

DNSSEC trigger

Or how to get
DNSSEC to
the end-user

Wouter Wijngaards
&
Olaf Kolkman



Executive Summary

How to get
DNSSEC to your
machine, without
too much of a
headache

`dnssec-trigger`

Run Unbound
Locally

Catch reconfigs
(DHCP etc)

Try to penetrate

If all fails call
user



Executive Summary

How to get
DNSSEC to your
machine, without
too much of a
headache

Fire and Forget



Motivation

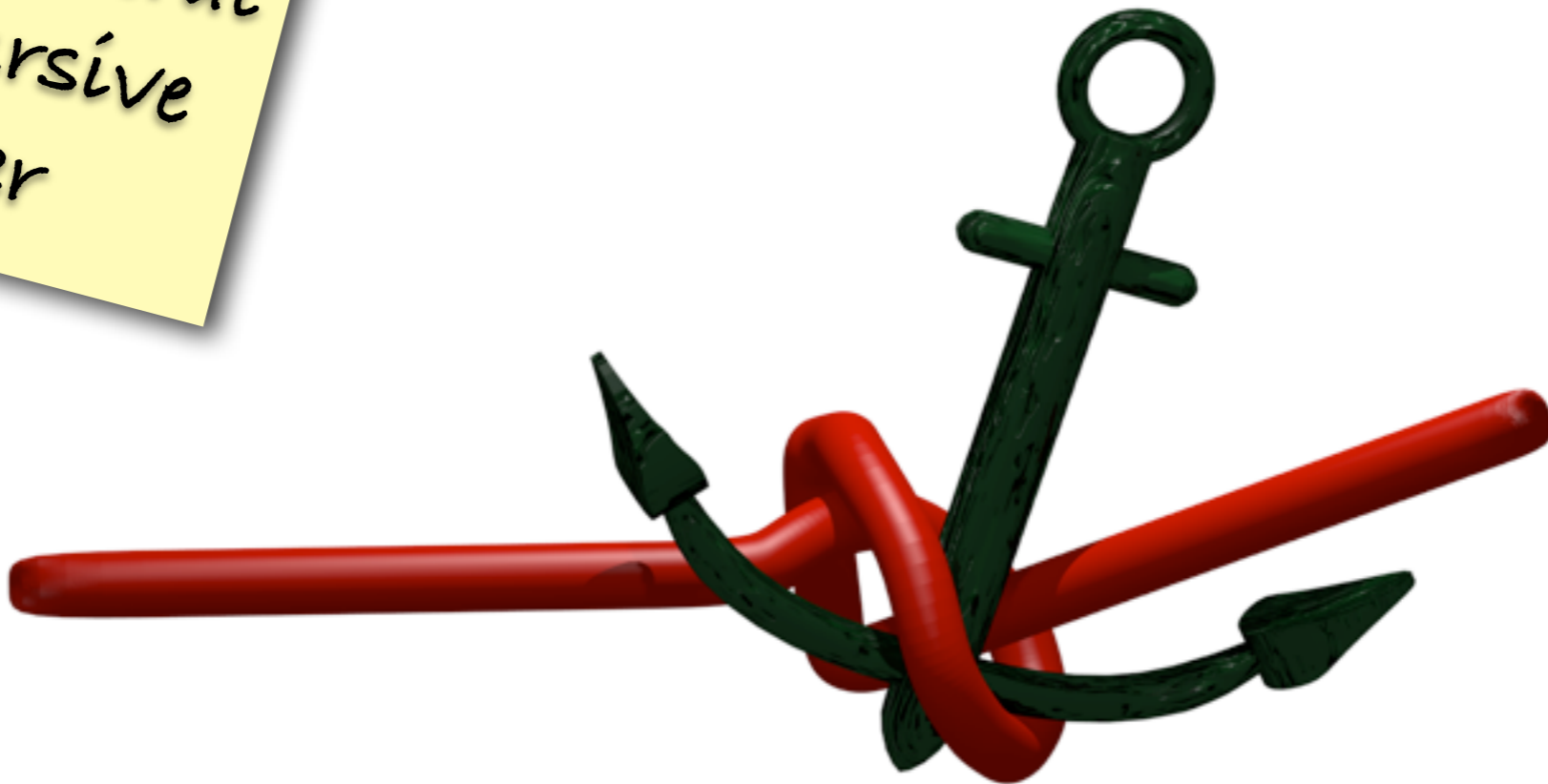
Or how to get
DNSSEC to
the end-user

Components

Automatic probing
and configuration
software

Unbound

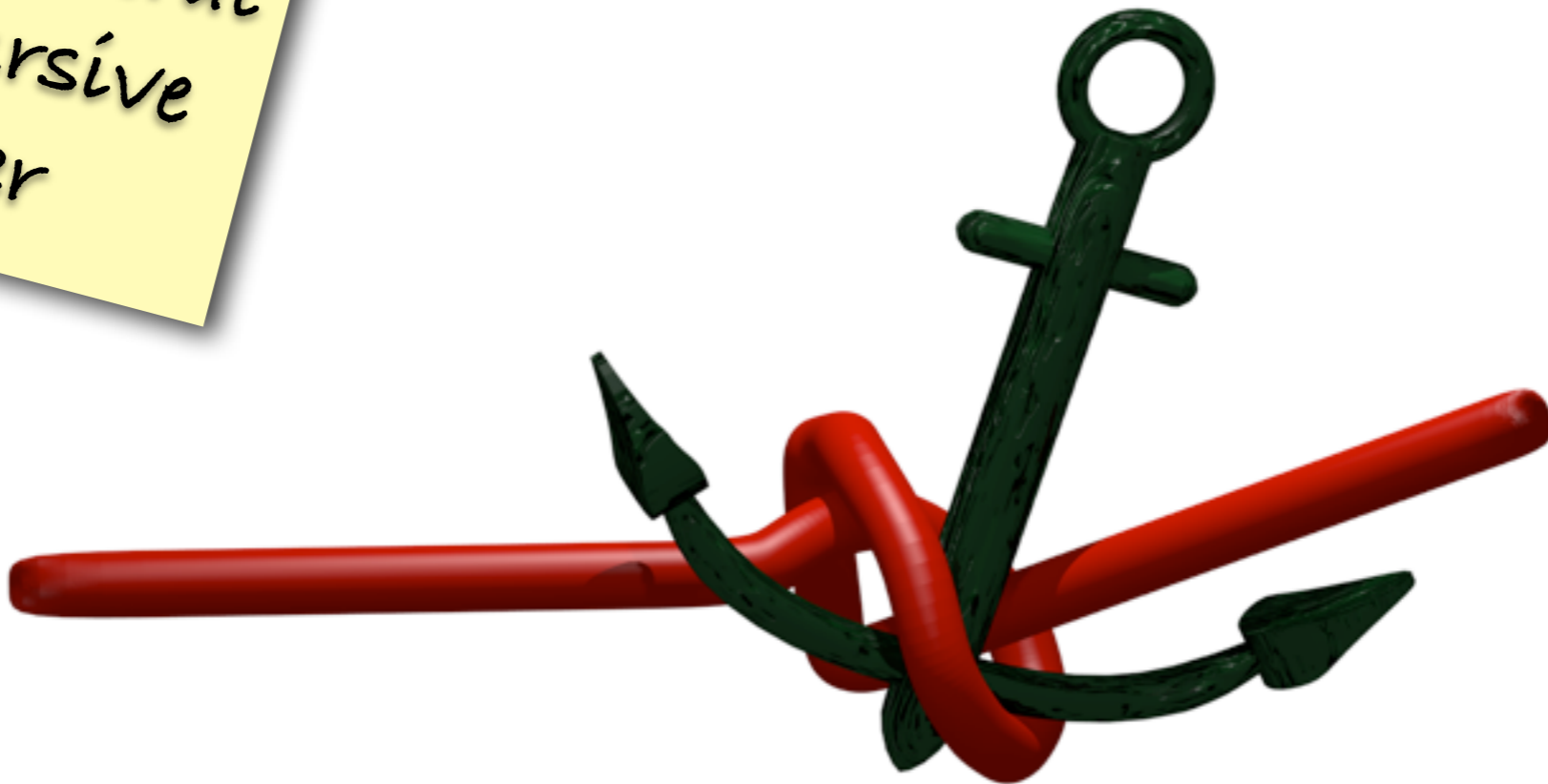
A (specific) general
purpose Recursive
Nameserver

