DNS - Software Compliance

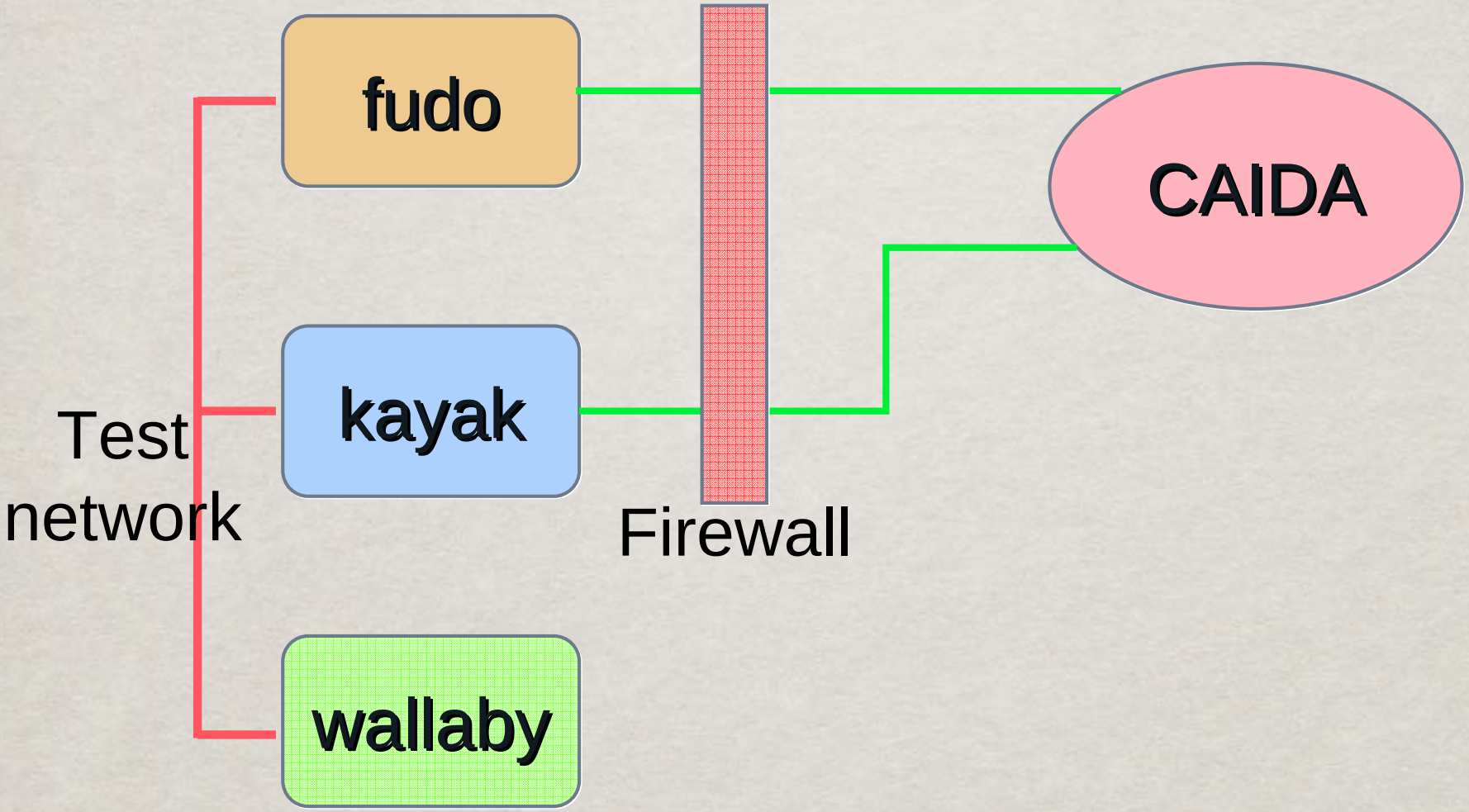
Ritesh Kumar
David Moore
Colleen Shannon

- Critical Distributed Infrastructure
  - Motivation for interoperability
- New standards: ipv6, DNS SEC
- Motivates: DNS software compliance test.

