BGP AS / ISP Security Ranking

Raphaël Vinot

Master 2 SSIC
ISFATES/DFHI
Université Paul Verlaine - Metz

Masterarbeit, 2010

Table of contents

Content

Internet and the peering

- Decentralized network
- Many operators
- Different types of peering

Border Gateway Protocol (BGP)

- Routing protocol of the Internet
- Associate Autonomous Systems and Networks
- Use policies (QoS and security)

Autonomous System (AS)

- Identify operators without using IPs
- One or more subnet for each ASN
- Assignation: IANA, RIR and LIR

Content

RIS Whois

- Routing Information Service (RIS)
- Updated every 8 hours

193.0.19.19

```
route: 193.0.18.0/23
origin: AS3333
descr: RIPE-NCC-AS RIPE Network Coordination Centre
lastupd-frst: 2010-06-21 15:10Z 198.32.176.24@rrc14
lastupd-last: 2010-08-31 22:48Z 198.32.160.187@rrc11
seen-at: rrc00,rrc01,rrc03,rrc04,rrc05,rrc06,rrc07,[...]
num-rispeers: 102
source: RISWHOIS
```

Whois

- More information (owner)
- Many, incompatible, databases
- Find the right server

Datasets

- Global
  - abuse.ch ZeuS Tracker
  - Dshield
- Particular AS
  - Arbor ATLAS/Active Threat Feed
  - Shadowserver

Content

Threats (no threads :))

Users just do not care. At all.

- Mobile devices and Internet
- Growing business
- *"non-profit" malicious software are dead*, Kaspersky - 2007

Botnet

- Botmaster
- Command & Control Server
- Bots

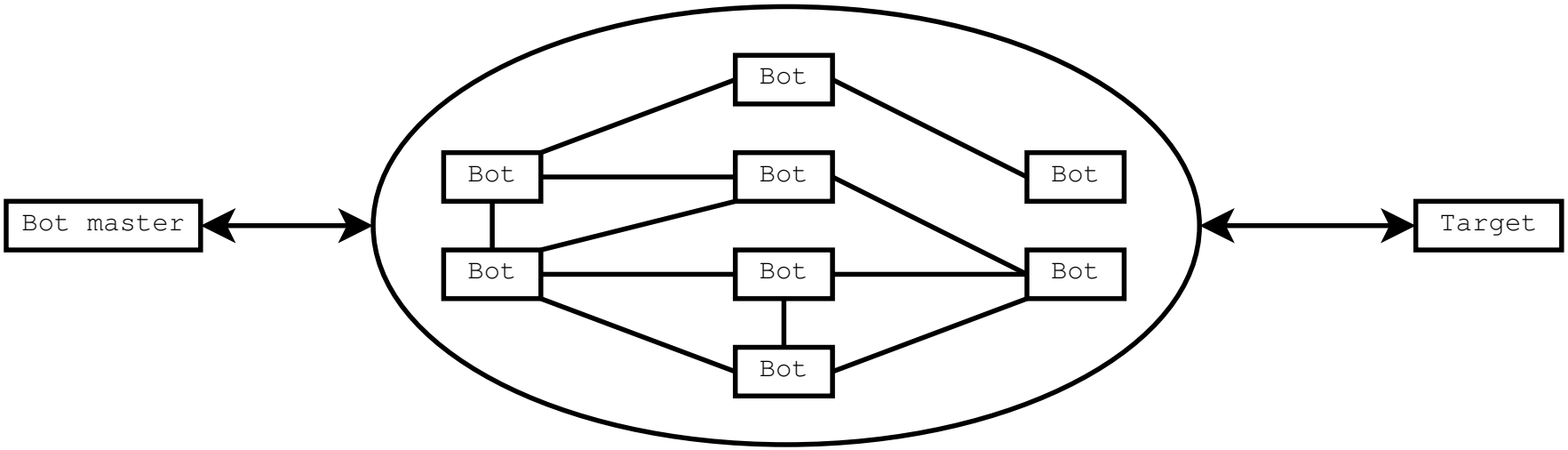


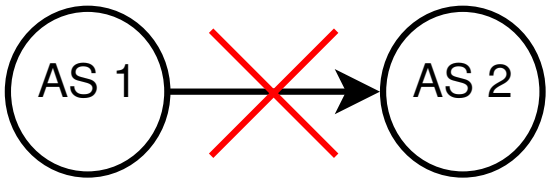
Figure: Botnet - Basics

- DDoS, phishing...