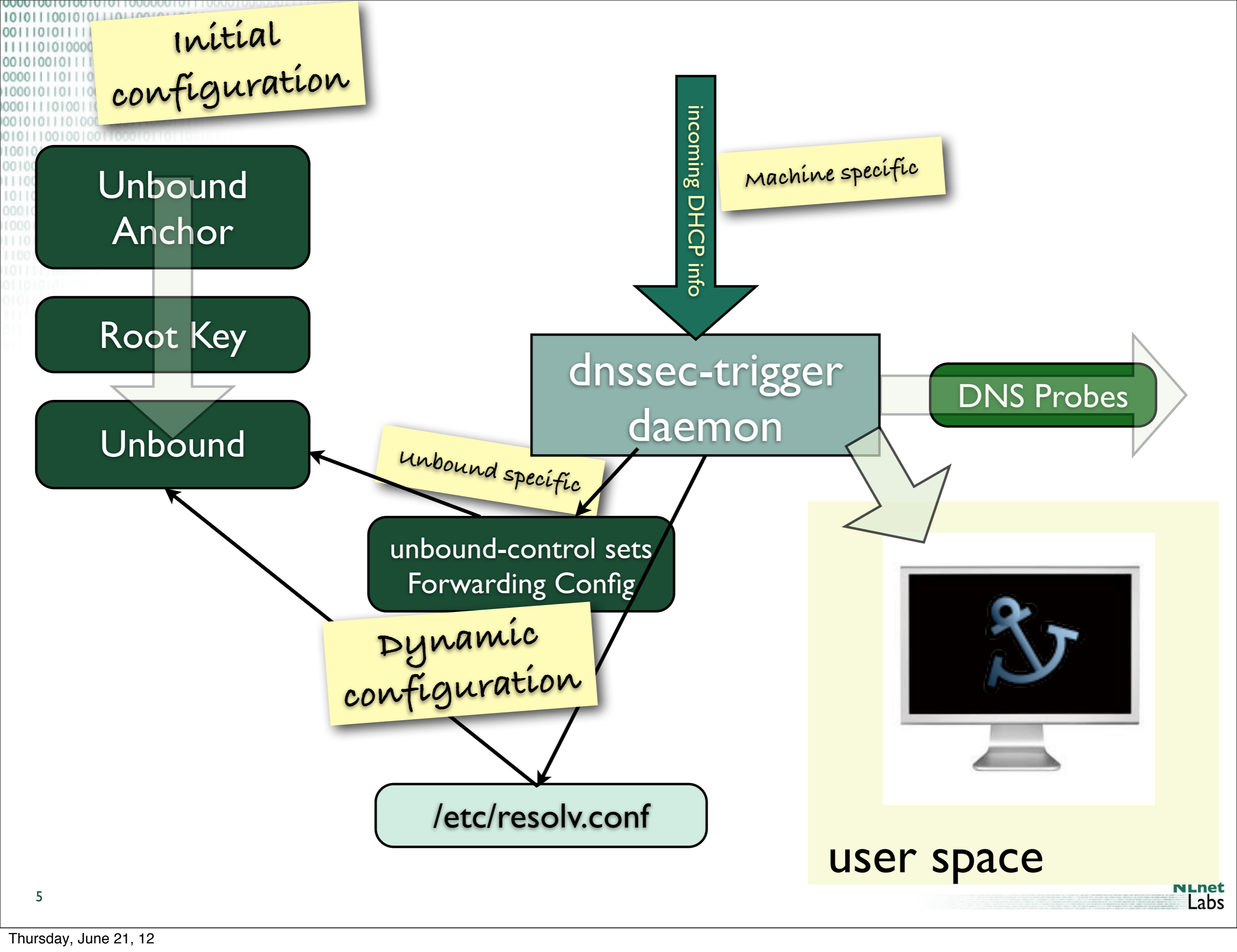


Unbound

Automatic probing
and configuration
software

A (specific) general
purpose Recursive
Nameserver