Test Methodology

- Scope: Test recursive resolvers only
- Method: Like Software testing
- Pros:
  - Lots of control (ipv6 roots)
- Cons:
  - No statement about current deployment

The Setup



- FreeBSD 4.8 / BIND 9
- Shell scripts for configs and launch
- Non-recursive DNS servers
  - root servers / top level domains
  - test servers

fudo

- FreeBSD 4.8 / BIND 4 / 8 / 9 and djbdns
- Recursive and caching resolvers
- Perl + sh scripts for tests and launch
- Easy to add tests and recursive resolvers
- Test summaries

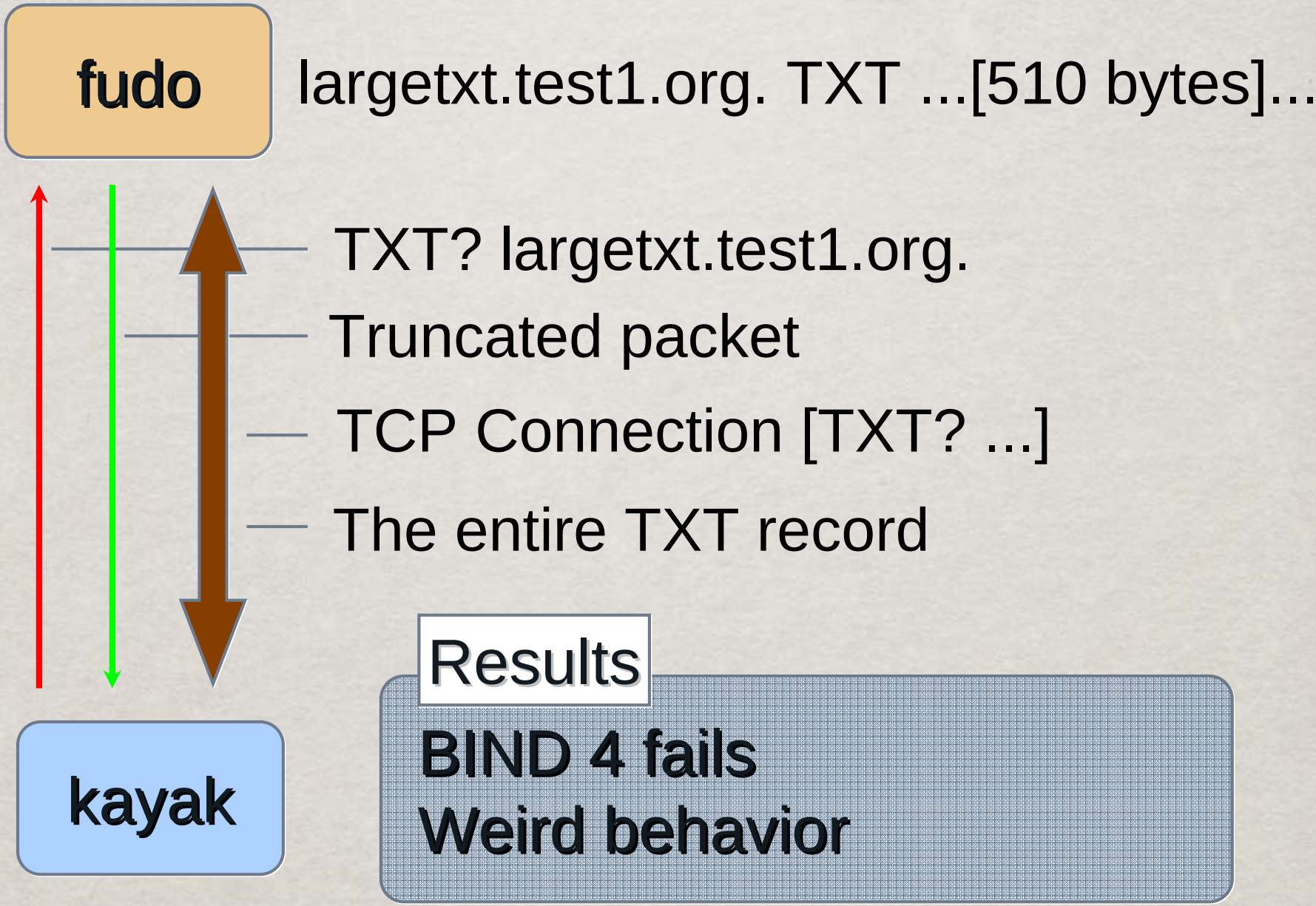
kayak

- Windows (NT?) / 2000 / XP / XP-SP2
- To do: Port test scripts

wallaby

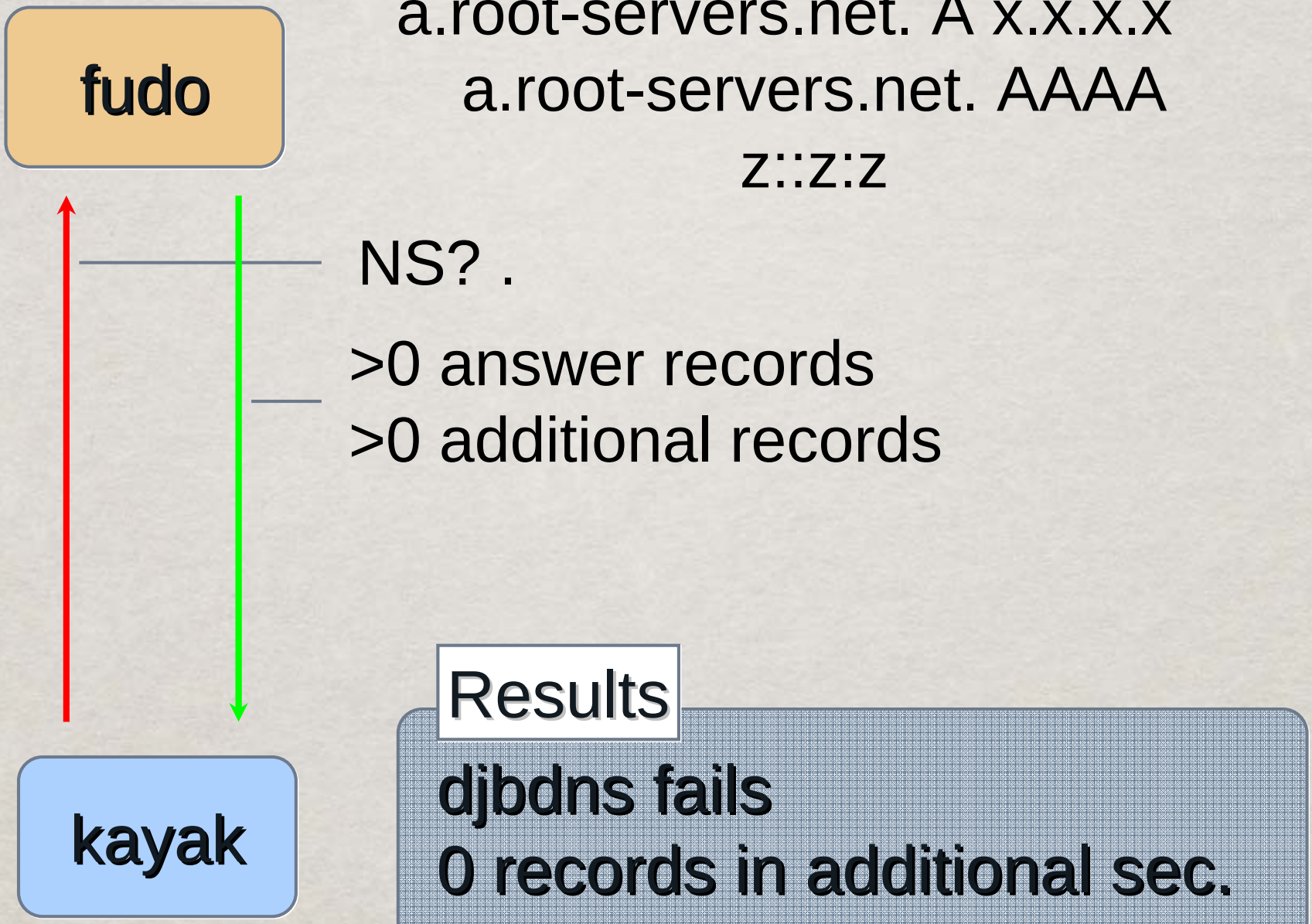
Tests

- TCP fallback
- IPv6 - IPv4 coexist test
- IPv6 only test
- Poisoning test


fudo
largetxt.test1.org. TXT ...[510 bytes]...
TXT? largetxt.test1.org.
Truncated packet
TCP Connection [TXT? ...]
The entire TXT record
kayak
Results
BIND 4 fails
Weird behavior