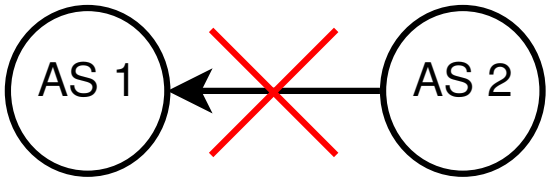
Content

Mitigation

- Traffic shaping
- Blackholing
- Depending on the attack
  - From the AS (DDoS, Command & Control Server)



  - To the AS (Phishing, keylogger)



Information

- Alert the user
- Contact the provider
- Contact the authorities
- History

Content

Requirements

- Fast
  - *mapreduce*-like processing
- Opensource
  - Affero GPLv3

High-level view

- Aggregation
  1. datasets
  2. RIS Whois and Whois entries
- Ranking

$$R = 1 + \frac{(SUM(occur * s\_impact) * SUM(vote))}{AS\_size}$$

occur	all the IPs from the ASN, by sources.
s_impact	value assigned to the source
vote	vote against this AS (actually not implemented)
AS_size	total of IPs

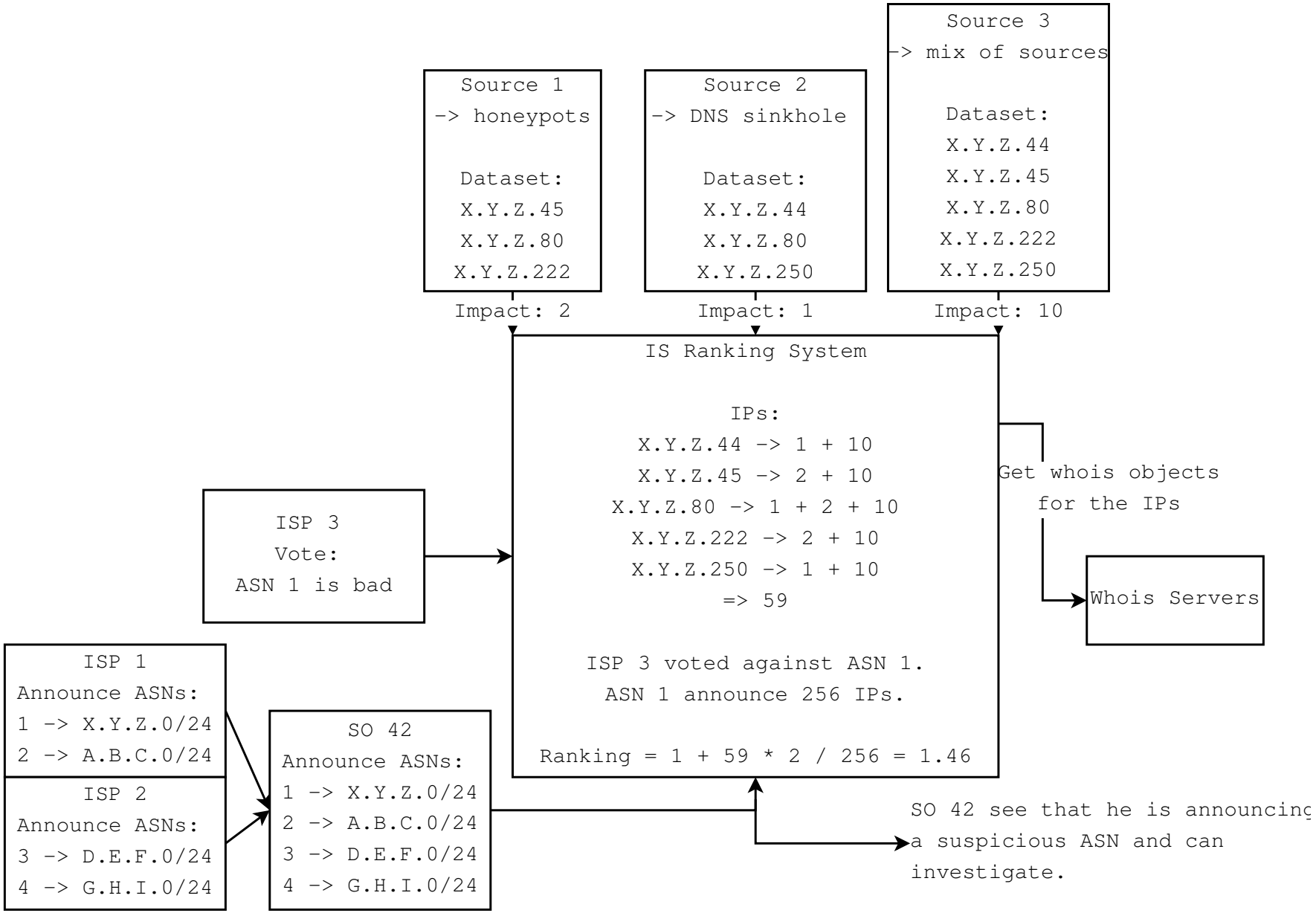


Figure: High level

Third party programs

- Redis
- MySQL
- libbgpdump
- Rgraph
- Cheetah and Cherrypy

Content

Input

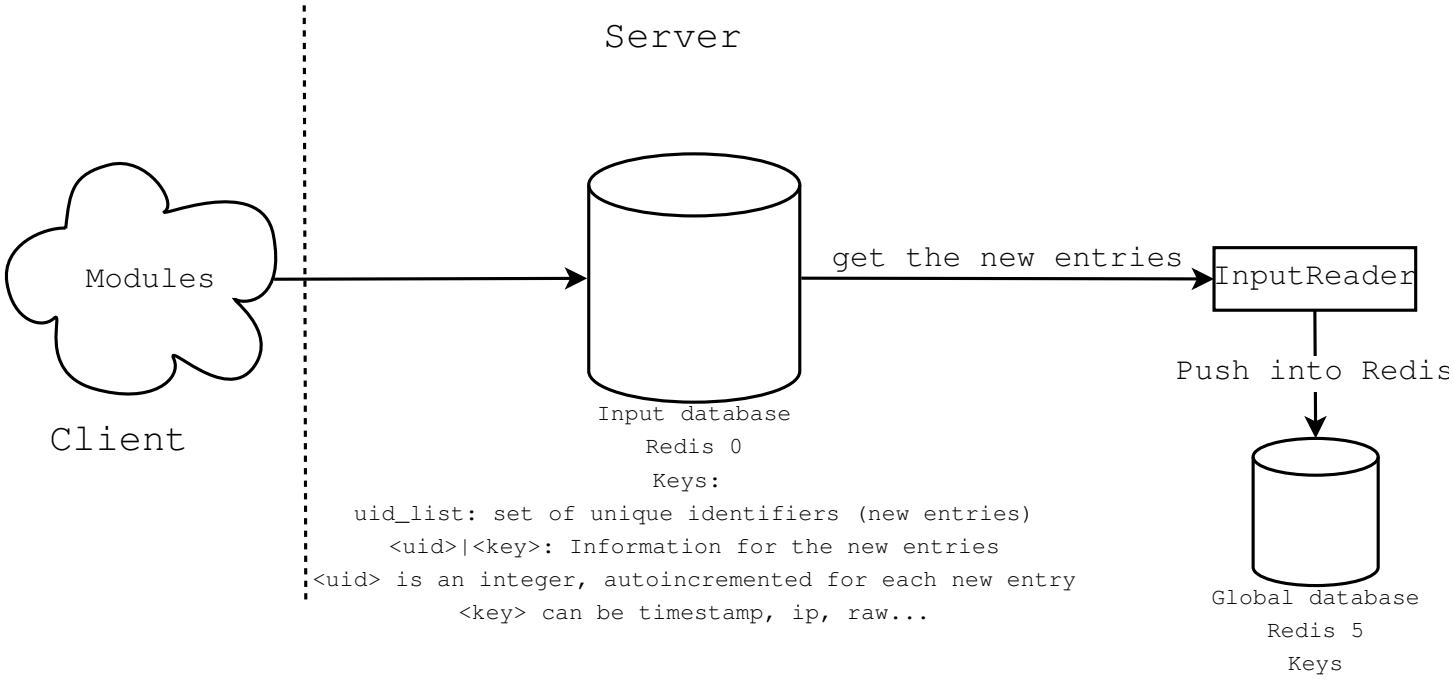


