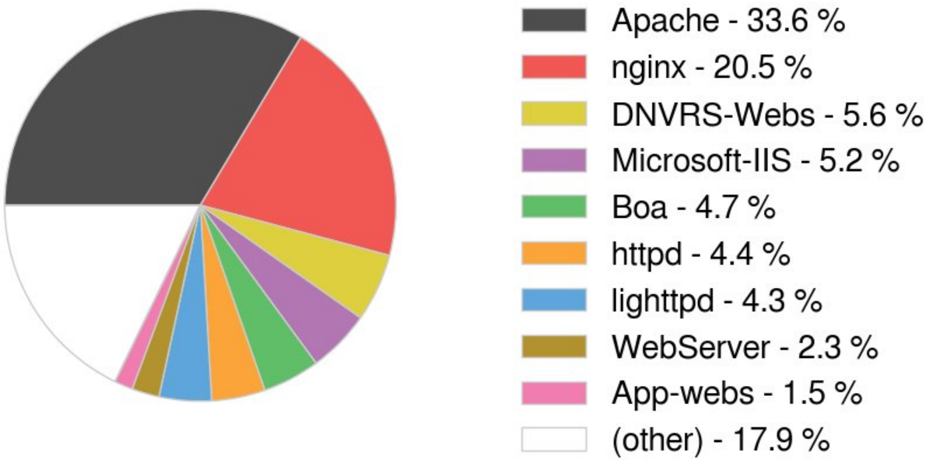


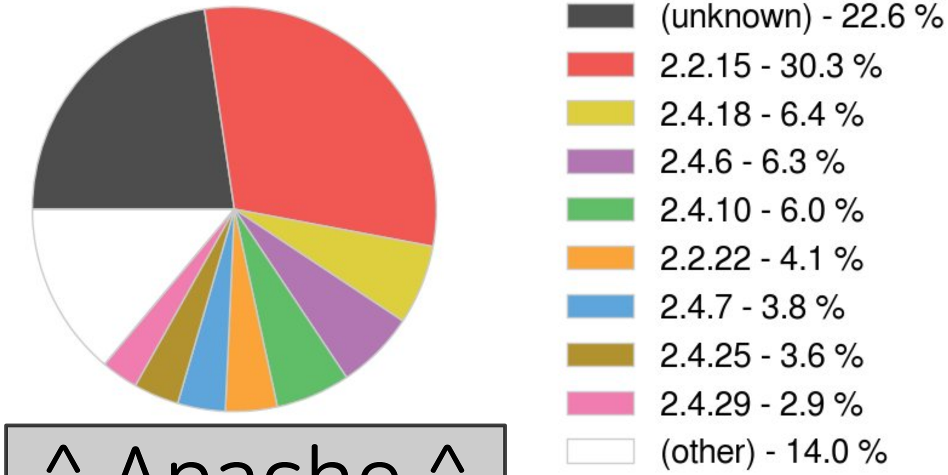
top isp per port (udp)



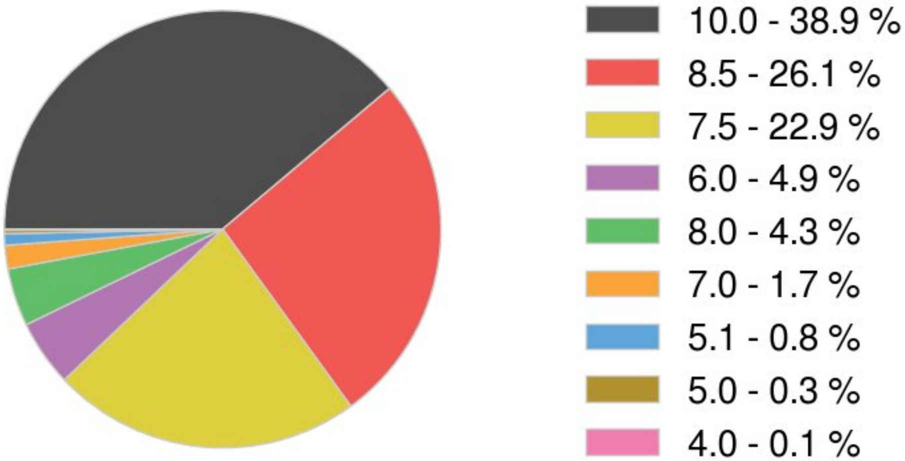
select actual ports per service (tcp)



