DNS/DNSSEC Workshop

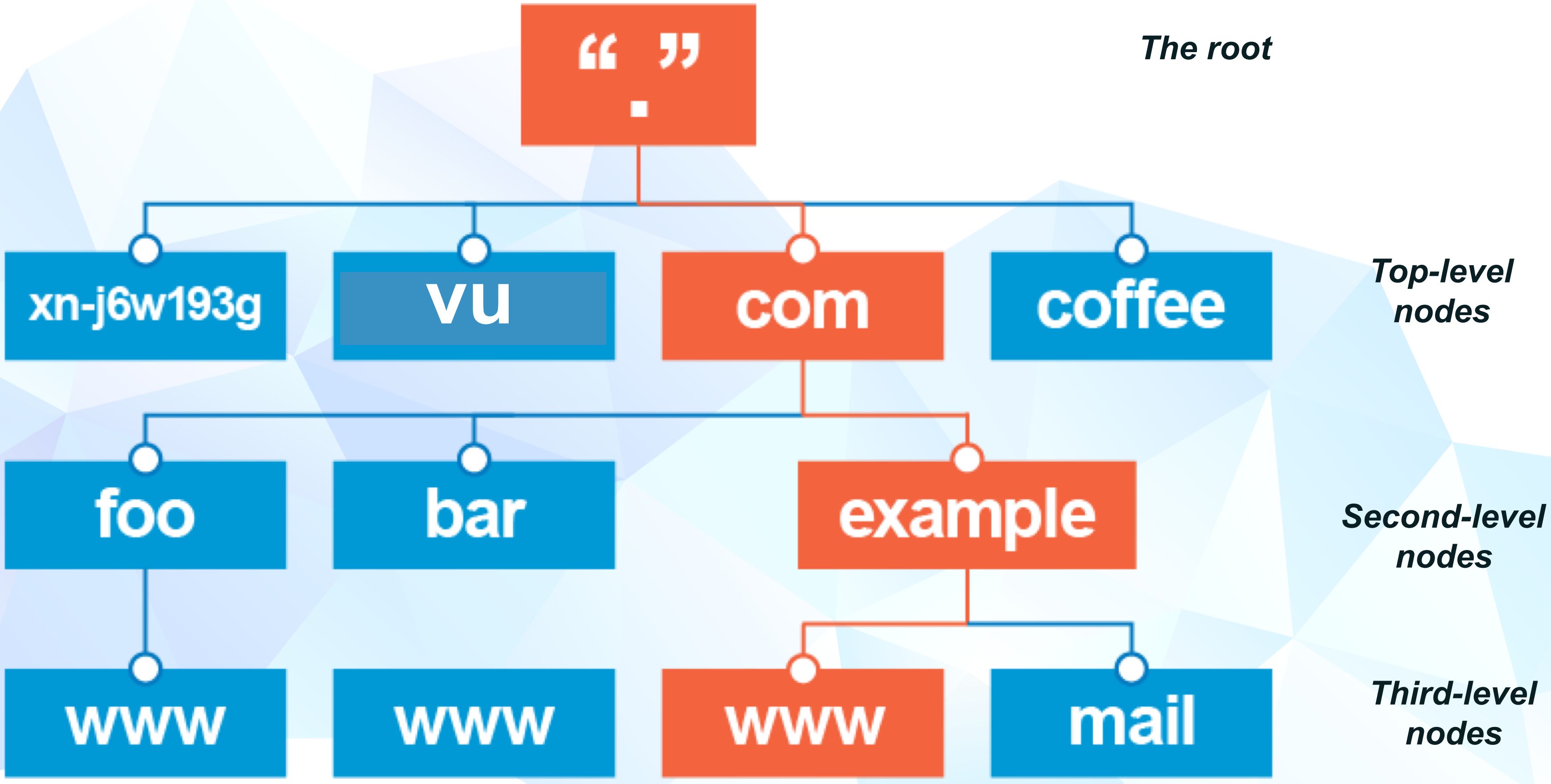
In Collaboration with TRBR – Port Vila - Vanuatu

Champika Wijayatunga – Regional Security Engagement Manager – Asia Pacific

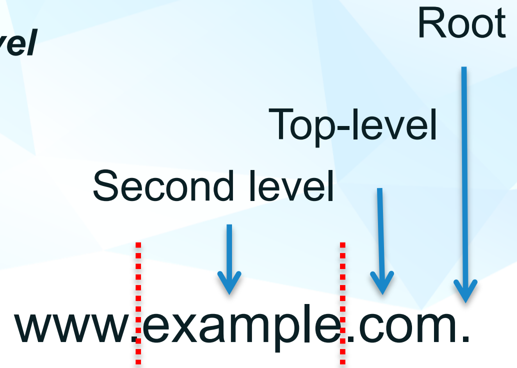
20-21 March 2019

DNS Concepts

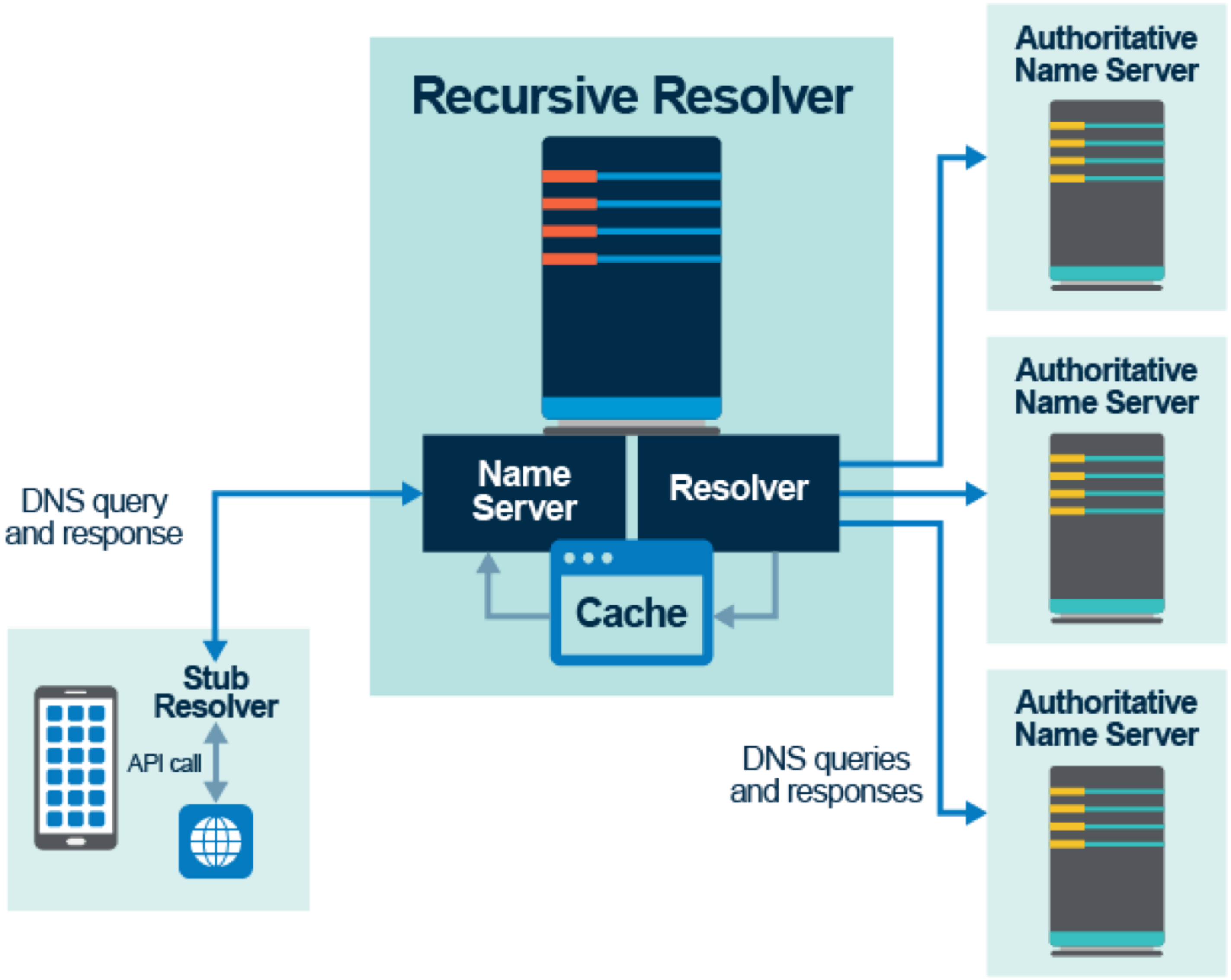
The Domain Name System (DNS)



