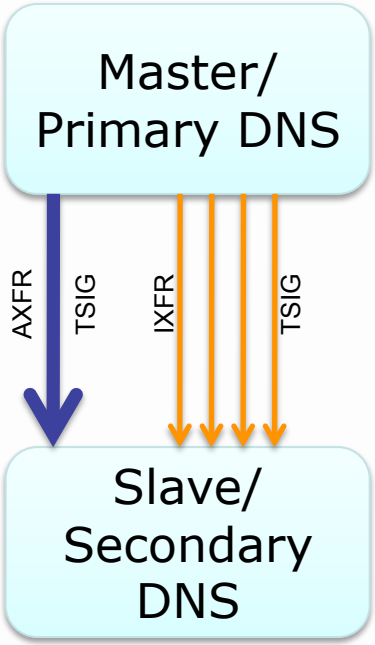
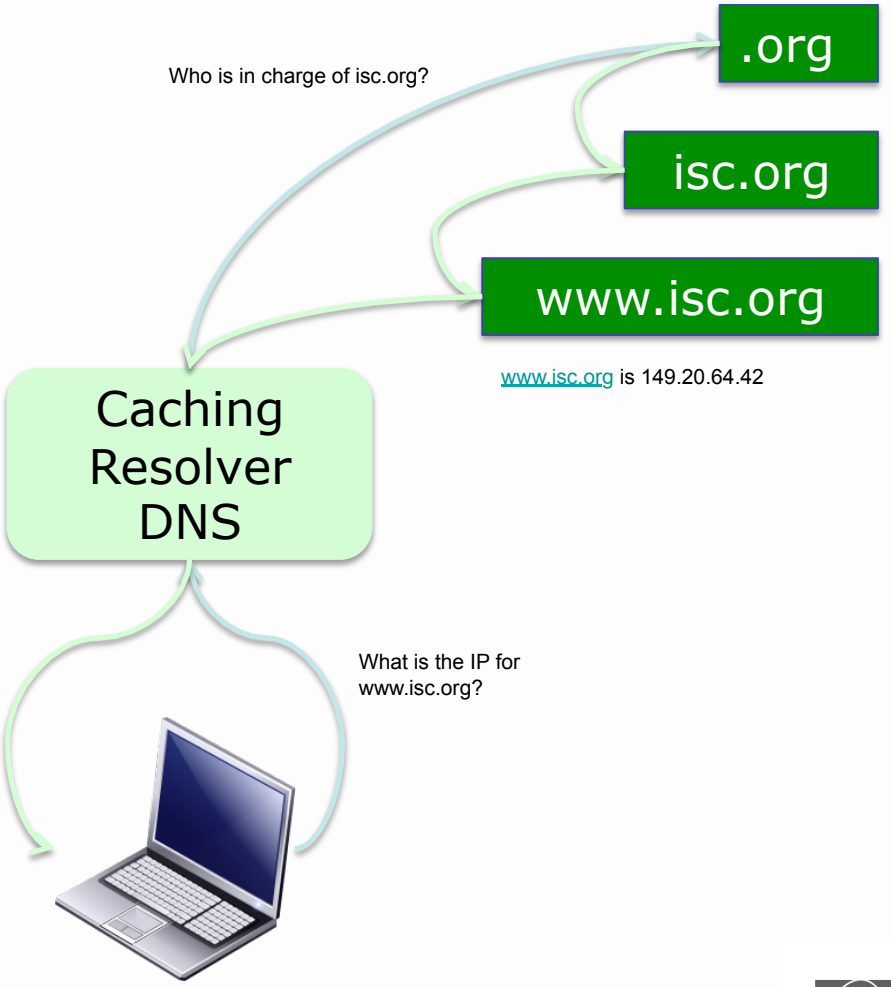
DNS Response Policy Zone (DNS RPZ)

DNS Response Policy Zone (DNS RPZ)

- DNS RPZ is *policy information* inside a specially constructed DNS zone.
- This enables DNS reputation data producers and consumers to cooperate in the application of such policy to real time DNS responses.
- DNS RPZ turns the *recursive DNS server* into a security hammer …
  - Provide the same capabilities of an anti-spam DNSBL (DNS Block List, ne RBL) and RHSBL (Right Hand Side Block List)….
  - … with greater degrees of scaling and speed.

