Beyond Prefixes: The Power of Routing Policies and IRRs

Milad Afshari | CAPIF4 | Almaty, September 2025

Who am I?

- Milad Afshari
- Enterprise Network Planning Manager @ MTN-Irancell(AS44244)
- Co-founder & PC chair of IRNOG
- PC member of CAPIF

Why This Talk?

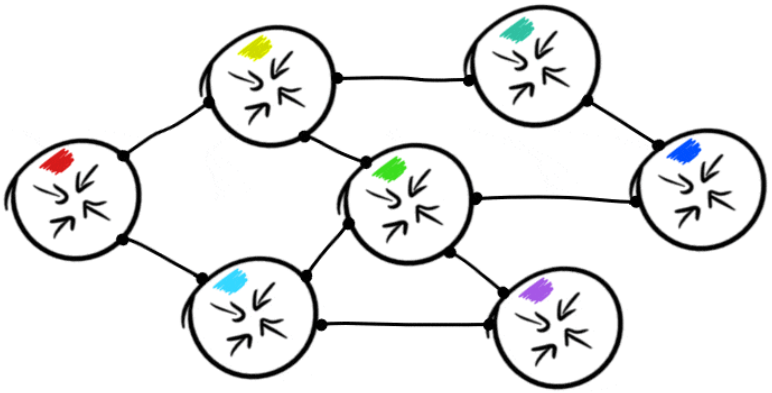
- Last year I spoke about routing security in the region. This year, since there is still room for improvement in Central Asia — including Kazakhstan — I decided to revisit the basics and highlight again why this topics matters:
  - BGP has no built-in security mechanisms
  - Misconfigurations and hijacks still happen
  - Routing policies and IRRs help us bring order
  - Goal: strengthen Internet resilience & security

BGP at a Glance: Strengths and Challenges

Internet Number Resources & BGP

- The Internet relies on identifiers:
  - IPv4 Addresses
  - IPv6 Addresses
  - Autonomous System Numbers (ASNs)

- BGP:
  - For nearly 30 years BGP has kept the Internet running, but it still faces security challenges. It was originally designed when the Internet was much smaller and based on a trust model between network operators



The Problem with BGP

- Prefix Hijacking: redirect traffic
- Route Leaks: instability & misrouting
- Misconfigurations: global outages
- No built-in verification

BGP Incidents Overview

AS7007 Incident

- **Event:** Software bug led to a large part of IP address ranges being misannounced as originating from AS7007.
- **Impact:** Traffic was redirected and overwhelmed AS7007's equipment, causing widespread disruption.

Pakistan Telecom and YouTube

Event: Pakistan Telecom attempted to block YouTube locally but accidentally propagated the block globally.

Impact: Global internet access to YouTube was disrupted.

Belarus BGP MITM Attack

Event: BGP-based man-in-the-middle attack targeting major US credit card companies and governments.

Impact: Interception of sensitive communications.

MyEtherWallet Attack

Event: BGP hijacking led to DNS redirection and phishing of cryptocurrency wallets.

Impact: $17 million stolen from users due to compromised TLS connections.

1.1.1.1 Route Leak

Event: The issue started on June 27, when Eletronet S.A. (AS267613) mistakenly announced a very specific route (1.1.1.1/32) to its peers and upstream providers.

Impact: The incident impacted around 300 networks across 70 countries, though Cloudflare noted that the overall impact was relatively low and many users did not notice significant disruption.

IRR (Internet Routing Registry)

Internet Routing Registry (IRR)

- IRR - the Internet Routing Registry
- Public routing policy databases
  - Used to register routing information
  - Declaration of BGP announcements, connected peers and routing policies
- Many IRR databases exist
  - Mostly mirroring each other
  - RIPE, APNIC, RADB, JPIRR, Level3, NTTCom, etc.