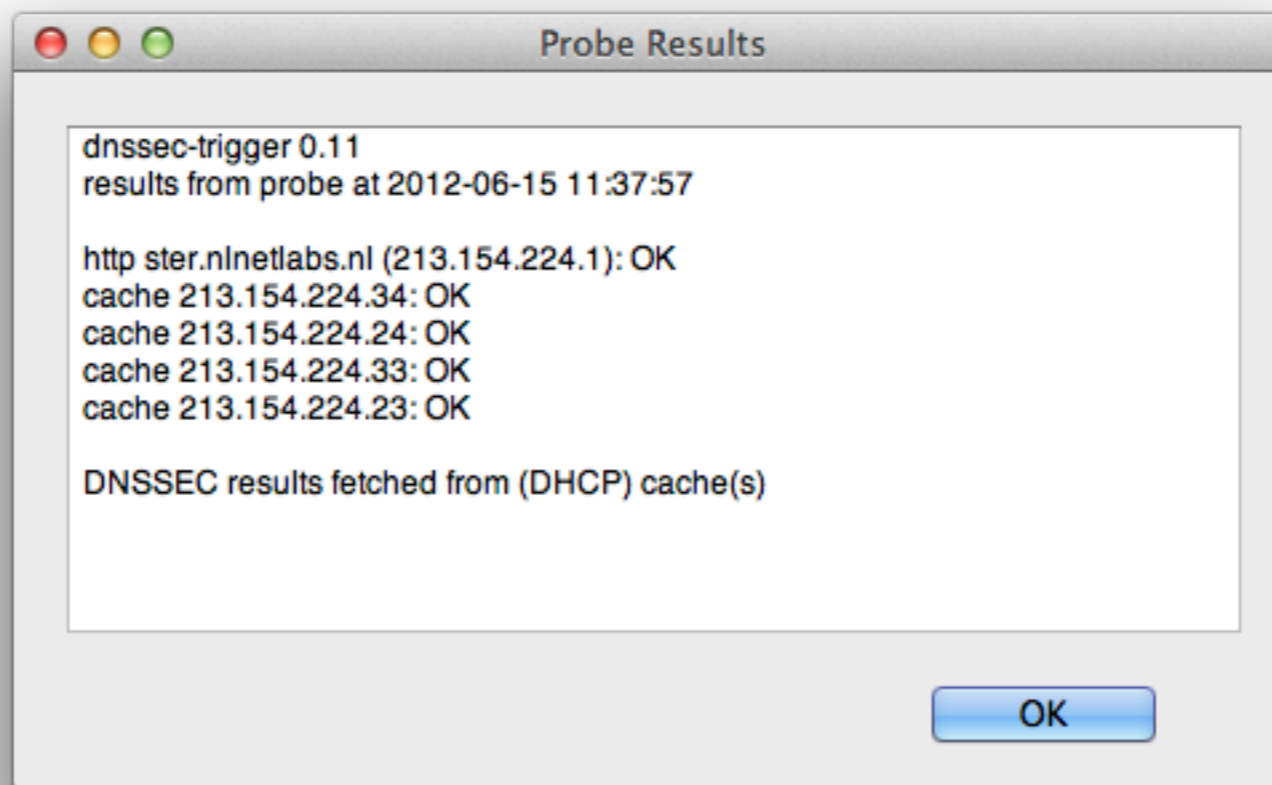




Normal Operation



Normal Operation



PROBE EXPECTATIONS

EDNS support

RRSIGs

DNSKEY and DS

Lengthy Packets
(>512)

