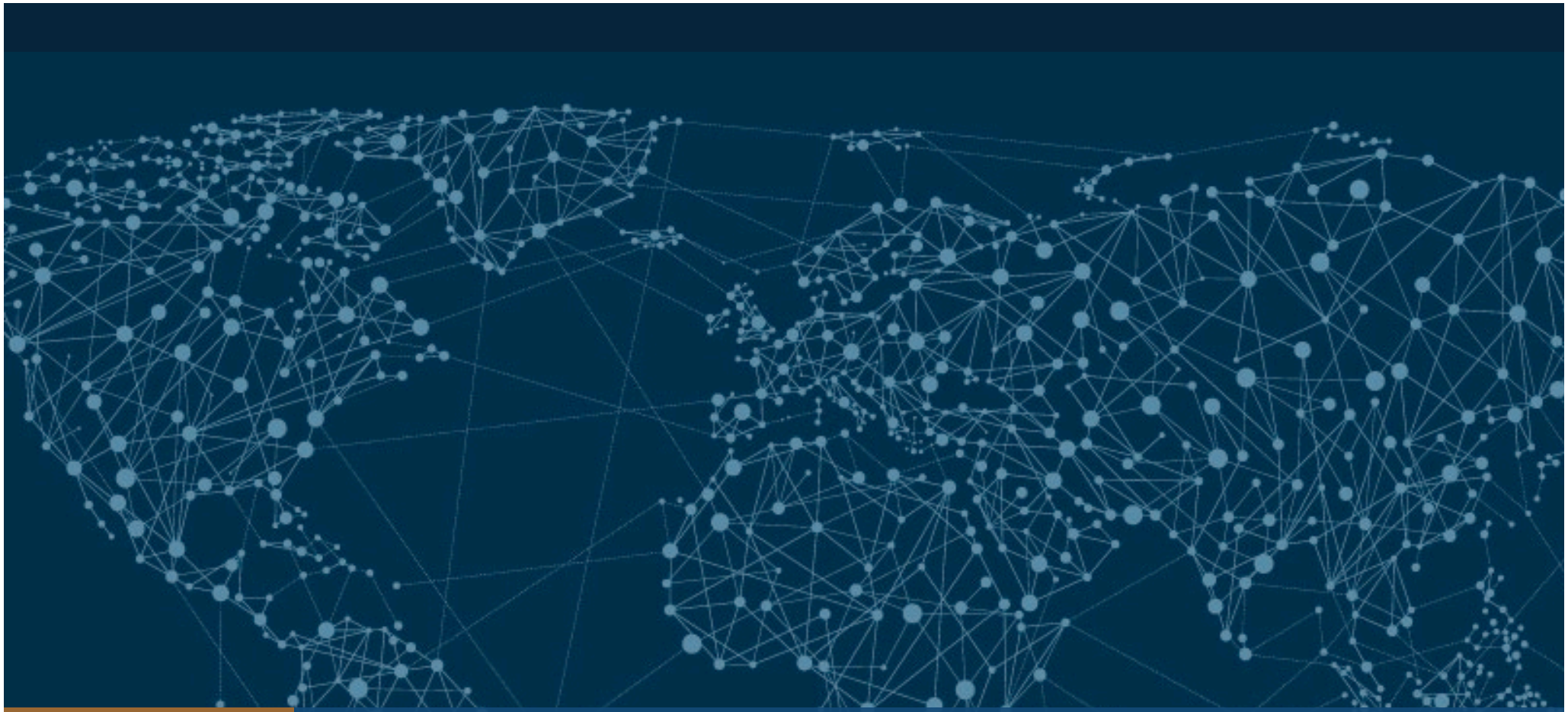


DOA: Some Observations From ICANN Office of the CTO/Research

Alain Durand, 2017

ICANN-OCTO/Research Engagement Since 2015

- The research branch of the Office of the CTO at ICANN started to look at DOA in 2015:
  - OCTO/Research had a number of interactions with Dr. Robert Kahn and his team at CNRI
  - OCTO/Research obtained a prefix end of 2015 and have been running an experimental DOA server since OCTO/Research moved to server code version 8.1 in 2016
- Output:
  - a number of memos to upper management and the board

Caveat

Complete and up-to-date documentation of the DOA data format, protocols on the wire and/or security protocols does not appear to be publicly available.

