Introduction to DNS and its vulnerabilities

Olaf M. Kolkman
olaf@nlnetlabs.nl

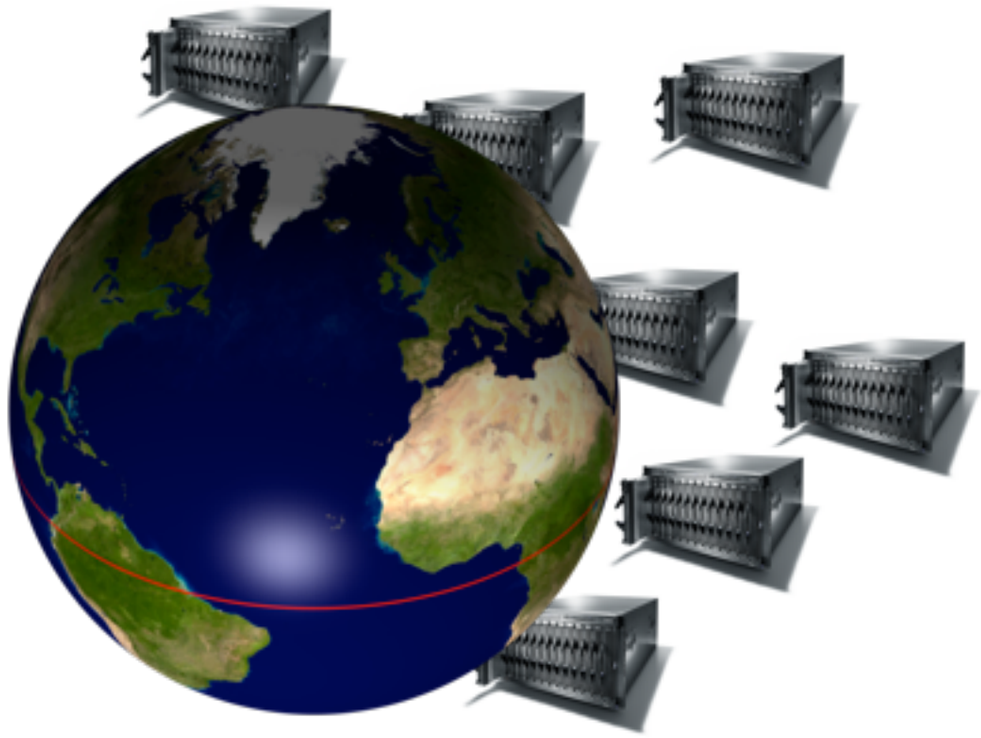
DNSSEC

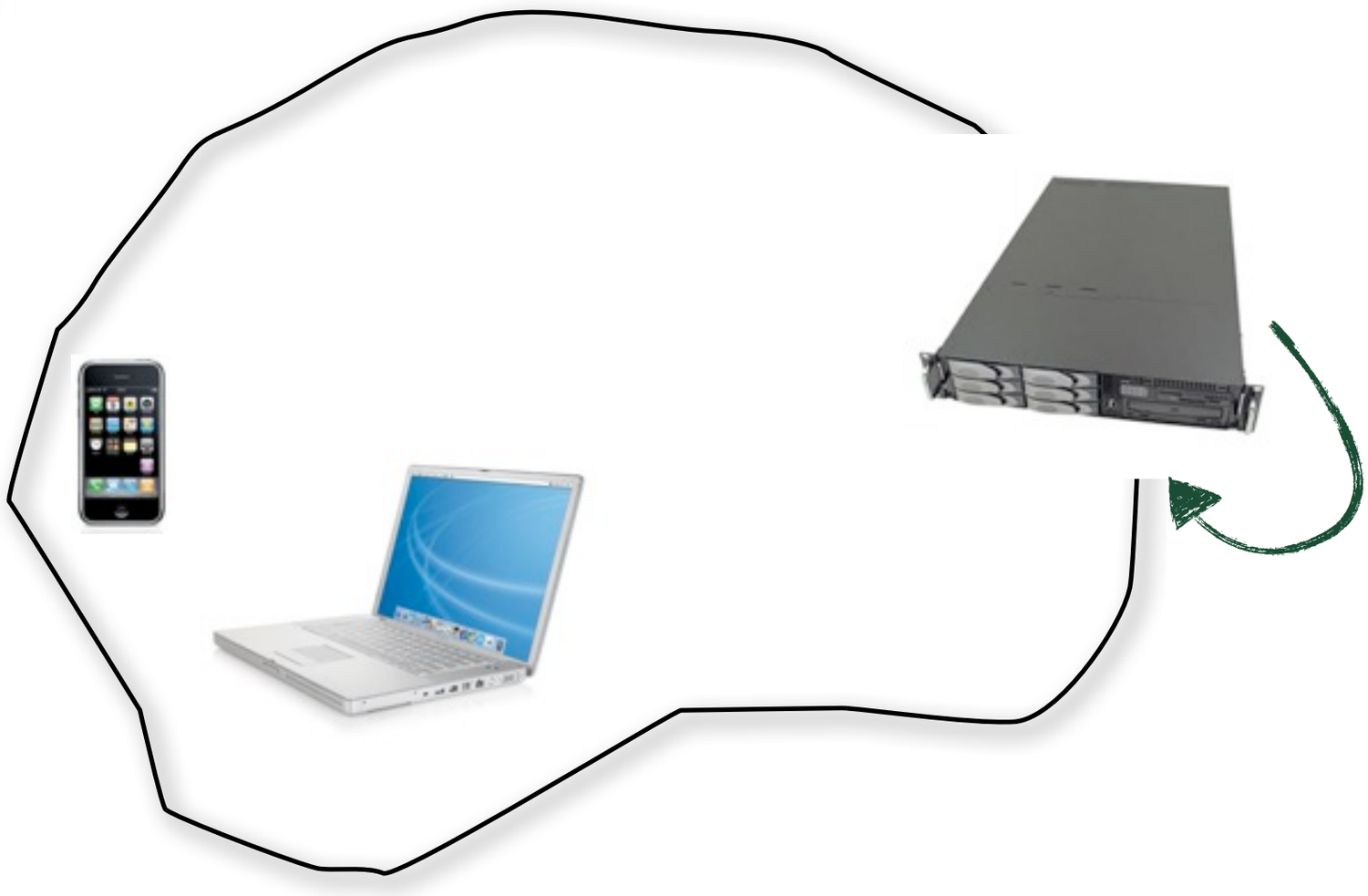
NLnet Labs

source: http://upload.wikimedia.org/wikipedia/commons/b/b7/KoreanPineSeeds.jpg

DNS and DNSSEC in a Nutshell

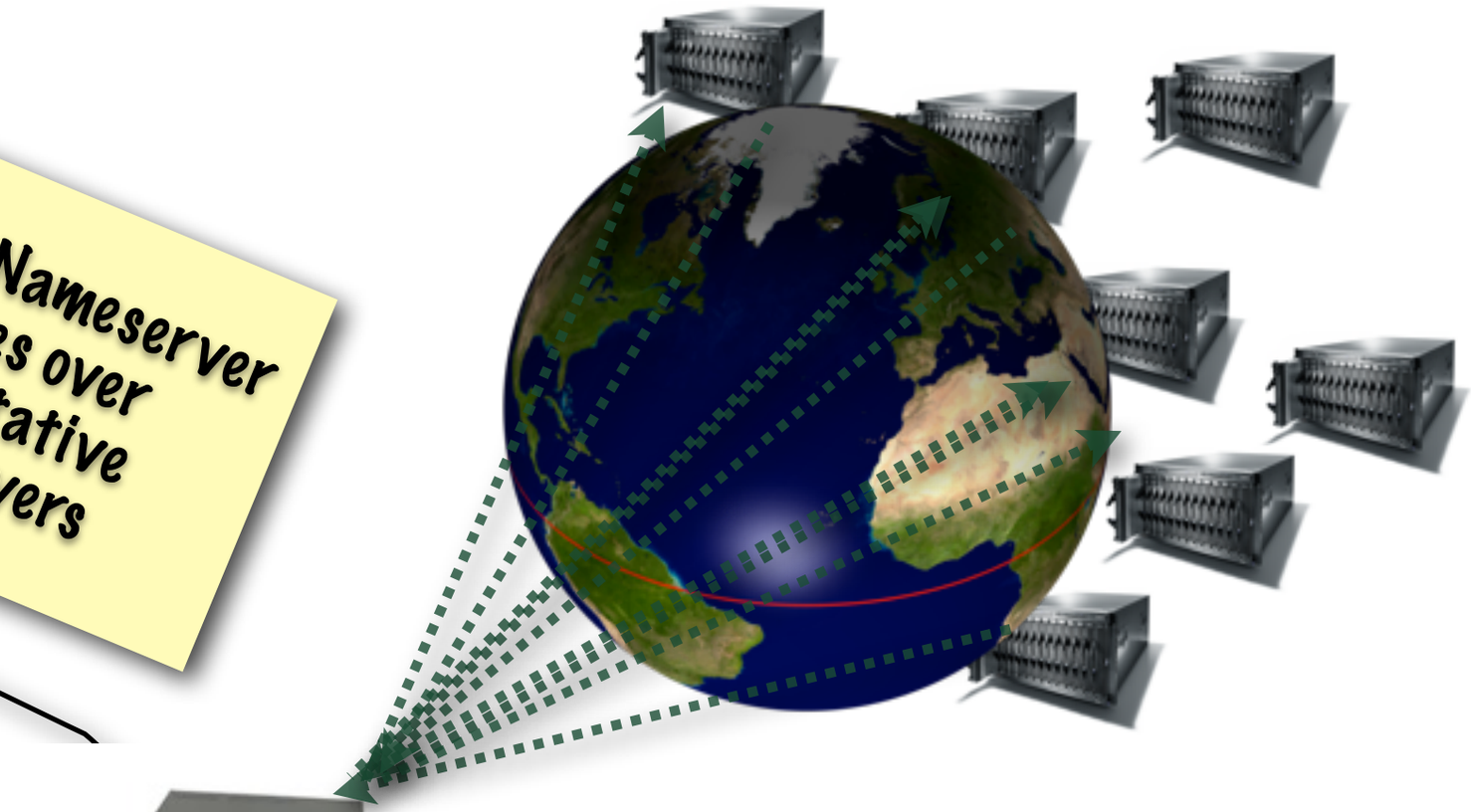
source: http://upload.wikimedia.org/wikipedia/commons/b/b7/KoreanPineSeeds.jpg





