ICANN NO. 51 | 12-16 OCTOBER 2014

LOS ANGELES

16 October 2014

Deploying the IETF's WHOIS Protocol Replacement

Francisco Arias

Director, Technical Services

Global Domains Division

Edward Lewis

Technical Services Sr. Manager

Global Domains Division

Agenda

- Introduction (10 min)

- What is RDAP (10 min)

- Status of RDAP (10 min)

- Path to Adoption (15 min)

- Q&A (30 min)

History on Replacing the WHOIS Protocol

- SSAC's SAC 051 Advisory (19 Sep 2011)

  - *The ICANN community should evaluate and adopt a replacement domain name registration data access protocol*

- Board resolution adopting SAC 051 (28 October 2011)

- Roadmap to Implement SAC 051 (4 June 2012)

- RDAP Community development within IETF WG since 2012

- Contractual provisions in .com, .name, .biz, .info, .org, 2012 RA, and 2013 RAA

- RDAP RFCs expected in the next few months

Registration Data Access Protocol

- Intended to replace the WHOIS (port-43) protocol

- Provides flexibility to support various policies

- Already operating at Regional Internet Registries

- Provide benefits improving on weaknesses in the WHOIS protocol

- Designed with the knowledge of a now mature industry

Status of RDAP Protocol
Web-Extensible Internet Registration Data Service (WEIRDS)

Murray Kucherawy
IETF WEIRDS WG Co-Chair
<superuser@gmail.com>

The Problem

- WHOIS has not scaled well to the needs of the modern Internet:

  1. Unformatted

  2. Unauthenticated

  3. ASCII-only

  4. Insecure

The Problem: Unformatted

- WHOIS defined no specific output format

  - Every WHOIS registry is free to return its results in any form it wishes

  - Difficult to request a reply and extract exactly the piece of information requested

The Problem: Unauthenticated

- Impossible to distinguish one client from another, apart from source IP address

  - Can't distinguish two clients from the same IP address at all (e.g., NATs or PATs)

  - Unable to give preferential service to, say, official ICANN queries or to law enforcement

  - "Preferential service" might mean higher rate limits, more detailed answers, etc., versus anonymous queries

The Problem: ASCII-only

- There are no provisions for internationalized output
  - All participants are forced to use English or at least Anglicized names

The Problem: Not extensible

- There are no provisions in the protocol for options, parameters, or extensions

The Problem: Insecure

- Protocol is a trivial cleartext query/ response mechanism
  - Any interloper can see both the question and the response
  - Can also see which registry is being queried, though that's probably less interesting

Previous Solutions

- WHOIS [RFC3912] has origins in the late 1970s

- RWHOIS [RFC1714] in 1994 was an attempt to introduce a hierarchical lookup structure, but uptake was weak

- IRIS [RFC3981] attempted to do something more modern in 2005, but became highly complex and also saw little deployment

WEIRDS and RDAP

- In 2011, some ICANN staffers approached ARIN to talk about a new alternative involving the IETF

- Based on the requirements of IRIS [RFC3707], the IETF undertook a new, simpler effort

- Formed the "Web Extensible Internet Registration Data Service" (WEIRDS) working group

  - BoF in spring 2012, WG formed summer 2012

- Broad participation from RIRs and registries

- Developing the Registration Data Access Protocol (RDAP)

Fundamentals of RDAP

- Transport used is HTTP
  - Widely deployed and developed infrastructure
  - Lots of open source options
  - Allows for use of HTTP authentication
    - Satisfies the differential service requirement
  - Allows for use of HTTPS
    - Satisfies the encryption requirement
  - Already has support for redirects

Fundamentals of RDAP

- Replies are JSON formatted, which supports UTF-8

  - Satisfies the standard format requirement

- Internationalized domain names (IDN [RFC3409]) supported in both the question and the answer

  - Question is encoded in the URI

  - Combination satisfies the internationalization requirement

Fundamentals of RDAP

- IANA will maintain bootstrap registries for domains, AS numbers, and network blocks

  - Registries will be published in JSON

  - Clients will periodically download the registry as a way of knowing where to send a query for a given AS range, network block, or TLD

- A query that lands in the wrong place can be redirected using HTTP 303

Fundamentals of RDAP

- Bootstrap data includes the base query location for every registry

  - RDAP specification explains how to form direct queries and basic search queries

  - Other interesting query formats can be defined later

  - Satisfies the extensibility requirement

- Registry of known response fields also provides extensibility

Fundamentals of RDAP

- Basic search is supported in the protocol, but not mandatory to implement

Implementation Status

- Any HTTP client can issue queries and receive replies

- ICANN has partnered with CNNIC to produce an open source implementation

  - https://github.com/cnnic/rdap

- ARIN has had an implementation for network numbers since the beginning

- APNIC has a prototype available

- LACNIC appears to be in private beta

- RIPE NCC has an open source implementation

  - https://github.com/RIPE-NCC/whois

- VeriSign and Afilias are doing proof-of-concept implementations for domain names

