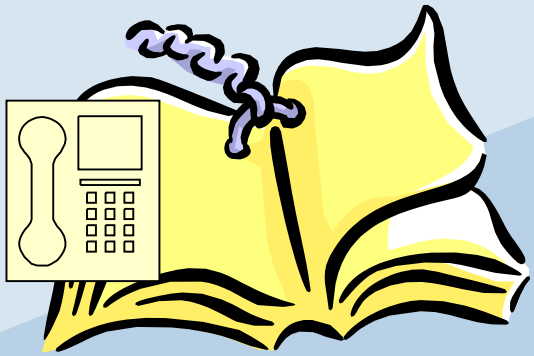
DNS and DNS Security 101

What is DNS?

The DNS is Often Compared to a Telephone Book



The World's Network – the Domain Name System

- Internet Protocol numbers are unique addresses that allow computers to find one another
- The Domain Name System matches IP numbers with a name
- DNS is the underpinning of unified Internet
- DNS keeps Internet secure, stable and interoperable
- ICANN was formed in 1998 to coordinate DNS

Domain Name System

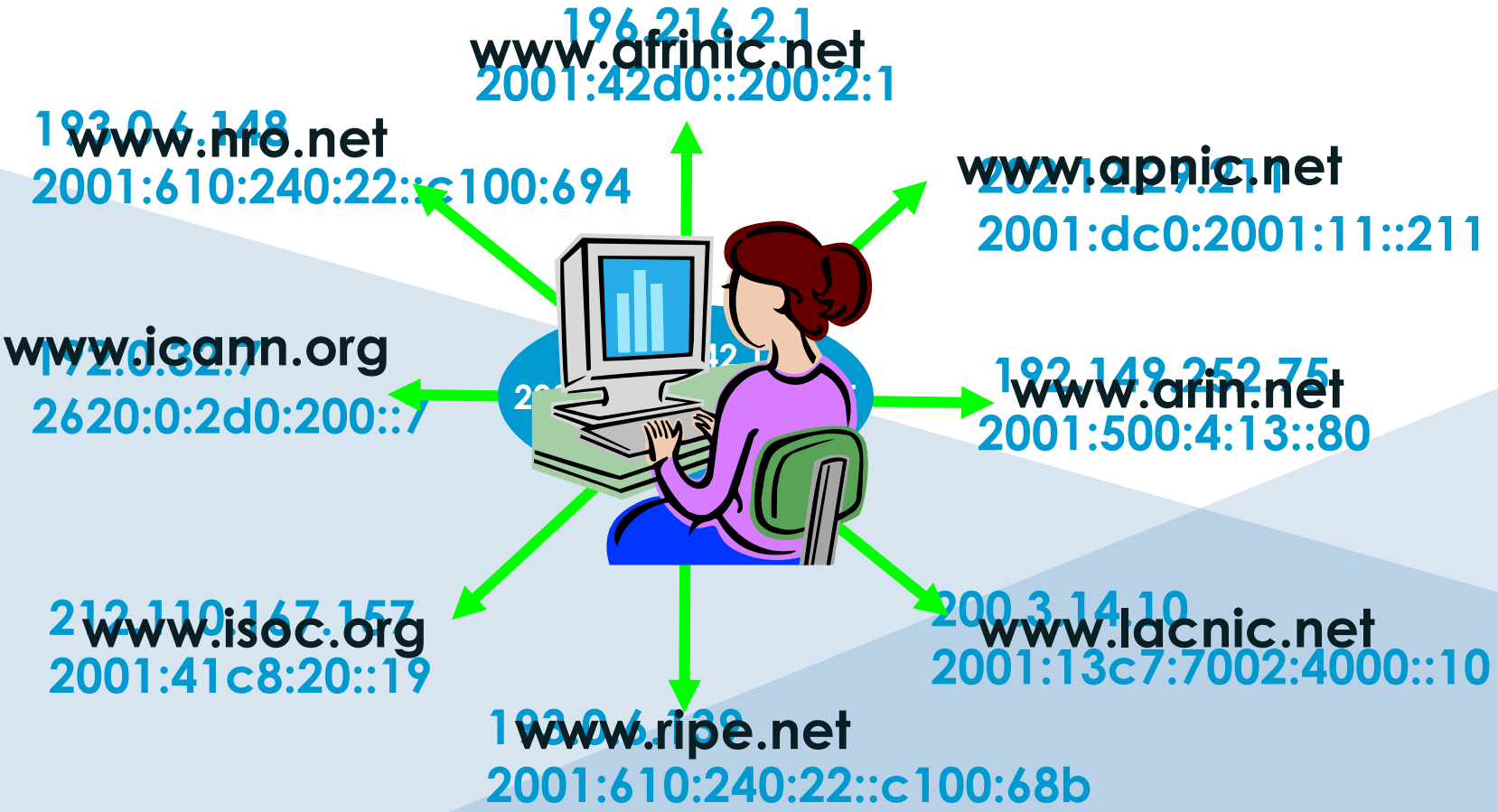
A distributed database primarily used to obtain the

IP address, a number, e.g.,
192.168.23.1 or fe80::226:bbff:fe11:5b32

that is associated with a

user-friendly name (www.example.com)

Names – Easier way for humans



History

1983 DNS was designed/invented by Paul Mockapetris (RFC882 & 883)

1984 Berkeley Internet Name Domain (BIND) Server developed
Original Seven Generic TLDs (.com, .edu, .gov, .int, .mil, .net, and .org)

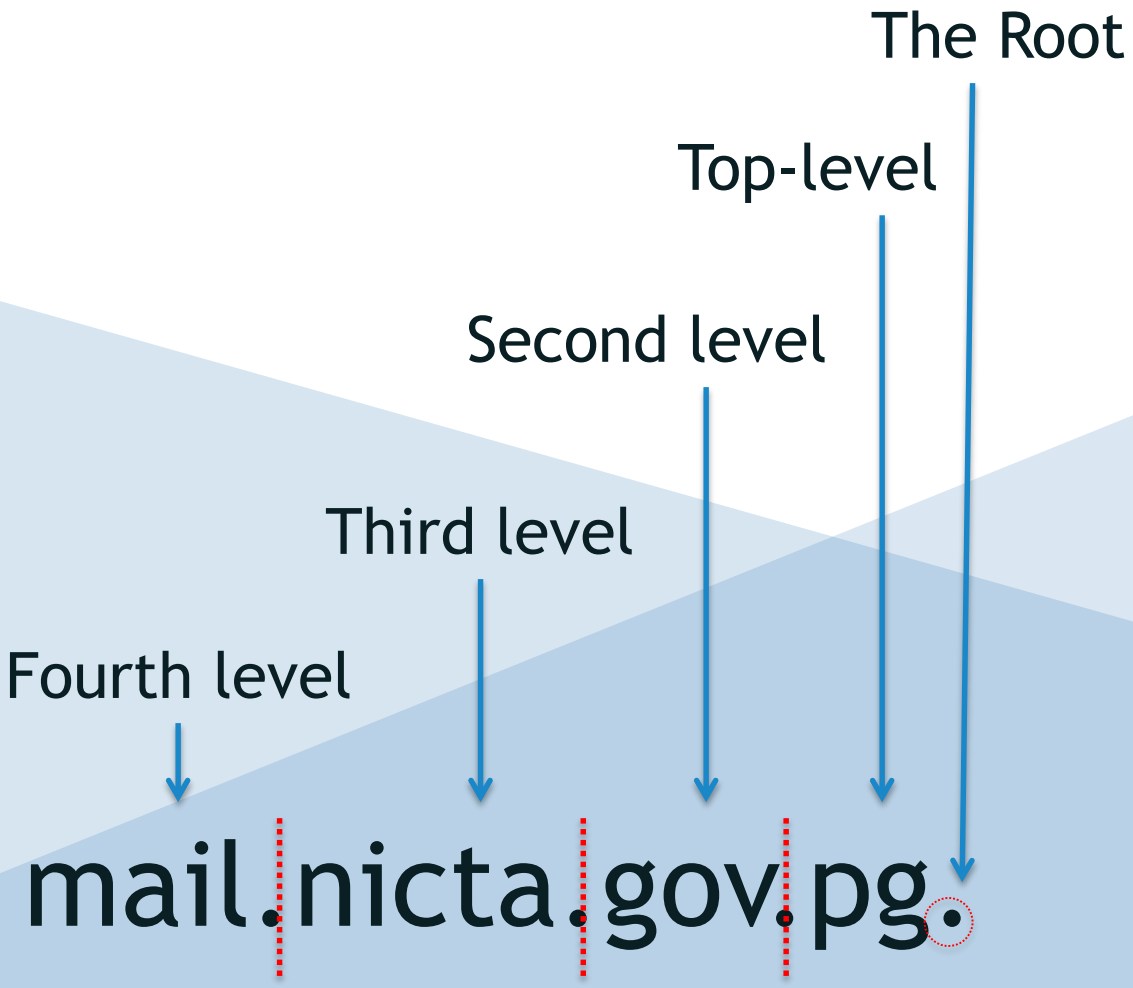
1985 First country codes assigned .us, .uk, and .il
1986 .au, .de, .fi, .fr, .jp, .kr, .nl and .se
1987 RFC1034 (Considered the first full DNS Specification)

…….. Country Code TLDs continue to be added….

