DNSSEC trigger

Or how to get DNSSEC to the end-user

Wouter Wijngaards
&
Olaf Kolkman

NLnet Labs

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

NLnet Labs

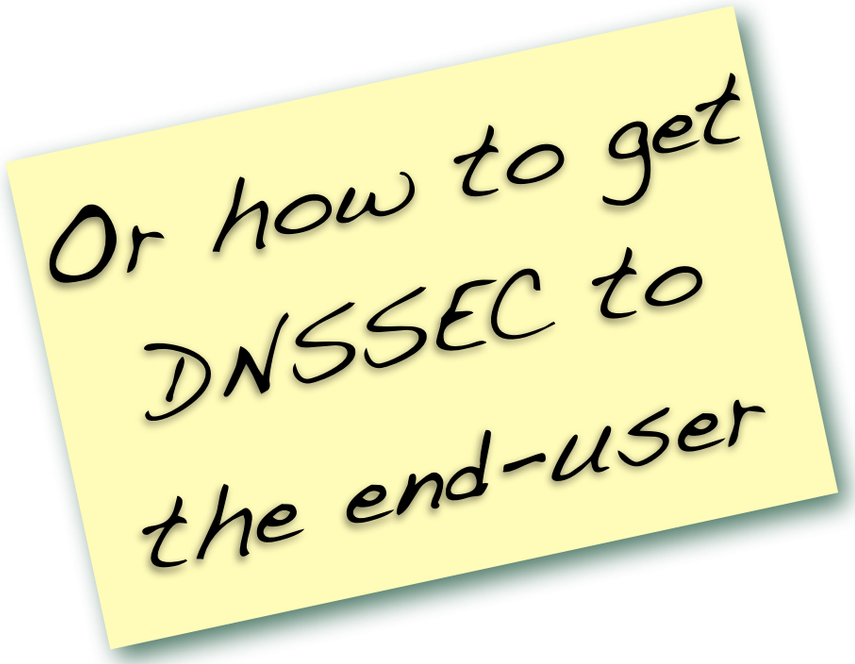
Executive Summary

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

Fire and Forget

NLnet Labs

Motivation



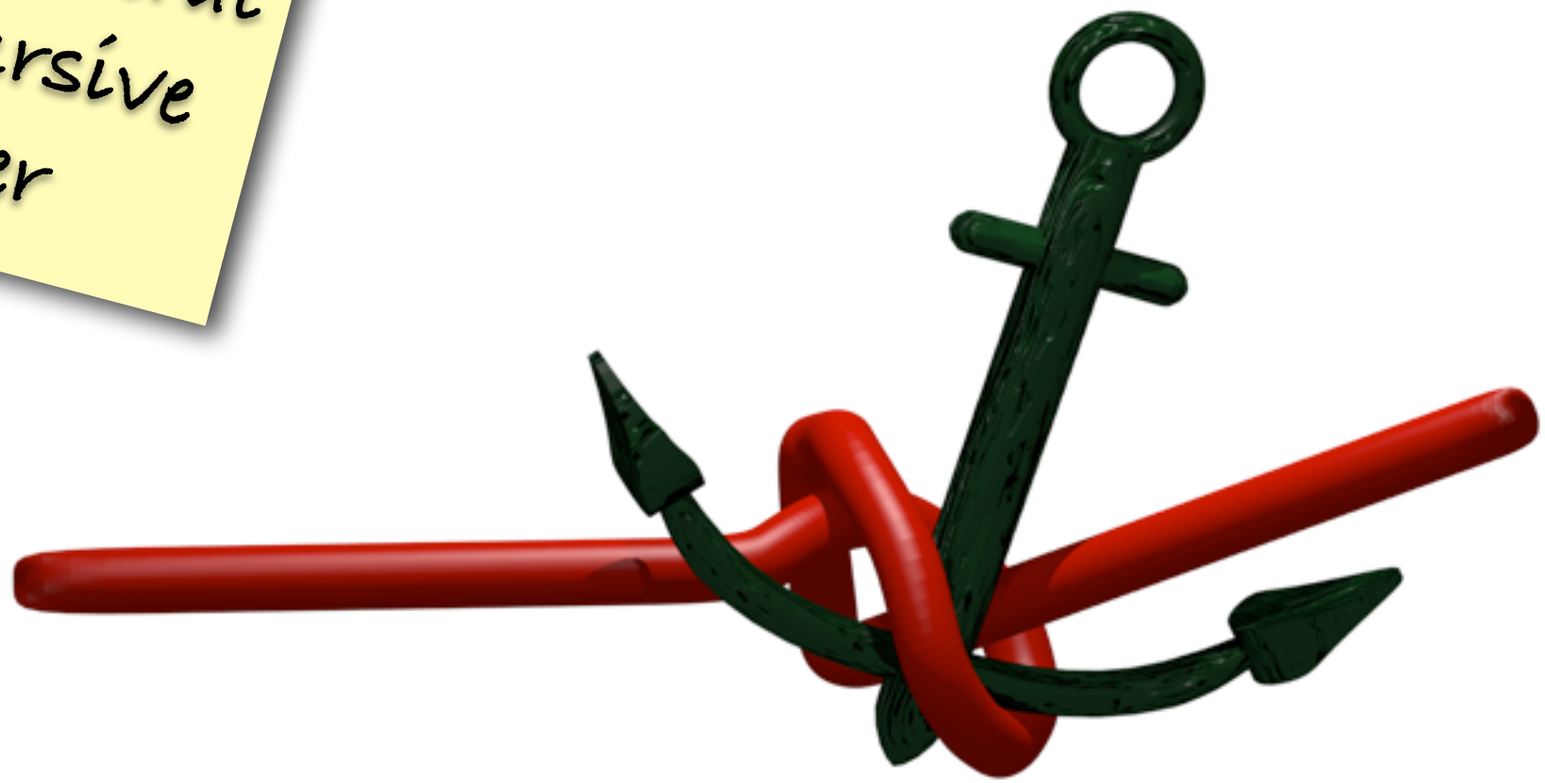
NLnet Labs