Specification Status

- Six documents
  - Object inventory
  - RDAP over HTTP
  - Query format
  - Security Considerations
  - JSON responses
  - Bootstrapping
- https://datatracker.ietf.org/wg/weirds/documents/

Specification Status

- Currently in IETF Last Call

- IESG review on October 30

- Assuming no serious concerns, goes to the RFC Editor queue

- RFC Editor lately takes about a month to publish as an RFC
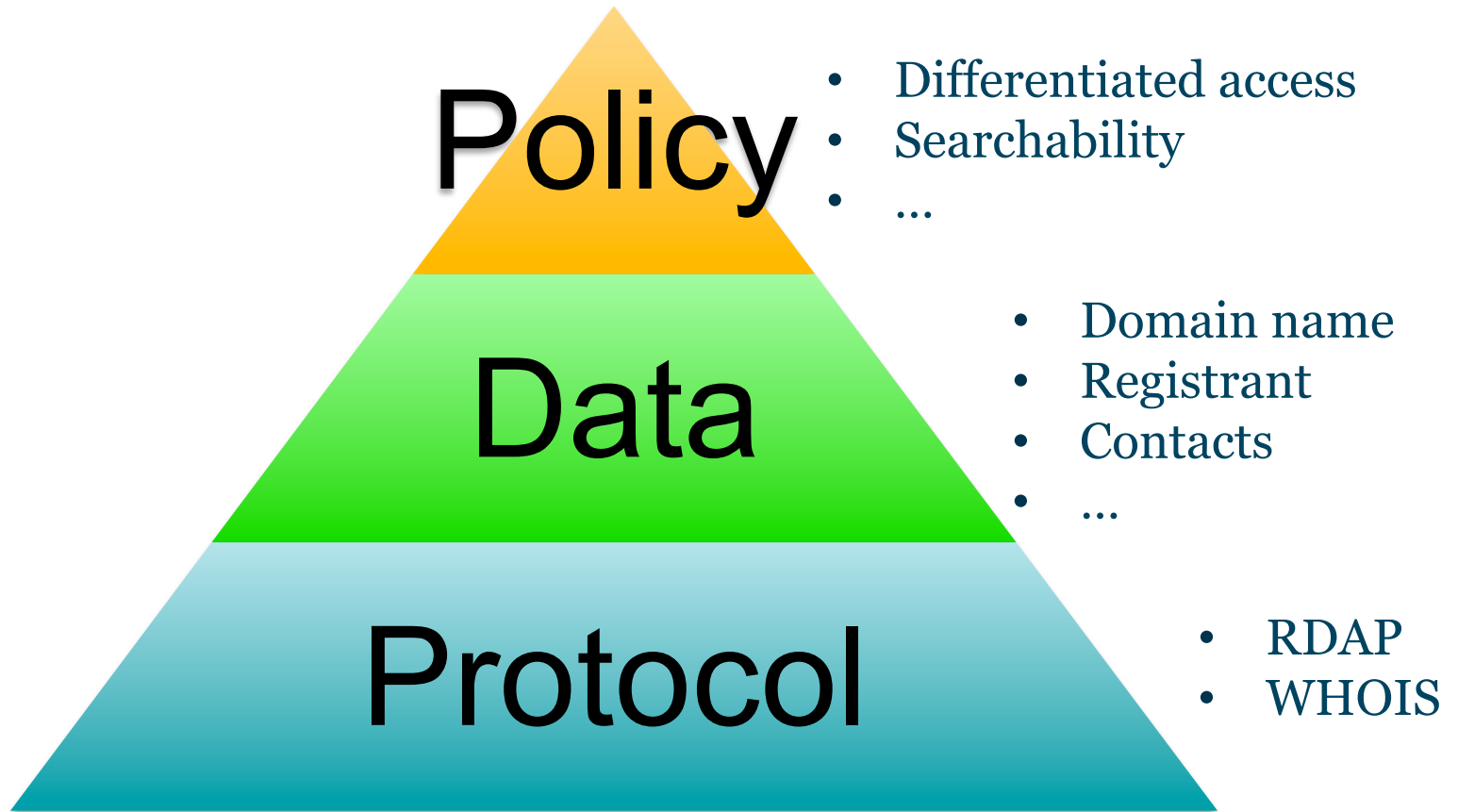
- Overall, very likely published by the end of 2014

