

# Getting the Most From RIPEstat

---

Workshop at RIPE 67, Athens, October 2013

Vesna Manojlovic and Christopher Amin



# Topics and Prerequisites

---

- Prerequisites:
  - Laptop and web browser
  - No programming skills needed
- Topics:
  - Searching via web interface
  - Comparing resources
  - Finding “anti-abuse” contact
  - Playing with BGPlay

# RIPEstat Introduction

---

- [stat.ripe.net](http://stat.ripe.net) is a “one-stop shop” for all information about Internet number resources
  - RIPE NCC: registration data and whois, routing (RIS), reverse DNS, RIPE Atlas measurements
  - External sources: IRR, RIR stats, geolocation, blacklists, M-Labs network activity
- Web-based, with additional interfaces:
  - Widgets, data API, text service, mobile app
- Search by: IPv4, IPv6 and ASN; hostname, country

# RIPEstat Web Interface

- Finding information using RIPEstat

The screenshot displays the RIPEstat web interface. At the top, a navigation bar includes links for Home, About RIPEstat, Documentation, Use Cases, and Logout. Below this, a breadcrumb trail shows the current location: Home > Data & Tools > RIPEstat. A prominent yellow search bar is labeled "Search RIPEstat" and contains a "Search input" callout. Below the search bar, a text field shows "Your network: AS3333, 2001:67c:2e8::/48" with an example "e.g.: IPv4 prefix/range, IPv6, ASN".

A callout labeled "Recent new features" points to a section titled "BGPlay is back!" which displays a network diagram and statistics such as "Number of ASes: 87", "Selected collector peers: 62", and "Total number of events: 95".

On the right side, a "System Statistics" section shows a "Query rate on RIPEstat" of "29.3 k". Below this is a "Quick Links" section with links to "Looking For Abuse Information", "FAQ", "Feedback", "Documentation", "Mobile Version", and "Widget List". A callout labeled "Links to most used features" points to this section.

At the bottom, there are three main content areas: "About RIPEstat" (with links to FAQ, Data Sources, Widget List, Top Queries, and Feedback), "Documentation" (with links to Interfaces & APIs, Demos, Roadmap, and Changelog), and "Use Cases" (with links to Notable Network Events, Compare Results, Looking for Abuse Information, and Global Internet Statistics). Each of these sections has a "LEARN MORE" link.

On the far right, an "On RIPE Labs" section lists recent articles: "Improved Routing Information Available via RIPEstat" (Aug 23, 2013), "Future of RIPE NCC Technical Services" (Aug 20, 2013), and "New in RIPEstat: In-widget Comparison and Monitoring" (Jul 24, 2013). A callout labeled "RIPEstat-related articles on RIPE Labs" points to this section.

# Web Interface Query: Results Page



# Tasks: Querying for a Resource Using a Web Interface

---

- Group Alpha:
  - What network announces 140.78.50.90?
  - Is 192.3.4.5 routed?
  - In which country is 91.229.42.0/23 used?
- Group Beta:
  - Query conference IP range
  - Which widget provides real-time routing status?
  - How many prefixes did Greece announce in January 2013?

- Time: 2 minutes
- Evaluation: 3 minutes

# Comparing Results

- Compare results in different widgets

The screenshot shows the RIPEstat website's 'Compare Results' interface. At the top, a yellow navigation bar contains links: 'RIPEstat Home', 'About RIPEstat', 'Documentation', 'Use Cases', and 'Login'. A blue arrow points from a callout bubble to the 'Use Cases' link. Below the navigation bar, a breadcrumb trail reads 'You are here: Home > Data & Tools > RIPEstat > Use Cases > Data Comparator'. The main heading 'Compare Results' is in red. Below it, a text instruction says 'Select up to six different widgets from the list to compare at one time. Different resources can be queried for each widget.' A large grey box contains a 'Select a widget' dropdown menu, with a blue arrow pointing from a callout bubble to it. Below the dropdown are two buttons: '+ Add' and 'Permalink'.

Go to "Use Cases" > "Compare Results"

Select a widget

RIPEstat Home • About RIPEstat • Documentation • Use Cases • Login

You are here: Home > Data & Tools > RIPEstat > Use Cases > Data Comparator

**Compare Results**

Select up to six different widgets from the list to compare at one time. Different resources can be queried for each widget.

Select a widget

+ Add Permalink



# Comparing Resources Between Widgets

**Compare Results**

Select up to six different widgets from the list to compare at one time. Different resources can be compared.

Select a widget:

and a resource:

Enter a resource

**Prefix Size Distribution (1205)**

by number of  
☒ Prefixes ☐ Addresses

IPv4

**AS Overview (1205)**

**JKU-LINZ-AS - University Linz**

This ASN is part of 1-65535, the 16-bit ASN Block. This block contains all 16-bit ASNs, which are allocated to the RIRs according to <http://www.lana.org/assignments/as-numbers/as-numbers.xml>. See RFC 1930 ⓘ

Showing results from 2013-08-30 00:00:00 UTC to 2013-08-30 08:00:00 UTC

- Select the “Prefix Size Distribution” widget
- Enter “AS1205”



# Comparing Resources Within One Widget



# Tasks: Compare Resources

---

- Group Alpha:
  - Compare the number of announced prefixes for two ASNs over the past two years using the widget comparison page
- Group Beta:
  - How does the Internet in Greece compare to another country?
  - Use in-widget comparison!