FQDN = **F**ully **Q**ualified **D**omain **N**ame



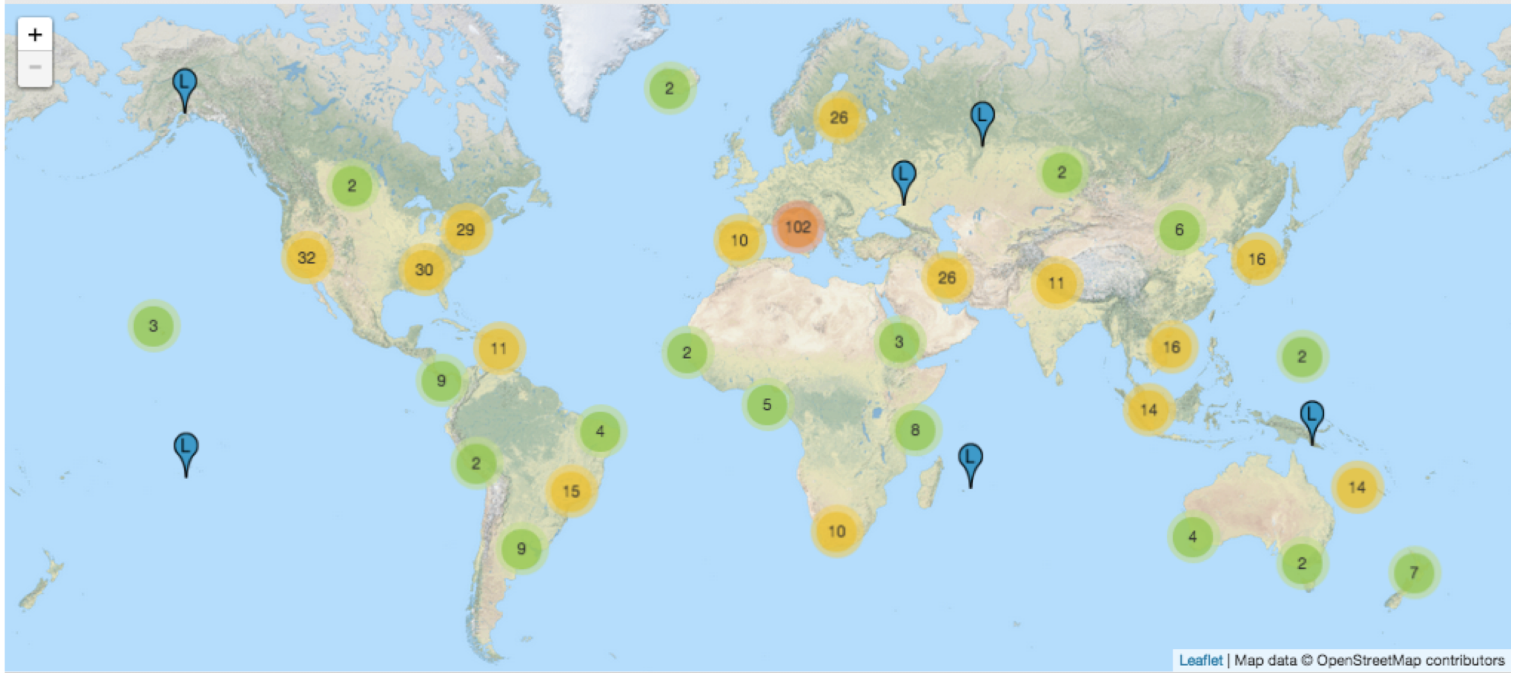
DNS Components at a Glance


Recursive Resolver
Name Server
Resolver
Cache
DNS query and response
Stub Resolver
API call
DNS queries and responses
Authoritative Name Server
Authoritative Name Server
Authoritative Name Server

DNS Servers

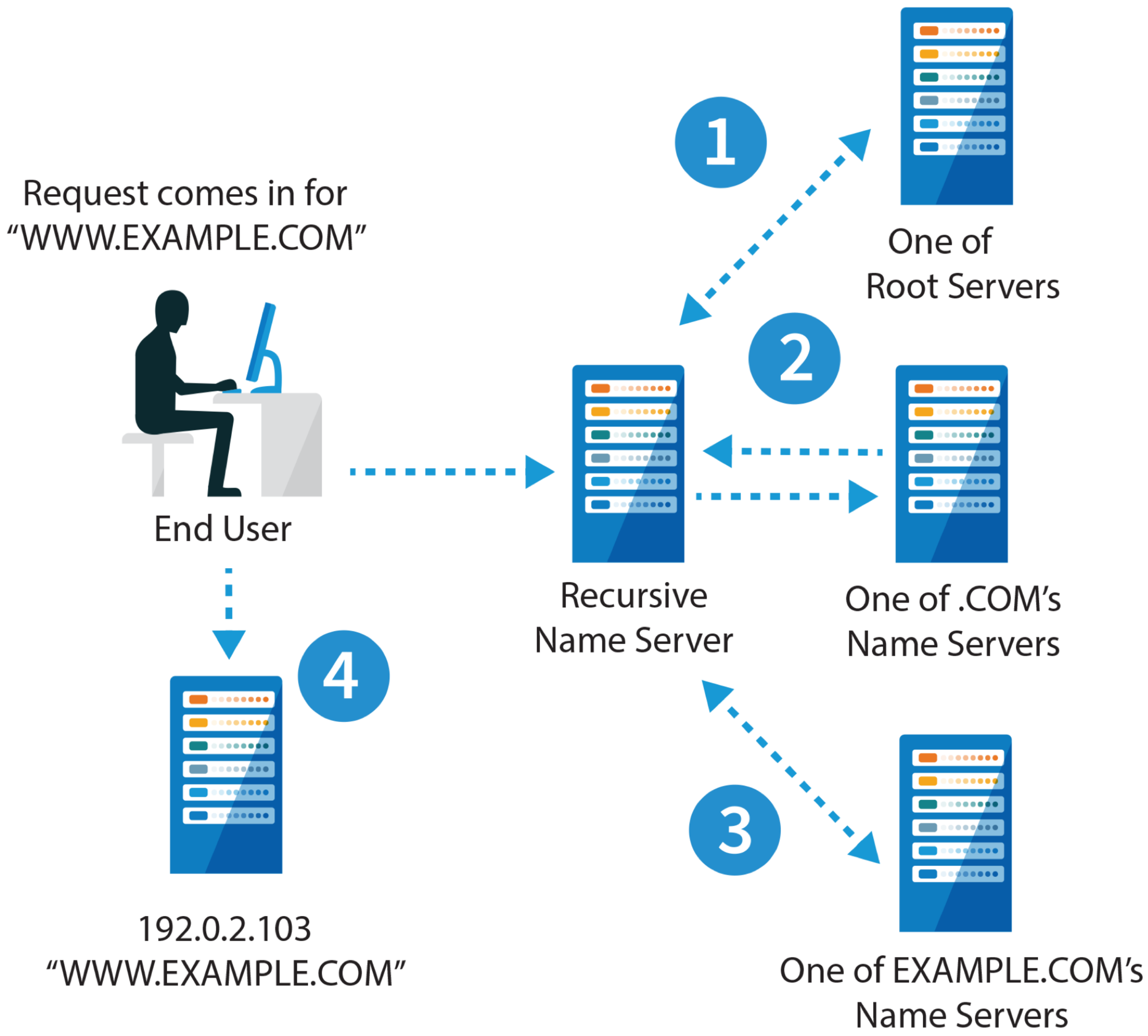
- Authoritative Servers
  - Root Servers
  - Primary
  - Secondary

- Recursive Servers
  - Or Recursive Resolvers
  - Or Caching Servers

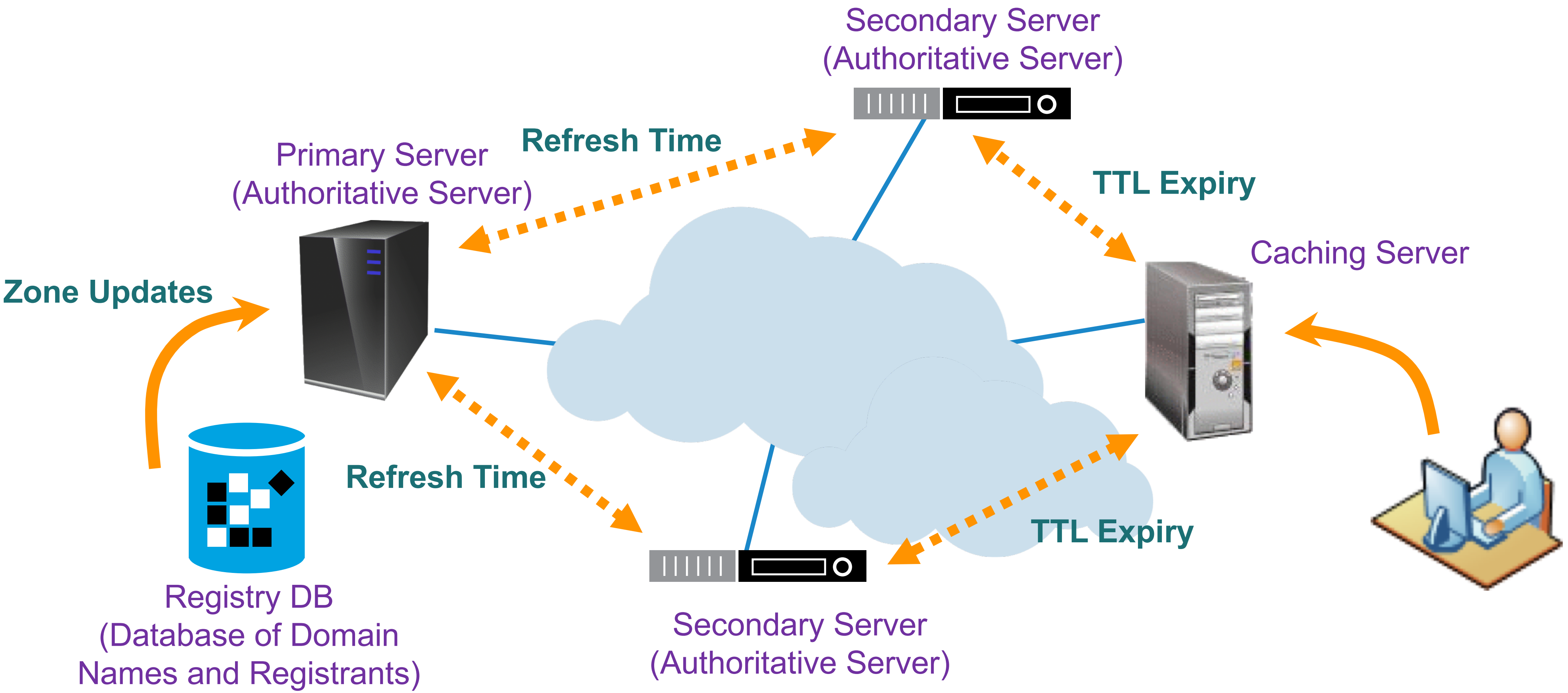


Leaflet | Map data © OpenStreetMap contributors

How DNS Works



Propagation of DNS Data



Zone Data and Resource Records (RR)

- Consists of resource mappings

```
Label      TTL    Class    Type   RData
www        3600    IN       A      192.168.0.1
```

- Most common types of RR
  - A
  - AAAA
  - NS
  - SOA
  - MX
  - CNAME

Resource Record	Function
Label	Name substitution for FQDN
TTL	Timing parameter, an expiration limit
Class	IN for Internet, CH for Chaos
Type	RR Type (A, AAAA, MX, PTR) for different purposes
RDATA	Anything after the Type identifier; Payload of the record