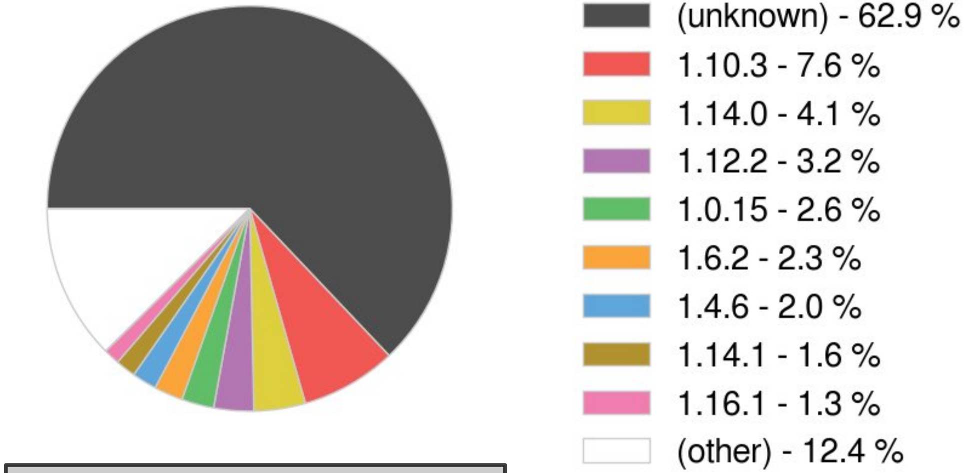




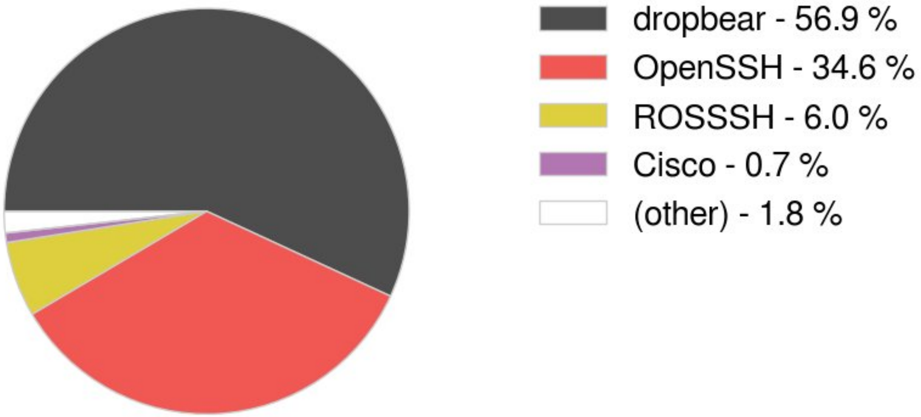
^ Apache ^

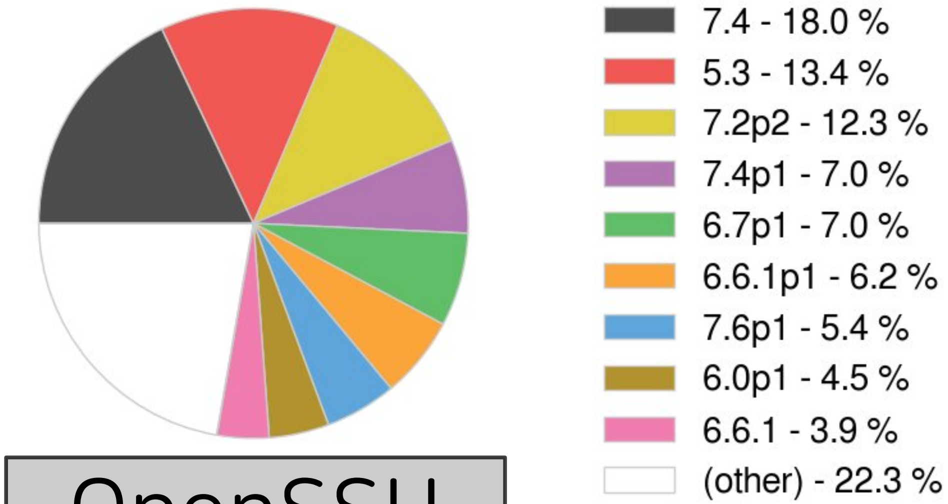


IIS

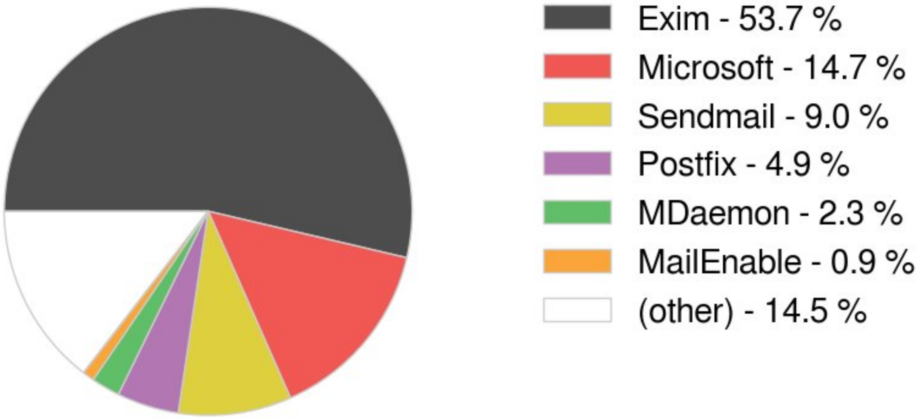


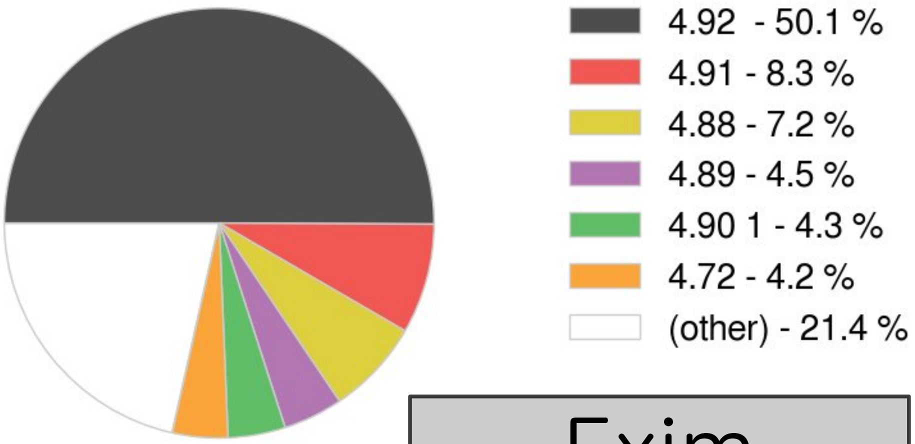
nginx





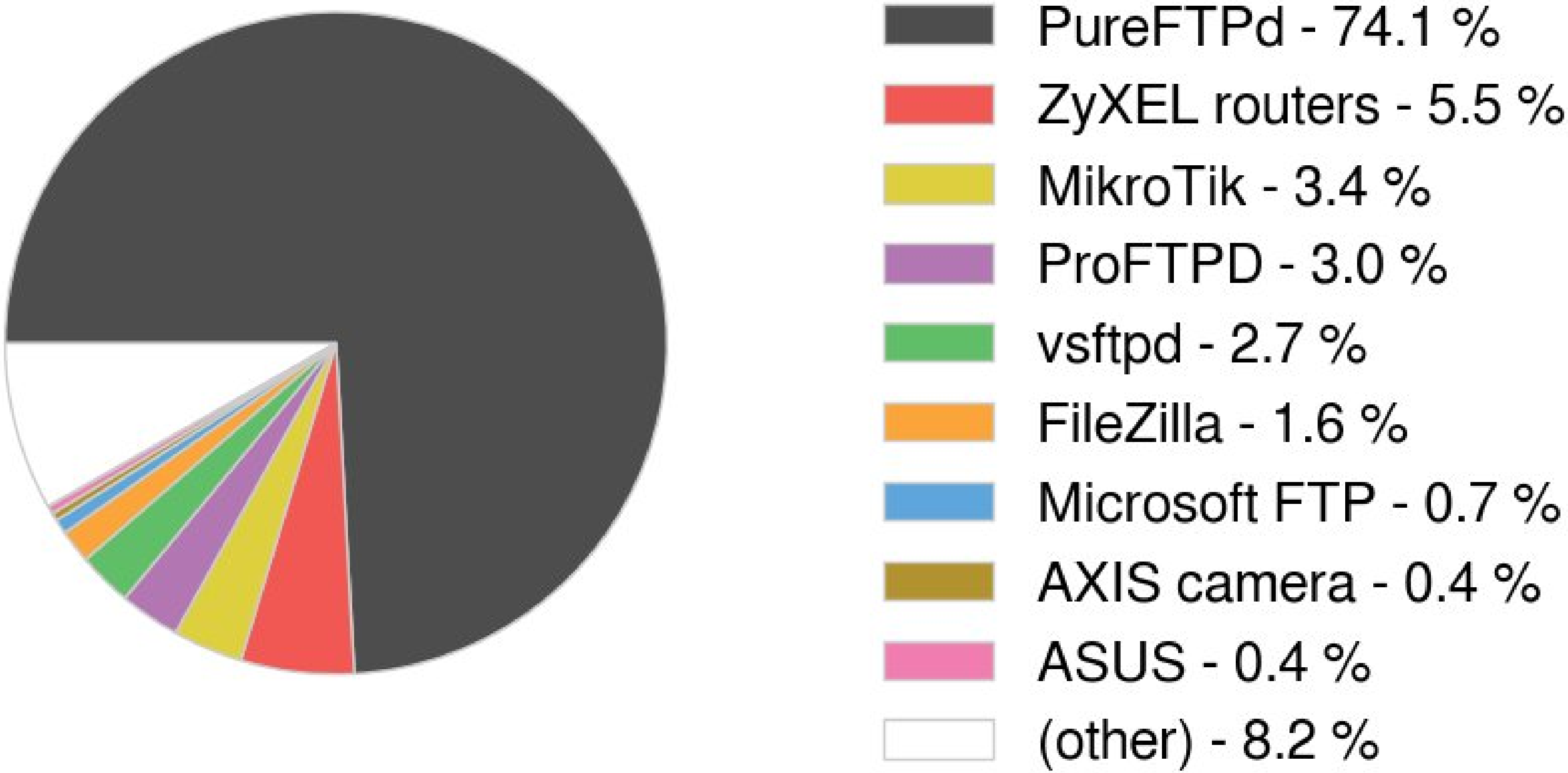
OpenSSH



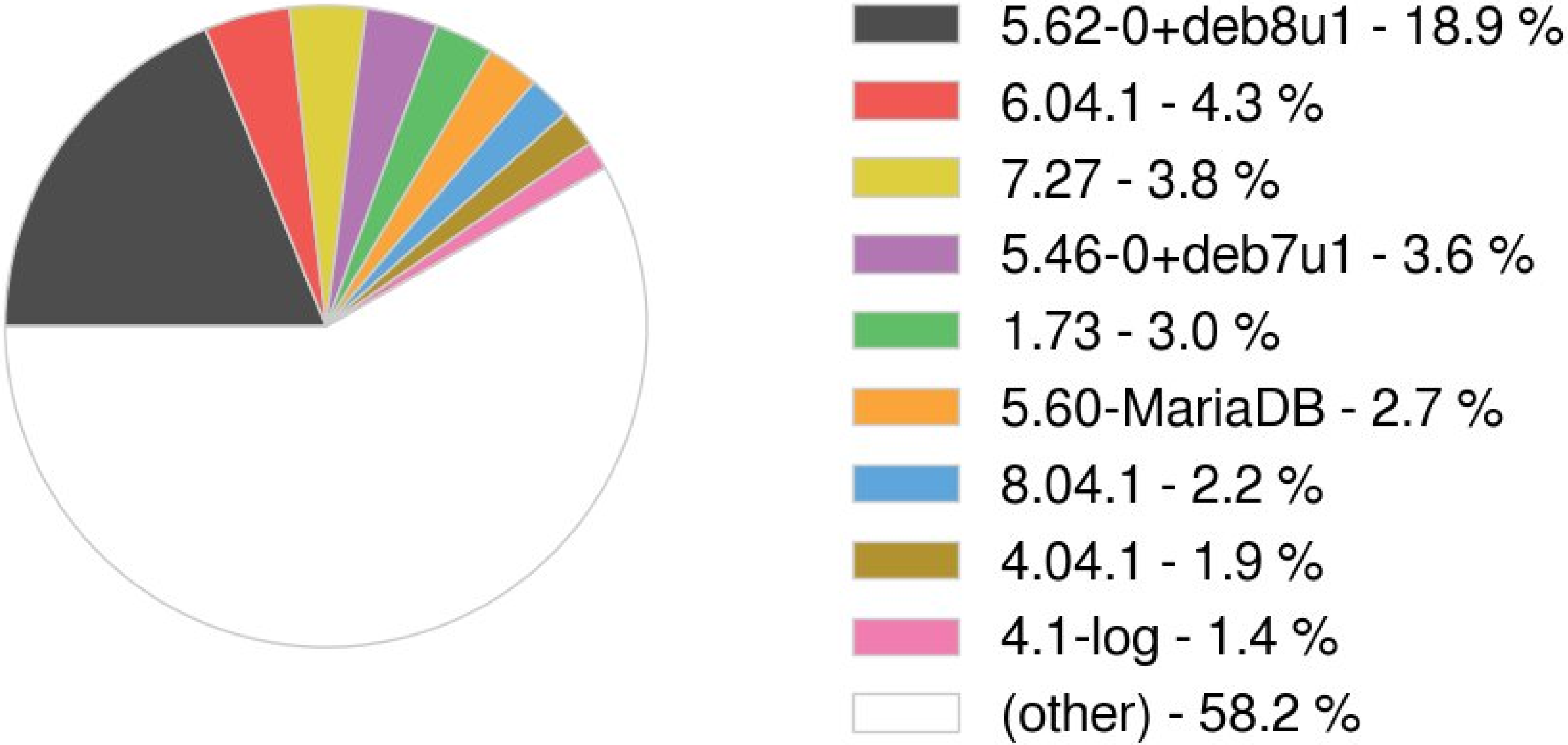


Exim

ftp servers


PureFTPd - 74.1 %
ZyXEL routers - 5.5 %
MikroTik - 3.4 %
ProFTPD - 3.0 %
vsftpd - 2.7 %
FileZilla - 1.6 %
Microsoft FTP - 0.7 %
AXIS camera - 0.4 %
ASUS - 0.4 %
(other) - 8.2 %

mysql versions



Interesting banners

- Ftp firmware update utility
  - 21/tcp on 28 broadband routers

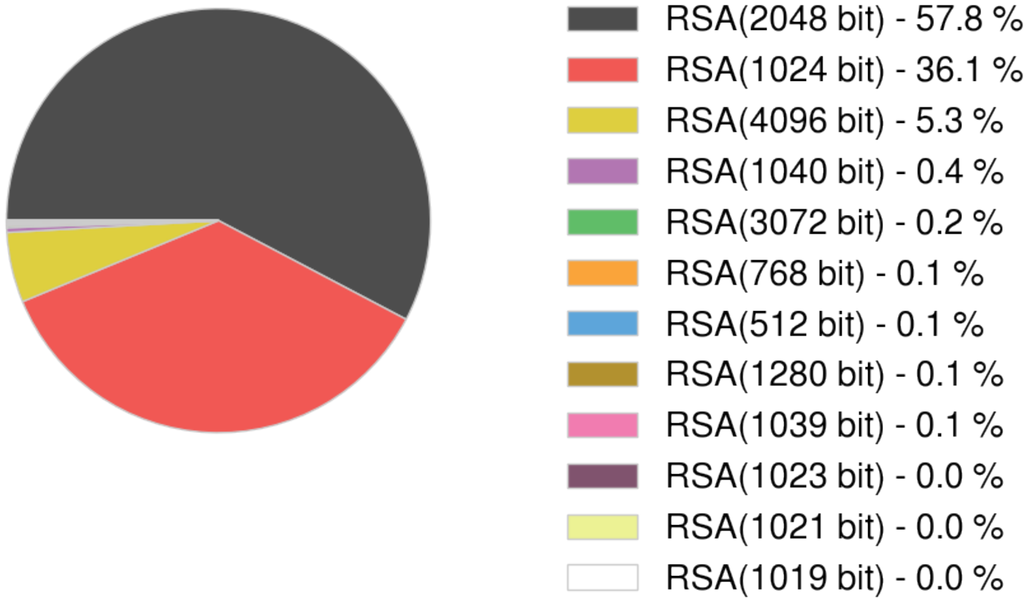
Certificates

107093 certs gathered from **50840** ip/ports

56274 non-CA certs from **42600** ip/ports

Certificates

- 125 use EC
  - 256 bit – 110
  - 384 bit – 15
- 56149 use RSA



Certificates

- 38.8% unique
- 61.5% unique excluding same IP
- **80.2%** unique excluding same /24