- Time: 2 minutes
- Evaluation: 3 minutes

# Finding Abuse Contacts and Reporting Abuse

## Take action in an abuse case with the Abuse Contact Finder

The screenshot shows the RIPEstat Abuse Contact Finder interface. At the top, a navigation bar includes links for RIPEstat Home, About RIPEstat, Documentation, and Use Cases. A callout bubble points to the 'Use Cases' link, stating: "Go to 'Use Cases' > 'Looking For Abuse Information'". Below the navigation bar, a breadcrumb trail reads: "You are here: Home > Data & Tools > RIPEstat > Use Cases > Looking For Abuse Information". The main heading is "RIPEstat Abuse Contact Finder". Below this, a paragraph states: "The RIPEstat Abuse Contact Finder may be able to help you find the email address that should be used to report network abuse originating from a particular IP address." Two informational boxes follow: the first says "You can learn more about network abuse in general and what you can do to stop it on the RIPE NCC's Abuse Information page." and the second says "You can learn more about how the RIPEstat Abuse Contact Finder works and how to report abuse in this tutorial on RIPE Labs." The main form area is titled "Abuse Contact Finder BETA" and features a text input field labeled "Enter an IP address". A callout bubble points to this field, stating: "Enter the IP address". Below the input field are links for "embed code", "permalink", and "info". A final note at the bottom states: "For regular RIPEstat users: this widget, of course, can also be found on the regular result page in the 'Anti Abuse' tab."

RIPEstat Home • About RIPEstat • Documentation • Use Cases

Go to "Use Cases" > "Looking For Abuse Information"

You are here: Home > Data & Tools > RIPEstat > Use Cases > Looking For Abuse Information

**RIPEstat Abuse Contact Finder**

The RIPEstat Abuse Contact Finder may be able to help you find the email address that should be used to report network abuse originating from a particular IP address.

You can learn more about network abuse in general and what you can do to stop it on the RIPE NCC's Abuse Information page.

You can learn more about how the RIPEstat Abuse Contact Finder works and how to report abuse in this tutorial on RIPE Labs.

**RIPEstat Abuse Contact Finder BETA**

Enter an IP address

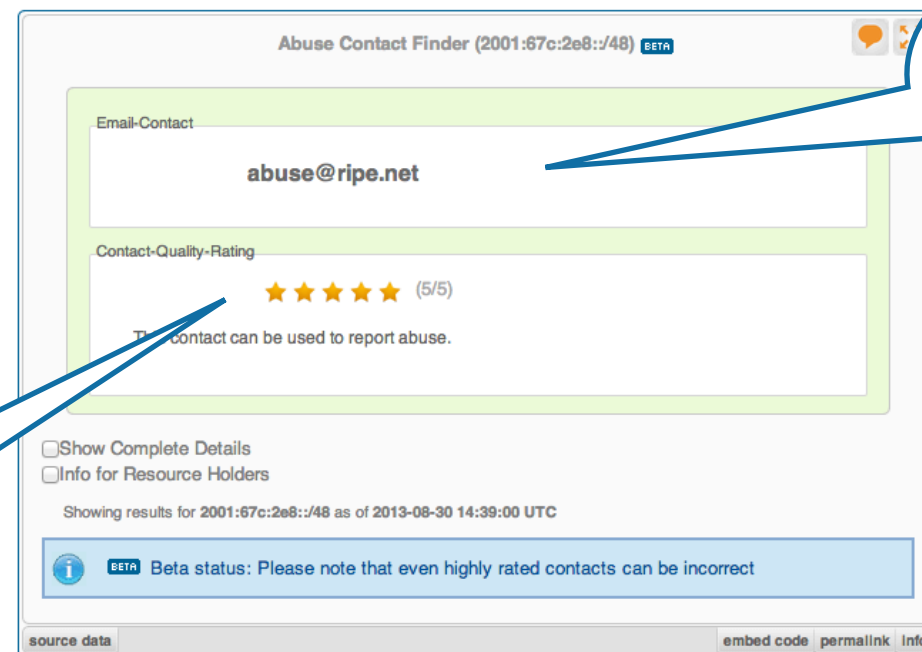
embed code permalink info

For regular RIPEstat users: this widget, of course, can also be found on the regular result page in the "Anti Abuse" tab.