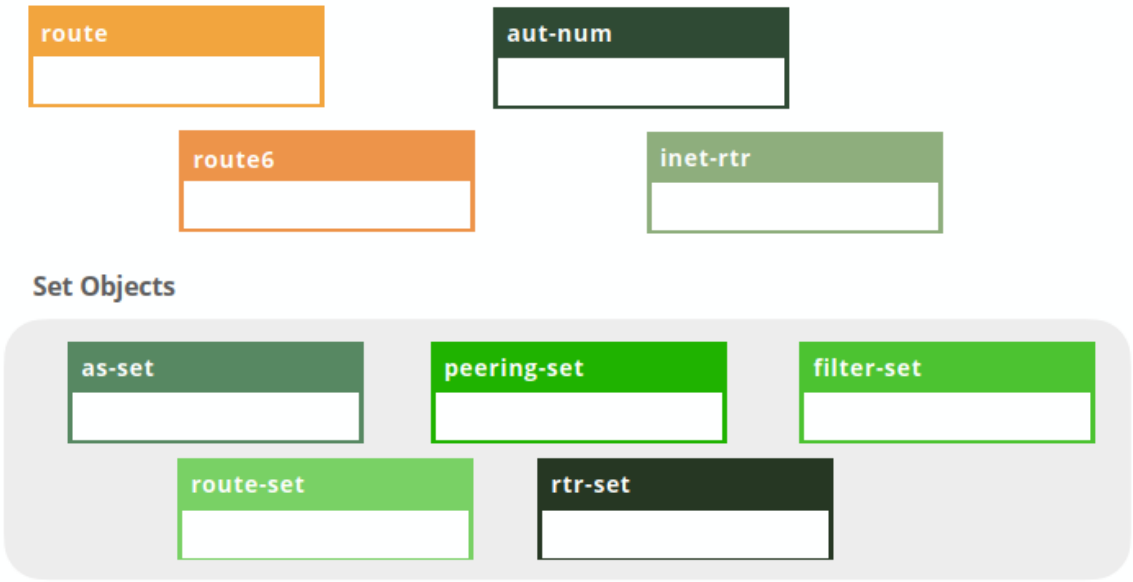
https://irr.net/

Why register routing information?

- Document your routing policy
  - Associate network prefixes with an origin AS
- Helps to filter unauthorized announcements
  - **Mitigates** route hijacks and denial of service
- Many transit providers and IXPs require it
  - They build their filters based on the Routing Registry

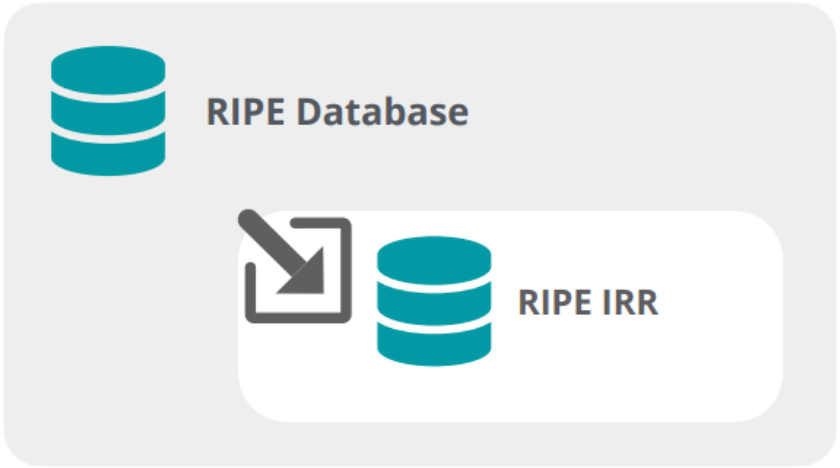
IRR Objects

- route / route6: prefixes
- aut-num: AS & policies
- route-set, filter-set: group policies
- Used to automate filtering