Top duplicate certificate #1

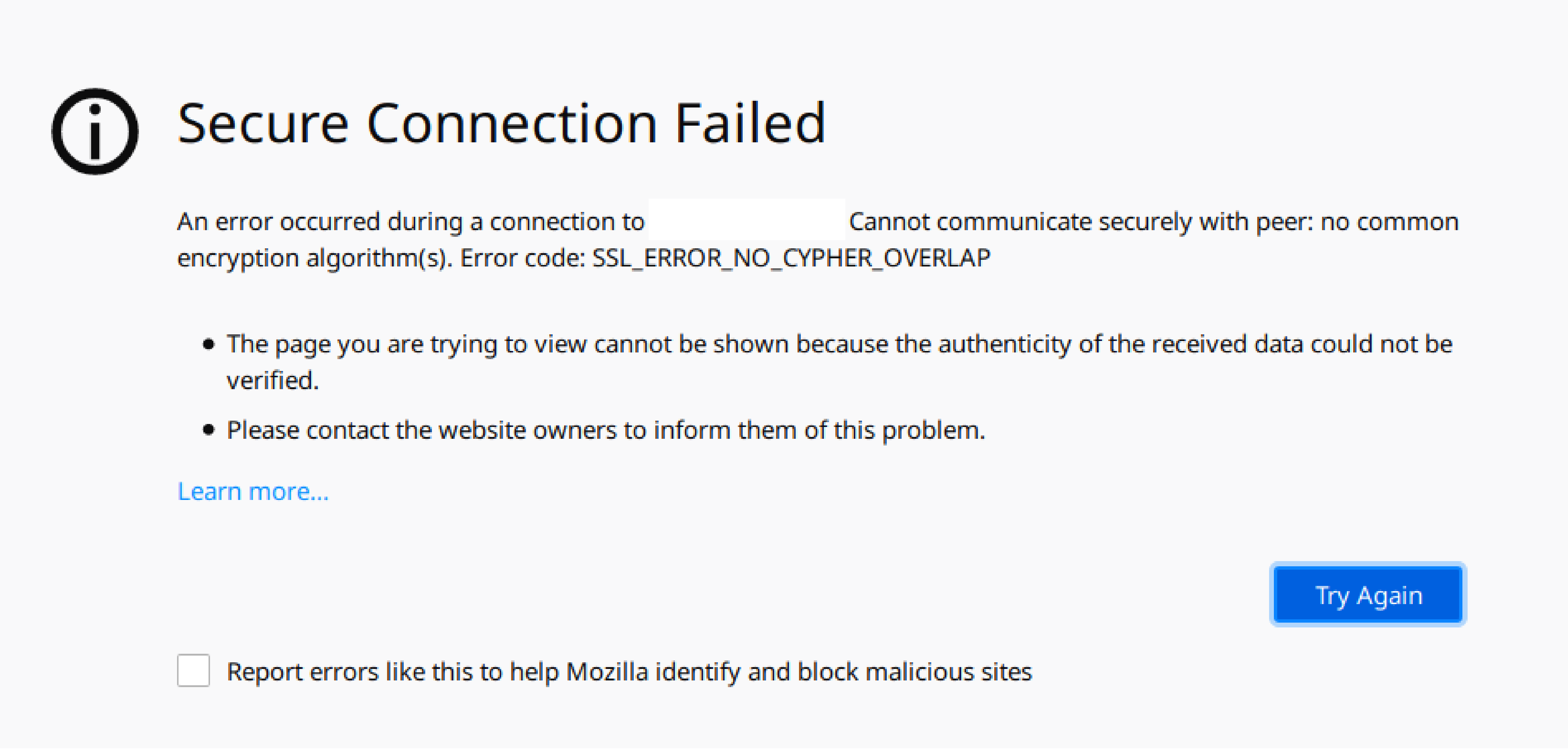
- **2056** Samsung smart TVs
- Not Before: Jan 1 00:00:00 1970 GMT
- Not After : Jan 1 00:00:00 2030 GMT
- Subject: ST = Surrey, C = GB, emailAddress = contact@samsung.com, O = Samsung SERI, OU = DTV, CN = server1

Top duplicate certificate #2

- **1408** Samsung smart TVs
- Not Before: Jan 1 00:00:00 1970 GMT
- Not After : Jan 1 00:00:00 2030 GMT
- Subject: ST = Surrey, C = GB, emailAddress = contact@samsung.com, O = Samsung SERI, OU = DTV, CN = 106.1.9.39

Top duplicate certificate #3

- **1273** dahua security cameras
- Not Before: Jun 18 09:16:23 2013 GMT
- Not After : Jun 19 09:16:23 2016 GMT
- Subject: CN = 192.168.1.108, C = CN, ST = ZHEJIANG, L = HANGZHOU, O = DAHUA, OU = DAHUATECH



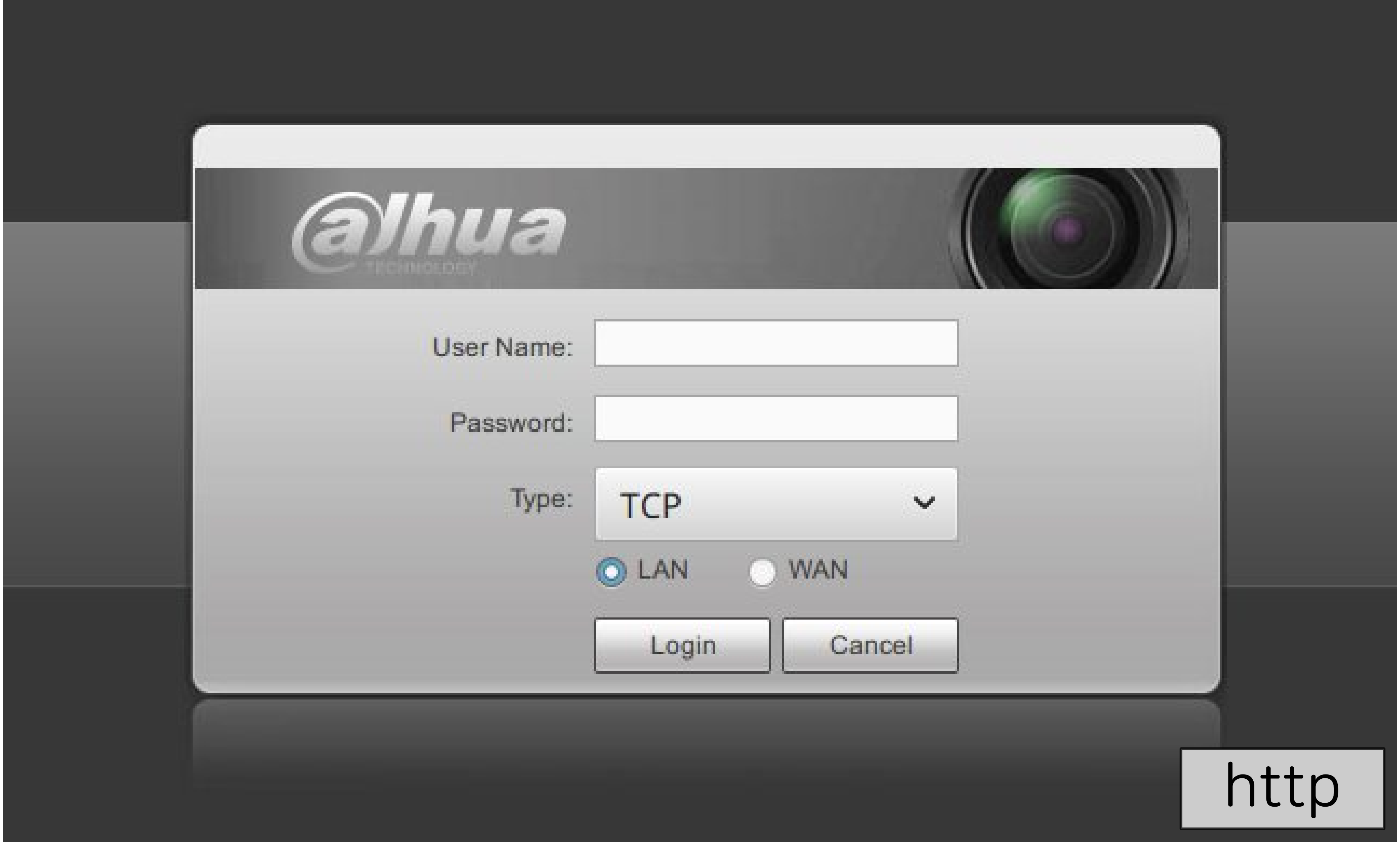
Secure Connection Failed

An error occurred during a connection to [redacted] Cannot communicate securely with peer: no common encryption algorithm(s). Error code: SSL_ERROR_NO_CYPHER_OVERLAP

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

Learn more…

☐ Report errors like this to help Mozilla identify and block malicious sites



User Name:

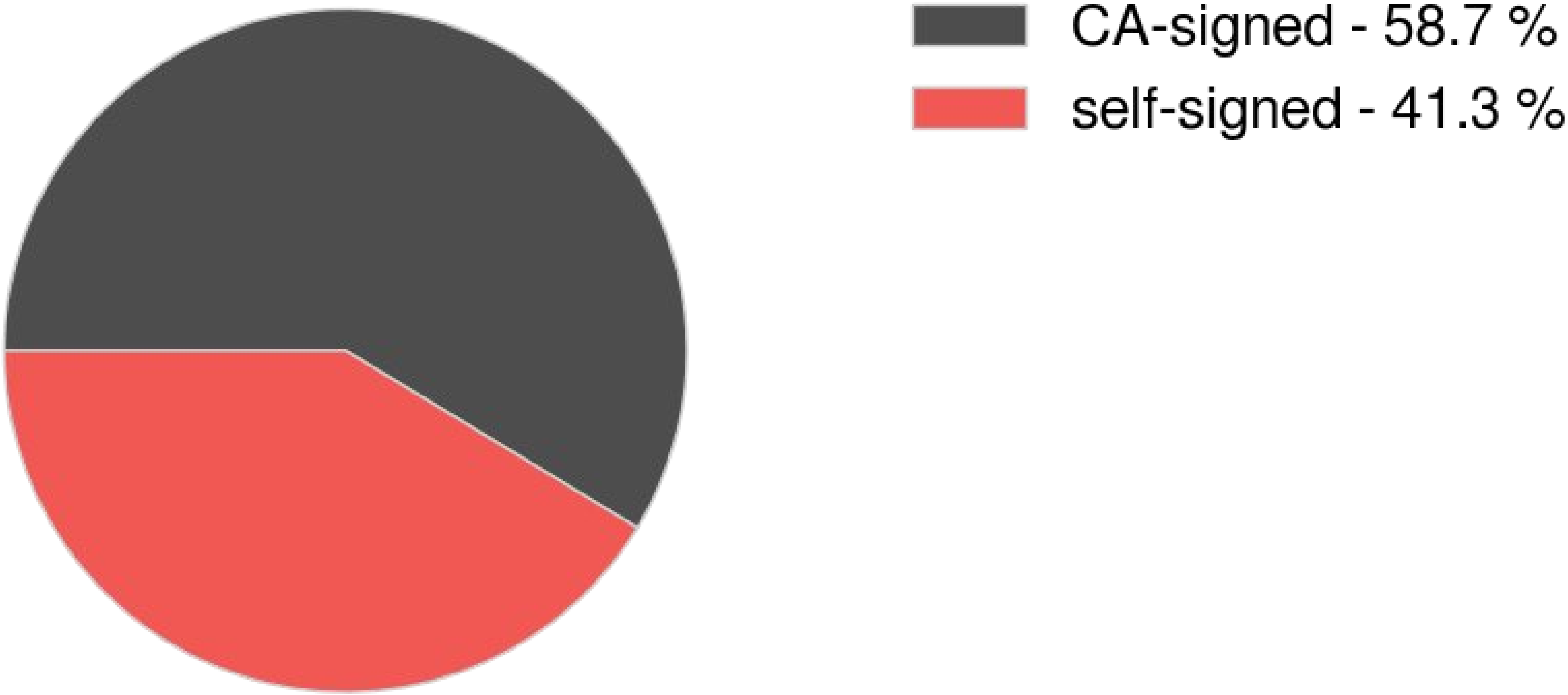
Password:

