Case-sensitivity in BIND and DNS

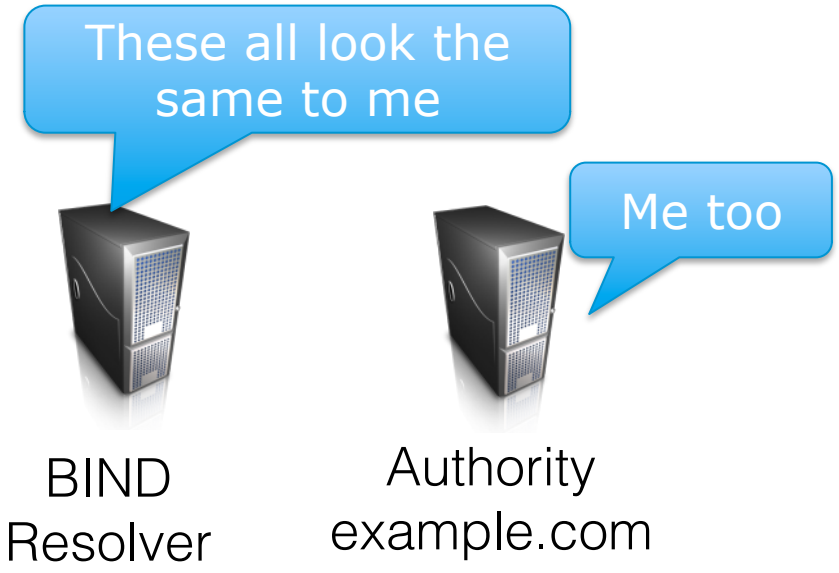
DNS-OARC October 2014

Vicky Risk and Evan Hunt, ISC

Background

In DNS, a request for any of these domains should be treated the same by a responder

- www.isc.org
- WWW.ISC.ORG
- WwW.iSc.oRg
- wWw.IsC.OrG



However

- The Requestor may consider them to be different questions
- The Requestor may even randomize the case in their question

  - ~~www.isc.org~~
  - ~~WWW.ISC.ORG~~
  - ~~WwW.iSc.oRg~~
  - wWw.IsC.OrG

User

Casing adds identity to the query

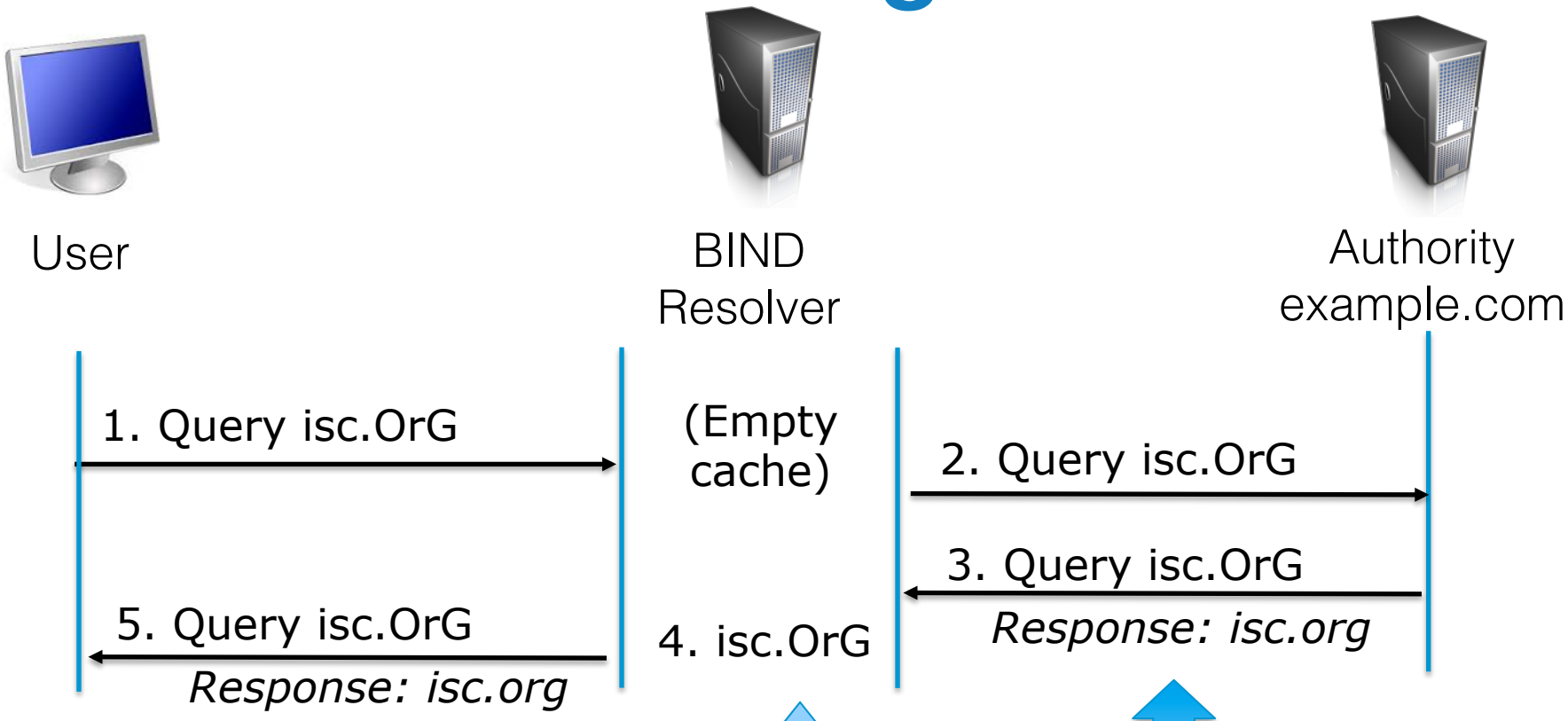
"Use of Bit 0x20 in DNS Labels to Improve Transaction Identity"
draft-vixie-dnsext-dns0x20-00.txt