Components

Automatic probing and configuration software

Unbound

A (specific) general purpose Recursive Nameserver

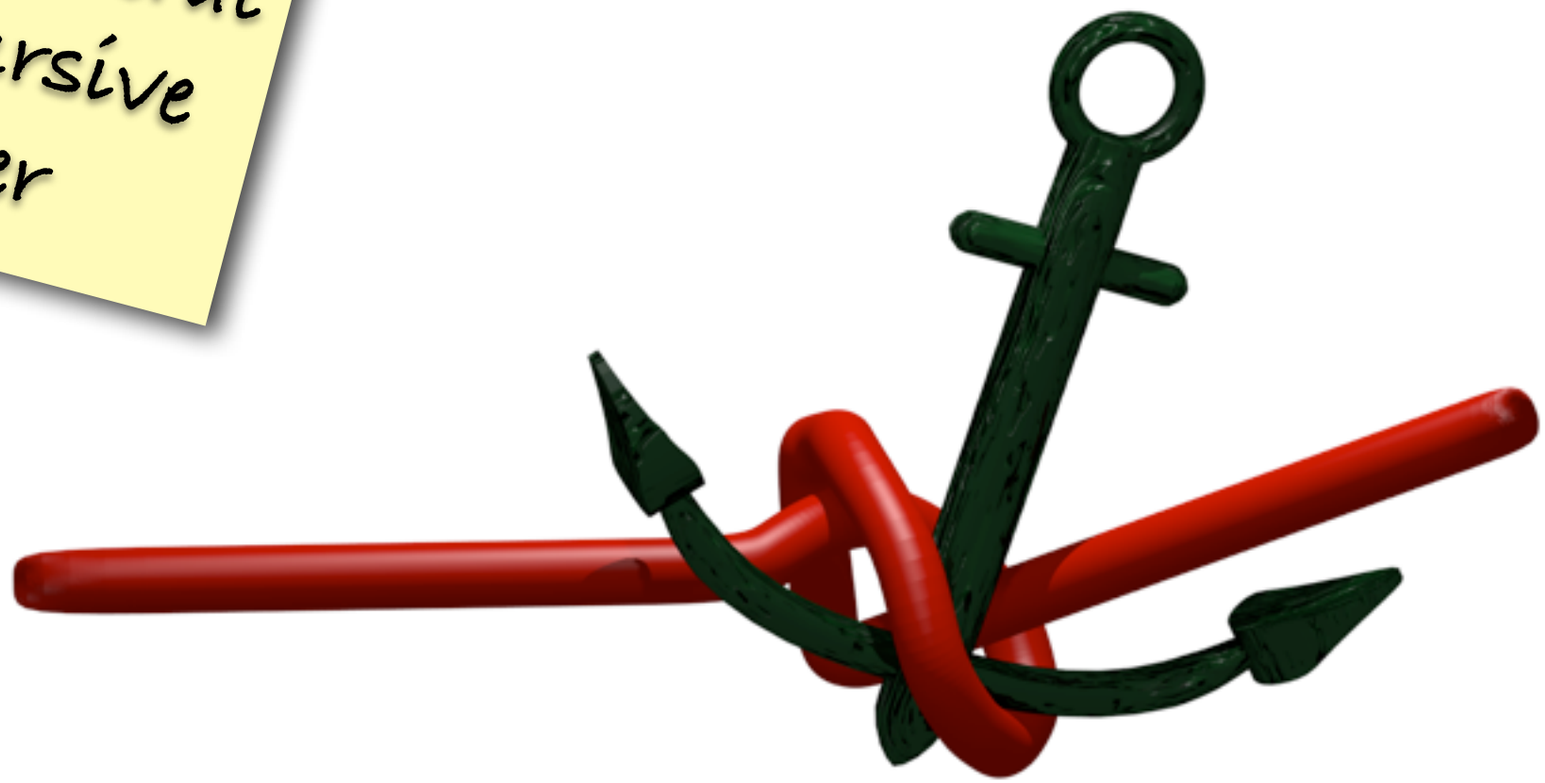


NLnet Labs

Unbound

A (specific) general purpose Recursive Nameserver

Automatic probing and configuration software



NLnet Labs

Initial configuration

Unbound Anchor

Root Key

Unbound

incoming DHCP info

