



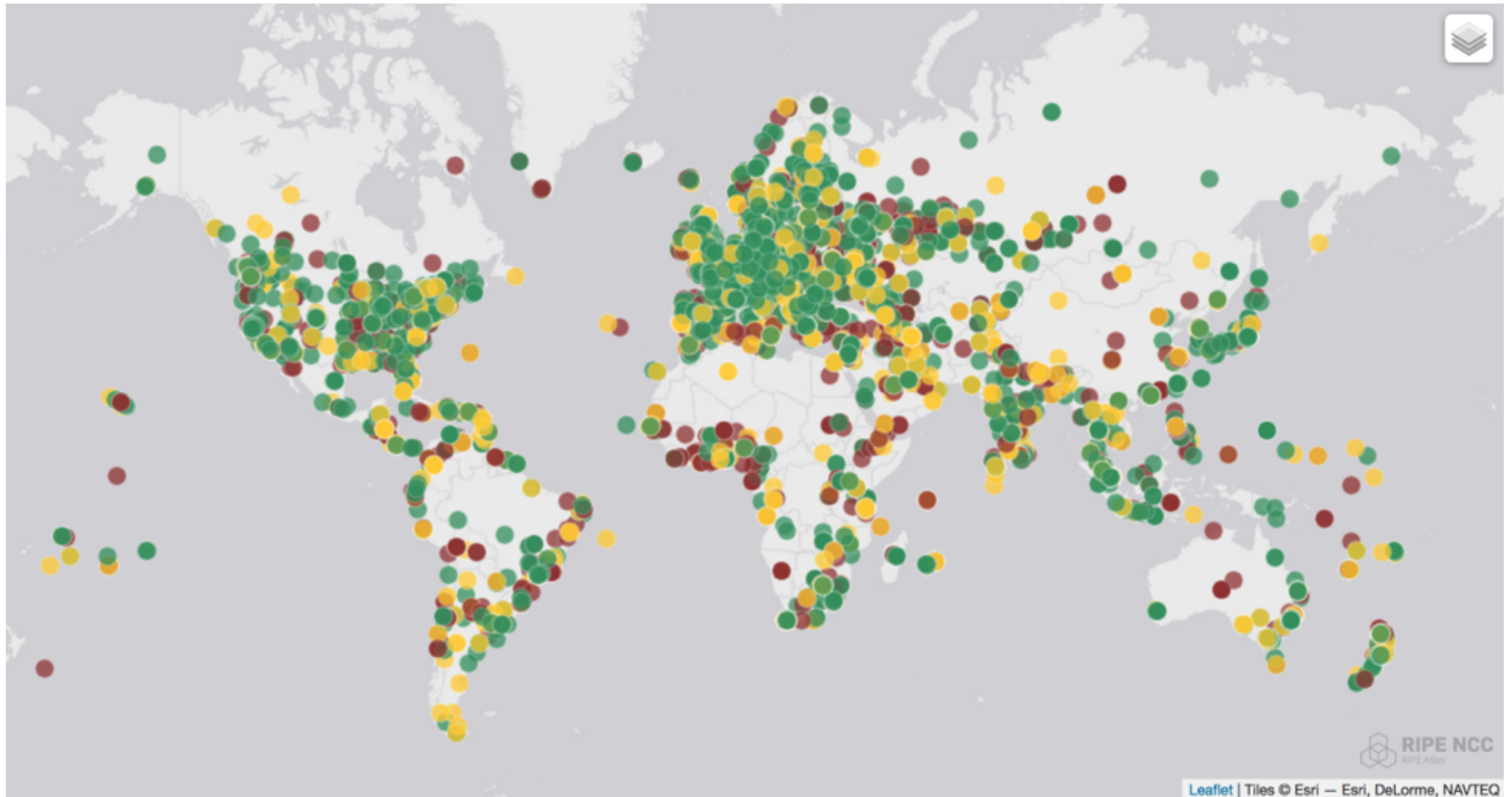
RIPE NCC
RIPE NETWORK COORDINATION CENTRE

How RIPE NCC tools can help with online investigations

The Internet Registry System



RIPE Atlas Coverage



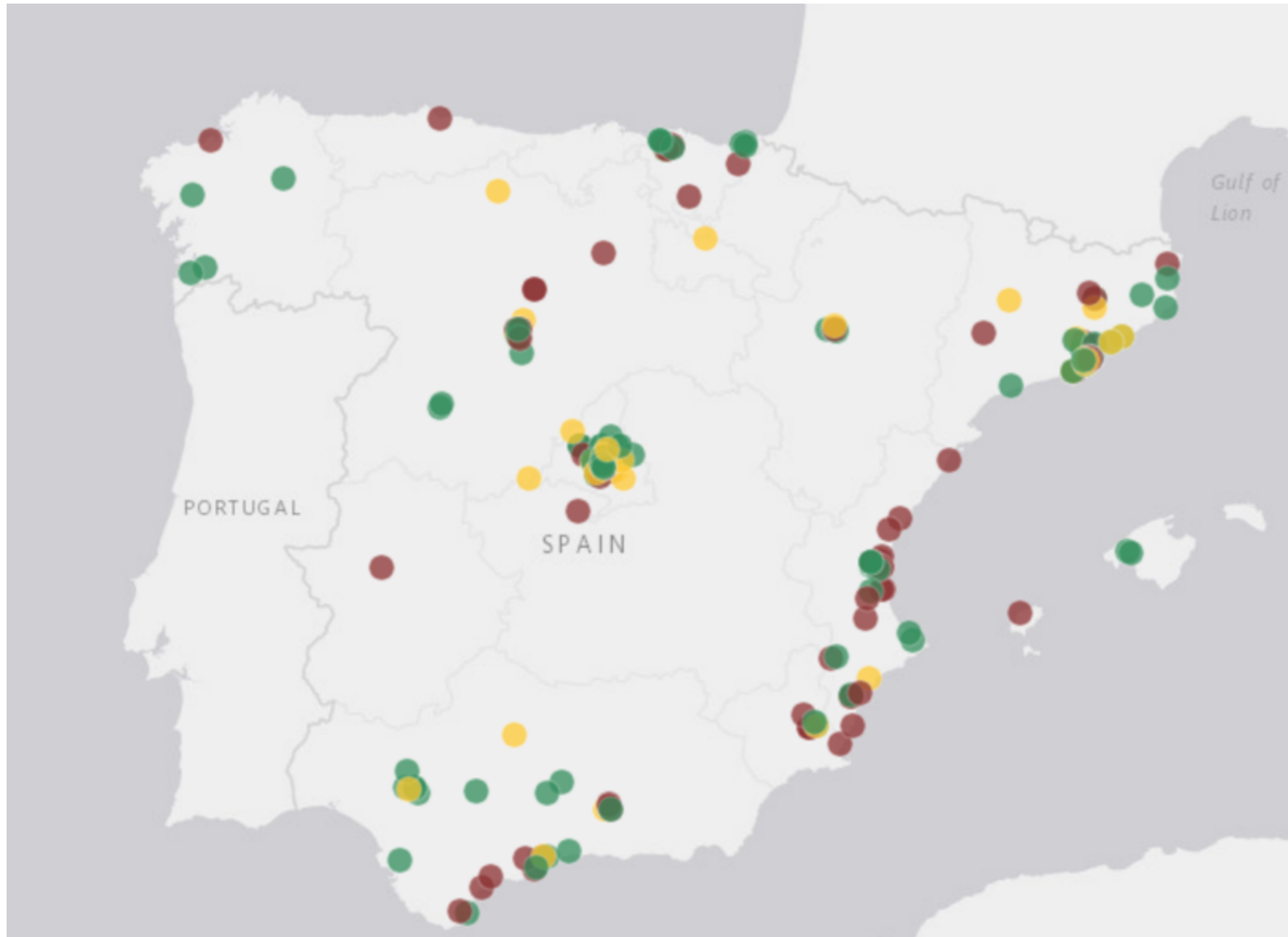
RIPE Atlas - atlas.ripe.net



- RIPE Atlas is a global active measurements platform
- Probes hosted by volunteers
- Data publicly available

"RIPE Atlas: A Global Internet Measurement Network" (PDF). Internet Protocol Journal 18. September 2015. ISSN 1944-1134.