- Version 2.1 of the protocol is documented in RFC3650, 3651 & 3652. Current version is 2.10
- The CNRI implementation is readily available, there might be others that we have not found.

As a result, it is not easy to separate what is protocol standard from what is implementation choice. The following description correspond to our best efforts at understanding how DOA works and there might be errors.

What Is DOA? What is it not?

- DOA is a distributed name resolution system.
  - It can be seen as a federation of local name resolution systems.
  - It associates (resolves) the name of an object to an indexed series of user defined types.

- DOA is not a directory:
  - DOA does not provide search services.
  - DOA is closer to DNS or NIS/NIS+ than it is to X500 or LDAP.

- DOA stores and retrieves data about digital objects.
- DOA does not enable (nor control) communications with physical devices.

DOA: Digital Object Architecture

Invented by Dr. Robert Kahn, CNRI

Multiple names:

- Handle System (first described in 1995)
- DOI: Digital Object Identifier (publishing industry)
- DOA: Digital Object Architecture
- DONA: Digital Object Network Architecture (the foundation)

What is DOA Used For?

DOA is known to have been used by:

- The publication industry: catalog books & articles
- The TV and movie industry: catalog assets
- Max Planck Institute: catalog experiment results

Persistence

DOA is promoted as providing persistence. An example is:

> A researcher publishes papers while working at University A. He subsequently moves to University B. If his papers were referenced by URLs pointing to University A, the links would no longer work. However, if he references his paper with a DOA handle, he can update the handle after he moves to University B, and the handle will now resolve to the papers hosted by his/her new employer…

However, a similar result could be achieve by the researcher registering his own domain name and using URL redirects.

Persistence is a property that is more related to organization structures and how they evolve than to the underlying technology.

- One could build persistent URLs (see tiny ULRs)
- DOA handles could change over time (e.g. prefix loss)

Persistence Best Practices: A Naming Convention

For handle prefixes:

- ❑ **Use numbers, not names.** Names tend to reflect organizations, which can change over time.

For handle local names:

- ❑ **Use a flat local name space.** Structures reflect organizations, which tend to change over time.
- ❑ **Use object names that are as generic as possible.** For example, MPAA uses what looks like a hexadecimal hash. 10.5240/7487-C990-425F-D706-1785-J is a handle for the “The Top Gun” show

Handle Syntax: Prefix/Local-name

Prefixes: dot-separated Unicode character strings, UTF-8 encoded.
As of 2017, only digits are used, except for special cases.

11738	zero-delimiter prefix
10.1038	one-delimiter prefix
20.500.1234	two delimiter prefix

Since 2016, new registrations can only be one-delimiter or more.

Local-name can be any local file.

Examples:

11738/ithi	→	https://www.icann.org/ithi
10.1038/nphys1170	→	http://www.nature.com/nphys/journal/v5/n1/full/nphys1170.html

Registration: MPA (Since 2016)

MPA (Multi Primary Administrator) perform prefix registration (and resolution) in the Global Handle Registry.

Note: there does not appear to be any publicly available documentation on how to become an MPA or what the responsibilities are.

CNRI is the original/main MPA.

CNRI registration cost as of 2016:
$50 One-time initial registration fee + $50/year

As of 1/2017, sub-prefixes (e.g. 11738.1935) must be registered directly with the MPA.

Governance

The DONA foundation has been created to assume the governance role in DOA. It is based in Geneva, Switzerland. All intellectual property rights (IPR) have been transferred from CNRI to the DONA foundation.