NSEC3 support

Transparent Proxy
that is transparent
to DNSSEC

AND IT WILL PROBE AGAIN

if insecure against
its will

exp backoff

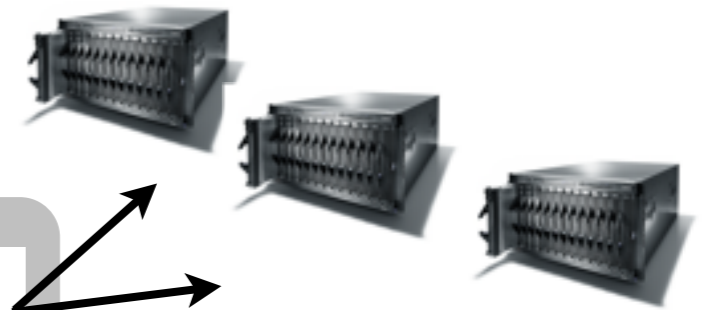
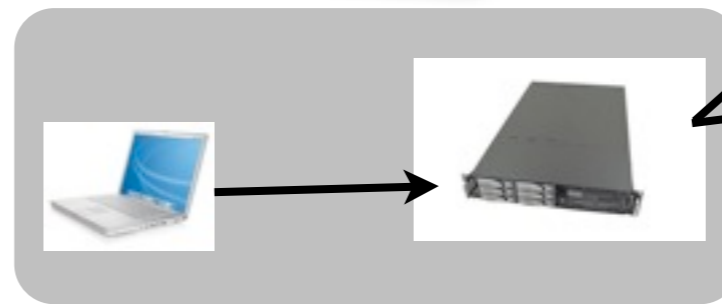
PROBING STRATEGY

All IPs in resolv.conf are tried in parallel, first response wins

PROBING STRATEGY

All IPs in resolv.conf are tried in parallel, first response wins

Use cache from DHCP

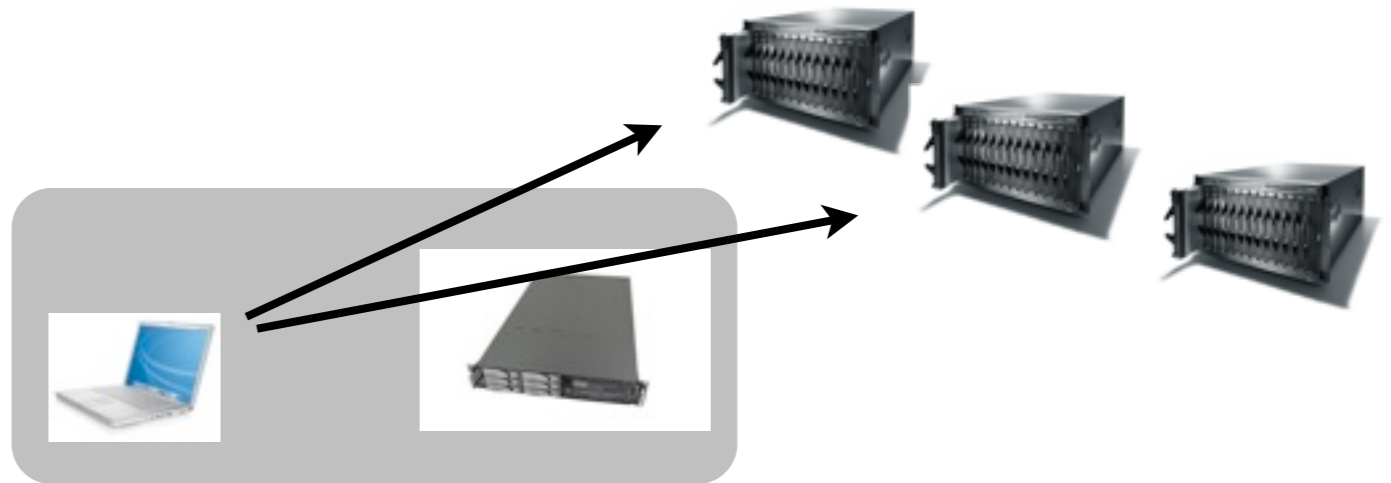
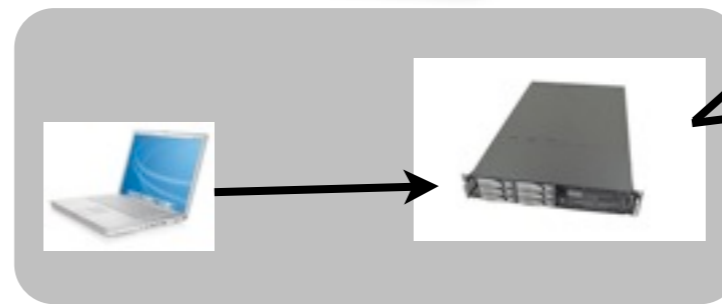


