NANOG 62 - 6 October 2014

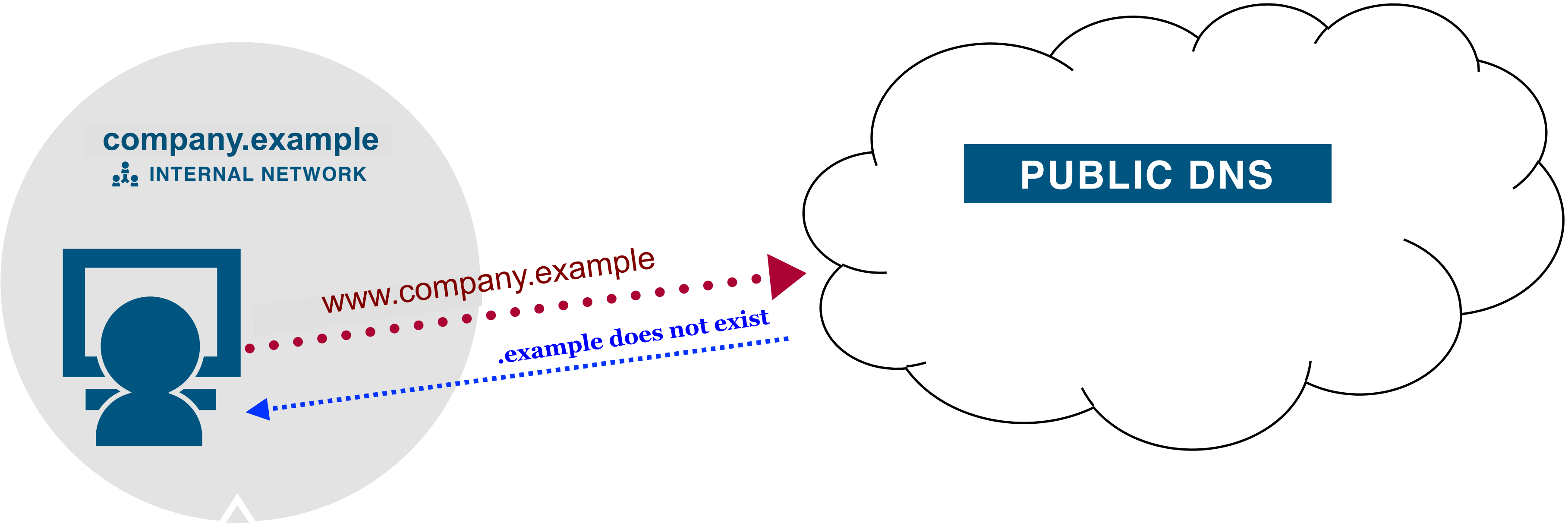
ICANN's Name Collision Controlled Interruption