Type: TCP

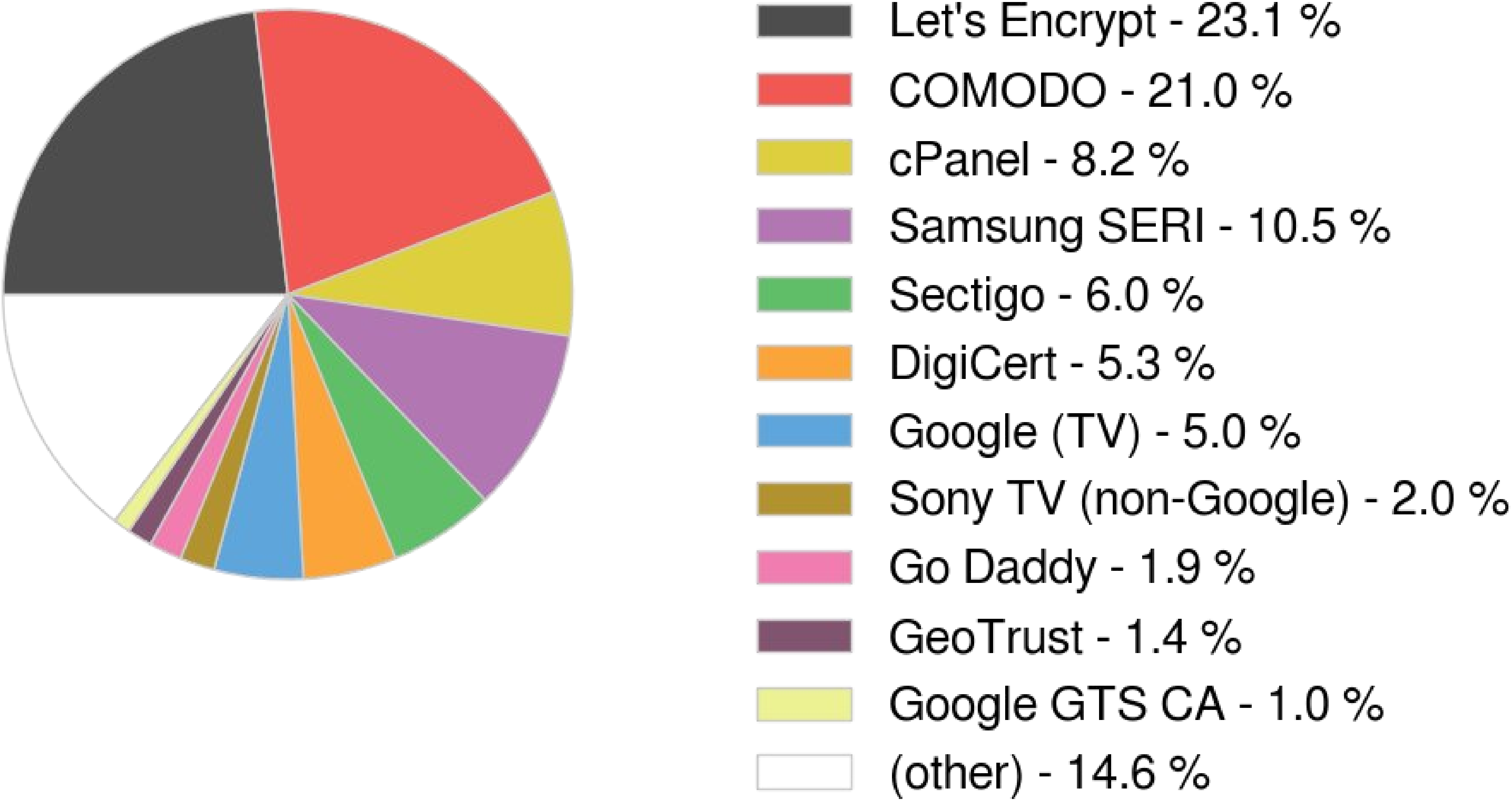
● LAN ○ WAN

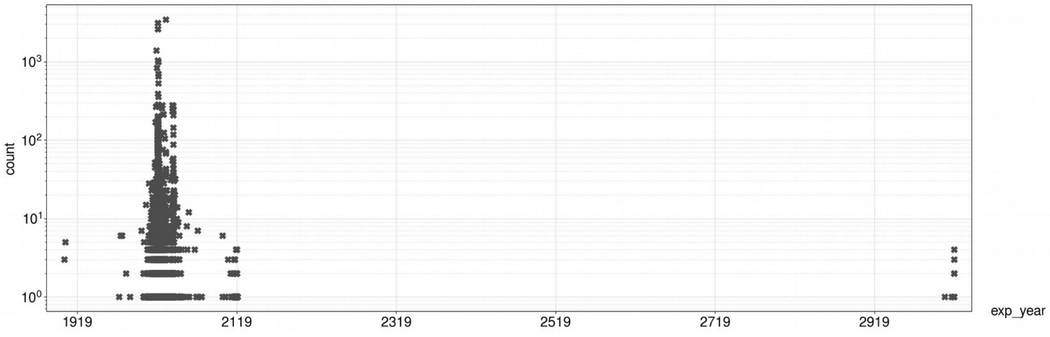
http

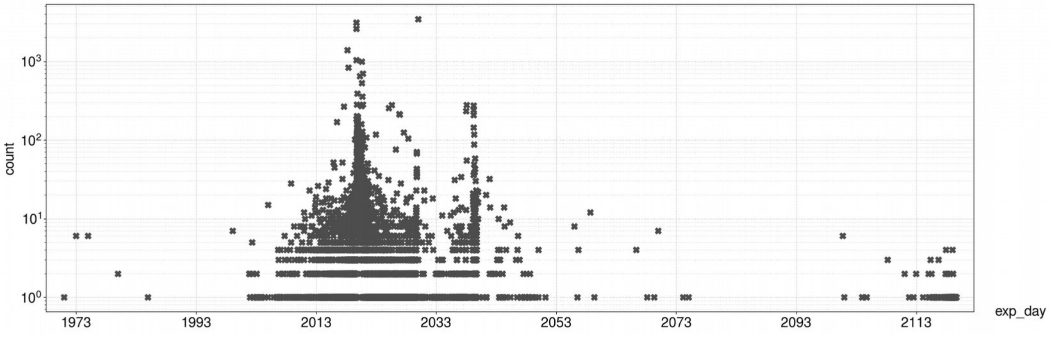
Cert issuers

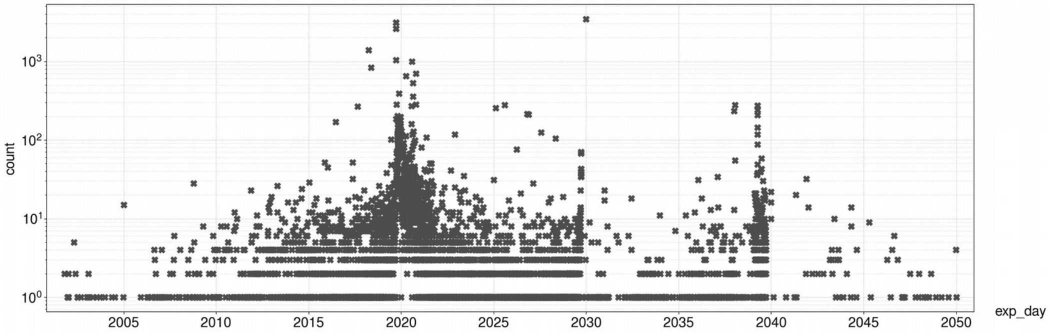


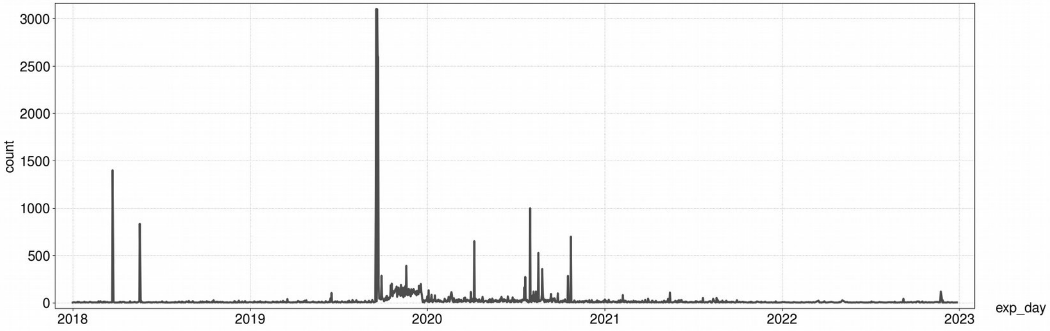
Authorities

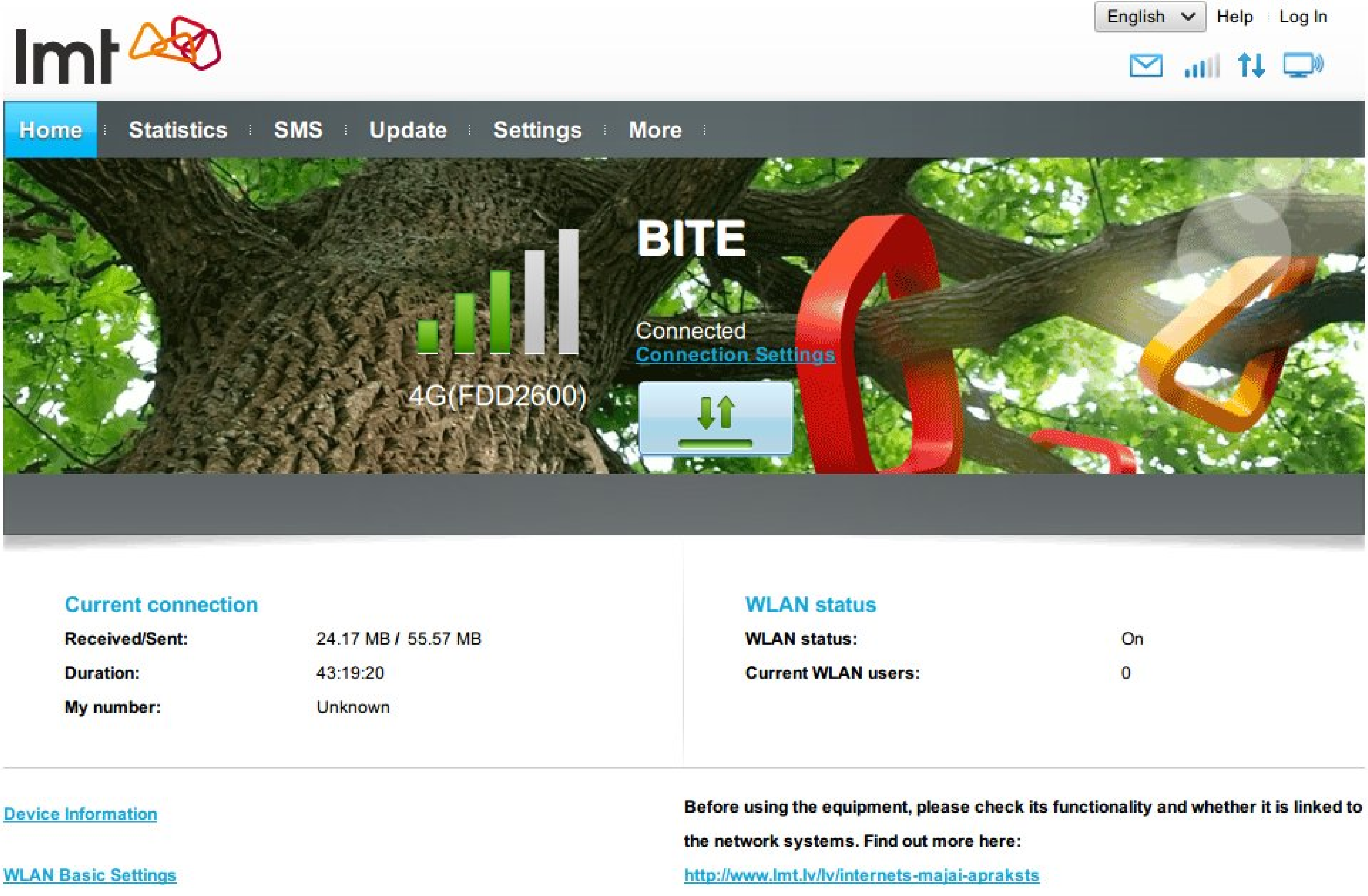



count
10^3
10^2
10^1
10^0
1919
2119
2319
2519
2719
2919
exp_year


count
10^3
10^2
10^1
10^0
1973
1993
2013
2033
2053
2073
2093
2113
exp_day


count
10^3
10^2
10^1
10^0
2005
2010
2015
2020
2025
2030
2035
2040
2045
2050
exp_day


count
3000
2500
2000
1500
1000
500
0
2018
2019
2020
2021
2022
2023
exp_day



Current connection

Received/Sent:	24.17 MB / 55.57 MB
Duration:	43:19:20
My number:	Unknown

WLAN status

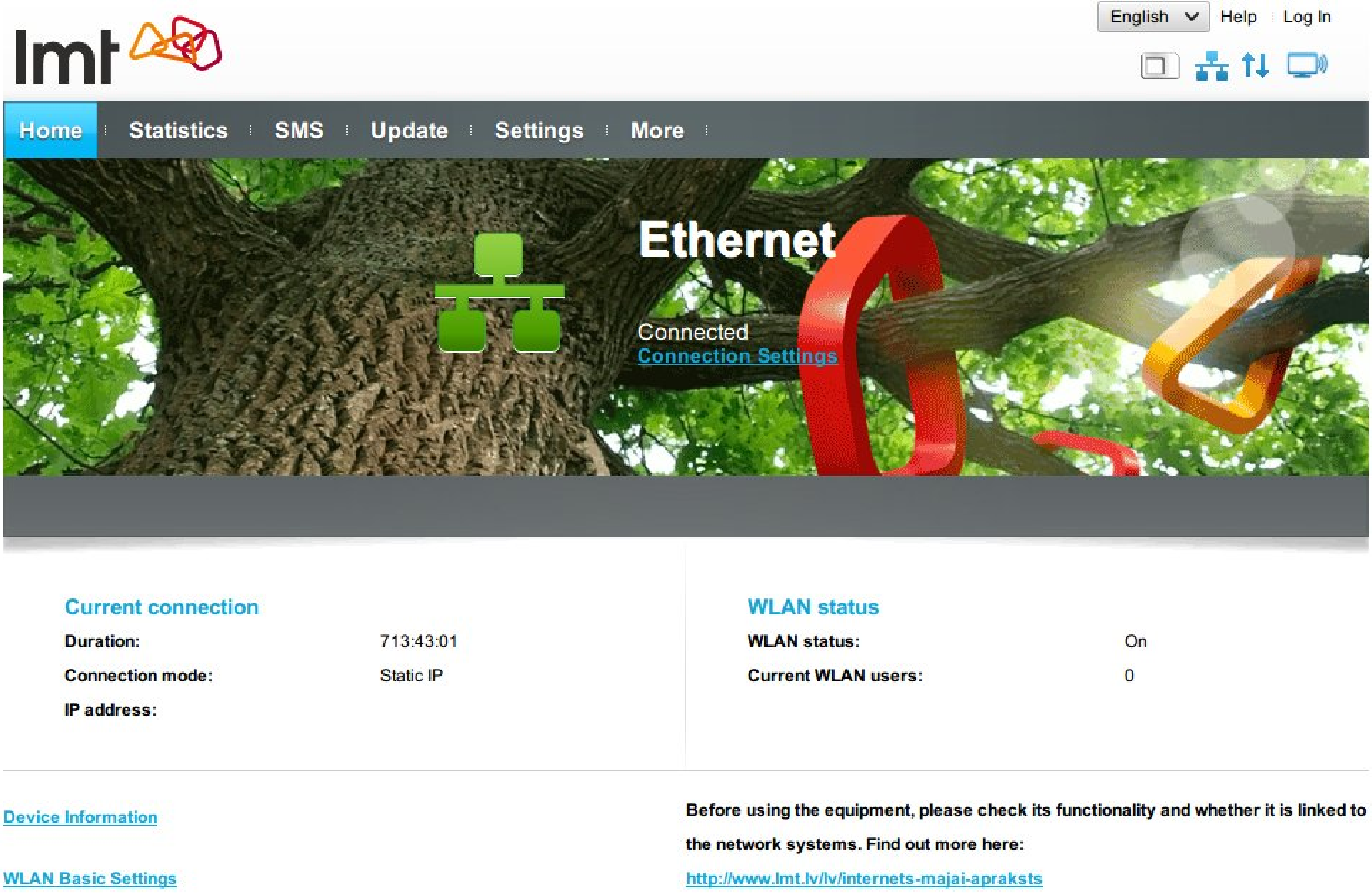
WLAN status:	On
Current WLAN users:	0

Device Information