- Using the case of the query adds another degree of entropy to make it more difficult to spoof a query
- Value coming back in the question section has to be in the same case as it was originally asked

What is the problem?

- Requestor may care about casing
- Resolver and authoritative servers don’t care about casing
- Resolver and authoritative servers may modify the casing inadvertently through
  1. Packet Compression
  2. Caching choices

Where is casing altered?



Compression

- We use compression (de-duplication) by default in BIND, although this is configurable
- Since they are the same domain, we only want a single label in the packet
- So, we ‘compress’ multiple instances to a common label (which could be any of these)

Case-insensitive Compression

Doesn't consider the case of the letters when looking for common suffixes

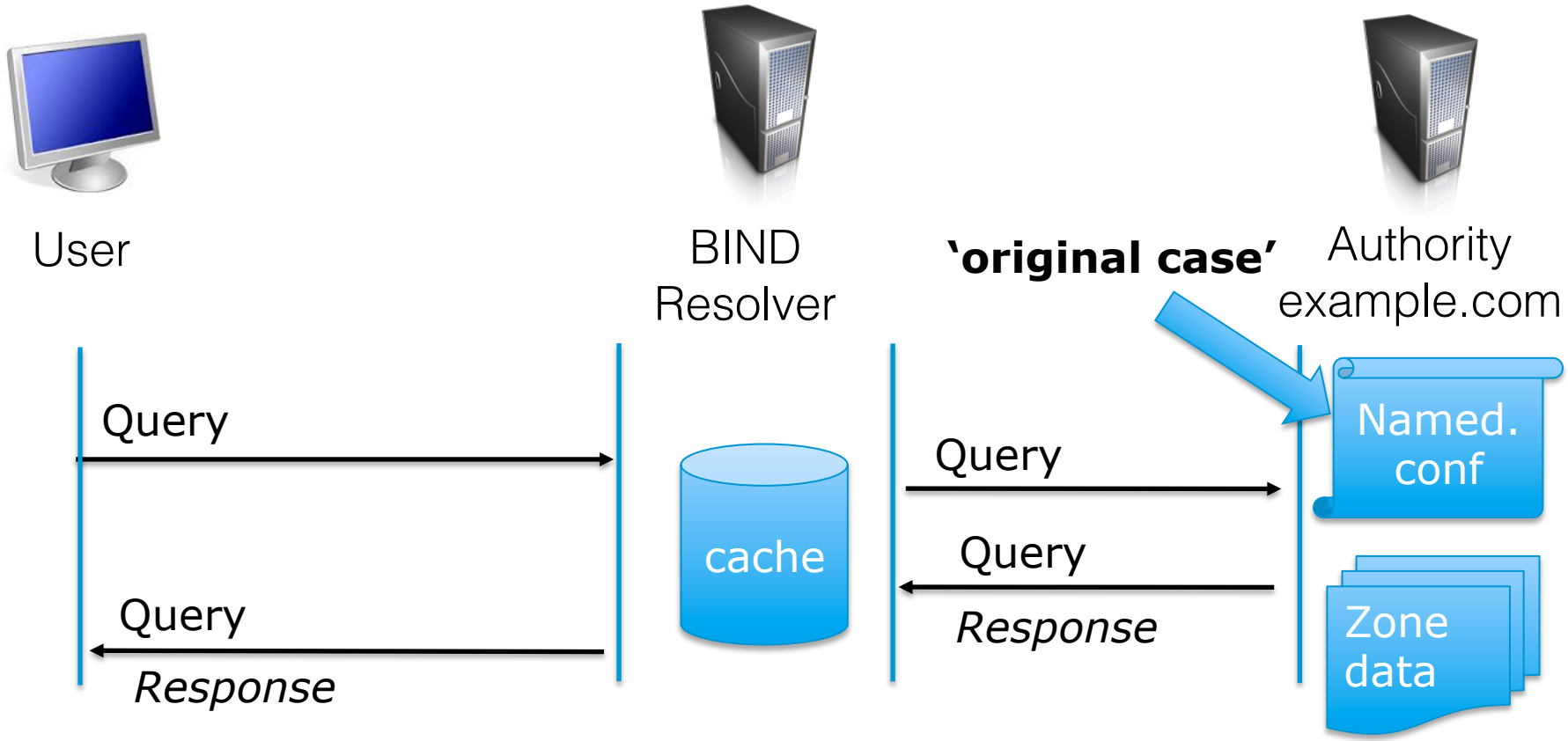
- When you have a common suffix, refer back to the first instance instead of repeating it
- The first occurrence is likely to be a **client query, not an authoritative response, or data in the cache**