Zone Files

```
$TTL 86400          ; 24 hours could have been written as 24h or 1d
$ORIGIN example.com.
@        IN       SOA        ns1.example.com.    hostmaster.example.com.      (
                                    2017092701 ; serial number
                                    3H          ; refresh
                                    15          ; retry
                                    1w          ; expire
                                    3h          ; nxdomain TTL          )

         IN       NS     ns1.example.com.                ; in the domain
         IN       NS     ns2.anotherexample.net.         ; external to domain
         IN       MX  10 mail.someotherexample.com.      ; external mail provider
ns1      IN       A      192.168.0.1                     ; name server definition
www      IN       A      192.168.0.2                     ; web server definition
ftp      IN       CNAME  www.example.com.                ; ftp server definition
host     IN       A      192.168.0.3                     ; host definition
```

Delegating a Zone

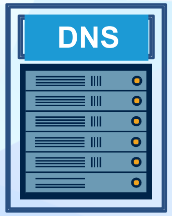
- Delegation is done by adding NS records
  - Ex: if example.com wants to delegate training.example.com to another party,

```
training.example.com.   NS ns1.training.example.com.
training.example.com.   NS ns2.training.example.com.
```

- Now how can we get to ns1 and ns2?
  - We must add a Glue Record

Delegating a Child Zone from a Parent Zone

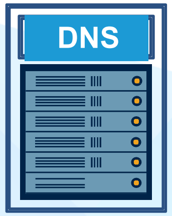
example.com (Parent Zone)



ns.example.com

1. Add NS records and glue
2. Make sure there is no other data from the training.example.test. zone in the zone file

training.example.com (Child Zone)



ns.training.example.com

1. Setup minimum two servers
2. Create zone file with NS records
3. Add all training.example.test data

DNS Resolver and Authoritative Server – Labs
Setting up and Configurations - Labs

Reverse DNS

Reverse Mapping

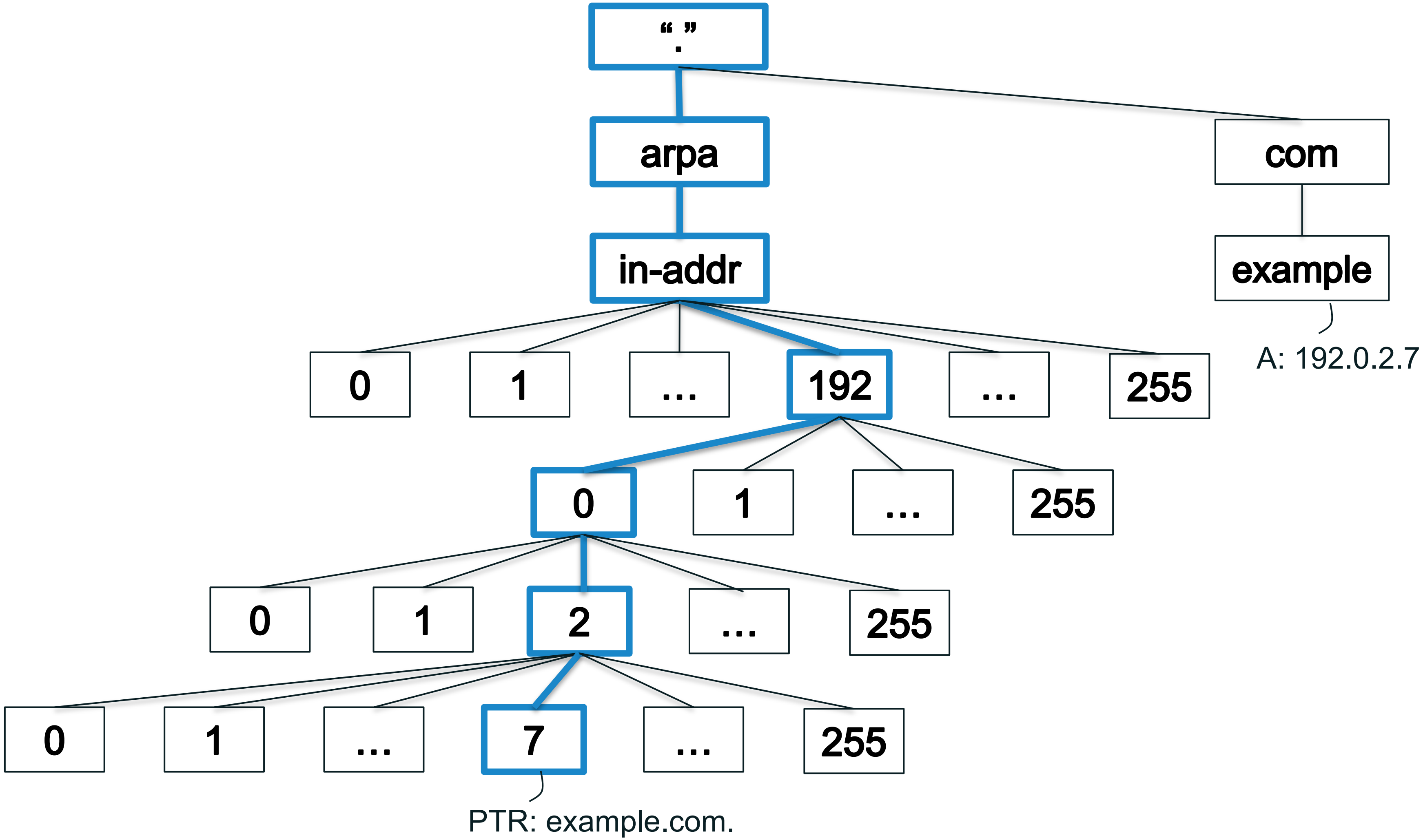
- Name-to-IP is “forward” mapping
- IP-to-name is “reverse” mapping
- Reverse mapping accomplished by mapping IP address space to the DNS name space
  - IPv4 addresses under *in-addr.arpa*
  - IPv6 addresses under *ip6.arpa*
- Uses PTR (pointer) records

```
7.2.0.192.in-addr.arpa.   PTR     host.example.com.
```

- Corresponds to this A record:

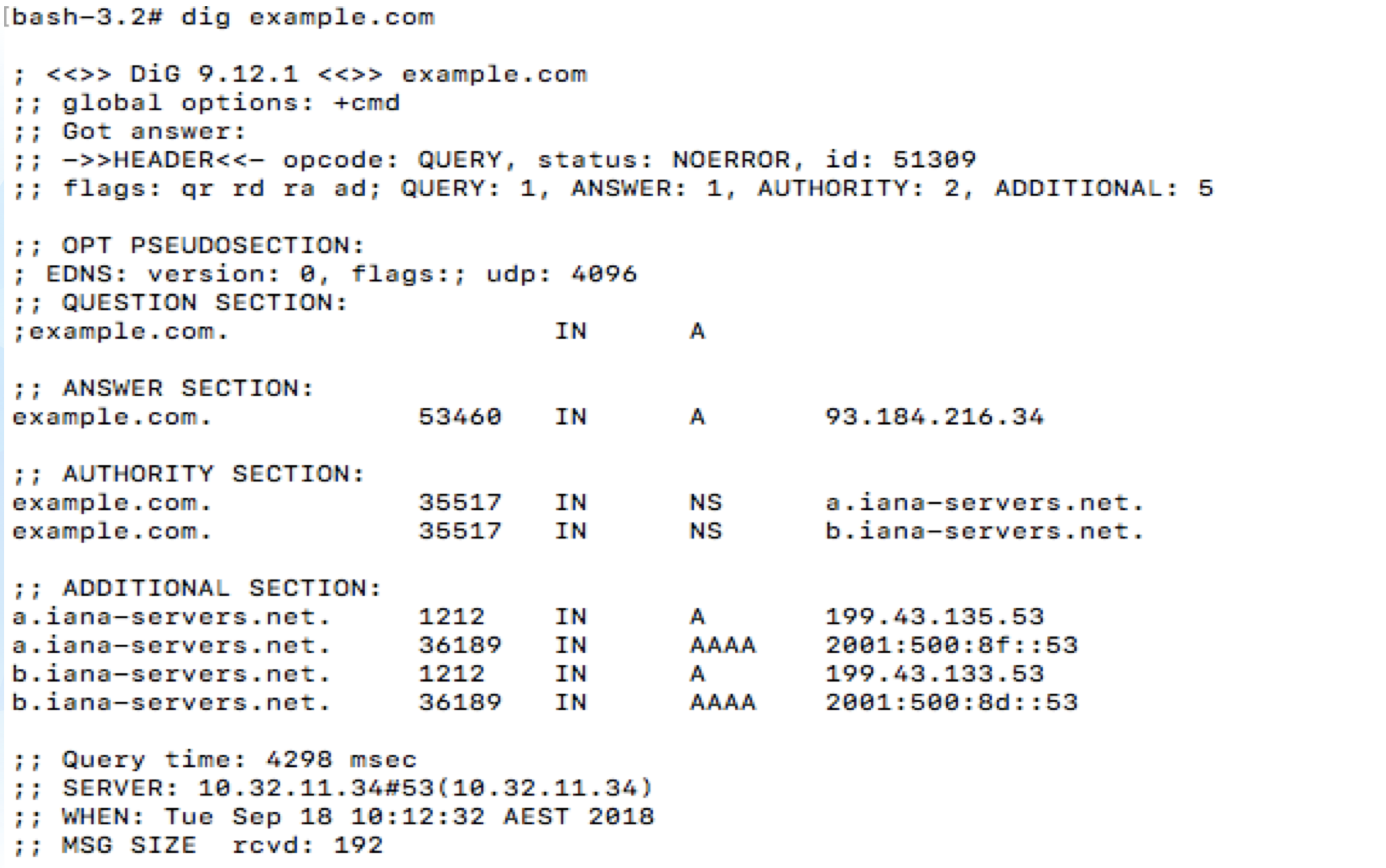
```
host.example.com.              A      192.0.2.7
```

