DNS Related Activities at the RIPE NCC

Henk Uijterwaal

RIPE NCC New Projects Group

Amersfoort, 29 August 2005

Agenda

- RIPE and the RIPE NCC
  - Who we are
  - What we do
- DNS related areas where we are active
- Conclusions

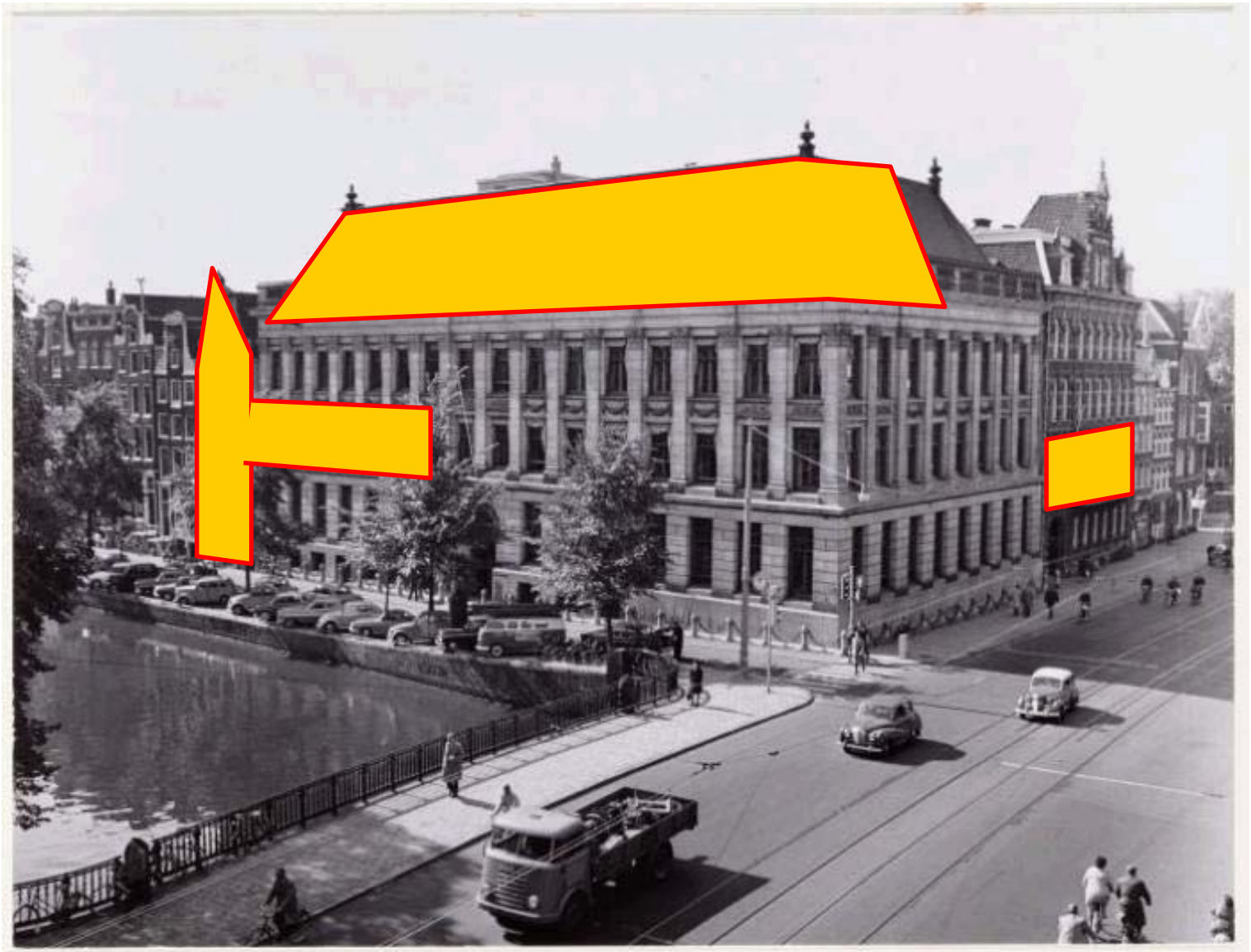
RIPE and the RIPE NCC

- RIPE: Réseaux IP Européen
  - Established 1989
  - Informal organization of people interested in wide area IP based networks
  - Platform for the administrative and technical coordination necessary to operate the Internet within the RIPE region
  - No formal membership
  - Volunteers doing work in working groups and through mailing lists
- Some activities became more and more work

RIPE and the RIPE NCC

- RIPE NCC: RIPE Network Coordination Centre
  - Established 1991
  - RIPE ≠ RIPE NCC
  - Organization to perform activities that its members need to organize as a group, even though they are competitors in other areas
  - Membership association: ± 4000 members
    - ISP's, Telco's, TLD's, research networks, corporations
  - Neutral, independent and not-for-profit
  - 100 staff from about 20 countries
  - Located in Amsterdam, NL

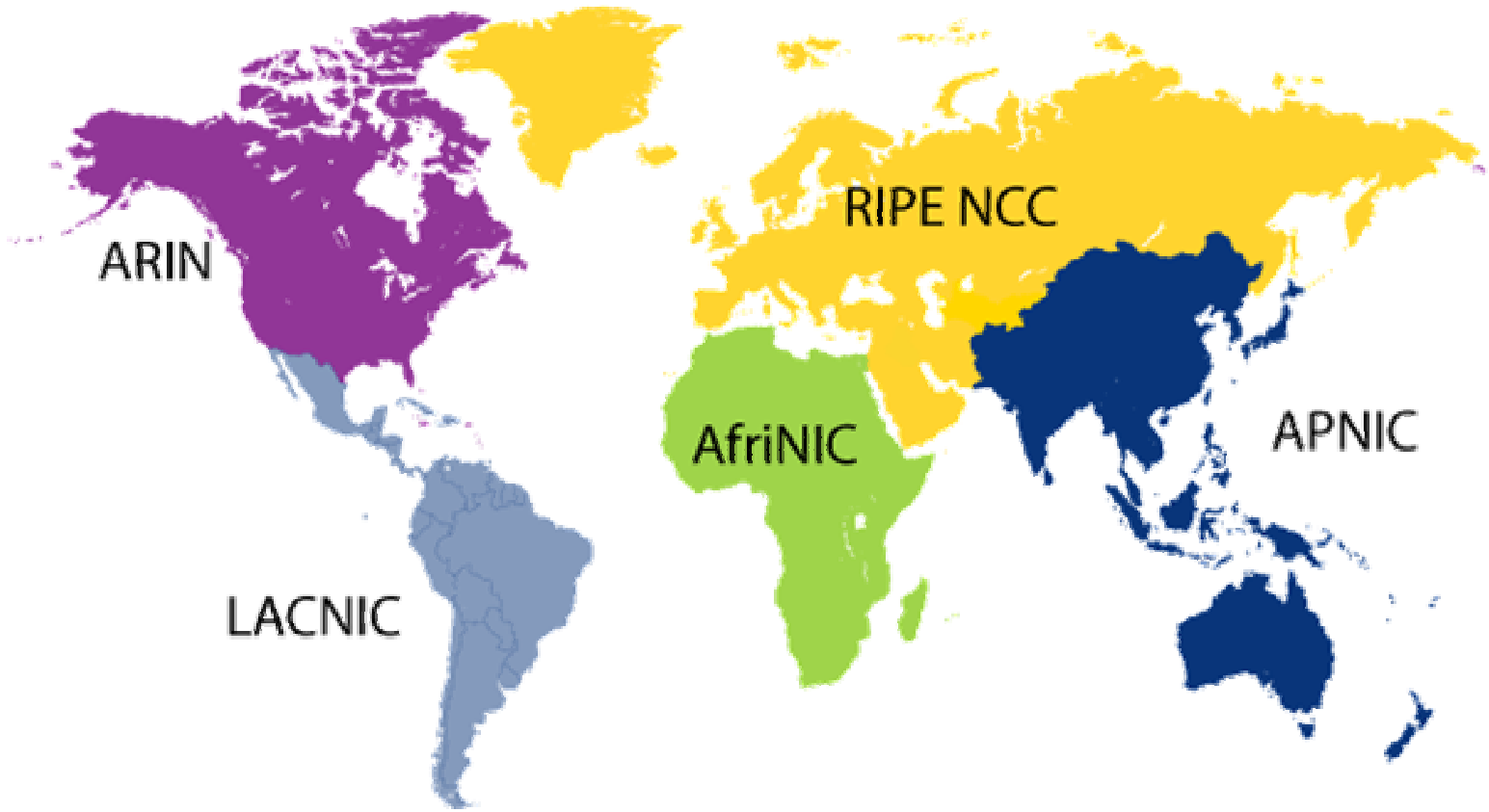
Our office



RIPE NCC's services

- Regional Internet Registry (RIR) services
  - 1 of 5 worldwide
  - IP and AS registration
  - In-addr.apra
- "whois" data-base with operational information
- Liaison with EU, goverments, ICANN, IETF, ITU, …
- Training courses (CIDR, RR, DNSSEC)
- Administrative support for RIPE
- New Projects

RIR Service Regions



RIR services only, other services for the entire community

DNS Related Activities

- Kroot and Kroot anycast
- DNSMON
- DNSSEC

- In-addr.apra
- Hostcount
- Training courses on DNSSEC

Agenda

- RIPE and the RIPE NCC
- DNS related areas where we are active
  - Kroot and Kroot anycast
  - DNSMON
  - DNSSEC
- Conclusions

Root Server System

- Provides name service for the root zone
  - gTLDs (.com, .org, .net, …)
  - ccTLDs (.nl, .de, .be, …)
- Key element in the Internet Infrastructure
- 13 root name servers
  - a.root-server … m.root-server.net
  - 13 is a practical limit
  - An average client comes here <8 times/week
- Hosting and location
  - Diversity of hosts and locations
  - No single point of failure

Location of Root Servers

- Locations were all selected before 1997
  - Based on Internet usage back then
  - Heavy bias towards the US (10 of 13)
- The Internet became a global utility since then
- Have root servers distributed more over the world
- But 13 servers is the practical limit
- Use anycast