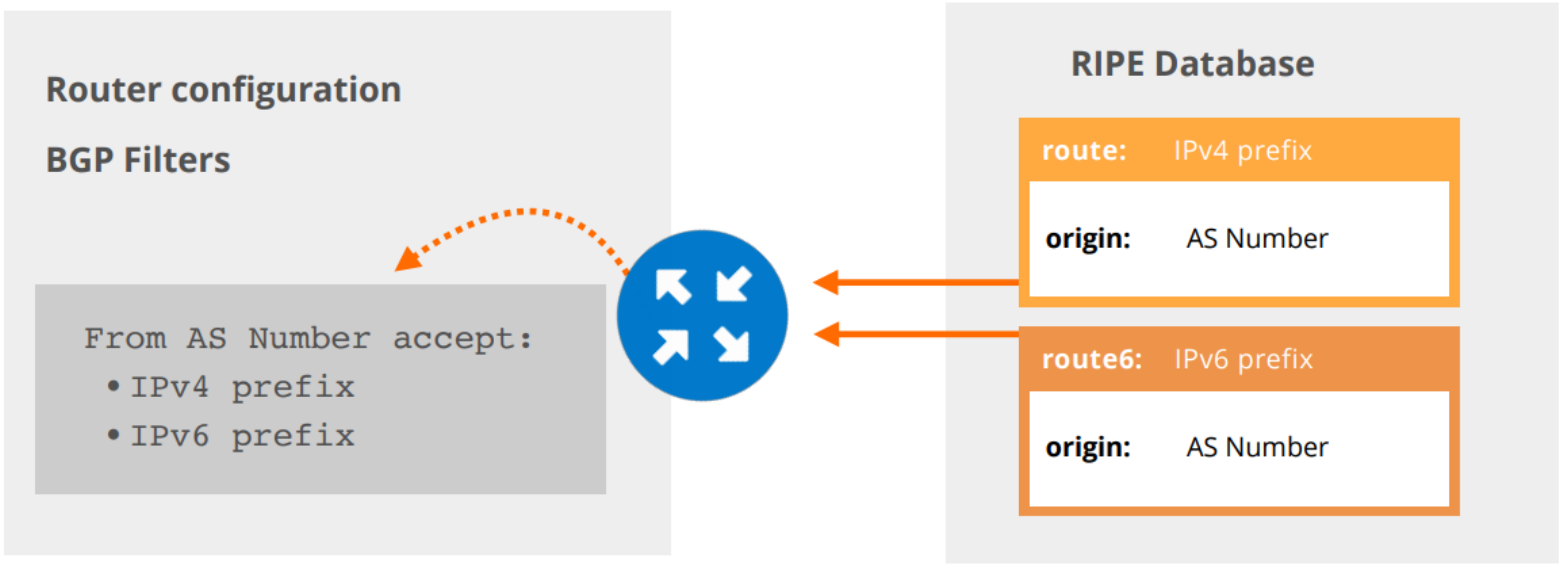
The RIPE Routing Registry

- The RIPE IRR is a subset of the RIPE Database
- Used for registering routing policy information
- Includes several objects
  - route(6), aut-num, filter-set, route-set, …
- The RIPE Routing Registry is a part of the global IRR system



route(6) objects

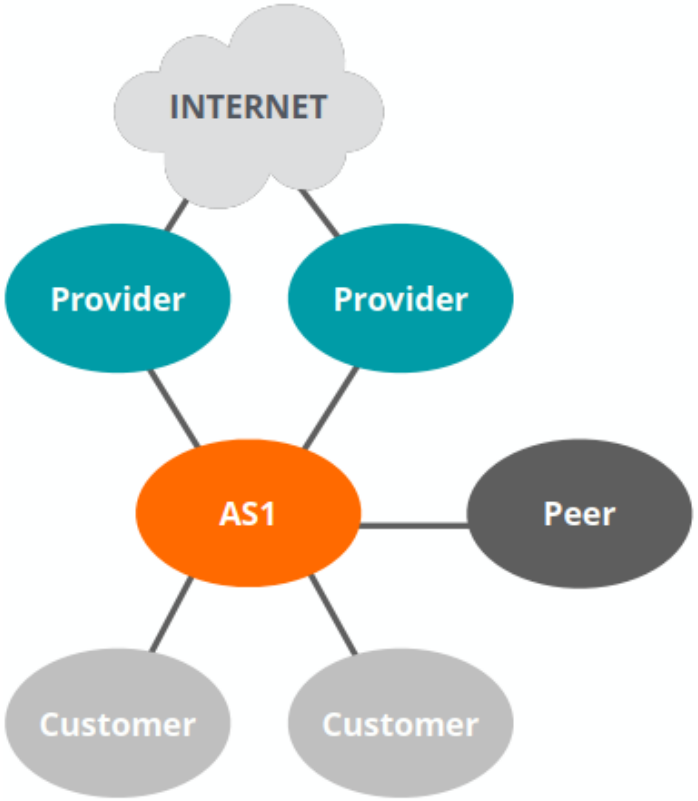
- Contains routing information for IPv4/IPv6 address space
- **Specifies from which AS a certain prefix may be originated**
- Used for creating BGP filters



BGP Routing Policy

What is a Routing Policy?