2000 Seven new TLDs added (.aero, .coop, .museum, .biz, .info, .name, and .pro)

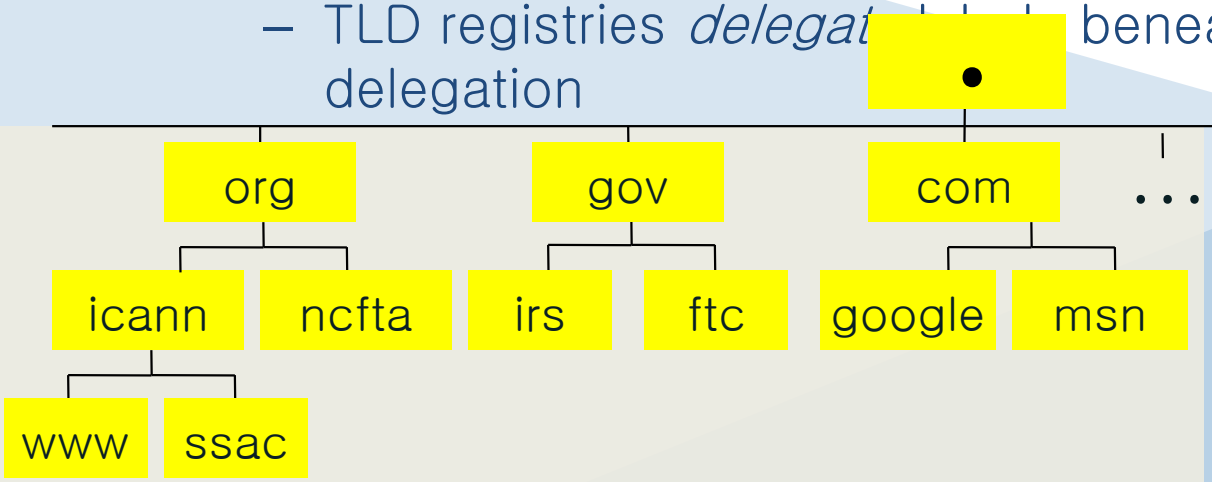
2012 New round of applications for gTLDs opened by ICANN

Domain Name's Structure

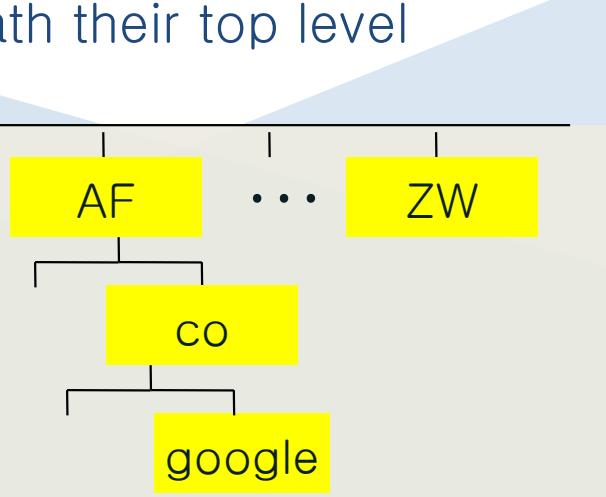


DNS Structure

- A **domain** is a node in the Internet name space
  - A domain includes all its descendants
- Domains have names
  - Top-level domain (TLD) names are generic or country-specific
  - TLD *registries* administer domains in the top-level
  - TLD registries *delegat* beneath their top level delegation