IP Anycast

- Point to point communication between a single client and the nearest destination server
  - RFC 1546 (1993)
- Clone a server
  - Multiple locations
  - Same IP address
  - Identical data
- Benefits
  - Distribution
  - Performance
  - Redundancy

Deployment of K root Anycast

- RIPE NCC has operated K root in London since 1997
  - Service for all ISP's
  - Neutral, independent
- Started to add anycast in 2003
- 2 kinds of nodes:
  - Global (3 sites)
  - Local (10 sites, only respond to queries from others at an IX)
  - Other root servers use anycast as well

Location of nodes

Creating more diversity

- bind
  - De facto standard root server software
  - Open source, carefully tested and well maintained by ISC
  - If there is a bug or exploit, one can potentially damage all root servers
- We need a second implementation
  - Joint project RIPE NCC with NLNET Labs
  - 2002-2005
  - Develop an alternative for bind

NSD or Name Server Daemon

- NSD is an authoritative only, high performance, simple and open source name server.
  - Written from scratch
  - The current stable release is NSD 2.3.0.
- Download at NLNET labs for free
  - Open source
  - Long term support commitment
- NSD runs on some of the k-root anycast nodes

Agenda

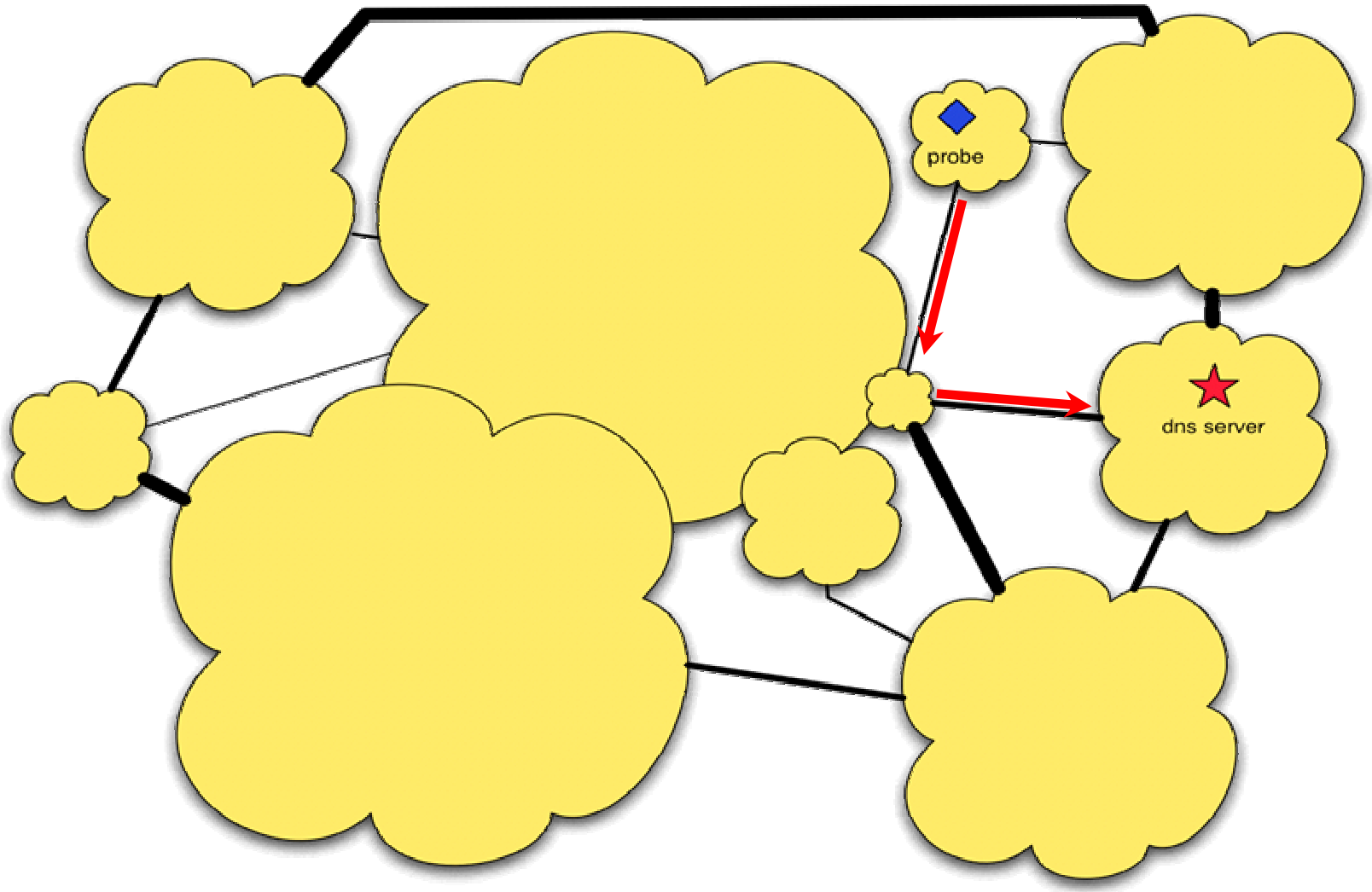
- RIPE and the RIPE NCC
- DNS related areas where we are active
  - Kroot and Kroot anycast
  - DNSMON
  - DNSSEC
- Conclusions

DNSMON: DNS Monitoring

- DNS service is important
- Measure performance

- There are lots of bad measurements out there!
  - Newspaper article: Ping from a journalist's home to root servers
  - Ping - what does it measure?
  - Where is the problem located?
- People (press, regulators) read those articles

