The IETF standards process
&
DNSSEC

Two separate topics mingled into one keynote

Olaf M. Kolkman

MENOG 2007, Doha Qatar

Who am I

- Director of NLnet Labs, a foundation performing R&D on open source and open standards
  - DNS is one of our areas of interest: NSD, DNSSEC, participation in standards process
- Chair of the Internet Architecture Board
  - This presentation is on personal title, I am not representing the IETF and/or IAB.

The IETF

- Internet Engineering Task Force
- Standard body for Internet technology
- Formed in 1986

The IETF's Mission

The goal of the IETF is to make the Internet work better.

The mission of the IETF is to produce high quality, relevant technical and engineering documents that influence the way people design, use, and manage the Internet in such a way as to make the Internet work better. These documents include protocol standards, best current practices, and informational documents of various kinds.

RFC3935

IETF “Standards”

- standards only when people use them
  - formal SDOs can create legally mandated standards
- IETF standards are freely available for anybody to implement*
- “*We reject kings, presidents and voting. We believe in rough consensus and running code*” (Dave Clark)
  - Technical competence is the only requirement for contributing
  - Contributions are on personal title, not on behalf of companies, organizations, or governements

* caveat: IPR encumbered technology

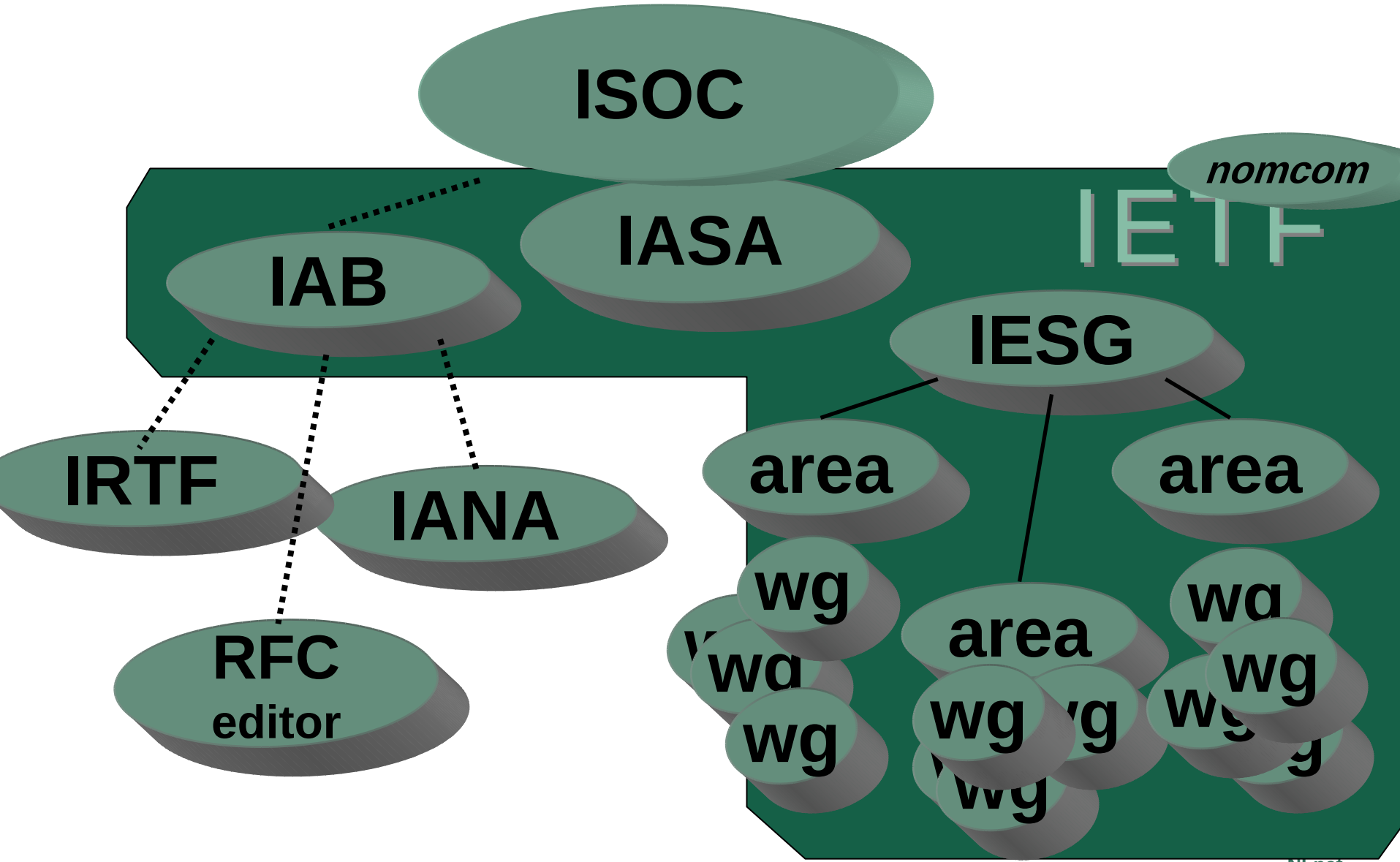
The Role & Scope of the IETF

- “above the wire and below the application”
  - IP, TCP, email, routing, IPsec, HTTP, FTP, ssh, LDAP,
  - SIP, mobile IP, ppp, RADIUS, Kerberos, secure email,
  - streaming video & audio, ...
- but wires are getting fuzzy
  - MPLS, GMPLS, pwe3, VPN, ...
- generally hard to clearly define IETF scope
  - constant exploration of edges