NLnet Labs

Recursive Nameserver Recurses over Authoritative nameservers



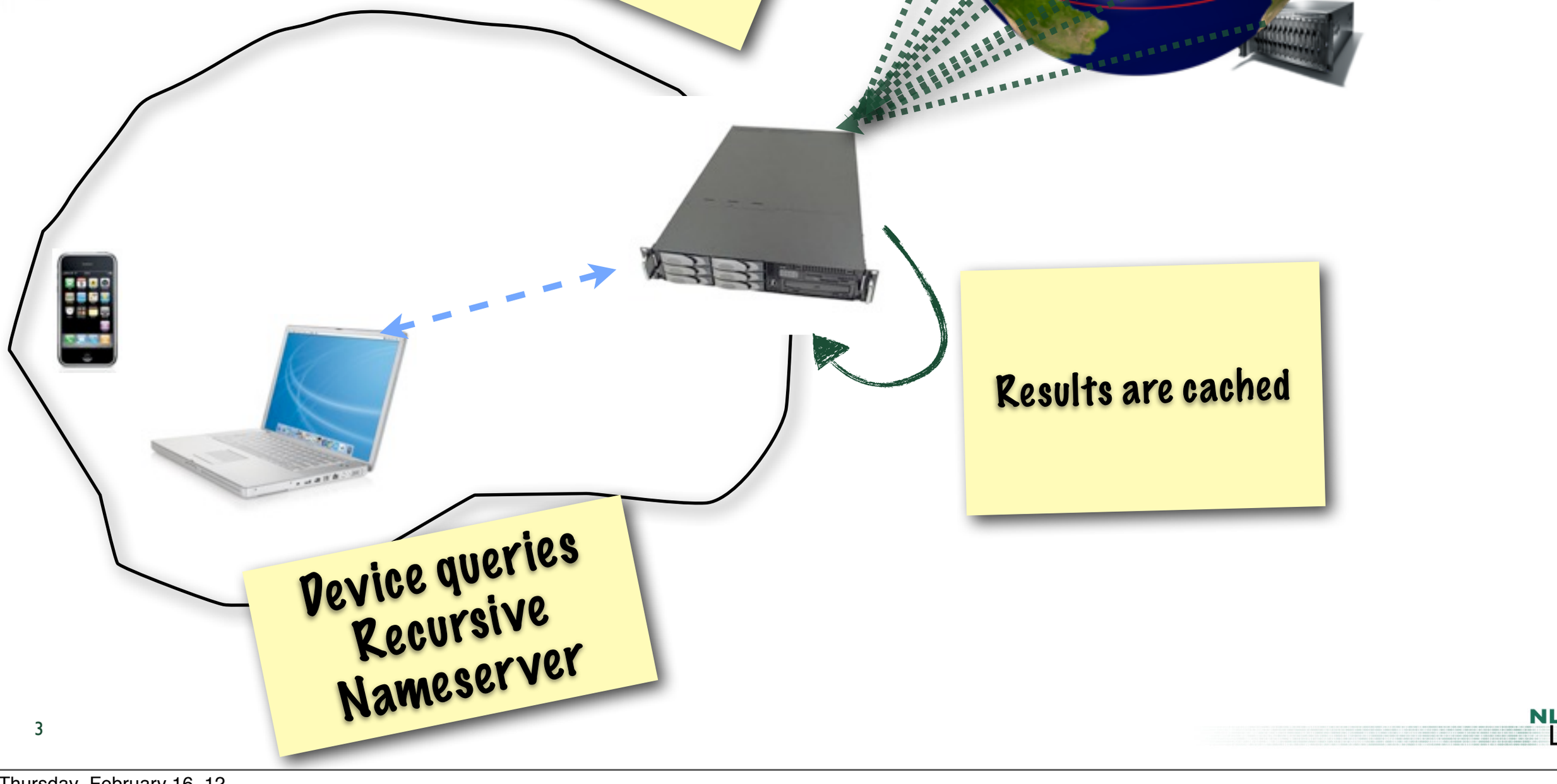
Device queries Recursive Nameserver

Results are cached

NLnet Labs

The DNS is highly distributive

...ve Nameserver
...rses over
...ritative
...meservers



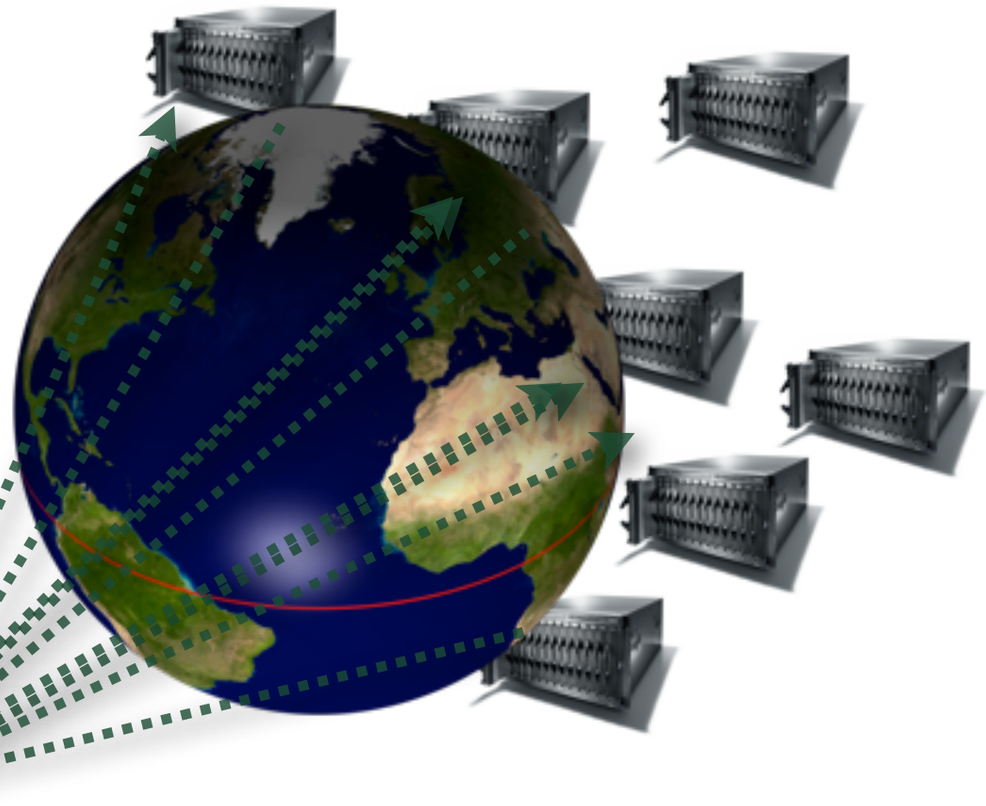
Results are cached

Device queries
Recursive
Nameserver

NLnet Labs

The DNS is highly distributive

ve Nameserver
rses over
ritative
meservers



Device queries
Recursive
Nameserver

DNS is implemented through 100s of thousands of machines

NLnet Labs

Authoritative Nameservers

ROOT

Stub Resolver

Recursive Nameservers

NL

NLnetLabs.NL

Authoritative Nameservers

ROOT

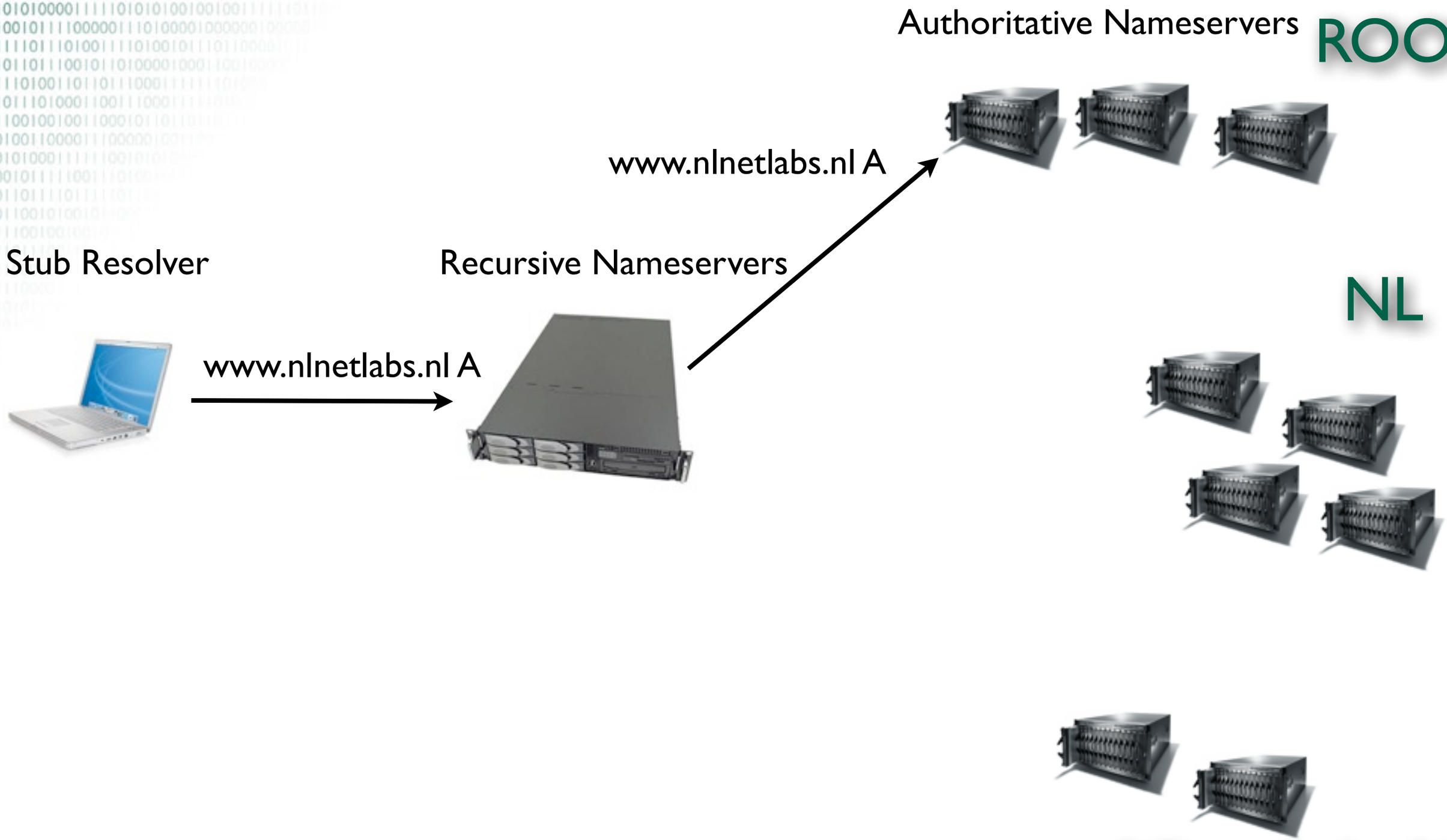
Stub Resolver

www.nlnetlabs.nl A

Recursive Nameservers

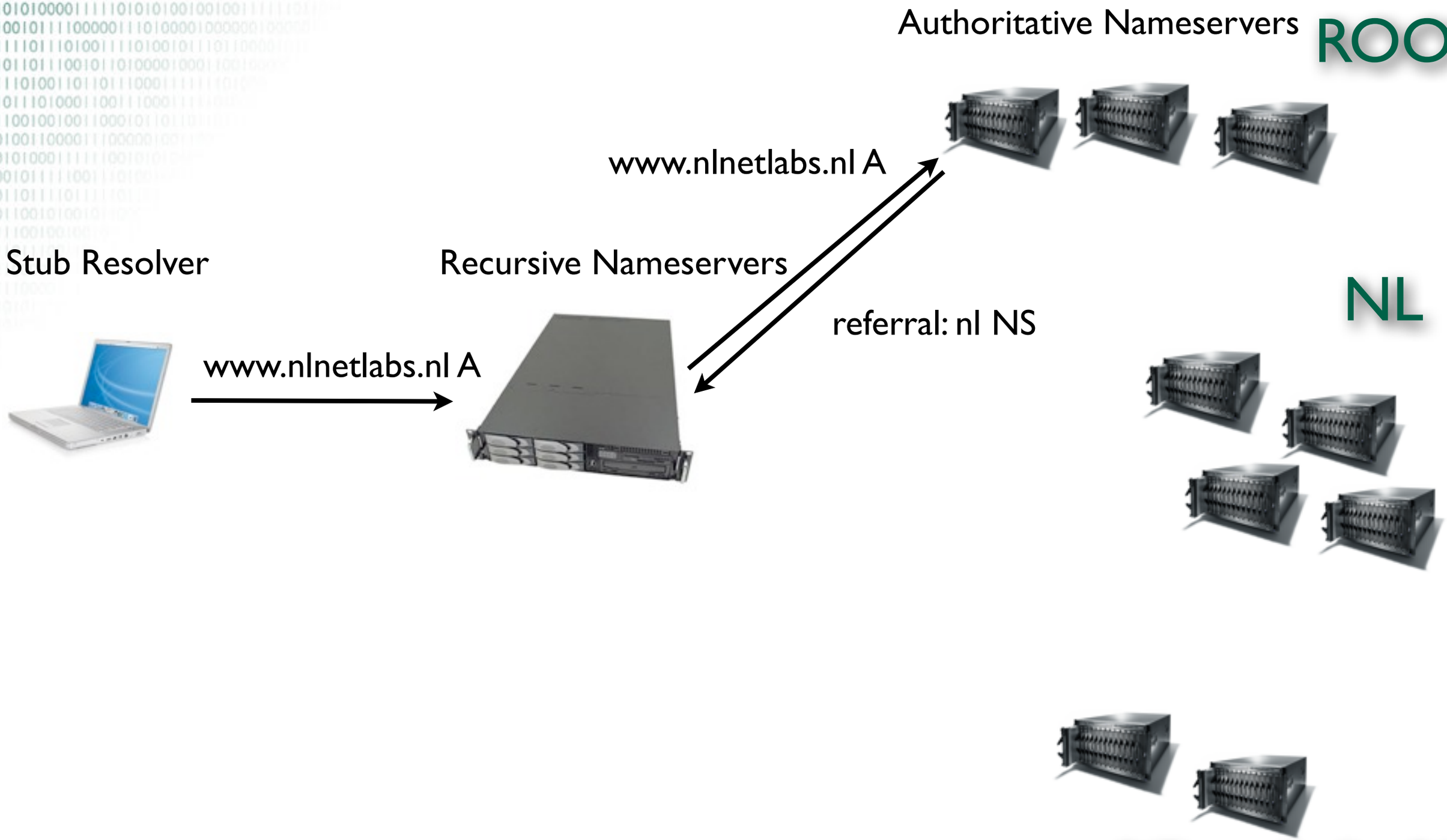
NL

NLnetLabs.NL

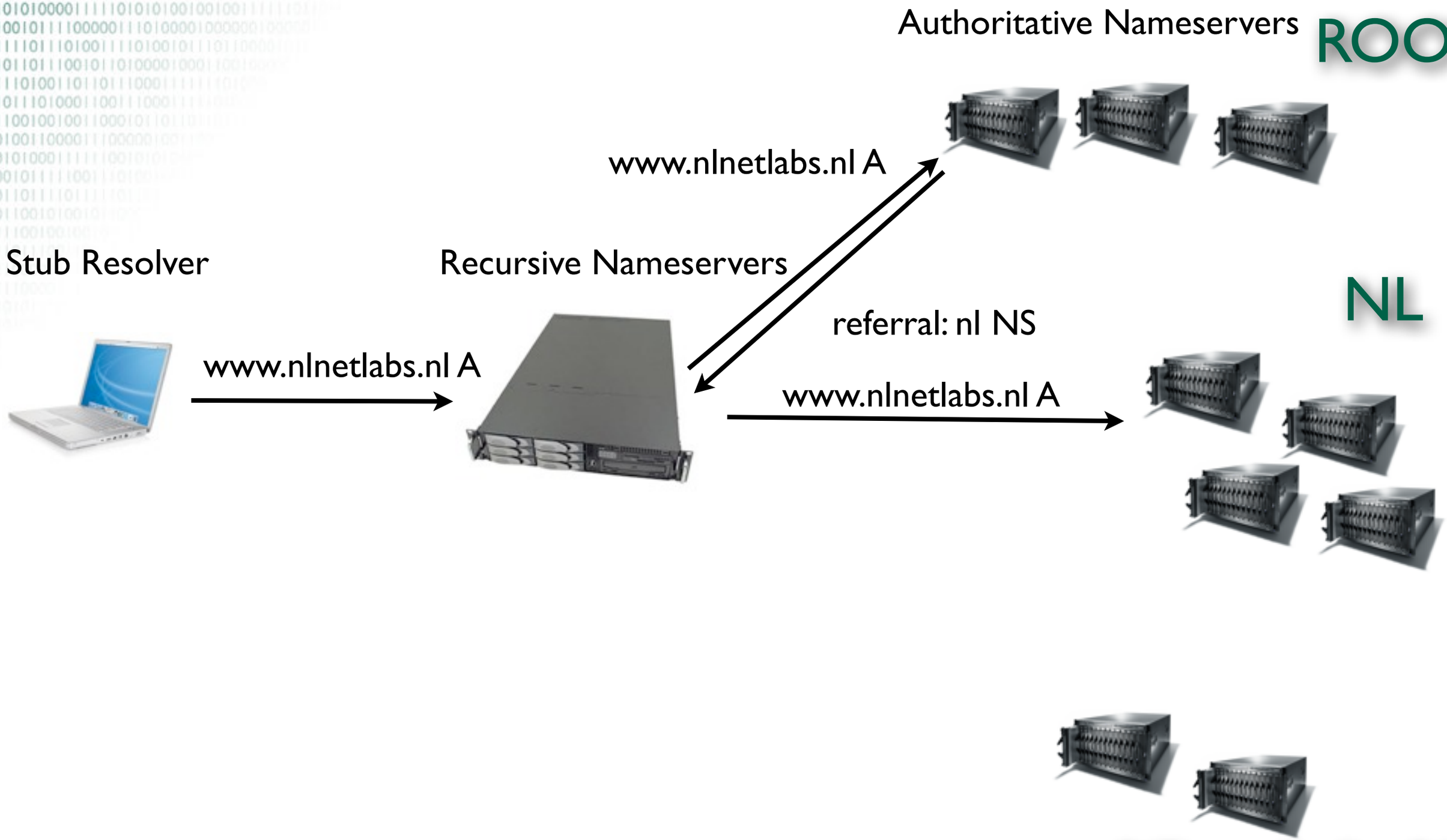


root.hints: location of the root servers

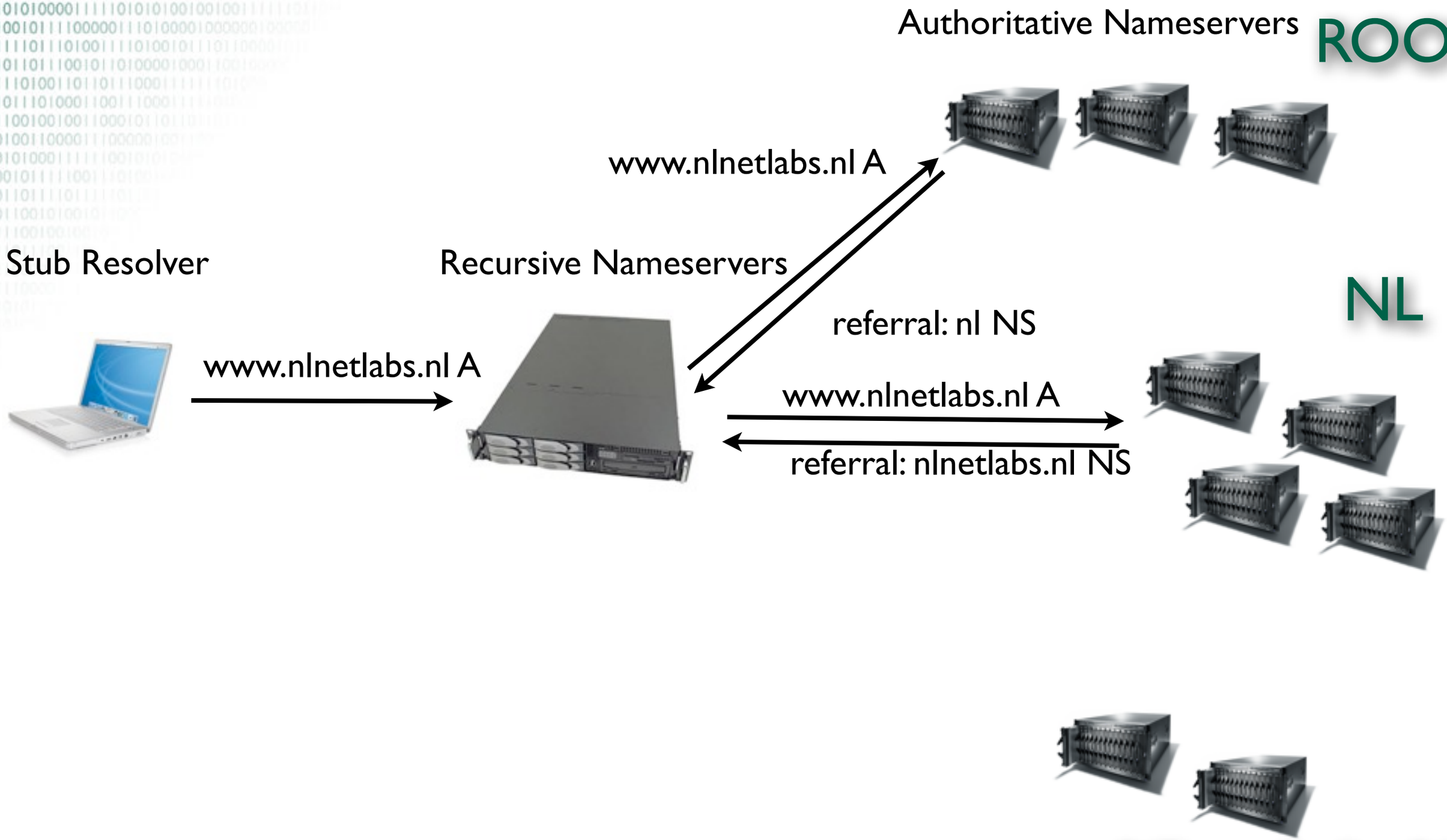
NLnet Labs



root.hints: location of the root servers



root.hints: location of the root servers



root.hints: location of the root servers

Authoritative Nameservers

ROOT

www.nlnetlabs.nl A

Stub Resolver

Recursive Nameservers

www.nlnetlabs.nl A