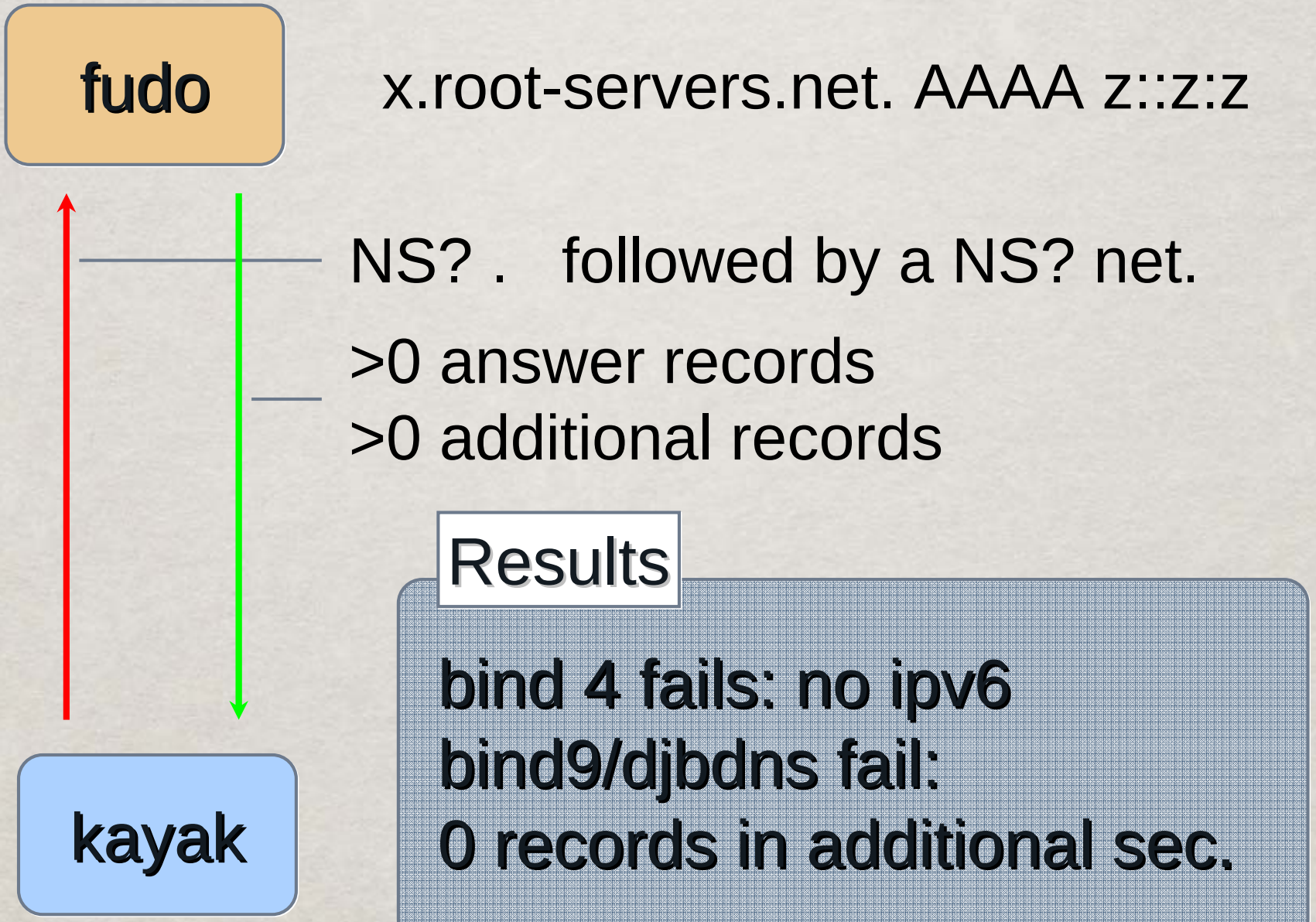
Tests

- TCP fallback
- IPv6 - IPv4 coexist test
- IPv6 only test
- Poisoning test


fudo
a.root-servers.net. A x.x.x.x
a.root-servers.net. AAAA
z::z:z
NS? .
>0 answer records
>0 additional records
kayak
Results
djbdns fails
0 records in additional sec.