- Who are your BGP peers? Which ASes?
- What is your BGP relationship with them?
  - Customer, Provider, Peer
- What are your routing decisions?
  - Which prefixes to accept?
  - Which prefixes to announce?
  - Which prefixes will be preferred in case of multiple routes?

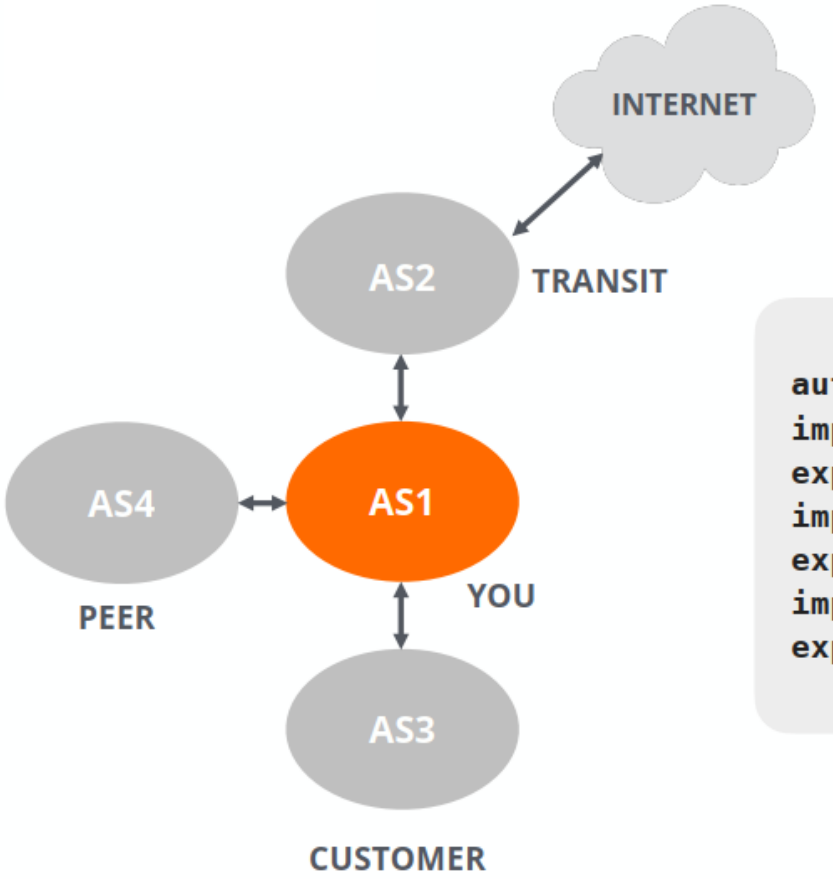


RPSL Language

- RPSL - Routing Policy Specification Language
- Allows network operators to specify their routing policies
  - Generic way to describe BGP configuration in the IRR
  - Not vendor-specific
- Originated from a RIPE Document (RIPE-181)
- Can be translated into router configuration

RFC 2622 - Routing Policy Specification Language
RFC 2650 - Using RPSL in Practice

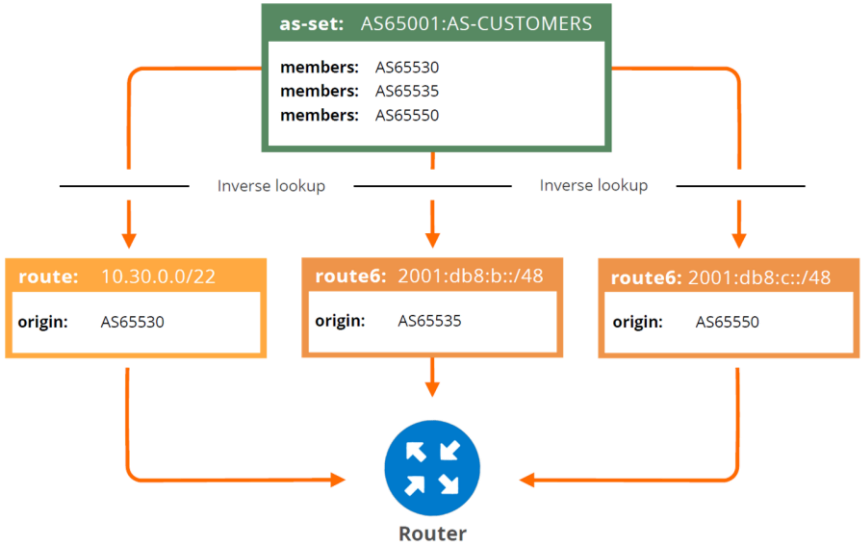
Routing Policies in Practice




```
aut-num:  AS1
import: from AS2 accept ANY
export: to AS2 announce AS1 AS3
import: from AS3 accept AS3
export: to AS3 announce ANY
import: from AS4 accept AS4
export: to AS4 announce AS1 AS3
```