Zoom in to Spain



RIPE Atlas Numbers



- 9,400 RIPE Atlas probes connected worldwide
- 4,100 Measurements collected per second
- 35,000 user-defined measurements per week

RIPE Atlas Measurements



- **Built-in** Global measurements towards root name servers
 - Visualised as Internet traffic maps
- **Built-in** Regional measurements towards RIPE Atlas anchors
- **Users** can run customised measurements
 - ping, traceroute, DNS, SSL/TLS, NTP and HTTP (only towards RIPE Atlas anchors)



Some Features

Most Popular Features



- Powerful and informative visualisations
- APIs to start measurements and get results
- Command line interface
- Streaming data for real-time results
- “Time Travel”

Monitoring using RIPE Atlas



- Integrate “status checks” with existing monitoring tools (such as Icinga, Nagios)
- Using real-time data streaming
 - Server monitoring
 - Detecting and visualising outages
- Developed by community: “RIPE Atlas Monitor”

Time Travel



- Allows you to look at historical data
- For Internet maps and measurement results

*⁶ Anchoring Measurement: Ping IPv6 for anchor cz-prg-as6881.anchors.atlas.ripe.net

General Information **Probes** Map Seismograph Latencymon (beta) Results Modification Log **Time Travel** ←

Time Travel

Choose your time destination with the slider, or type it explicitly into the box.

Probe	ASN (v4)	ASN (v6)		Time	RTT
1285	3243	3243		2015-9-22 8:35	69.320
2131	1955			2015-9-22 8:35	✗ Unreachable
6001	3333	3333		2015-9-22 8:36	19.540
6002	39029	39029		2015-9-22 8:37	33.486
6003	29432	29432		2015-9-22 8:35	116.361
6004	2486	2486		2015-9-22 8:35	17.466
6005	34288	34288		2015-9-22 8:37	15.982

Use Cases on RIPE Labs



- Measuring Internet Access Disruptions
 - <https://labs.ripe.net/Members/emileaben/internet-access-disruption-in-turkey>
 - <https://labs.ripe.net/Members/emileaben/internet-access-disruption-in-the-gambia-2016>
- Measuring DNS Censorship and Hijacking
 - https://labs.ripe.net/Members/babak_farrokhi/operator-level-dns-redirection
 - https://labs.ripe.net/Members/stephane_bortzmeyer/dns-censorship-dns-lies-seen-by-atlas-probes

Use Cases on RIPE Labs



- Monitoring connectivity and connectivity problems
 - https://labs.ripe.net/Members/annika_wickert/using-ripe-atlas-to-monitor-game-service-connectivity
 - https://labs.ripe.net/Members/jason_read/using-ripe-atlas-to-measure-cloud-connectivity
 - https://labs.ripe.net/Members/stephane_bortzmeyer/using-ripe-atlas-to-debug-network-connectivity-problems



More Information

- <https://atlas.ripe.net/>
- <https://labs.ripe.net/atlas>
- Webinars, Training Courses
- Targeted workshops



RIPE WHOIS Database

RIPE Database



- Public Internet resource and routing registry database
- Answers:
 - Who is using an address block?
 - How can I contact them?
- All 5 RIRs have their own database
 - <http://www.iana.org/whois>

Other Registries



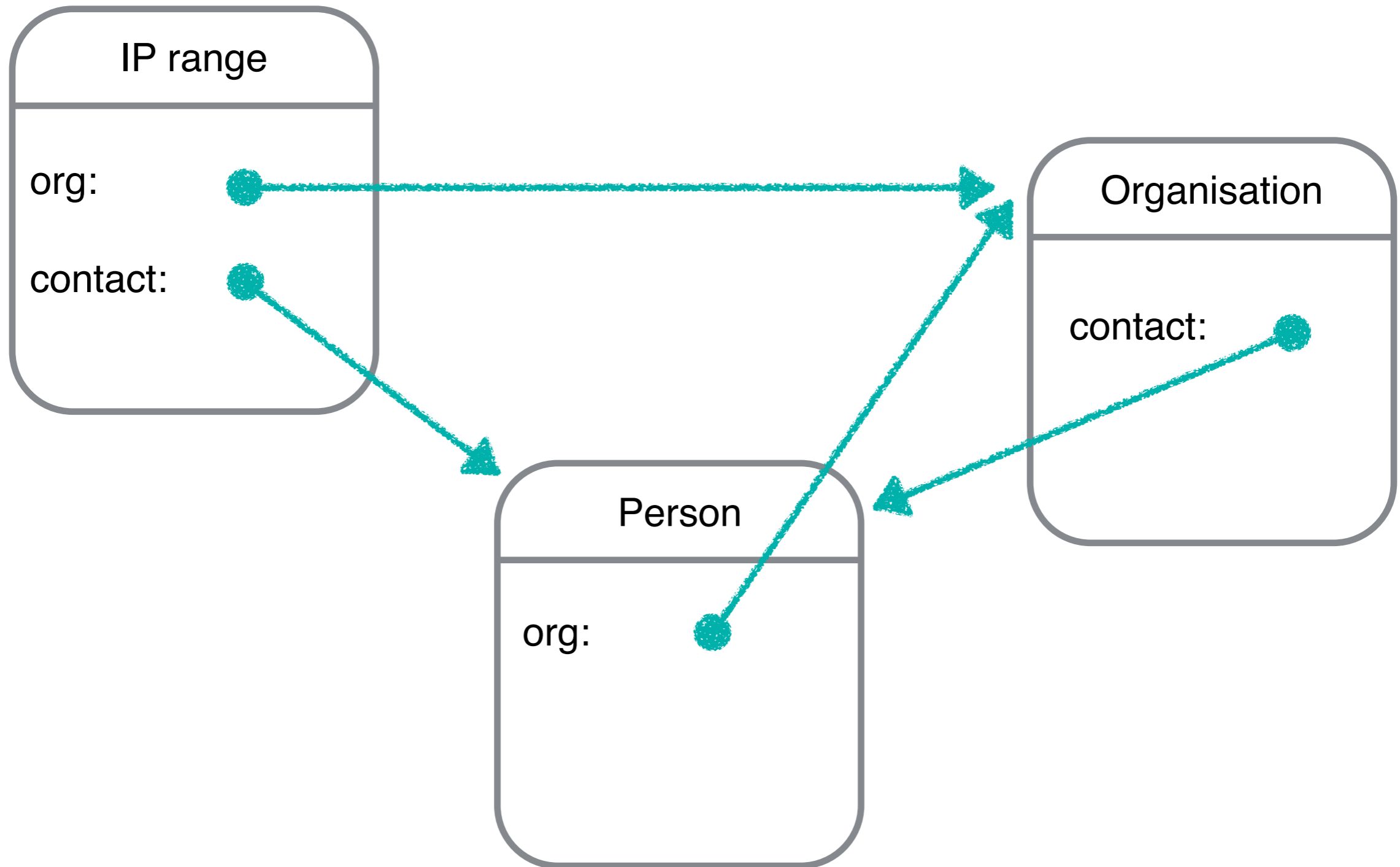
- IANA
 - <http://www.iana.org/numbers>
- Regional Internet Registries
 - <http://whois.arin.net/ui/advanced.jsp>
 - http://www.apnic.net/apnic-info/whois_search
 - <http://www.afrinic.net/en/services/whois-query>
 - <http://lacnic.net/cgi-bin/lacnic/whois?lg=EN>

RIPE Database Objects



- Resources
 - inetnum, inet6num, aut-num
- Contact
 - organisation, person, role
- Routing
 - route, route6
- Reverse DNS
 - domain
- Object protection
 - mntner

Objects Are Related To Each Other



Querying the RIPE Database



- Web interface
- Command line
- Full Text Search
- Restful API (XML/JSON)

193.0.24.1

Show full object details ?
 Do not retrieve related objects ?