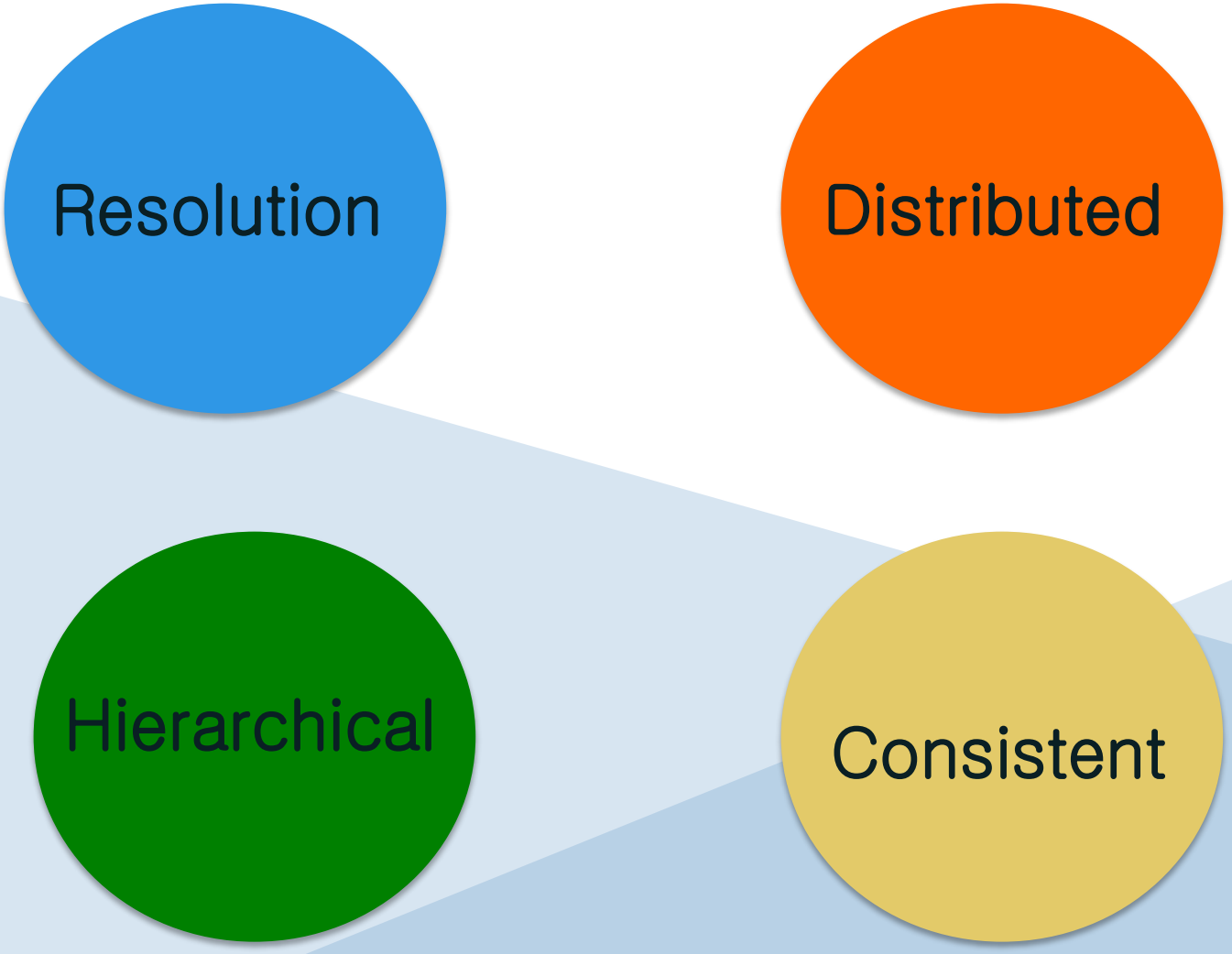


Names in generic Top Level Domains

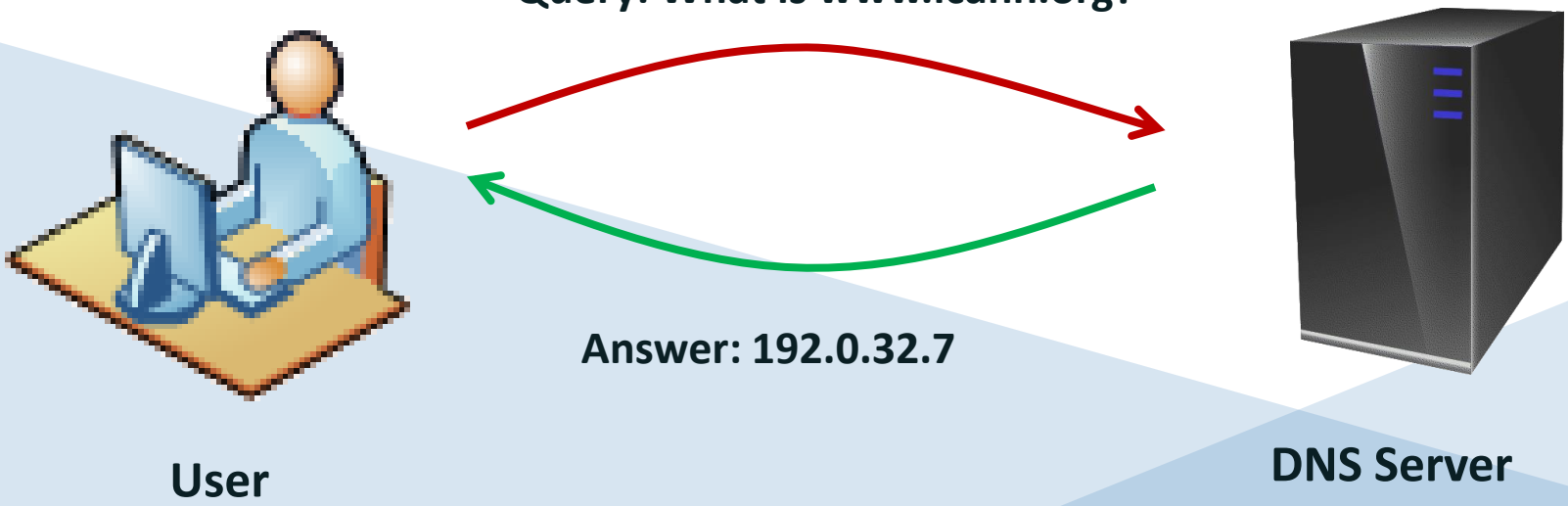


Names in country-code TLDs

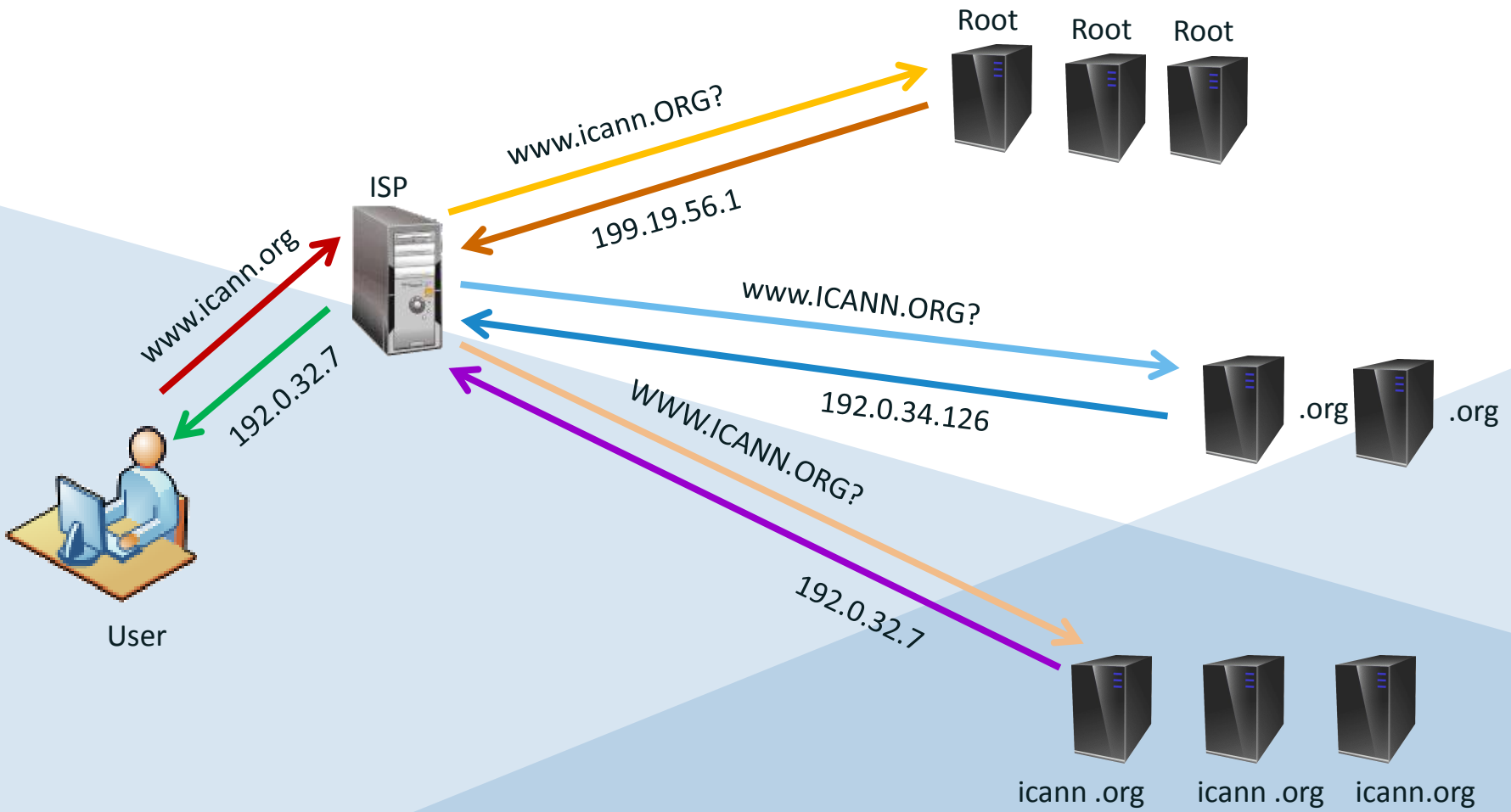
Key Elements of DNS



DNS Operation



DNS Operation



DNS Servers

- Root Servers
- DNS Authoritative
  - Primary
  - Secondary
- DNS Resolver
  - Recursive
  - Cache
  - Stub resolver

What do the Root-Server Operators do?

- Copy a very small database, the content of which is currently decided by IANA
- Put that database in the servers called ‘Root Servers.
- Make the data available to all Internet users
- Work stems from a common agreement about the technical basis
  - Everyone on the Internet should have equal access to the data
  - The entire root system should be as stable and responsive as possible

What do the Root-Server Operators do not do?

- Interfere with the content of the database
  - E.g. run the printing presses, but don't write the book
- Make policy decisions
  - Who runs TLDs, or which domains are in them
  - What systems TLDs use, or how they are connected to the Internet

How Secure are the Root Servers?

- Physically protected
- Tested operational procedures
- Experienced, professional, trusted staff
- Defense against major operational threat – i.e. DDoS.
  - Anycast
    - Setting up identical copies of existing servers
    - Same IP address
    - Exactly the same data.
    - Standard Internet routing will bring the queries to the nearest server
    - Provides better service to more users.