Machine specific

dnssec-trigger daemon

DNS Probes

Unbound specific

unbound-control sets Forwarding Config

Dynamic configuration

/etc/resolv.conf

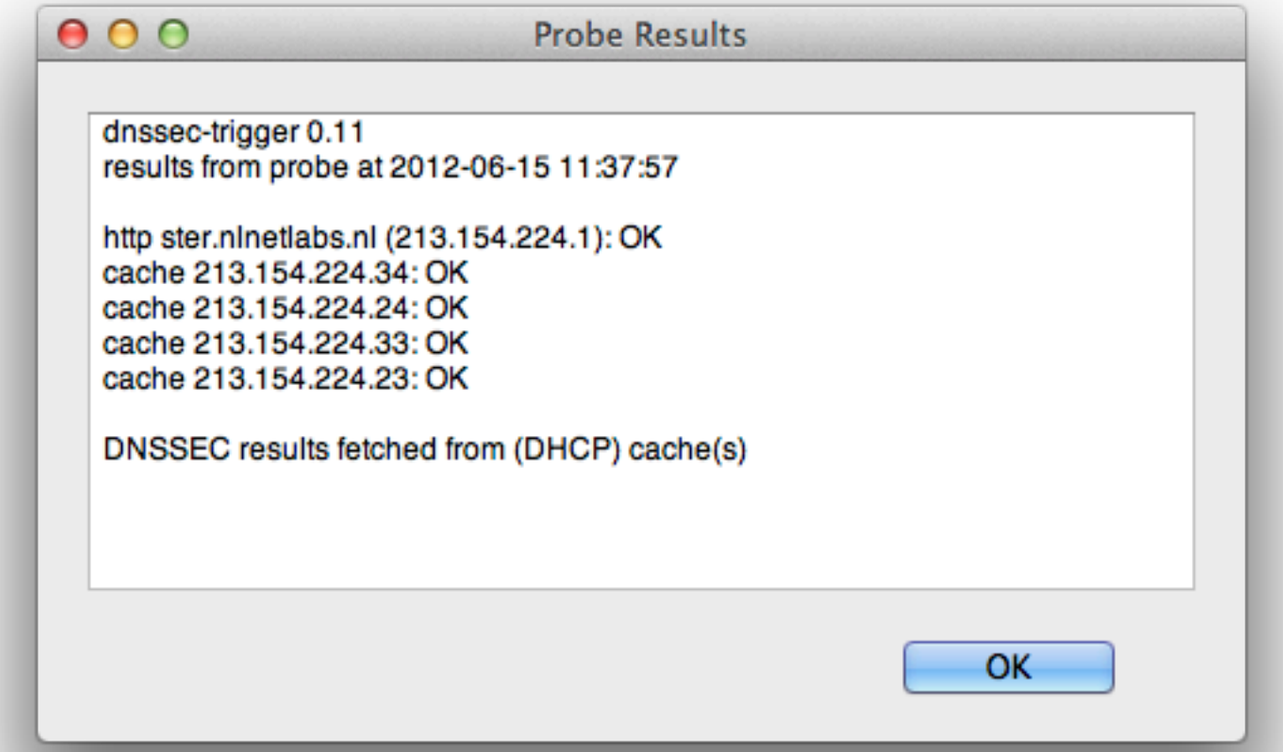
user space

NLnet Labs

Normal Operation

NLnet Labs

Normal Operation



NLnet Labs

PROBE EXPECTATIONS

EDNS support

RRSIGS

DNSKEY and DS

NSEC3 Support

Lengthy Packets (>512)