Reverse Mapping



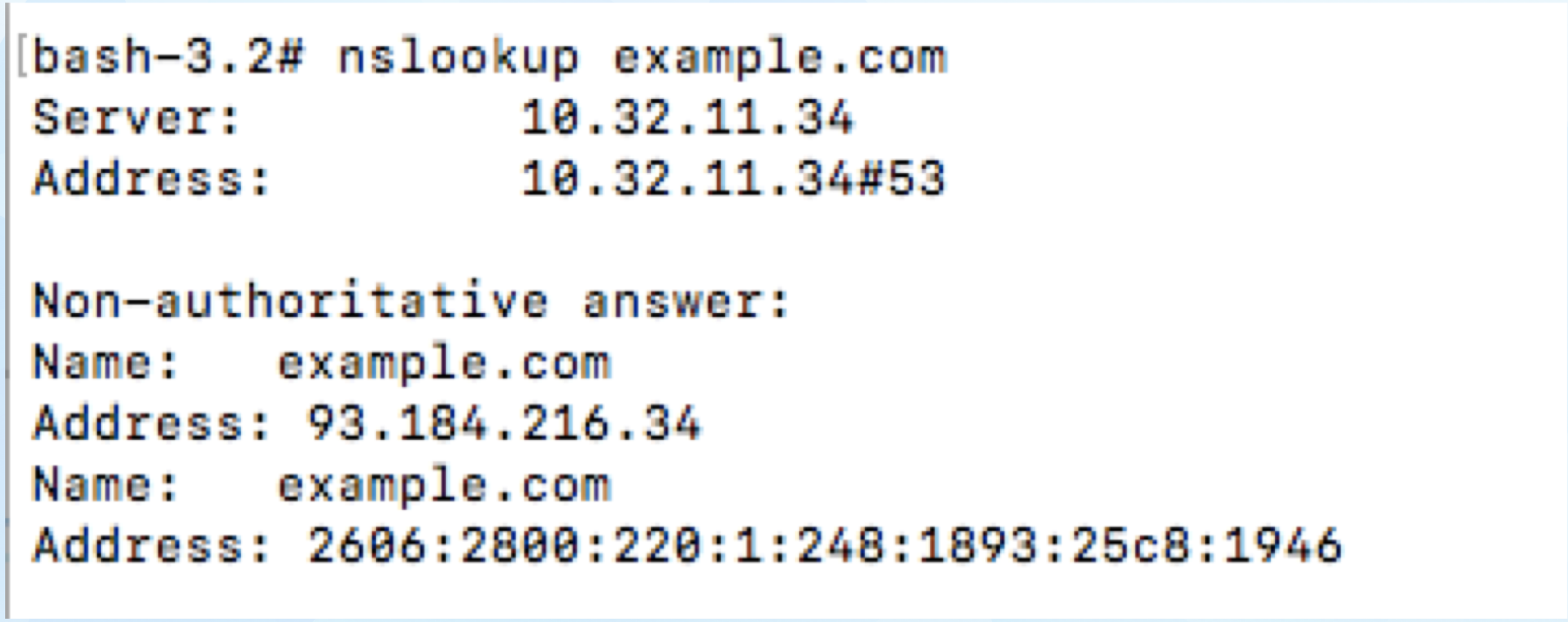
DNS Debugging Tools and Utilities

dig



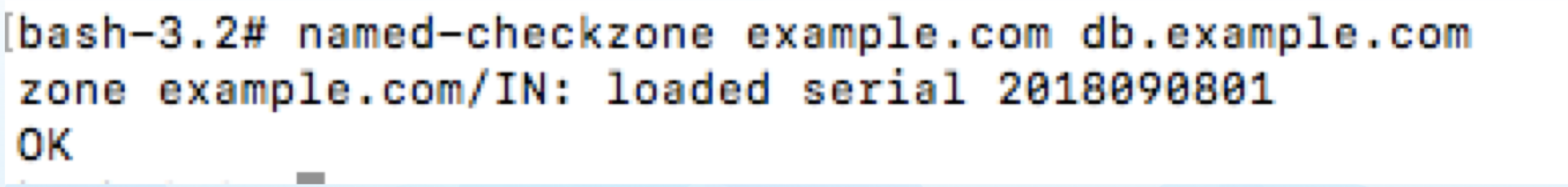
```
[bash-3.2# dig example.com

; <<>> DiG 9.12.1 <<>> example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51309
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;example.com.                   IN      A

;; ANSWER SECTION:
example.com.            53460   IN      A       93.184.216.34

;; AUTHORITY SECTION:
example.com.            35517   IN      NS      a.iana-servers.net.
example.com.            35517   IN      NS      b.iana-servers.net.

;; ADDITIONAL SECTION:
a.iana-servers.net.     1212    IN      A       199.43.135.53
a.iana-servers.net.     36189   IN      AAAA    2001:500:8f::53
b.iana-servers.net.     1212    IN      A       199.43.133.53
b.iana-servers.net.     36189   IN      AAAA    2001:500:8d::53

;; Query time: 4298 msec
;; SERVER: 10.32.11.34#53(10.32.11.34)
;; WHEN: Tue Sep 18 10:12:32 AEST 2018
;; MSG SIZE  rcvd: 192
```

nslookup

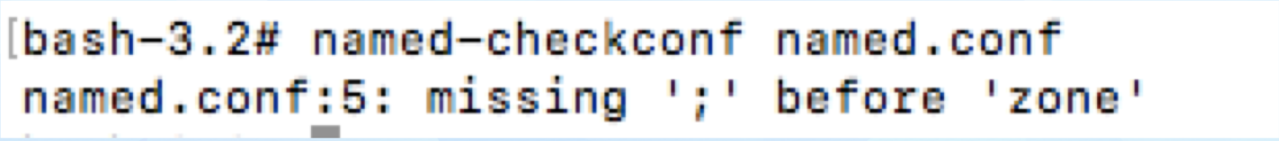


```
[bash-3.2# nslookup example.com
Server:          10.32.11.34
Address:         10.32.11.34#53

Non-authoritative answer:
Name:    example.com
Address: 93.184.216.34
Name:    example.com
Address: 2606:2800:220:1:248:1893:25c8:1946
```

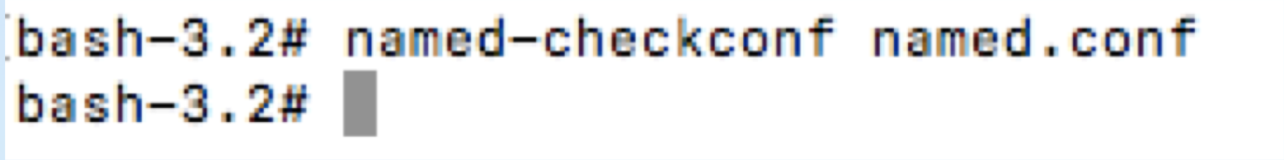
named-checkzone and named-checkconf



```
[bash-3.2# named-checkzone example.com db.example.com
zone example.com/IN: loaded serial 2018090801
OK
```



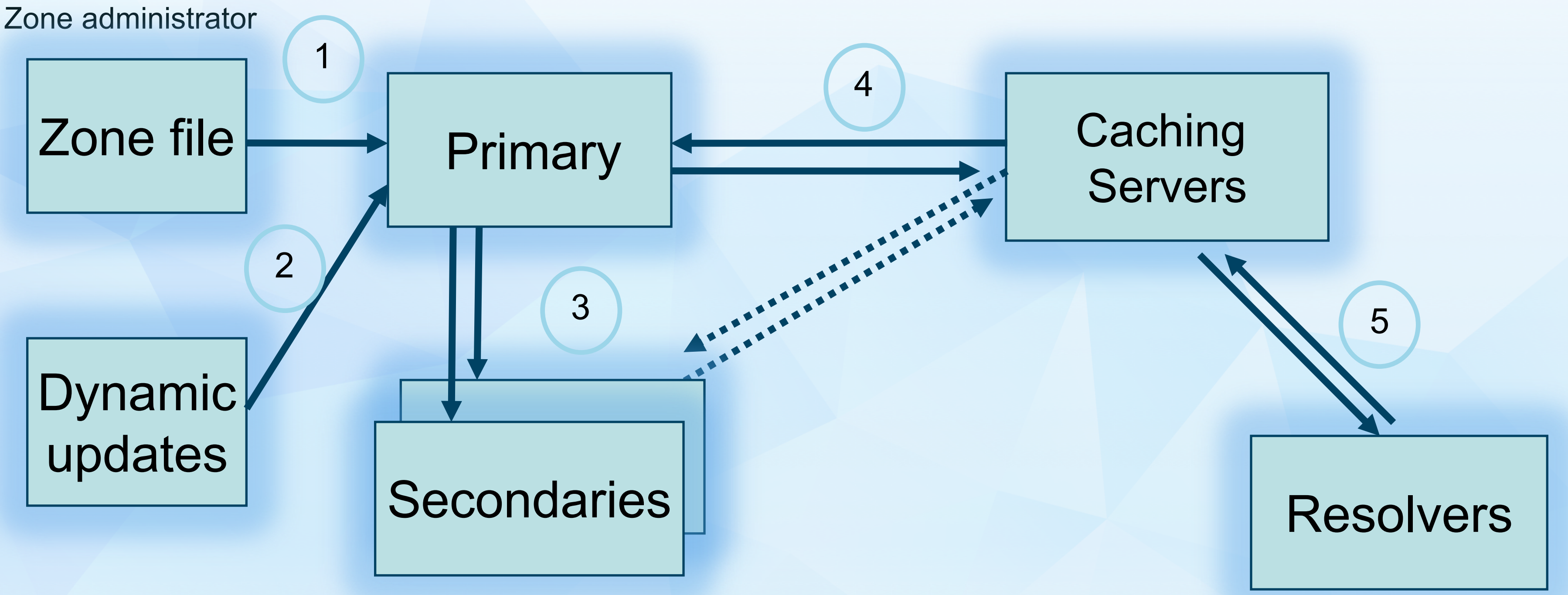
```
[bash-3.2# named-checkconf named.conf
named.conf:5: missing ';' before 'zone'
```



```
[bash-3.2# named-checkconf named.conf
bash-3.2# █
```