referral: nl NS

NL

www.nlnetlabs.nl A

referral: nlnetlabs.nl NS

www.nlnetlabs.nl A

NLnetLabs.NL

root.hints: location of the root servers

Authoritative Nameservers

ROOT

www.nlnetlabs.nl A

Stub Resolver

Recursive Nameservers

NL

referral: nl NS

www.nlnetlabs.nl A

www.nlnetlabs.nl A

referral: nlnetlabs.nl NS

www.nlnetlabs.nl A

Answer: www.nlnetlabs.nl A 213.154.224.1

NLnetLabs.NL

root.hints: location of the root servers

Authoritative Nameservers

ROOT

www.nlnetlabs.nl A

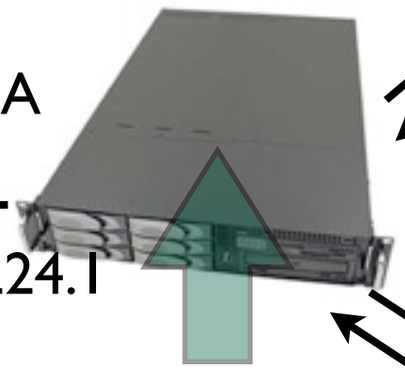
Stub Resolver

Recursive Nameservers

NL

referral: nl NS

www.nlnetlabs.nl A



www.nlnetlabs.nl A

www.nlnetlabs.nl A 213.154.224.1

referral: nlnetlabs.nl NS

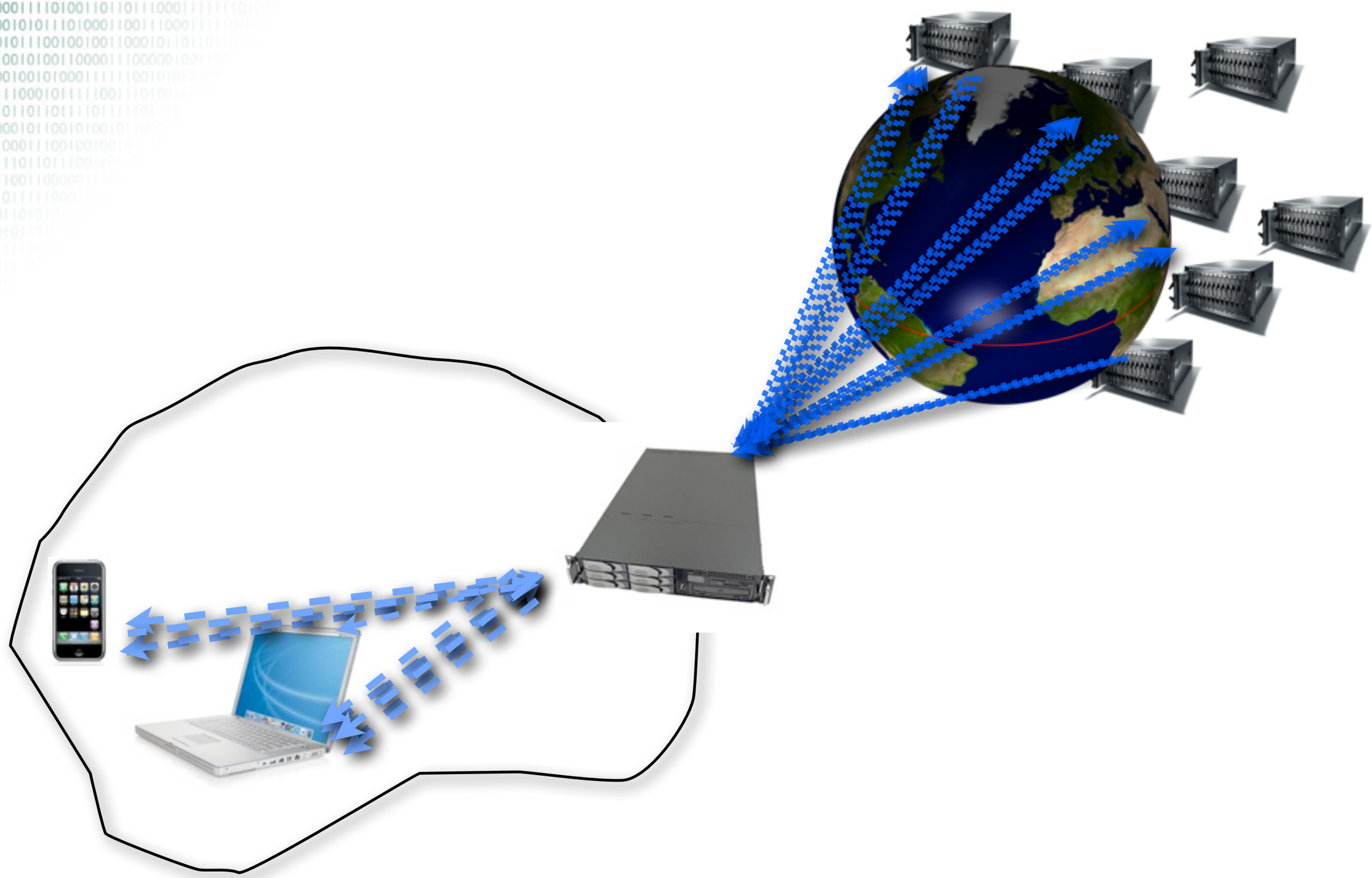
www.nlnetlabs.nl A 213.154.224.1

www.nlnetlabs.nl A

Answer: www.nlnetlabs.nl A 213.154.224.1

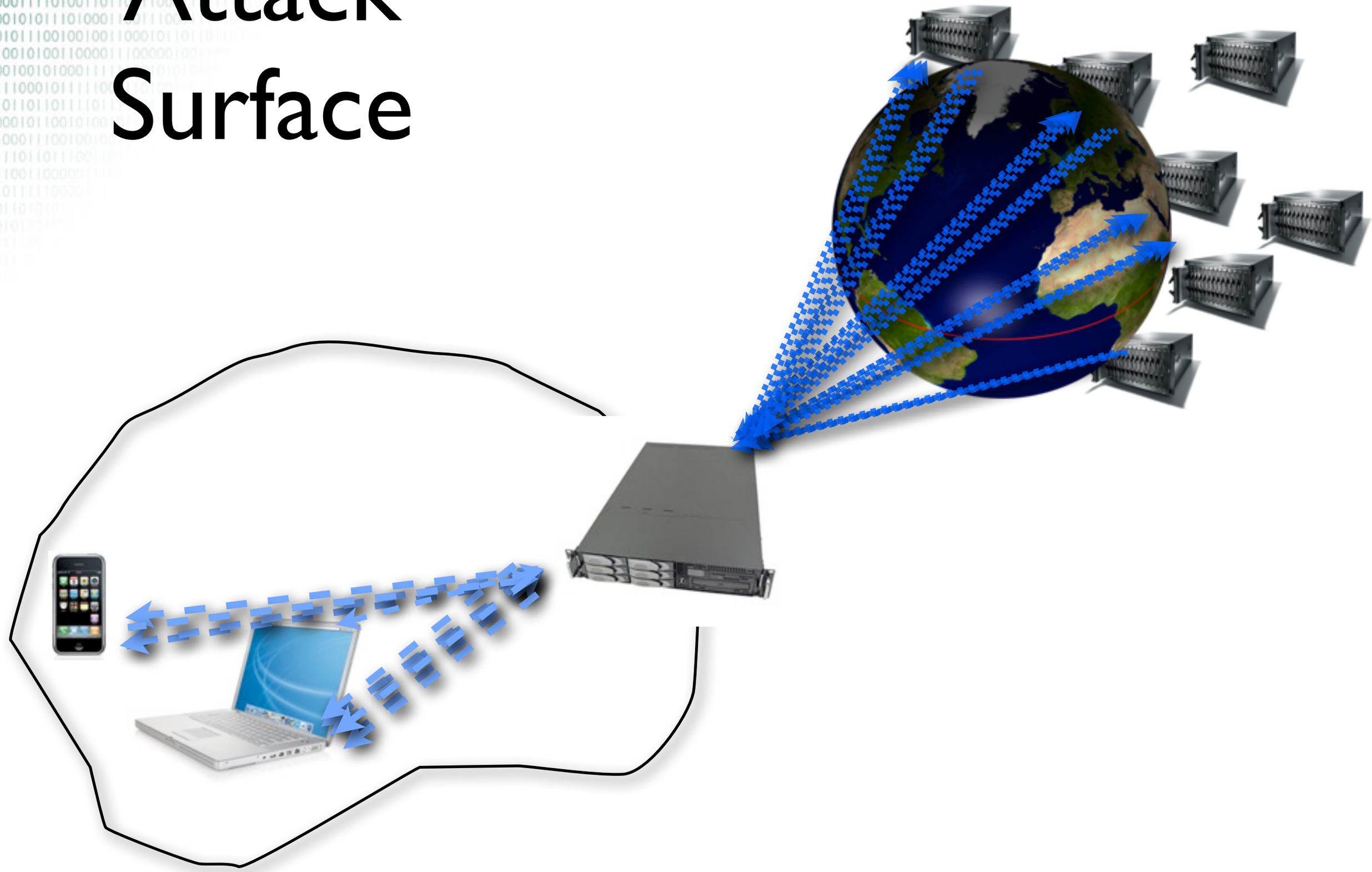
NLnetLabs.NL

root.hints: location of the root servers

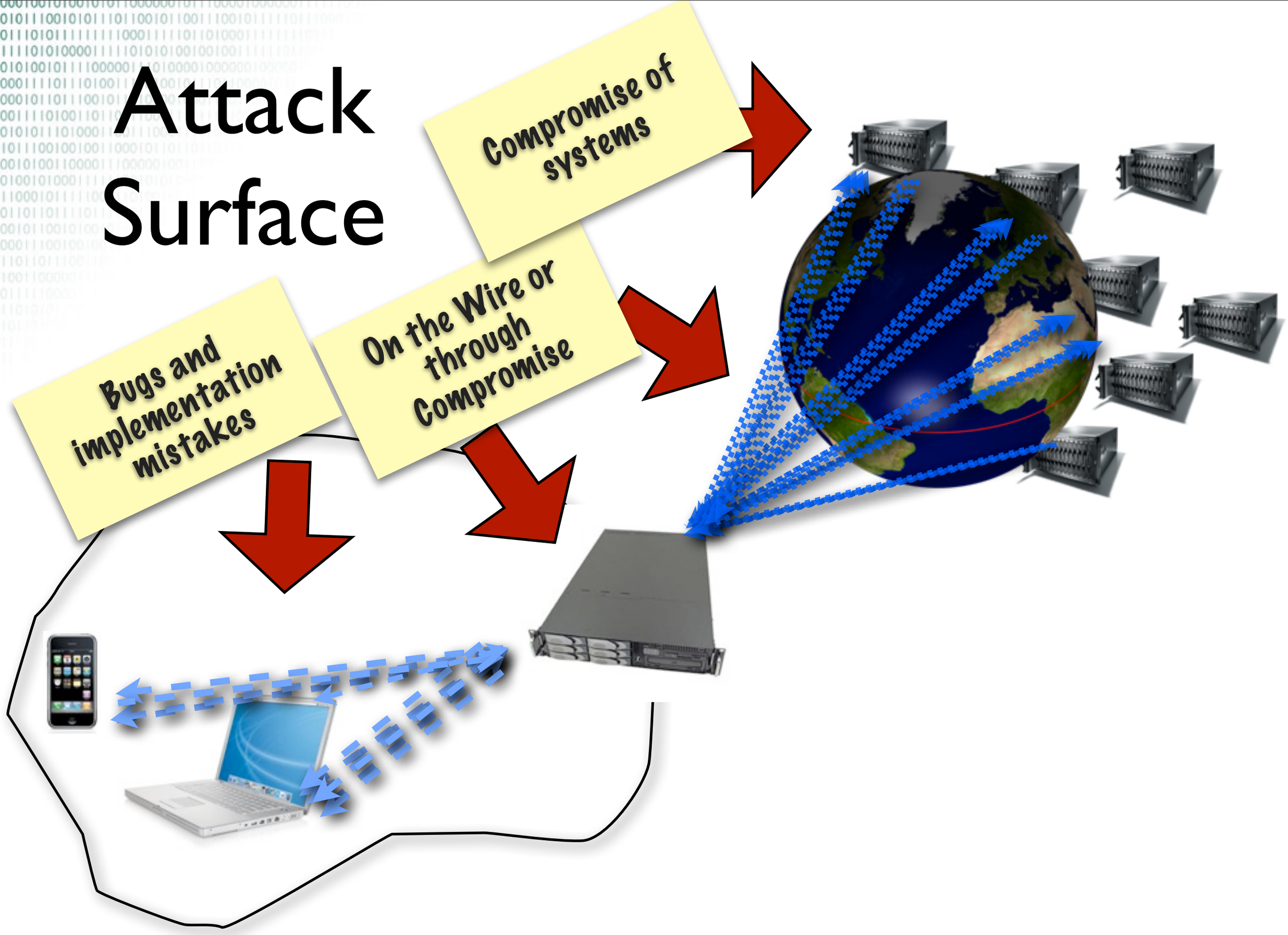


NLnet Labs

Attack Surface



Attack Surface



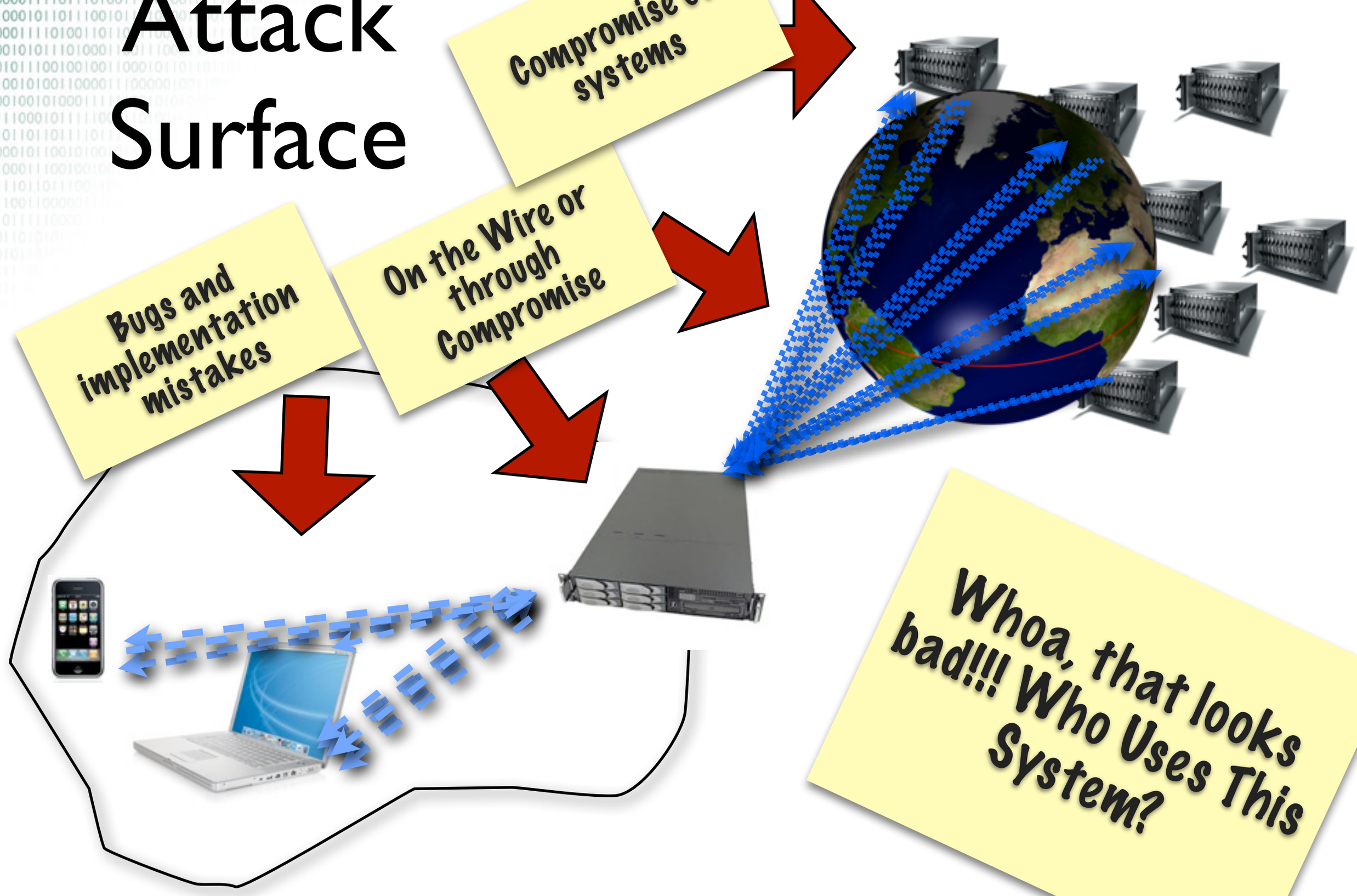
NLnet Labs

Attack Surface

Compromise of systems

On the Wire or through Compromise

Bugs and implementation mistakes



Whoa, that looks bad!!! Who Uses This System?