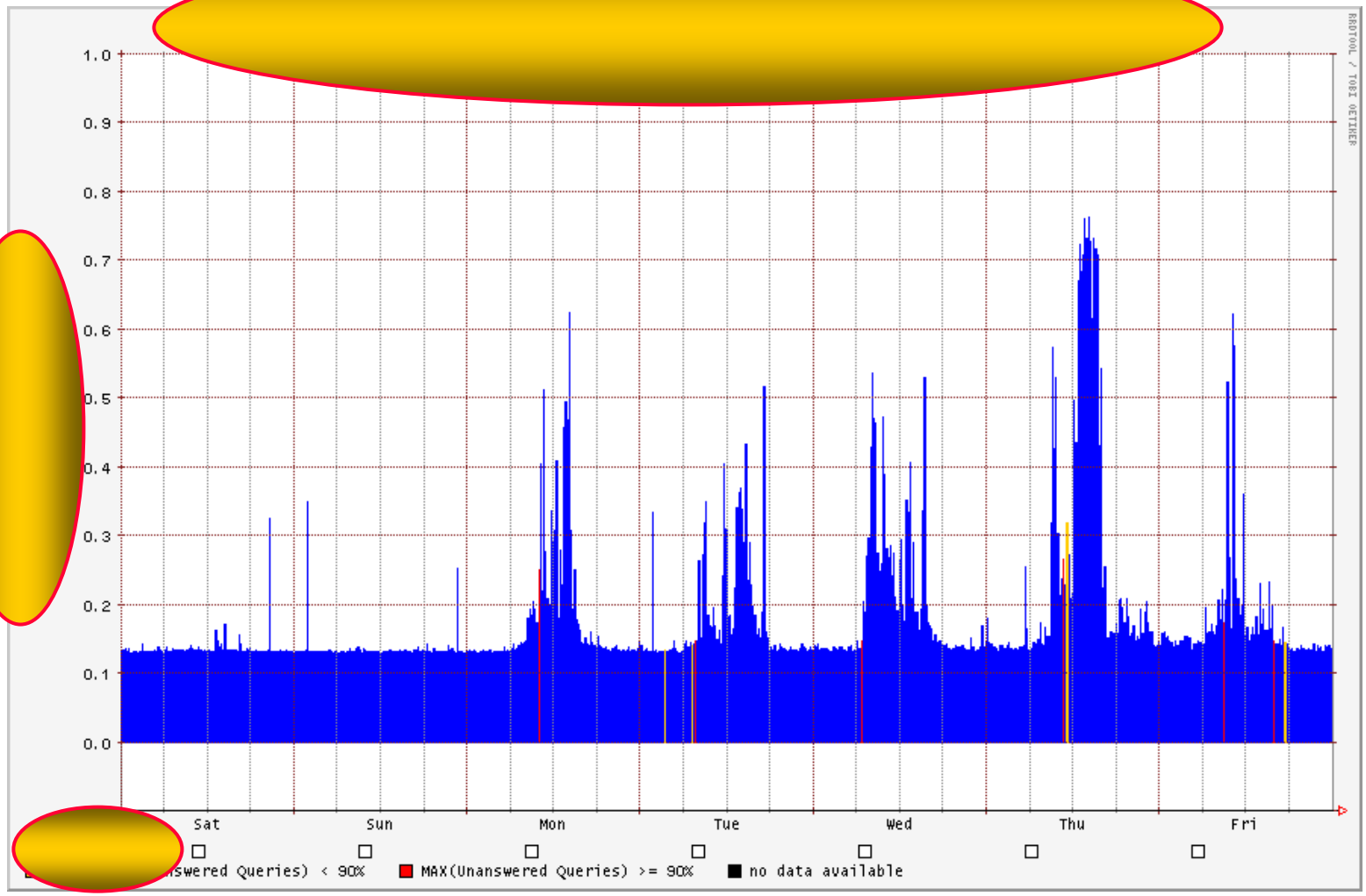
DNS Service is important

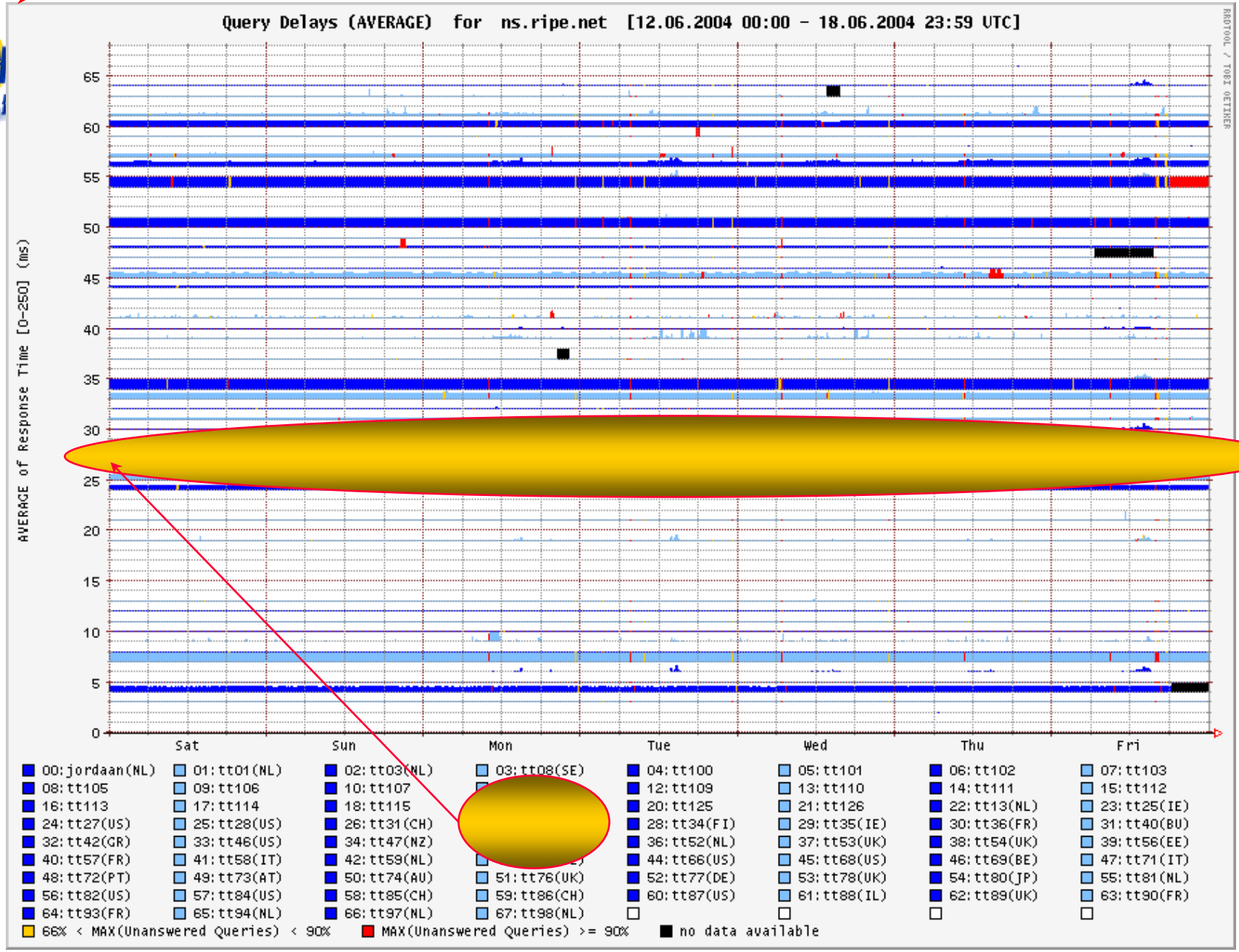


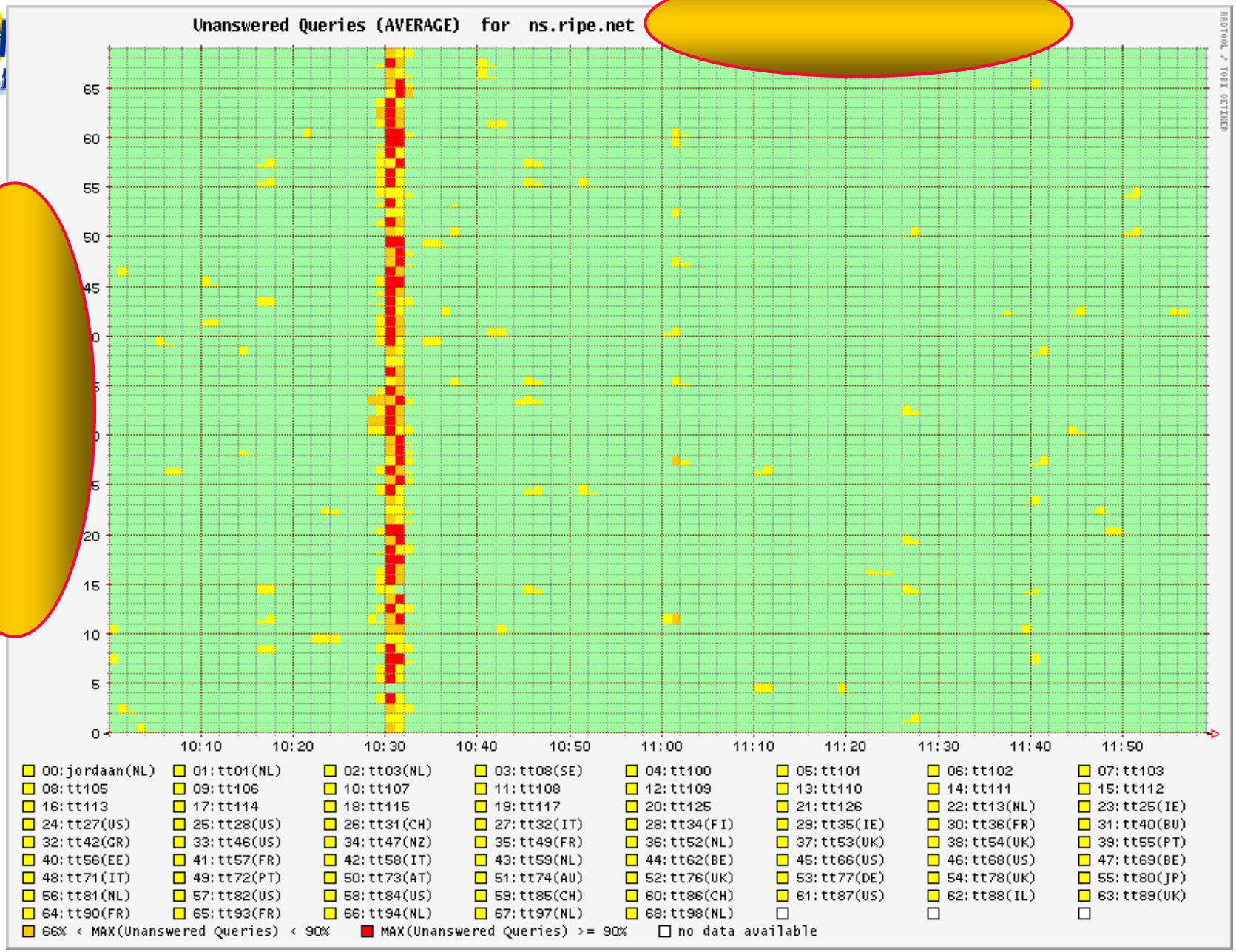
DNSMON Goals

- Better Measurements
  - From multiple points
  - Real DNS traffic
- Independent and Objective
- Interactive and better presentation
  - Stacked plots allow people to easily see trends