Root Server Map

Root Server Operation @ICANN

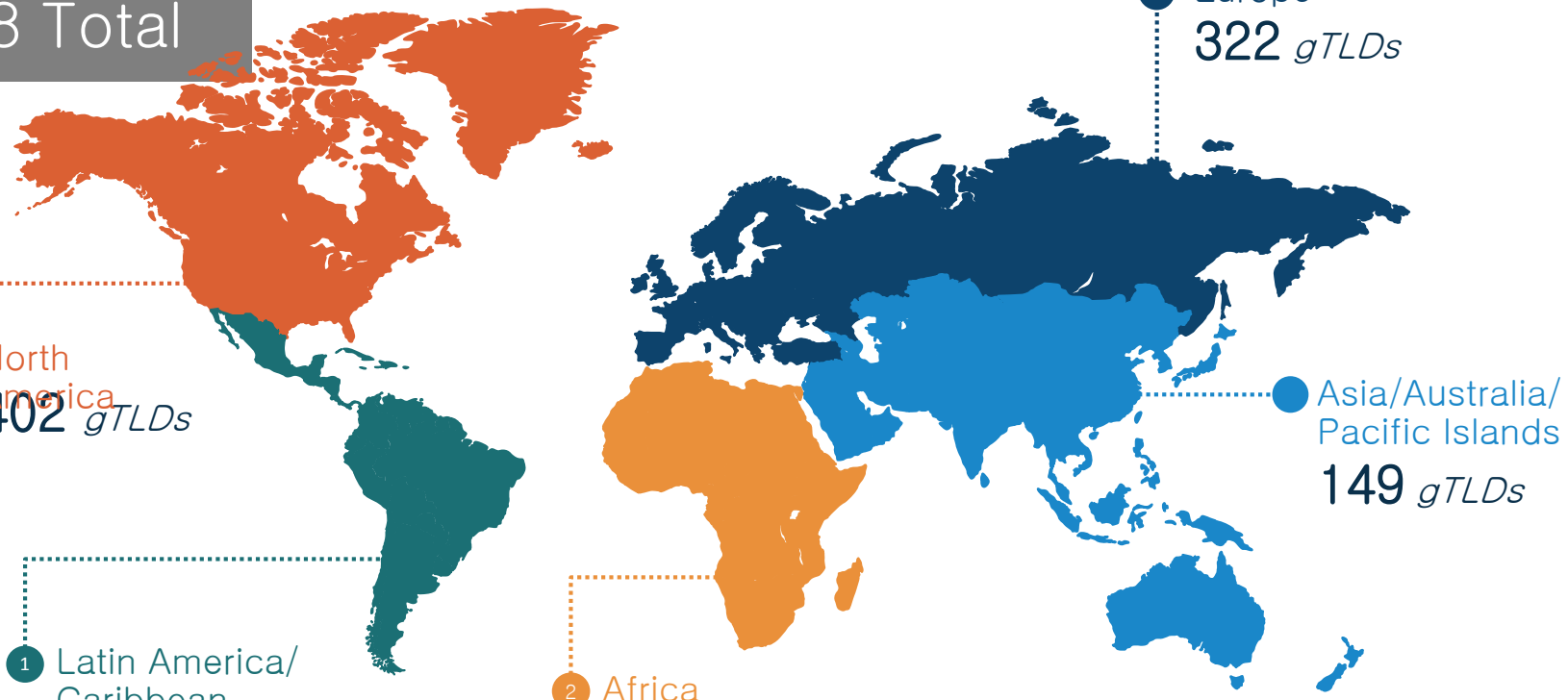
- ICANN is the L-Root Operator
- L-Root nodes keep Internet traffic local and resolve queries faster
- Make it easier to isolate attacks
- Reduce congestion on international bandwidth
- Redundancy and load balancing with multiple instances

L–Root presence


Registry, Registrar Model

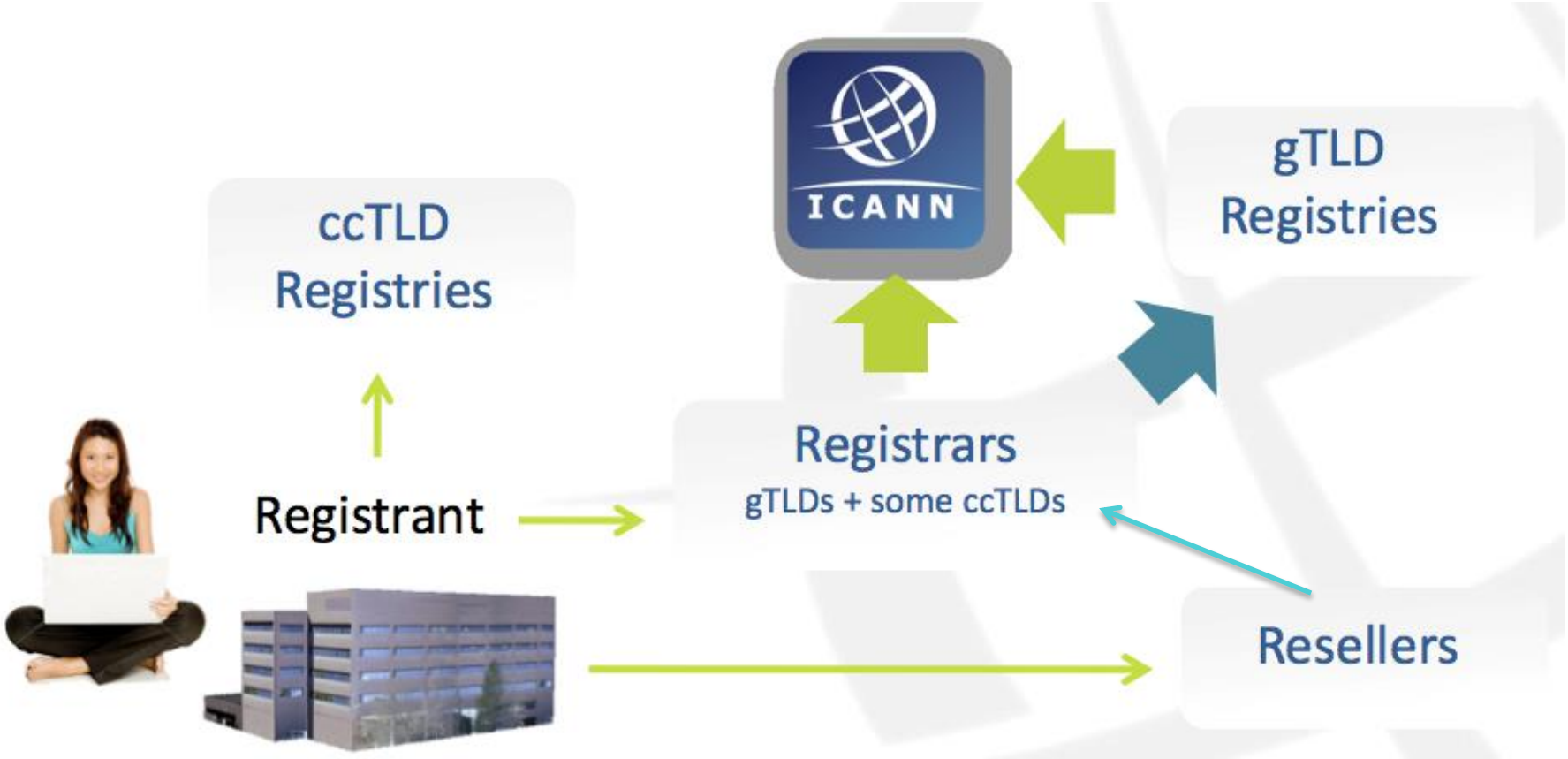
Regional Distribution of Delegated gTLDs