In-depth information about abuse finder

Enter the IP address

# Finding Abuse Contacts

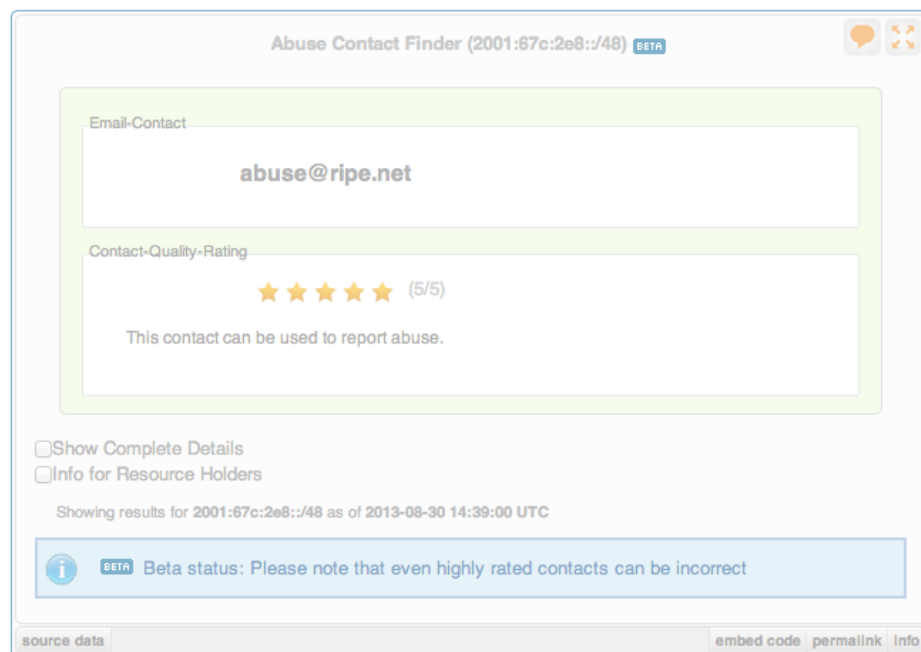


Email address to report abuse to

Rating of the contact

# Finding Abuse Contacts and More Information

Details about the resource and abuse contact:



Abuse Contact Finder (2001:67c:2e8::/48) **BETA**

Email-Contact  
**abuse@ripe.net**

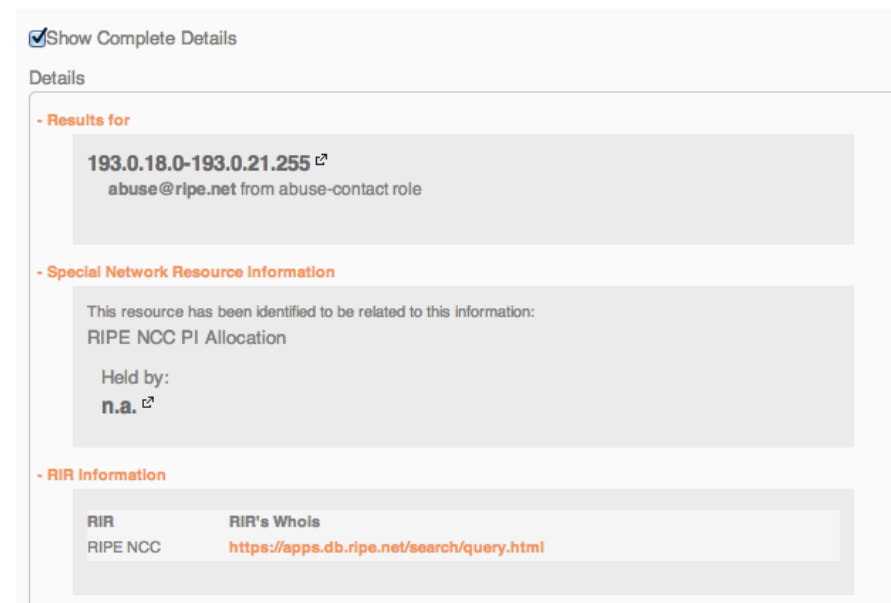
Contact-Quality-Rating  
★★★★★ (5/5)  
This contact can be used to report abuse.

☐ Show Complete Details  
☐ Info for Resource Holders

Showing results for 2001:67c:2e8::/48 as of 2013-08-30 14:39:00 UTC

**BETA** Beta status: Please note that even highly rated contacts can be incorrect

source data embed code permalink info



☒ Show Complete Details

Details

- Results for  
**193.0.18.0-193.0.21.255** [↗](#)  
abuse@ripe.net from abuse-contact role

- Special Network Resource Information  
This resource has been identified to be related to this information:  
RIPE NCC PI Allocation  
Held by:  
**n.a.** [↗](#)

- RIR Information

RIR	RIR's Whois
RIPE NCC	<a href="https://apps.db.ripe.net/search/query.html">https://apps.db.ripe.net/search/query.html</a>

# Tasks: Find Abuse Contacts and Update/Report

---

- Group Alpha:
  - What is the abuse contact for 193.0.20.22 or the hotel network?
- Group Beta:
  - Check an IP address from your home network

- Possible actions:
  - If it is your resource: keep abuse-c info up-to-date
  - If it is not your resource: email the resource holder