You can search up to 5 terms at once in the search box above, separating them with a semicolon.

Sources	Types	Hierarchy Flags	Inverse lookup
<input checked="" type="radio"/> RIPE Database ?			
<input type="radio"/> TEST Database ?			
<input type="radio"/> Global Resource Service (GRS) ?			

By submitting this form you explicitly express your agreement with the [RIPE Database Terms and Conditions](#)

Search

Query Results



Responsible organisation: [Reseaux IP Europeens Network Coordination Centre \(RIPE NCC\)](#)
Abuse contact info: abuse@ripe.net

```
inetnum:          193.0.24.0 - 193.0.30.255 ←
netname:          RIPENCC-MEETING-PUBLIC
descr:           Reseaux IP Europeens Network Coordination Centre (RIPE NCC)
remarks:         RIPE NCC Training Services & RIPE Meetings
remarks:         This space is used as public space during RIPE meetings
country:         NL
admin-c:         JDR-RIPE
admin-c:         BRD-RIPE
tech-c:          OPS4-RIPE
status:          ASSIGNED PA
mnt-by:          RIPE-NCC-MNT
mnt-routes:     RIPE-NCC-MNT
mnt-domains:    RIPE-NCC-MNT
created:         2013-10-09T14:42:14Z
last-modified:  2013-10-09T14:42:14Z
source:         RIPE
```

Options for Queries



Search term

Show full object details ?
 Do not retrieve related objects ?

You can search up to 5 terms at once in the search box above, separating them with a semicolon.

Sources Types Hierarchy Flags Inverse lookup

RIPE Database ?
 TEST Database ?
 Global Resource Service (GRS) ?

By submitting this form you explicitly express your agreement with the [RIPE Database Terms and Conditions](#)

Search

Results With Related Objects



Search term: 193.0.24.1

inetnum: 193.0.24.0 - 193.0.30.255
netname: RIPENCC-MEETING-PUBLIC
descr: RIPE NCC
country: NL
admin-c: JDR-RIPE
admin-c: BRD-RIPE
tech-c: OPS4-RIPE
status: ASSIGNED PA
mnt-by: RIPE-NCC-MNT
created: 2013-10-09T07:58:22Z
last-modified: 2013-10-09T08:34:09Z
source: RIPE

route: 193.0.24.0/21

route: 193.0.24.0/21
descr: RIPE-MEETINGS
origin: AS2121
mnt-by: RIPE-NCC-MNT
created: 2008-04-09T11:04:18Z
last-modified: 2012-04-24T10:09:25Z
source: RIPE

role: RIPE NCC Operations
address: Singel 258
address: person: Brian Riddle
address: IT Manager
phone: address: RIPE NCC - Operations

person: Jochem de Ruig
address: RIPE NCC
address: Singel 258
address: 1016AB Amsterdam
address: The Netherlands
phone: +31 20 535 4444
fax-no: +31 20 535 4445
nic-hdl: JDR-RIPE
mnt-by: RIPE-NCC-MNT
created: 2011-02-10T12:04:37Z
last-modified: 2011-02-10T12:04:37Z
source: RIPE

source: RIPE

Results Without Related Objects



Search term:

inetnum: 193.0.24.0 - 193.0.30.255
netname: RIPENCC-MEETING-PUBLIC
descr: RIPE NCC
country: NL
admin-c: JDR-RIPE
admin-c: BRD-RIPE
tech-c: OPS4-RIPE
status: ASSIGNED PA
mnt-by: RIPE-NCC-MNT
created: 2013-10-09T07:58:22Z
last-modified: 2013-10-09T08:34:09Z
source: RIPE

route: 193.0.24.0/21
descr: RIPE-STOCKHOLM
origin: AS201965
mnt-by: RIPE-NCC-MNT
created: 2015-04-20T12:17:39Z

route: 193.0.24.0/21
descr: RIPE-MEETINGS
origin: AS2121
mnt-by: RIPE-NCC-MNT
created: 2008-04-09T11:04:18Z
last-modified: 2012-04-24T10:09:25Z
source: RIPE

Navigating the Hierarchy

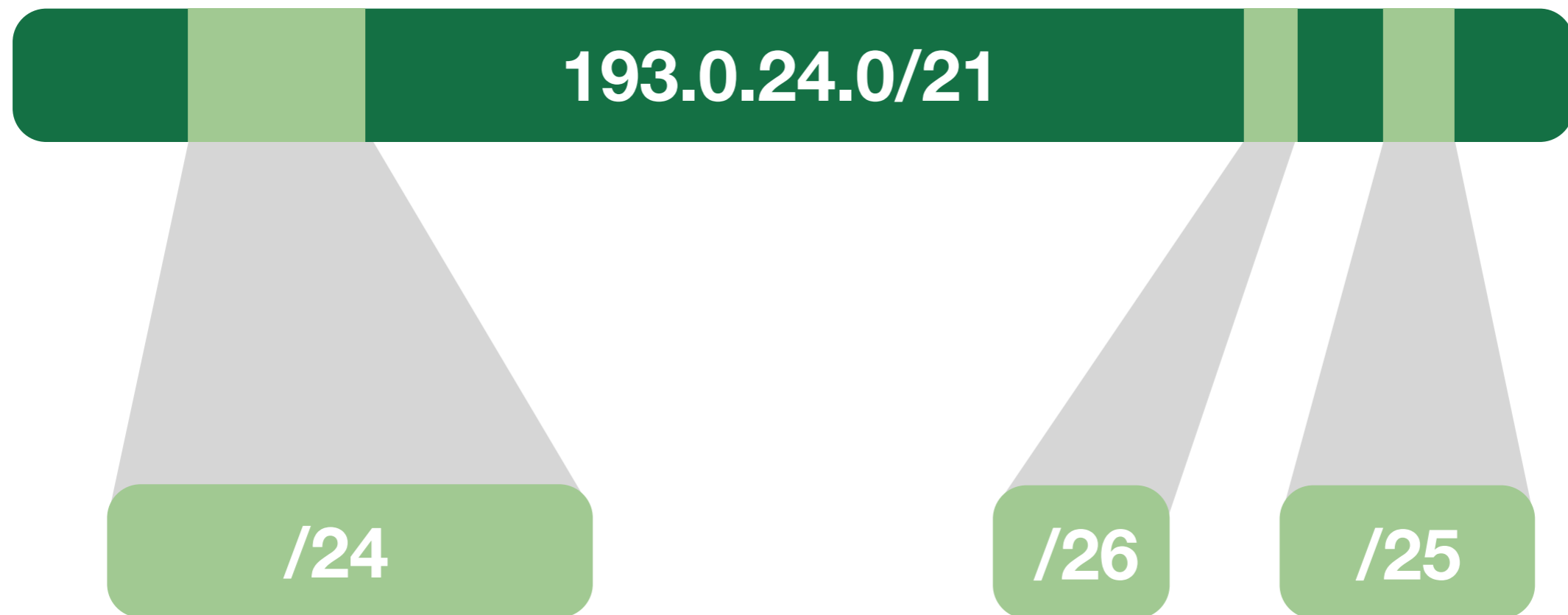


- With IP space, you want to find what is under or above the inetnum object
 - Under = More Specific
 - Above = Less Specific
- There are flags: -m, -M, -I, -L
- Also in the “Hierarchy Flags” tab