WLAN Basic Settings

Before using the equipment, please check its functionality and whether it is linked to the network systems. Find out more here:

http://www.lmt.lv/lv/internets-majai-apraksts



Ethernet

Connected

Connection Settings

Current connection

Duration:	713:43:01
Connection mode:	Static IP
IP address:	

WLAN status

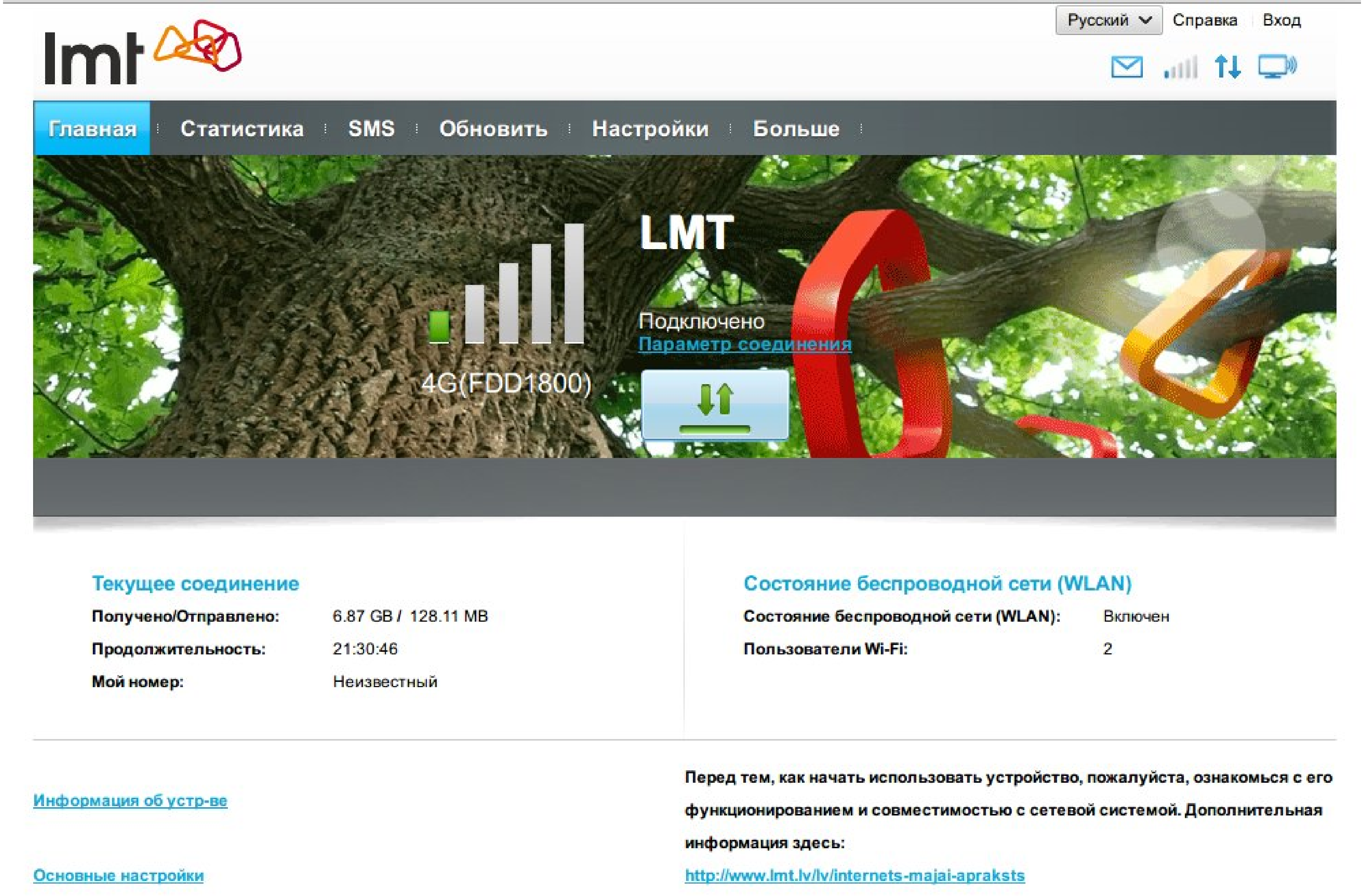
WLAN status:	On
Current WLAN users:	0

Device Information

WLAN Basic Settings

Before using the equipment, please check its functionality and whether it is linked to the network systems. Find out more here:

http://www.lmt.lv/lv/internets-majai-apraksts



Подключено
Параметр соединения

Текущее соединение

Получено/Отправлено:	6.87 GB / 128.11 MB
Продолжительность:	21:30:46
Мой номер:	Неизвестный

Состояние беспроводной сети (WLAN)