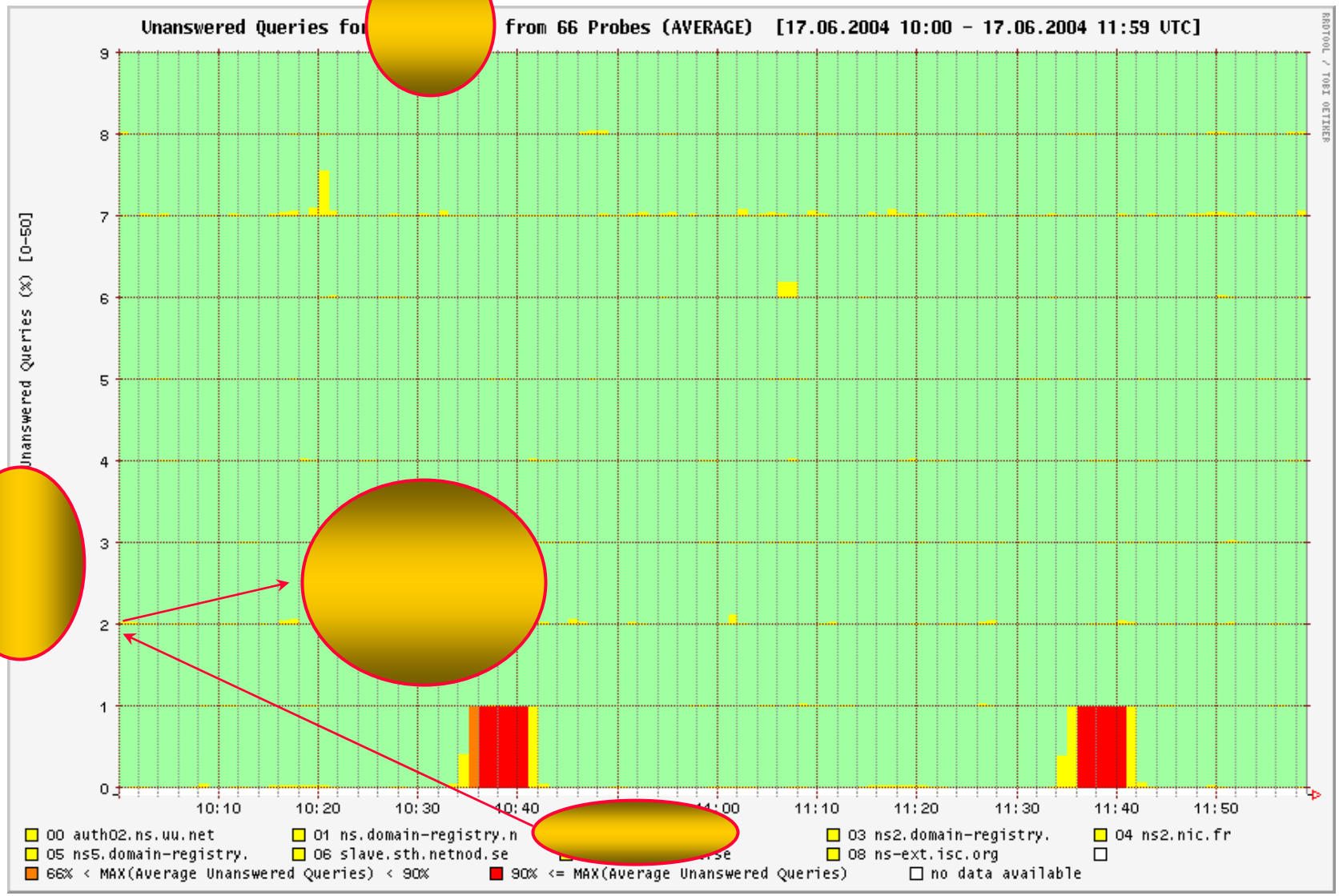
Single Point Measurement




Query Delays (AVERAGE) for ns.ripe.net [12.06.2004 00:00 - 18.06.2004 23:59 UTC]
AVERAGE of Response Time [0-250] (ms)
0
5
10
15
20
25
30
35
40
45
50
55
60
65
Sat
Sun
Mon
Tue
Wed
Thu
Fri
00:jordaan(NL)
01:tt01(NL)
02:tt03(NL)
03:tt08(SE)
04:tt100
05:tt101
06:tt102
07:tt103
08:tt105
09:tt106
10:tt107
12:tt109
13:tt110
14:tt111
15:tt112
16:tt113
17:tt114
18:tt115
20:tt125
21:tt126
22:tt13(NL)
23:tt25(IE)
24:tt27(US)
25:tt28(US)
26:tt31(CH)
28:tt34(FI)
29:tt35(IE)
30:tt36(FR)
31:tt40(BU)
32:tt42(GR)
33:tt46(US)
34:tt47(NZ)
36:tt52(NL)
37:tt53(UK)
38:tt54(UK)
39:tt56(EE)
40:tt57(FR)
41:tt58(IT)
42:tt59(NL)
44:tt66(US)
45:tt68(US)
46:tt69(BE)
47:tt71(IT)
48:tt72(PT)
49:tt73(AT)
50:tt74(AU)
51:tt76(UK)
52:tt77(DE)
53:tt78(UK)
54:tt80(JP)
55:tt81(NL)
56:tt82(US)
57:tt84(US)
58:tt85(CH)
59:tt86(CH)
60:tt87(US)
61:tt88(IL)
62:tt89(UK)
63:tt90(FR)
64:tt93(FR)
65:tt94(NL)
66:tt97(NL)
67:tt98(NL)
66% < MAX(Unanswered Queries) < 90%
MAX(Unanswered Queries) >= 90%
no data available


Unanswered Queries (AVERAGE) for ns.ripe.net
65
60
55
50
45
0
5
20
15
10
5
0
10:10
10:20
10:30
10:40
10:50
11:00
11:10
11:20
11:30
11:40
11:50
00:jordaan(NL)
01:tt01(NL)
02:tt03(NL)
03:tt08(SE)
04:tt100
05:tt101
06:tt102
07:tt103
08:tt105
09:tt106
10:tt107
11:tt108
12:tt109
13:tt110
14:tt111
15:tt112
16:tt113
17:tt114
18:tt115
19:tt117
20:tt125
21:tt126
22:tt13(NL)
23:tt25(IE)
24:tt27(US)
25:tt28(US)
26:tt31(CH)
27:tt32(IT)
28:tt34(FI)
29:tt35(IE)
30:tt36(FR)
31:tt40(BU)
32:tt42(GR)
33:tt46(US)
34:tt47(NZ)
35:tt49(FR)
36:tt52(NL)
37:tt53(UK)
38:tt54(UK)
39:tt55(PT)
40:tt56(EE)
41:tt57(FR)
42:tt58(IT)
43:tt59(NL)
44:tt62(BE)
45:tt66(US)
46:tt68(US)
47:tt69(BE)
48:tt71(IT)
49:tt72(PT)
50:tt73(AT)
51:tt74(AU)
52:tt76(UK)
53:tt77(DE)
54:tt78(UK)
55:tt80(JP)
56:tt81(NL)
57:tt82(US)
58:tt84(US)
59:tt85(CH)
60:tt86(CH)
61:tt87(US)
62:tt88(IL)
63:tt89(UK)
64:tt90(FR)
65:tt93(FR)
66:tt94(NL)
67:tt97(NL)
68:tt98(NL)
66% < MAX(Unanswered Queries) < 90%
MAX(Unanswered Queries) >= 90%
no data available

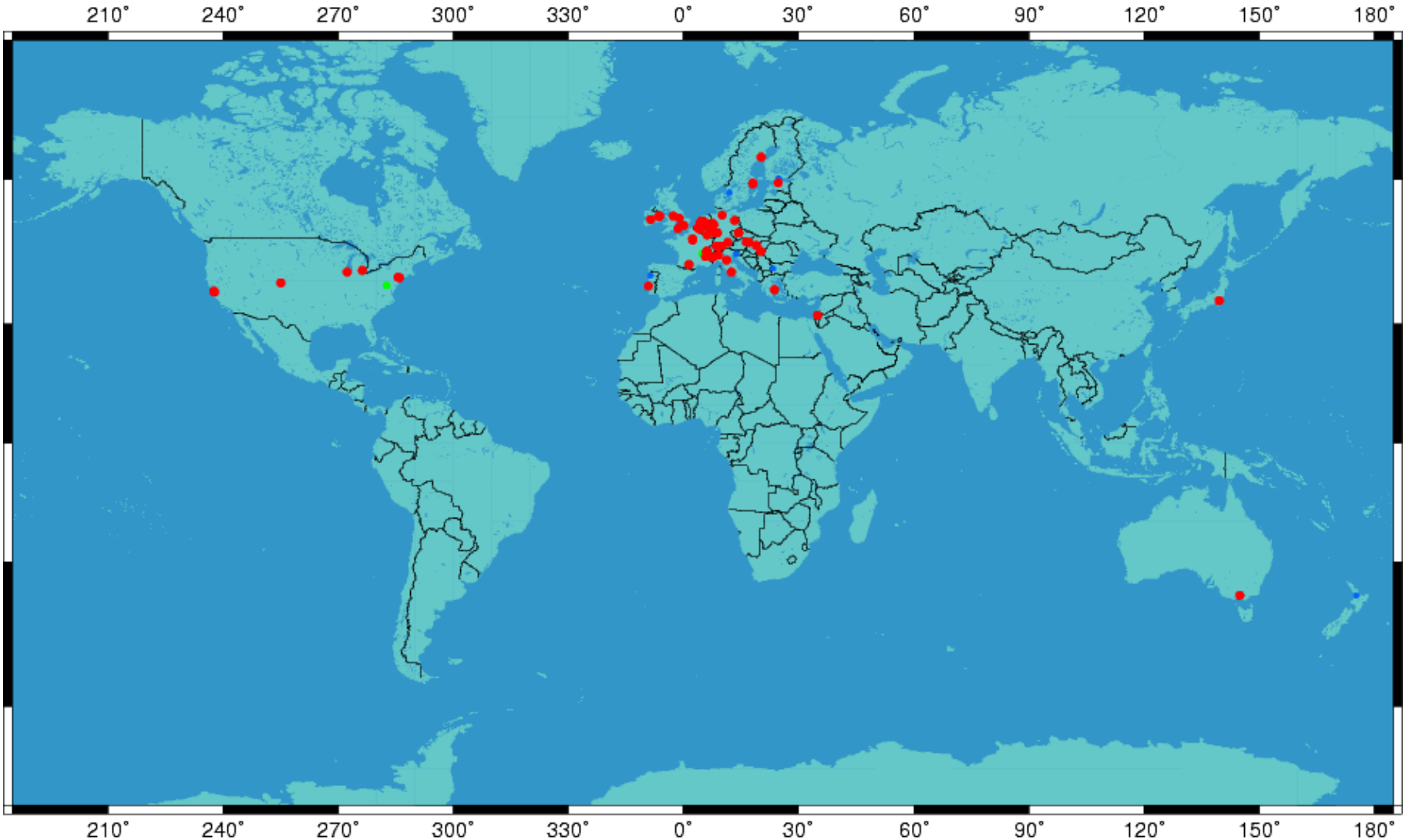
Average over a domain



Views of the data

- Server View
  - shows quality of service provided by the server to all probes
- Domain View
  - summarises quality of service provided by all servers serving a domain
- Probe View
  - shows quality of service provided by all servers at a particular probe location
  - Of interest to TB host (probe host)

dnsmon Probe Locations



What is Measured

- Real DNS queries
- Poisson distributed, ~60/hour/server/probe
- From 70+ probes around the world

- Response time
- Server instance ID (anycast, load balancing)
- SOA version number
- Server software version

What is ***Not*** Measured

- DNS queries used in actual name resolution
- Total DNS serv***ice*** quality, e.g. ‘user experience’

- RIPE region bias

- Effects that last less than about a minute

But still very comprehensive measurements!