DNS Security Concepts

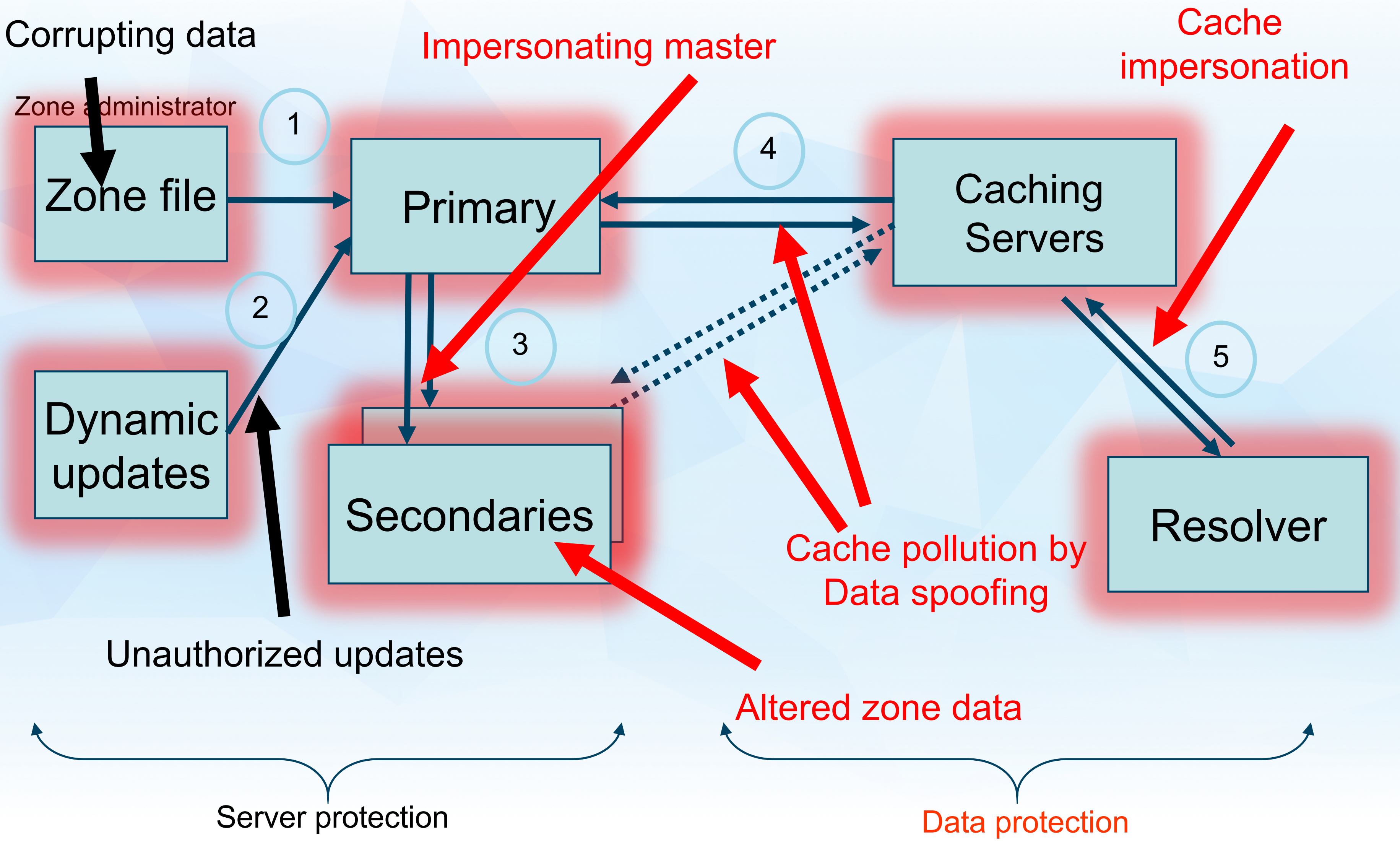
DNS: Data Flow



www.facebook.com.subdomain.phishing.vu

tvvitter.com

DNS Vulnerabilities



The Bad

- Cache Poisoning Attacks
  - Vulnerable resolvers add malicious data to local caches
- DNS Hijacking
  - A man in the middle (MITM) or spoofing attack forwards DNS queries to a name server that returns forge responses
- E.g. DNSChanger
  - One of the biggest cybercriminal takedown in history
- 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.
- DNS is relied on for unexpected things though insecure.

Technical Requirements

- Networks and Servers (redundant)
- Back office systems.
- Physical and Electronic Security
- Quality of Service (24/ 7 availability!)
- Name Servers
- DNS software (BIND, NSD, etc.)
- Registry software
- Diagnostic tools (ping, traceroute, zonecheck, dig)
- Registry Registrar Protocol

Name Server Considerations

- Support technical standards
- Diverse bandwidth to support above
- Authoritative vs Recursive
- Authoritative Servers must answer authoritatively
- Turn off recursion!
- Recursive Servers should be providing recursion only to designated clients

Secondary Name Server Choice - Diversity is important

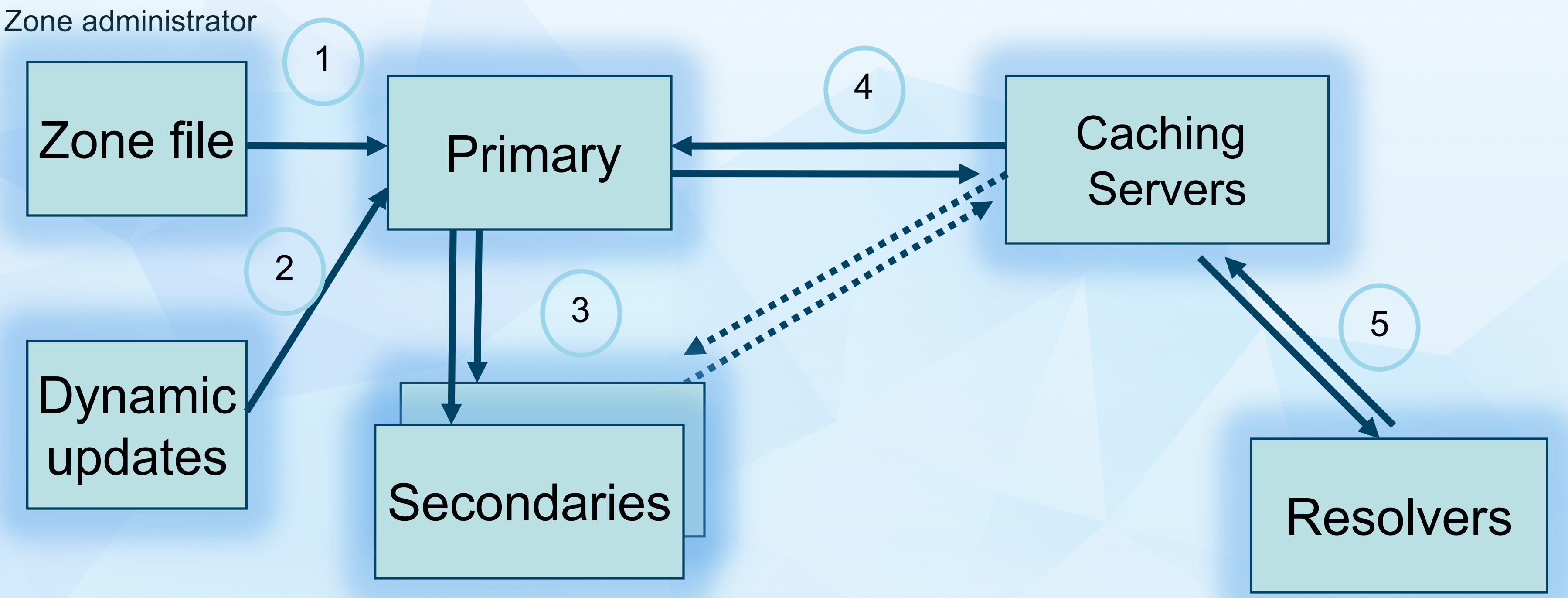
- Don’t place all on the same LAN/building/segment
- Network diversity
- Geographical diversity
- Institutional diversity
- Software and hardware diversity

Know Your SLAs

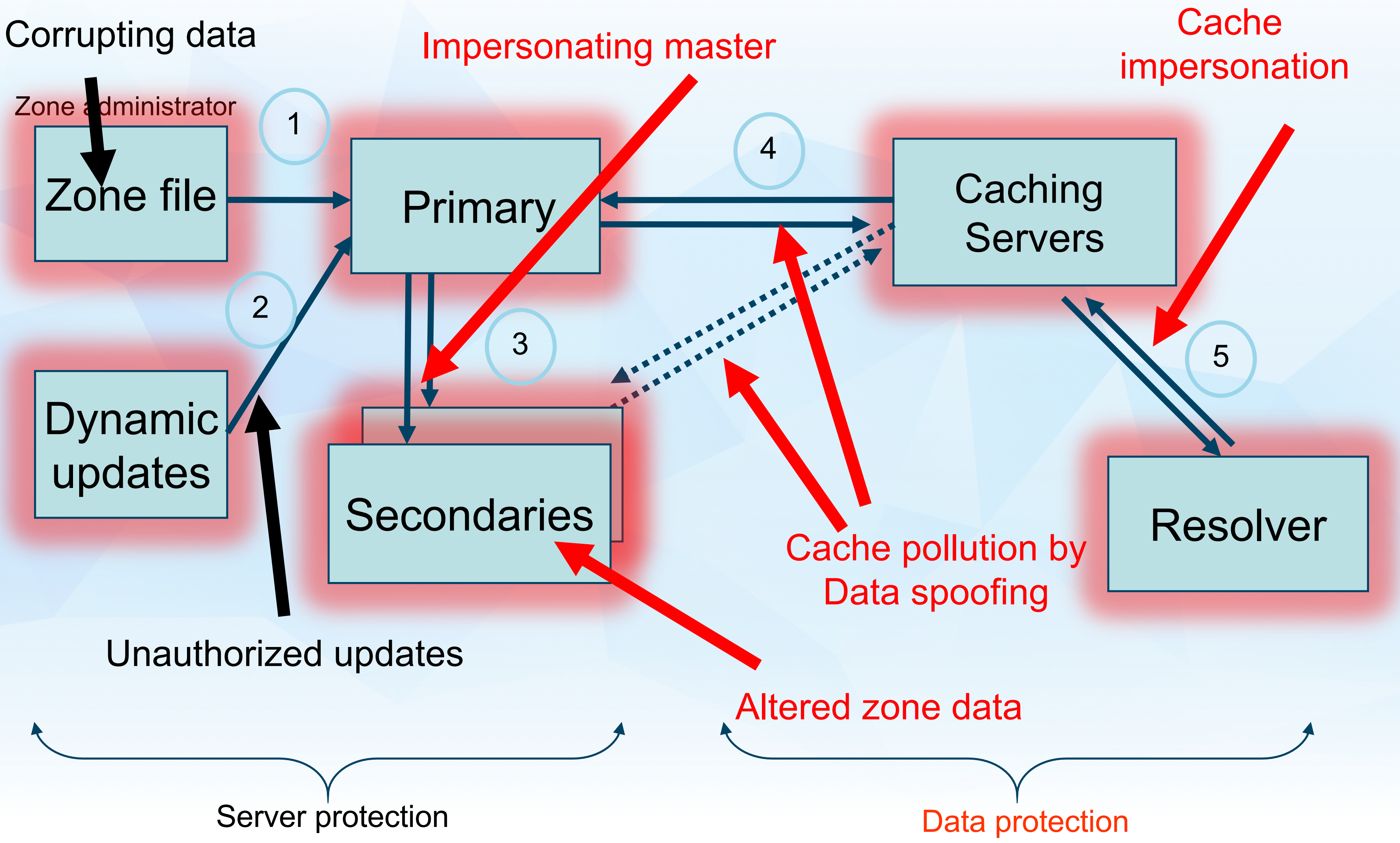
- Functioning name servers are the most critical/visible service
- All other services also need to be considered
  - Billing
  - Whois server, webservers
  - Registrar APIs
- Consider your service level targets and how you will meet them
- DNS servers always on, other systems mostly on?