- Time: 2 minutes
- Evaluation: 3 minutes

# Let's BGPlay!

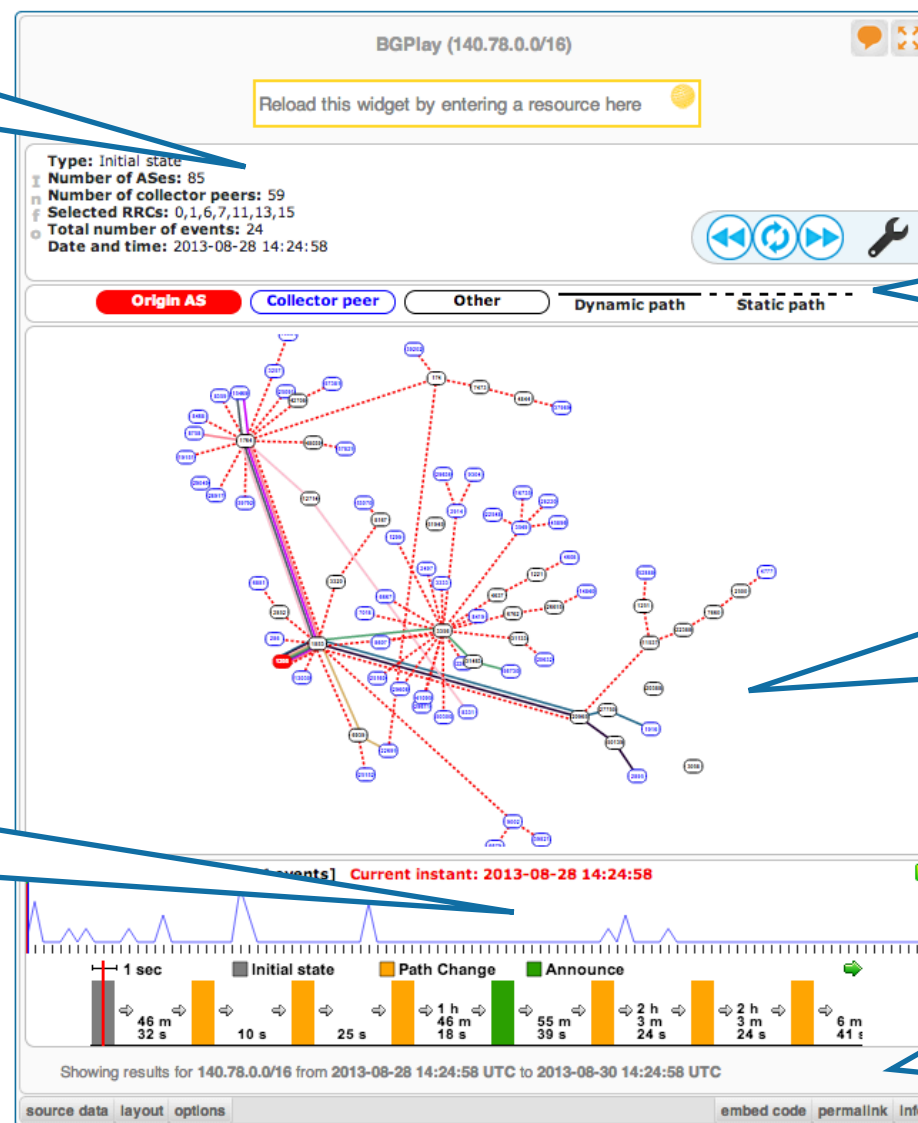
---

- Use BGPlay to see how your network is routed
  - BGPlay is a tool that shows routing history in an animated and highly interactive manner
- Go to: <https://stat.ripe.net/widget/bgplay>