NLnet Labs

enterprise

Recursive DNS

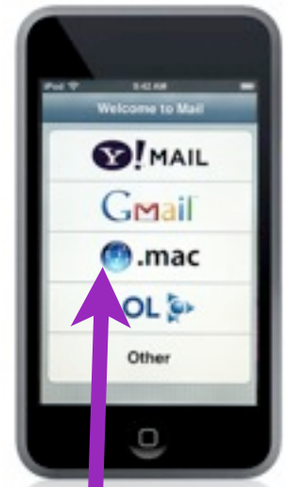
Mail server

Internet

NLnet Labs

enterprise

Recursive DNS



Mail server

Mail server

Internet

NLnet Labs

enterprise

Recursive DNS

Mail server

Internet

NLnet Labs

enterprise

Recursive DNS

Internet

Mail server

NLnet Labs

enterprise

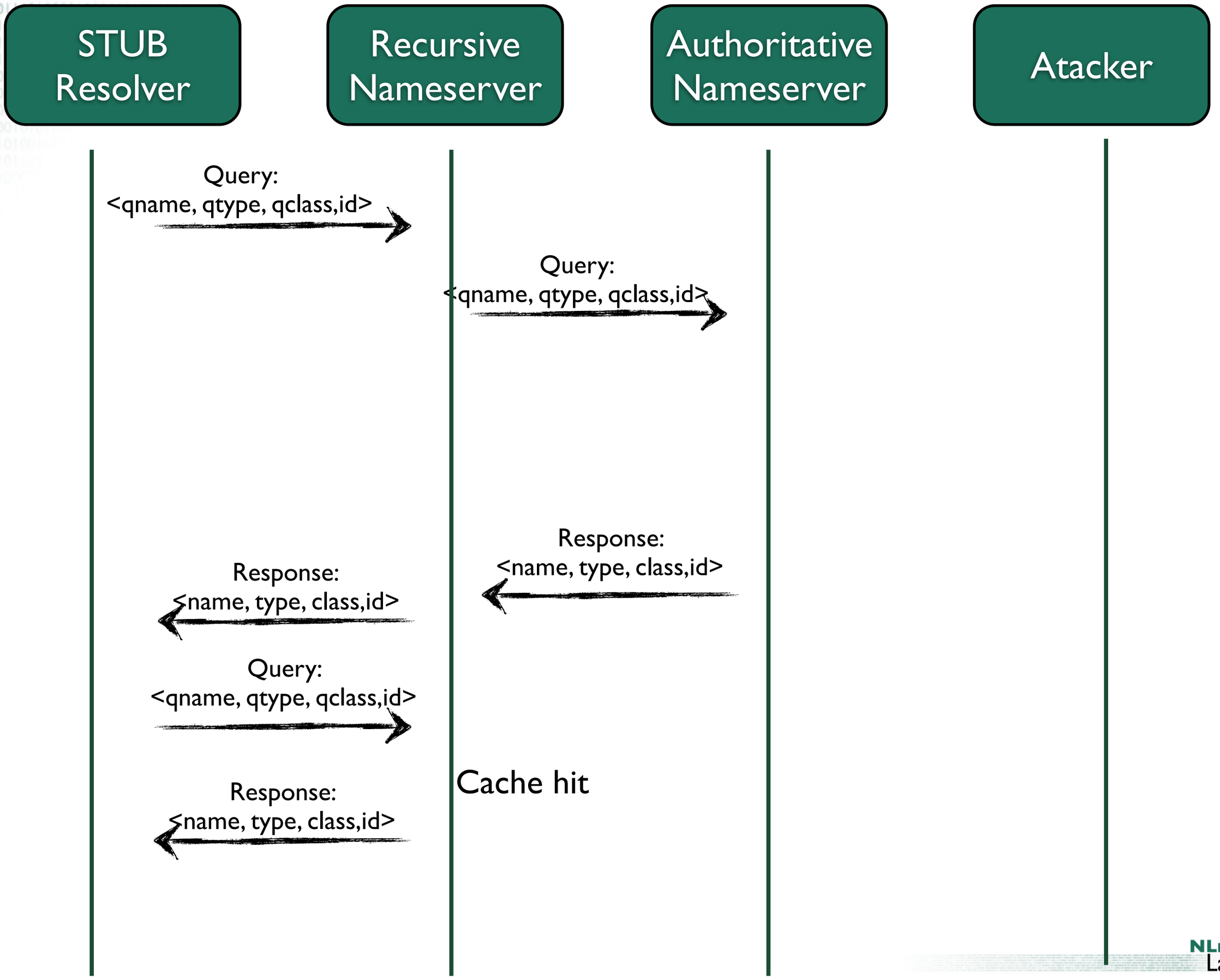
Recursive DNS

Mail server

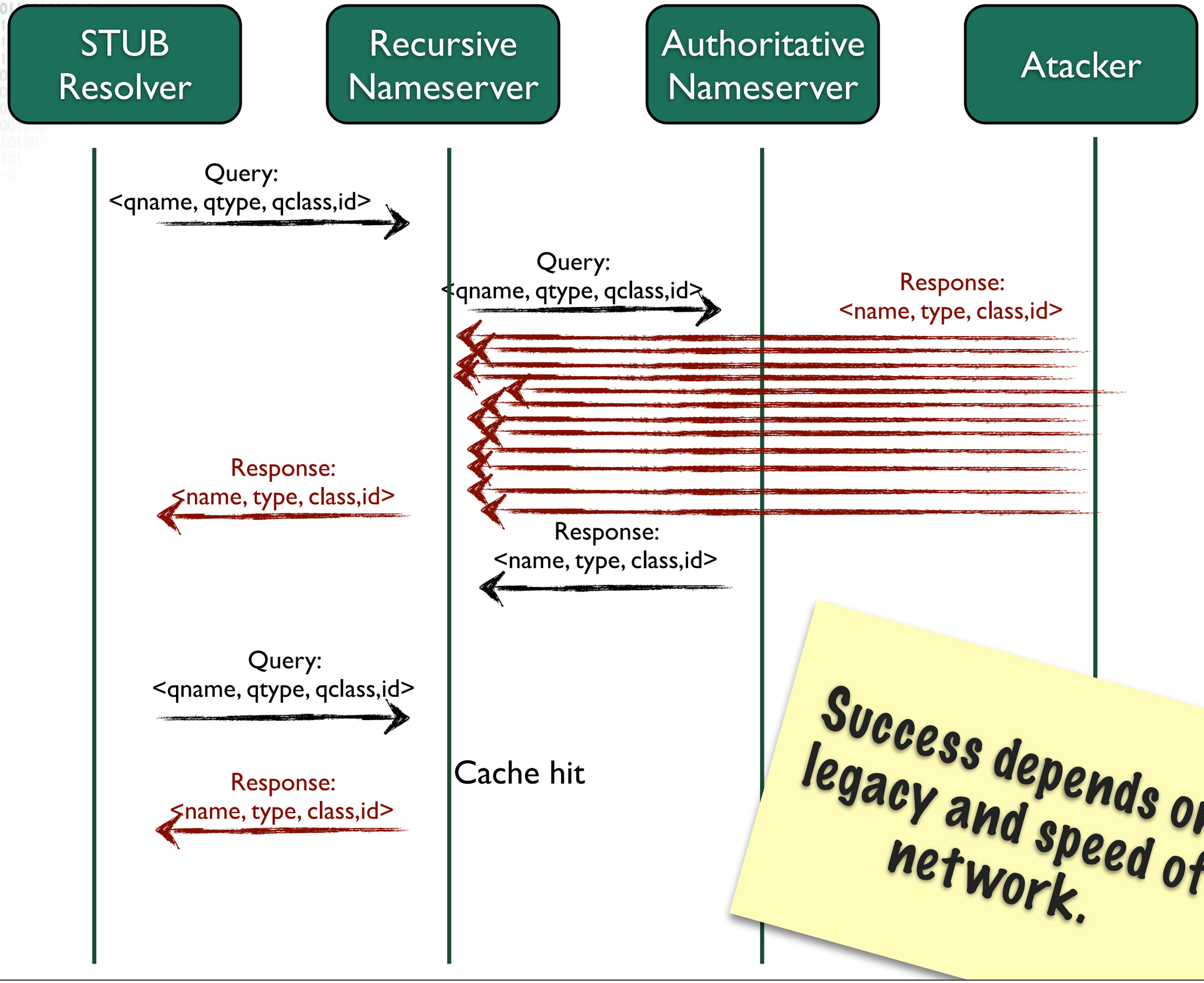
Mail server

Internet

Labs


STUB Resolver
Recursive Nameserver
Authoritative Nameserver
Atacker
Query: <qname, qtype, qclass,id>
Query: <qname, qtype, qclass,id>
Response: <name, type, class,id>
Response: <name, type, class,id>
Query: <qname, qtype, qclass,id>
Cache hit
Response: <name, type, class,id>

NLnet Labs


STUB Resolver
Recursive Nameserver
Authoritative Nameserver
Atacker
Query: <qname, qtype, qclass,id>
Query: <qname, qtype, qclass,id>
Response: <name, type, class,id>
Response: <name, type, class,id>
Response: <name, type, class,id>
Query: <qname, qtype, qclass,id>
Cache hit
Response: <name, type, class,id>
Success depends on legacy and speed of network.

STUB Resolver

Recursive N...rver

Authoritative Nameserver

Atacker

And on various properties that the attacher needs to match

Query:
qtype, qclass,id>

Response:
<name, type, class,id>

Response:
<name, type, class,id>

Response:
<name, type, class,id>

Query:
<qname, qtype, qclass,id>

Cache hit

Response:
<name, type, class,id>

Success depends on legacy and speed of network.

STUB Resolver

Recursive Nameserver

Authoritative Nameserver

Atacker

And on various properties that the attacher needs to match

Query ID

Query:
qtype, qclass,id>

Response:
<name, type, class,id>

Response:
<name, type, class,id>

Query:
<qname, qtype, qclass,id>

Response:
<name, type, class,id>

Cache hit

Success depends on legacy and speed of network.

STUB Resolver

Recursive N[illegible]rver

Authoritative Nameserver

Atacker

And on various properties that the attacher needs to match

Query ID

Source Port

Query:
qtype, qclass,id>

Response:
<name, type, class,id>

Response:
<name, type, class,id>

Query:
<qname, qtype, qclass,id>

Response:
<name, type, class,id>

Cache hit

Success depends on legacy and speed of network.

STUB Resolver

Recursive N[illegible]rver

Authoritative Nameserver

Atacker

And on various properties that the attacher needs to match

Query ID

Source Port

0X20

Query:
qtype, qclass,id>

Response:
<name, type, class,id>

Response:
<name, type, class,id>

<qname, qtype, qclass,id>

Response:
<name, type, class,id>

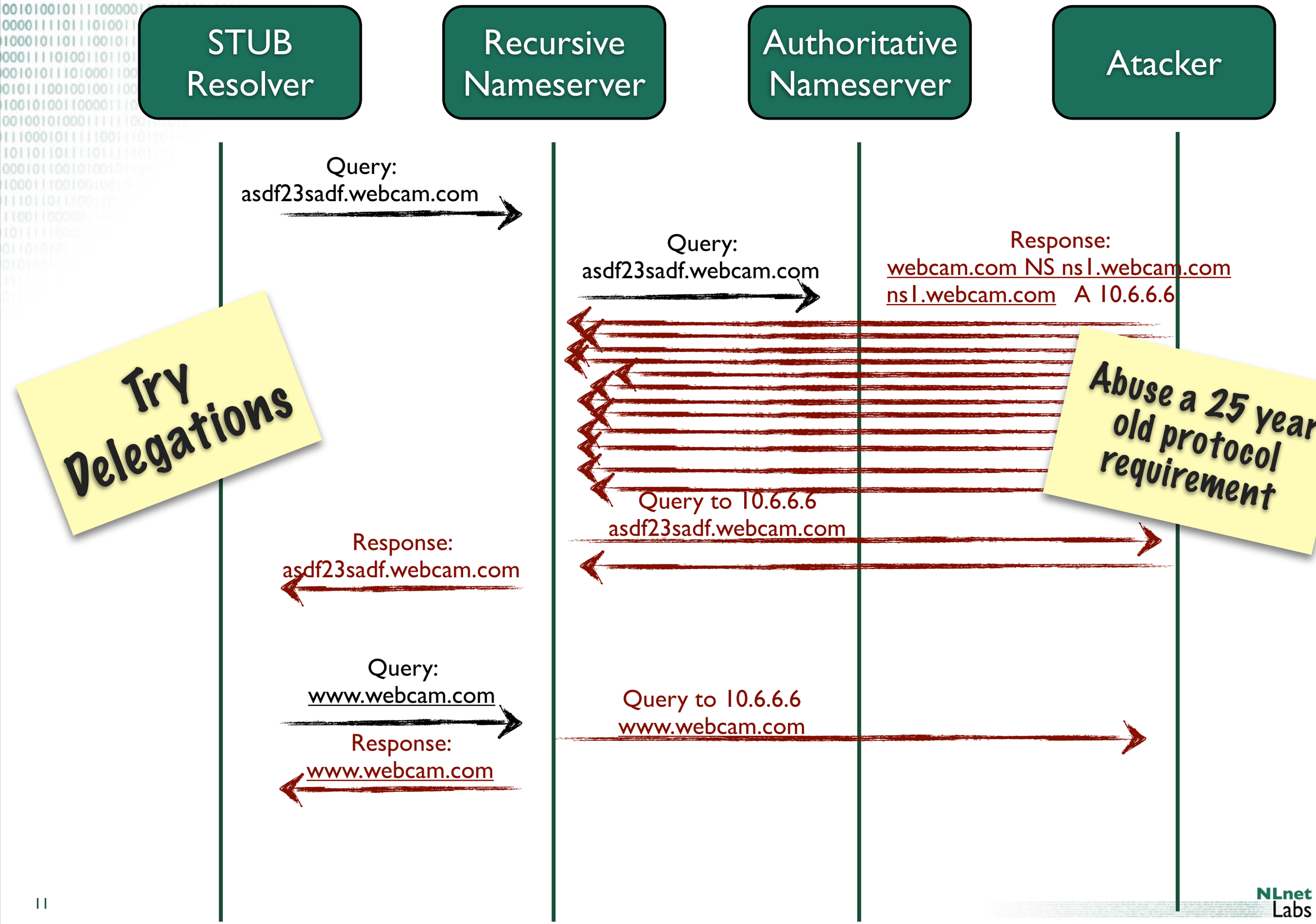
Cache hit

Success depends on legacy and speed of network.

TTL saves you?!?
I don't think so....

Dan Kaminsky's image from zdnet.com

Security Popstar


STUB Resolver
Recursive Nameserver
Authoritative Nameserver
Atacker
Query: asdf23sadf.webcam.com
Query: asdf23sadf.webcam.com
Response: webcam.com NS ns1.webcam.com
ns1.webcam.com A 10.6.6.6
Try Delegations
Abuse a 25 year old protocol requirement
Query to 10.6.6.6 asdf23sadf.webcam.com
Response: asdf23sadf.webcam.com
Query: www.webcam.com
Query to 10.6.6.6 www.webcam.com
Response: www.webcam.com

NLnet Labs

Do attacks happen in practice?

Would you notice?

NLnet Labs

Do attacks happen in practice?

Why would one attack the DNS?

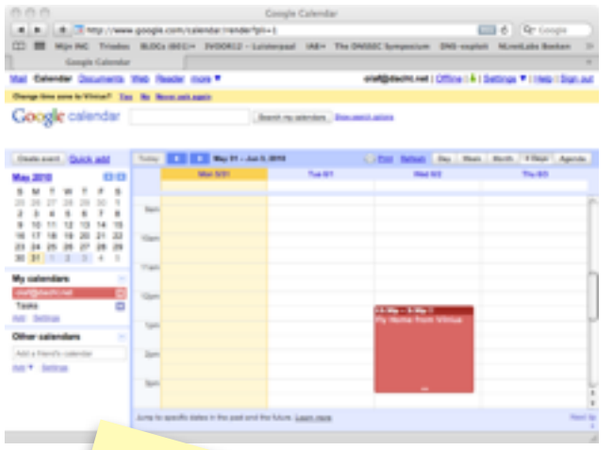
While one could be doing other things

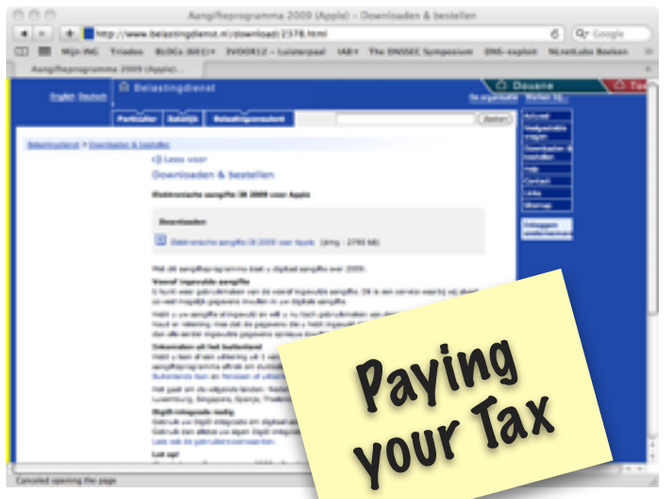
NLnet Labs

How to Protect?