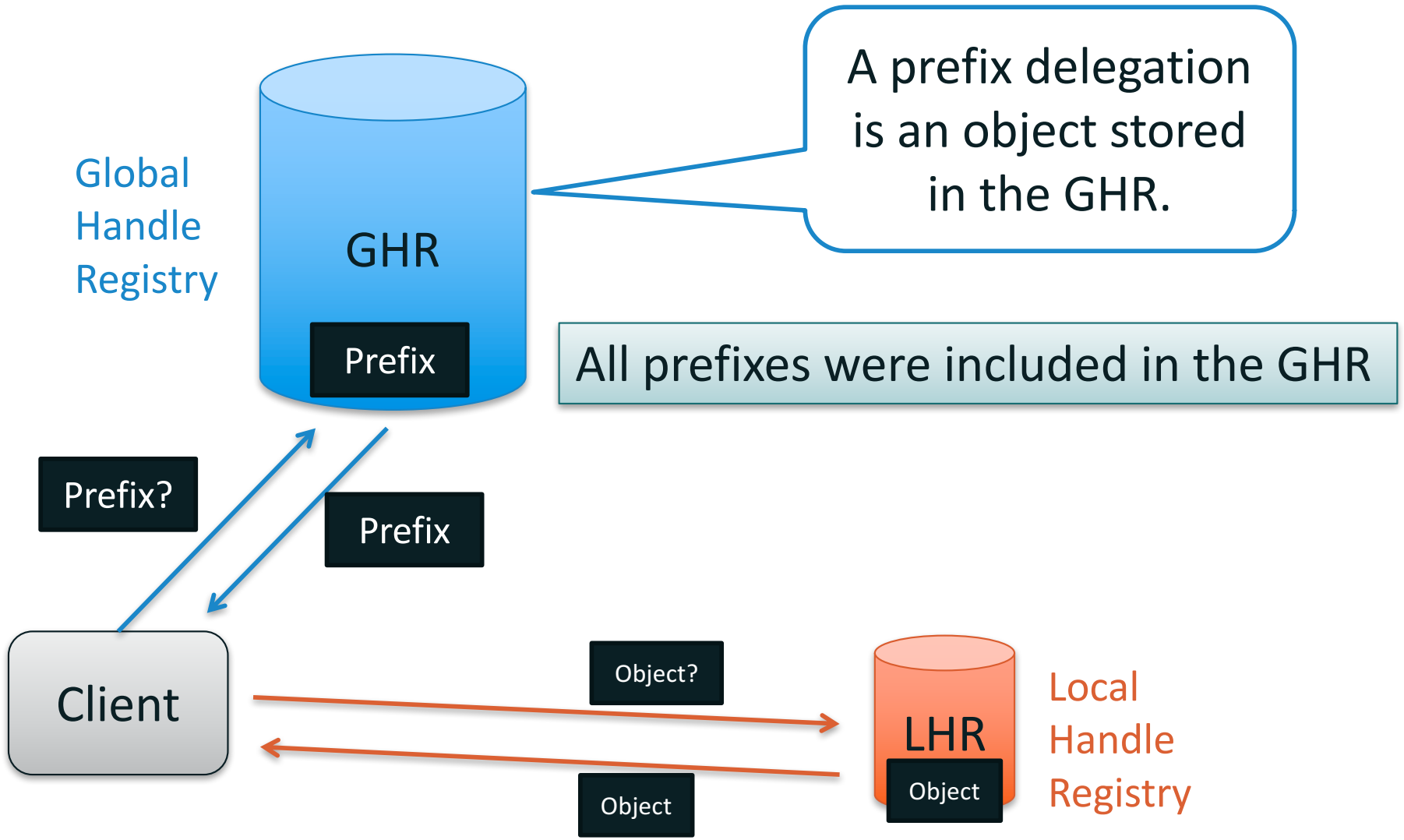
The DONA foundation assumes the combined roles of:

- protocol evolution (similar role as IETF does for DNS)
- policy development (similar role as ICANN does for DNS)
- GHR operation (similar role as root server operators do for DNS)