DNSMON Users

- Network Operators
- TLD Administrators
  - Both for a fee
  - Full support

- Internet Community
  - Governments, regulators, researchers, …
  - Free but delayed data
  - Limited support

Participate as a Network Operator

- Install a test box in your network
  - DNSMON
  - Network performance (delay, loss, jitter, …)
    - RFC2679-2680
  - NTP server
- Buy hardware and service contract
  - €2000 hardware, €1000/year service
- Available for everybody

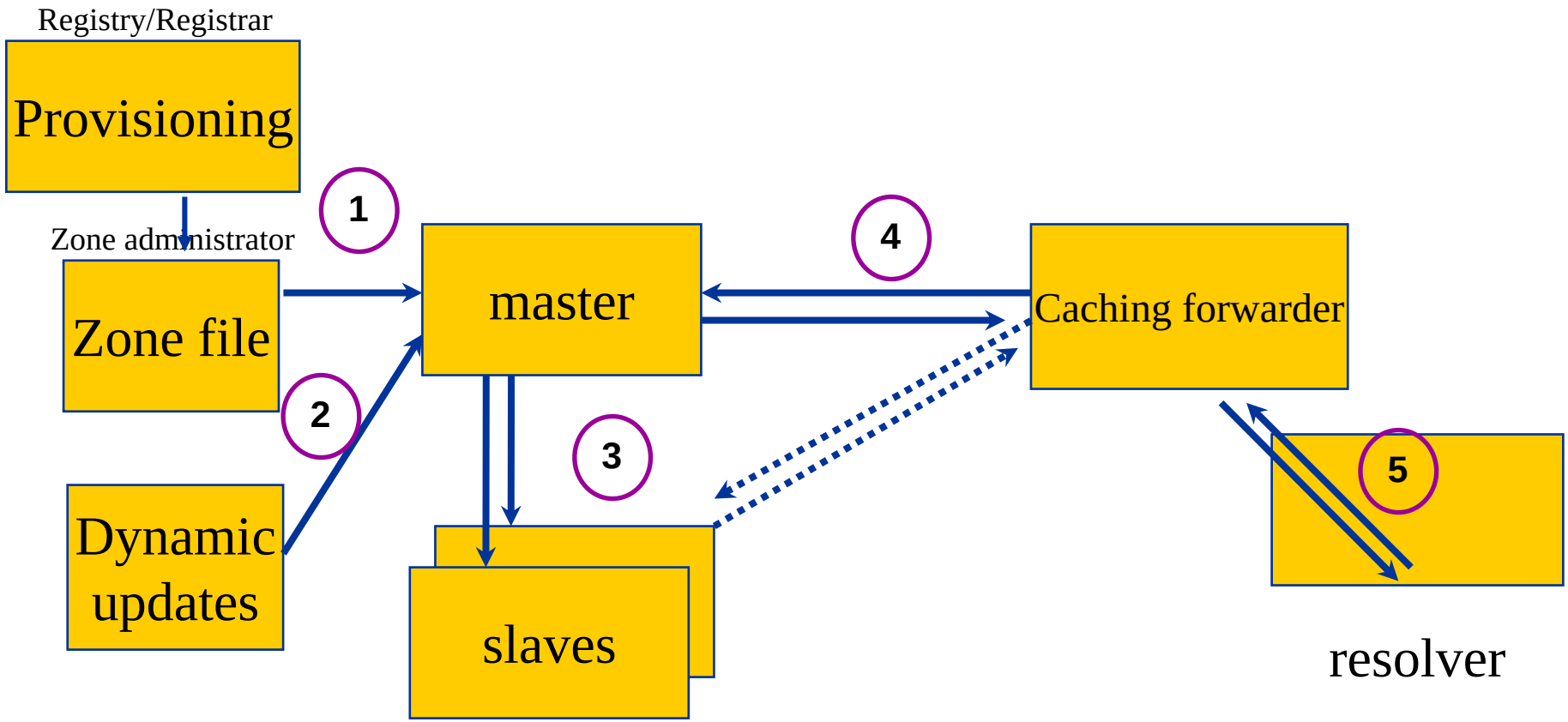
Service for Network Operators

- Non-exclusive
  - TLD Administrators are also a paying user
- Benefits
  - Credible 3rd party monitoring
  - Help desk support
  - Influence development
  - Guarantee of 12 months service continuity
  - Other network measurements
  - NTP server

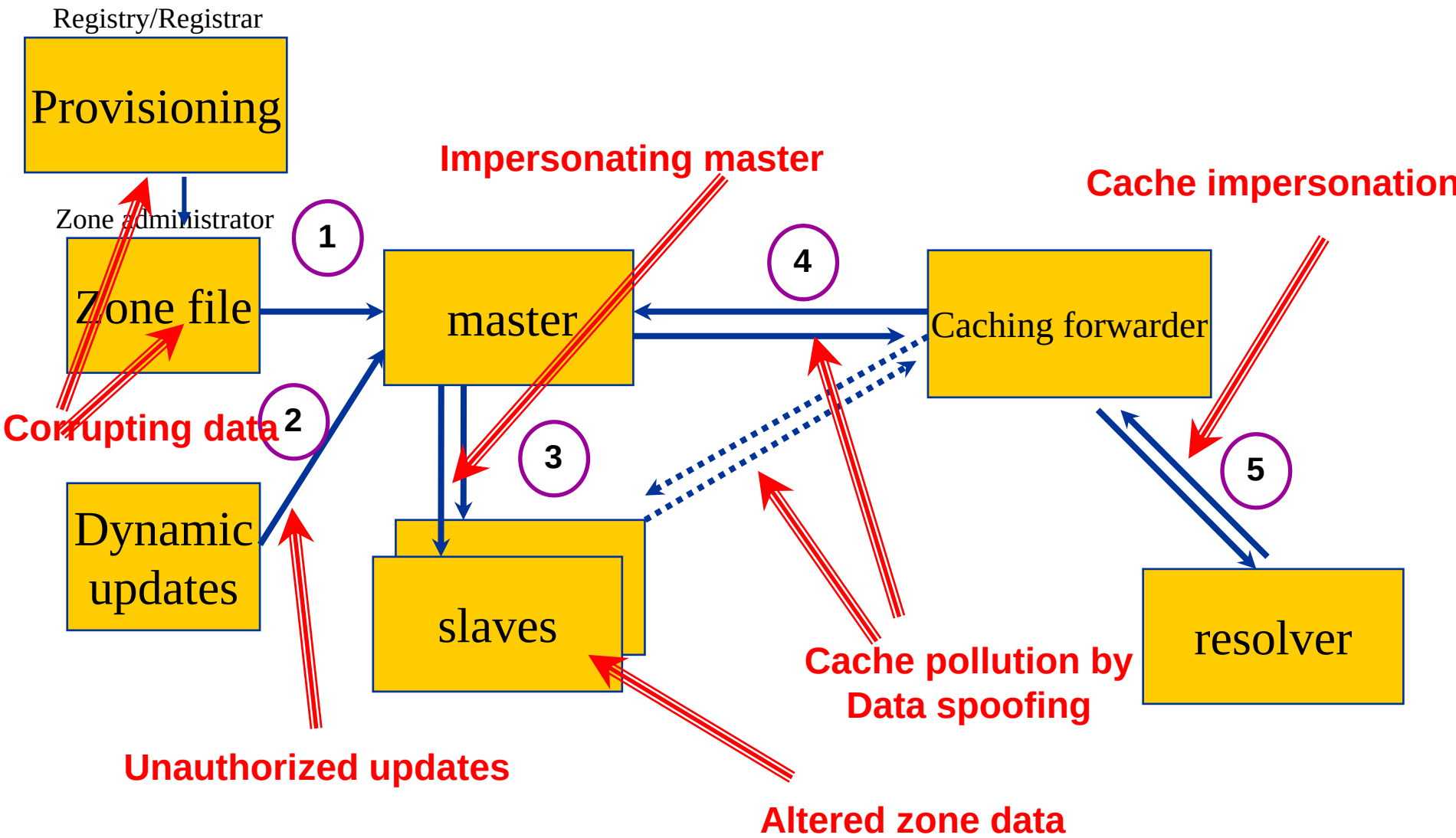
Agenda

- RIPE and the RIPE NCC
- DNS related areas where we are active
  - Kroot and Kroot anycast
  - DNSMON
  - DNSSEC
- Conclusions

DNS: Data Flow

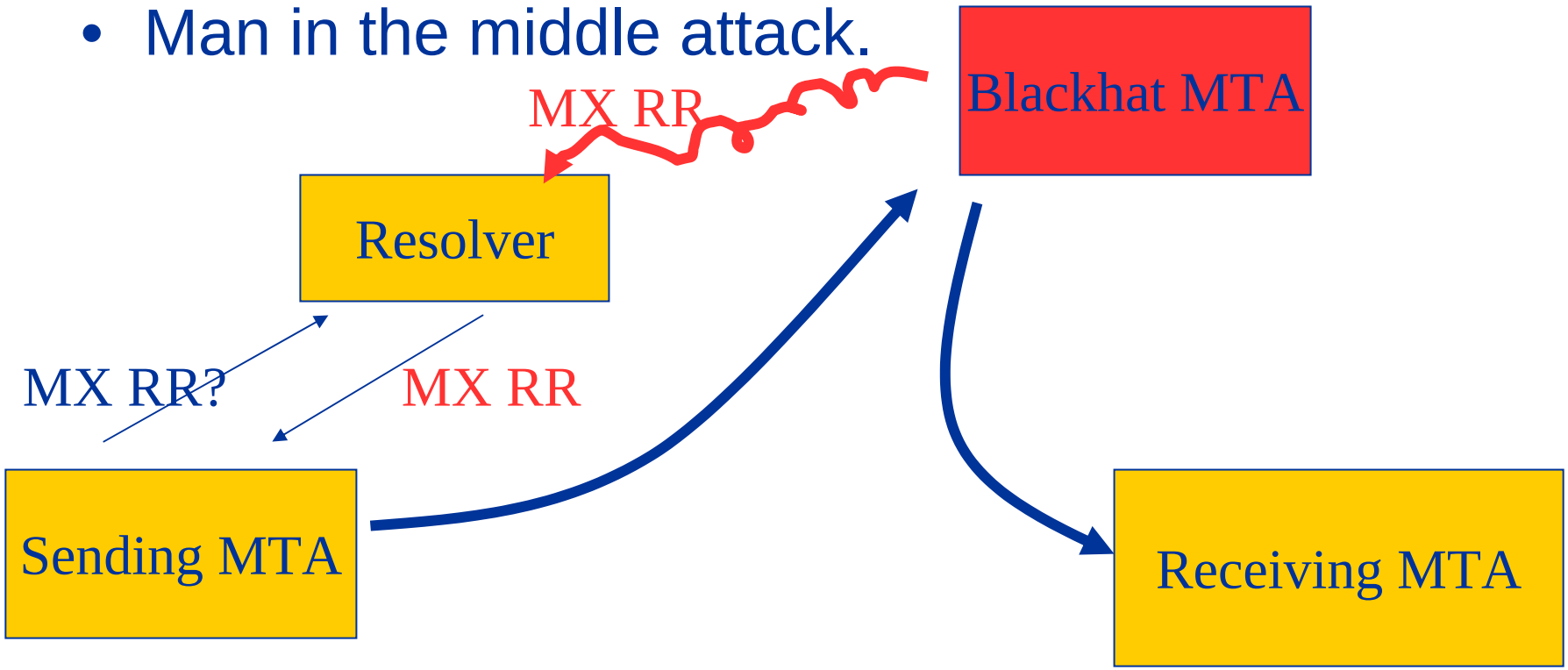


DNS Vulnerabilities



DNS exploit example

- Mail gets delivered to the MTA listed in the MX RR.
- Man in the middle attack.