Why would one attack the DNS?

Follow the Money





NLnet Labs

Money

Don't all these transactions use SSL and Certificates?

The role of a CA

3rd party trust broker

NLnet Labs

The role of a CA

3rd party trust broker

Subject Requests

NLnet Labs

The role of a CA

3rd party trust broker

Subject Requests

RA performs checks

NLnet Labs

The role of a CA

3rd party trust broker

Subject Requests

RA performs checks

RA tells CA to sign

NLnet Labs

The role of a CA

3rd party trust broker

Subject Requests

RA performs checks

RA tells CA to sign

Browser trusts CA signed certificates

NLnet Labs

The role of a CA

3rd party trust broker

EV Extended Validation

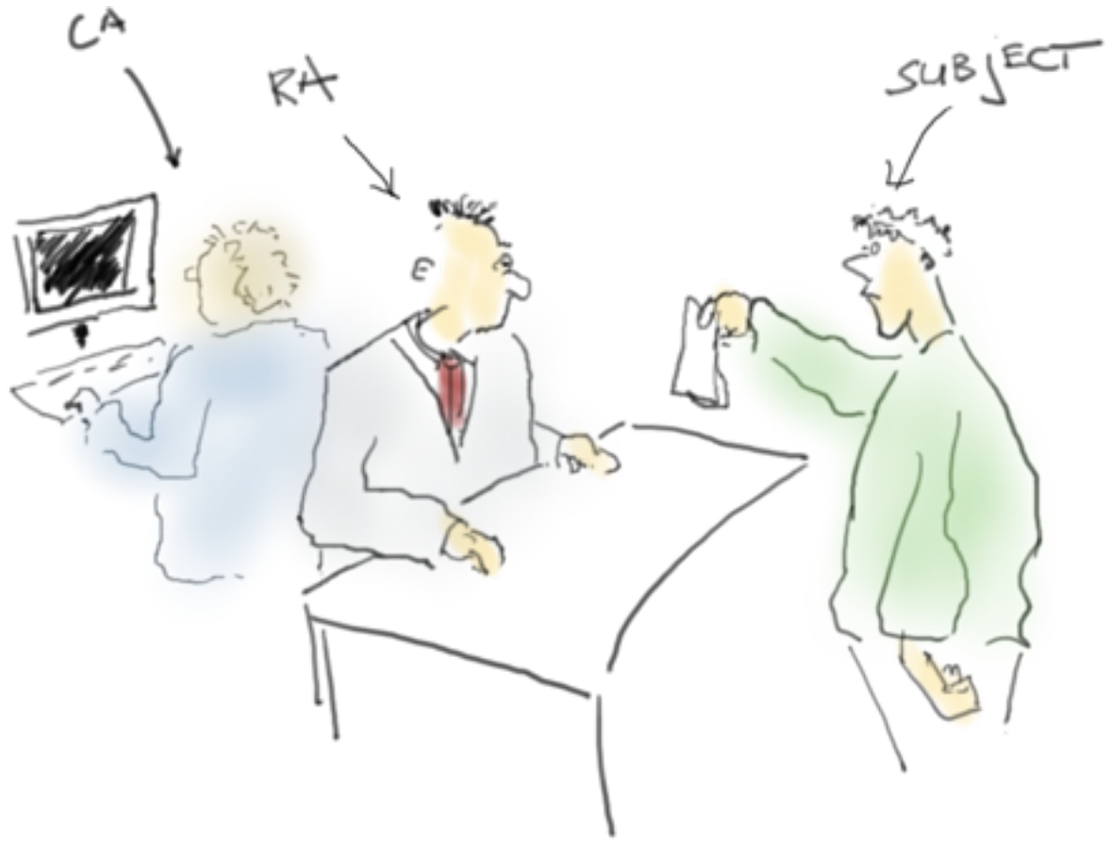
Subject Requests

RA performs checks

RA tells CA to sign

Browser trusts CA signed certificates

NLnet Labs



However all these little men are a wee bit expensive

NLnet Labs

However all these little men are a wee bit expensive

AUTOMATE THE LOT

DV
Domain Validation

Subject: Please sign certificate for Example.com

RA sends a mail to well known address @example.com

When mail returned CA will sign

NLnet Labs

DV
Domain Validation

All these checks are based on information fetched from the DNS

Hold that thought for Jakob's presentation

NLnet Labs

Provisioning Vulnarabilities

DNS System Vulnerabilities

Registrars & Registrants

Server vulnarability

Man in the Middle

Secondary DNS

Registry

pri ry DNS

Secondary DNS

spoofing & Man in the Middle

NLnet Labs

NLnet Labs

Taking Unbound as example

Other servers might make other choices, but any modern resolver takes similar approaches

DNSSEC

NLnet Labs

Security Choices in Unbound

- In general, a modern paranoid resolver
- DNSSEC support.
- RFC 2181 support completely
- Fine grained. Keeps track of where RRSets came from and won't upgrade them into answers.
- Does not allow RRSets to be overridden by lower level rrsets

Filtering

- Scrubber:
- Only in-bailiwick data is accepted in the answer
  - The answer section must contain only answer
  - CNAME, DNAME checked that chain is correct
    - CNAME cut off and only the first CNAME kept
      - Lookup rest yourself do not trust other server
    - DNAME synthesize CNAME by unbound do not trust other server. Also cut off like above.
    - DNAME from cache only used if DNSSEC-secure.

Filtering II

- No address records in authority, additional section unless relevant – i.e. mentioned in a NS record in the authority section.
- Irrelevant data is removed
  - When the message only had preliminary parsing and has not yet been copied to the working region of memory

Entropy

- Randomness protects against spoof
  - Arc4random() (OpenBSD): crypto strong. May not be perfectly random, but predicting it is a cryptographical breakin.
    - Real entropy from OS as seed
- Query id – all 16 bits used.
- Port randomisation – uses all 16bits there, goes out of its way to make sure every query gets a fresh port number

Entropy II

- Destination address, and ipv4/ipv6. RTT band of 400msec (=everything).
  - Its not the timewindow but the randomness
- Query aggregation – same queries are not sent out – unless by different threads
- Qname strict match checked in reply
- 0x20 option
- Harden-referral-path (my draft) option
- Can use multiple source interfaces!
  - 4 outgoing IP address add +2 bits

Other measures

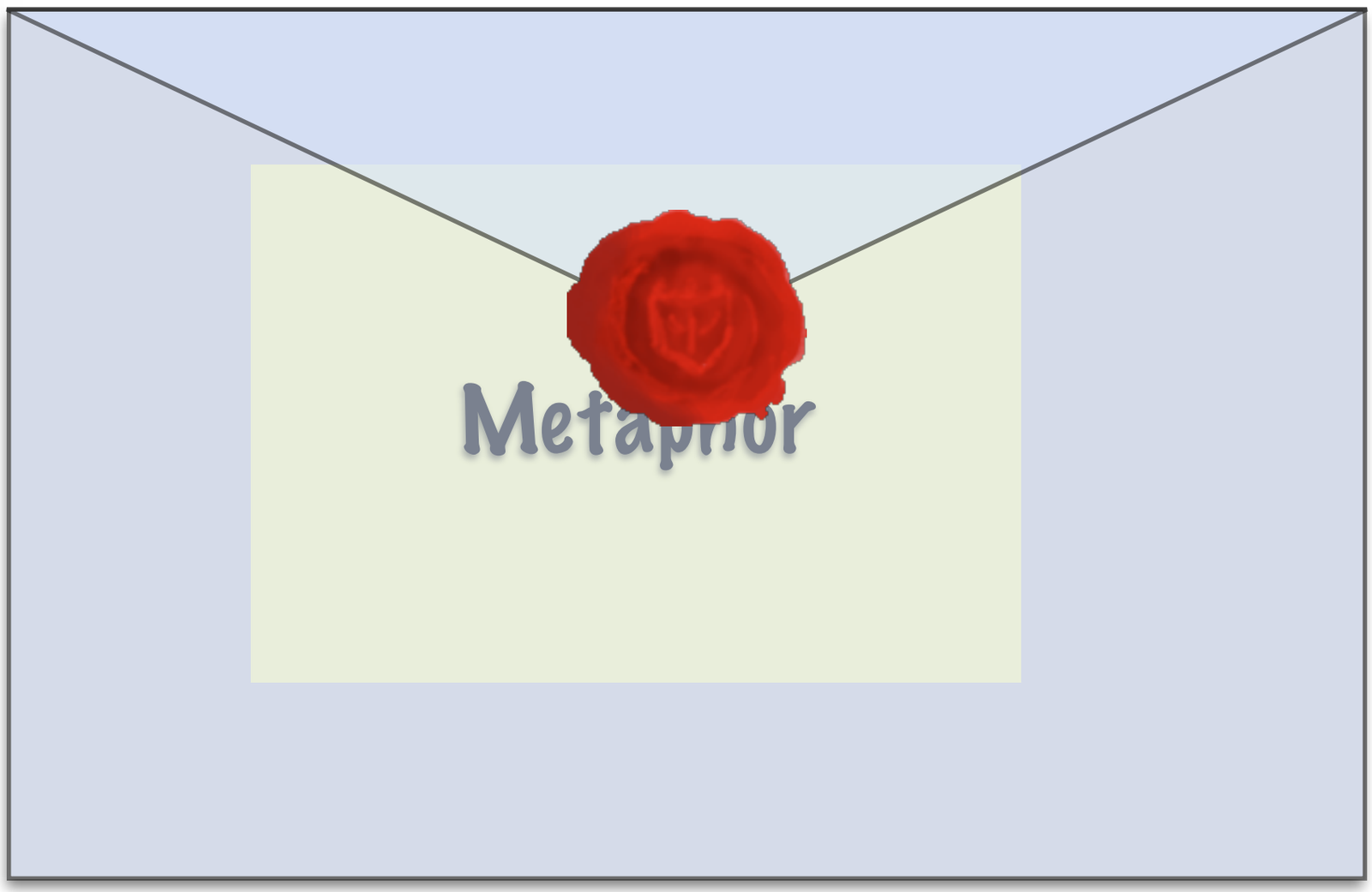
- Not for the wire itself
  - Heap function pointer protection (whitelisted)
  - Chroot() by default
  - User privileges are dropped (lots of code!)
  - ACL for recursion
  - No detection of attacks – assume always under attack
  - version.bind hostname.bind can be blocked or configured what to return (version hiding)
  - Disprefer recursion lame servers – they have a cache that can be poisoned

Arms Race...

Introducing DNSSEC

DNSSEC

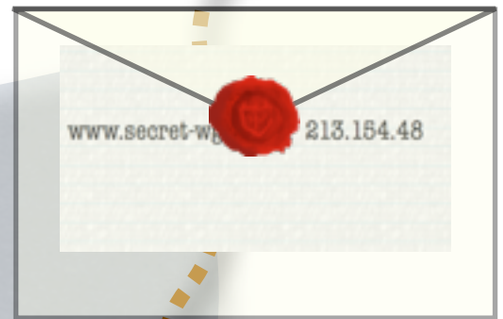
NLnet Labs

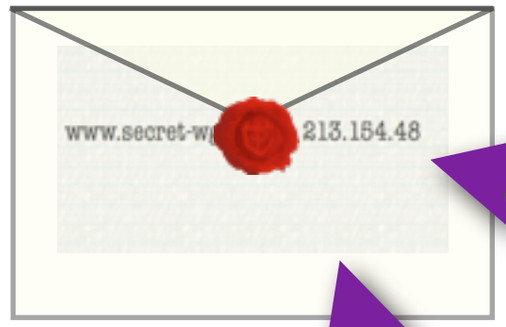

Metaphor


Metaphor

End to End Security

Registrars & Registrants





Secondary DNS

primary DNS

Registry

Secondary DNS

NLnet Labs

All done using Public Key crypto

DNSKEY:
Public key from the keypair

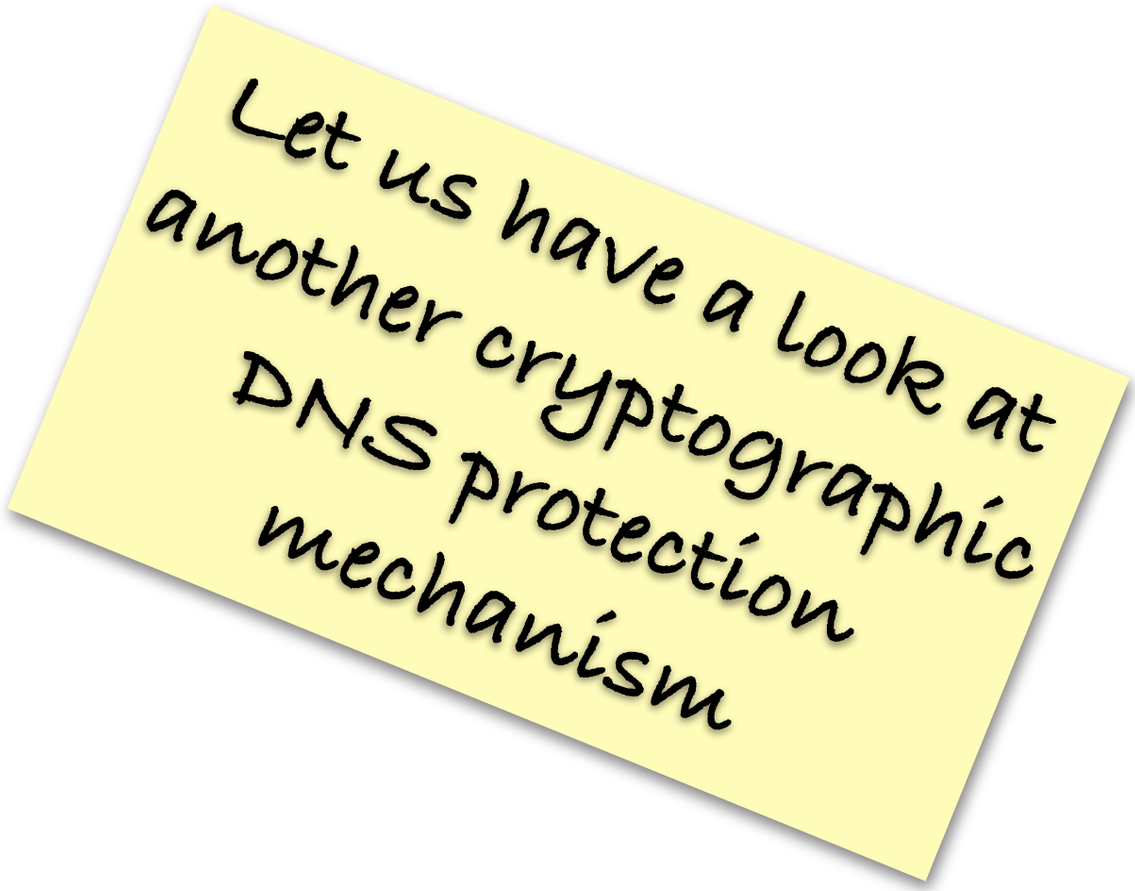
RRSIG: Signatures made with a private key from the keypair