Edward Lewis
Technical Services
ICANN

Agenda

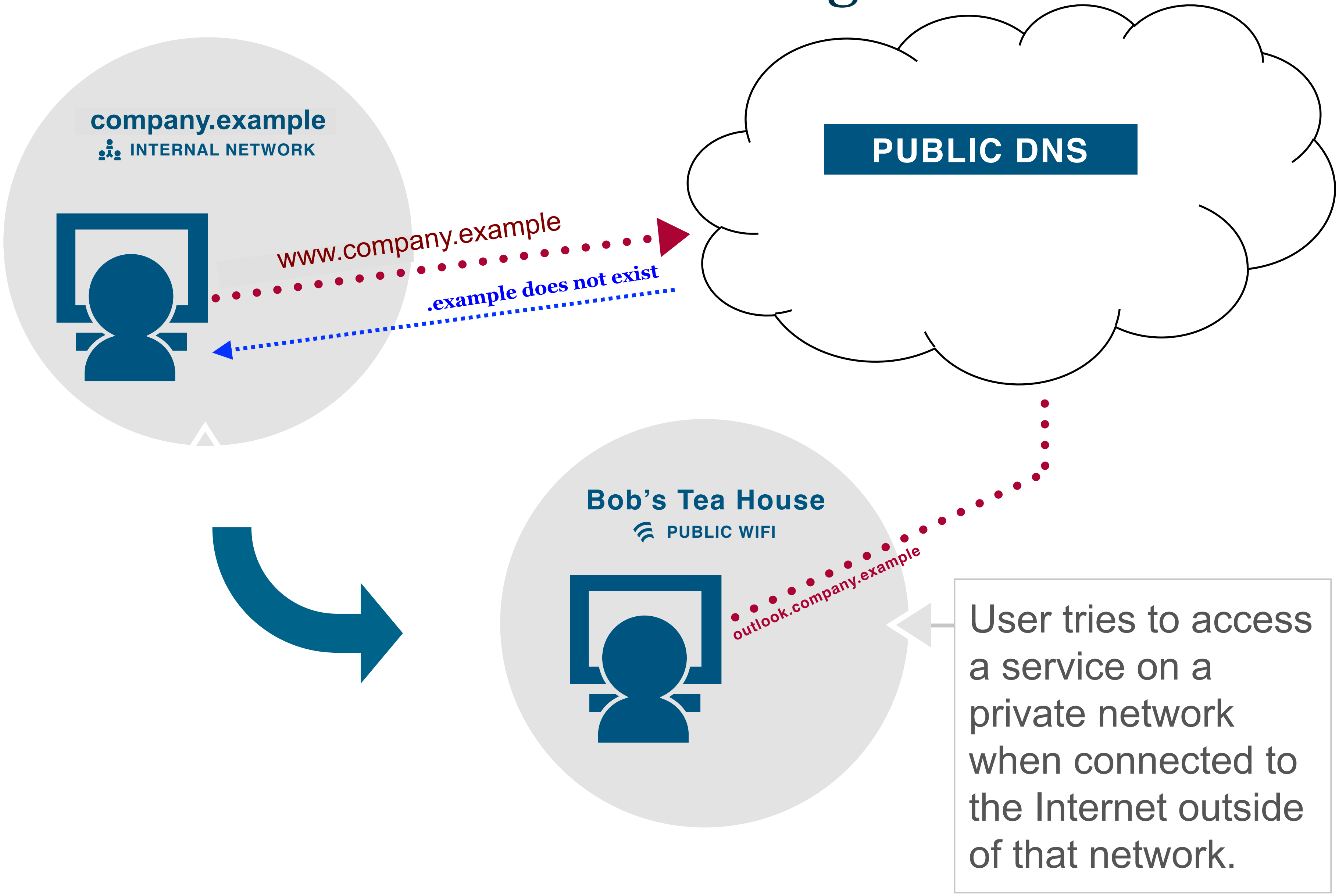
- Name Collisions
- Controlled Interruption
- Check Your Logs/Intrusion Detection Systems
- Where to Get Help

Name Collision – The Leak



Private network configured in such a way that could “leak” the request to the public Domain Name System, when using a name in a private network that *does not exist* in the public DNS