# Let's BGPlay!

BGP event, ASN or  
ASN path details



Control panel:  
- Covered time  
period  
- RRC selection

Interactive graph visualisation

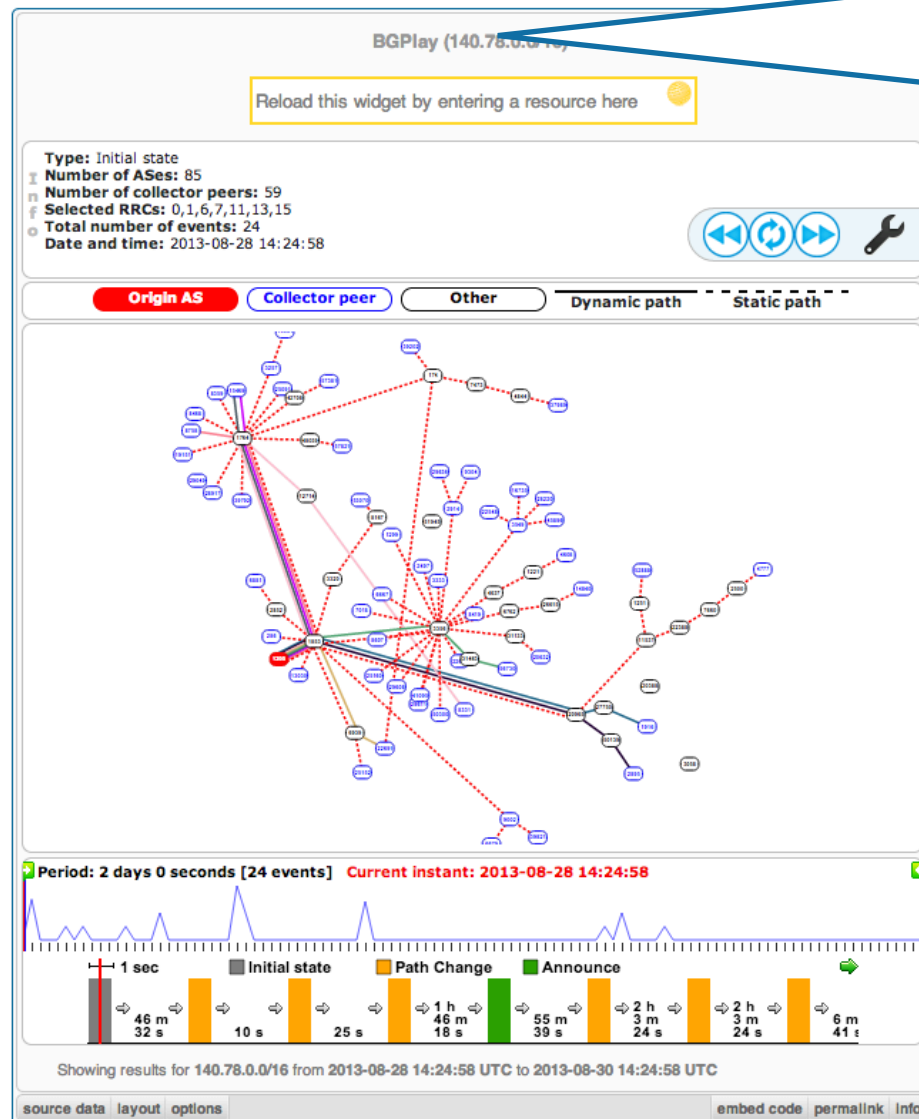
Control timeline

Selection timeline

# Let's BGPlay!

## Examples:

- Prefix with announcements & withdrawals:  
84.205.64.0/24
- Check IPv6 connectivity:  
2001:67c:2e8::/48
- Multi-homed prefix:  
199.7.80.0/24



# Let's BGPlay!

---

## Tasks:

- Find the up-stream provider for AS1205
- Is AS3333 multi-homed?
- Check the IPv6 connectivity of your own network

- Time: 5 minutes
- Evaluation: 10 minutes

# Contact & Information:

- <https://stat.ripe.net>
- Mailing List: **mat-wg@ripe.net**
- Articles & updates on RIPE Labs
  - **<https://labs.ripe.net/ripestat>**
- Questions: **stat@ripe.net**



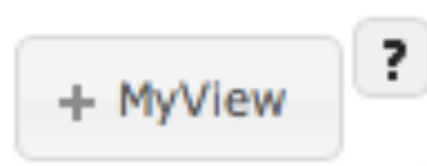
# RIPEstat Advanced Topics

---

1. Creating “My View”
  - Prerequisite: RIPE NCC Access account
2. Looking up the history of your RIPE Database objects
  - Prerequisites: RIPE NCC membership and RIPE NCC Access account
- **Other advanced topics will not be covered!**
  - **Programming skills needed**
  - **Only here for your homework**
- Embedding a widget in your site
- Using RIPEstat Data API