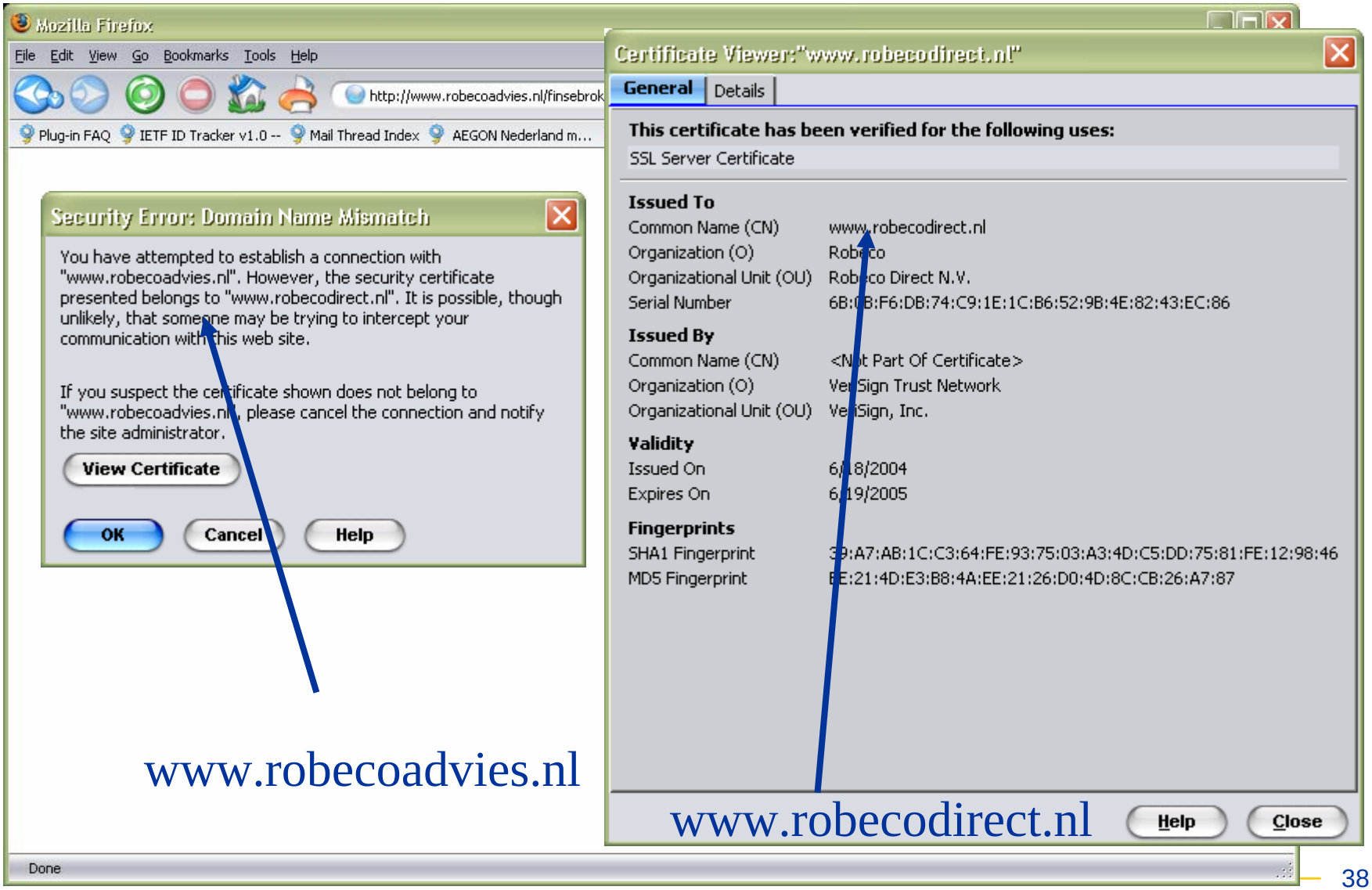
Possible DNS attacks

- Redirect traffic/Mail man in the middle
  - ‘Ouch, that mail contained sensitive information’
  - Who per default encrypts all their mails?
  - “We’ll notice when that happens, we have log files”
  - You have to match address to MTA for each logline.
- SPF, DomainKey and family
  - Technologies that use the DNS to mitigate spam and phishing: $$$ value for the black hats
- StockTickers, RSS feeds
  - Send out false information
- ENUM
  - Mapping telephone numbers to services in the DNS

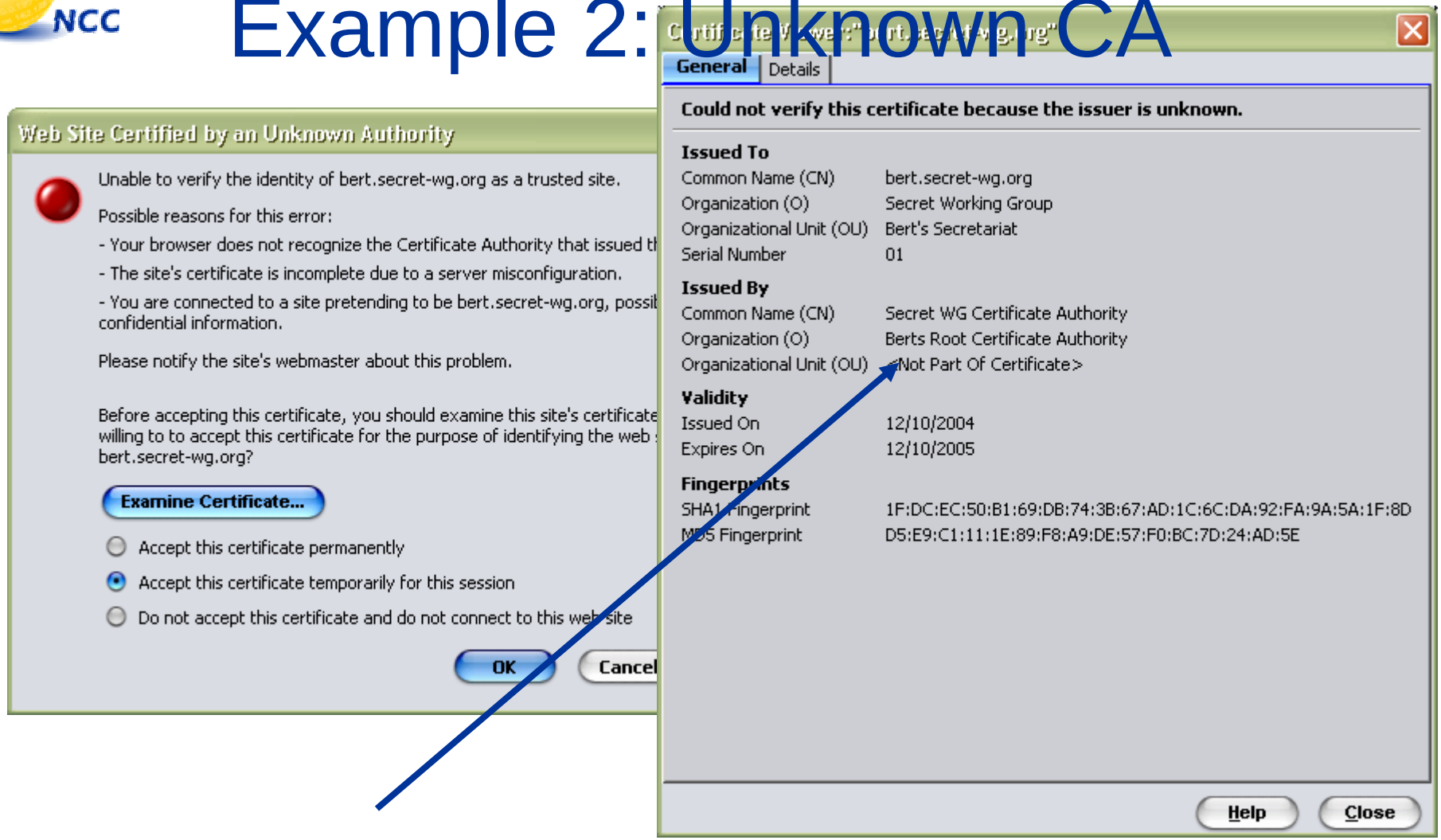
Mitigate by deploying SSL?