888 Total

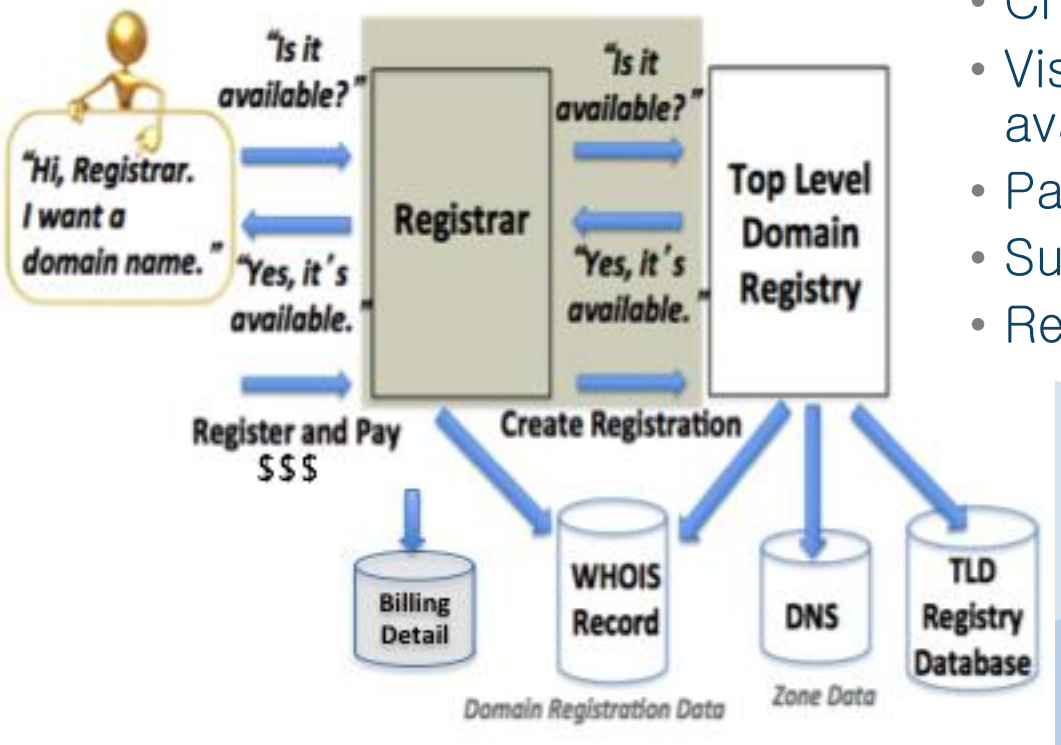


Data as of January 2016
Categorized by ICANN region

The Registry/Registrar Ecosystem



Domain Name Registration

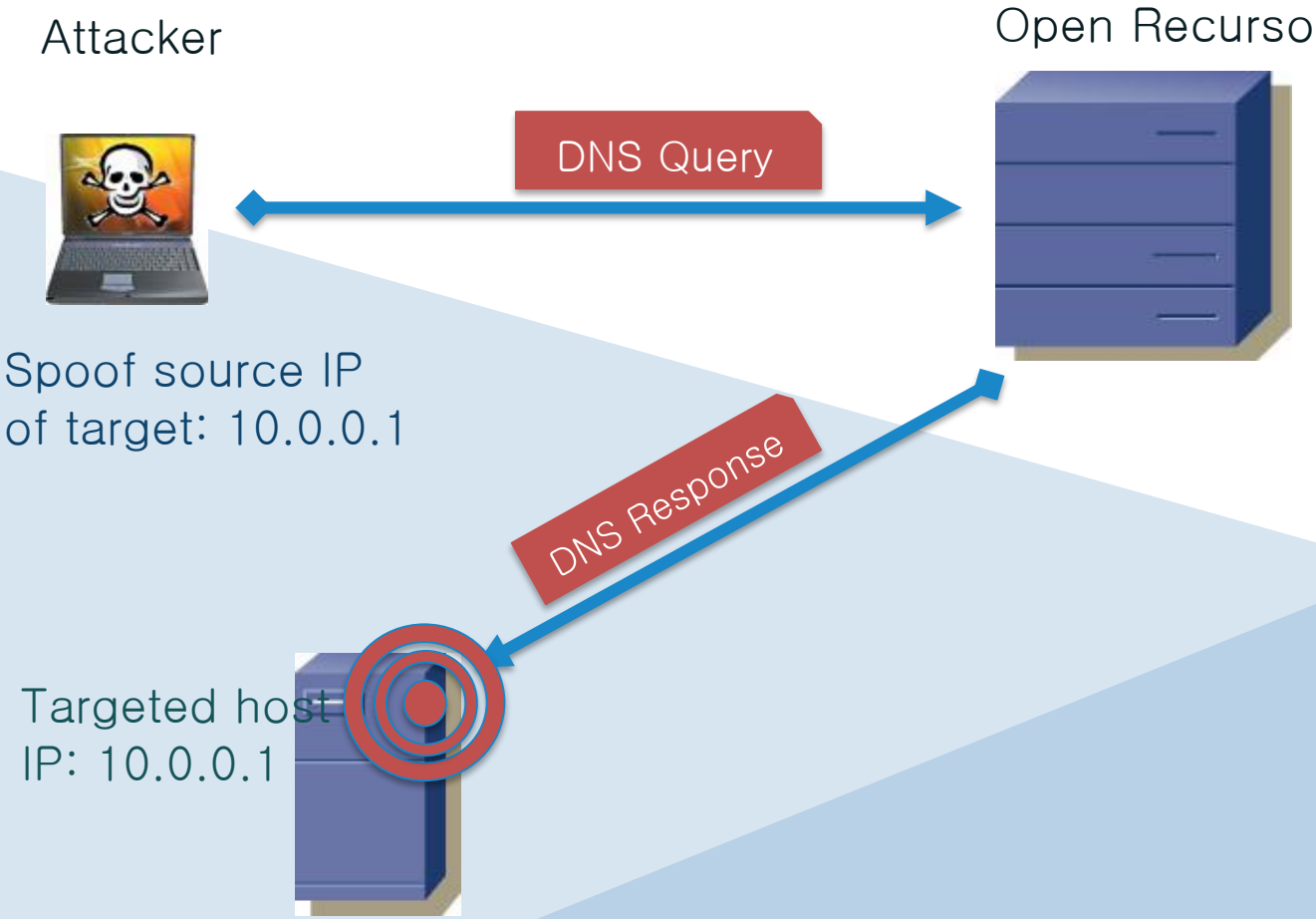


How to register a domain:

- Choose a string e.g., `example`
- Visit a registrar to check string availability in a TLD
- Pay a fee to register the name
- Submit registration information
- Registrar and registries manage:
  - "string" + TLD (managed in registry DB)
  - Contacts, DNS (managed in Whois)
  - DNS, status (managed in Whois DBs)
  - Payment information