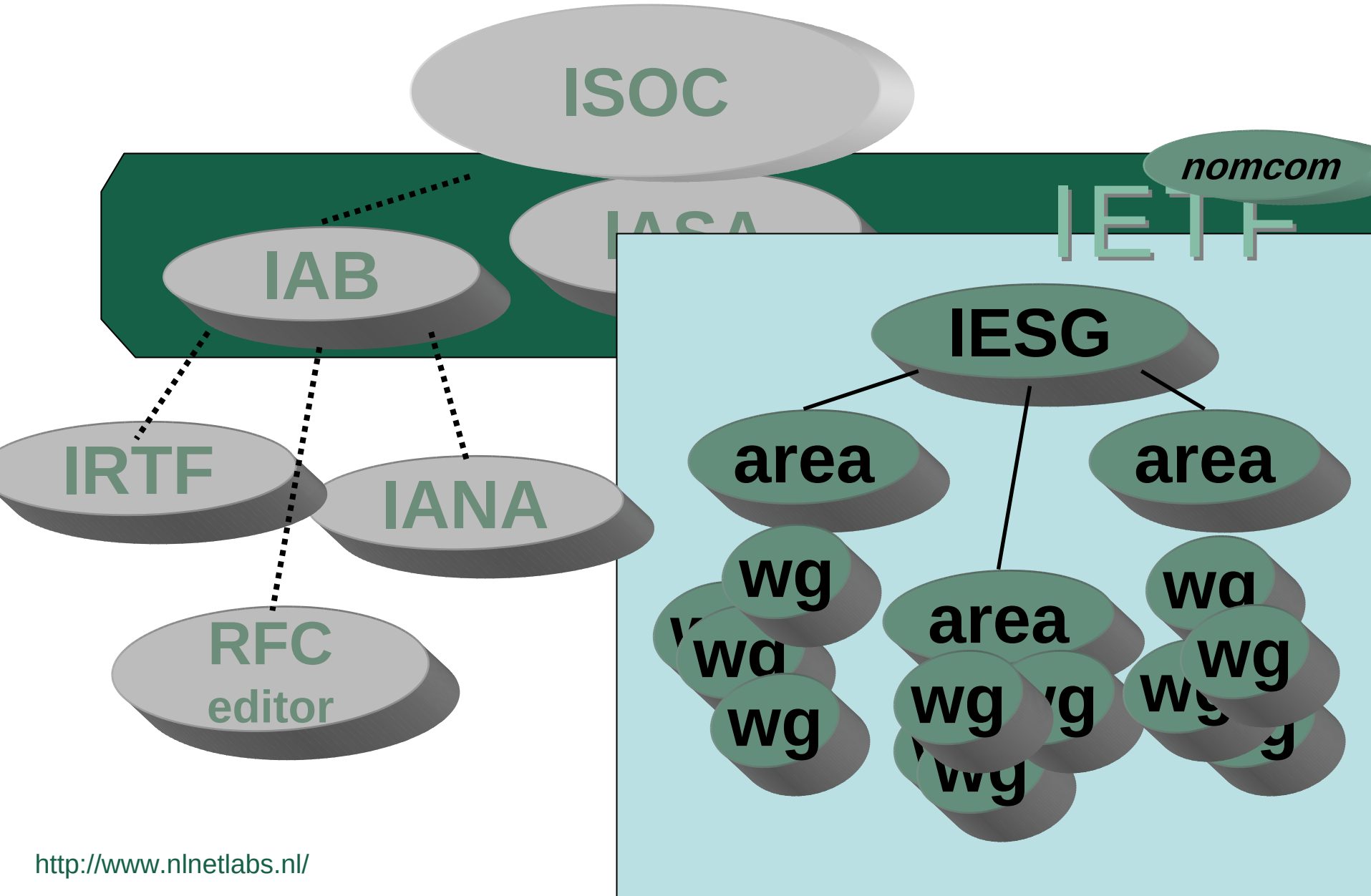
Overview of the IETF

- The IETF is not a formal entity; “It does not exist”
- There are no members and there is no voting
- Between 1200 and 2000 people that meet 3 times per year
- Many more that do work on mailing list
- Work takes place in an organized fashion

Top Level View of Organization



Top Level View of Organization



IETF Areas

- General Area (gen) (1 WGs)
- Applications (app) (14 WGs)
- Internet (int) (30 WGs)
- Operations & Management (ops) (16 WGs)
- Routing (rtg) (15 WGs)
- Security (sec) (17 WGs)
- Real-time Applications (rai) (16 WGs)
- Transport (TSV) (13 WG)

IESG

- Internet Engineering Steering Group
- ADs + IETF Chair
- process management and RFC approval body
- approves WG creation
- provides technical review & approves publication of IETF documents
  - reviews and comments on non-IETF submissions
- multi-disciplinary technical review group

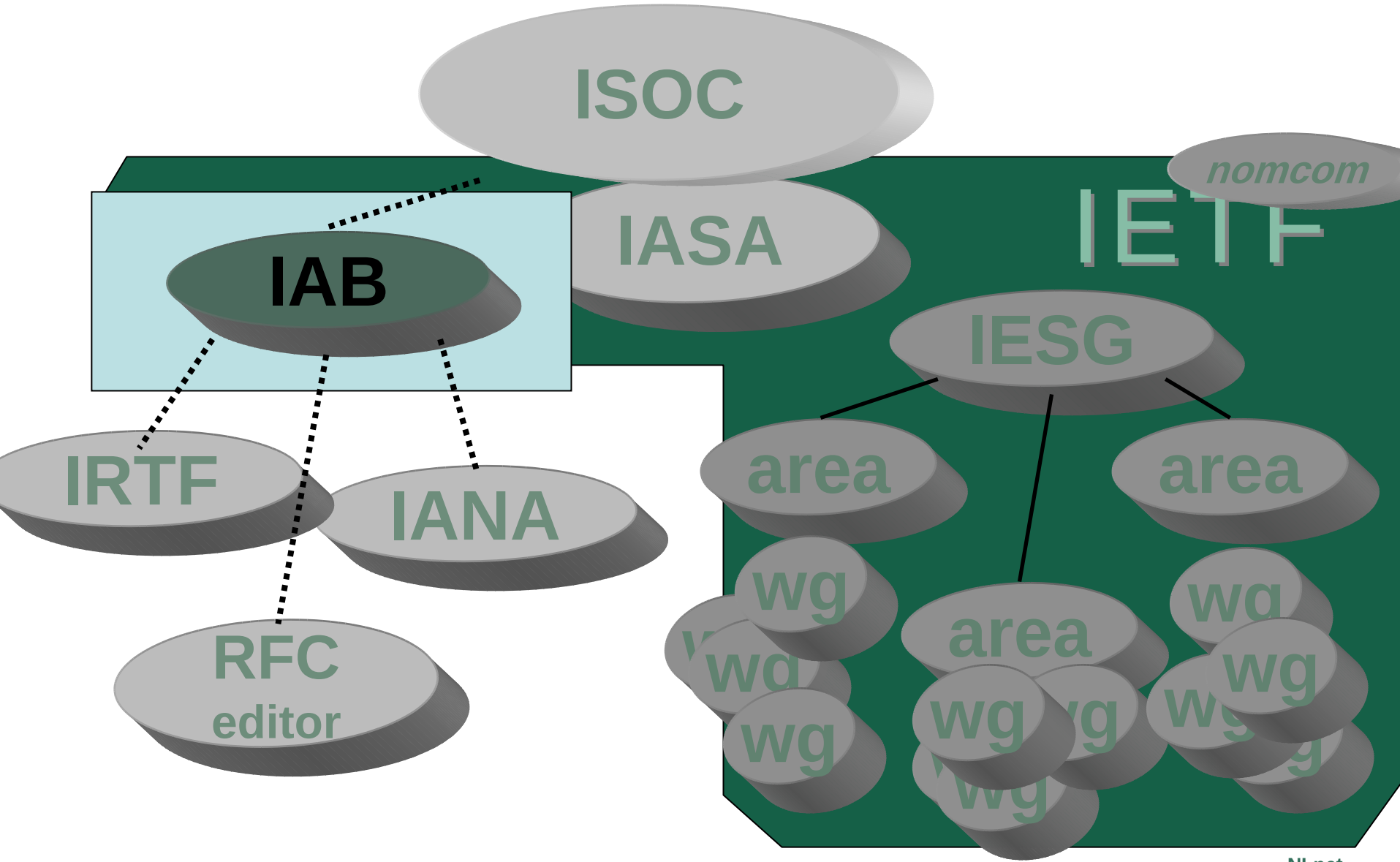
Working Groups

- this is where the IETF primarily get its work done
  - on mailing list
  - face-to-face meetings focused on key issues (ideally)
  - note: face-to-face meetings generally very short
- working group focused by charter agreed between chair and area director
  - restrictive charters with milestones
  - working groups closed when their work is done
- charter approved by IESG with IAB advice
- AD with IESG has final say on charter

Working Groups. contd.