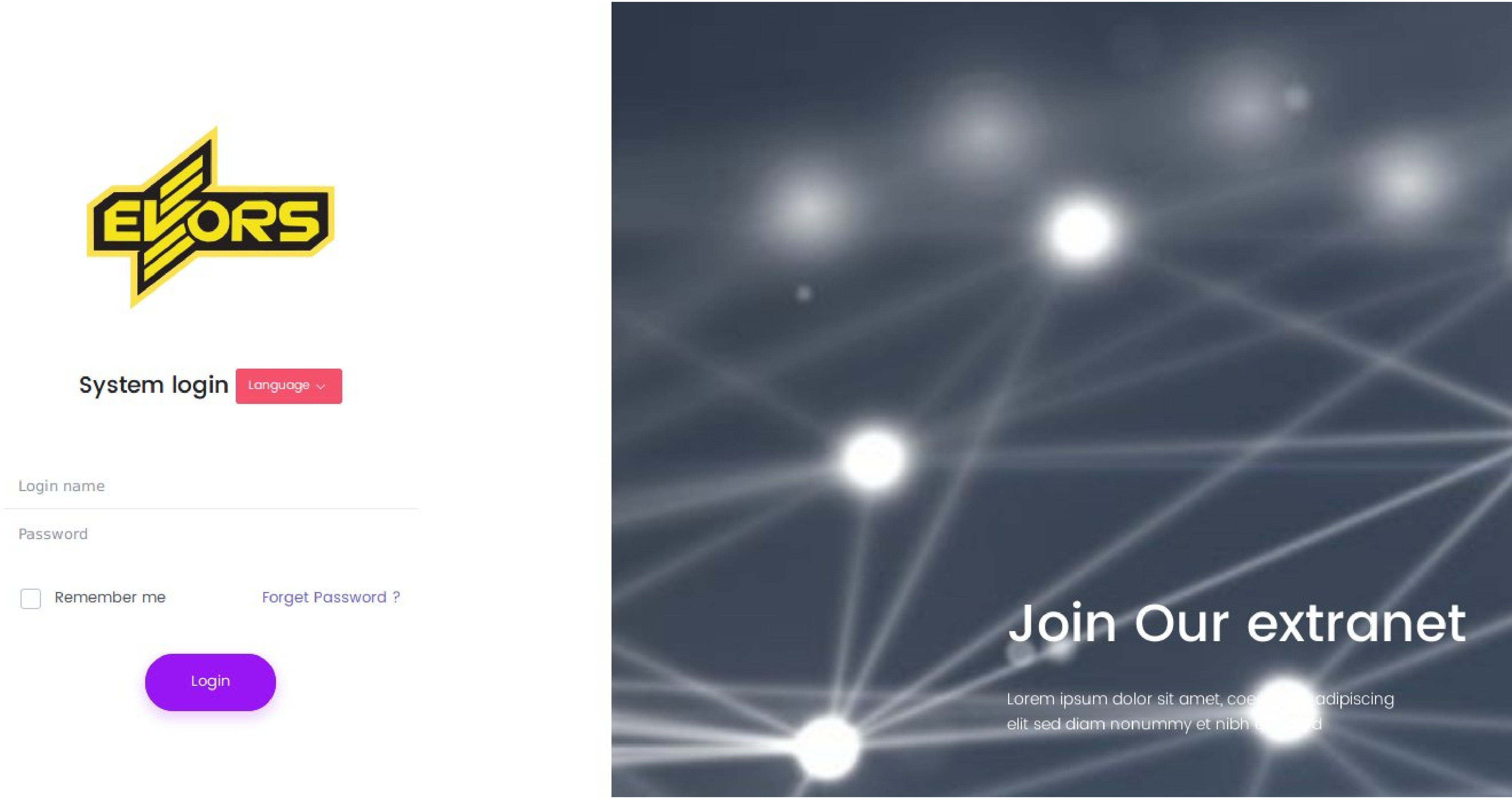
Состояние беспроводной сети (WLAN):	Включен
Пользователи Wi-Fi:	2

Информация об устр-ве

Основные настройки

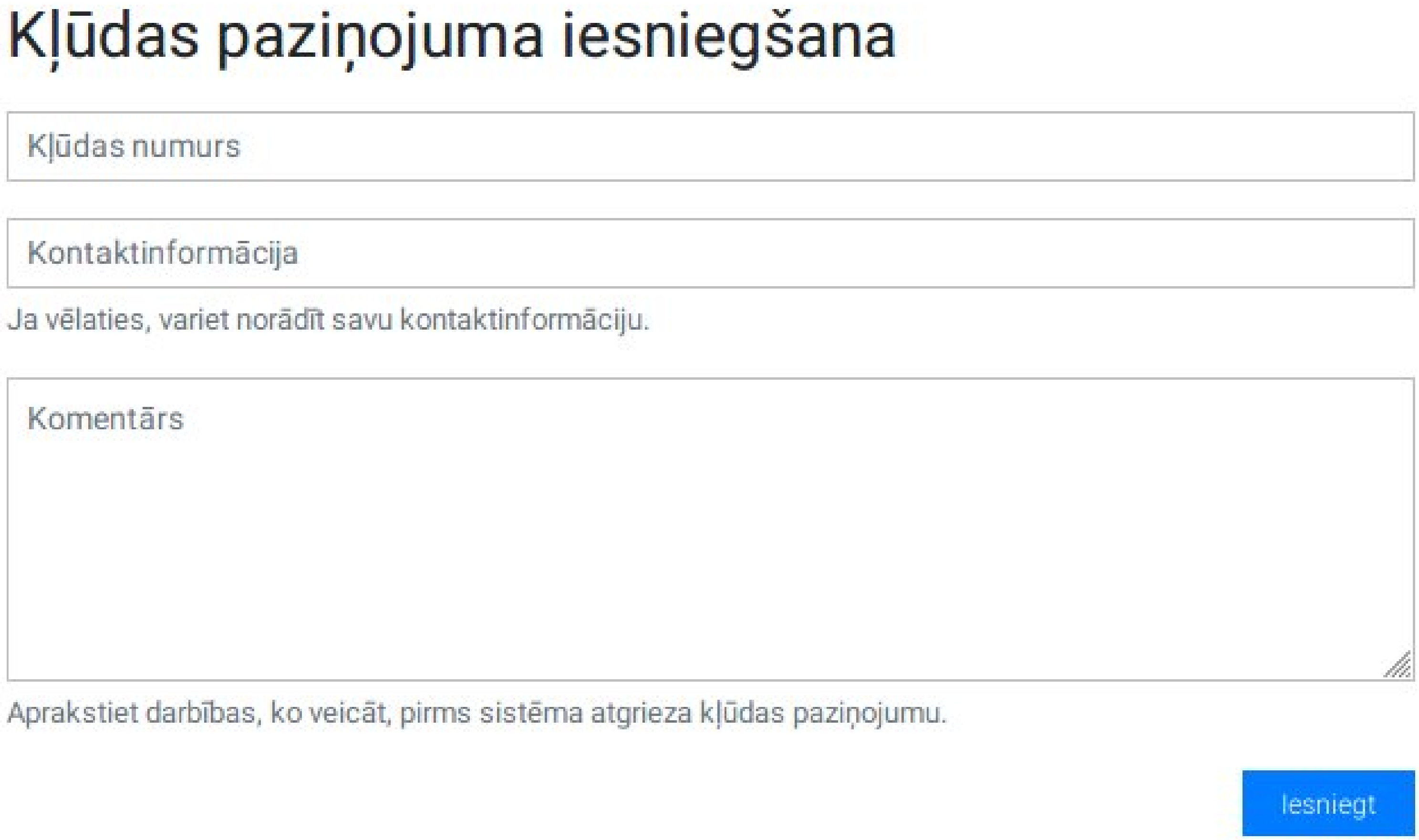
Перед тем, как начать использовать устройство, пожалуйста, ознакомься с его функционированием и совместимостью с сетевой системой. Дополнительная информация здесь:

http://www.lmt.lv/lv/internets-majai-apraksts



Join Our extranet

Lorem ipsum dolor sit amet, coe[illegible]adipiscing elit sed diam nonummy et nibh [illegible]d



Kļūdas paziņojuma iesniegšana

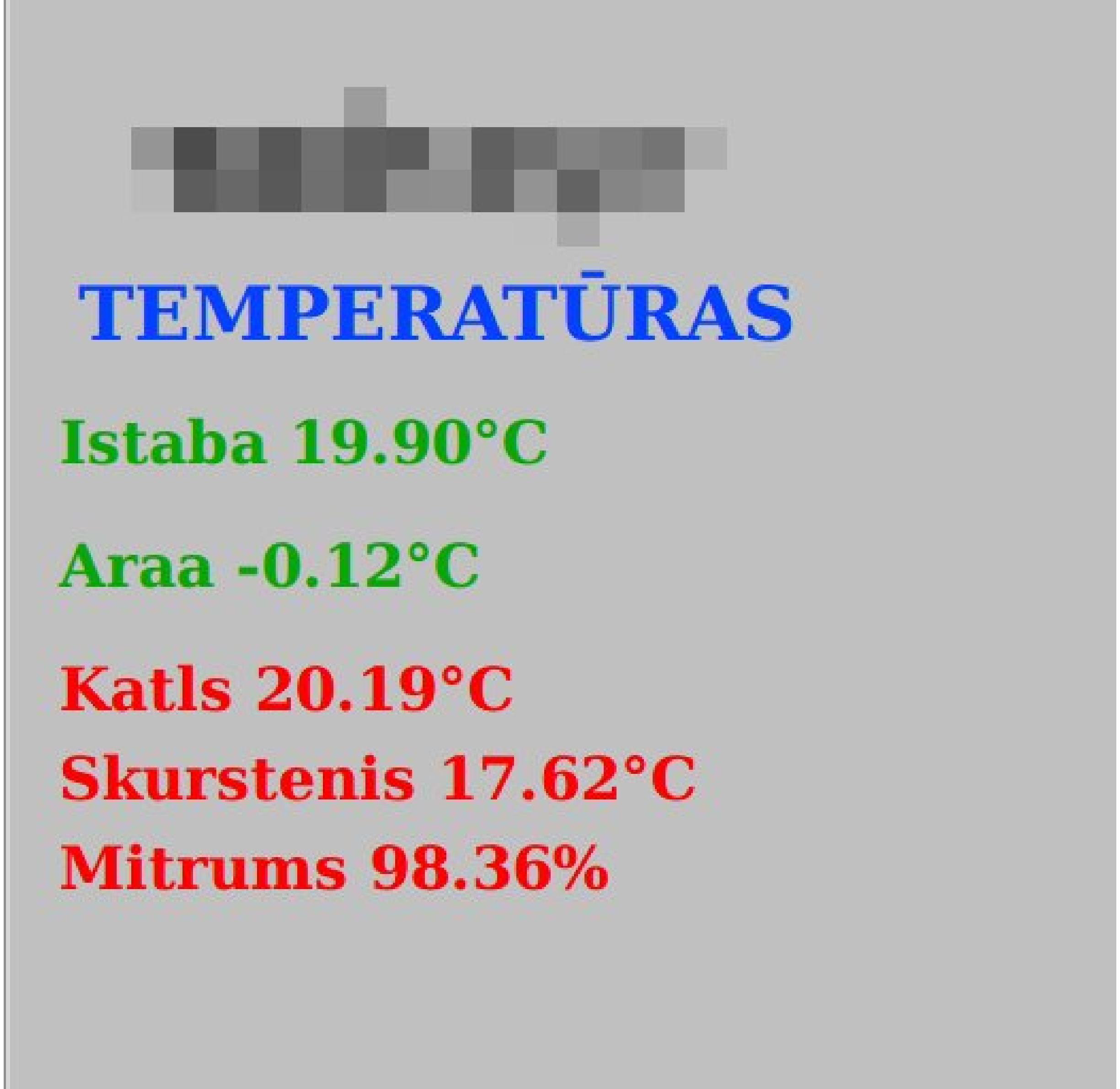
Kļūdas numurs

Kontaktinformācija

Ja vēlaties, variet norādīt savu kontaktinformāciju.