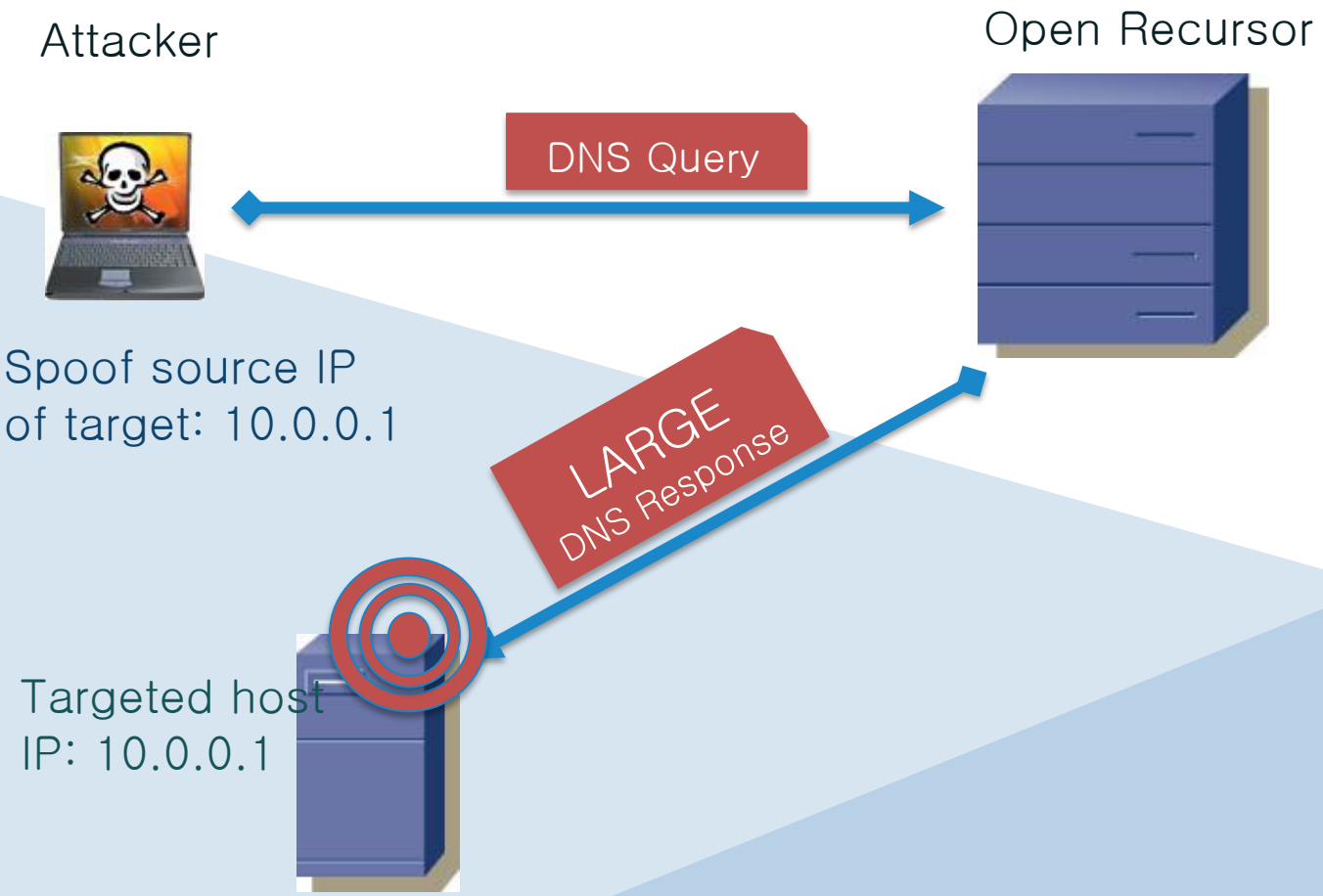

DNS Security

Reflection attack



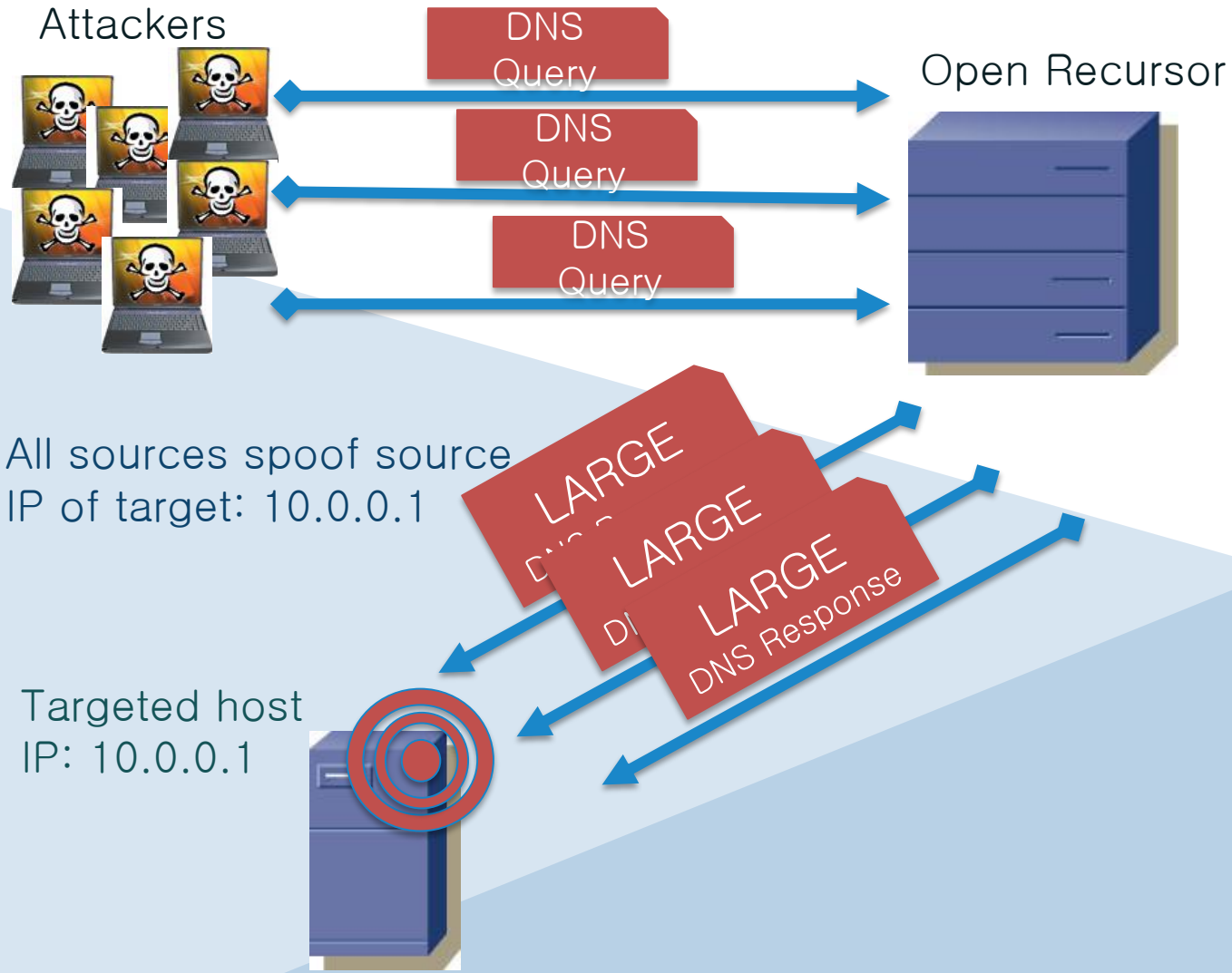
- Attacker sends DNS messages to recursor from spoofed IP address of target
- Recursor sends response to targeted host
- Response delivered to targeted host

Reflection and Amplification attack



- Attacker sends DNS messages to recursor from spoofed IP address of target
- Recursor sends LARGE responses to targeted host
- *Amplified* responses delivered to targeted host consume resources faster

Distributed reflection and amplification attack (DRDoS)



- Launch reflection and amplification attack from 1000s of origins
- Reflect through open recursor
- Deliver 1000s of large responses to target

Basic Cache Poisoning

Attacker

- Launches a spam campaign where spam message contains http://loseweightfastnow.com
- Attacker's name server will respond to a DNS query for loseweightnow.com with malicious data about ebay.com
- Vulnerable resolvers add malicious data to local caches
- The malicious data will send victims to an eBay phishing site for the lifetime of the cached entry

My Mac

What is the IPv4 address for loseweightfastnow.com

I'll cache this response… and update www.ebay.com

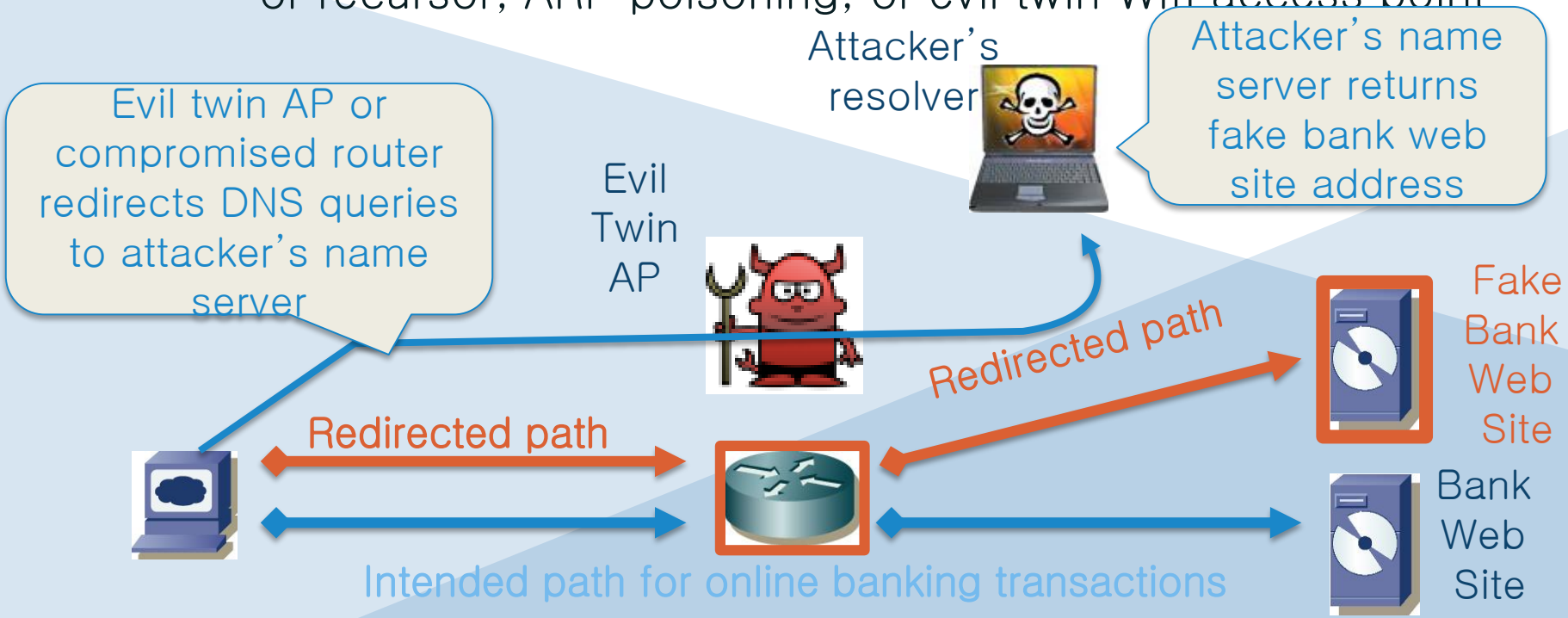
My local resolver

loseweightfastnow.com IPv4 address is 192.168.1.1
ALSO *www.ebay.com is at 192.168.1.2*