Transparent Proxy that is transparent to DNSSEC

AND IT WILL PROBE AGAIN

If insecure against its will

exp backoff

NLnet Labs

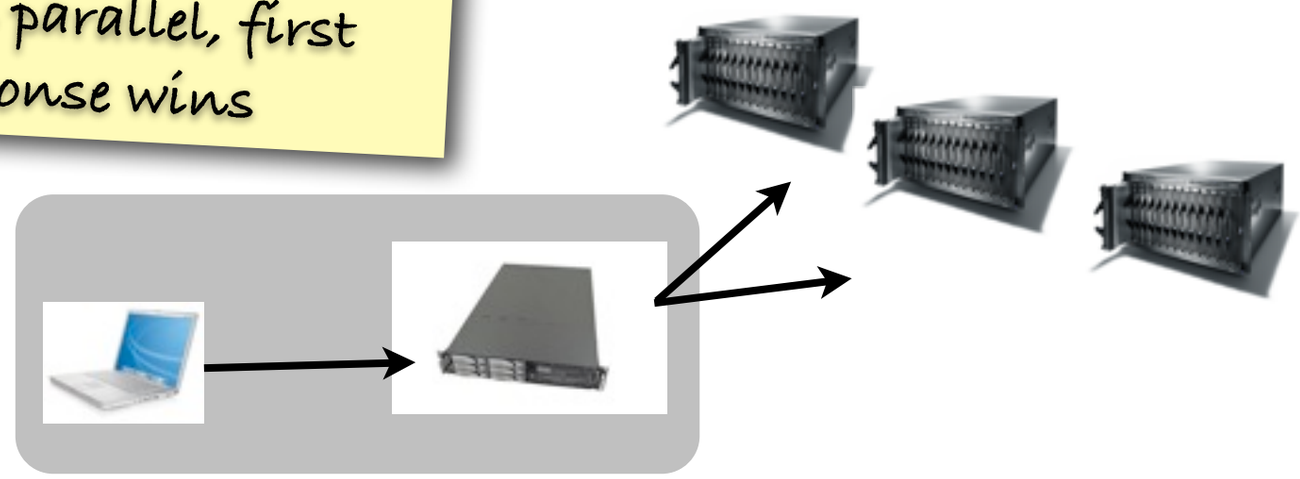
PROBING STRATEGY

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

PROBING STRATEGY

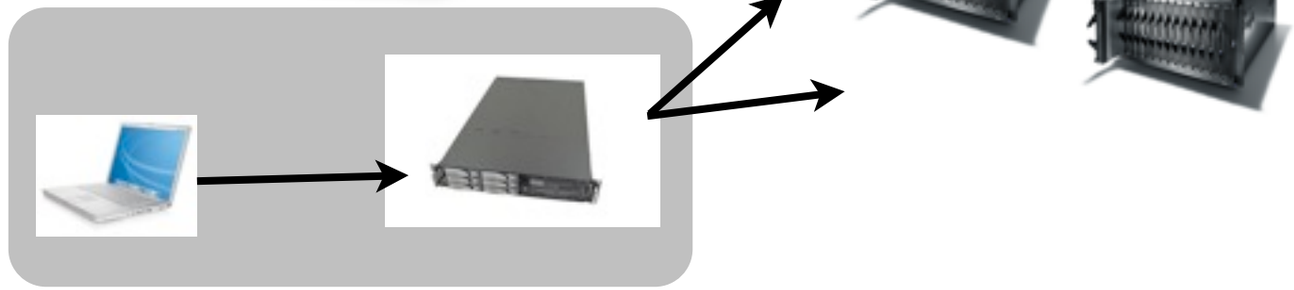
All IPs in resolv.conf are tried in parallel, first response wins