Komentārs

Aprakstiet darbības, ko veicāt, pirms sistēma atgrieza kļūdas paziņojumu.



[redacted]

TEMPERATŪRAS

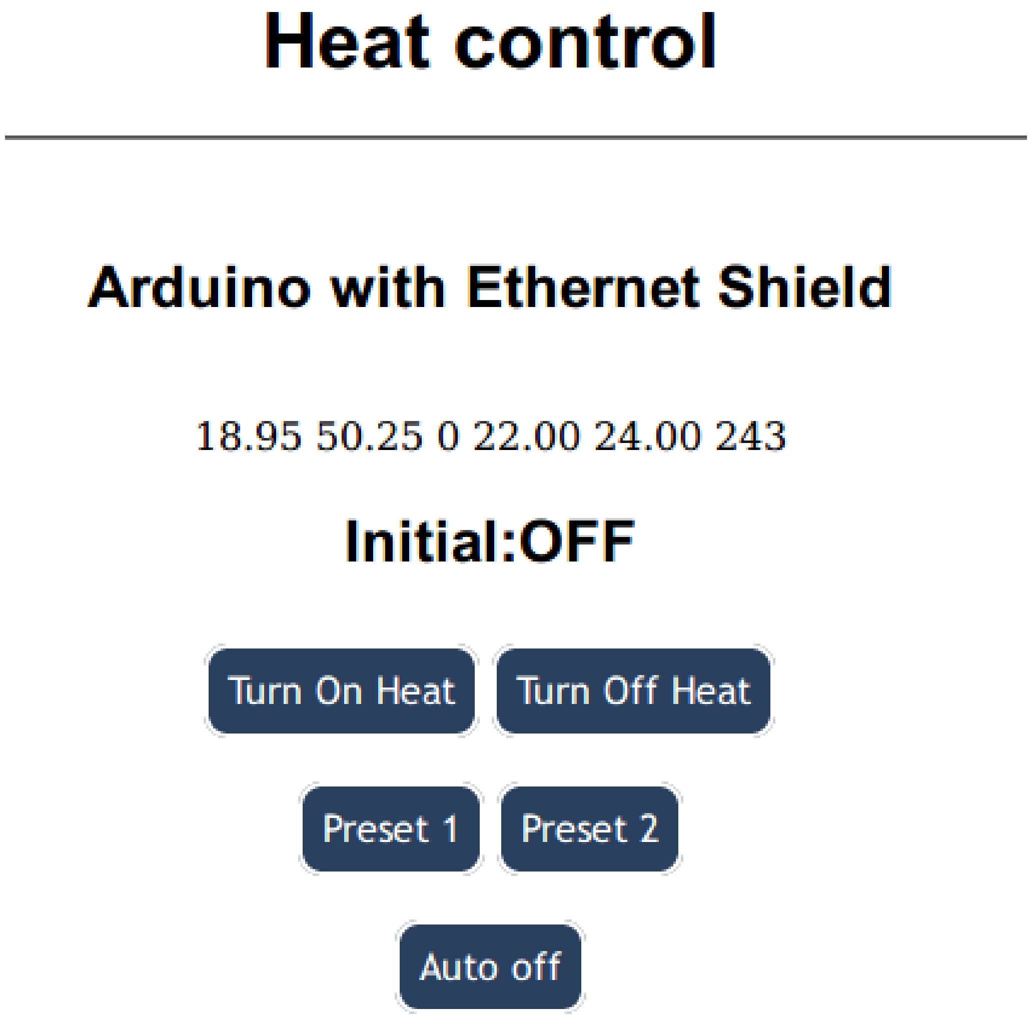
Istaba 19.90°C

Araa -0.12°C

Katls 20.19°C

Skurstenis 17.62°C

Mitrums 98.36%

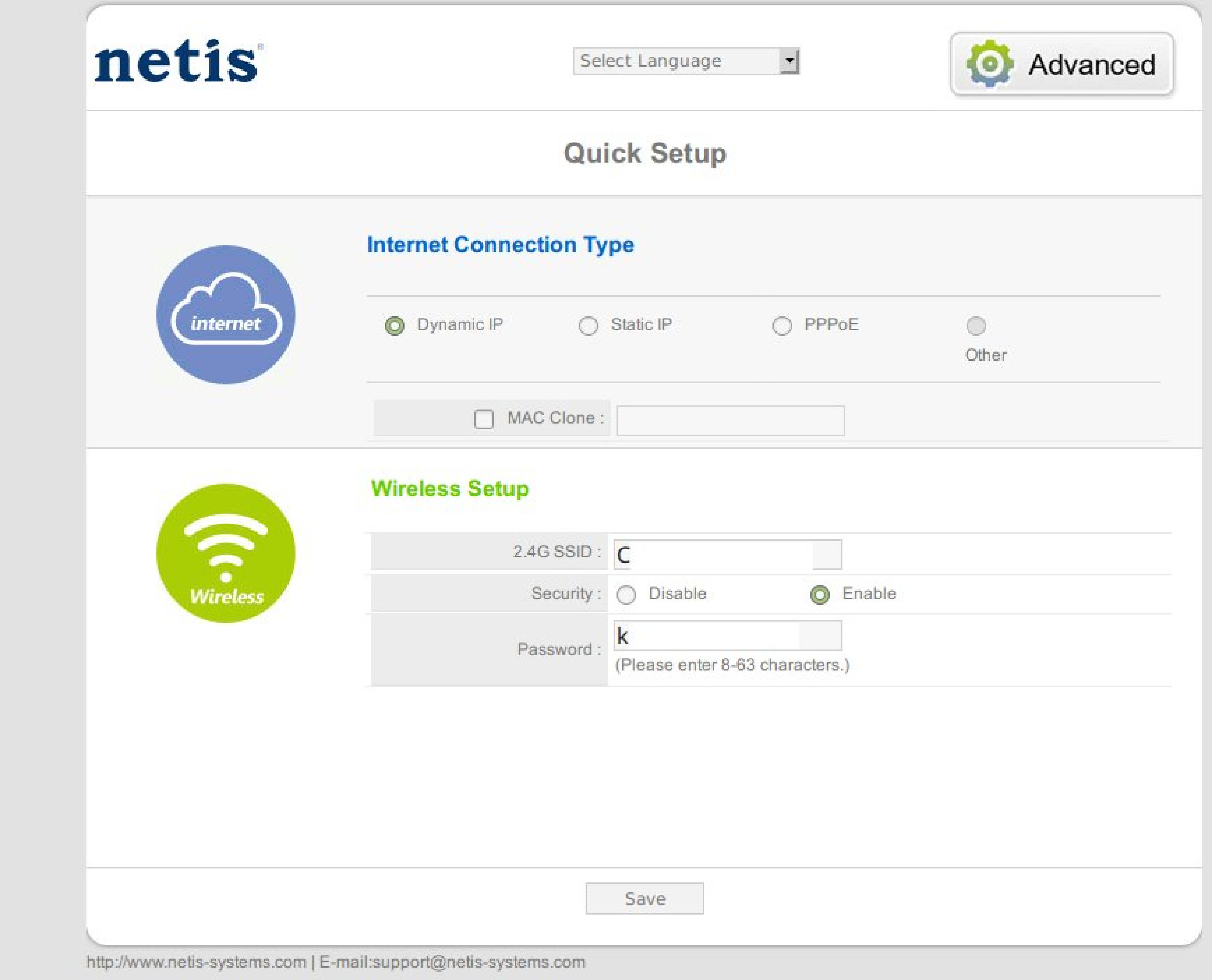


Heat control

Arduino with Ethernet Shield

18.95 50.25 0 22.00 24.00 243

Initial:OFF



Quick Setup

Internet Connection Type

● Dynamic IP ○ Static IP ○ PPPoE ○ Other

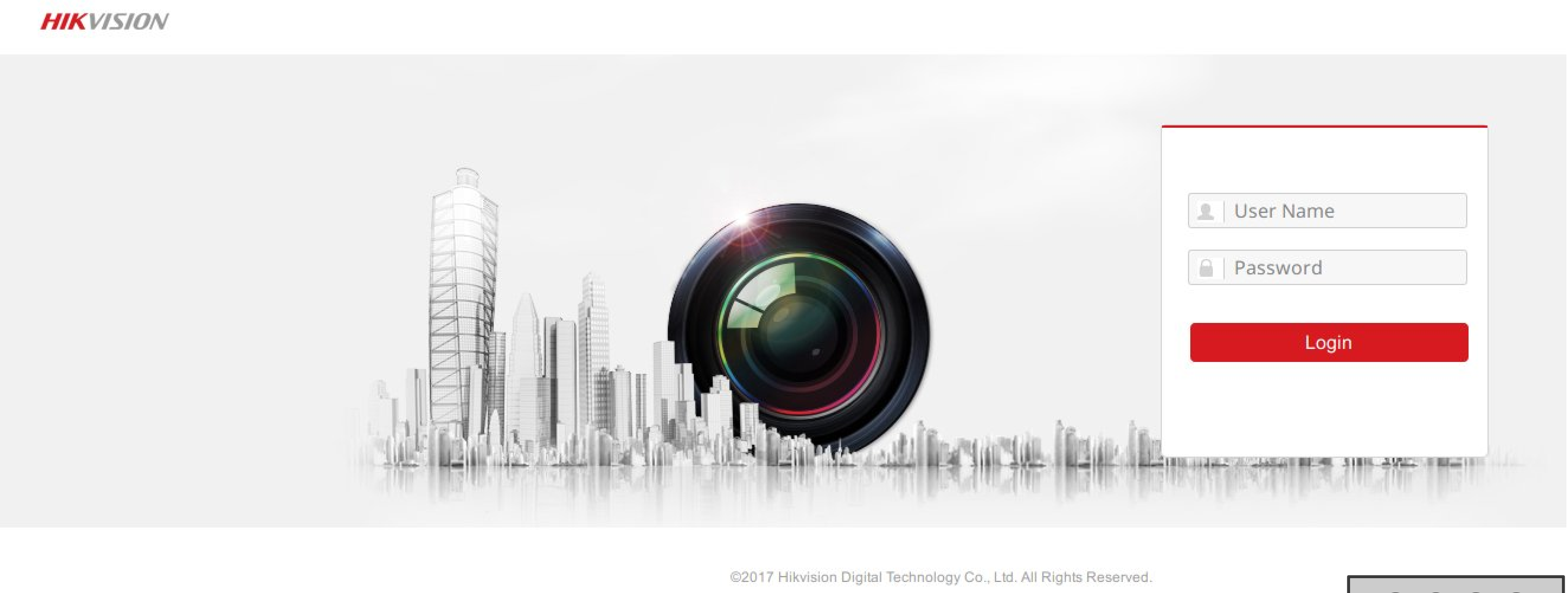
□ MAC Clone :

Wireless Setup

2.4G SSID :	C
Security :	○ Disable ● Enable
Password :	k (Please enter 8-63 characters.)