ecrime name server

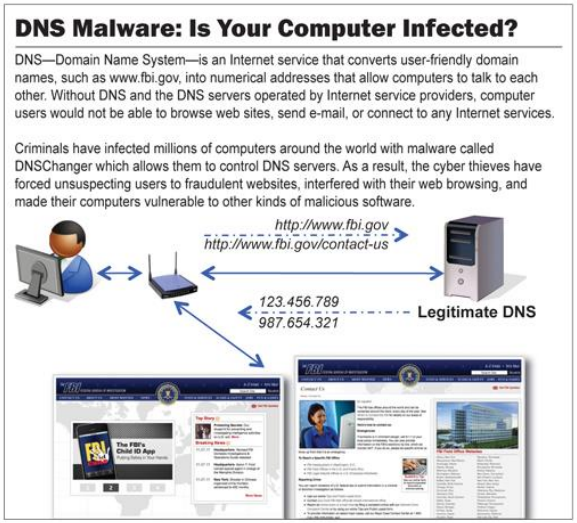
Query Interception (DNS Hijacking)

- A man in the middle (MITM) or spoofing attack forwards DNS queries to a name server that returns forge responses
  - Can be done using a DNS proxy, compromised access router or recursor, ARP poisoning, or evil twin Wifi access point



The Bad

- DNSChanger
  - Biggest Cybercriminal Takedown in History
  - 4M machines, 100 countries, $14M



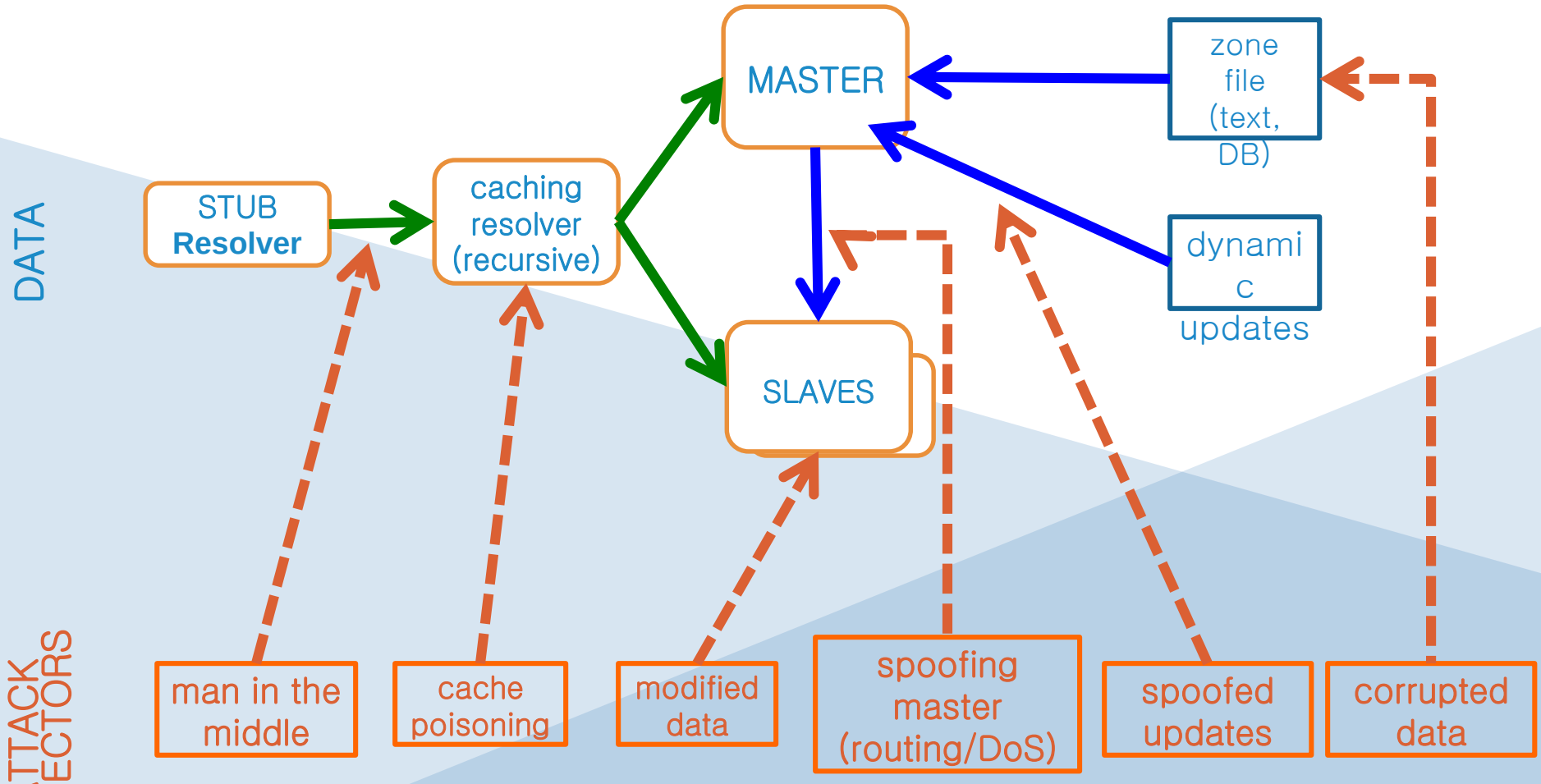
- And many other DNS hijacks in recent times

- SSL / TLS doesn't tell you if you've been sent to the correct site, it only tells you if the DNS matches the name in the certificate. Unfortunately, majority of Web site certificates rely on DNS to validate identity.

- DNS is relied on for unexpected things though insecure.