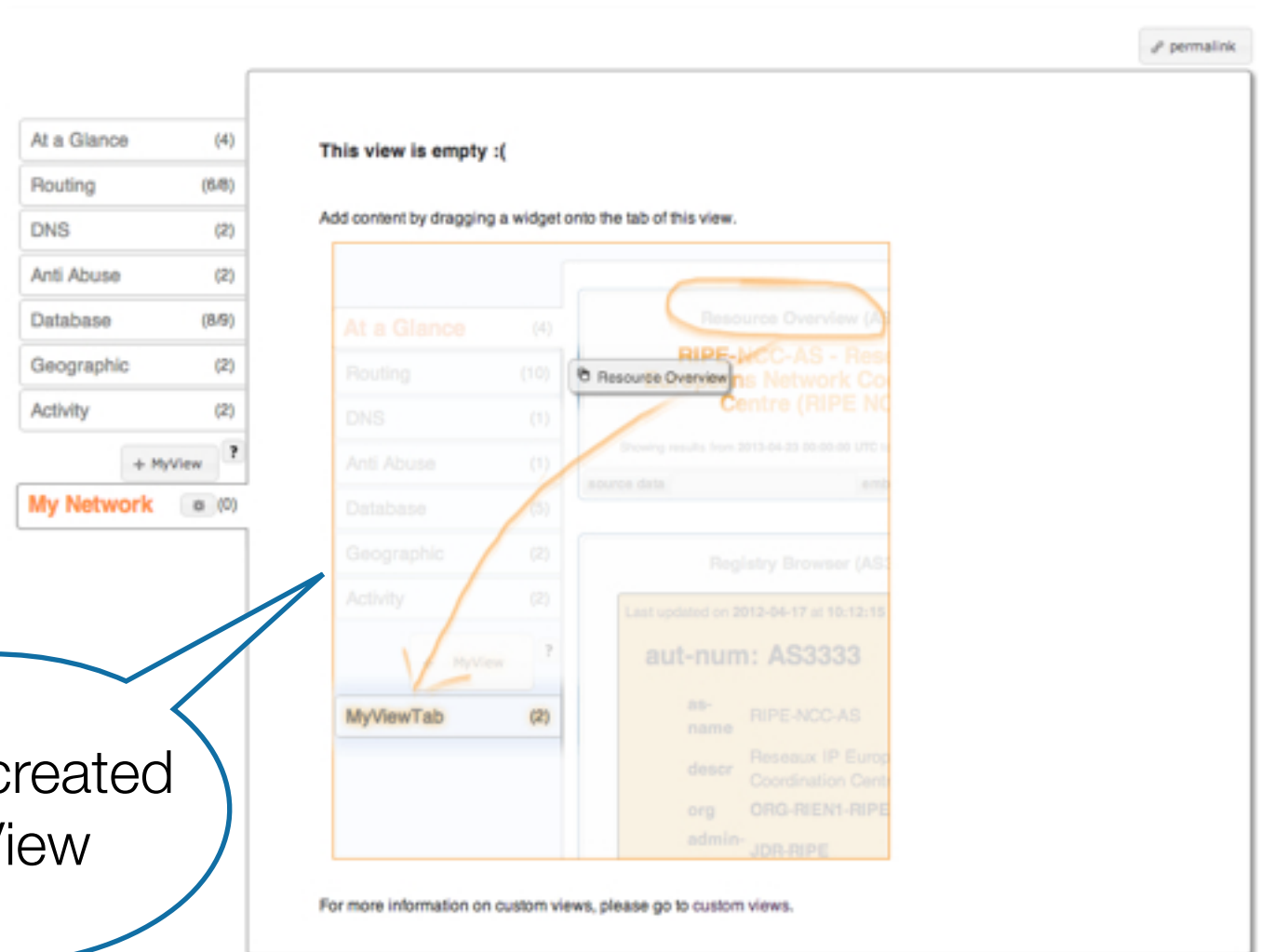
# MyViews: Creating Custom Views

- Click the “MyView” Button



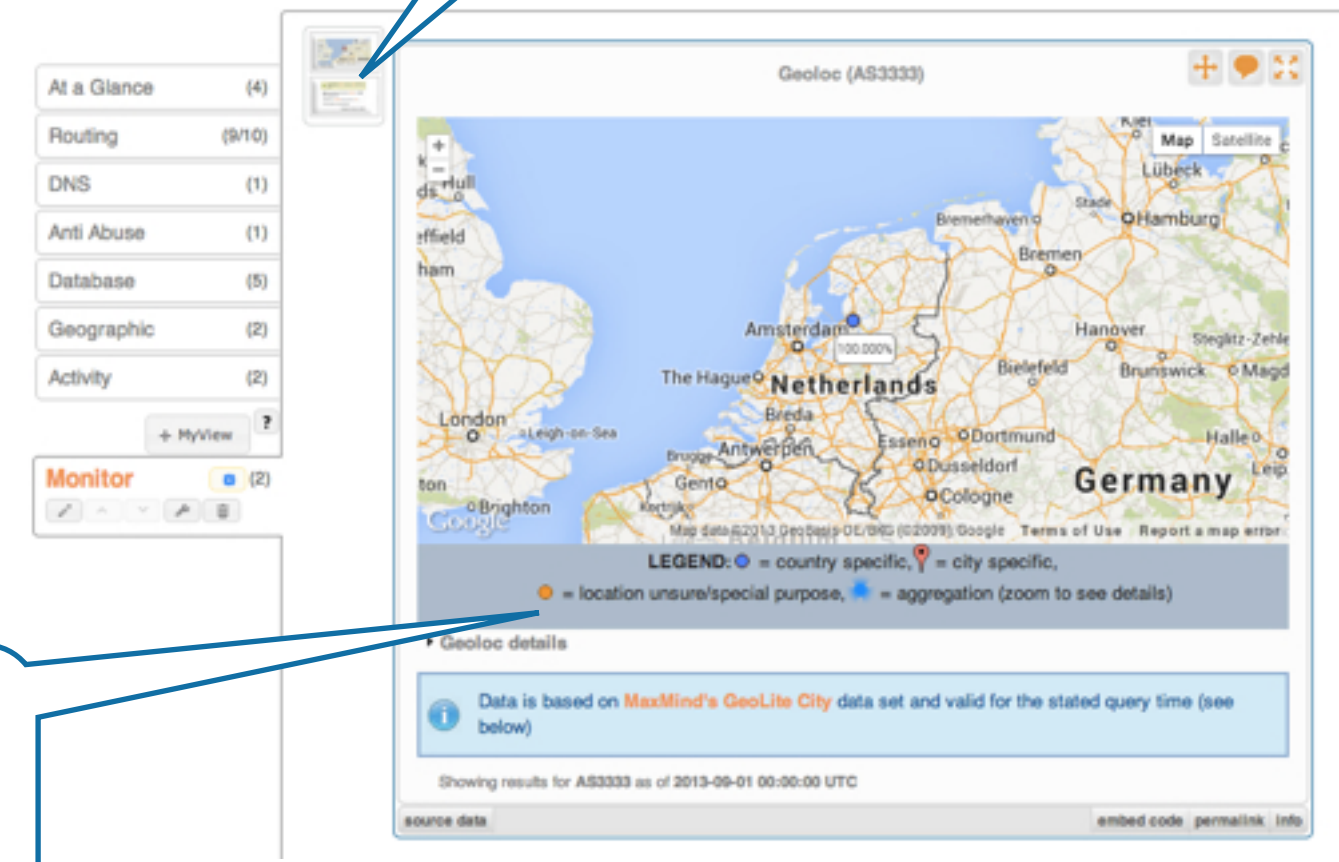
- Drag and drop a widget onto the “MyView” button