- Claim: SSL is not the magic bullet
  - (Neither is DNSSEC)
- Problem: Users are offered a choice
  - happens to often
  - users are not surprised but annoyed
- Not the technology but the implementation and use makes SSL vulnerable

Example 1: mismatched CN

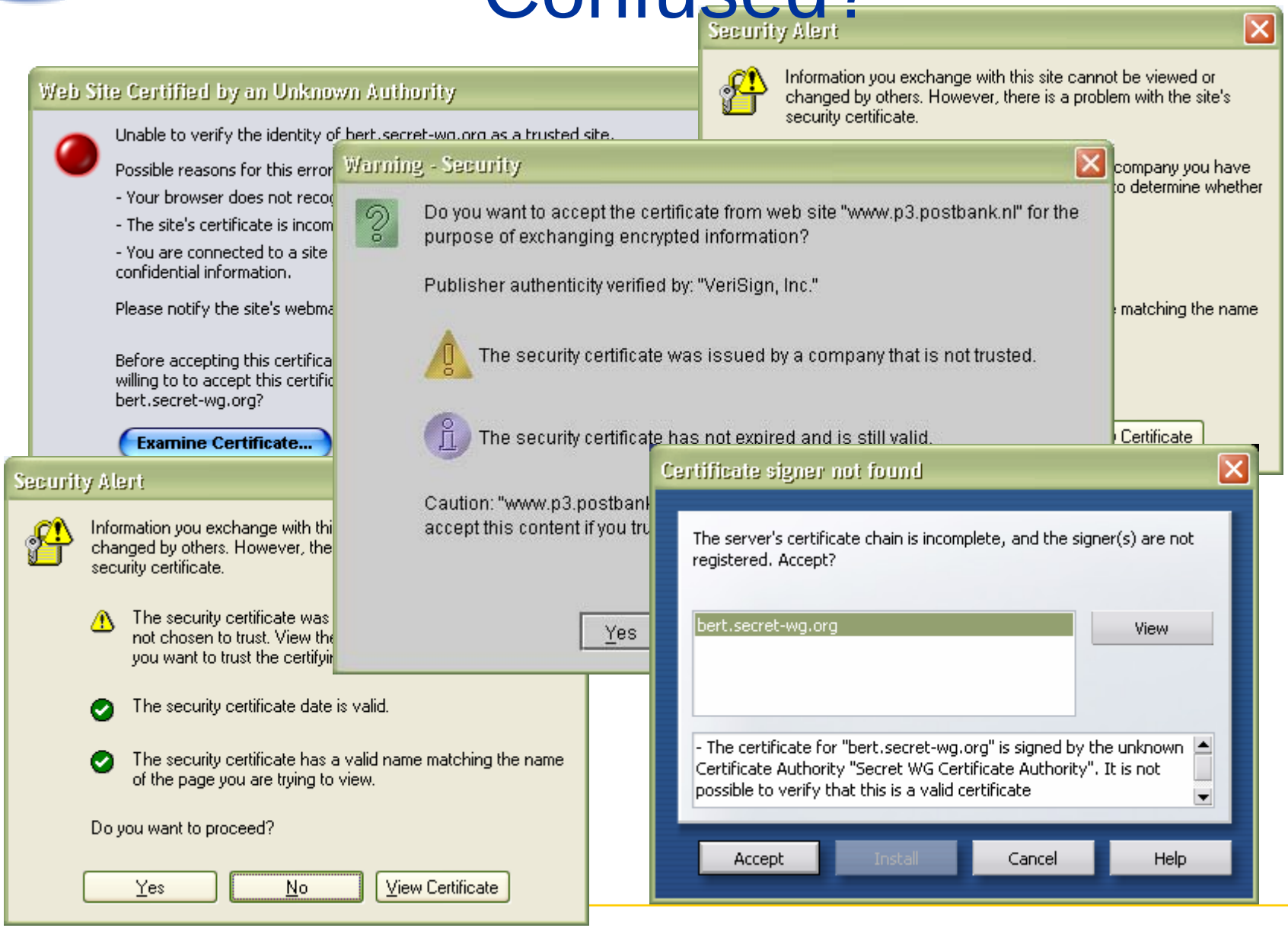


Example 2: Unknown CA



Unknown Certificate Authority

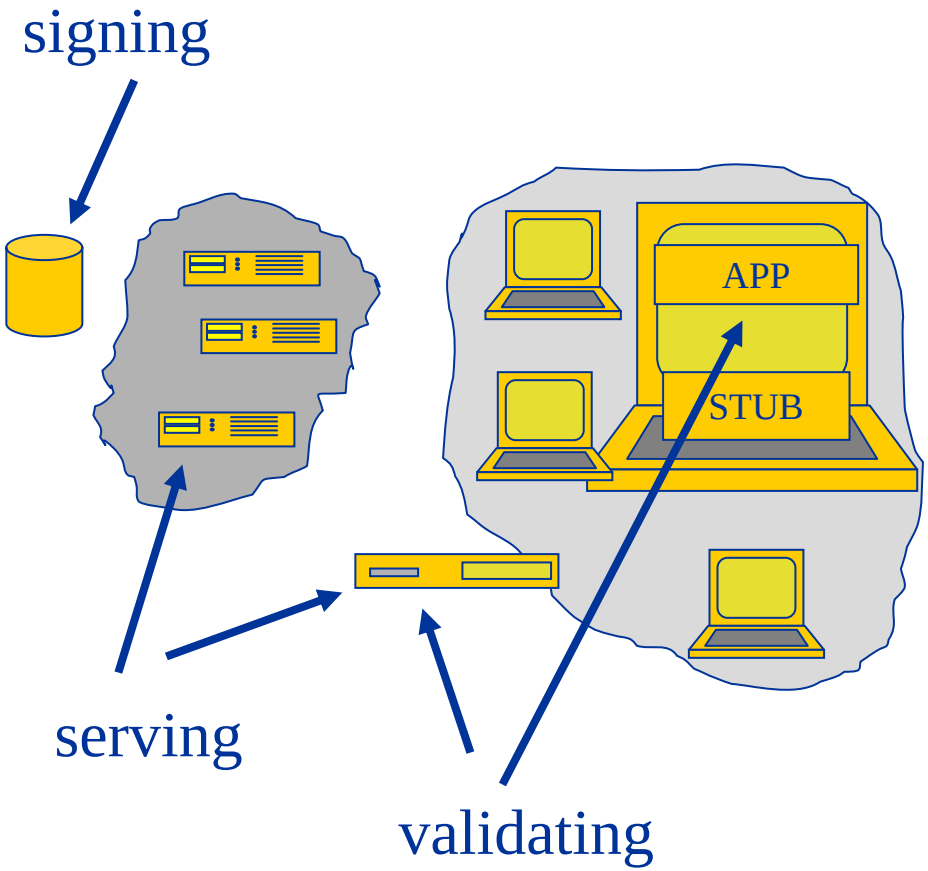
Confused?


Web Site Certified by an Unknown Authority
Unable to verify the identity of bert.secret-wg.org as a trusted site.
Possible reasons for this error
- Your browser does not recog
- The site's certificate is incom
- You are connected to a site
confidential information.
Please notify the site's webma
Before accepting this certifica
willing to to accept this certific
bert.secret-wg.org?
Examine Certificate...
Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
company you have
to determine whether
matching the name
Certificate
Warning - Security
Do you want to accept the certificate from web site "www.p3.postbank.nl" for the purpose of exchanging encrypted information?
Publisher authenticity verified by: "VeriSign, Inc."
The security certificate was issued by a company that is not trusted.
The security certificate has not expired and is still valid.
Caution: "www.p3.postbank
accept this content if you tru
Yes
Security Alert
Information you exchange with thi
changed by others. However, the
security certificate.
The security certificate was
not chosen to trust. View the
you want to trust the certifyi
The security certificate date is valid.
The security certificate has a valid name matching the name of the page you are trying to view.
Do you want to proceed?
Yes
No
View Certificate
Certificate signer not found
The server's certificate chain is incomplete, and the signer(s) are not registered. Accept?
bert.secret-wg.org
View
- The certificate for "bert.secret-wg.org" is signed by the unknown Certificate Authority "Secret WG Certificate Authority". It is not possible to verify that this is a valid certificate
Accept
Install
Cancel
Help

How does DNSSEC come into the picture

- DNSSEC secures the name to address mapping
  - Digital signatures
  - Without the need for certificates
- DNSSEC provides an “independent” trust path.
  - The person administering “https” is most probably a different from person from the one for “DNSSEC”
  - The chains of trust are most probably different
  - See acmqueue.org article: “Is Hierarchical Public-Key Certification the Next Target for Hackers?”

DNSSEC is ready to be deployed



Protocol spec is clear on:

- Signing
- Serving
- Validating

Implemented in

- Signer
- Authoritative servers
- Security aware recursive nameservers

DNSSEC deployment

- DNSSEC development
  - Protocols were finished this spring
  - Implementations and tools exist
- DNSSEC can be deployed today
  - Start at your site
  - Incremental deployment was a design feature
  - No flag dates are needed
- DNSSEC is new technology
  - Tools have some rough edges
  - Lack of experience

NCC Contribution

- Protocol development
- Development of tools

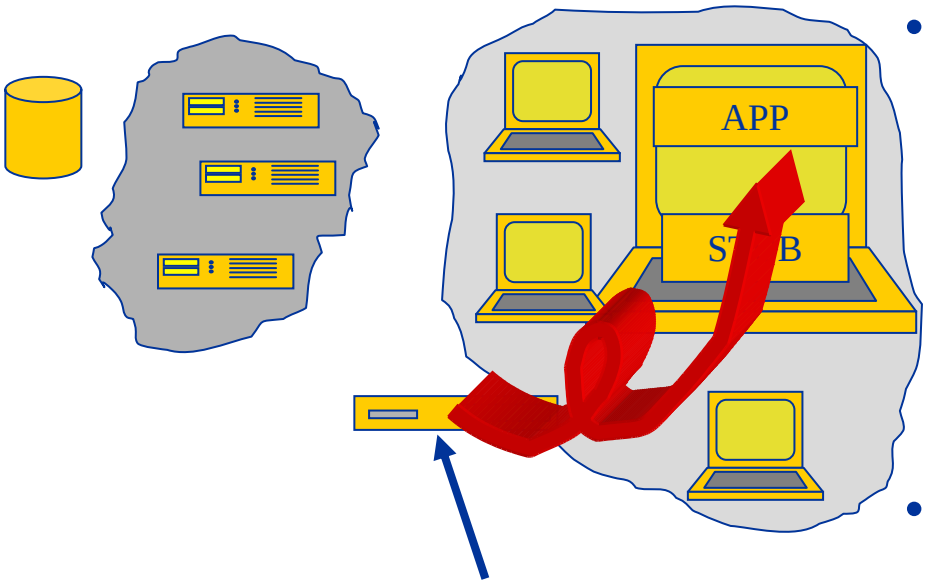
- Training, community awareness
  - DNSSEC howto