- no defined membership
  - just participants
- “Rough consensus and running code...”
  - no formal voting
  - can do show of hands or hum - but no count
  - does not require unanimity
  - disputes resolved by discussion
  - mailing list and face-to-face meetings
  - final decisions must be verified on mailing list
  - taking into account face-to-face discussion

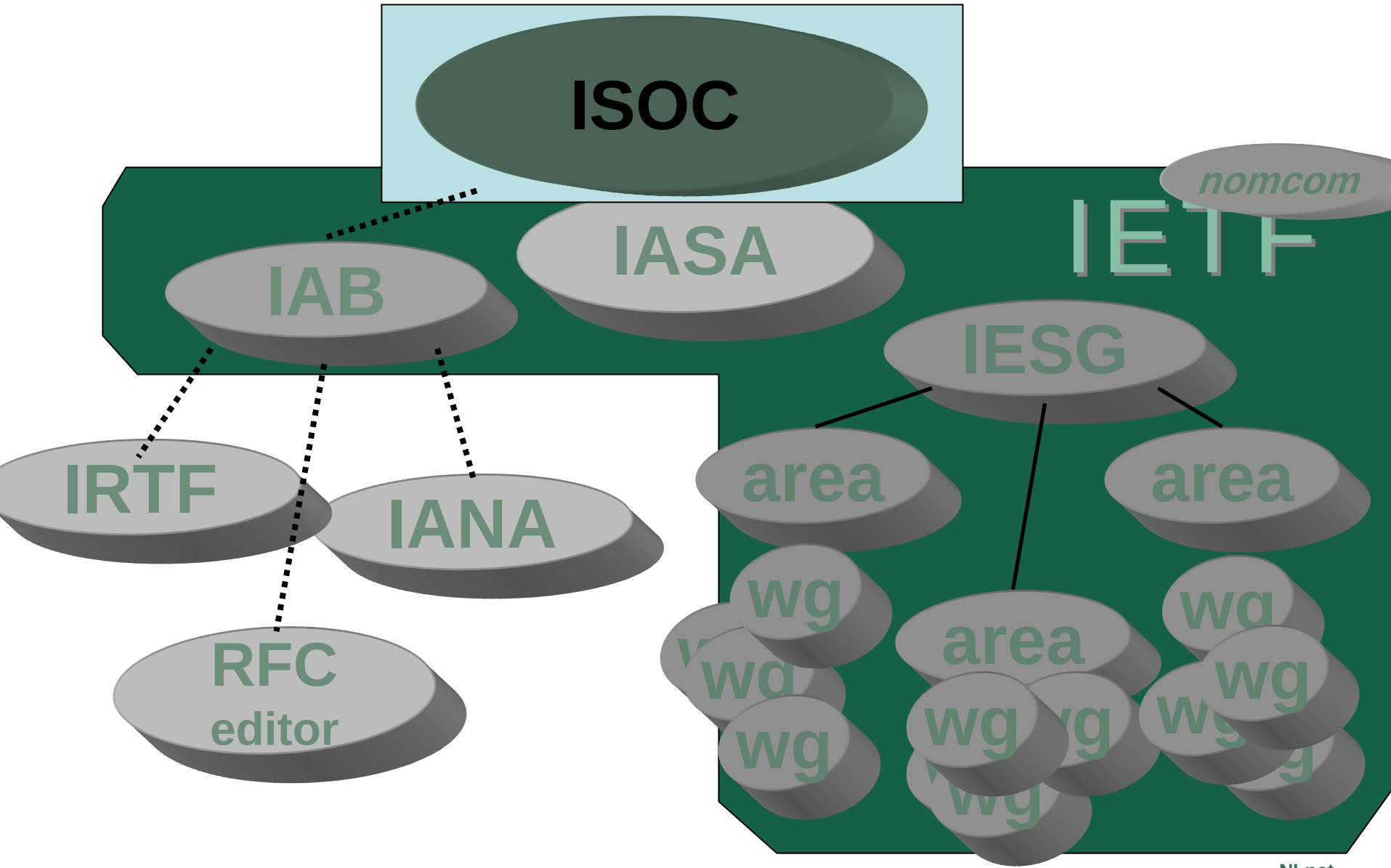
Top Level View of Organization



Internet Architecture Board (IAB)

- provides overall architectural advice
  - to IESG, IETF & ISOC
  - hosts workshops (sometimes)
- deals with IETF external liaisons
- advises on establishment of IRTF & IETF working groups
- appoints IRTF chair
- approves IETF-IANA
- oversees RFC Editor function

Top Level View of Organization



The Internet Society (ISOC)

- non-profit, non-governmental, international, professional membership organization
  - 100 organizational and 20,000 individual members in over 180 nations
- organizational and administrative home for IETF
  - legal umbrella, insurance, IASA home, etc
- ISOC BoT part of appeal chain
- ISOC president appoints chair of nomcom
- IAB chartered by ISOC
- ISOC president is on the IAB list & calls
- IETF (through IAB) appoints 3 ISOC trustees
  - join at www.isoc.org
- Publishers of …..

IETF

IETF Journal

IETF 69 • Chicago
October 2007
Volume 3, Issue 2

Published by the Internet Society in cooperation with the Internet Engineering Task Force

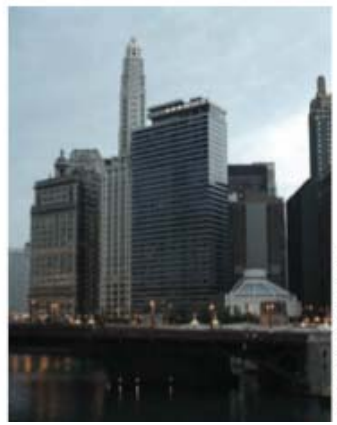
Inside this issue

IPv6 Captures the Spotlight at IETF 69

From the Editor's Desk, by Mirjam Kühne

If it were possible to assign a theme to the IETF 69 meeting in Chicago last July, the obvious choice would be IPv6. Now that IPv6 has become an integral part of the community, as evidenced by the number of working groups that are connected to it, it is the actual deployment of IPv6 that is capturing the attention of the IETF.

A good place to start is the summary of a special meeting that took place at IETF 69 with the IESG and the IAB (see below). The purpose of the meeting was to find out what the IETF can do to help with the deployment of IPv6. Similarly, Shane Kerr takes a look at the historical development of IPv6 in an effort to determine if opportunities were missed then and, if so, whether they might offer useful lessons on the deployment issues we face now. (See page 9.)