PROBING STRATEGY

All IPs in resolv.conf are tried in parallel, first response wins

Use cache from DHCP

Full resolver mode, querying authority servers directly



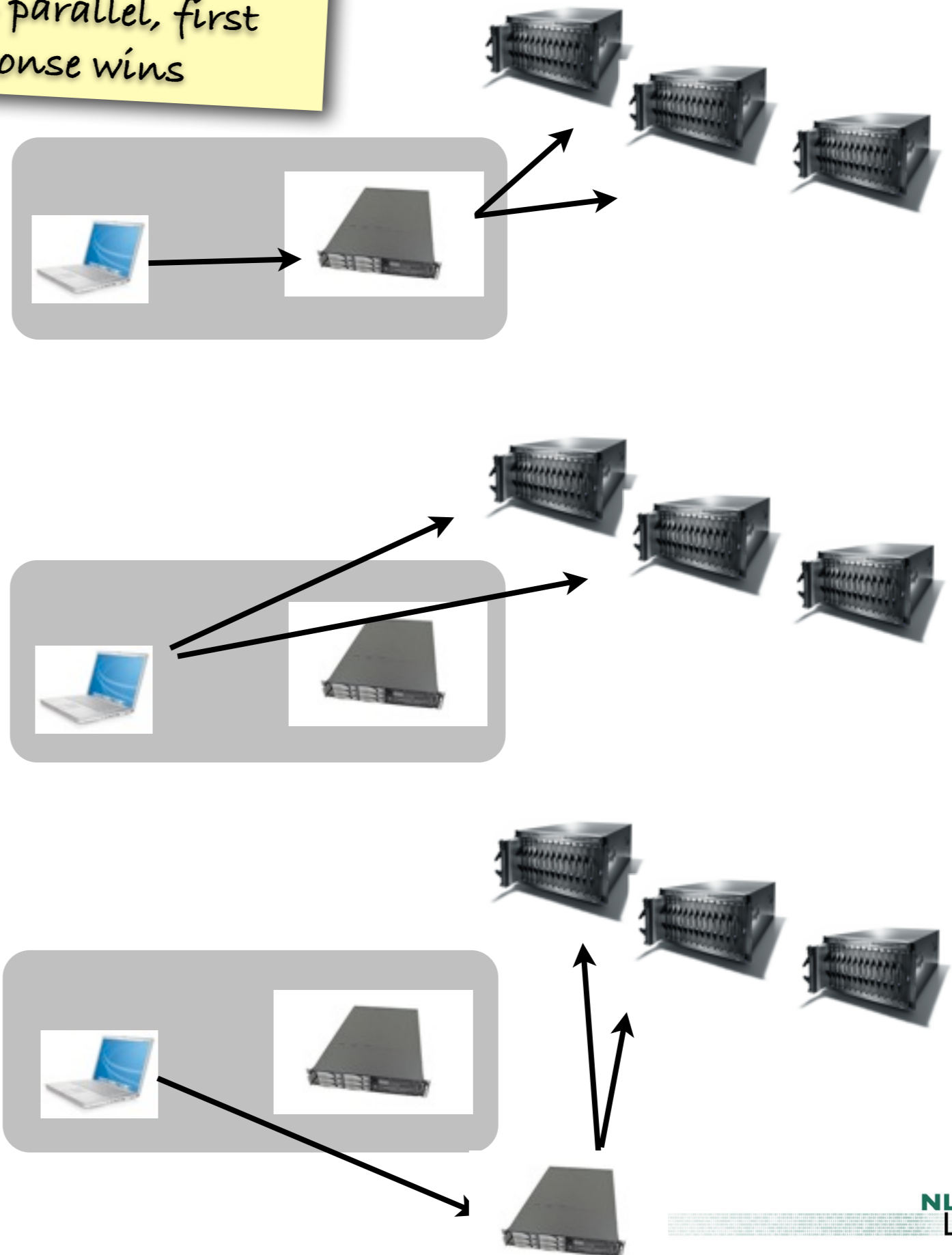
PROBING STRATEGY

All IPs in resolv.conf are tried in parallel, first response wins

Use cache from DHCP

Full resolver mode, querying authority servers directly

Port 80 and 443 to an NLnet Labs resolver



ON THE ROAD

No pop-ups if everything just works

Only during probing operation

No Web Access

There is no web access on this network. Do you have to login for that?