- Deployment on reverse tree
  - Expected Q3/2005

Outstanding issues

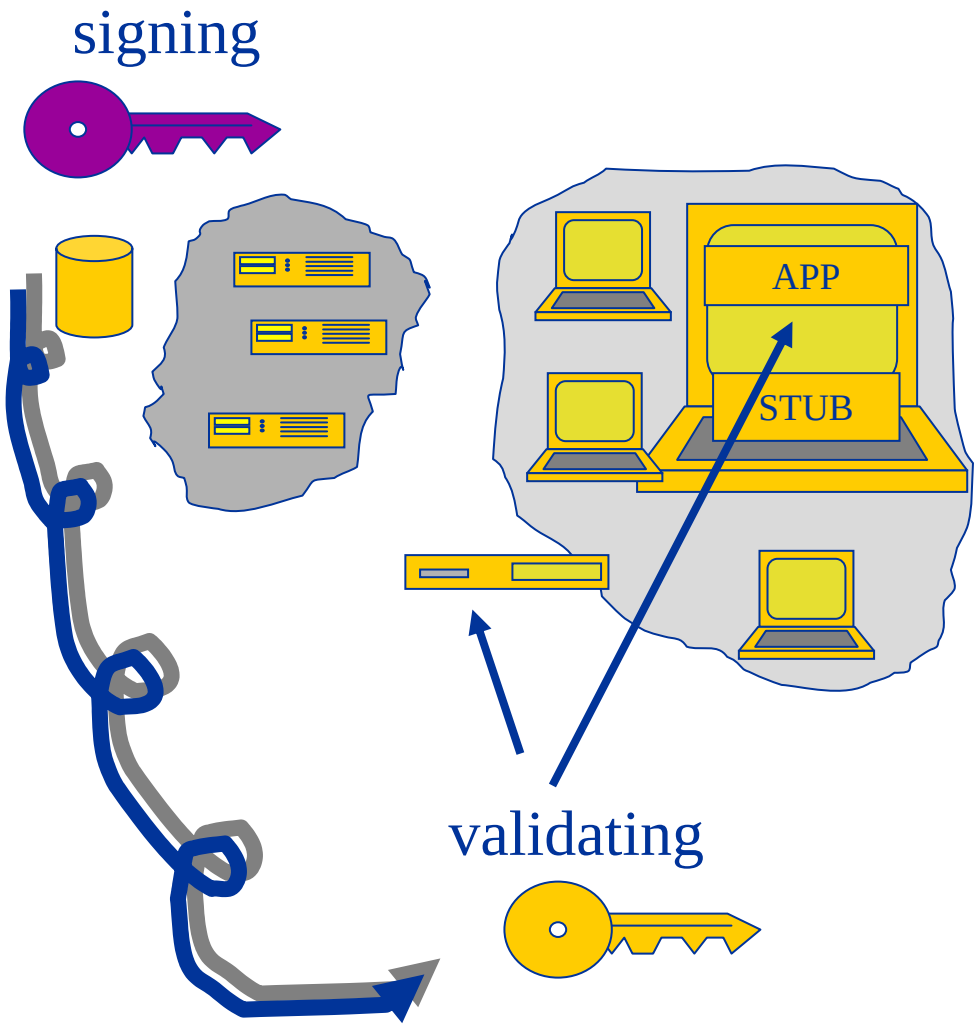
- “the last mile”
- Key management and key distribution
- NSEC walk

The last mile



- How to get validation results back to the user
- The user may want to make different decisions based on the validation result
  - Not secured
  - Time out
  - Crypto failure
  - Query failure
- From the recursive resolver to the stub resolver to the Application
- Expected to solve itself as soon as the infrastructure is there

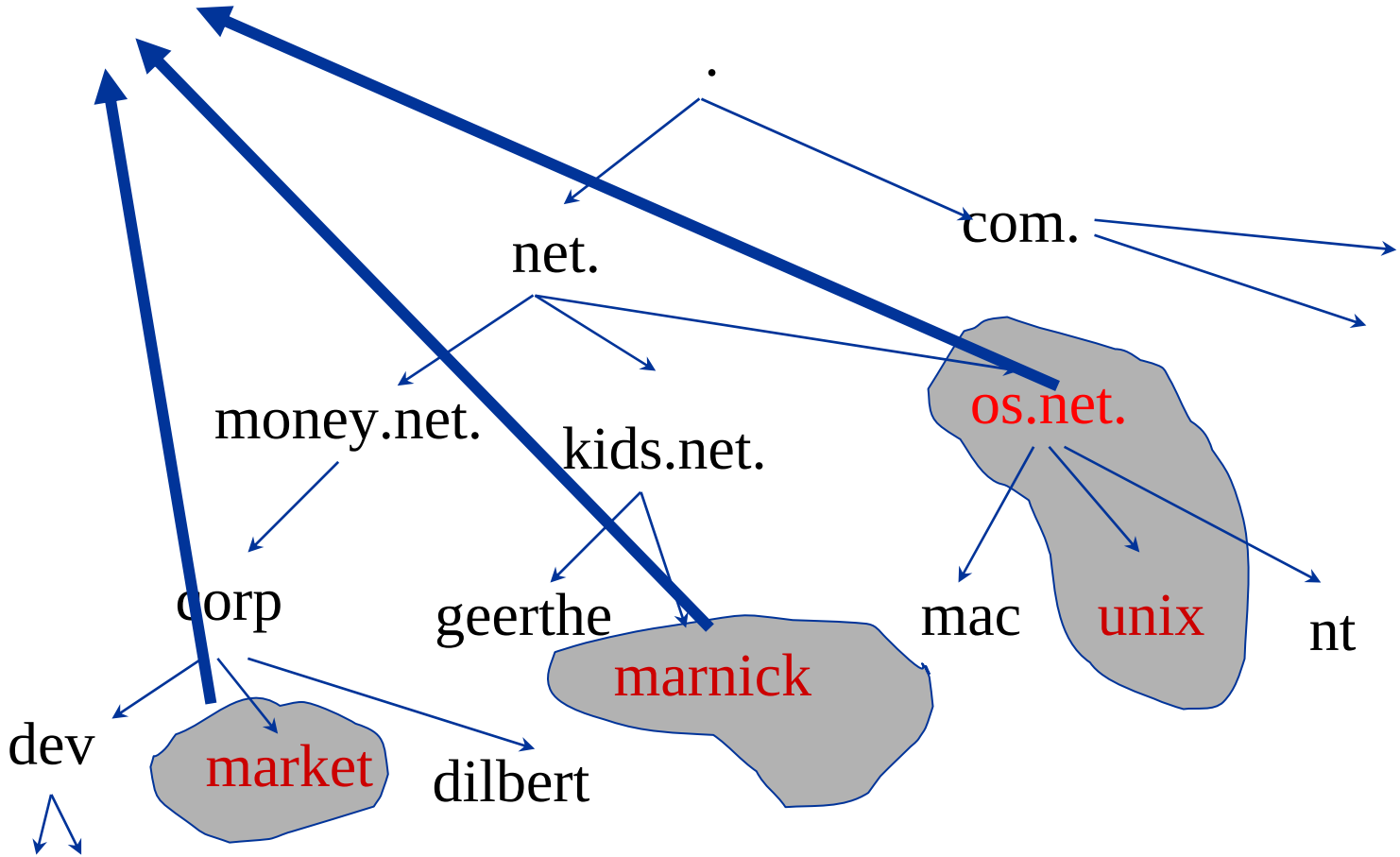
Problem Area



Key Management

- Keys need to propagate from the signer to the validating entity
- The validating entity will need to “trust” the key to “trust” the signature.
- Possibly many islands of security

Secure Islands and key management



Secure Islands

- Server Side
  - Different key management policies for all these islands
  - Different rollover mechanisms and frequencies

- Client Side
  (Clients with a few to 10, 100 or more trust-anchors)
  - How to keep the configured trust anchors in sync with the rollover
  - Bootstrapping the trust relation

NSEC walk

- A record to prove that something does not exist
  - @foo.com
    - a.foo.com
    - n.foo.com
    - o.foo.com
- Nsec record says that there are no other hosts
  - @foo.com
    - a.foo.com nsec n.foo.com
    - n.foo.com
    - o.foo.com nsec @

NSEC walk

- This gives information about the zone
- Policy and privacy issues
- Work starting to study possible solutions
  - Requirements are gathered
  - If and when a solution is developed it will be co-existing with DNSSEC-BIS !!!
  - Until then on-line keys will do the trick.

Agenda

- RIPE and the RIPE NCC
- DNS related areas where we are active
- Conclusions

Conclusions

- RIPE NCC is a service organization for ISP's
- DNS related services include
  - K root
  - DNSMON: Monitoring of root and TLD servers
  - DNSSEC: Security for DNS

Further reading: Kroot

- Operations: www.root-servers.org
- Analysis: www.caida.org/projects/dns-analysis
- Anycast:
  - RFC 1546 and RFC 3258
  - http://www.ietf.org/rfcXXXX.txt
- K root anycasting
  - RIPE document RIPE268
  - http://www.ripe.net/ripe/docs
- Contact: k-anycast@ripe.net

Further reading: DNSMON

- Sites:
  - http://dnsmon.ripe.net: DNSMON site
  - http://www.ripe.net/ttm: TTM site
- Documentation (http://www.ripe.net/ripe/docs):
  - RIPE324: DNSMON for TLD Administrators
  - RIPE297: TTM/DNSMON service for LIR's
  - TTM Glossy
- Email:
  - ttm@ripe.net

Further reading: DNSSEC

- Some links
  - http://www.dnssec.net
  - http://www.ripe.net/disi/dnssec_howto
- "Is Hierarchical Public-Key Certification the Next Target for Hackers" can be found at:
  http://www.acmqueue.org/modules.php?name=Content&pa=showpage&pid=181
- Contact: disi@ripe.net

Questions, Discussion