DigiNotar® A VASCO COMPANY

DNS Data Flow



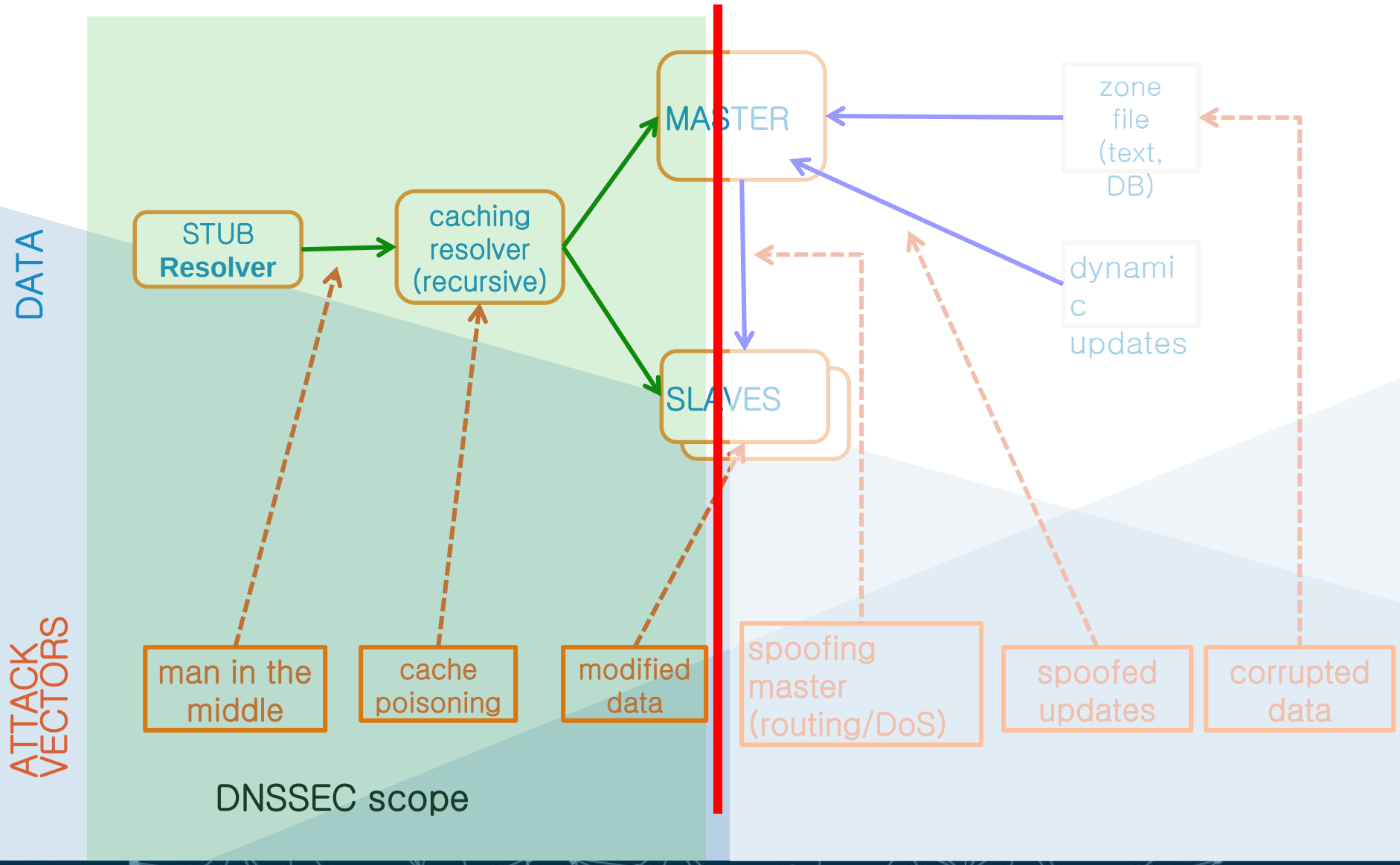
Securing DNS

- There are two aspects when considering DNS Security
  - Server protection
  - Data protection
- Server protection
  - Protecting servers
    - Make sure your DNS servers are protected (i.e. physical security, latest DNS server software, proper security policies, Server redundancies etc.)
  - Protecting server transactions
    - Deployment of TSIG, ACLs etc. (To secure transactions against server impersonations, secure zone transfers, unauthorized updates etc.)
- Data protection
  - Authenticity and Integrity of Data
    - Deployment of DNSSEC (Protect DNS data against cache poisoning, cache impersonations, spoofing etc.)

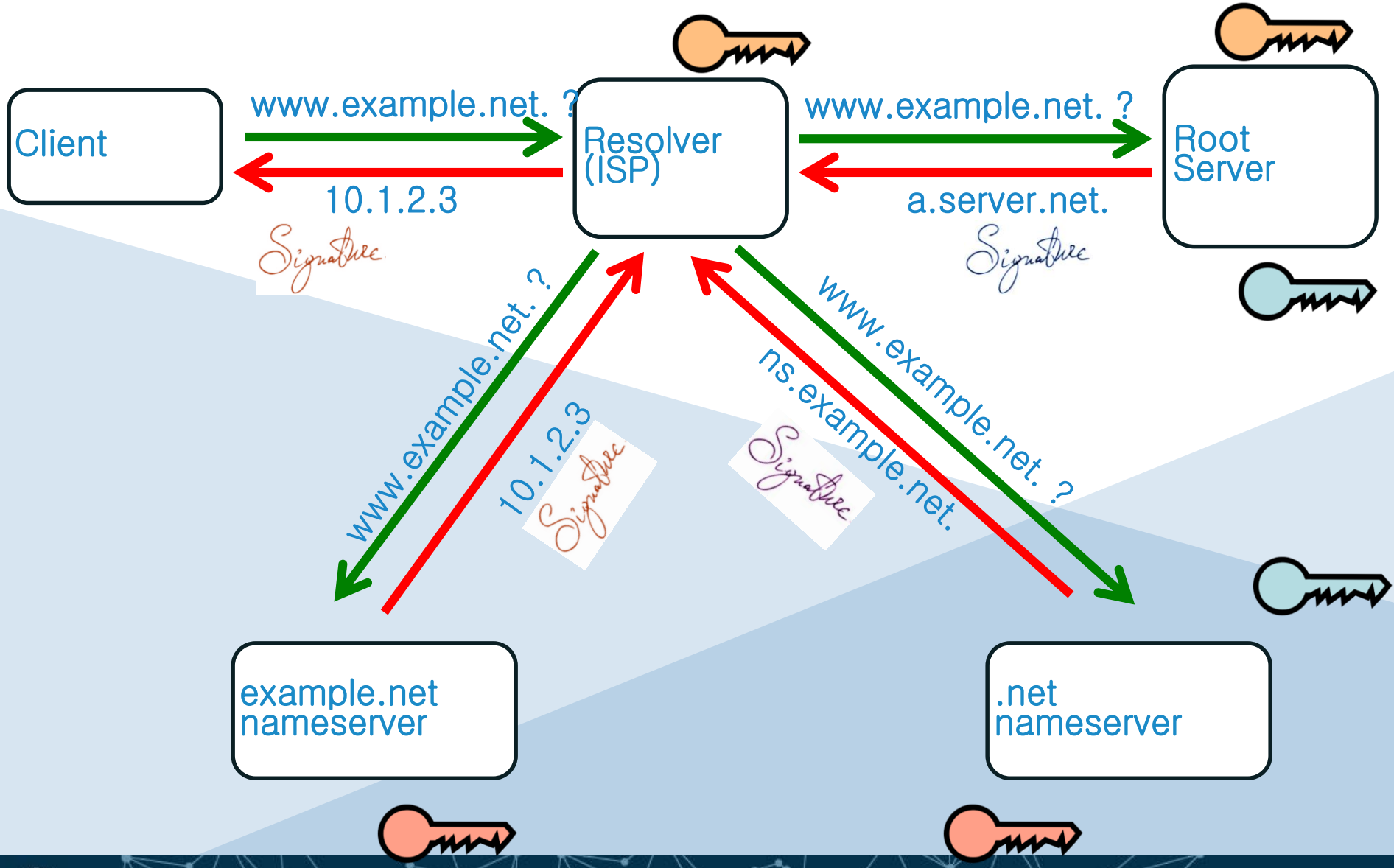
Where DNSSEC fits in

- CPU and bandwidth advances make legacy DNS vulnerable to MITM attacks
- DNS Security Extensions (DNSSEC) introduces digital signatures into DNS to cryptographically protect contents
- With DNSSEC fully deployed a business can be sure a customer gets un-modified data (and visa versa)

What DNSSEC solves and what's not



How DNSSEC Works



The Business Case for DNSSEC

- Cyber security is becoming a greater concern to enterprises, government, and end users. DNSSEC is a key tool and differentiator.

- DNSSEC is the biggest security upgrade to Internet infrastructure in over 20 years. It is a platform for new security applications (for those that see the opportunity).

- DNSSEC infrastructure deployment has been brisk but requires expertise. Getting ahead of the curve is a competitive advantage.

DNSSEC ccTLD Map

DNSSEC: So what's the problem?

- Not enough IT departments know about it or are too busy putting out other security fires.
- When they do look into it they hear old stories of FUD and lack of turnkey solutions.
- Registrars*/DNS providers see no demand leading to "chicken-and-egg" problems.

*but required by new ICANN registrar agreement

What you can do

- *For Companies:*
  - Sign your corporate domain names
  - Just turn on validation on corporate DNS resolvers
- *For Users:*
  - Ask ISP to turn on validation on their DNS resolvers
- *For All:*
  - Take advantage of DNSSEC education and training


DNSSEC: Internet infrastructure upgrade to help address today's needs and create tomorrow's opportunity.