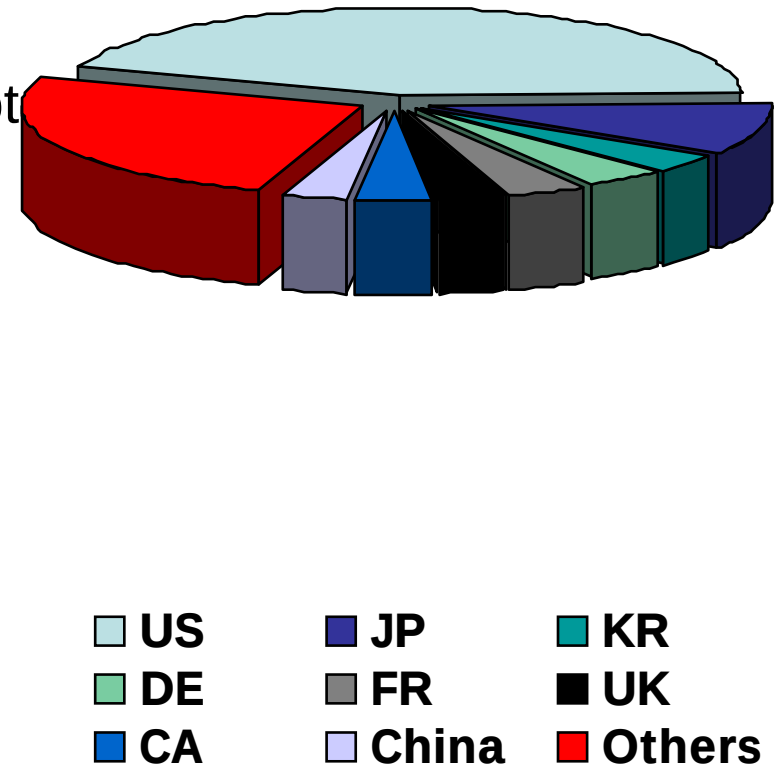


Alexandru Petrescu

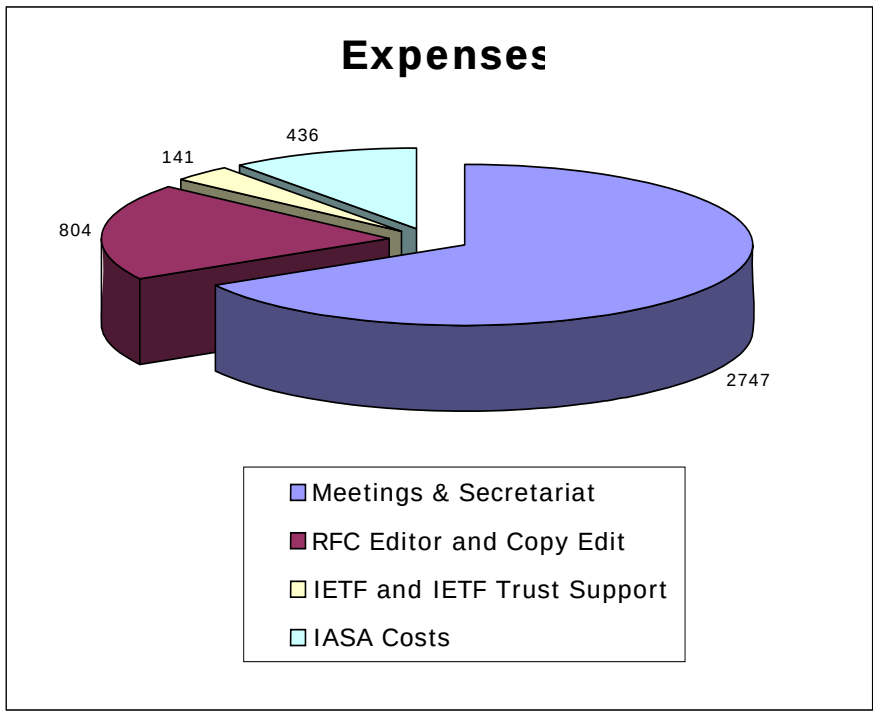
One topic that frequently comes up in discussions of IPv6

IETF69 Participants

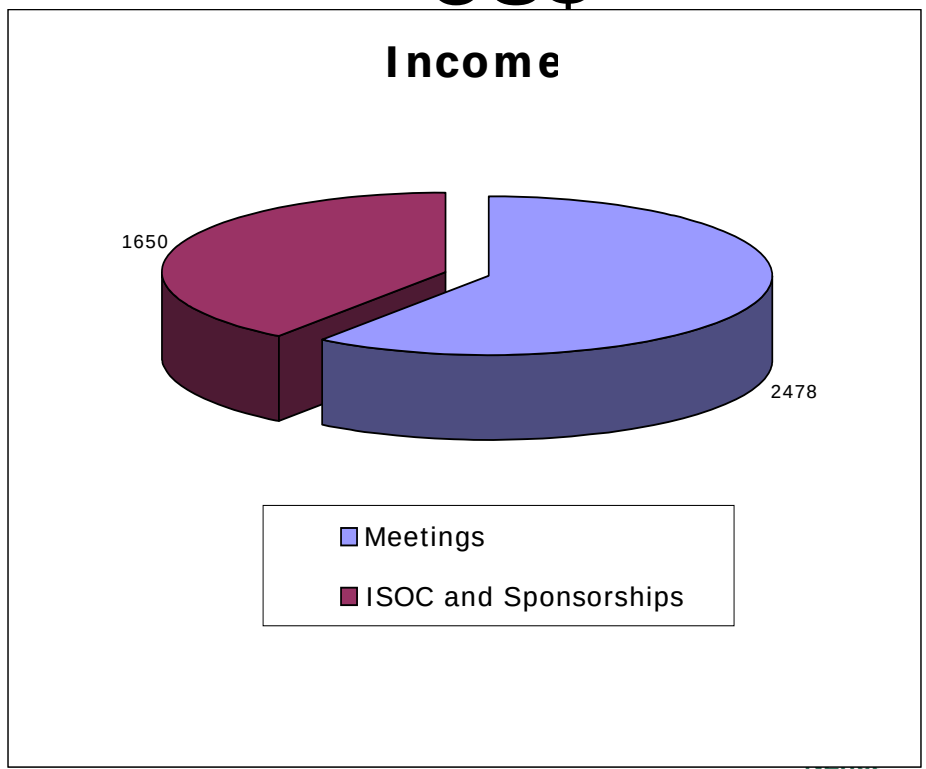
- 1146 people
  - IETF66 - Montreal: 1236 tot
- 40 countries
  - IETF66 - Montreal: 44



Sustaining the Organization



2007 budget 4,128 k US$



How about those Standards?

- RFC is a “Request for Comments”
- Multiple flavors:
  - Standards Track RFC
    - Proposed, Draft and Full standards
    - Best Current Practices
  - Informational RFCs

What is a RFC?