Newly created MyView



# Customizing MyViews

Re-order widgets as you like



The screenshot shows the RIPE MyViews interface. On the left is a sidebar with a list of widgets: 'At a Glance (4)', 'Routing (9/10)', 'DNS (1)', 'Anti Abuse (1)', 'Database (5)', 'Geographic (2)', and 'Activity (2)'. Below these is a '+ MyView ?' button and a 'Monitor' section with a blue square icon and '(2)'. The main area displays a map titled 'Geoloc (AS3333)' showing Europe. A blue dot marks a location in the Netherlands. Below the map is a legend: 'LEGEND: ● = country specific, ● = city specific, ● = location unsure/special purpose, ● = aggregation (zoom to see details)'. Below the legend is a 'Geoloc details' section with an information icon and text: 'Data is based on MaxMind's GeoLite City data set and valid for the stated query time (see below)'. At the bottom, it says 'Showing results for AS3333 as of 2013-09-01 00:00:00 UTC'. At the very bottom of the main area are links for 'source data', 'embed code', 'permalink', and 'info'.

- Rename
- Re-order
- Control visibility
- Remove



# Tasks: Creating New “Views”

---

- Create a RIPE NCC Access account (if you don't already have one!)
- Create a MyView for a prefix containing the following widgets:
  - Routing Status
  - Looking Glass
  - Routing History
- Create another MyView with at least two widgets, and give it a meaningful name

# The History of your RIPE Database Objects

- Prerequisite: RIPE NCC membership / LIR
- Tasks:
  - Log in at RIPEstat home page from LIR account
  - Check “Object Browser”
  - Choose any time-frame in the past

2011-02-17T11:11:50 to 2012-09-11T08:33:22

2011-02-17T11:11:50 to 2012-09-11T08:33:22

2010-03-17T14:00:47 to 2011-02-17T11:11:49

2009-12-02T12:27:22 to 2009-12-02T12:49:48

2009-12-02T12:49:49 to 2010-03-17T14:00:47

2006-02-21T15:46:47 to 2009-12-02T12:27:21

2004-10-22T12:43:46 to 2004-10-31T02:08:07

2004-10-31T02:08:10 to 2006-02-21T15:46:47

2003-05-22T11:20:09 to 2004-10-22T12:43:45

2003-04-12T06:32:27 to 2003-05-22T11:20:08

2003-03-17T12:15:57 to 2003-04-12T06:32:26

2003-03-17T11:41:15 to 2003-03-17T12:03:20

2003-03-17T11:40:18 to 2003-03-17T11:41:14

Show all fields

RIPE-NCC-MNT

2003-03-17T12:15:57 to 2003-04-12T06:32:26

About 13 changes since 2003-03-17T11:40:18.

