

BCOP FOR THE USE OF IRR DATABASES BY IXP ROUTE SERVERS

RECOMMENDATION
FOR IXP OPERATORS
(DRAFT V1.0)

S. KONSTANTARAS – AMS-IX

M. D'ITRI - MINAP

W. van GULIK – ROMANDIX

A. DINU – INTERLAN IX

K. BLUMBERG – TORIX

INTRODUCTION.....	3
Scope.....	4
Recommendation for the use of IRR databases	4
Grace period	5

INTRODUCTION

The root of the Internet Number Registry System is the IANA, the Internet Assigned Numbers Authority, which manages the complete pool of all possible IP addresses and AS numbers. It allocates blocks of these resources to the five Regional Internet Registries (RIRs): RIPE NCC, ARIN, APNIC, AfriNIC and LACNIC. RIRs suballocate those resources to Local Internet Registries (LIRs): Internet Service Providers (ISPs) and end users. In order to keep track of those allocations and ownership of the resources, RIRs operate public databases that host all relevant information in objects written in the RPSL language.

Throughout the time of birth, development and rapid expansion of the global internet infrastructure, several unofficial IRR databases appeared with local significance and being operated either by private companies (e.g., Level 3) or independent institutions (e.g., Canarie). Those DBs aim to provide a two-fold functionality to their customers:

- Mirror the data of the official IRR databases to provide shorter response times.
- Operate as a local IRR publishing RPSL objects documenting their own and their customers' policies.

The latter one was strengthened by the lack of official IRR DBs for an extended period. Although RIPE RIR exists since 1989, other RIRs were established much later (e.g. ARIN 1997 or AFRINIC 2004). Hence, big telco carriers who needed to provide IRR services to their customers or peers, had to either build their own IRR DB system or rely on existing third-party databases to create and publish RPSL objects.

Although these practices were used in the past to cover the missing gaps, they have introduced some important discrepancies as well, which can confuse IXP and other network operators causing different operational behaviors.

For example, although a network operator might have been allocated IP space in the RIPE region, which would be registered in the RIPE DB, the owner of this network might have decided to publish their policy in an unofficial IRR DB (e.g., RADB). Therefore, if an IXP operator or another peering partner did not query that IRR DB then they would not be able to view and resolve these RPSL objects.

While it could be argued that retrieving the data from a private IRR DB (which are openly accessible in most cases) is a quick way to overcome the issue, it is not a scalable solution and can create object conflicts.

We define an object conflict as the situation where an RPSL object for a network resource (i.e., usually an aut-num, as-set, route or route6 object) exists in different versions in two or more databases.

In general, replicating objects is not harmful if the object maintainer keeps the data consistent across authorized and unauthorized DBs. Unfortunately, this is not happening in real life and results in outdated objects existing in different IRR DBs for the same resource.

Scope

This document introduces a new recommendation for IXP operators regarding the use of IRR databases for retrieving policies and building filters for the BGP sessions of IXP route servers. The goal of this effort is to establish a consistent behavior among IXP operators about which IRR databases they should trust to retrieve RPSL objects.

The authors understand that, in some regions, it is likely that many RPSL objects, in the excluded unofficial IRR databases, might be more up to date compared to the ones in the supported RIR databases. In that case, the IXP operator following this policy may try to communicate with the member who maintains the object and recommend updating the RPSL objects in the appropriate RIR database. Once the resource holder fixes the inconsistency, all operators will benefit from the result.

Recommendation for the use of IRR databases

IXP operator must trust and use only the following IRR databases for building and maintaining Route Server filters:

- **AFRINIC DB**
- **APNIC DB**
 - **APJJ**
 - **CNNIC**
 - **JPNIC**
 - **KRNIC**
 - **TWNIC**
 - **VNNIC**
 - **IRINN**
- **ARIN DB**
- **LACNIC DB**
 - **NIC.MX**
 - **NIC.BR**
- **RIPE DB**

The listed databases are the ones managed by the official RIRs, which are responsible for delegating Internet resources to networks. They are the only IRRs which can be used safely, because they guarantee that only the entity to which an IP network has been allocated, is allowed to create route or route6 objects referencing that network.

In case an IXP member has registered their policies in a different IRR database, the IXP operator has no obligations to deviate from this policy and comply with customer's demands to use other IRRs. This policy does not forbid nor mandate IXP operators from manually maintaining private filters and exceptions for their members.

On the other hand, it is mandatory for IXP operators to use all the listed databases to generate their filters. Before this policy takes effect, IXPs shall make multiple best-effort attempts to warn their members relying on unofficial IRRs about the need to replicate their policies in the appropriate IRR.

Grace period

The authors understand that the adoption of this recommendation will result in a massive transfer of RPSL objects from non-supported databases to the supported ones. This procedure, although not difficult to perform with modern tools, would still require some planning and time.

Therefore, the policy introduces a grace period of 12 months in which the list of allowed databases is supplemented by these:

- RADB
- RIPE-NONAUTH
- NTT
- LEVEL3

The grace period shall start by the time the IXP operators announce to members and customers that they will support this recommendation. The grace period is completely optional and can be omitted if the IXP operators claim full readiness for the full adoption of the recommendation.

At the end of the grace period, IXP operators must stop supporting these additional IRRs and operate filter generation tools that will only query the RIR databases.

During the grade period, IXPs will make multiple best effort attempts to warn their members relying on these IRRs about the need to replicate their policies in the appropriate IRR.