- RFC used to stand for Request for Comments
  - now just a (brand) name
  - tend to be more formal documents than early RFCs
- IETF document publication series
- RFC 1 Host Software - Apr 7 1969
- now over 5000 RFCs
- not all RFCs are standards!
  - see RFC 1796
  - though some vendors imply otherwise
- many types of RFCs

RFC Repository Contains:

- standards track
  - OSPF, IPv6, IPsec ...
- obsolete Standards
  - RIPv1
- requirements
  - Host Requirements
- policies
  - Classless InterDomain
  - Routing
- april fool's day jokes
  - IP on Avian Carriers ...
  - ... updated for QoS
- poetry
  - 'Twas the night before startup
- white papers
  - On packet switches with infinite storage
- corporate documentation
  - Ascend multilink protocol (mp+)
- experimental history
  - Netblt
- process documents
  - IETF Standards Process

Standards Track RFCs:

- Best Current Practices (BCP)
  - policies or procedures (best way we know how)
- 3-stage standards track
  - Proposed Standard (PS)
  - good idea, no known problems
  - Draft Standard (DS)
  - stable
  - multiple interoperable implementations
  - note: interoperability not conformance
  - Internet Standard (STD)
  - wide use

Other RFC Types

- Informational
- Experimental
- Historical

Concluding

- IETF's Goal: to make the Internet work Better
- Open to participation by all
  - Only takes subscription to a mailing list and technical expertise
  - '*Rough consensus and running code*'
- Not all RFCs are standards

DNSSEC
as a case study of
protocol development problems

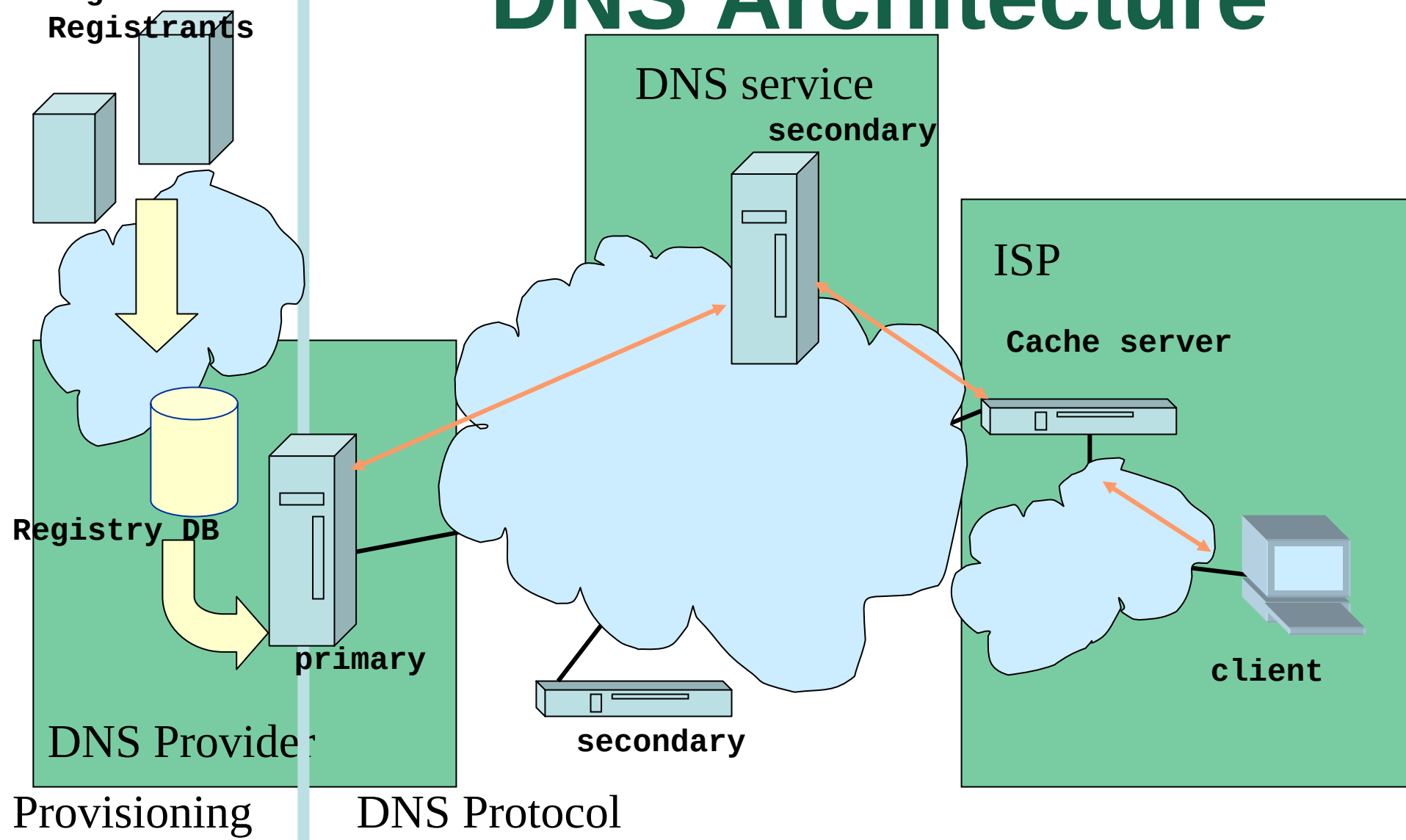
- Why adding security later is difficult.
- Why running code and rough consensus
- Why security, protocol and operator presence is important (cross area review).
- Changing requirements