More Specific inetnums: -m



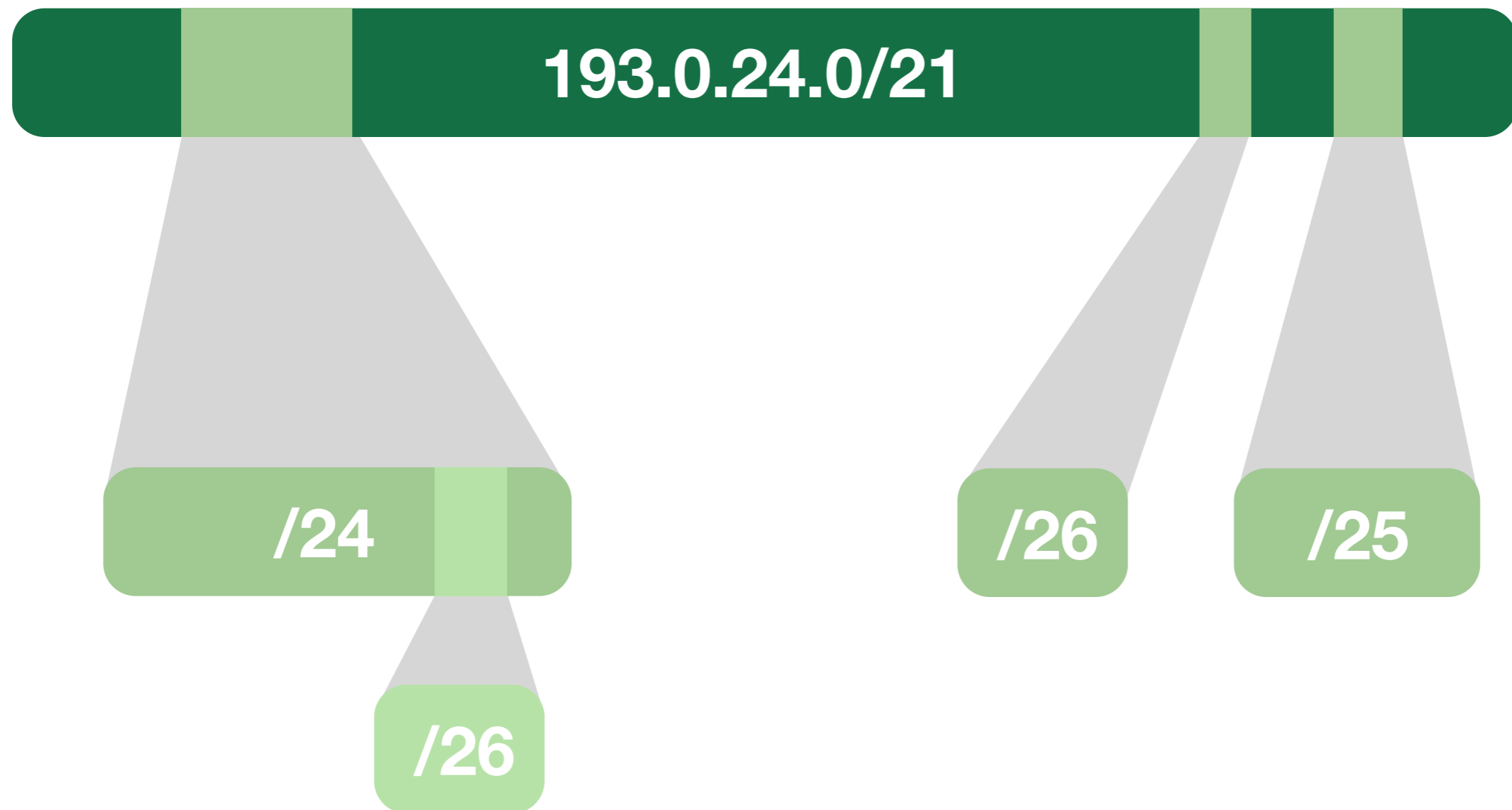
-m 193.0.24.0/21



More Specific inetnums: -M



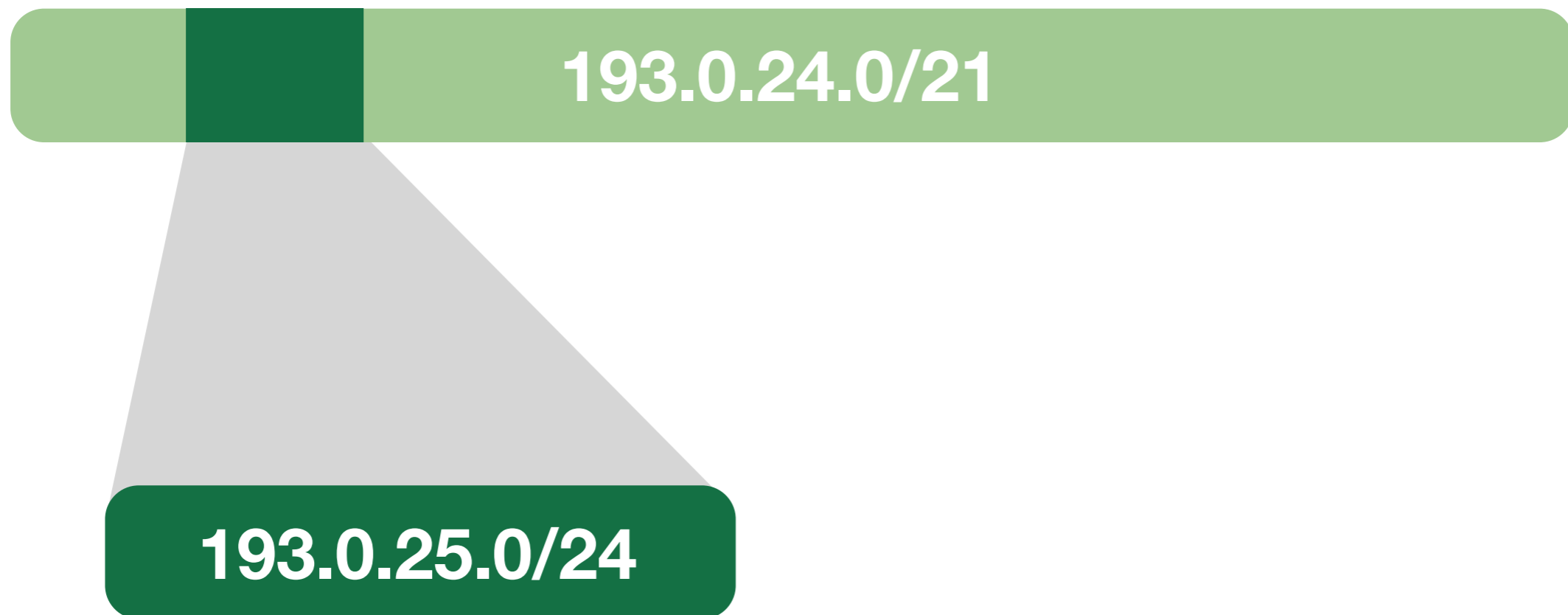
-M 193.0.24.0/21