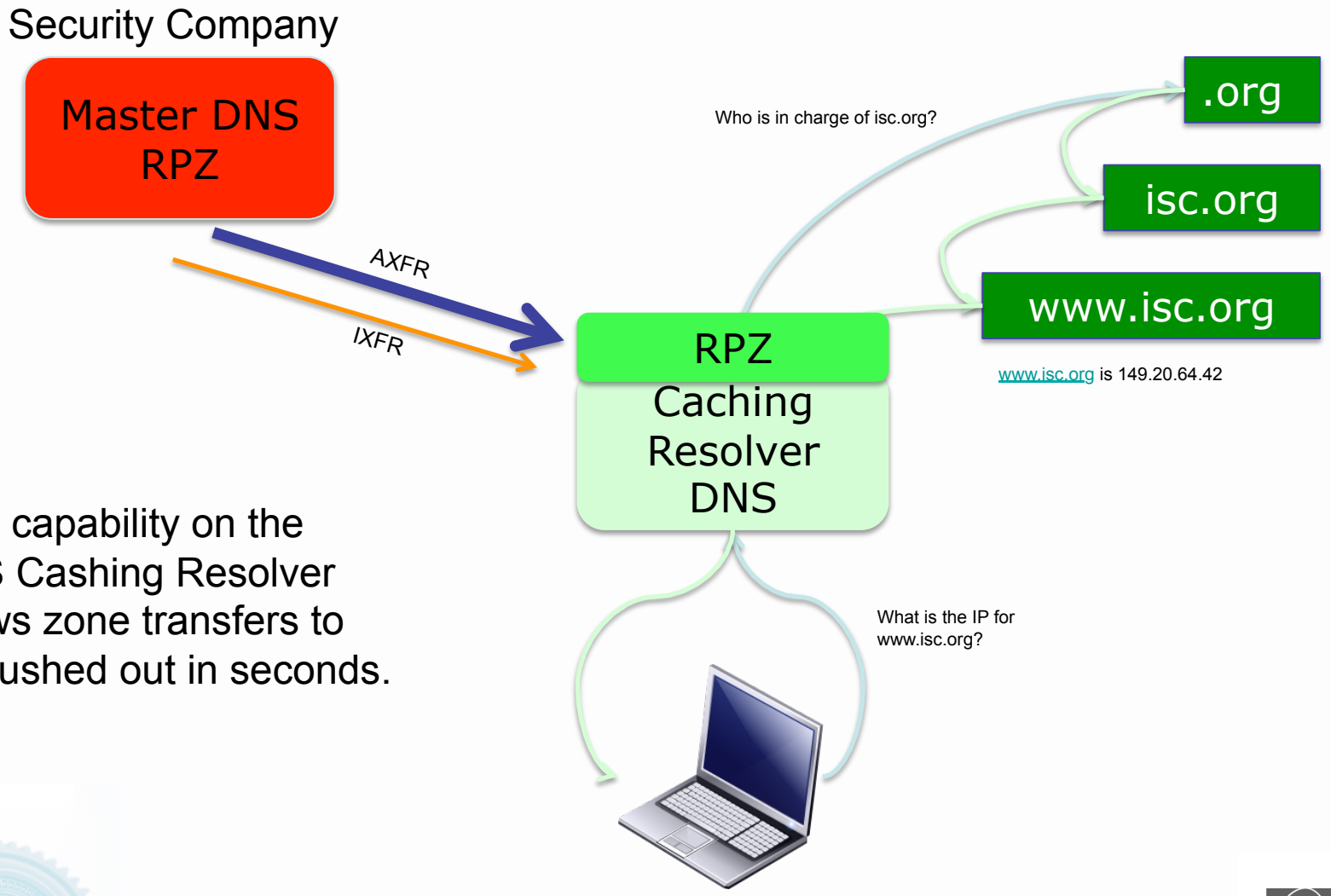
Core DNS Principles





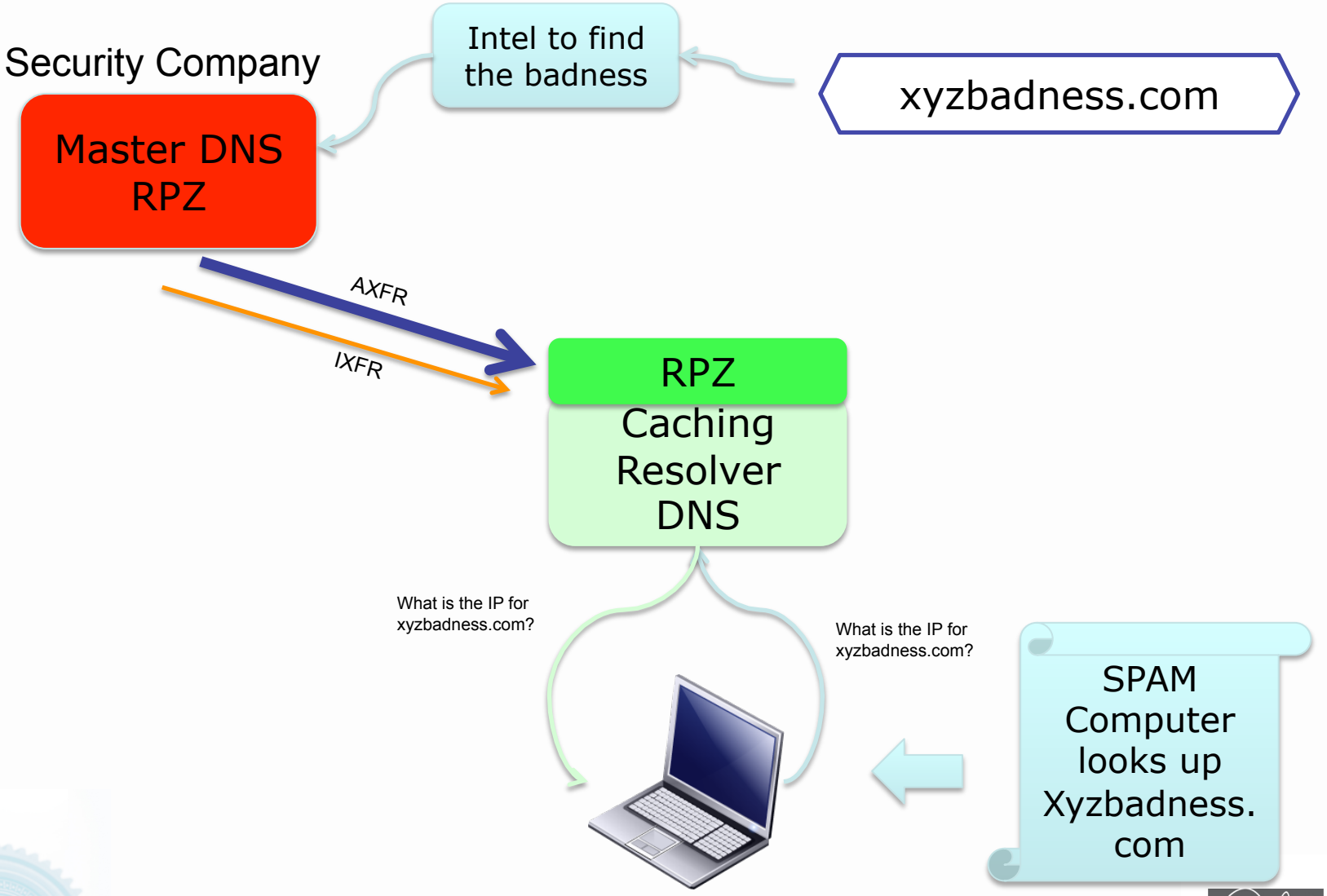
AXFR - Full Zone Transfers
IXFR - Incremental Zone Transfers
TSIG - **Transaction SIGnature**
used to secure the AXFR/IXFR

DNS RPZ



RPZ capability on the DNS Cashing Resolver allows zone transfers to be pushed out in seconds.

DNS RPZ in Action



Possible DNS RPZ Uses

- Block or redirect malicious drop sites (DNS used by URLs)
- Block ability of C&C to find its way back using DNS
- Walled garden notification for infected clients
- Services that use PTR lookups (IP reputation can map into here)

DNS RPZ & SURBL

SURBL DATASHEET

- What is SURBL RPZ?
  - SURBL RPZ is a version of SURBL's high-quality anti-spam, anti-phishing and anti-malware data in the form of a DNS Response Policy Zone (DNS RPZ). DNS RPZs are used to deny or modify the resolution of low-reputation domains, in other words, to deny DNS services for known-bad domains. SURBL is the world's first provider of RPZ data.
- Why use SURBL RPZ?
  - SURBL RPZ data are typically used to protect users from visiting objectionable or dangerous spam, phishing or malware web sites. Doing so can prevent identity theft, phishing attacks, malware infection, loss of revenue due to visiting objectionable spam sites, and more. This is made possible by SURBL's highly-regarded, multi-sourced, real-time intelligence about such domains.
- How to use SURBL RPZ