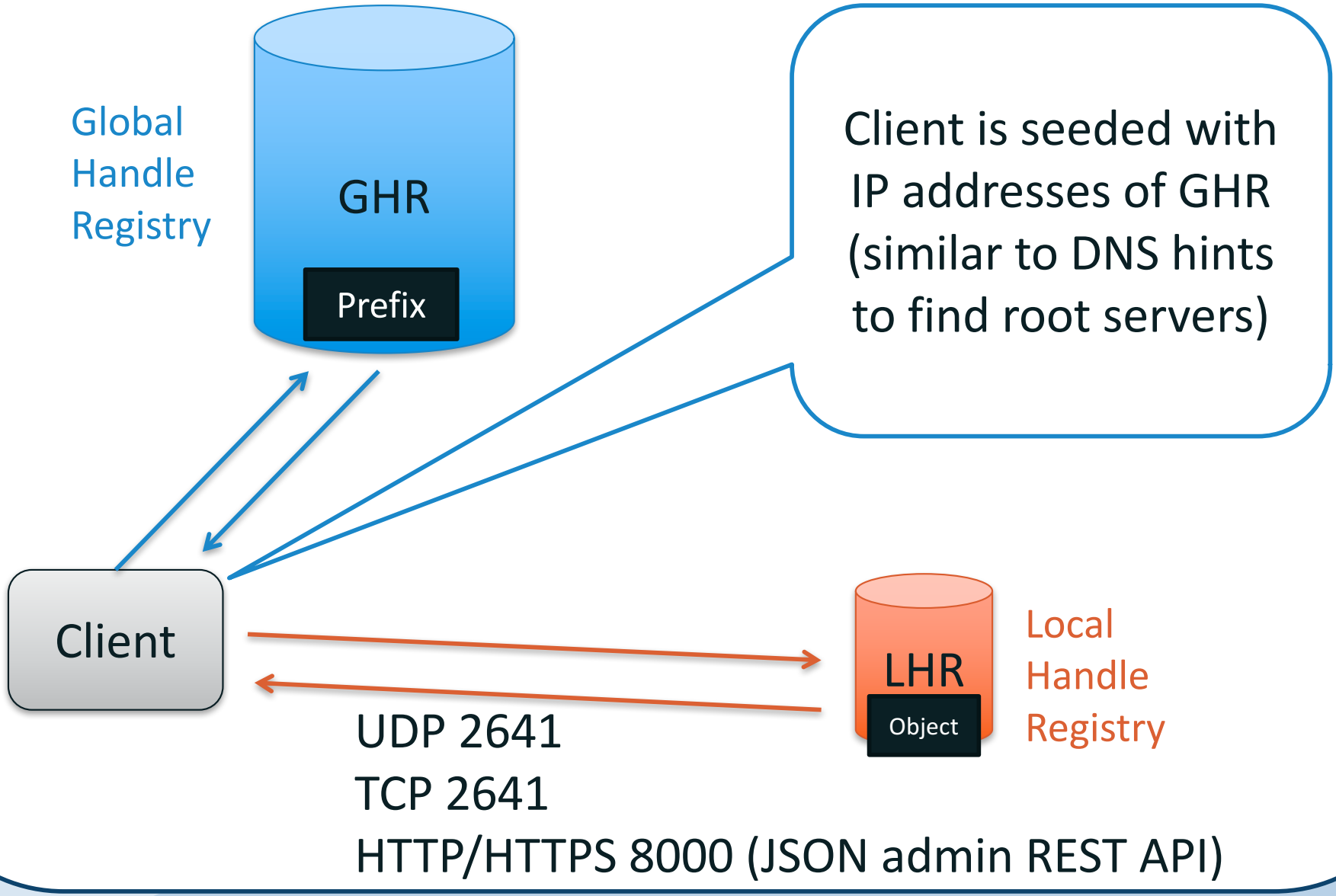
There is a MoU between the DONA foundation and the ITU:

- ITU provide secretariat function
- ITU will provide reconstruction in case of DONA failure