RDAP and ICANN

- RDAP plays a prominent role in addressing the recommendations of the ICANN EWG on Directory Services
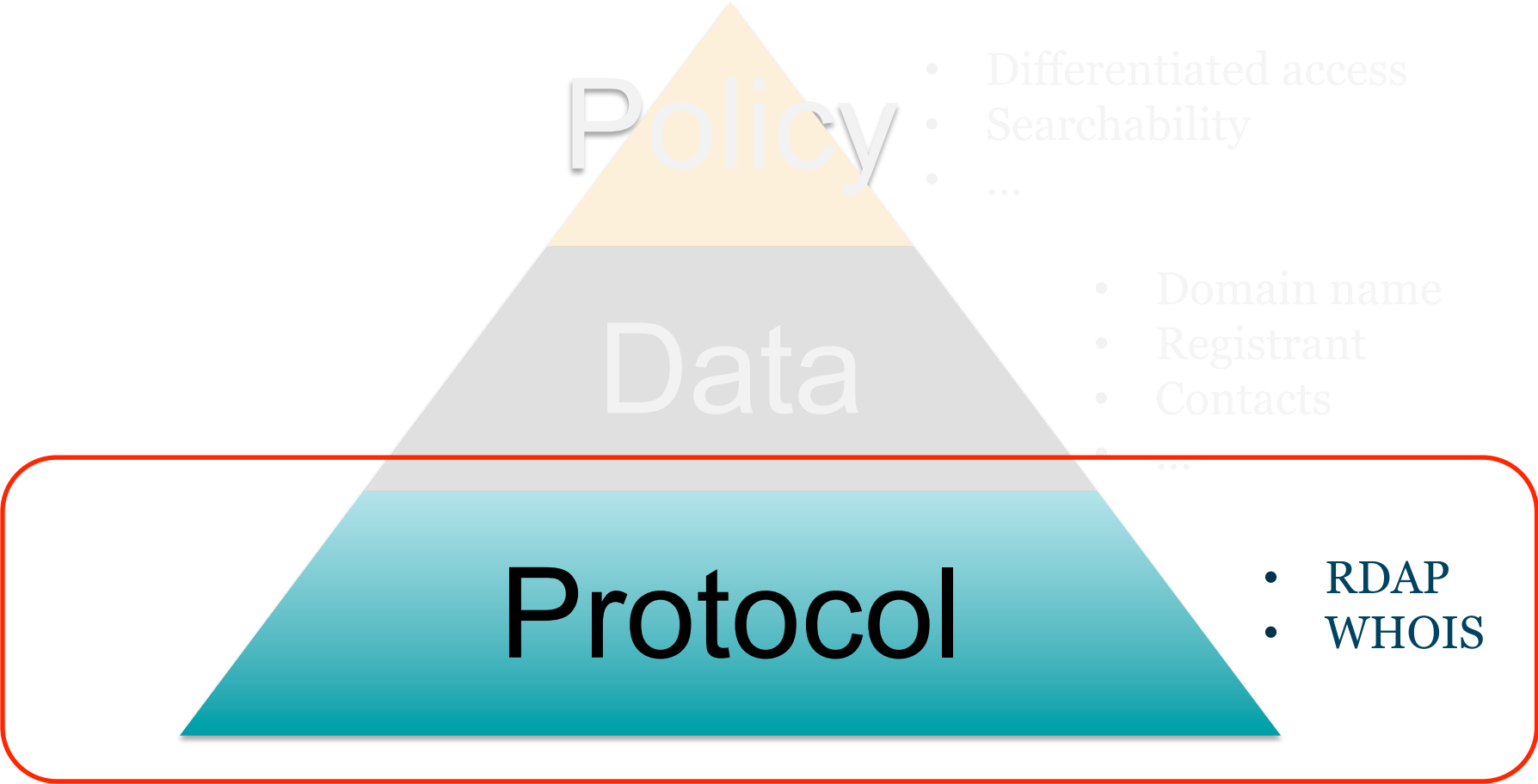
Path to Adoption

Simplified Anatomy

- Differentiated access
- Searchability
- ...

- Domain name
- Registrant
- Contacts
- ...

- RDAP
- WHOIS

Policy

Data

Protocol

Focus of this Effort

Policy
- Differentiated access
- Searchability
- …

Data
- Domain name
- Registrant
- Contacts
- …

Protocol
- RDAP
- WHOIS

RDAP Provides/Enables

- Standardized query, response, and error messages

- Extensibility

- Distributed sources – Redirection (if needed)

- Searchability (where applicable)

- Differentiated access (where applicable)

- Internationalization (pending T&T PDP)

- An incremental step towards a potential policy outcome from the EWG report

High-Level Roadmap

- RDAP attains IETF Proposed Standard status

- RDAP Implementations available

- RDAP operational profile defined

- RDAP deployment

- WHOIS (port-43) turn off

Questions

- Should RDAP deployment be synchronized with Thick Whois policy implementation?

- Once all Registries are Thick, is there a reason for registrars to offer RDAP/WHOIS/Web Whois?

- How long after RDAP deployment to turn off WHOIS?

GDD + Related Sessions

Thursday, 16 October

- o DNSSEC Key Rollover Workshop

Engage with ICANN on Web & Social Media

twitter.com/icann

gplus.to/icann

facebook.com/icannorg

weibo.com/icannorg

linkedin.com/company/icann

flickr.com/photos/icann

youtube.com/user/ICANNnews

icann.org