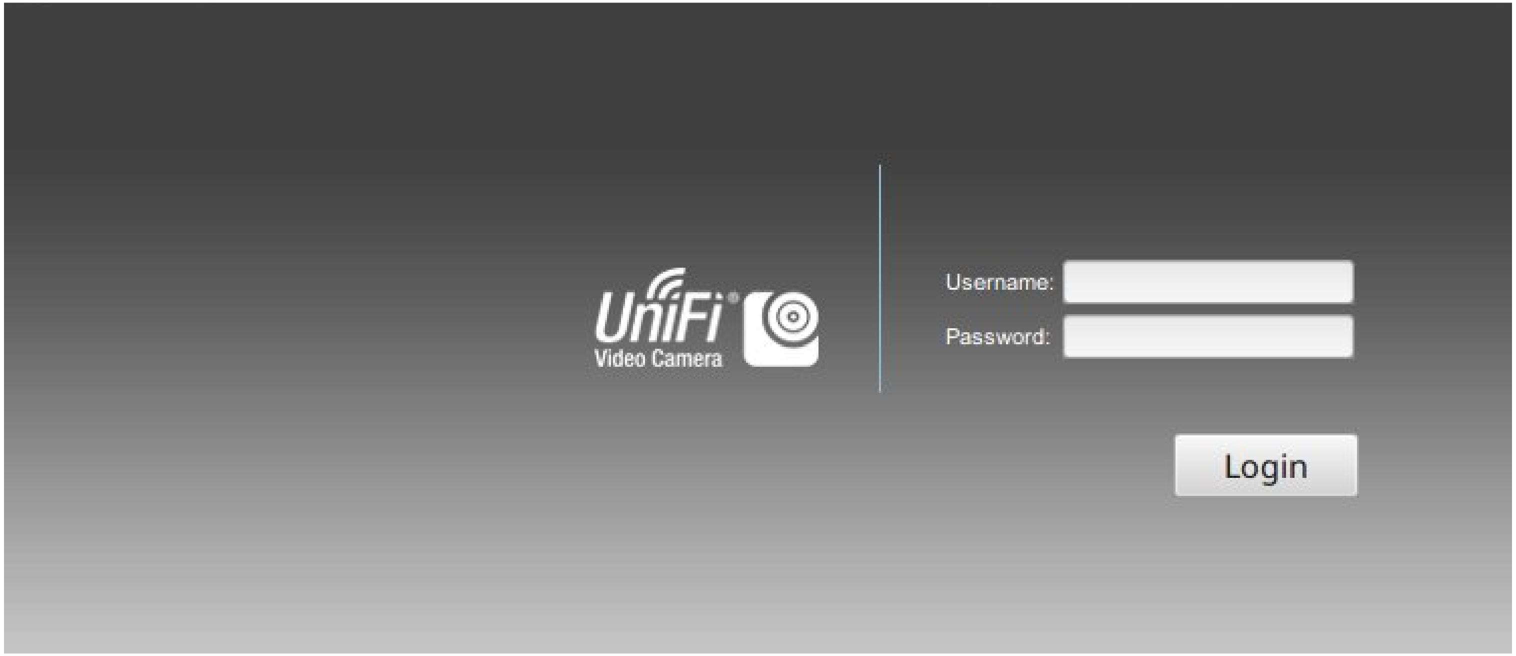
Save

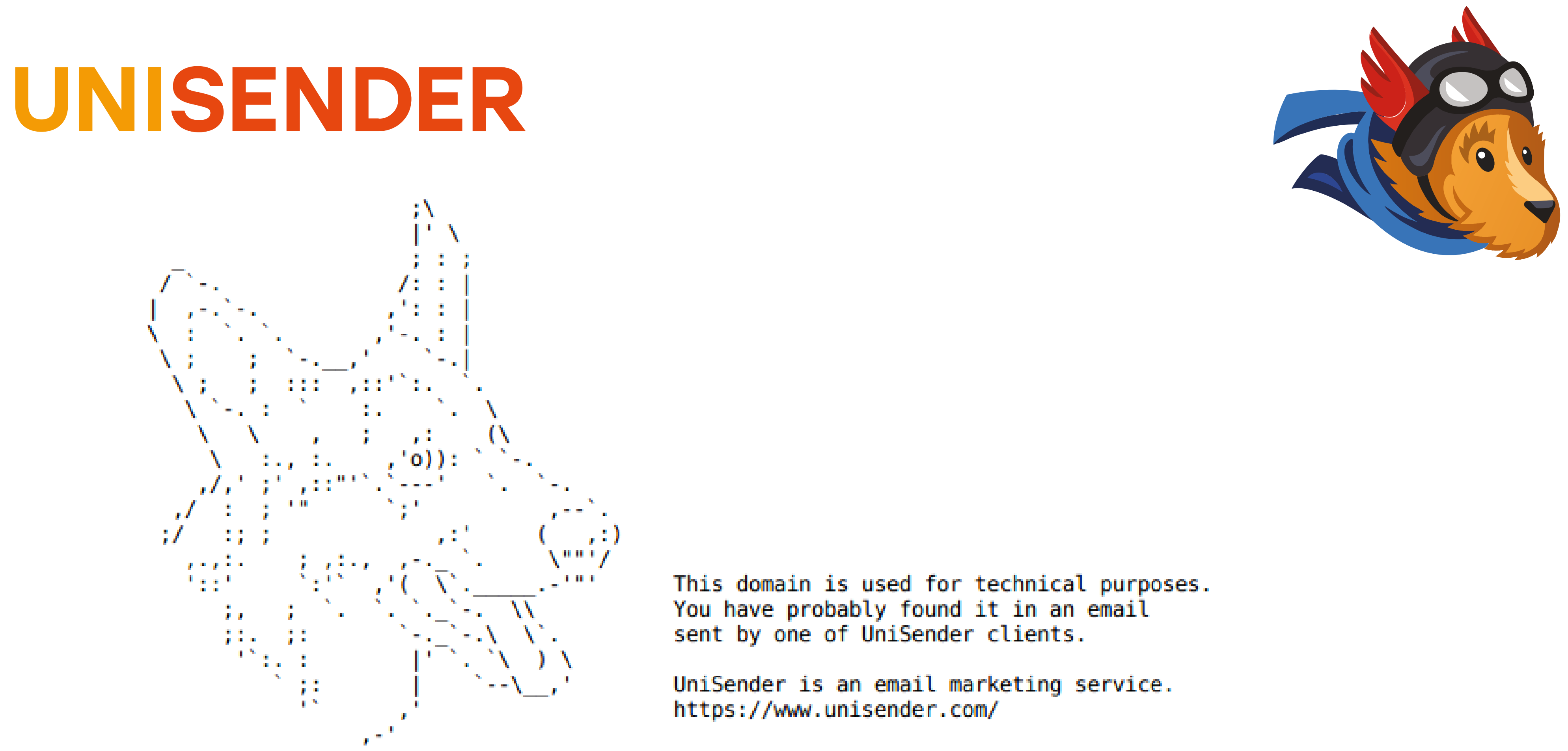
http://www.netis-systems.com | E-mail:support@netis-systems.com



©2017 Hikvision Digital Technology Co., Ltd. All Rights Reserved.

2899

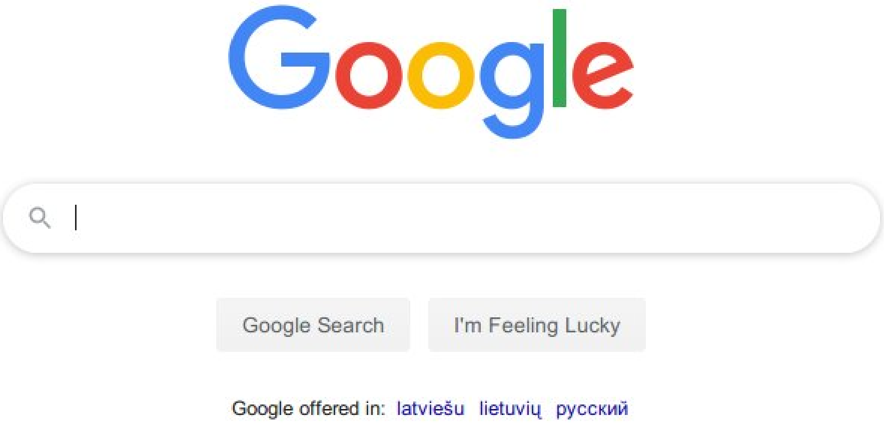

UniFi Video Camera
Username:
Password:
Login



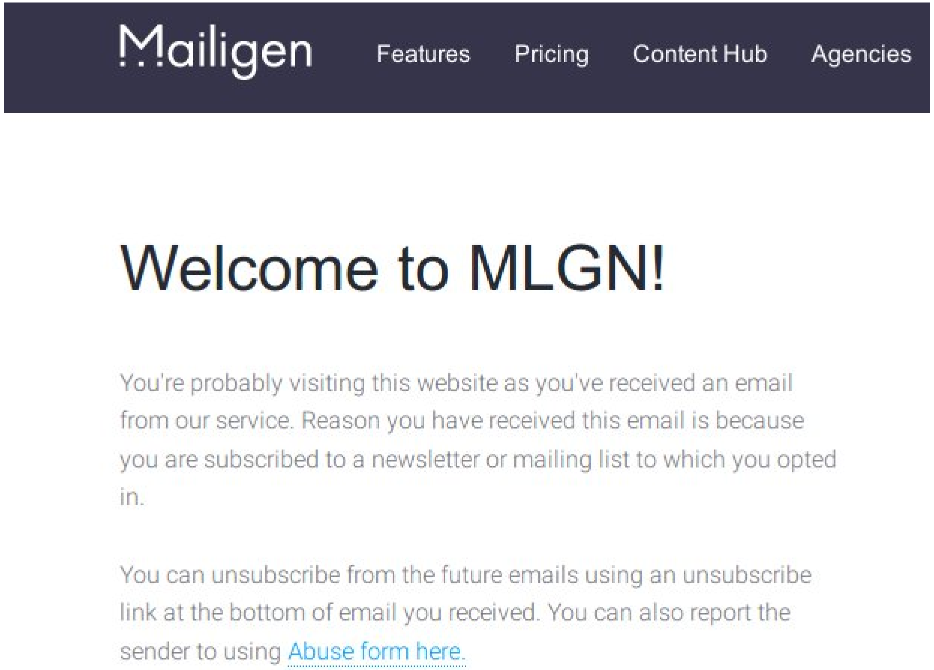
UNISENDER

```
This domain is used for technical purposes.
You have probably found it in an email
sent by one of UniSender clients.

UniSender is an email marketing service.
https://www.unisender.com/
```

1028


Google
Google Search
I'm Feeling Lucky
Google offered in: latviešu lietuvių русский

760



Welcome to MLGN!

You're probably visiting this website as you've received an email from our service. Reason you have received this email is because you are subscribed to a newsletter or mailing list to which you opted in.

You can unsubscribe from the future emails using an unsubscribe link at the bottom of email you received. You can also report the sender to using Abuse form here.

500

Watch my presentations: https://kirils.org/

Follow me @KirilsSolovjovs

Obviously,
All the screenshots and logos in the presentation are used on a fair-use basis.

Furthermore, obviously,
No affiliation is claimed with any companies mentioned in the presentation.