Figure: Input of new information

- Modules push the information into redis
- A “reader” push them into MySQL

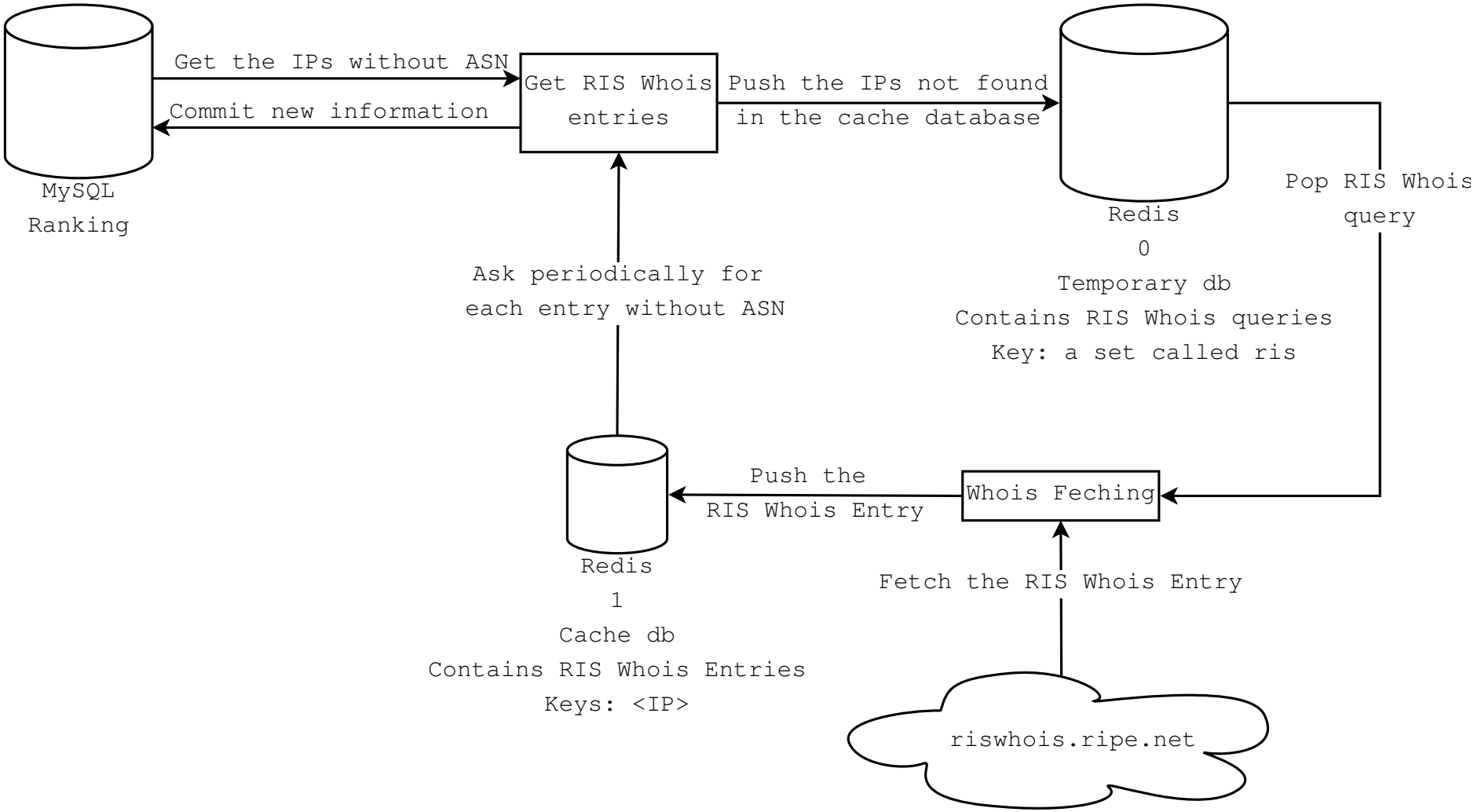


Figure: RIS Whois fetching

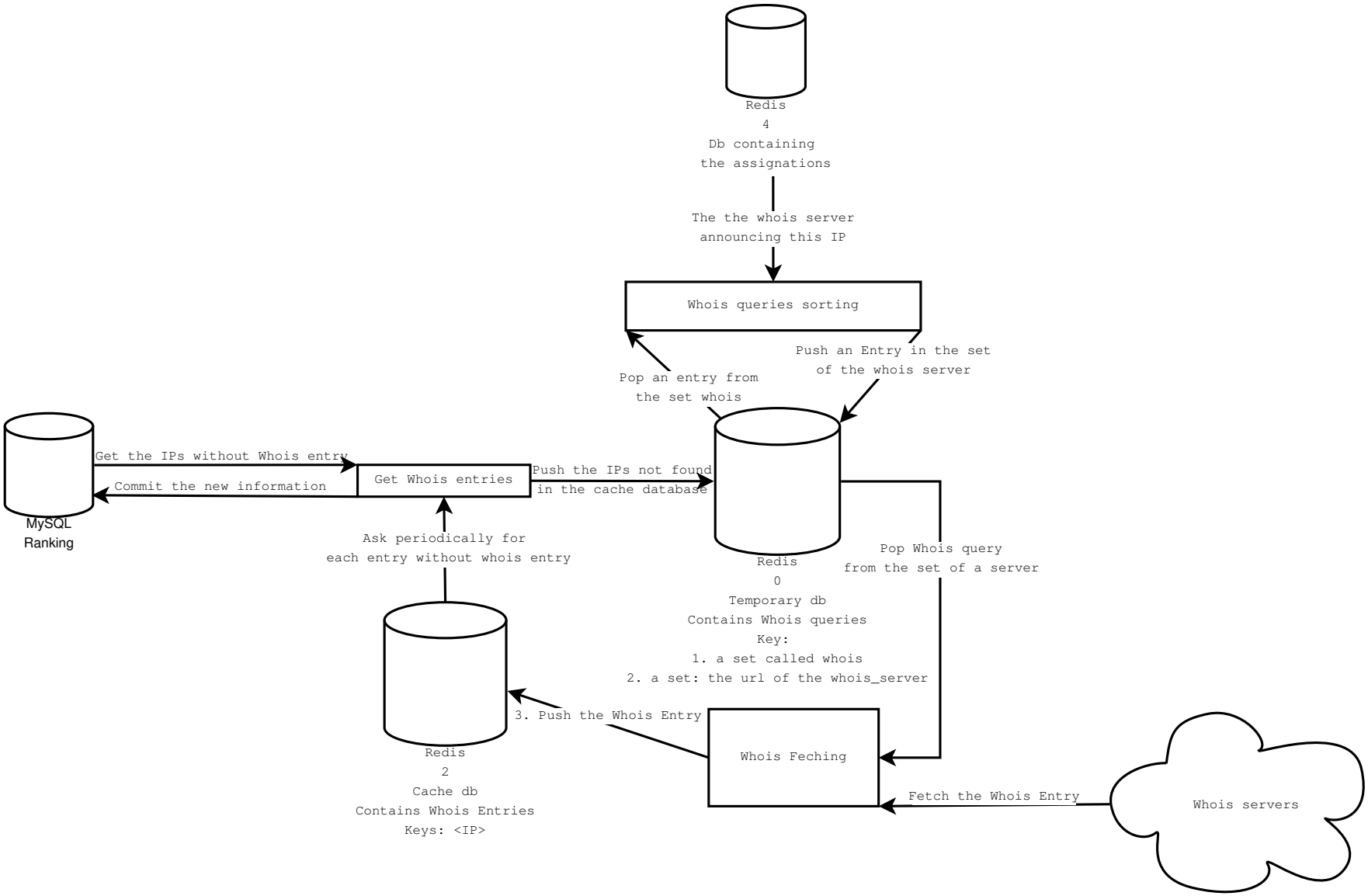


Figure: Whois Fetching

Ranking

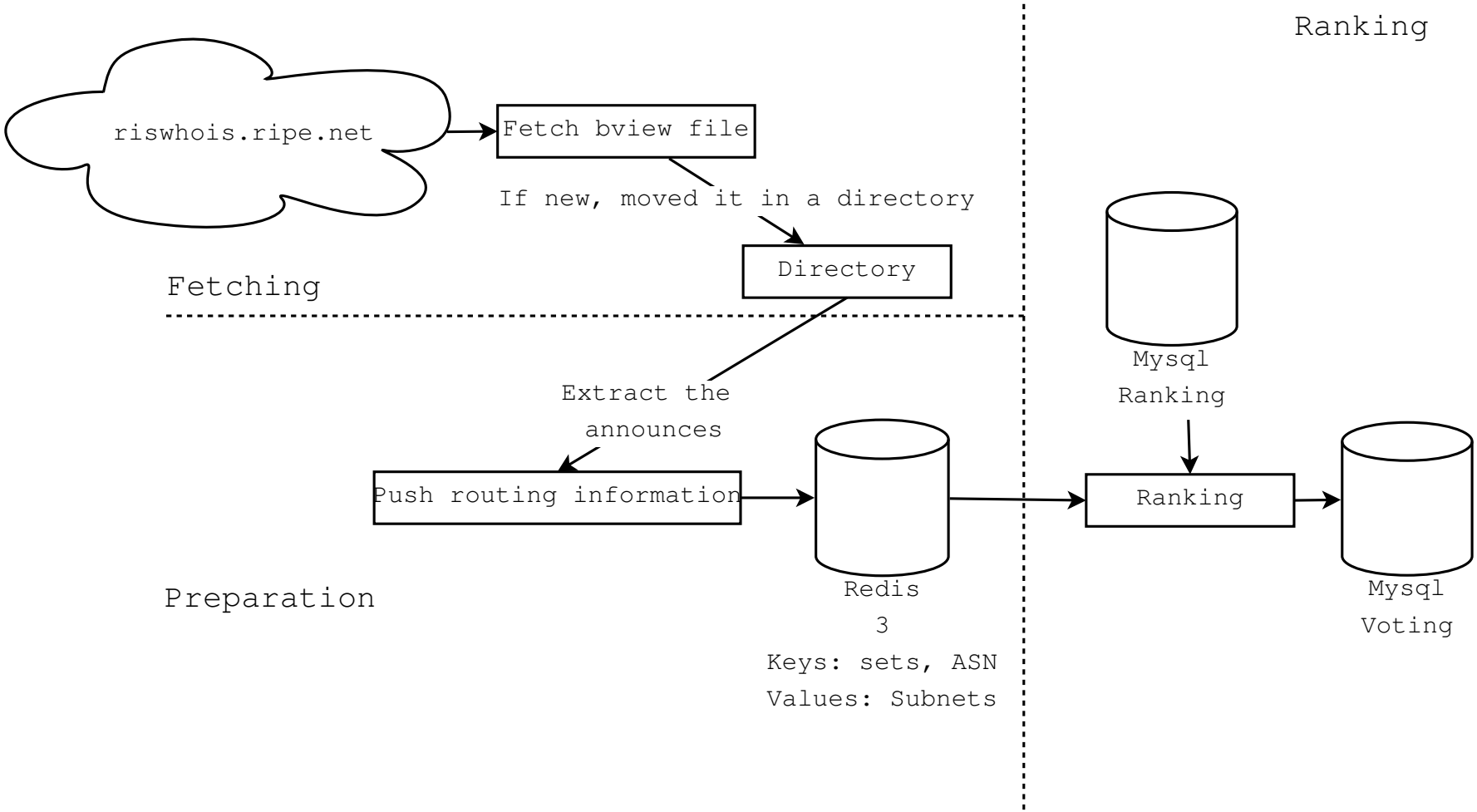


Figure: Ranking

Modules

- Supported information:
  - Always: IP and Source
  - If possible: Timestamp
  - Sometimes: Infections type, raw field
- Multiprocessing
- Format:
  - $< UID >:< FIELD >$
  - List of UID
- Interest: No limitations on the type of the sources

Website and first results.

Fragen ?