DNSSEC

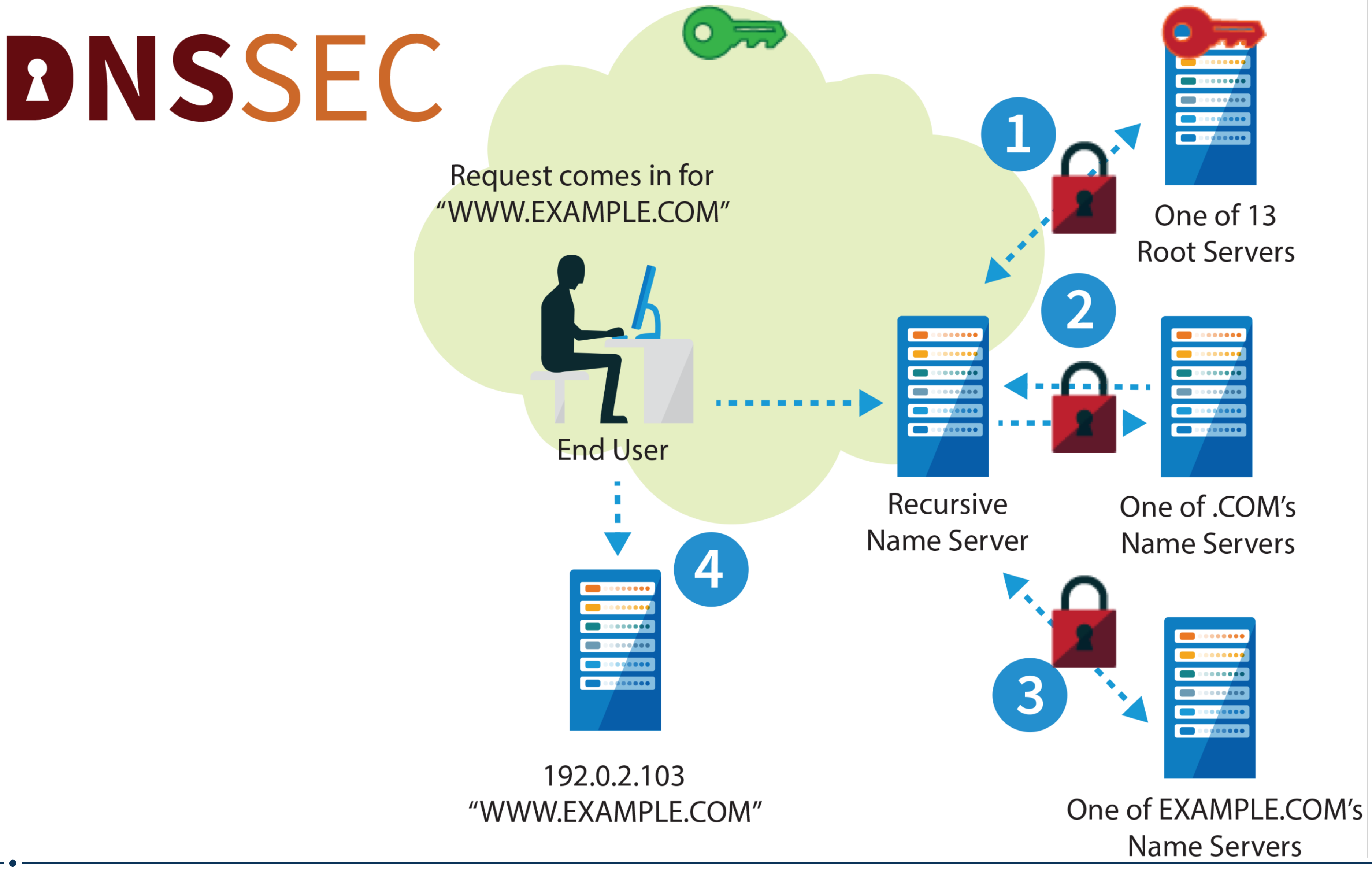
DNS: Data Flow



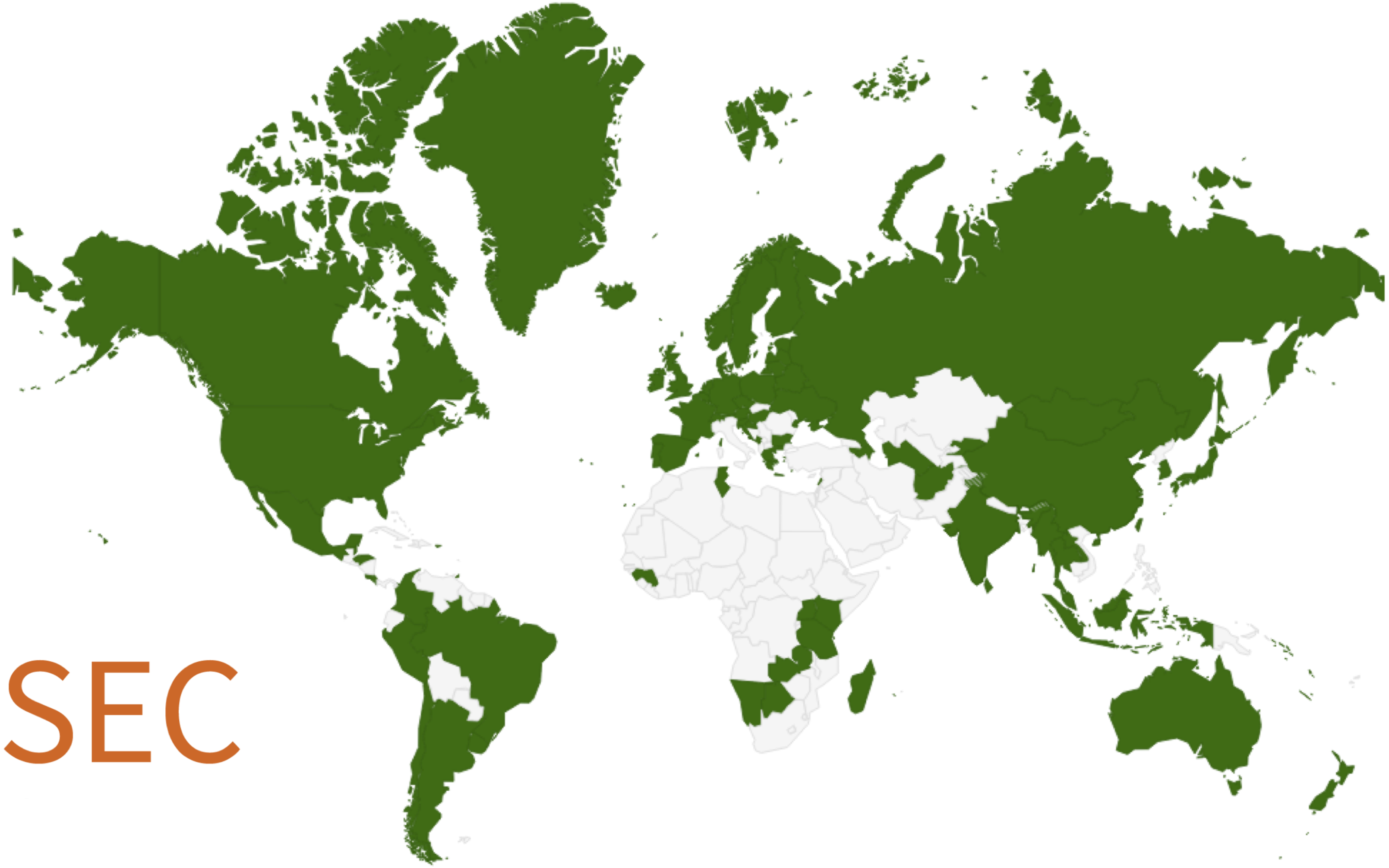
DNS Vulnerabilities



How DNSSEC Works

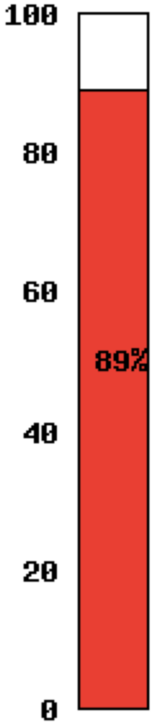


DNSSEC ccTLD Map

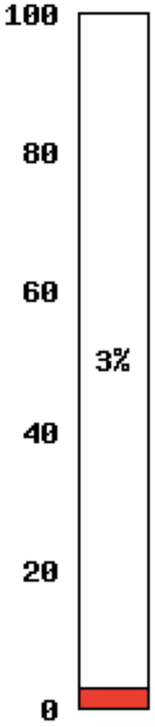


DNSSEC

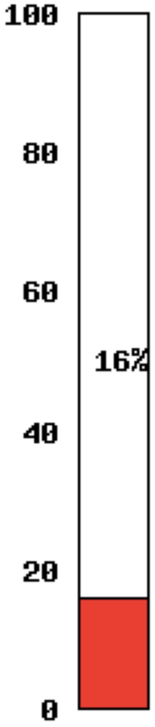
DNSSEC Deployment



% of TLDs signed in root

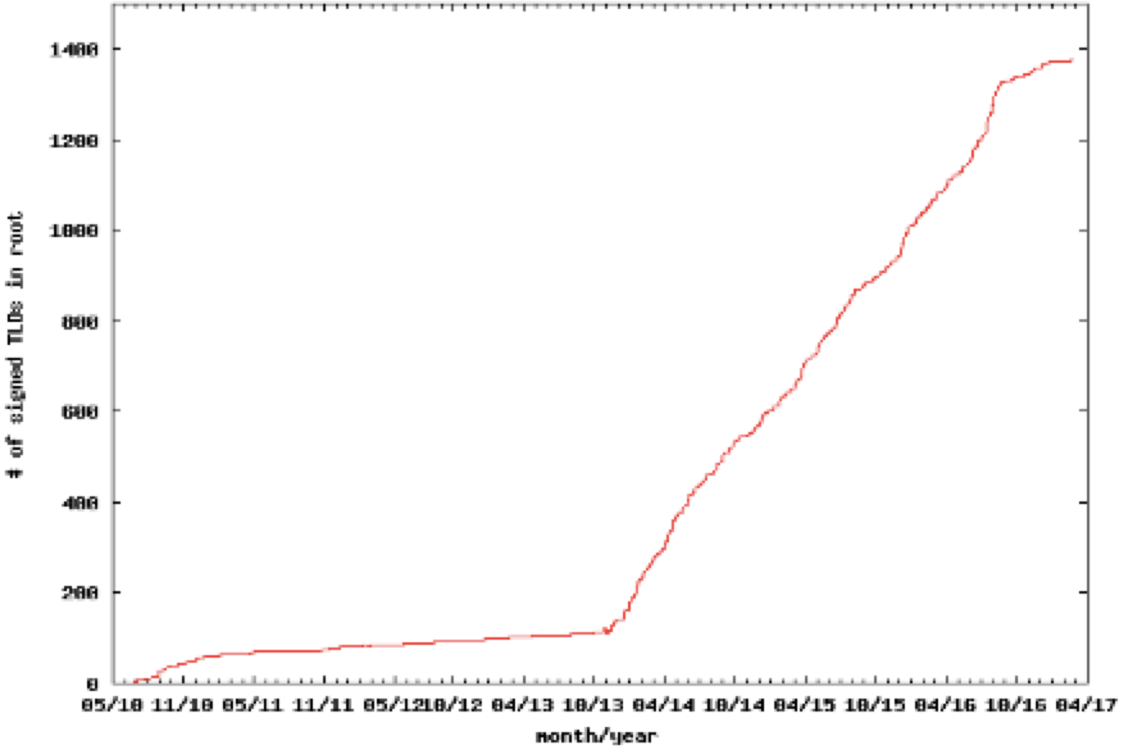


Approx % of these 2LDs signed



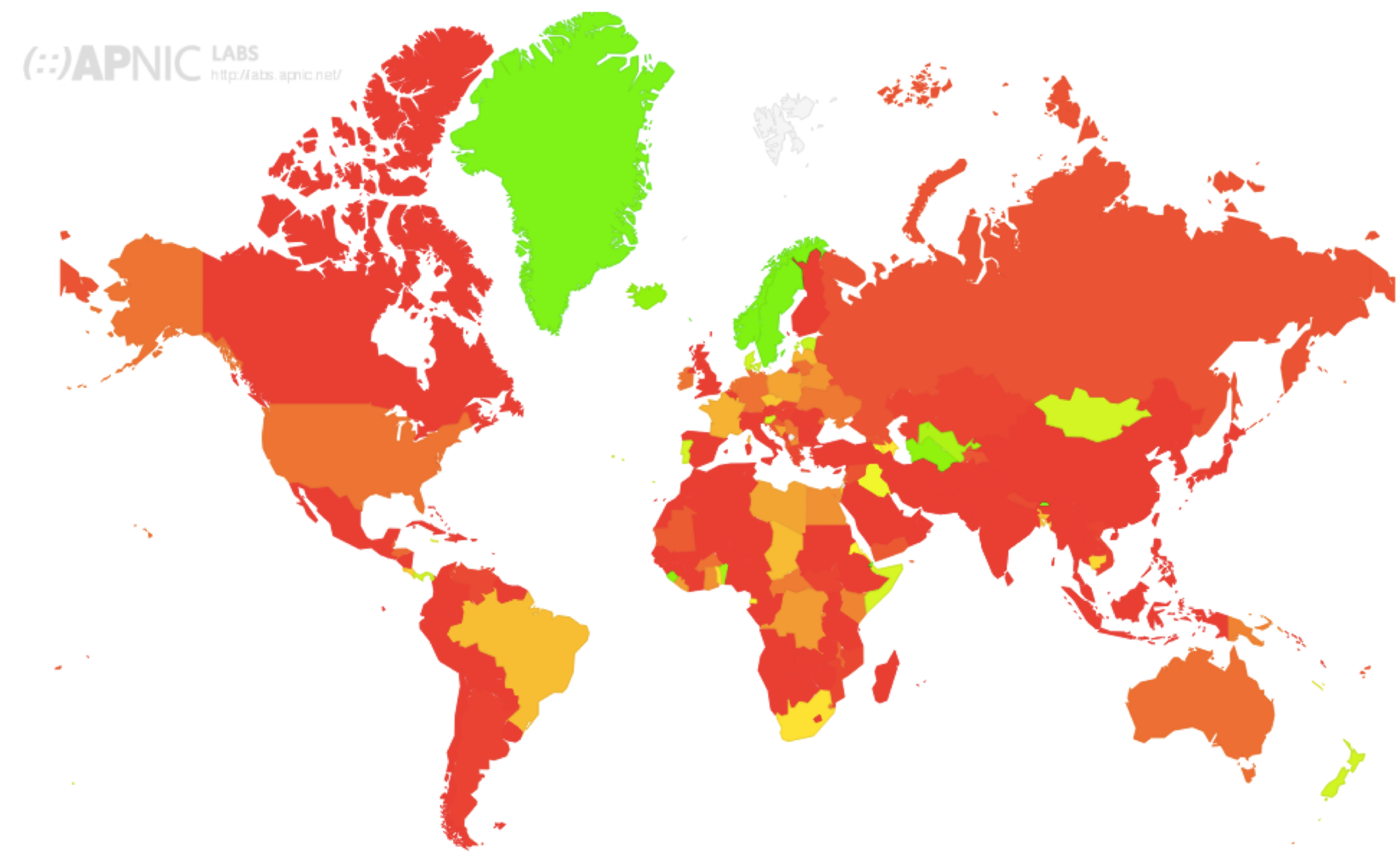
Approx* % Users Validating

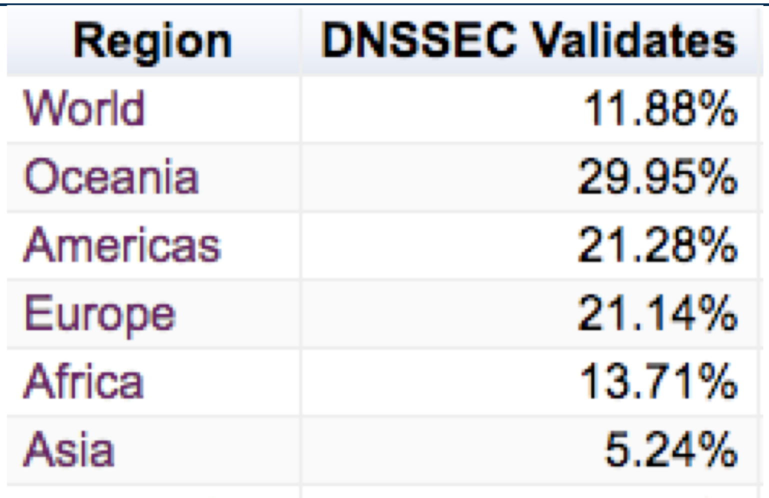
Trend



DNSSEC Validations

DNSSEC Validation Rate by country (%)





Region	DNSSEC Validates
World	11.88%
Oceania	29.95%
Americas	21.28%
Europe	21.14%
Africa	13.71%
Asia	5.24%

Country	DNSSEC Validates