Show all fields

**inetnum: 193.0.0.0/21**

netname RIPE-NCC

descr RIPE Network Coordination Centre

country NL

status ASSIGNED PI

mnt-by RIPE-NCC-MNT

↑

route: 193.0.0.0/21 [route] Show all

↓

person: Daniel Díaz Luengo [admin-c] Show all

role: RIPE NCC Operations [tech-c] Show all

mntner: RIPE-NCC-MNT [mnt-by, mnt-lower] Show all

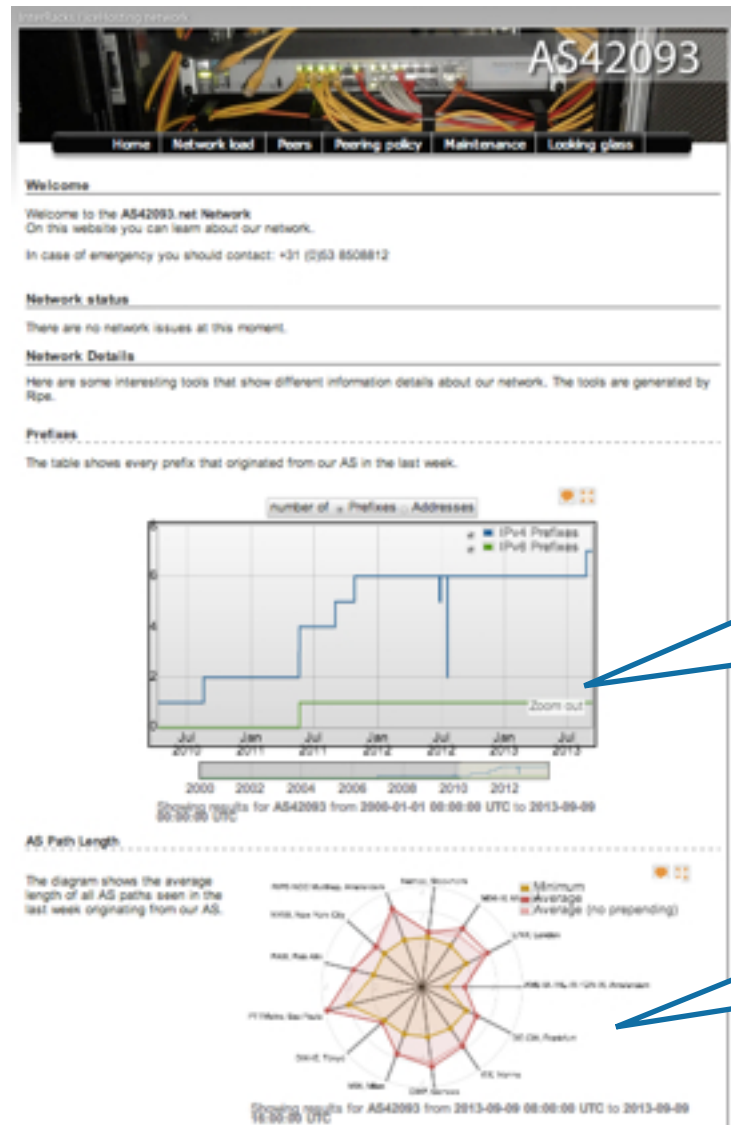
# Embedding Widgets On Your Own Site

---

- What is the concept?
  - Widgets are based purely on web standards and were developed with ‘embedability’ in mind.
  - Every widget available via the RIPEstat web interface can be embedded on your own site.
- RIPEstat Widget API documentation:  
[https://stat.ripe.net/docs/widget\\_api](https://stat.ripe.net/docs/widget_api)

# Embedding Widgets On Your Own Site

This ISP embedded widgets on its page.



# Embedding Widgets On Your Own Site

---

## Tasks:

- Create a simple dashboard page to monitor your network
  - Create a simple HTML page
    - Download the sample page:
      - [https://stat.ripe.net/widgets/demo/widget\\_home.html](https://stat.ripe.net/widgets/demo/widget_home.html)
- Embed three widgets of your choice
- Make the widget smaller and remove the RIPEstat logo

# Using RIPEstat Data API

---

## Using raw data output

- What is the concept?

The RIPEstat Data API provides the lowest level of access to data. This data can be fed into custom applications or just used for scripting.

- RIPEstat Widget API documentation:

[https://stat.ripe.net/docs/data\\_api](https://stat.ripe.net/docs/data_api)

# Use RIPEstat Data API

---

## Tasks:

- Use your browser to retrieve all announced prefixes for the AS6412
- Perform a simple check on your resource if it is seen on the Internet:
  - Create a simple script using resource-overview or routing-status



# Creating a Nagios Check

---

- Create a Nagios check using the RIPEstat Data API
  - Nagios is a monitoring tool that supports the development of custom checks (like other similar tools)
- Result codes for a check show the state:

State	Result
Ok	0
Warning	1
Error	2

# Create a Nagios check

## Example of a Python-based check:

```
if args.transit:
    transit = args.transit.split(',')
origin = args.origin.split(',')
nagios_status = 0
origin_errors = 0
transit_errors = 0
nagios_message = ""
url = "https://%s/data/looking-glass/data.json?resource=%s" % (args.statserver, urllib2.quote(args.prefix, ''))
lookingglass_raw = urllib2.urlopen(url)
lookingglass_json = json.load(lookingglass_raw)
if lookingglass_json['data_call_status'] != "supported":
    print "WARN: %s is under maintance " % (args.statserver)
    sys.exit(1)
for rrc in lookingglass_json['data']['rrcs']:
    for peer in lookingglass_json['data']['rrcs'][rrc]['entries']:
        aspath = peer['as_path'].split()
        details = peer['details'][0].split()
        peer_addr = details[0]
        nexthop = details[2]
        router_id = details[3]

        if len(aspath) > args.minpath:
            if aspath[-1] not in origin :
                origin_errors += 1
                nagios_message = nagios_message + ( "Origin mismatch %s (%s): %s; " % (rrc, peer_addr, aspath[-1]))
            if args.transit:
                if aspath[-2] not in transit :
                    transit_errors += 1
                    nagios_message = nagios_message + ( "Transit mismatch %s (%s): %s; " % (rrc, peer_addr, aspath[-2]))

if origin_errors == 0 and transit_errors == 0:
    nagios_message = "OK: %s Origin is %s " % (args.prefix, args.origin)
    if args.transit:
        nagios_message = "%s and all transits match %s" % (nagios_message, args.transit)
elif origin_errors >= args.crit or transit_errors >= args.crit:
    nagios_status = 2
    nagios_message = "ERROR: " + nagios_message
elif origin_errors >= args.warn or transit_errors >= args.warn:
    nagios_status = 1
    nagios_message = "WARN: " + nagios_message
```

# Contact & Information:

- <https://stat.ripe.net>
- Mailing List: **mat-wg@ripe.net**
- Articles & updates on RIPE Labs
  - **<https://labs.ripe.net/ripestat>**
- Questions: **stat@ripe.net**