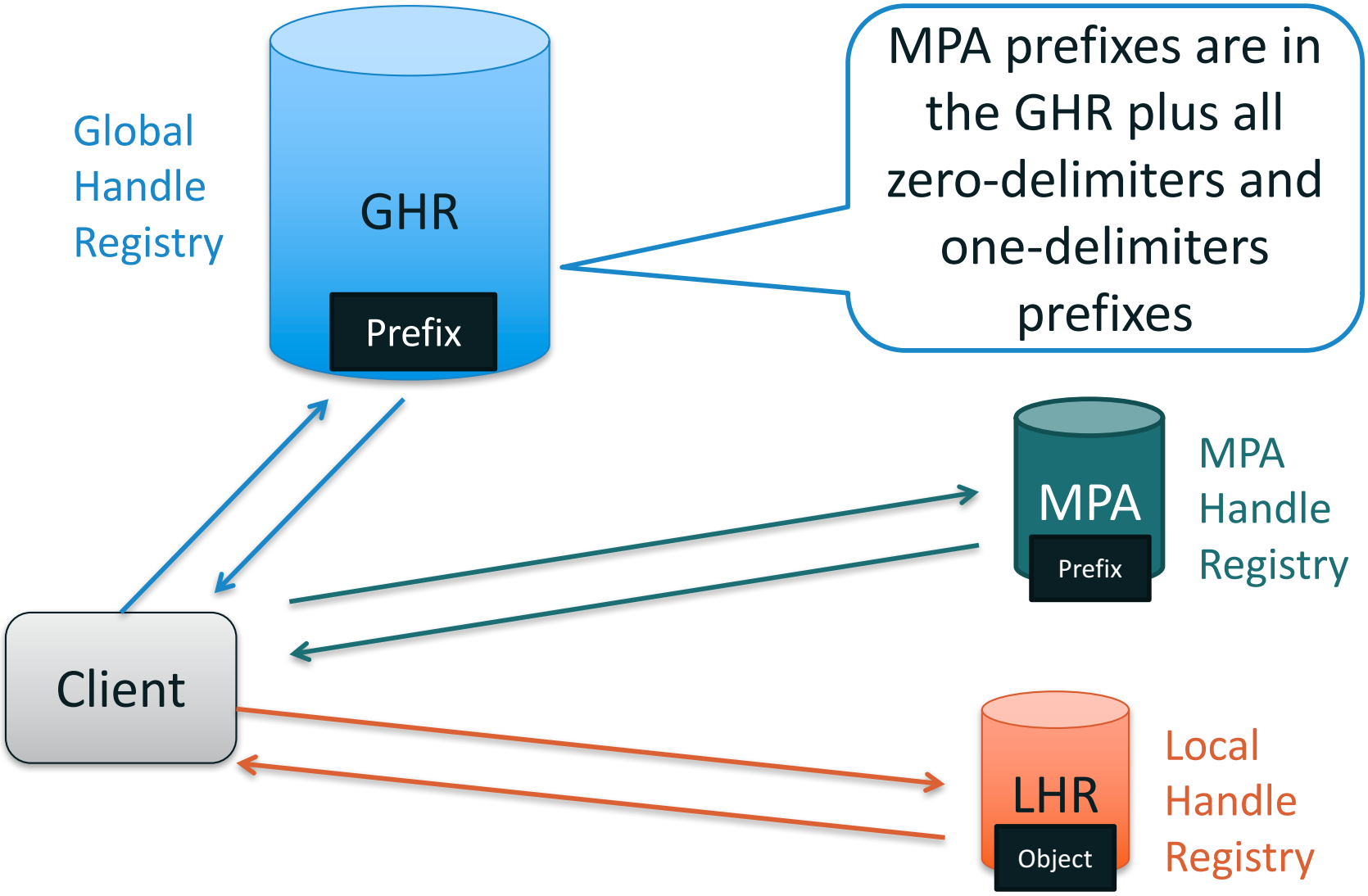
GHR/LHR: Original Design



Resolution: Bits on the Wire