Less Specific inetnums: -I



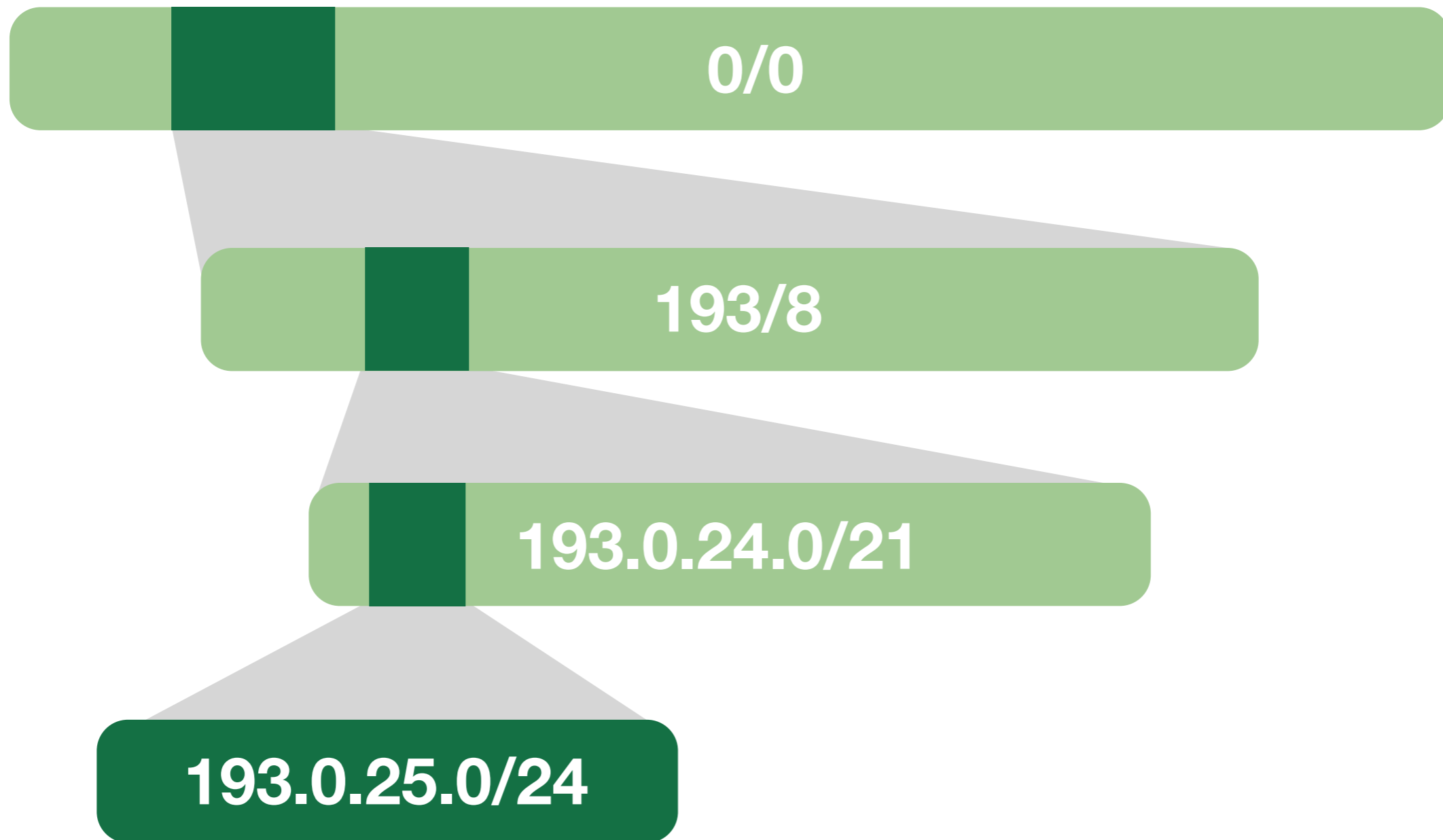
-I 193.0.25.0/24



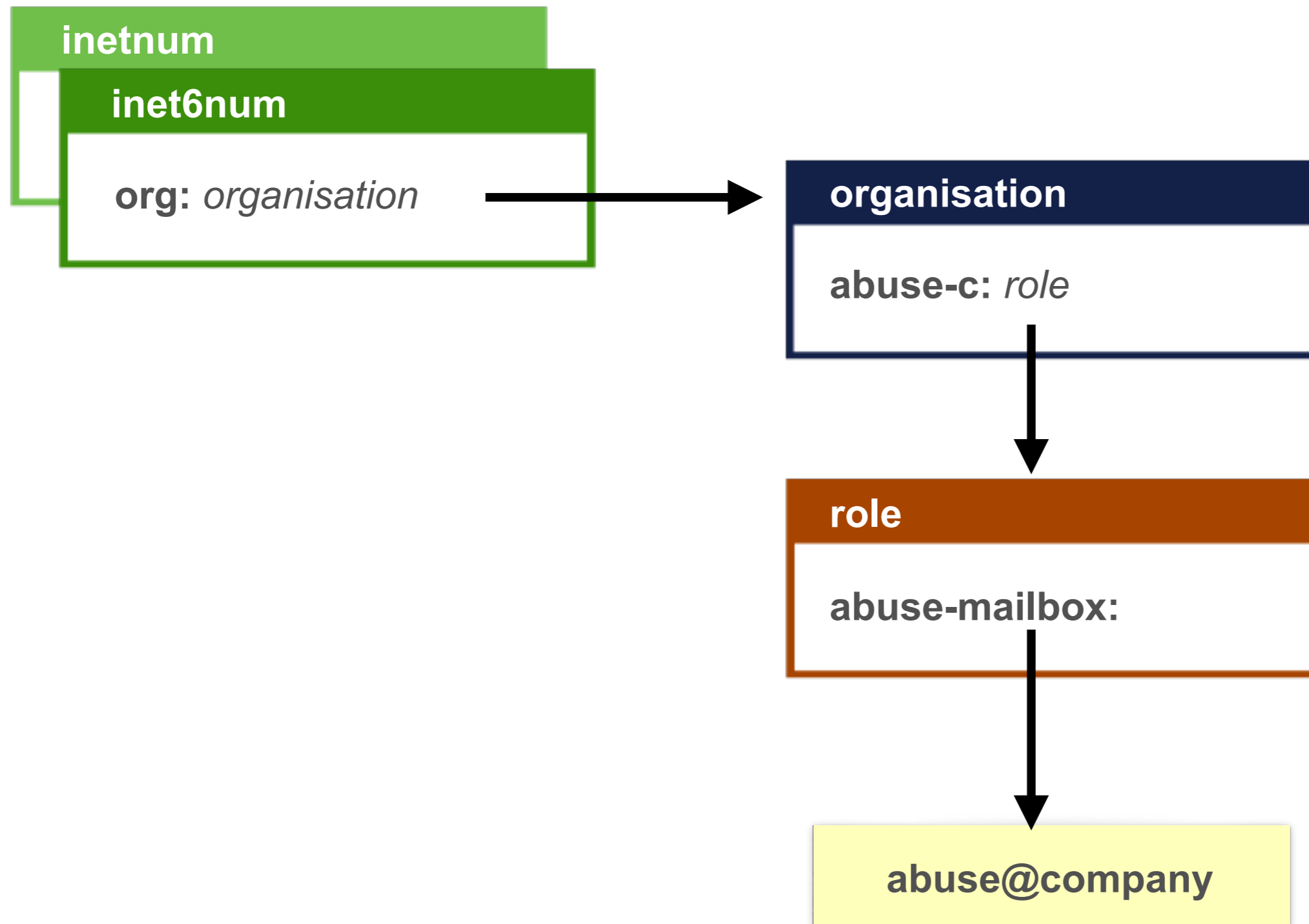
Less Specific inetnums: -L



-L 193.0.25.0/24



Where is the abuse-c?