Use cache from DHCP



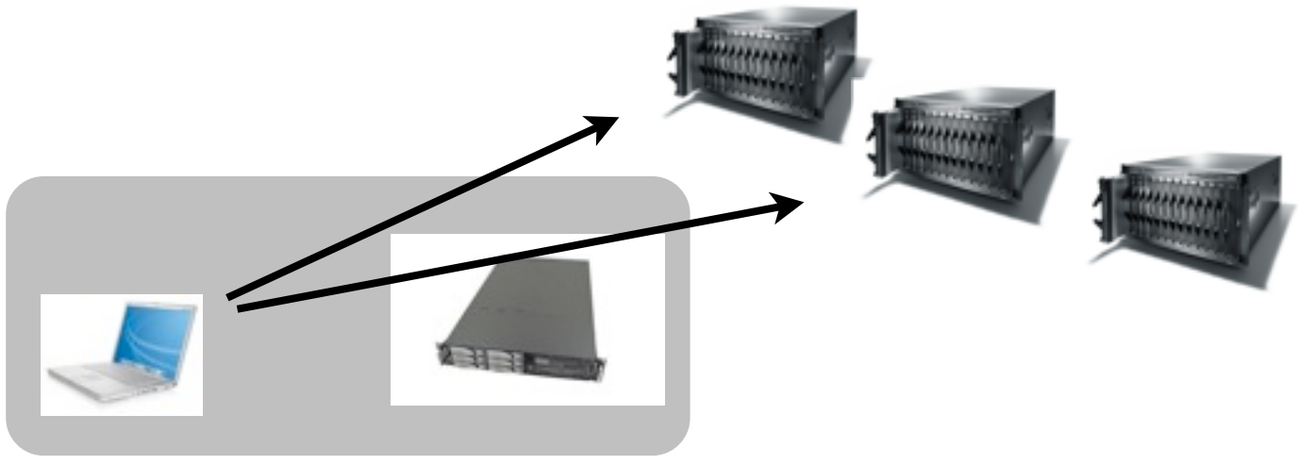
PROBING STRATEGY

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



Use cache from DHCP

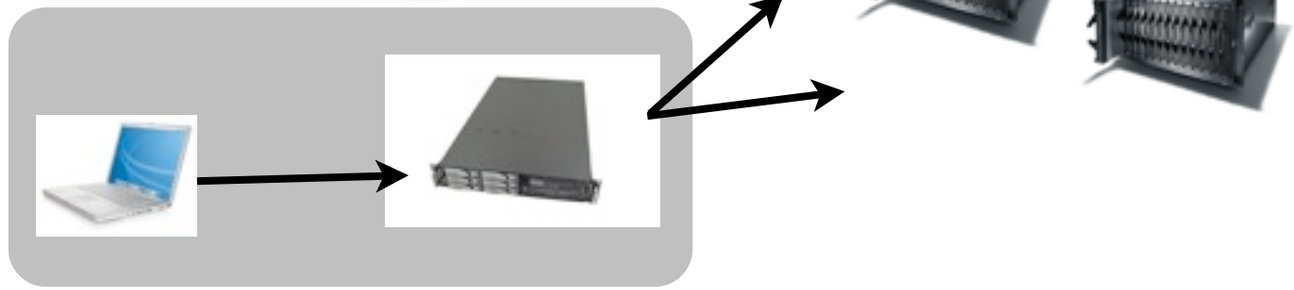
Full resolver mode, querying authority servers directly