IRRs & BGP Automation

- Tools available that get the policy data from the IRRs
  - Extract prefixes from route(6) objects
  - Query the IRRs over Whois protocol
- Some can generate complete router configurations
- Most are open source tools
- **Generating a Prefix Filter:**



RPSL tools for BGP automation

- **IRRToolset (written in C++)**
  - https://github.com/irrtoolset/irrtoolset
- **Rpsltool (perl)**
  - https://github.com/rfc1036/rpsltool
- **IRR Power Tools (PHP)**
  - https://github.com/6connect/irrpt
- **bgpq4 (C)**
  - https://github.com/bgp/bgpq4
- **Filtergen (Level 3)**

  - https://github.com/anchor/filtergen

  - whois -h filtergen.level3.net RIPE::ASxxx

```
ripe@ripe:~$ bgpq4 -s -6 as3333 -l FROM_CUSTOMER_RIPENCC
no ipv6 prefix-list FROM_CUSTOMER_RIPENCC
ipv6 prefix-list FROM_CUSTOMER_RIPENCC seq 1 permit 2001:610:240::/42
ipv6 prefix-list FROM_CUSTOMER_RIPENCC seq 2 permit 2001:67c:2e8::/48
ipv6 prefix-list FROM_CUSTOMER_RIPENCC seq 3 permit 2a13:27c0::/29
ipv6 prefix-list FROM_CUSTOMER_RIPENCC seq 4 permit 2a13:27c0:10::/44
ripe@ripe:~$
ripe@ripe:~$
ripe@ripe:~$
ripe@ripe:~$
ripe@ripe:~$
ripe@ripe:~$
ripe@ripe:~$
ripe@ripe:~$ bgpq4 -s -4 as3333 -l FROM_CUSTOMER_RIPENCC
no ip prefix-list FROM_CUSTOMER_RIPENCC
ip prefix-list FROM_CUSTOMER_RIPENCC seq 1 permit 193.0.0.0/21
ip prefix-list FROM_CUSTOMER_RIPENCC seq 2 permit 193.0.10.0/23
ip prefix-list FROM_CUSTOMER_RIPENCC seq 3 permit 193.0.12.0/23
ip prefix-list FROM_CUSTOMER_RIPENCC seq 4 permit 193.0.18.0/23
ip prefix-list FROM_CUSTOMER_RIPENCC seq 5 permit 193.0.20.0/23
ip prefix-list FROM_CUSTOMER_RIPENCC seq 6 permit 193.0.22.0/23
ip prefix-list FROM_CUSTOMER_RIPENCC seq 7 permit 193.230.194.0/24
ripe@ripe:~$
```

bgpq4 example

IRR Limitations

- **IRRs may contain conflicting data**
  - Distributed databases that mirror each other
- **No central authority**
  - Who will verify the accuracy of the data?
- **No verification of holdership**
  - In some IRRs, you can create objects without checks
- **Not updated properly**
  - Information is missing, outdated or incorrect

RPKI

- Verifies the association between resource holders and their Internet number resources
- Attaches digital certificate to IP addresses and AS numbers
  - RPKI is based on an X.509 certificate profile defined in RFC3779.
- Only ~50% of IPv4 covered by RPKI
- IRR still critical for remaining space
- Dual use = best security today

References

- https://ripe.net
- https://academy.ripe.net
- https://iana.org
- https://irr.net
- https://www.kentik.com/blog/a-brief-history-of-the-internets-biggest-bgp-incidents
- https://academy.ripe.net
- https://stat.ripe.net
- https://labs.apnic.net/measurements

Thank you!
Any Questions?