Inverse Lookup



JD-RIPE

Show full object details ?

Do not retrieve related objects ?

You can search up to 5 terms at once in the search box above, separating them with a semicolon.

Sources	Types	Hierarchy Flags	Inverse lookup
?			
<input type="checkbox"/> abuse-mailbox	<input type="checkbox"/> member-of	<input type="checkbox"/> nserver	
<input type="checkbox"/> admin-c	<input type="checkbox"/> mnt-by	<input type="checkbox"/> org	
<input type="checkbox"/> auth	<input type="checkbox"/> mnt-domains	<input type="checkbox"/> origin	
<input type="checkbox"/> author	<input type="checkbox"/> mnt-irt	<input checked="" type="checkbox"/> person	
<input type="checkbox"/> fingerpr	<input type="checkbox"/> mnt-lower	<input type="checkbox"/> ping-hdl	
<input type="checkbox"/> form	<input type="checkbox"/> mnt-nfy	<input type="checkbox"/> referral-by	
<input type="checkbox"/> irt-nfy	<input type="checkbox"/> mnt-ref	<input type="checkbox"/> ref-nfy	
<input type="checkbox"/> local-as	<input type="checkbox"/> mnt-routes	<input type="checkbox"/> tech-c	
<input type="checkbox"/> mbrs-by-ref	<input type="checkbox"/> notify	<input type="checkbox"/> upd-to	
		<input type="checkbox"/> zone-c	

By submitting this form you explicitly express your agreement with the [RIPE Database Terms and Conditions](#)

Search

Referenced person object



inet6num: 2001:db8::/32
descr: my IPv6 range
mnt-by: RIPE-NCC-HM-MNT
org: ORG-BB2-RIPE
admin-c: JE777-RIPE
tech-c: **JD1-RIPE**

aut-num: AS64551
descr: my AS number
mnt-by: RIPE-NCC-HM-MNT
org: ORG-BB2-RIPE
tech-c: **JD1-RIPE**
tech-c: LA789-RIPE

mntner: LIR-MNT
admin-c: **JD1-RIPE**
tech-c: LA789-RIPE
mnt-by: LIR-MNT

role: Bluelight Staff
nic-hdl: BLS77-RIPE
admin-c: **JD1-RIPE**
address: Sesame Street 1
e-mail: staff@example.org

-i person JD1-RIPE

person: John Smith
nic-hdl: JD1-RIPE
address: Sesame Street 1
phone: +1 555 0101
e-mail: john@example.org
mnt-by: LIR-MNT

Referenced person object



inet6num: 2001:db8::/32
descr: my IPv6 range
mnt-by: RIPE-NCC-HM-MNT
org: ORG-BB2-RIPE
admin-c: JE777-RIPE
tech-c: JD1-RIPE

aut-num: AS64551
descr: my AS number
mnt-by: RIPE-NCC-HM-MNT
org: ORG-BB2-RIPE
admin-c: **JD1-RIPE**
tech-c: LA789-RIPE

mntner: LIR-MNT
admin-c: **JD1-RIPE**
tech-c: LA789-RIPE
mnt-by: LIR-MNT

role: Bluelight Staff
nic-hdl: BLS77-RIPE
admin-c: **JD1-RIPE**
address: Sesame Street 1
e-mail: staff@example.org

-i admin-c JD1-RIPE

person: John Smith
nic-hdl: JD1-RIPE
address: Sesame Street 1
phone: +1 555 0101
e-mail: john@example.org
mnt-by: LIR-MNT

Referenced Organisation



inet6num: 2001:db8::/32
descr: My IPv6 range
org: **ORG-BB2-RIPE**
admin-c: JE777-RIPE
tech-c: JD1-RIPE

inetnum: 85.23.16.0/21
descr: My v4 allocation
org: **ORG-BB2-RIPE**
admin-c: JE777-RIPE
tech-c: JD1-RIPE

inetnum: 85.111.185.0/21
descr: Other v4 allocation
org: **ORG-BB2-RIPE**
admin-c: JE777-RIPE
tech-c: JD1-RIPE

aut-num: AS64551
descr: my AS number
org: **ORG-BB2-RIPE**
admin-c: JE777-RIPE
tech-c: JD1-RIPE

-i org **ORG-BB2-RIPE**

organisation: **ORG-BB2-RIPE**
admin-c: JD1-RIPE
tech-c: LA789-RIPE
abuse-c: **AR789-RIPE**
mnt-by: LIR-MNT

Full Text Search



RIPE Database text search

This service allows searches over the full text of the RIPE Database object data.

The search is done on object text without regard for any relationships. Multiple search terms should be separated with a space.

[Advanced Search](#)

By submitting this form you explicitly express your agreement with the [RIPE Database Terms and Conditions](#)

Search

Search results

This is the RIPE Database full text search service.
The RIPE Database is subject to [Terms and Conditions](#).

[1] 2 3

domain: [205.149.82.in-addr.arpa](#)
descr=Reverse delegation for [Bluelight 2nd/24](#)

domain: [210.149.82.in-addr.arpa](#)
descr=Reverse delegation for [Bluelight 2nd/24](#)

domain: [201.156.178.IN-ADDR.ARPA](#)
mnt-by=RO-BLUELIGHT, descr=BLUELIGHT

domain: [200.156.178.IN-ADDR.ARPA](#)
mnt-by=RO-BLUELIGHT, descr=BLUELIGHT

inet6num: [2a01:4f8:201:31ea::/64](#)
netname=BLUE-LIGHT

Full Text Search - Advanced



Search term

+ Basic Search

All
 Any
 Exact Match

Search only within the following objects:

- as-block
- as-set
- aut-num
- domain
- filter-set
- inet-rtr
- inet6num
- inetnum**
- irt
- key-cert
- mntner
- organisation
- peering-set
- person
- poem
- poetic-form
- role
- route
- route-set
- route6
- rtr-set

Search within the following fields: ?

- admin-c
- changed
- country
- created
- descr
- geoloc
- inetnum
- language
- last-modified
- mnt-by
- mnt-domains
- mnt-irt
- mnt-lower
- mnt-routes
- netname
- notify
- org
- remarks
- source
- sponsoring-org
- status
- tech-c

By submitting this form you explicitly express your agreement with the [RIPE Database Terms and Conditions](#)

Search



RIP Estat

Explanation

What is RIPEstat?



- One interface for multiple data sources

<http://stat.ripe.net/>

Search RIPE **stat**

Your network: AS3333, 2001:67c:2e8::/48 e.g.: IPv4 prefix/range, IPv6, ASN



What can you query?