Realization of a problem

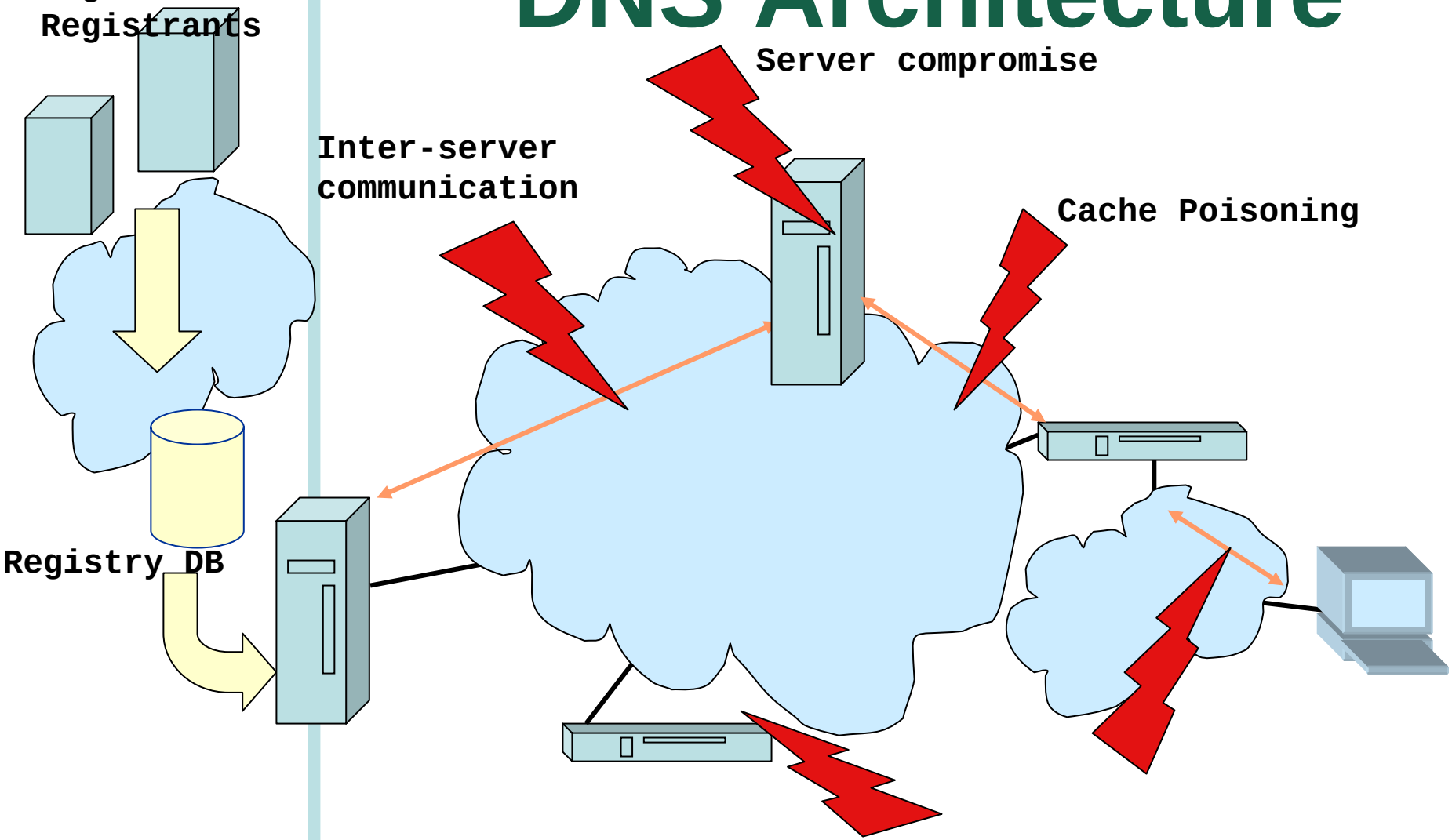
- DNS
  - 1st implementation (Jeeves) by Paul Mockapetris in 1983 (RFC 882/883)
  - The current Full Standard published in 1986 (RFC 1034/1035)
  - Steve Bellovin discovers major flaw in 1990, publishes in 1995
    - http://www.cs.columbia.edu/~smb/papers/dnshack.ps
- Research started on DNSSEC in the 1990-1995 timeframe

So what is the problem?