  - SURBL RPZ is available via DNS zone transfer using recent versions of BIND 9. Local SURBL RPZ queries are answered by your local BIND recursive nameserver where they can be used to deny resolution (NXDOMAIN is the default behavior) or to send traffic to a local walled garden for example, instead of allowing the successful resolution known-bad domains. Other RPZ-supported behaviors are available by modifying the response values as needed in your operational environment. SURBL RPZ data are available by private incremental zone transfer.

- **Please contact us using the Data Feed Request form on our web site www.surbl.org in order to arrange access, or call Arnie Bjorklund 866-931-9228 x237, arnieb@mxtools.com**

ISC

DNS RPZ Uptake/Concerns?

- Pre-announced to usual DNSBL suspects – positive feedback
- Administrators can manage their own local RPZ and combine it with other zone feeds.
- New markets & ecosystem for security vendors.
- Are we teaching bad guys to not use DNS?

ISC's Role with DNS RPZ

- ISC has three roles with DNS RPZ as a new "hammer" in our security toolkit:
  - Code and Functionality in BIND & working with all DNS Recursive Resolver Software Vendors to insure everyone is adopting the same formats.
  - Work with all potential Black List Providers.
  - Work with Operators on DNS RPZ Deployment.
- ISC will NOT be providing any black list capacities. Our role is to help design, build, and deploy the "hammer" as a new tool in our security toolkit.

Links

- Discussion List
  - https://lists.isc.org/mailman/listinfo/dnsrpz-interest
- Taking back the DNS, Paul Vixie, 29th July 2010
  - http://www.isc.org/community/blog/201007/taking-back-dns-0
- Google “taking back the dns”
- Draft Specification
  - ftp://ftp.isc.org/isc/dnsrpz/isc-tn-2010-1.txt
- BIND 9.8
  - ftp://ftp.isc.org/isc/bind9/9.8.0/