NLnet Labs

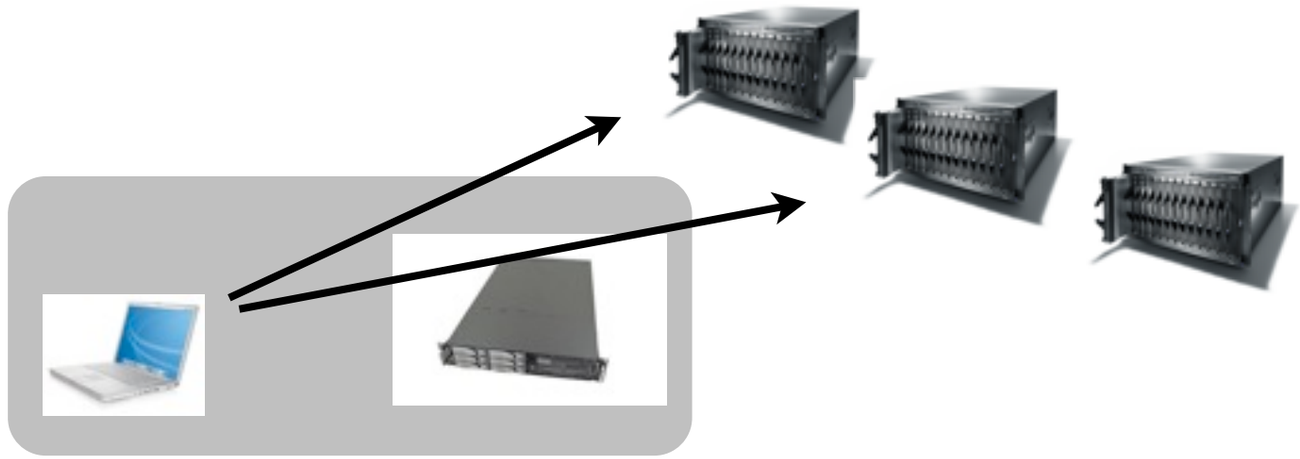
PROBING STRATEGY

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

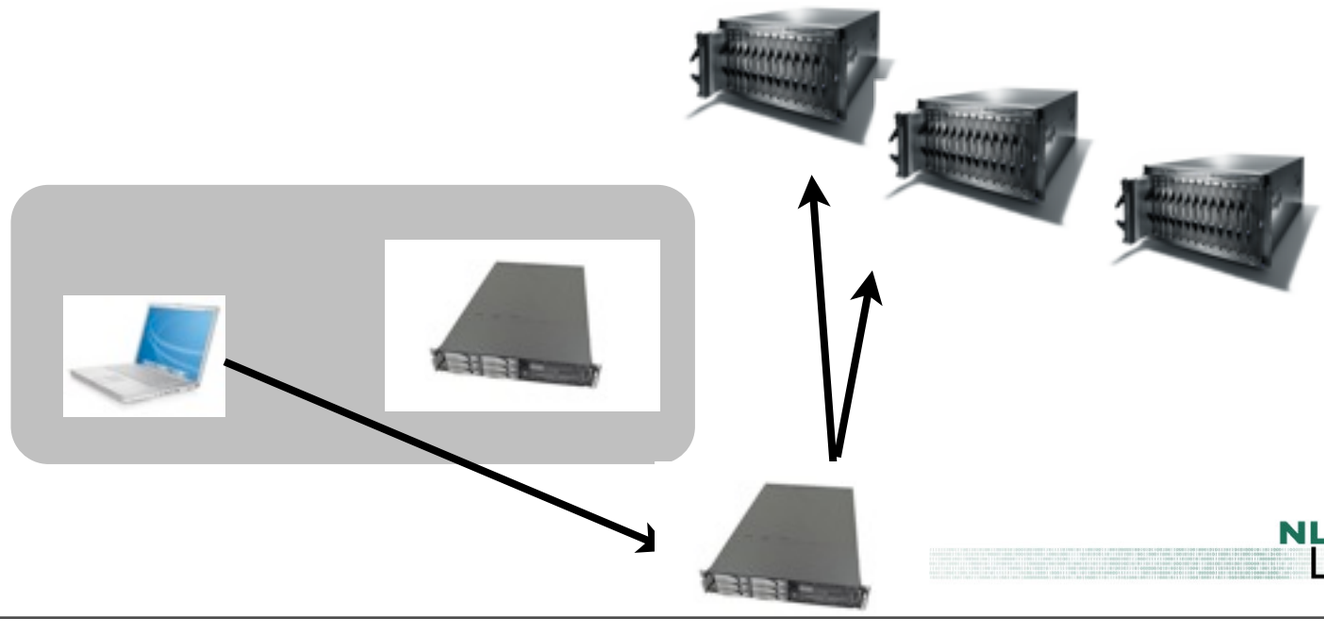


Use cache from DHCP

Full resolver mode, querying authority servers directly



Port 80 and 443 to an NLnet Labs resolver



NLnet Labs

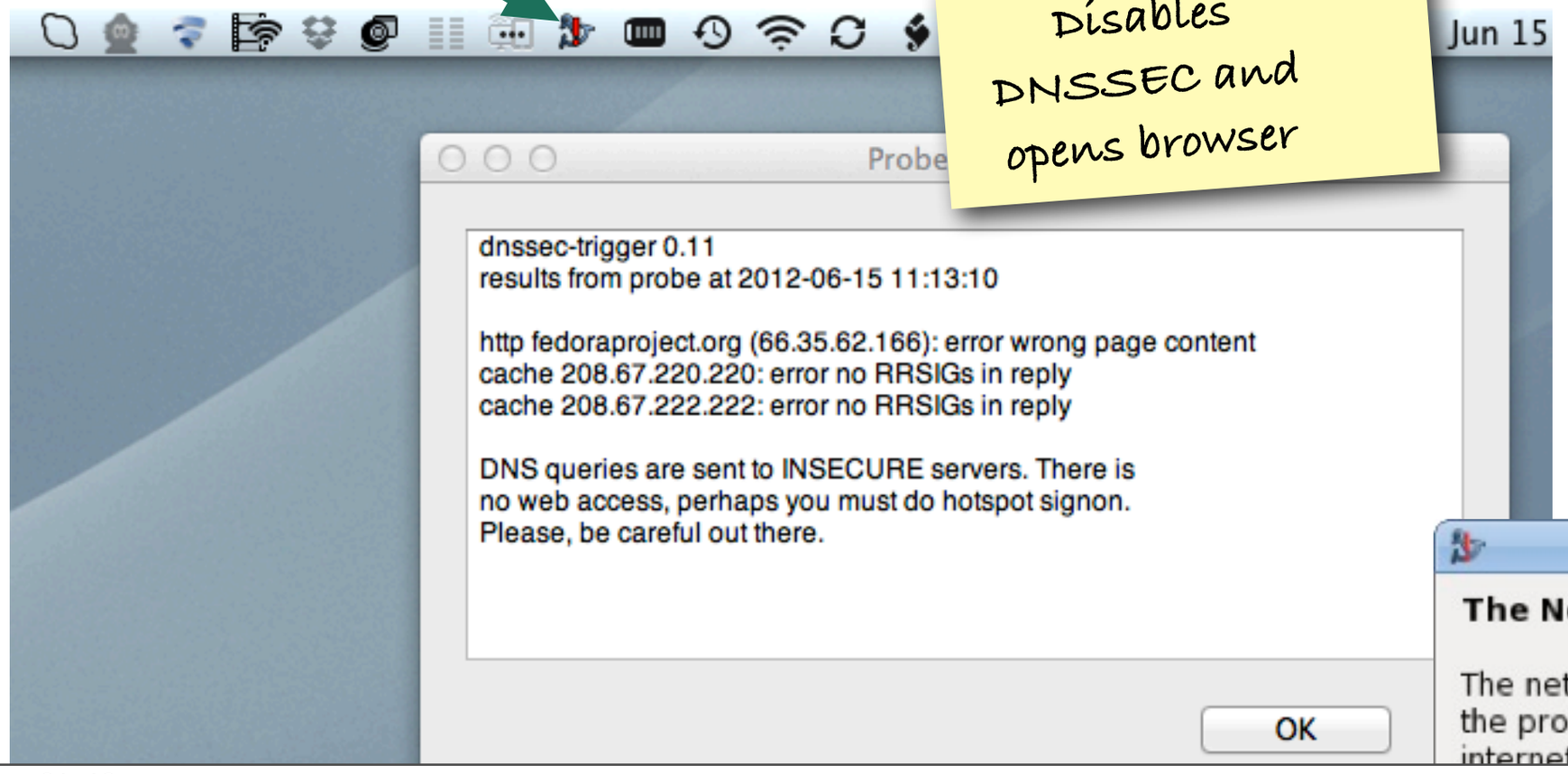
ON THE ROAD

No Pop-ups if everything just works