DNS Architecture

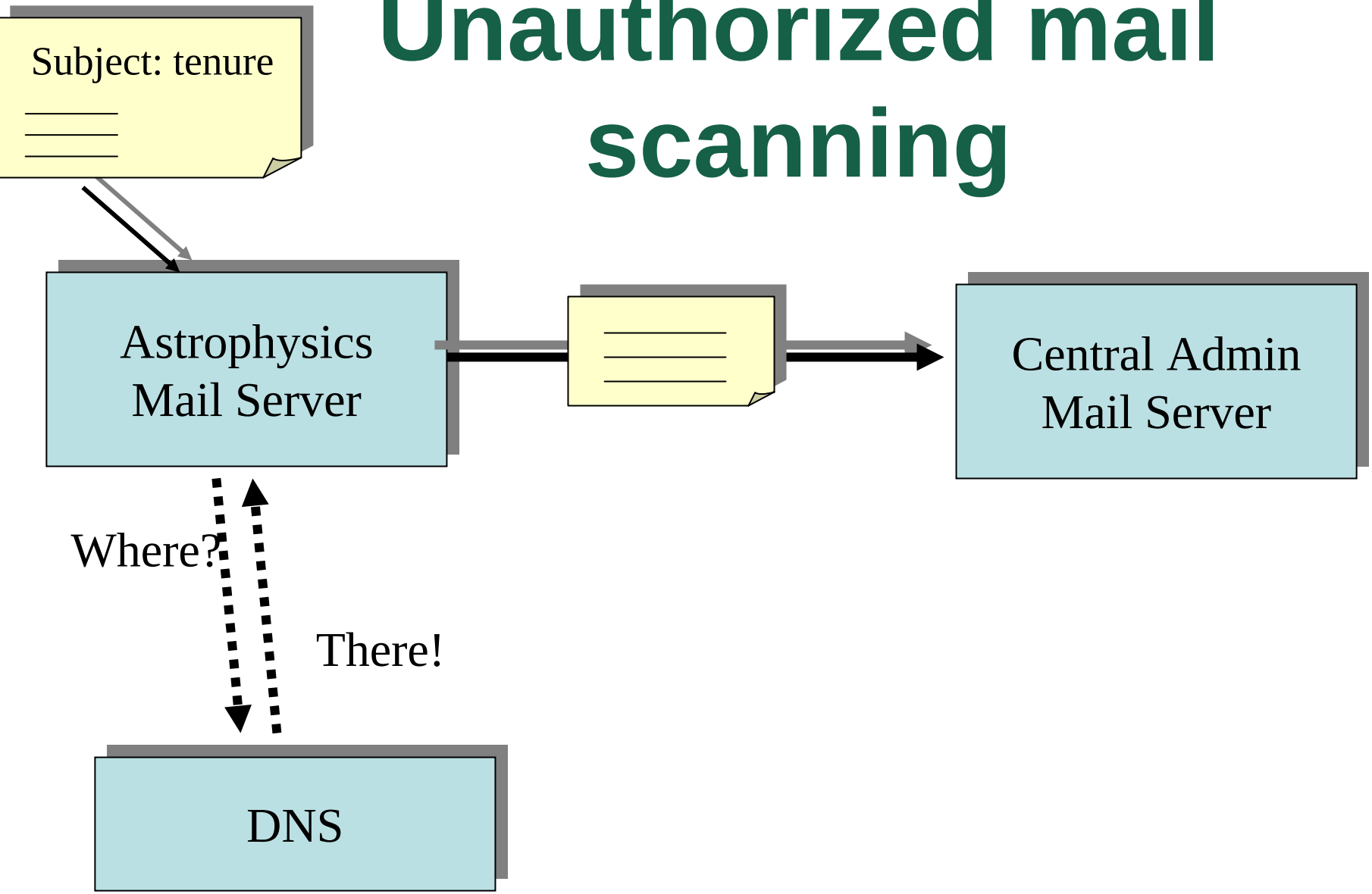


DNS Architecture

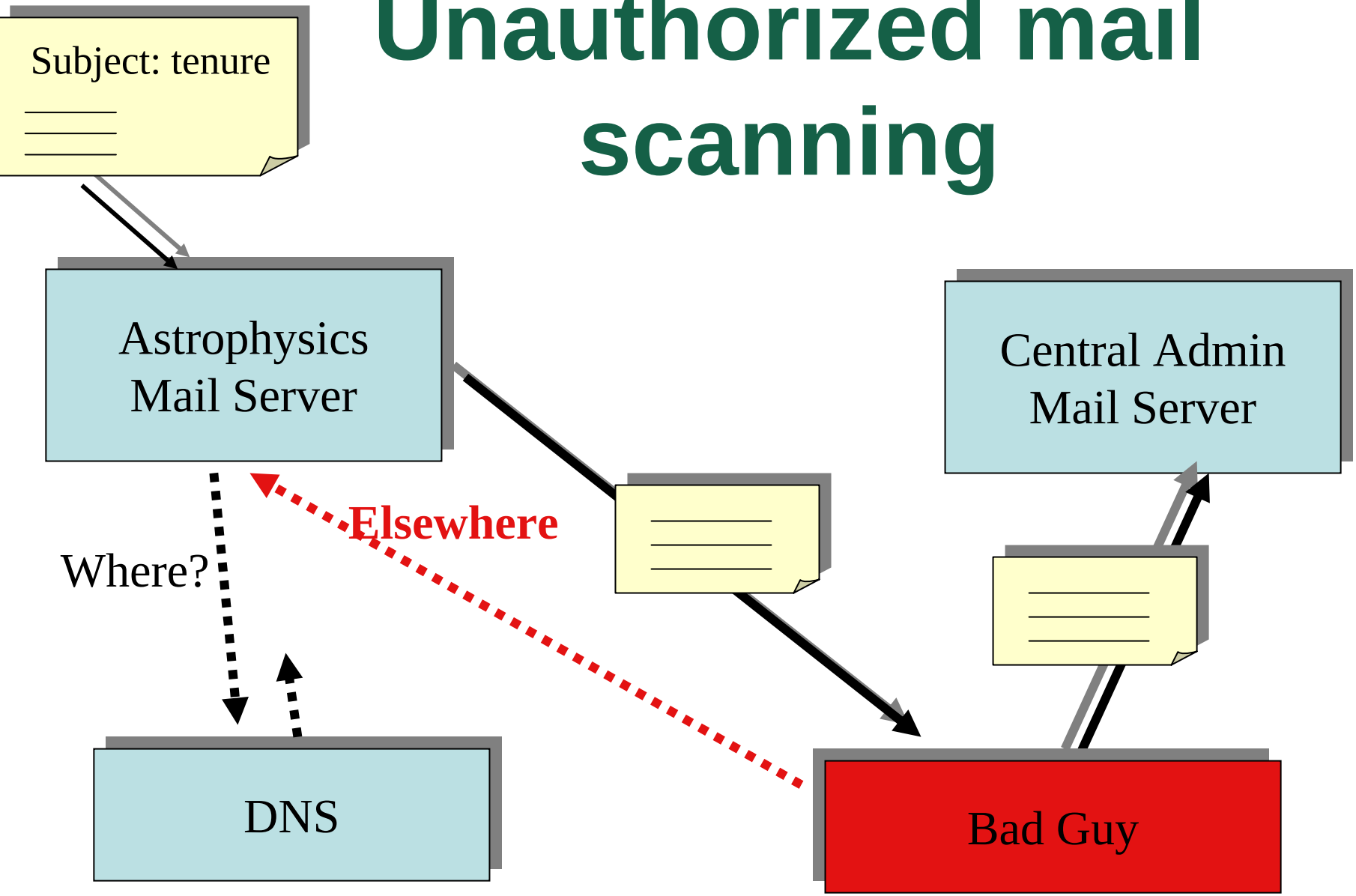


Provisioning DNS Protocol

Example: Unauthorized mail scanning



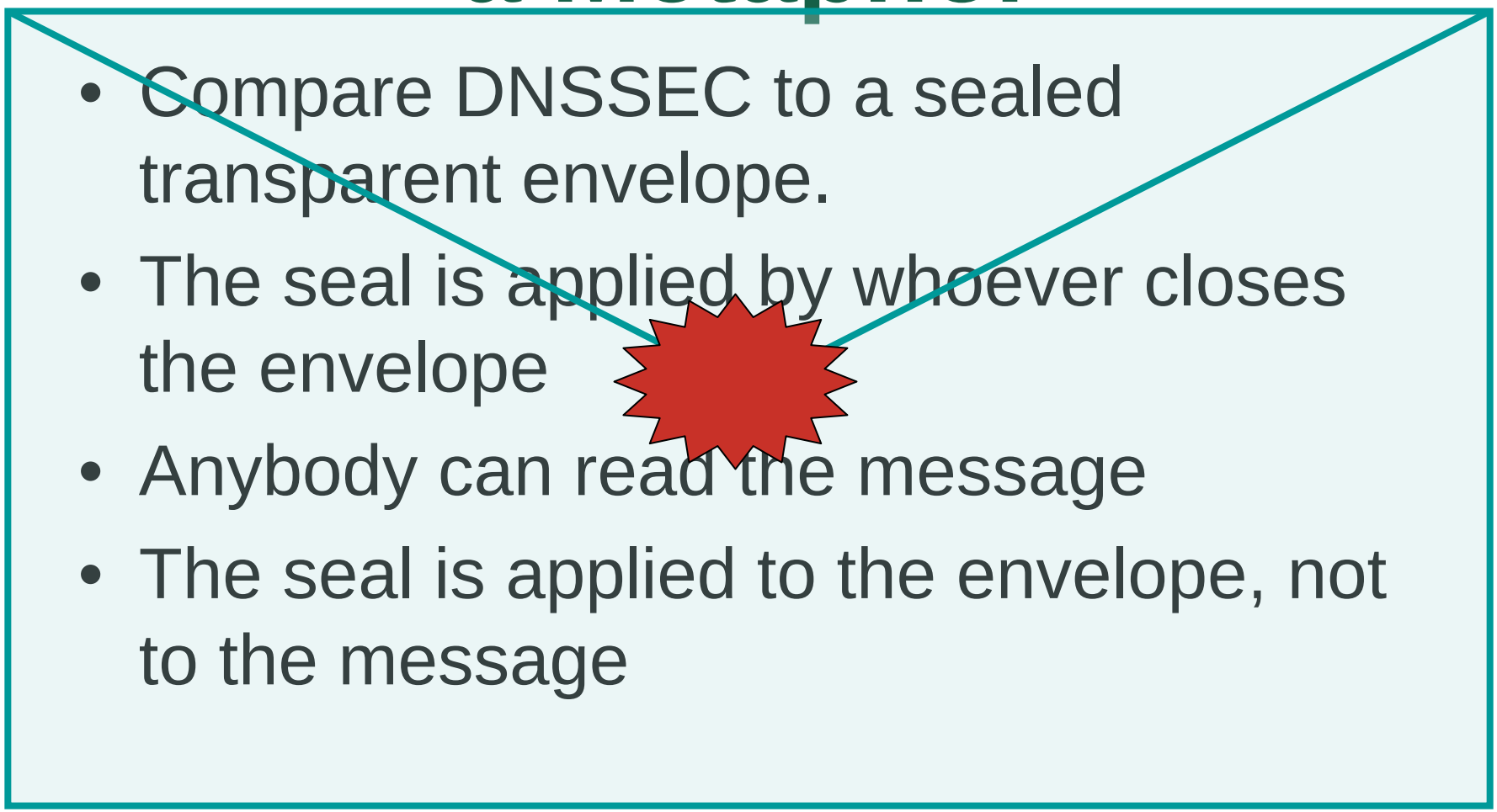
Example: Unauthorized mail scanning



Where Does DNSSEC Come In?