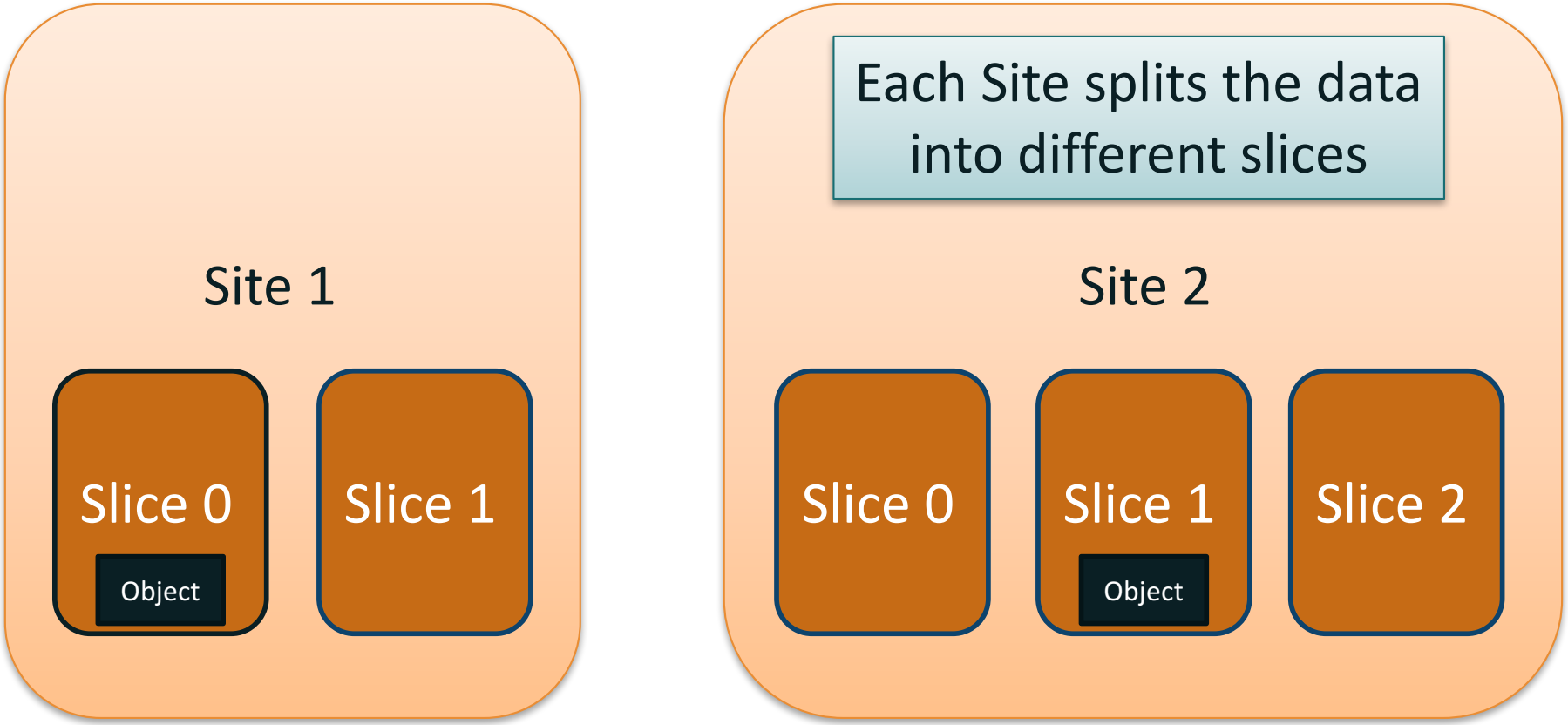
Resolution /Scaling: MPA Design (2016)



Handle Registry Scaling (Applies to GHR, MPA, LHR)