Greenland	89.56%
Kiribati	89.04%
Sweden	81.76%
Australia	24.29%
United States	23.26%
Singapore	22.20%
Malaysia	16.96%
Japan	6.93%
United Kingdom	6.38%
Thailand	4.29%
India	3.30%
China	1.01%

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

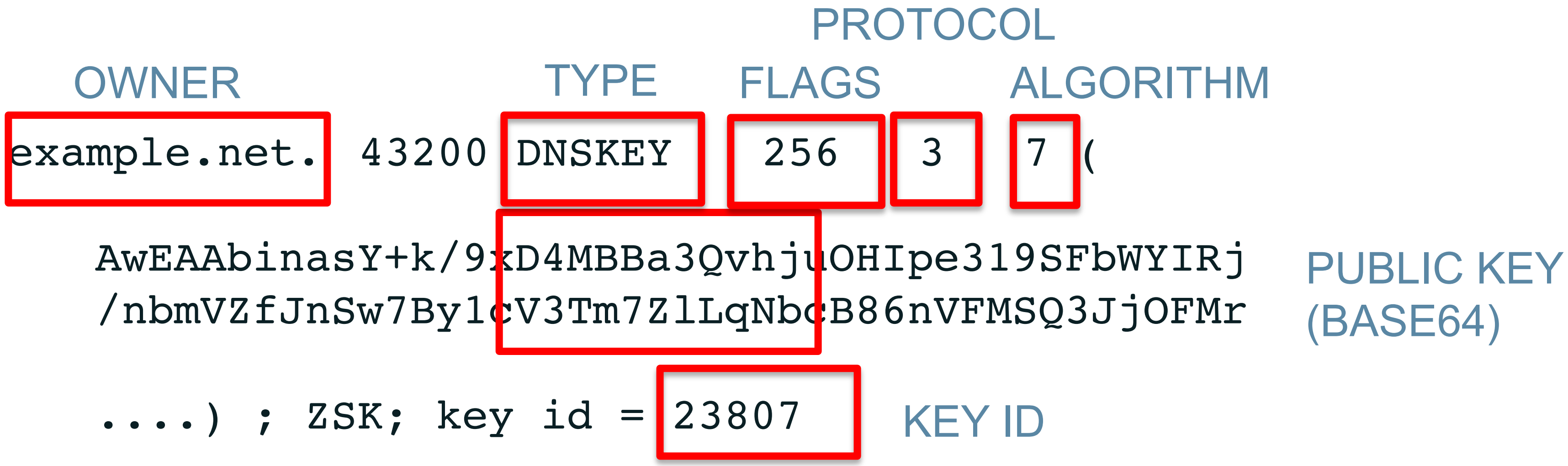
Setting up DNSSEC and Securing Zones

New RRs

- Adds five new DNS Resource Records:

1. DNSKEY: Public key used in zone signing operations.
2. RRSIG: RRset signature
3. NSEC &
4. NSEC3: Returned as verifiable evidence that the name and/or RR type does not exist
5. DS: Delegation Signer. Contains the hash of the public key used to sign the key which itself will be used to sign the zone data. Follow DS RR's until a ”trusted” zone is reached (ideally the root).