Name Collision – The Roaming Leak

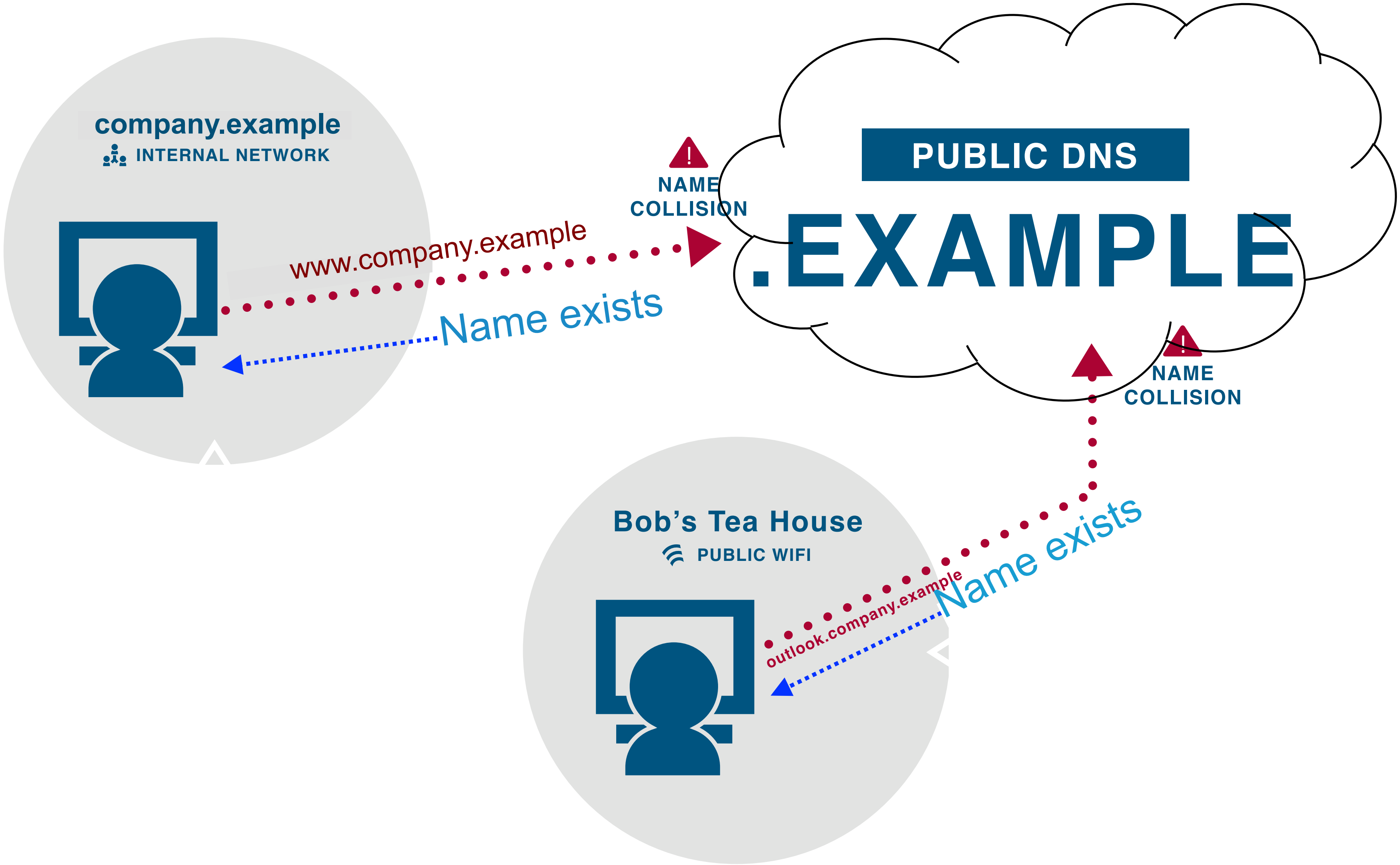


User tries to access a service on a private network when connected to the Internet outside of that network.

Why Does This Happen?

- Local DNS Name spaces
  - Use of “adopted” names, from documentation
  - Split-brain DNS
- Search List Processing
  - Use of short unqualified domain names
  - Falling back on DNS lookup failure

Name Collision – The “Crunch”



As New Top-Level Domains are Added

- Once-failing names might “succeed”
  - The name to address result may be different

- Operational Interruption
  - At best, updates are needed
  - At worst, data and information may be leaked

How to Avoid Interruption

- Pre-emptive strike
  - Use only Fully Qualified Domain Names
  - Avoid or limit reliance on search lists
  - Use globally-recognized registered names
  - Deterministic - good!
- But you may not catch all the places where short, unqualified domain names have been used

Controlled Interruption

- When a new top-level domain opens
  - A set of responses are returned to names that might be subjects of collision
  - Designed to be a nuisance to those leaking queries
  - Designed to contain the damage of a data breach
- “Breadcrumbs” left in
  - Logs (of connection failures)
  - Intrusion Detection Systems (suspicious addressing)

127.0.53.53

- A “curious” loopback address
  - Meant to make connections fail, no data sent out
  - Meant to encourage operators to “look this up”
- Other clues that fixes are needed
  - Mail server (MX) is “**your-dns-needs-immediate-attention**”
  - SRV lookup returns that same hostname
  - TXT record says “**Your DNS configuration needs immediate attention**”

What to Do?

- If there is a reasonable belief of demonstrable, severe harm, report it to ICANN
  - https://forms.icann.org/en/help/name-collision/report-problems
- For further information, consult
  - https://www.icann.org/en/system/files/files/name-collision-mitigation-01aug14-en.pdf
- Or
  - https://www.icann.org/resources/pages/name-collision-2013-12-06-en

Q&A

- The URL for the Mitigation Guide, once again:
  - https://www.icann.org/en/system/files/files/name-collision-mitigation-01aug14-en.pdf

- Want to know “what’s coming”?
  - https://newgtlds.icann.org/newgtlds.csv
  - Includes TLD name, contract date, delegation date

Social Media

https://twitter.com/ICANN

http://gplus.to/icann

https://www.facebook.com/icannorg

http://weibo.com/icannorg

http://www.linkedin.com/company/icann