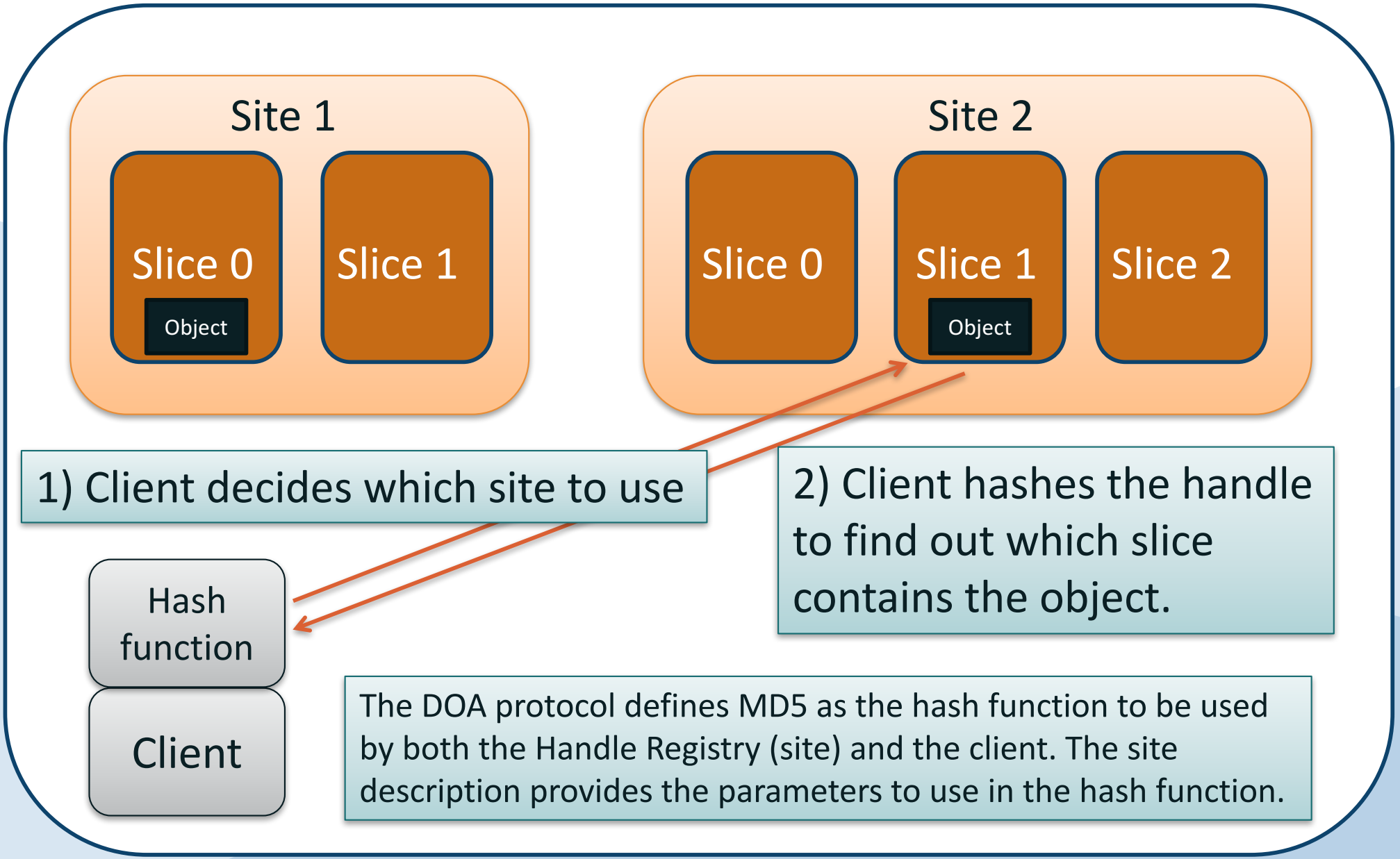
The handle describing the LHR prefix points to a list of sites

Each site contains the full set of data



Each site describe the hashing algorithm parameters used to find the slice where the queried object is maintained.

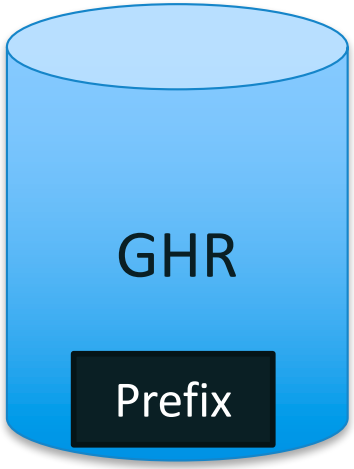
Client Resolution with Multiple Sites & Slices



Resolution /Security: Client Validation

Responses from the handle registry servers are signed using the private key of the server.