While you login you are insecure, for backwards compatibility, until dnsssec-trigger can detect web access.

Skip this if you do not have to log in on this network.

Skip Log in

Probe fails to get through, are you in a hotel?

Disables DNSSEC and opens browser

The screenshot shows a Linux desktop with a top panel containing various system icons. A terminal window titled "Probe" is open, displaying the following text:

```
dnsssec-trigger 0.11
results from probe at 2012-06-15 11:13:10

http fedoraproject.org (66.35.62.166): error wrong page content
cache 208.67.220.220: error no RRSIGs in reply
cache 208.67.222.222: error no RRSIGs in reply

DNS queries are sent to INSECURE servers. There is
no web access, perhaps you must do hotspot signon.
Please, be careful out there.
```

An "OK" button is visible at the bottom of the terminal window. In the bottom right corner, a system dialog box titled "Network DNSSEC Failure" is displayed with the following text:

The Network Fails to Support DNSSEC

The network you are connected to does not support the provided DNS caches, nor via contacting servers directly (it filters traffic to this end). It

10101100101011011001011001100101110111
001101011111100011101101000111110111
111101010000111101010100100100111110111
0010100101110000111010000100000100001
0000111011101001110100101101100001111
1000101101110010110100001000110010001
000111010011011011100011111101001
001010111010001100111000111101001
01011100100100110001011011011111
100101001100001110000010011001
0010010100011111100101010001
11100010111110011010010001
1011011011110111101111011111
000101100101001010011001100110011001
1110110111001111110011001100110011001
110011000110011111110011001100110011001
1011111111111111111111111111111111111111



```
Probe Results

dnssec-trigger 0.11
results from probe at 2012-06-15 11:17:34

ssl443 213.154.224.3: OK
tcp80 213.154.224.3: OK
authority 199.7.83.42: error no answer, REFUSED
http ster.nlnetlabs.nl (213.154.224.1): OK
cache 208.67.222.222: error no RRSIGs in reply
cache 208.67.220.220: error no RRSIGs in reply

DNSSEC results fetched from open resolvers over TCP

OK
```



DNSSEC trigger worked around the local DNS resolver

10101100101011011001011001100101110111
001101011111100011101101000111110111
111101010000111101010100100100111110111
00101001011100001110100001000000100001
0000111011101001110100101101100001111
1000101101110010110100001000110010001
00011101001101101110001111110101
00101011101000110011100011110101
010111001001001100010110110111
10010100110000111000001001100
001001010001111100101010001
1110001011110011010010001
101101101110111101110111
000101100101001010011001
10011100100100101
111011011100111
110011000011111



```
Probe Results

dnssec-trigger 0.11
results from probe at 2012-06-15 11:17:34

ssl443 213.154.224.3: OK
tcp80 213.154.224.3: OK
authority 199.7.83.42: error no answer, REFUSED
http ster.nlnetlabs.nl (213.154.224.1): OK
cache 208.67.222.222: error no RRSIGs in reply
cache 208.67.220.220: error no RRSIGs in reply

DNSSEC results fetched from open resolvers over TCP

OK
```



DNSSEC trigger worked around the local DNS resolver

And you never even noticed



Network Manager
Netconfig

WSALookupService
(XP, Vista, 7)

Scripts, ifconfig,
ipconfig



GTK2



Unity



Windows Native



Cocoa OS X



101011
001110
111110
00101
0000
1000
0001
001
010
10
00

Designed for dynamic environments (road warriors)

But also used on 70 \$ routers

or behind all the others to route around DNSSEC support in those routers

See the following presentation.

<https://www.dnssec-deployment.org/index.php/2012/03/is-a-70-router-fast-enough-for-dnssec/>

RECENT IMPROVEMENTS

Auto detecting hot-spot sign-on

Software Update for Windows and OSX

RPM readily available.



That's it folks

Questions:
olaf@nlnetlabs.nl

or
wouter@nlnetlabs.nl

If you use our software then consider to support
NLnet Labs' mission Financially:
<http://www.nlnetlabs.nl/labs/contributors/>