New RR: DNSKEY



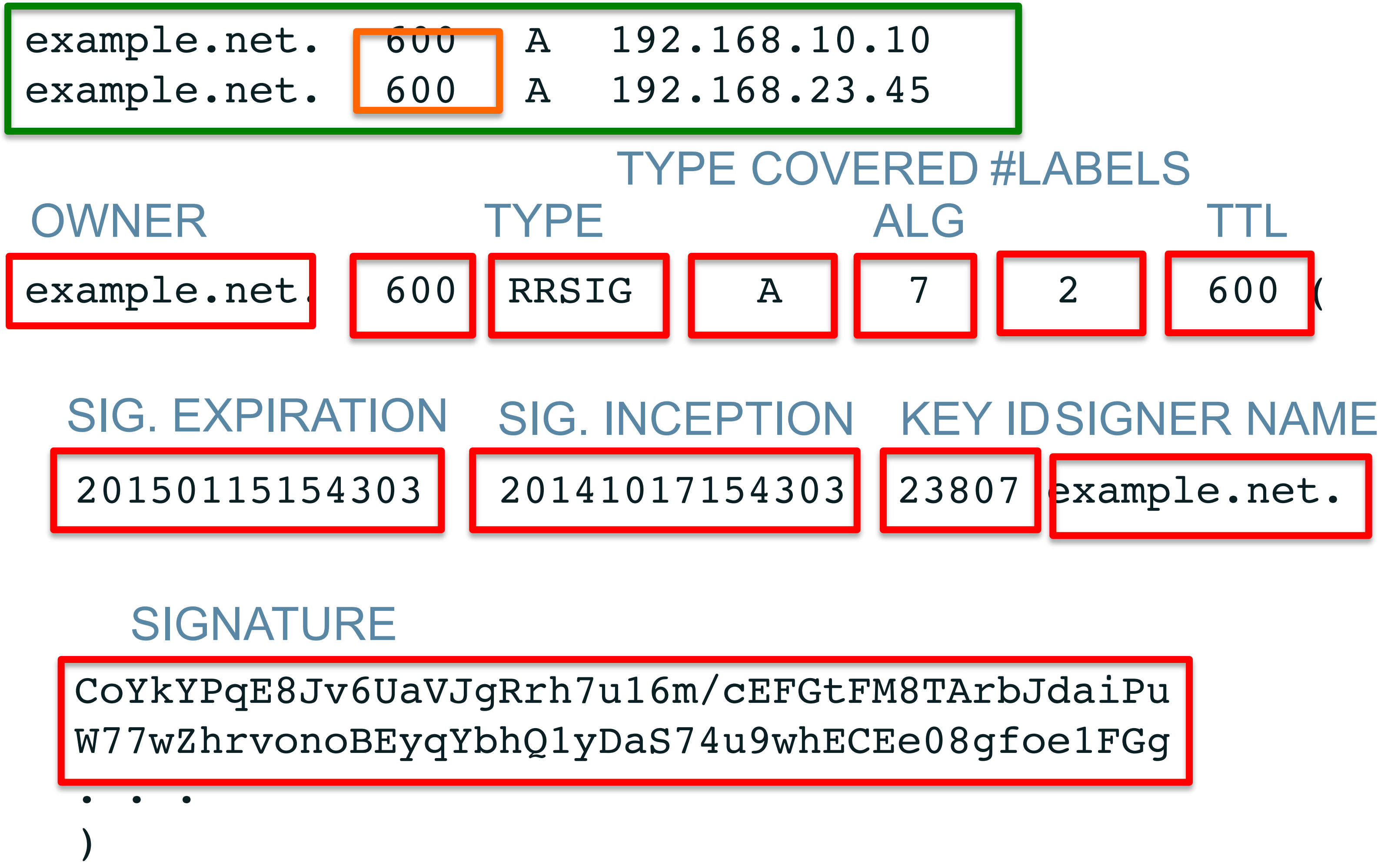
```
example.net.  43200 DNSKEY  256  3  7 (
    AwEAAbinasY+k/9xD4MBBa3QvhjuOHIpe319SFbWYIRj
    /nbmVZfJnSw7By1cV3Tm7ZlLqNbcB86nVFMSQ3JjOFMr
    ....) ; ZSK; key id = 23807
```

- FLAGS determines the usage of the key
- PROTOCOL is always 3 (DNSSEC)
- ALGORITHM can be (3: DSA/SHA-1, 5: RSA/SHA1, 8: RSA/SHA-256, 12: ECC-GOST)
  - http://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xml

DNSKEY: Two Keys, not one…

- Key Signing Key (KSK)
  - Pointed to by parent zone in the form of DS (Delegation Signer). Also called Secure Entry Point.
  - Used to sign the Zone Signing Key
  - Flags: 257
- Zone Signing Key (ZSK)
  - Signed by the KSK
  - Used to sign the zone data RRsets
  - Flags: 256
- This decoupling allows for independent updating of the ZSK without having to update the KSK, and involve the parents (i.e. less administrative interaction)

New RR: RRSIG (Resource Record Signature)



```
example.net.   600   A   192.168.10.10
example.net.   600   A   192.168.23.45
```

TYPE COVERED #LABELS

OWNER TYPE ALG TTL

```
example.net.   600   RRSIG   A   7   2   600 (
```

SIG. EXPIRATION SIG. INCEPTION KEY ID SIGNER NAME

```
20150115154303   20141017154303   23807   example.net.
```

SIGNATURE

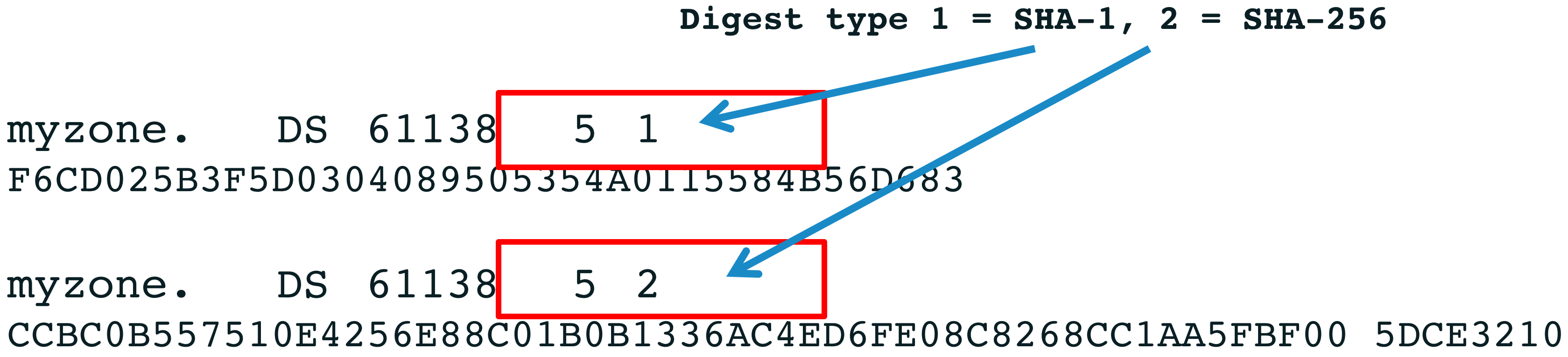
```
CoYkYPqE8Jv6UaVJgRrh7u16m/cEFGtFM8TArbJdaiPu
W77wZhrvonoBEyqYbhQ1yDaS74u9whECEe08gfoe1FGg
. . .
)
```

RRSIG

- Typical default values
  - Signature inception time is 1 hour before.
  - Signature expiration is 30 from now
  - Proper timekeeping (NTP) is required
- What happens when signatures run out?
  - SERVFAIL
  - Domain effectively disappears from the Internet for validating resolvers
- Note that keys do not expire
- No all RRSets need to be resigned at the same time

New RR: DS (Delegation Signer)

- Hash of the KSK of the child zone
- Stored in the parent zone, together with the NS RRs indicating a delegation of the child zone.
- The DS record for the child zone is signed together with the rest of the parent zone data
- NS records are NOT signed (they are a hint/pointer)



Digest type 1 = SHA-1, 2 = SHA-256

```
myzone.   DS  61138   5  1
F6CD025B3F5D0304089505354A0115584B56D683

myzone.   DS  61138   5  2
CCBC0B557510E4256E88C01B0B1336AC4ED6FE08C8268CC1AA5FBF00 5DCE3210
```

Key Rollovers

- Try to minimise impact
  - Short validity of signatures
  - Regular key rollover

- Remember: DNSKEYs do not have timestamps
  - the RRSIG over the DNSKEY has the timestamp

- Key rollover involves second party or parties:
  - State to be maintained during rollover
  - Operationally expensive

Engage with ICANN – Thank You and Questions

ICANN

One World, One Internet

Visit us at **icann.org**

Email: champika.wijayatunga@icann.org

- @icann
- facebook.com/icannorg
- youtube.com/icannnews
- flickr.com/icann
- linkedin/company/icann
- slideshare/icannpresentations
- soundcloud/icann