NSEC and NSEC3
For pre-calculated Denial of Existence

DS
For delegating Security

NLnet Labs

But more on that later



DNSSEC

NLnet Labs

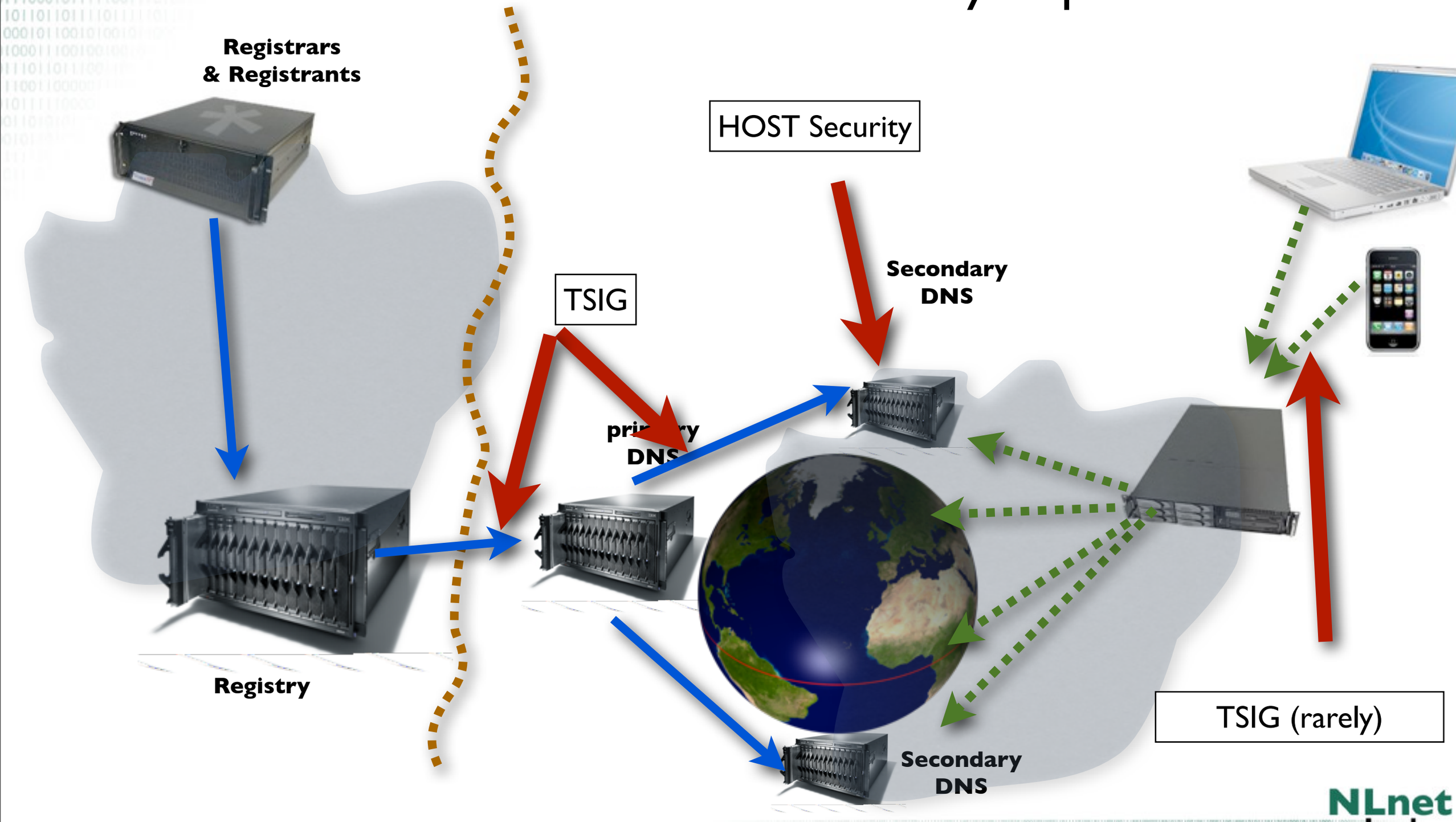
Securing Host-Host Communication

DNSSEC

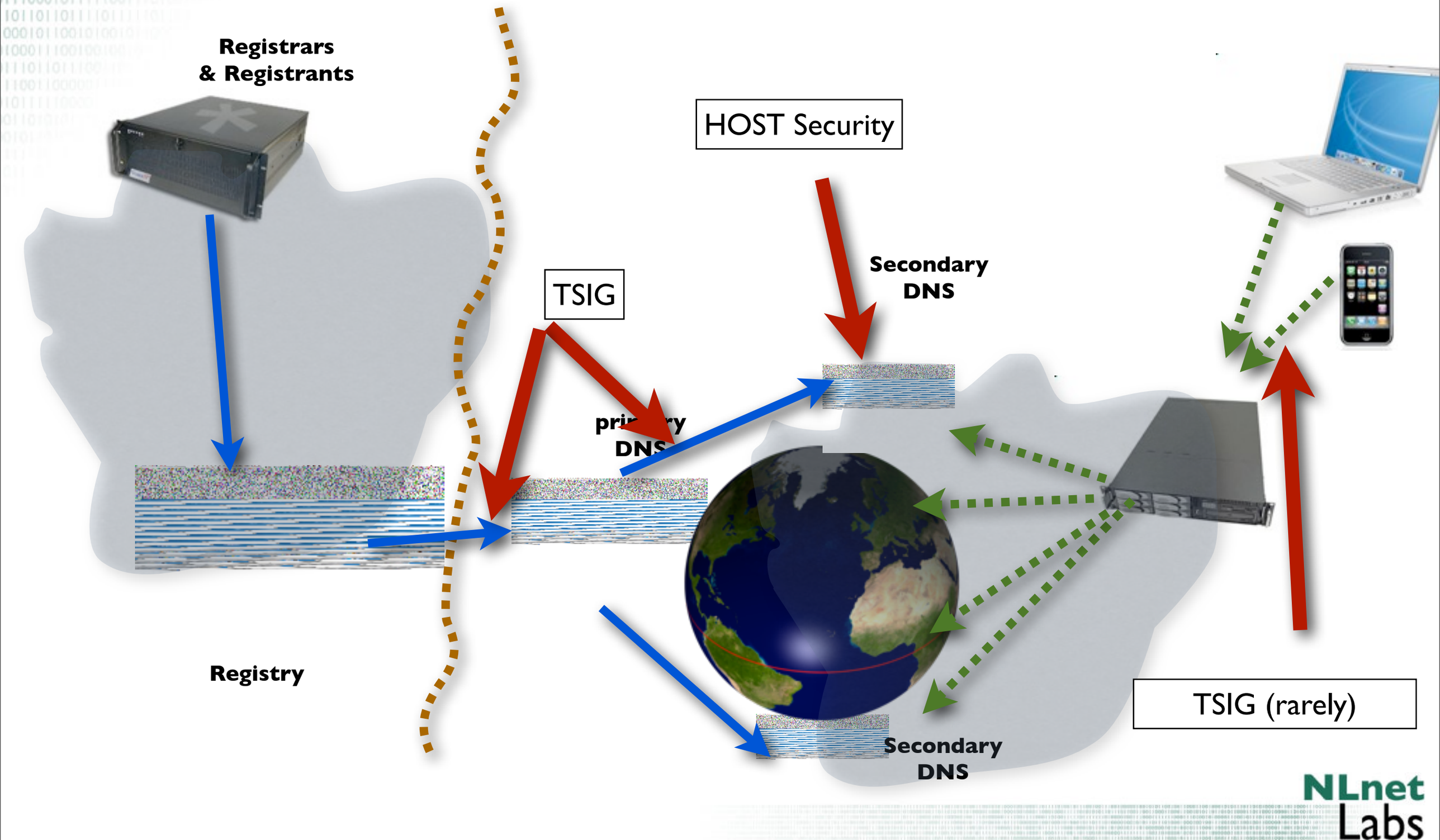
NLnet Labs

Data flow through the DNS

What should you protect...



Data flow through the DNS



NLnet Labs

Transaction Signature: TSIG

- TSIG (RFC 2845)
  - –Authorising dynamic updates and zone transfers
  - –Authentication of caching forwarders
  - –Independent from other features of DNSSEC
- One-way hash function
  - –DNS question or answer and timestamp
- Traffic signed with “shared secret” key
- Used in configuration, **NOT** in zone file