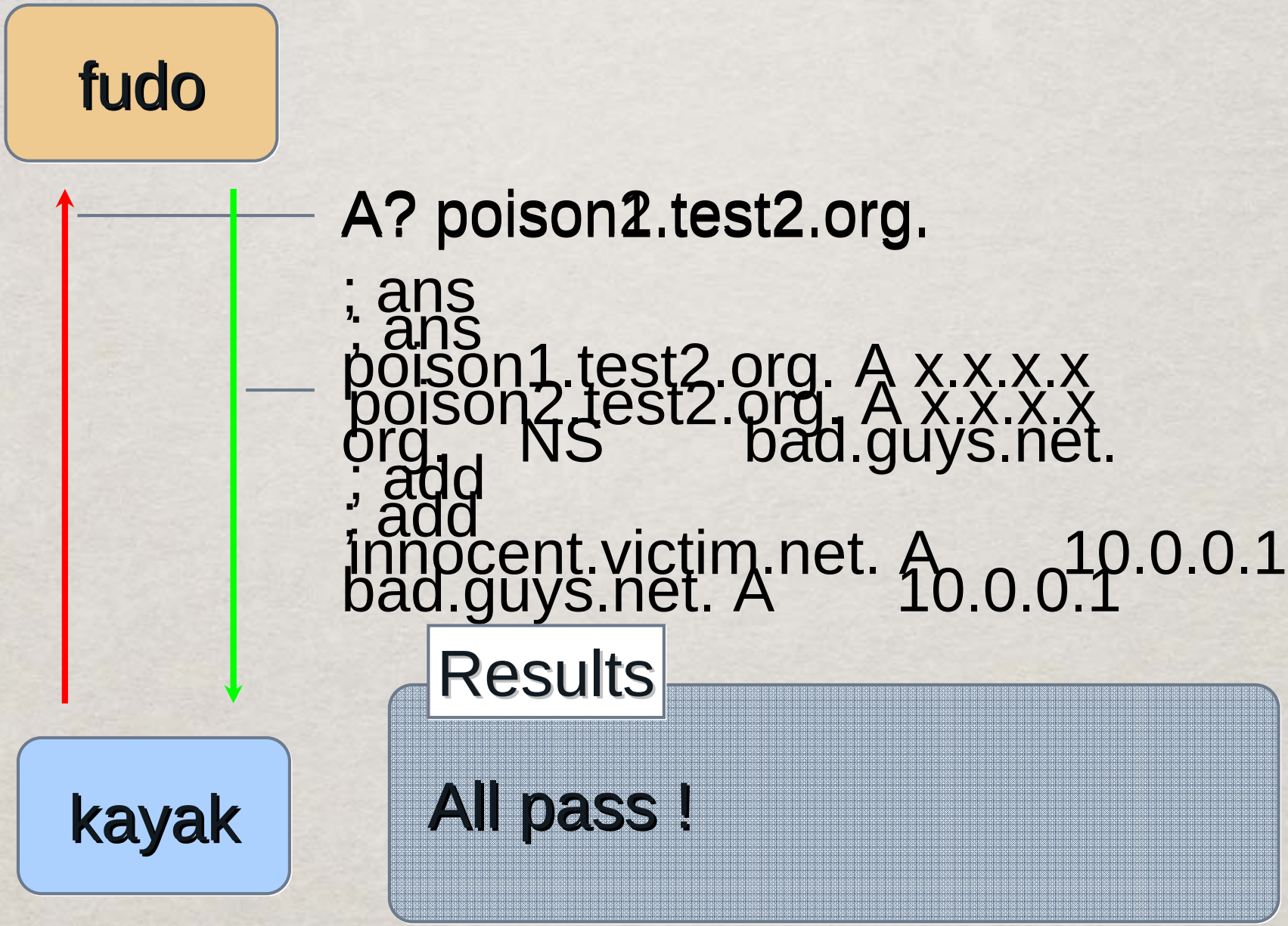
Tests

- TCP fallback
- IPv6 - IPv4 coexist test
- IPv6 only test
- Poisoning test


fudo
x.root-servers.net. AAAA z::z:z
NS? . followed by a NS? net.
>0 answer records
>0 additional records
Results
bind 4 fails: no ipv6
bind9/djbdns fail:
0 records in additional sec.
kayak

Tests

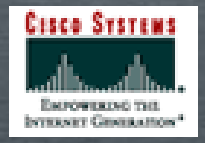
- TCP fallback
- IPv6 - IPv4 coexist test
- IPv6 only test
- Poisoning test


fudo
A? poison1.test2.org.
; ans
poison1.test2.org. A x.x.x.x
; add
innocent.victim.net. A 10.0.0.1
kayak
Results
All pass !

DNS-OARC

&

1st DNS-OARC WOrkshop



- DNS - Operations, Analysis, and Research Center

- Common platform for DNS operators
  - Share information (attack characteristics)
  - Measurement studies and tests
  - Analysis and Outreach

- ISC and CAIDA are (seriously) involved

Why?

- DNS is critical
- DNS is **not** secure (yet)
- Attacks on DNS are growing
- Study of newer techniques like Anycast

Topics Discussed

- Governance, Internet and naming
- DNS measurements
- DNS security

Internet Governance

- ICANN/IANA, UN/ITU and US DoC
  - Internet vs Telecommunications
- Motivation for Network Researchers to
  - Spread education
  - Provide guidance to policy making
- Working Group on Internet Governance
  - http://www.wgig.org/

DNS Measurements

- Tools for secure statistics collection
- RFC1918 updates
- Effect of Anycast deployment
  - Is localization working?
- Stats on Poisoning

DNS Security

- DLV (DNSSEC Lookaside Validation)
- Instead of tracking bots, track botnets
- Population model study of botnets
- KarstNet: A method of “sinking“ botnets
- Real botnet sizes look staggering

Thanks!

http://oarc.isc.org/