- IPv6 address
- IPv4 address
- ASN
- Hostname
- Country code

RIPEstat:



- **One interface for all IP resources related data**
 - Registry data, routing, reverse DNS, active measurements, 3rd party data (blacklist, geolocation)

Default Results



RIPEstat Home · About RIPEstat · Documentation · Use Cases · Login

You are here: Home > Data & Tools > RIPEstat > AS3333

AS3333

RIPEstat Search

permalink

At a Glance (4)

- Routing (1)
- DNS (1)
- Anti Abuse (1)
- Database (5)
- Geographic (2)
- Activity (2)
- Suggestions (1)

+ MyView

AS Overview (AS3333)

Announced

Holder of this ASN:
RIPE-NCC-AS Reseaux IP
Europeens Network
Coordination Centre (RIPE
NCC),NL

Showing results for AS3333 as of 2014-07-25 08:00:00 UTC

source data embed code permalink info

Registry Browser (AS3333)

Last updated on 2014-05-27 at 11:51:38 UTC.

aut-num: AS3333

as-name	RIPE-NCC-AS
descr	Reseaux IP Europeens Network Coordination Centre (RIPE NCC)
org	ORG-RIEN1-RIPE
admin-c	JDR-RIPE
admin-c	BRD-RIPE
tech-c	OPS4-RIPE
mnt-by	RIPE-NCC-END-MNT
mnt-by	RIPE-NCC-MNT

Showing results for AS3333 as of 2014-07-25 13:32:47 UTC

RIPE NCC members can access historical information by signing in with their LIR's RIPE NCC Access account.

source data embed code permalink info

Geoloc (AS3333)

Map Satellite

Map Data Terms of Use Report a map error

• Geoloc details

Data is based on MaxMind's GeoLite City data set and valid for the stated query time (see below)

Showing results for AS3333 as of 2014-07-25 08:00:00 UTC

source data embed code permalink info

Routing Status (AS3333)

At 2014-07-25 08:00:00 UTC, AS3333 was visible to 100% of 96 IPv4 and 100% of 95 IPv6 RIS full peers.

© First ever seen as origin announcing 193.0.0.0/21, on 2004-01-03 00:00:00 UTC.

Originated IPv4 prefixes: 6
Originated IPv6 prefixes: 1
Observed BGP neighbours: 509
Address space announced (IPv4): 4608 IPs
Address space announced (IPv6): equiv. to 1 /48s

• Advanced Settings

Showing results for AS3333 as of 2014-07-25 08:00:00 UTC

Results exclude routes with very low visibility (less than 3 RIS peers)

source data embed code permalink info

Widgets

More tabs with results

Create a RIPE NCC Access Account



<https://access.ripe.net>

The screenshot shows a web browser window with the URL <https://access.ripe.net>. The page features the RIPE NCC logo and navigation links such as "Manage IPs and ASNs", "Analyse", "Participate", "Get Support", "Publications", and "About Us". A search bar is present with the text "Search the content of this website". The main content area is titled "Sign in using your RIPE NCC Access account" and includes a "Sign in" button and a "Forgot your password?" link. A yellow box highlights a new feature: "New: Two-step verification. Learn more...". The footer contains social media icons and a list of links: Home, Sitemap, Contact us, Service Announcements, Privacy Statement, Cookies, and Copyright Statement.

Registry Browser Widget



- click on another object to refocus query

Registry Browser (109.110.192.0/19)

Reload this widget by entering a resource here

2011-08-04 16:00:28Z to 2012-12-17 14:02:27Z
Last changed on 2011-08-04 at 16:00:28Z.

inetnum: 109.110.192.0/19 [Show more](#)

descr ASTER Sp. z.o.o.
netname PL-ACC-20091113
country PL
org ORG-ACCL1-RIPE
status ALLOCATED PA
mnt-by RIPE-NCC-HM-MNT

↑

↓

route: 109.110.192.0/19 [route] [Show more](#)

route: 109.110.192.0/19 [route] [Show more](#)

organisation: ORG-ACCL1-RIPE [org] [Show more](#)

role: ACC TEAM [admin-c, tech-c] [Show more](#)

mntner: RIPE-NCC-HM-MNT [mnt-by] [Show more](#)

mntner: PL-ASTER-ZG-MNT [mnt-lower, mnt-routes] [Show more](#)

mntner: ACC-MNT [mnt-lower, mnt-routes] [Show more](#)

Registry Browser Widget



- historic information one click away

Registry Browser (109.110.192.0/19)

2016-09-15 16:04:48 UTC to 2017-01-23 13:24:23 UTC
2016-08-09 14:37:07 UTC to 2016-09-15 16:04:47 UTC
2016-06-02 10:41:48 UTC to 2016-08-09 14:37:06 UTC
2016-04-14 08:11:27 UTC to 2016-06-02 10:41:47 UTC
2016-04-11 18:17:08 UTC to 2016-04-14 08:11:26 UTC
2015-08-06 13:02:20 UTC to 2016-04-11 18:17:07 UTC
2012-12-19 12:27:57 UTC to 2015-08-06 13:02:19 UTC
2011-08-04 16:00:28 UTC to 2012-12-19 12:27:56 UTC
2011-04-26 09:26:26 UTC to 2011-08-04 16:00:27 UTC
2011-03-03 13:20:58 UTC to 2011-04-26 09:26:25 UTC
2011-02-28 15:58:55 UTC to 2011-03-03 13:20:57 UTC
2009-11-26 10:43:38 UTC to 2011-02-28 15:58:54 UTC
2009-11-23 13:25:57 UTC to 2009-11-26 10:43:37 UTC

mnt-by MNT-LGI

↑

route: 109.110.192.0/19 [route] Show more

1 × organisation, 1 × role, 3 × mntner

organisation: ORG-UTKS1-RIPE [org] Show more

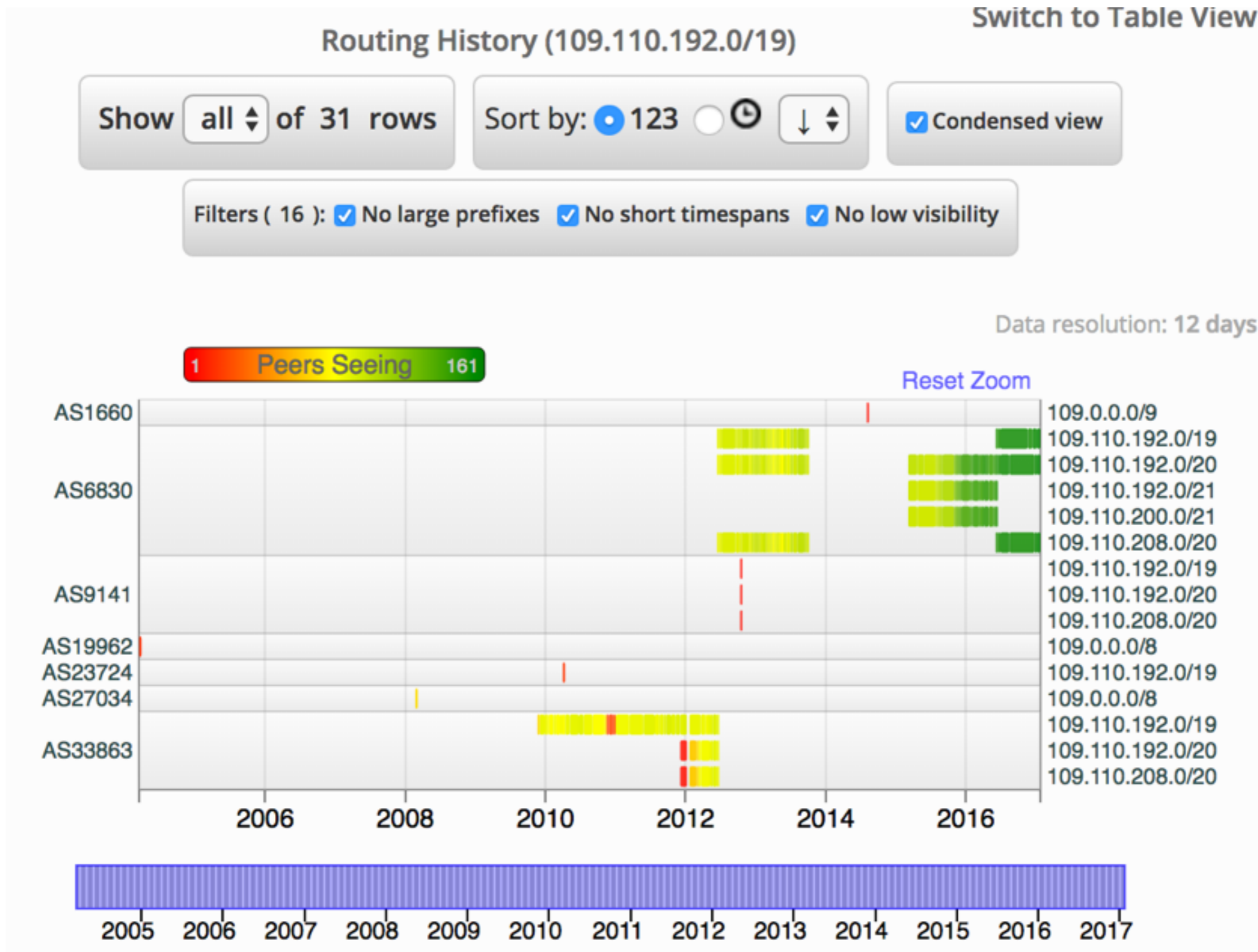
role: UPC Polska [admin-c, tech-c] Show more