TSIG Example

DNSSEC

NLnet Labs

TSIG Example

Slave

KEY:
$h@r3dS3cr3t

Master

DNSSEC

NLnet Labs

TSIG Example

Slave

KEY:
$h@r3dS3cr3t

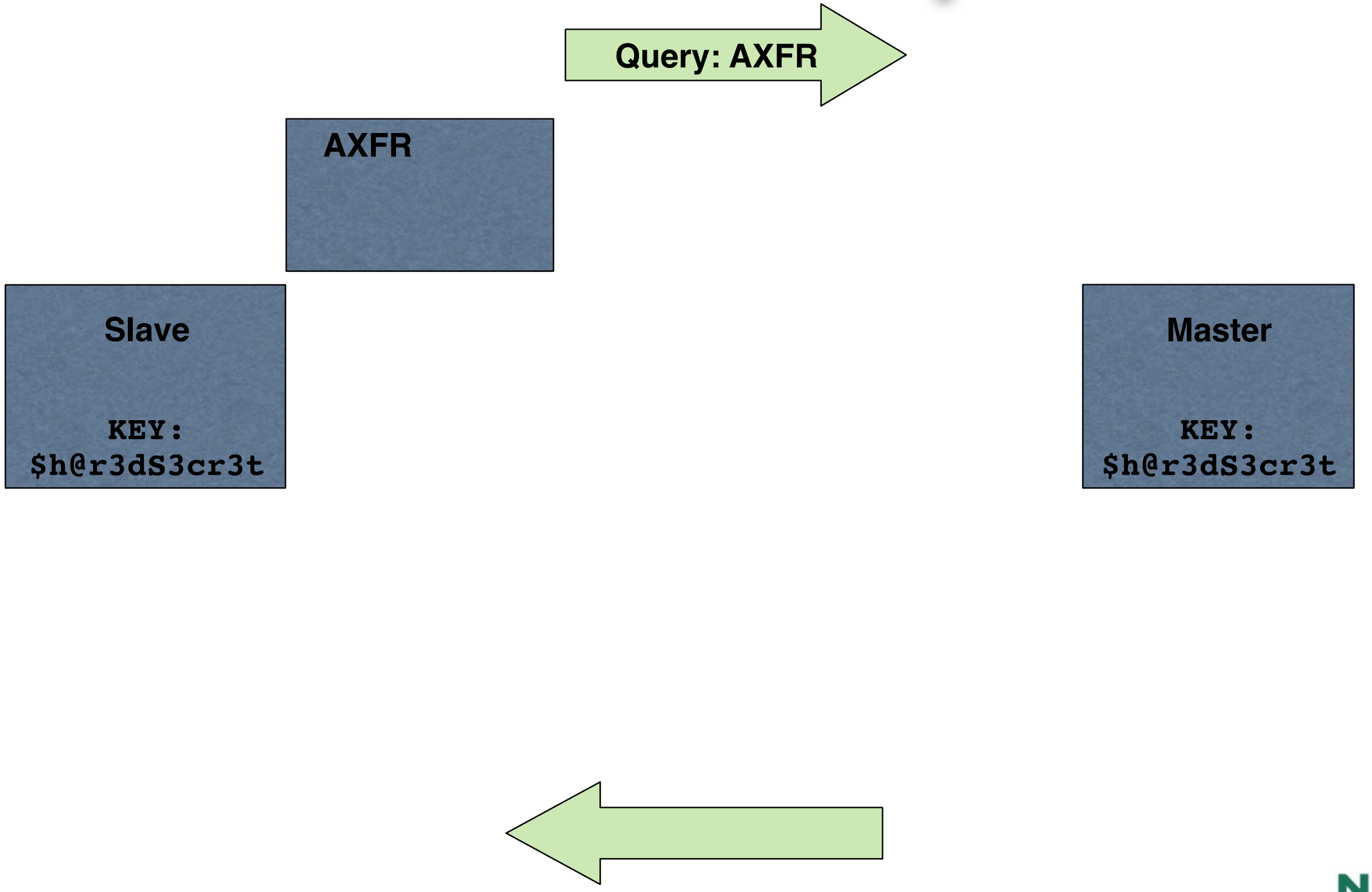
Master

KEY:
$h@r3dS3cr3t

DNSSEC

NLnet Labs

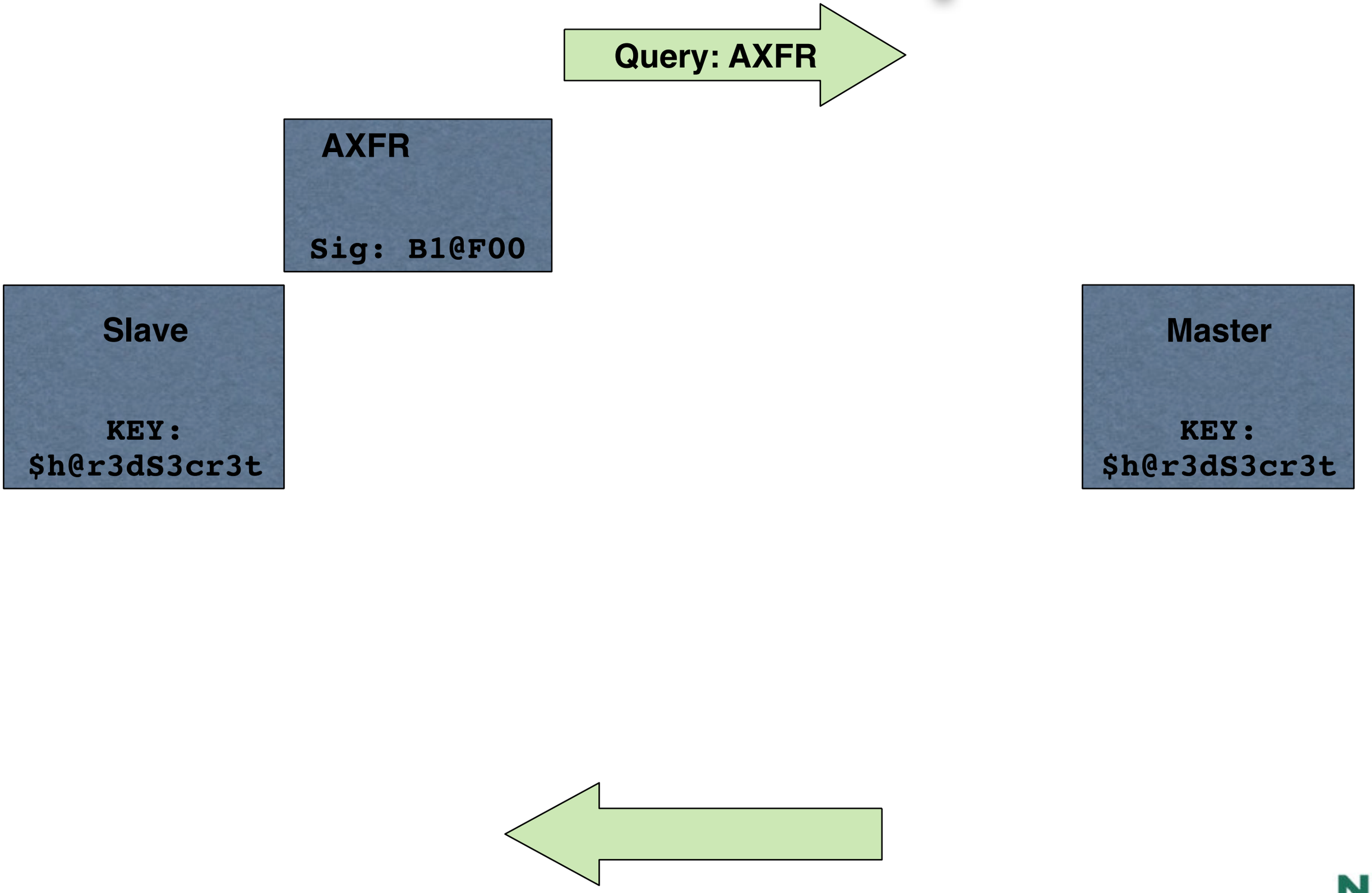
TSIG Example



DNSSEC

NLnet Labs

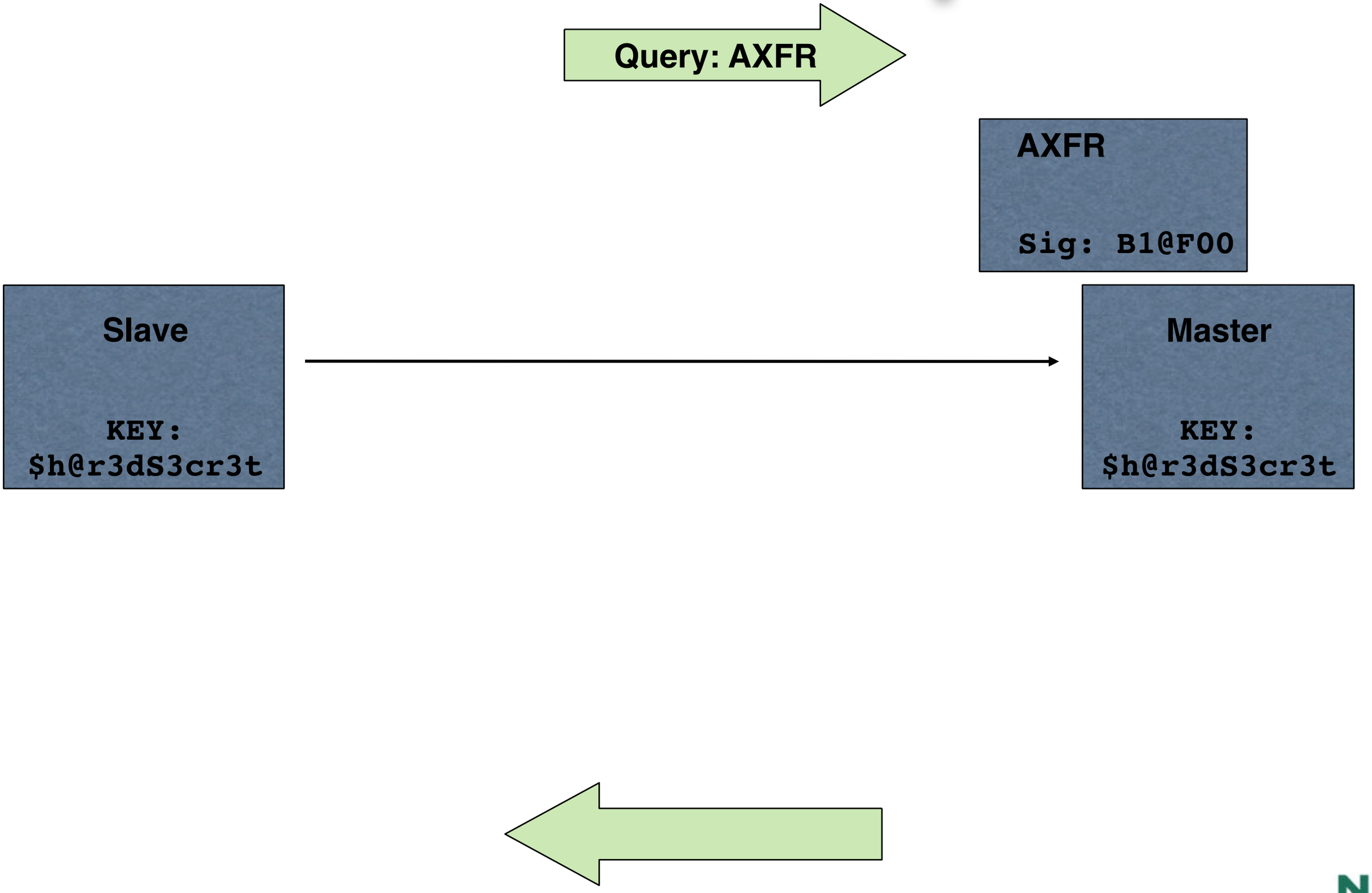
TSIG Example



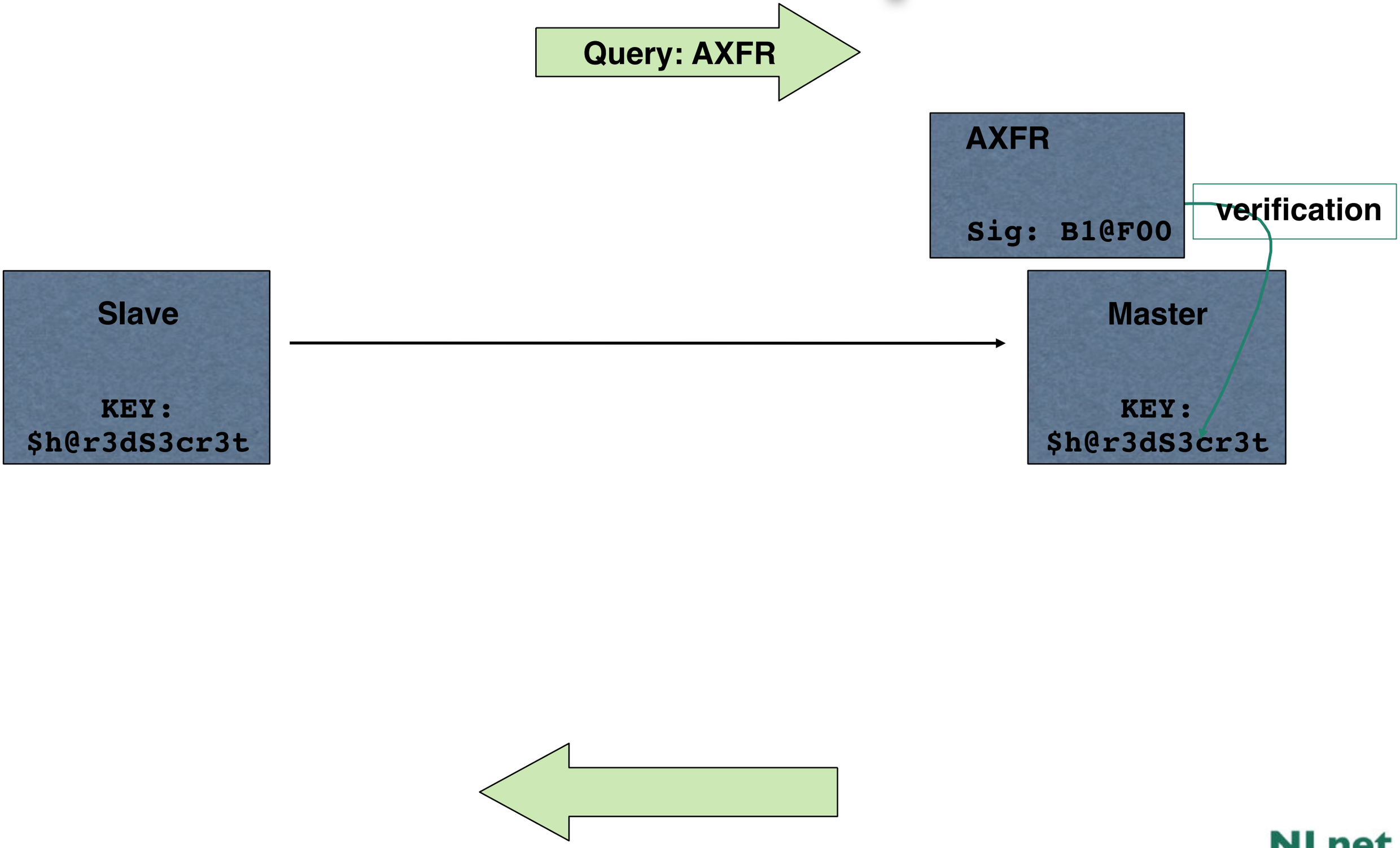
DNSSEC

NLnet Labs

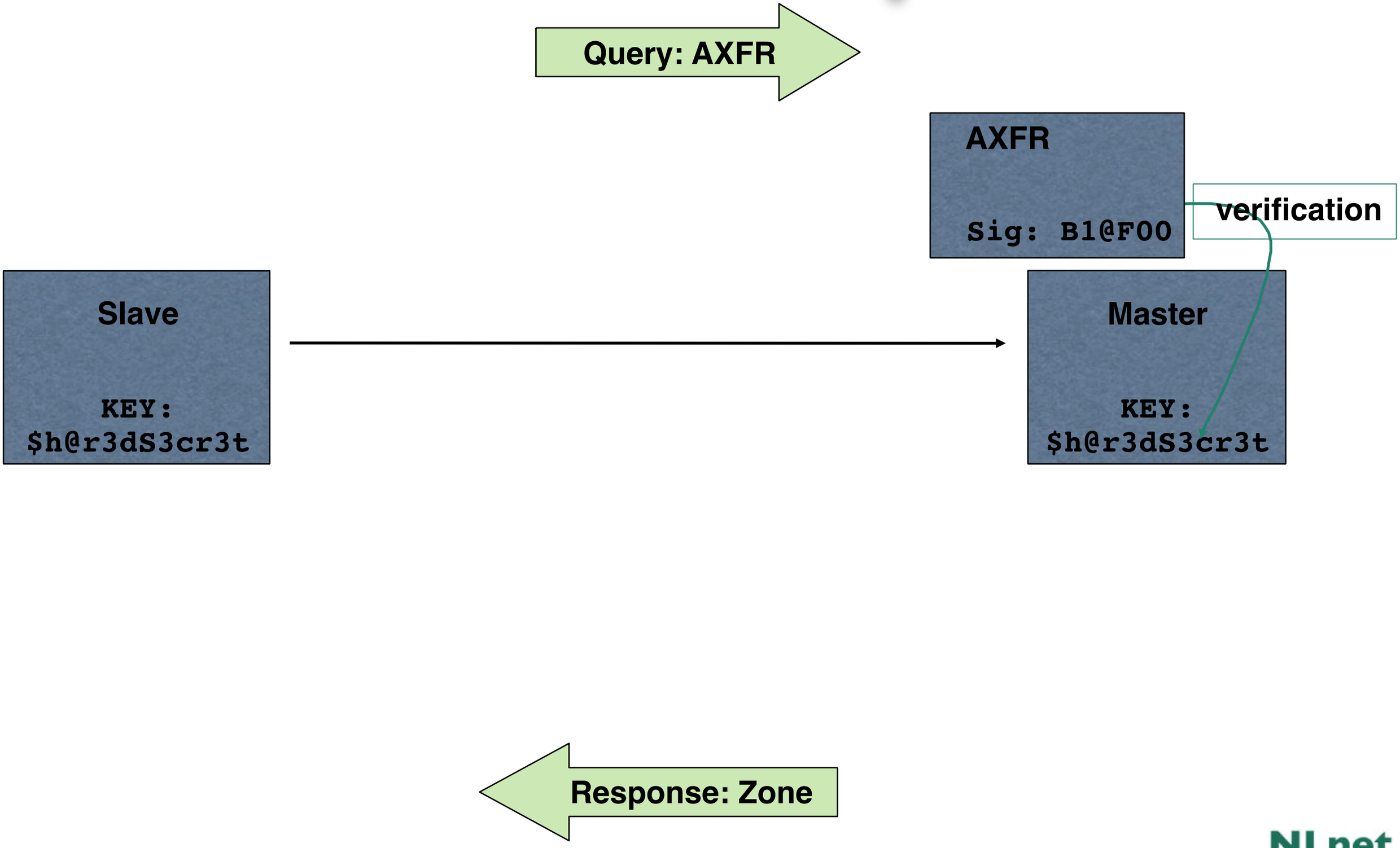
TSIG Example



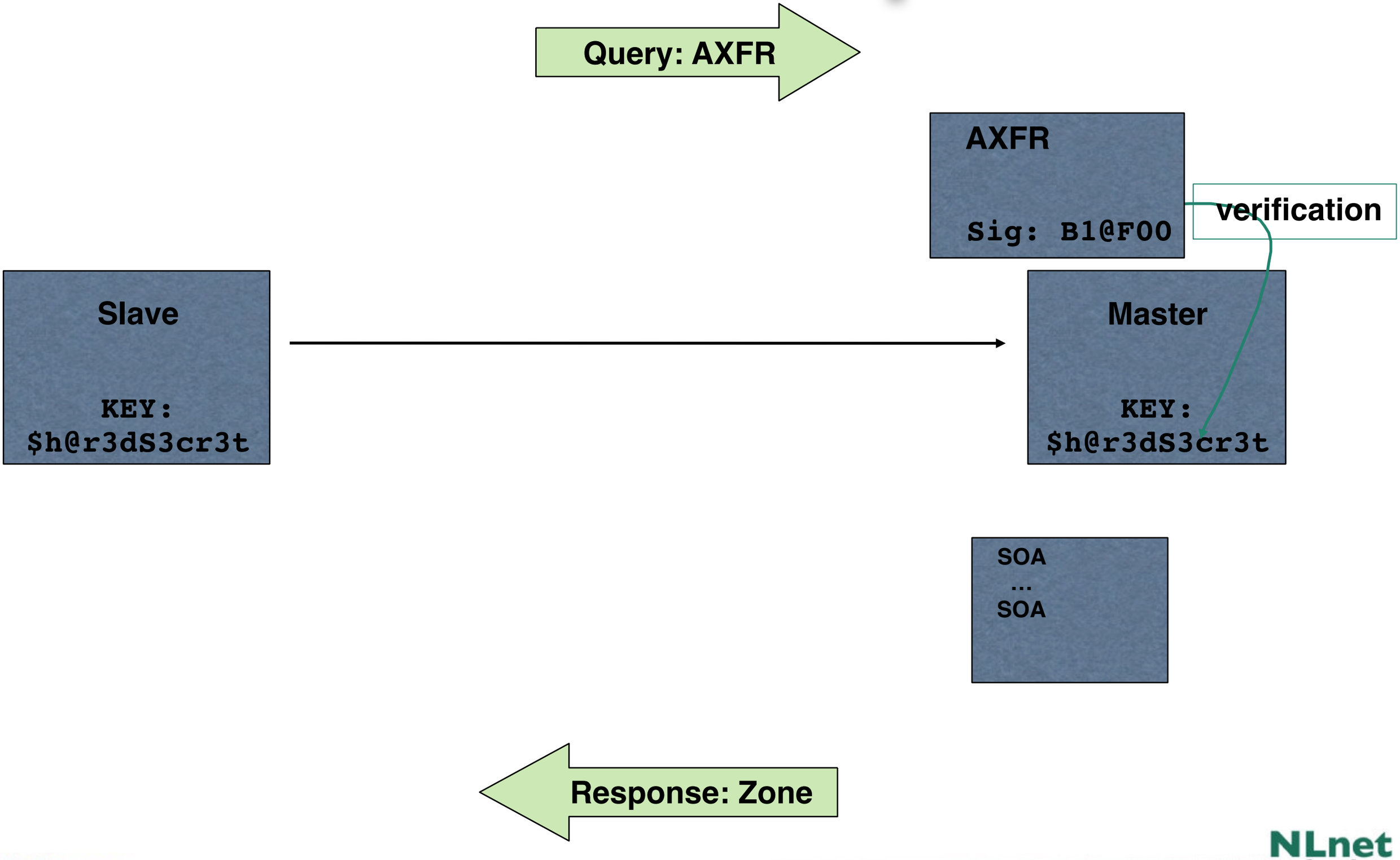
TSIG Example



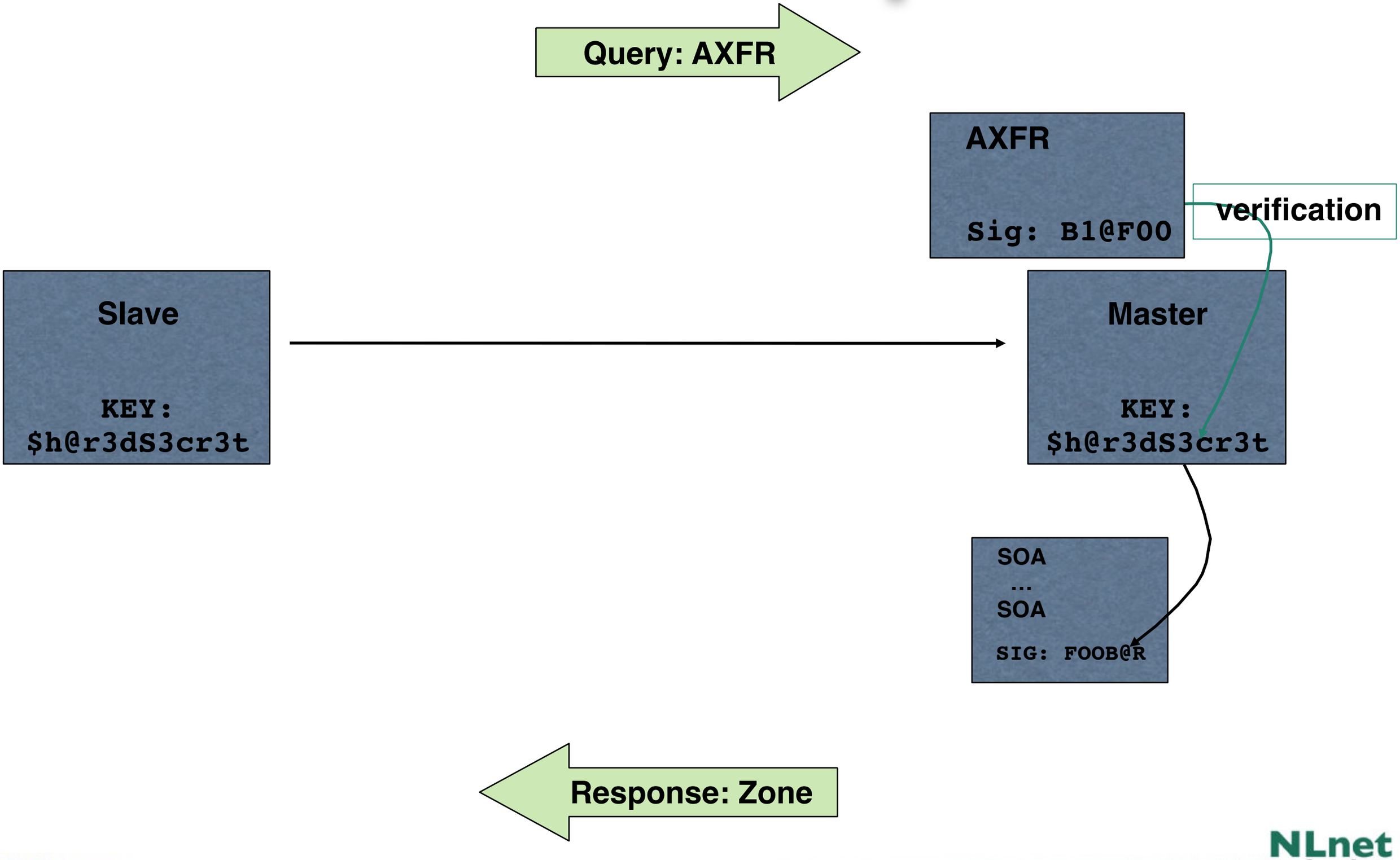
TSIG Example



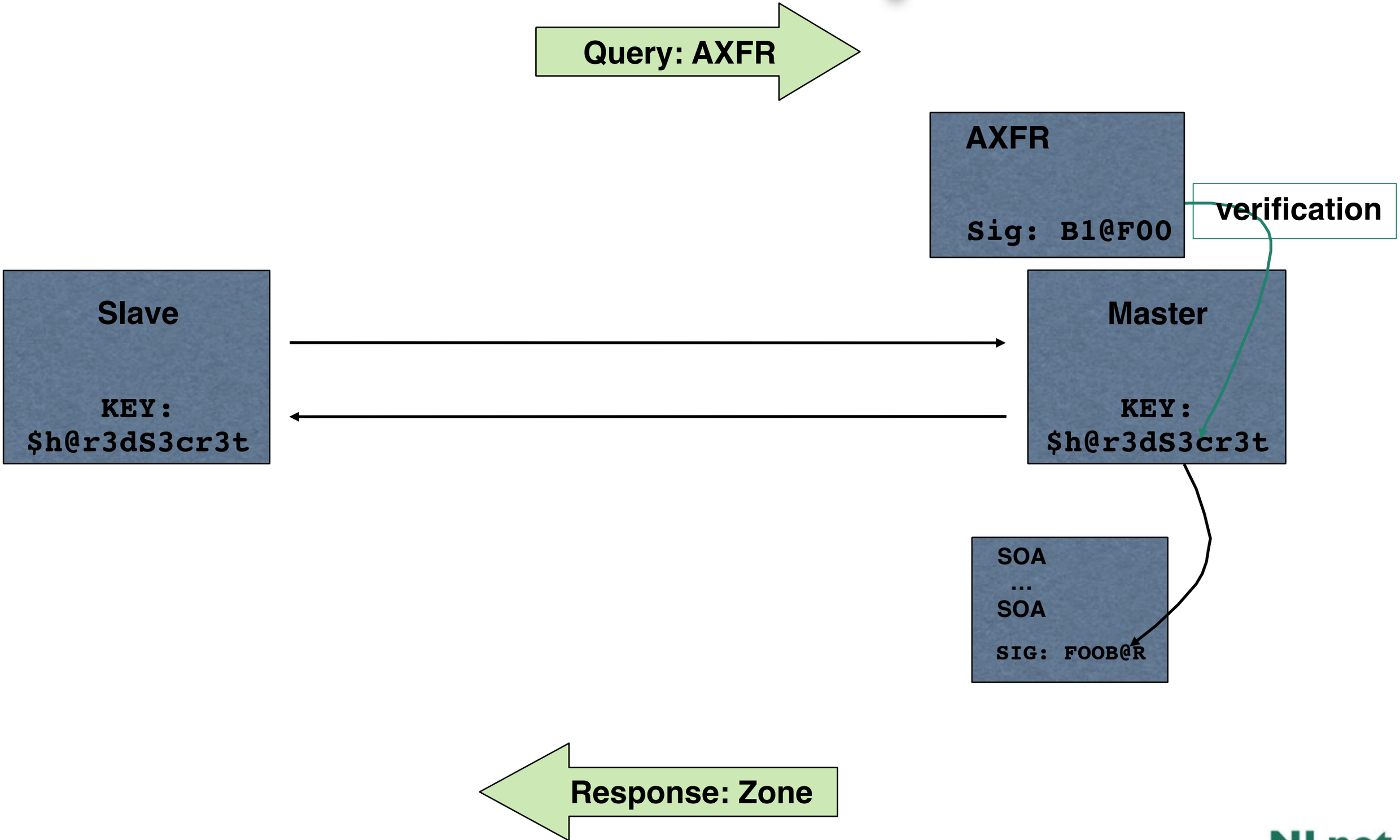
TSIG Example



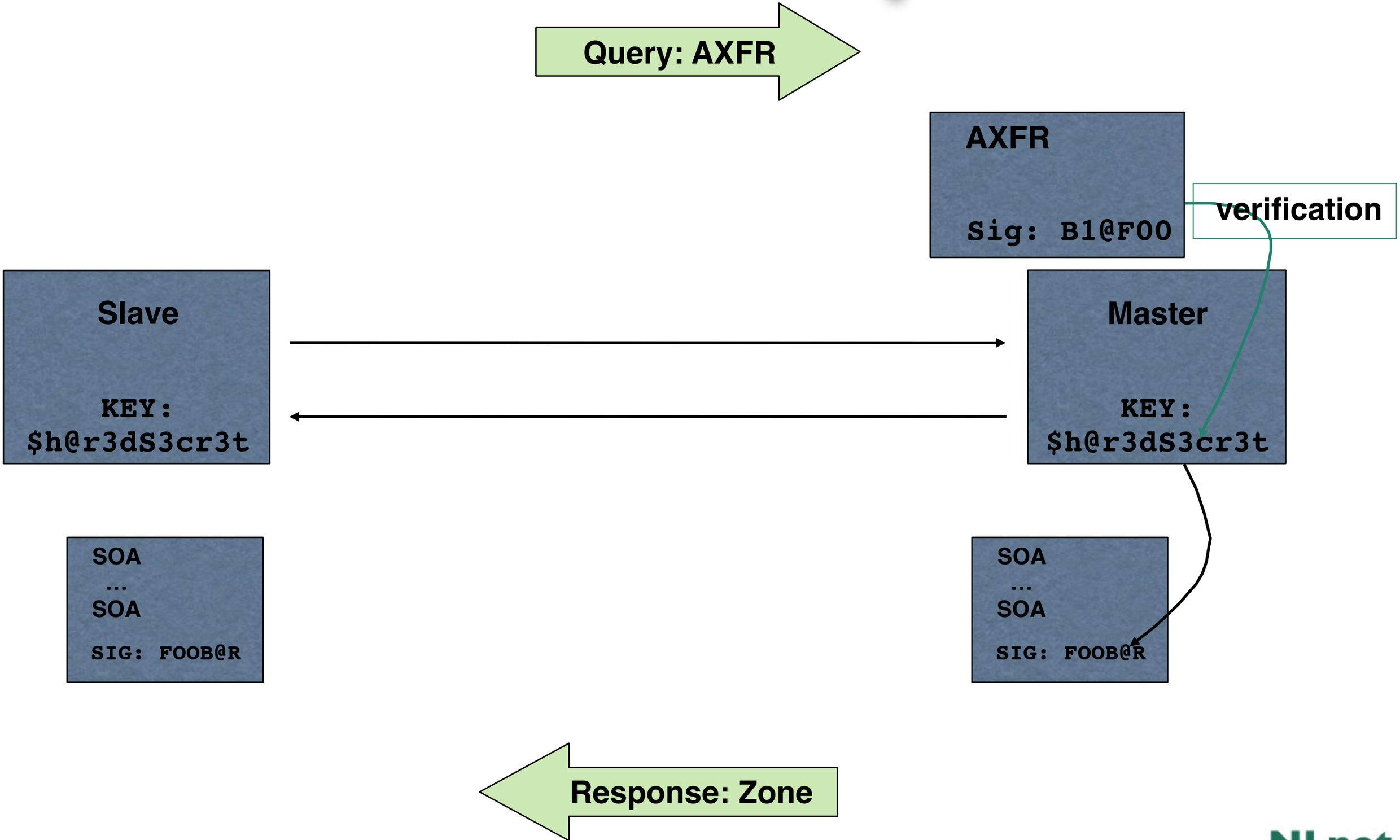
TSIG Example



TSIG Example



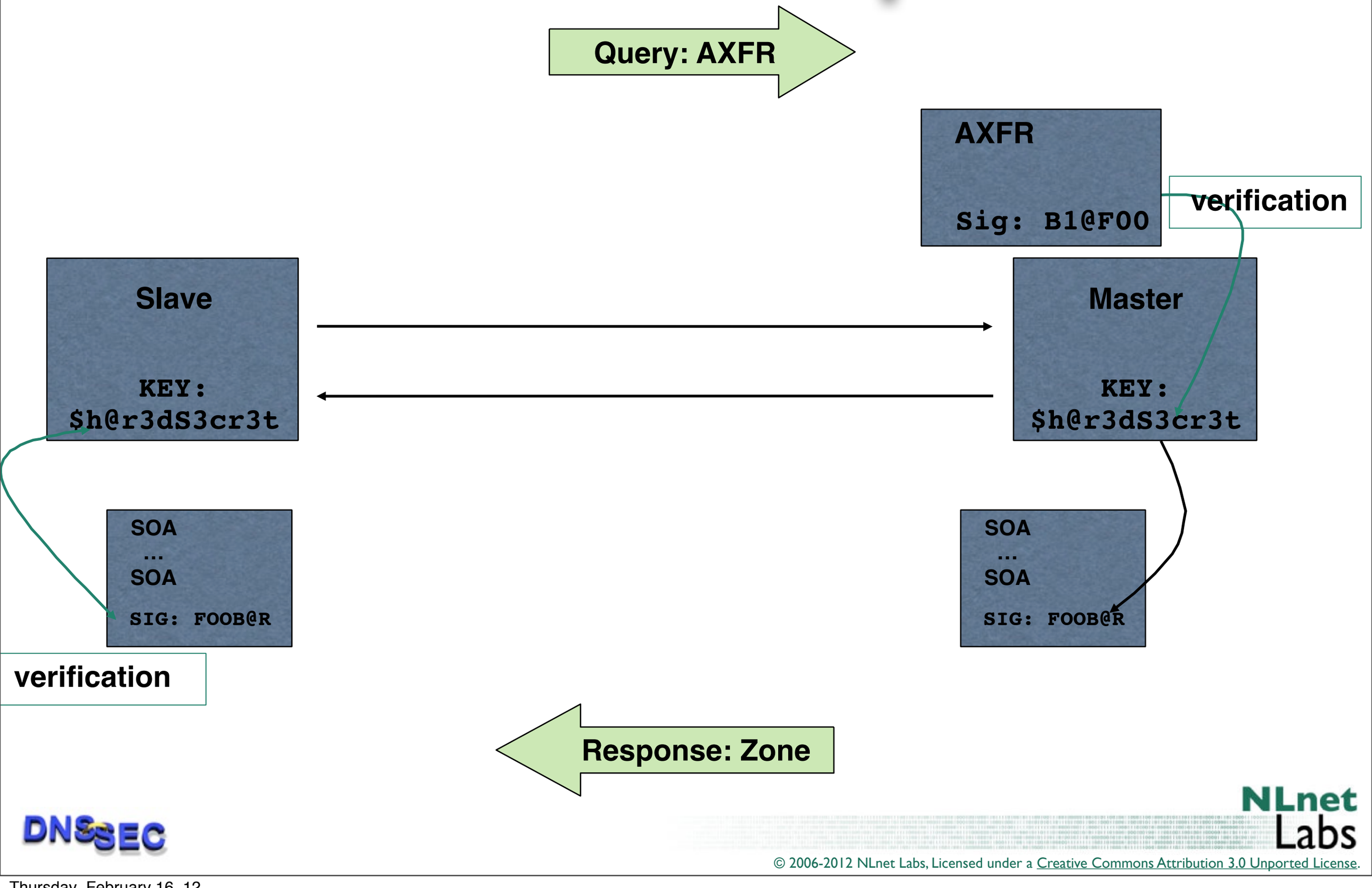
TSIG Example



DNSSEC

NLnet Labs

TSIG Example



TSIG for Zone Transfers

1. Generate secret
2. Communicate secret
3. Configure servers
4. Test

DNSSEC

NLnet Labs

Importance of the Time Stamp