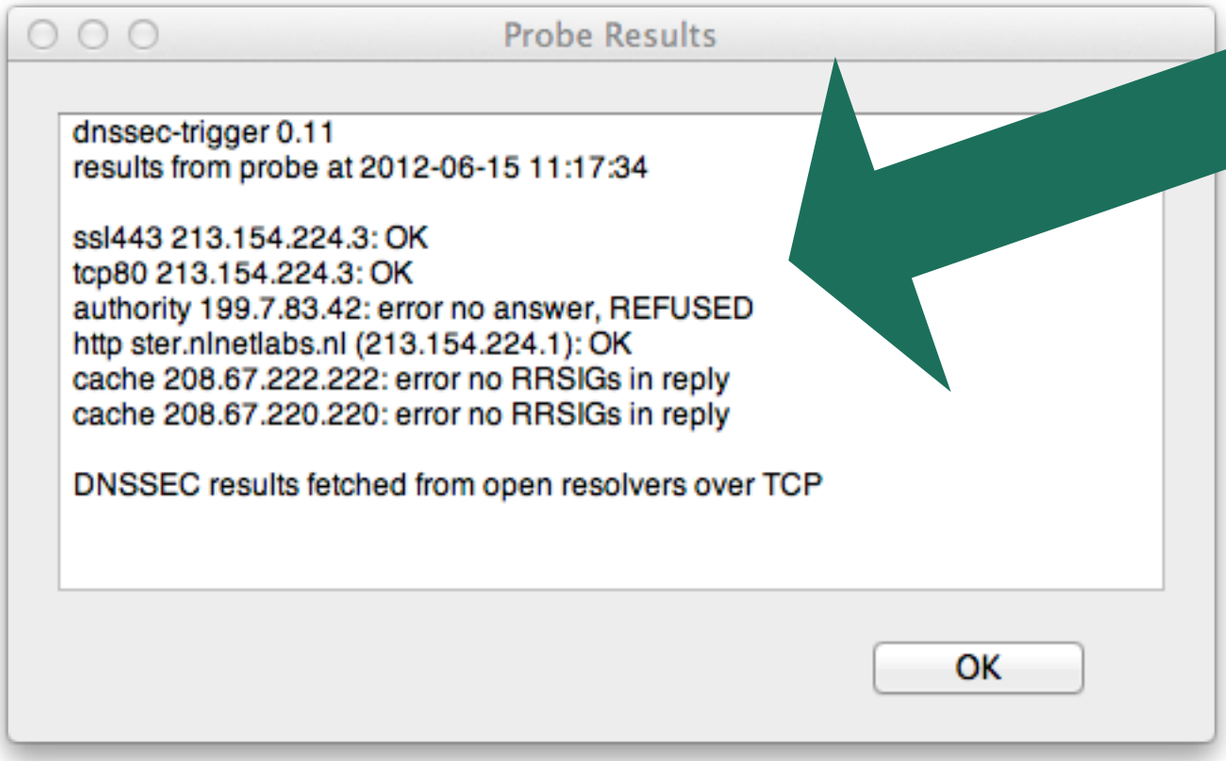
Only during probing operation

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

Disables DNSSEC and opens browser

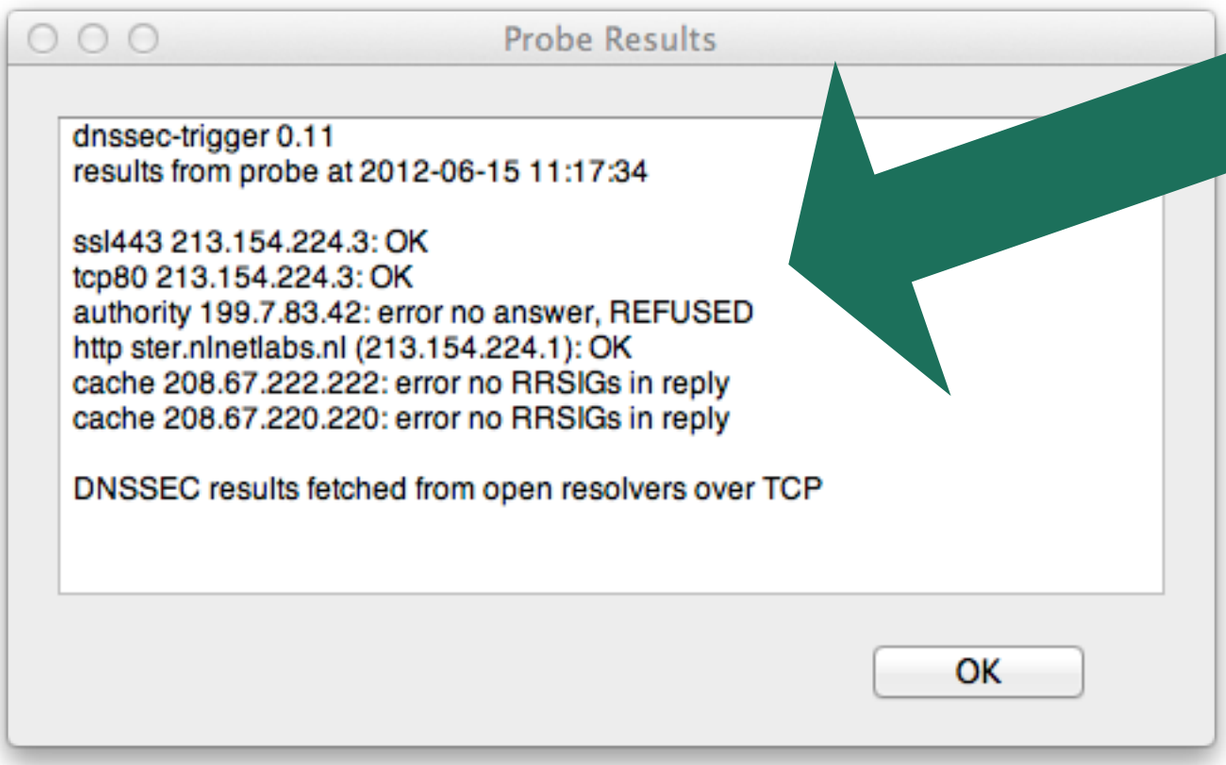


NLnet Labs



DNSSEC trigger worked around the local DNS resolver

NLnet Labs



DNSSEC trigger worked around the local DNS resolver

And you never even noticed

NLnet Labs

Network Manager
Netconfig

WSALookupService
(XP, Vista, 7)

scripts, ifconfig,
ipconfig

GTK2

Unity

Windows Native

Cocoa OS X

NLnet Labs

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.

Mailing list for user experiences

http://open.nlnetlabs.nl/mailman/listinfo/dnssec-trigger

Webpage

http://nlnetlabs.nl/projects/dnssec-trigger/

NLnet Labs

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/

NLnet Labs