CRISP Update

Shane Kerr and Engin Gündüz, RIPE NCC

September 2004

Background and Overview

CRISP is an IETF working group. Its charter describes its work:

> In the standard operation of Internet systems, various labels and data are managed globally -- domain names, IPv4 and IPv6 addresses, etc. From time to time, for operational and administrative purposes, users of the Internet need to be able to find and access registered information associated with those labels.

In the past the WHOIS protocol served this need. However, this WHOIS protocol is missing a number of features that are deemed useful:

- Mechanism to find authoritative servers
  With the current WHOIS databases is that it is not easy for a user to know which RIR to query for information.

- Structured queries
  Each WHOIS server has its own query format. For example, to query the ARIN Database for information about an AS number, you would use:

  ```
  whois -h whois.arin.net a 6
  ```

  To query the RIPE Database for information, you would use:

  ```
  whois -h whois.ripe.net -Taut-num as7
  ```

- Well-defined schema for replies
  The information that each server returns to a query is different for each server. The differences are in meaning as well as format.

- Standard error conditions
  No standard exists for returning error conditions.

- Data integrity
  Clients have no way to know whether the reply is actually from the server queried.

- Client authentication
  Servers have no way to identify clients. This is useful for setting rate limits for performance and privacy reasons. Currently most operators use client IP address, but this is not useful for clients with temporary addresses. IPv6 poses problems for operators using client IP address as well.

- Referrals to servers with better information about a resource
  Servers have no way to direct clients to better servers.

The CRISP working group was chartered to design a protocol that had these features.

The CRISP working group has agreed to use IRIS as the protocol. Basically, it is a replacement for the WHOIS protocol. This means that it is a query-only protocol, with a profile for domain and domain-related data (**dreg**), and a separate profile for Internet number and number-related data (**areg**). These profiles are similar, but reflect the differences in the things they describe.

Details of IRIS

IRIS is a client/server protocol. Both client and server include the protocol version, to future-proof the implementations. The protocol uses XML as the exchange format.

There are several profiles. Currently the domain registry (**dreg**) and address registry (**areg**) are defined. These are both extensible. It is possible to define additional profiles in the future, for example a routing registry, although this will require client changes to support new profiles.

IRIS supports client-side referrals. This means that the server tells the client the location of a server with better information. This is similar to how a non-recursive DNS server works.

Each profile defines one or more mechanisms for service location. In **dreg** clients use the DNS to find the appropriate server, by doing a set of either bottom-up or top-down queries. In **areg** a well-known server will act as the root to the clients.

Each record has a globally unique identifier, allowing entities to be referenced unambiguously.

Servers may allow or require clients to authenticate themselves. Servers can then use this information to prevent mining, support different levels of access, and so on.

Differences Between WHOIS and IRIS

IRIS provides the features listed above, all of which are missing in WHOIS. However, in order to use IRIS to query about IP addresses and AS numbers, users will need to have an IRIS client that implements the **areg** profile. The **areg** schemas is similar to the contents of RIR databases, but different.. The key differences for users of the RIPE Database are outlined here.

- No Information Only Useful to Data Maintainers

Objects and attributes related to security have no equivalent. This includes MNTNER, KEY-CERT, and IRT objects, as well as “mnt-by:”, “mnt-lower:”, “mnt-routes:”, “mnt-irt:”, “mnt-ref:”.

Attributes for notification have no equivalent. This includes “notify:”, “mnt-nfy:”, “upd-to:”, “irt-nfy:”, “ref-nfy:”.

Information about changed date, like the “changed:” attribute, will be optionally available, but will not include an e-mail address.

- No Routing Information

The **areg** profile has no provisions for routing information. This includes attributes in the AUT-NUM class related to routing: “import:”, “export:”, “default:”, and “member-of:”. There are no INET-RTR or ROUTE objects. Also, there are no set related objects, including AS-SET, ROUTE-SET, FILTER-SET, PEERING-SET, or RTR-SET.

New attributes and classes added in RPSLng will also not be present.

Sample Object

The following is an example of a typical AS number. Information in the highlighted attributes will not be returned in IRIS. The other information will be returned in XML, and may be formatted by the client as appropriate. This may include localisation of the attribute names for other languages.

```
aut-num:        AS30720
as-name:        VWE-Extranet-AS
descr:          VWE Extranet
import:         from AS8341 accept ANY
import:         from AS12394 accept ANY
export:         to AS8341 announce AS30720
export:         to AS12394 announce AS30720
admin-c:        HVEN1-RIPE
tech-c:         HVEN1-RIPE
mnt-by:         DLW-MNT
mnt-routes:     DLW-MNT
changed:        hostmaster@ripe.net 20031114
source:         RIPE
```

IRIS is designed to provide contact and organisation details, and no unnecessary information.

The Future

Work in the IETF continues, but is approaching completion. The steps to be completed are:

- Mature and finalise the **areg** draft
- Push the **areg** draft to become a standards-track RFC
- Review final proposals (for example a proposal for UDP transport), and close the working group

These steps are expected to be finished in November 2004.

Parallel to this work, the RIPE NCC will put a prototype into production. The goal of this prototype is to serve as a technology test-bed, to see what the real operational issues with IRIS are. It is now planned to base the prototype on a Verisign reference implementation. Verisign has two open-source servers, available on their research site:

http://iris.verisignlabs.com/

The initial version will act as a proxy to the RIPE Whois Database. Subsequent versions will be designed based on the experience with this proxy.

A third effort occurring with this work will be an outreach to authors of client software. It is important that users have ways of accessing the service for it to be successful.