- TSIG/SIG(0) signs a complete DNS request / response with time stamp
  - To prevent replay attacks
  - Currently hardcoded at five minutes

- Operational problems when comparing times
  - Make sure your local time zone is properly defined
  - **`date -u`** will give UTC time, easy to compare between the two systems
  - Use NTP synchronisation!

DNSSEC

NLnet Labs

Authenticating Servers Using SIG(0)

- Alternatively, it is possible to use SIG(0)
  - –Not yet widely used
  - –Works well in dynamic update environment
- Public key algorithm
  - –Authentication against a public key published in the DNS
- SIG(0) specified in RFC 2931

DNSSEC

NLnet Labs

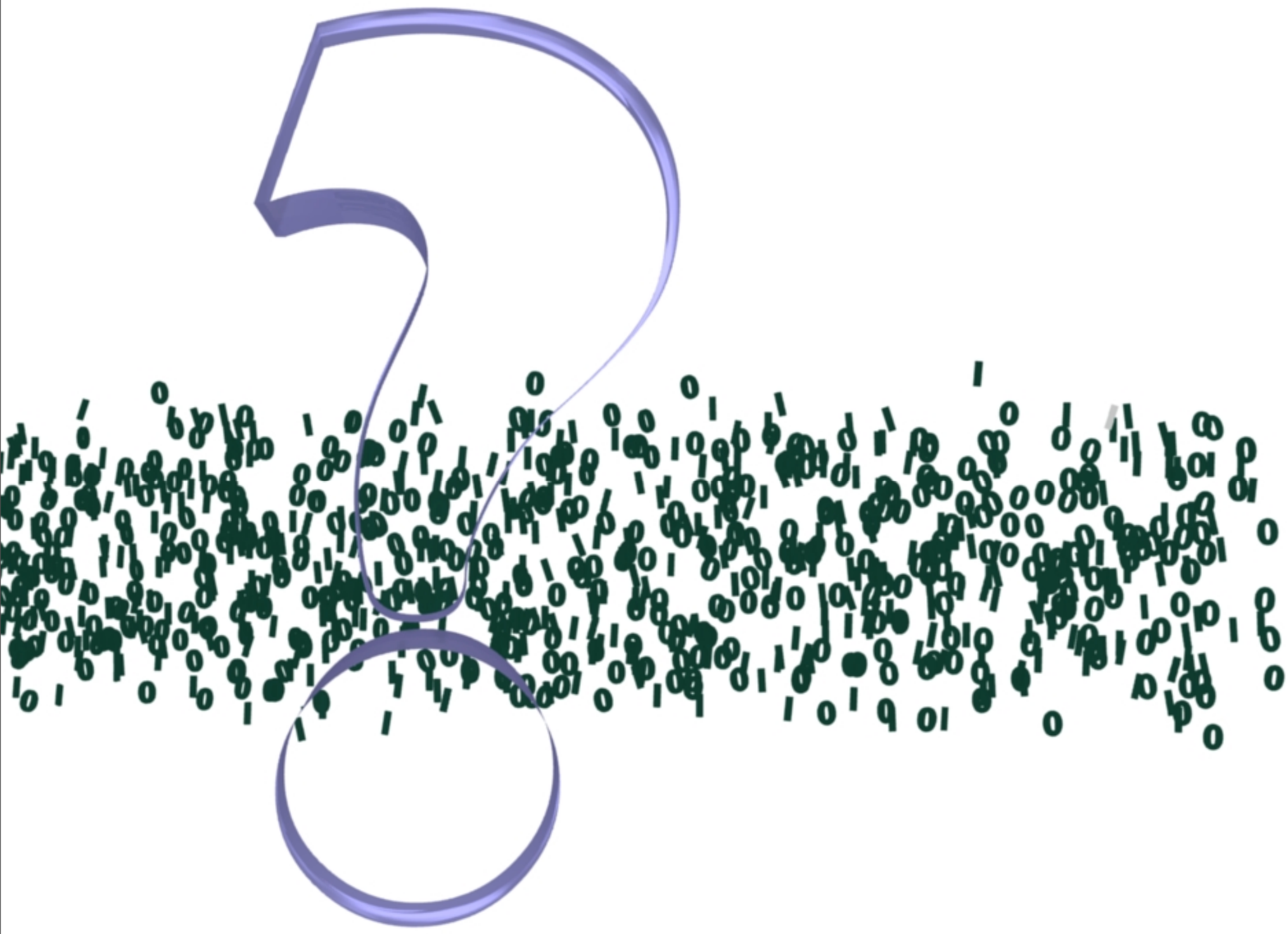
Cool Application

- Use TSIG-ed dynamic updates to configure configure your laptops name

- My laptop is know by the name of aagje.secret-wg.org
  - http://ops.ietf.org/dns/dynupd/secure-ddns-howto.html
  - Mac OS users: there is a bonjour based tool.
    - www.dns-sd.org

DNSSEC

NLnet Labs



DNSSEC

NLnet Labs