mntner: RIPE-NCC-HM-MNT [mnt-by] Show more

mntner: MNT-LGI [mnt-by, mnt-lower] Show more

Showing results for 109.110.192.0/19 as of 2017-01-23 13:24:23 UTC

Routing History Widget



Anti Abuse & Blacklist Entries



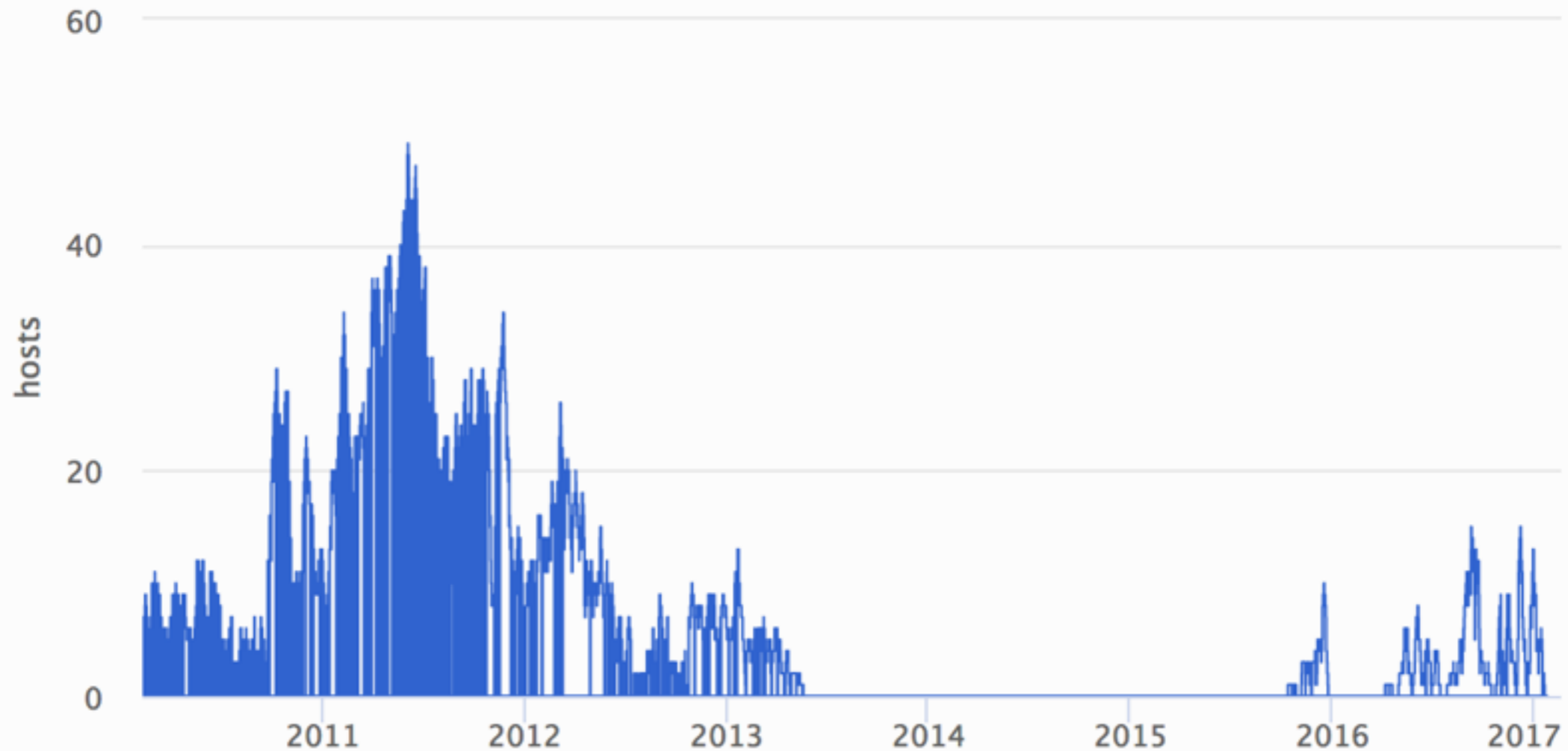
Abuse Contact Finder (109.110.192.0/19)

Email-Contact

abuse@upc.pl

Uce-protect 1 results

Blacklist Entries (109.110.192.0/19)



▼ Blacklist details

RIPE NCC WHOIS client



Source code can be found here:

<ftp://ftp.ripe.net/ripe/tools/dbase/software/ripe-whois-client-3.2.2.tar.gz>

- Only to be used with RIPE WHOIS DB
- 'whois help' show all options
- --list-versions
- --diff-versions <version-number:version-number>
- --show-version <version-number>

RIPE NCC WHOIS client



--list-versions

```
ivo$ /usr/local/bin/whois --list-versions 193.0.0.0/21
```

```
1      2003-03-17 13:15  ADD/UPD
2      2003-04-12 08:32  ADD/UPD
3      2003-05-22 13:20  ADD/UPD
4      2004-10-22 14:43  ADD/UPD
5      2004-10-31 03:08  ADD/UPD
```


RIPE NCC WHOIS client



--show-version

```
ivo$ /usr/local/bin/whois --show-version 2 193.0.0.0/21
```

```
inetnum:      193.0.0.0 - 193.0.7.255
netname:      RIPE-NCC
descr:        RIPE Network Coordination Centre
descr:        Amsterdam, Netherlands
remarks:      Used for RIPE NCC infrastructure.
country:      NL
admin-c:      AMR68-RIPE
tech-c:       OPS4-RIPE
status:       ASSIGNED PI
mnt-by:       RIPE-NCC-MNT
mnt-lower:    RIPE-NCC-MNT
source:       RIPE # Filtered
```

RIPE NCC WHOIS client



--diff-versions

```
ivo$ /usr/local/bin/whois --diff-versions 2:3 193.0.0.0/21
```

```
% Difference between version 2 and 3 of object "193.0.0.0 -  
193.0.7.255"
```

```
@@ -7,2 +7,3 @@
```

```
admin-c:          AMR68-RIPE  
+admin-c:         RDK-RIPE  
tech-c:          OPS4-RIPE
```



Questions