Global Handle Registry



Client is seeded with a master public key of the GHR, similar to DNSSEC KSK

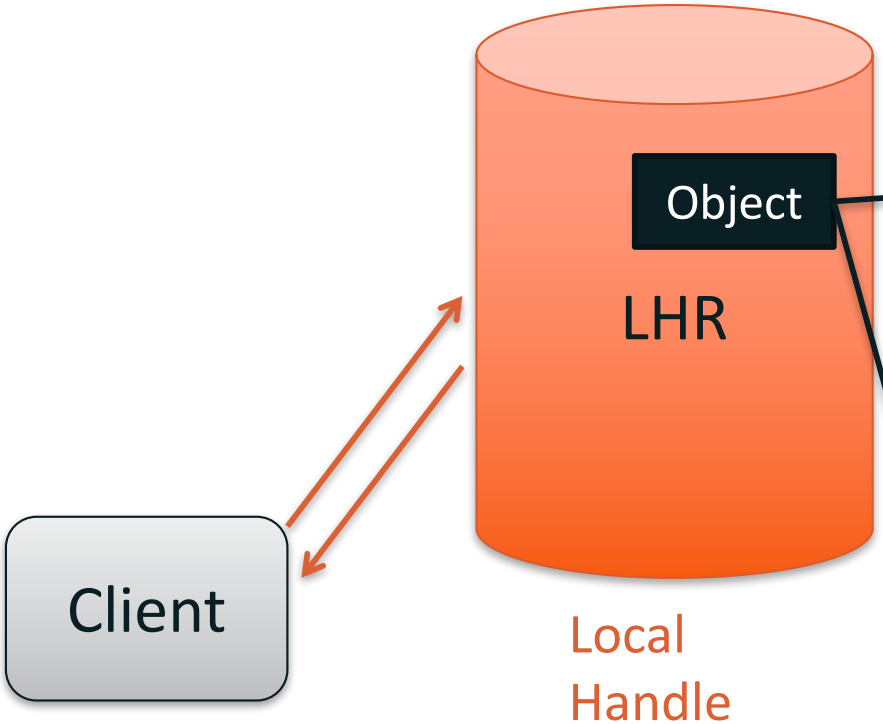
Client

Local Handle Registry

If the master public key changes, all the clients need to be manually updated.

Object Management: Same Channel as Resolution

Each object in the LHR has its own administrative control



Permission include:
- Public/Private Read
- Public/Private Write
- Public/Private Execute

Access control is done either with TLS authentication using public key/private key or by challenge/response based on a secret key.

In version 2.1 of the protocol, the client decide which hash function to use for challenge/response: MD5 or SHA-1.

JSON Admin REST API

DOA servers run a JSON/REST API on port 8000. Examples:

- GET /api/handles/{handle}
  Get specific handle

- PUT /api/handles/{handle}?index={index}
  Put specific indexed handle

- DELETE /api/handles/{handle}?index={index}
  Delete specific indexed handle

- GET /api/handles?prefix={prefix}
  List handles under prefix

Requests may be authenticated by sending an “authorization” header

Resolution /Proxy

Very few DOA clients exists, no DOA native support in browsers

Java client comes with DOA CRNI distribution

There is Firefox plug-in: hdl://11738/ithi

- actually not a native client, forward requests to a proxy
- will not work with next version of Firefox (v.53: API change)

Many applications use proxies:

DOIs are very often seen with a URL of a proxy:

https://hdl.handle.net/11738/ithi

In 2014, the American Psychological Association changed their cross-reference syntax recommendations from:

doi:10.1037/rmh0000008 to use the proxy form:

http://dx.doi.org/10.1037/rmh0000008

The use of proxies has privacy implications as the proxy logs contain user resolution history and the cache on the proxy contains resolved data.

Comparison of DOA and DNS

	DOA	DNS
Syntax	Dot-separated UTF-8 No length limitation	DNS-on-wire format DNS name format
Bits on Wire	UDP/TCP 2641, HTTP/HTTPS 8000	UDP/TCP port 53, DNS/TLS
Resolution	GHR LHR Replication Caching server Slicing	Root servers Authoritative servers Secondary servers Caching Resolvers Anycast
Data Administration	Per object	Per DNS zone
Data Management	In-band	Out-of-band
Data Objects	Extensible indexed types, predefined or opaque	Defined RR types TBD DOA RR type

Comparison of DOA and DNS: Security and Privacy

	DOA	DNS
Security/ Authentication	DOA clients can force servers to use MD5-based challenge-response authentication	
Automatic Key Rollover Mechanism	Not supported	RFC 5011 ICANN KSK rollover
Privacy	Relying on proxies creates a privacy concern. Deploying DOA clients is difficult. There are no native operating system or browser implementations. Deployment of clients is further hindered by the key rollover issues mentioned above.	Recursive resolvers share the same privacy issues as proxies. However, privacy-conscious users may opt to run their own resolvers.

Comparison of DOA and DNS: Governance

	DOA	DNS
Registration	MPAs	Registries and registrars
Protocol Extensions	DONA	IETF
Policy Development	DONA	ICANN
Operation	DONA/CNRI/MPAs	Root, TLD, and resolver operators

More Information

Handle System: http://www.handle.net
DONA foundation:http://www.dona.net