RFC 1035

§2.3.3 - "Character Case"

When data enters the domain system, its original case should be preserved whenever possible. *In certain circumstances this cannot be done. For example, if two RRs are stored in a database, one at x.y and one at X.Y, they are actually stored at the same place in the database, and hence only one casing would be preserved. The basic rule is that case can be discarded only when data is used to define structure in a database, and two names are identical when compared in a case insensitive manner.*

When does data enter the system?



What should we do …

- We looked at the RFC
  - It seemed we were non-compliant
- We consulted with all the major operating system packagers of BIND
  - They agreed, we should change
- We changed BIND behavior

New BIND Behavior

- Compression when answering queries is **case-sensitive**
- This change went into 9.6-ESV-R11,9.8.7,9.9.5,9.9.5(sub) & 9.10.0
- Query is saved in the cache in the case it was **answered** in – as it always was, but now, the case of the answer may be different from the case of the question

Result

- So far, we have had two support cases related to this
- These were clients that incorrectly cared about the case of the ANSWER
- In one case, an enterprise network saw a widespread phone outage due to unexpected casing

PS.

- We have since added an ACL to make it possible to revert to the old behavior, if necessary
- This feature is in BIND 9.10, 9.8.6 and 9.8.8

Impact on the DNS

- As BIND authoritative systems and caching resolvers are updated, gradually, the DNS will see changes in case preservation
  - Through (compressed) authoritative responses
  - Through responses from cache
- Possible compatibility impacts

Other things we could do

To minimize the impact on clients that incorrectly care about the case of the **ANSWER**

- Lower case all upstream queries.
- This prevents camel case making its way through to the authoritative servers and back into the cache from non case preserving authoritative servers.
- Lower case is also the most common way records are published and looked up. This minimises the impact on broken clients.
- We probably will do this.

Survey of DNS servers

Server	version	Behavior
NSD	3.2	Case-insensitive
NSD	4.0	Case-insensitive
Knot	1.4rc1	(encountered a known bug)
PowerDNS	3.2	Case-insensitive
Yadifa	1.0.3	Case-insensitive
Microsoft.net	?	Case-insensitive
Nominum.com	?	Case-insensitive
BIND	<change	Case-insensitive

http://workbench.sidnlabs.nl/

References

- RFC 1035, see section 2.3.3
  https://datatracker.ietf.org/doc/rfc1035/
- Expired draft on using casing to add identity to queries
  http://tools.ietf.org/id/draft-vixie-dnsext-dns0x20-00.txt
- Source.isc.org, commit# 3645
- https://kb.isc.org/article/AA-01113/0/