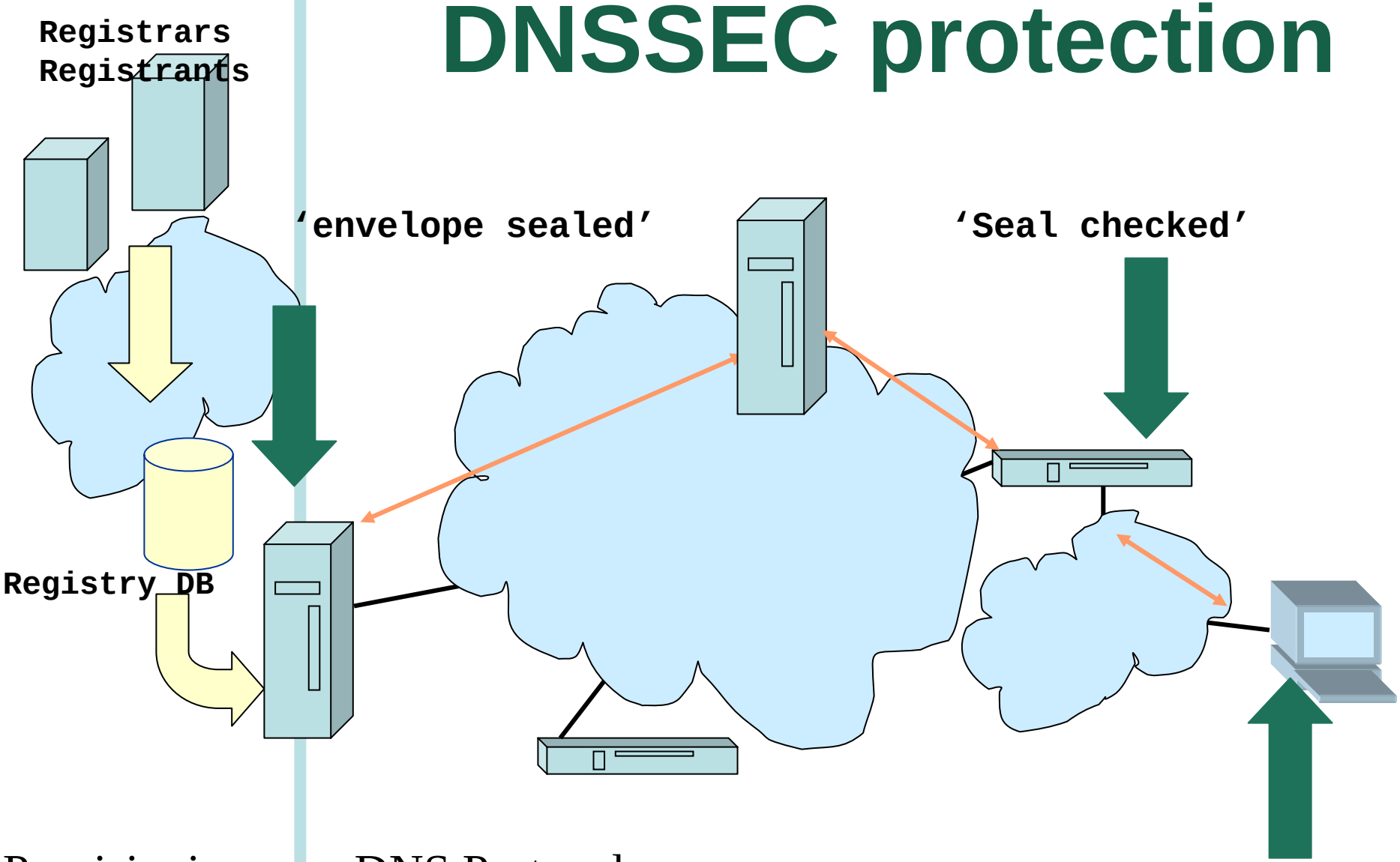
- DNSSEC secures the name to resource record mapping
  - T[illegible]ers

Solution
a Metaphor



- Compare DNSSEC to a sealed transparent envelope.
- The seal is applied by whoever closes the envelope
- Anybody can read the message
- The seal is applied to the envelope, not to the message

DNSSEC protection



Provisioning DNS Protocol

DNSSEC history the first phase

- **1993**
  - First “BOF” on DNSSEC during the IETF 28 in Houston, TX.
- **1994**
  - DNS Security Working Group chartered
- **1997**
  - RFC2065, a predecessor of RFC 2535, is published.

The first 4 years

- DNSSEC was being developed by security specialists rather than DNS experts
- Some implicit requirements were taken into account
  - No documentation of the actual thread discussion
- Advanced DNS features not incorporated
  - Dynamic updates only partly done in RFC2065

DNSSEC history the second phase

- **1999**
  - RFC2535 is published by the IETF. The DNSSEC protocol looks to be finally finished. BIND9 is developed to be the first DNSSEC capable implementation.
- **2000**
  - DNSEXT group established
  - First groups implementing DNSSEC

Another 4 year

- Refining of the specifications
- Getting cross area review
- Moving from prototype code to production code
- Interest from DNS operators
  - Operational experience of DNSSEC on larger scale: key-exchange between child and parent shown to be problematic
- Back to the drawing board after about 8 years after the problem was first recognized

DNSSEC history
The 3rd phase

- **2003-2005**
  - RFC 3655, RFC 3658, RFC 3755, RFC 3757 and RFC 3845: all incremental improvements
- **2004**
  - RFC 3833 “Thread Analysis of the Domain Name System”
- **March 2005**
  - RFC RFC 4033-4035, DNSSEC-bis published
  - One set of documents, stable and deployable

4 years for DNSSEC-bis

- 4 years of DNSSEC bis development
- DNSSEC bis is complete and extendable
- Rough consensus, running code and operator involvement
- However
  - New requirements brought to the table at a very late stage
  - Zone enumeration problematic for deployment for (some) European registries

DNSSEC history 4th cycle

- **2005 - 2007**
  - Authenticated denial of existence improvement
    - Within the DNSSEC-bis framework
    - Based on an old idea
  - Key management methodology
  - SHA1 vulnerability and its impact on DNSSEC
    - DNSSEC written with algorithm-agility in mind RFC4509

Zone walking

- Proof that nothing exist by declaring what the spans are in which nothing exists.
- There is no data between
  - A and C, C and P, P and Y, Y and A
  - So now you know the zone content: A, C, P, Y

```
twiki.secret-wg.org.  10  IN  NSEC  ( www.secret-wg.org.
                                      CNAME RRSIG NSEC )
```

4 years after DNSSEC-bis

- Development takes long, the protocol is complex
  - NSEC3 (the solution for zone walking) is almost through IESG
    - DNS and security specialists were both needed and present
  - Automatic Key rollover mechanism is standardized (RFC4989)
  - DLV has been published as informational (RFC 5074)
    - Not a standard

Take away

- IETF WG drives the work
  - Dependent on the folk who happen to be around
- Rough consensus and running code
  - Multiple workshops and production quality code were instrumental for the development of DNSSEC bis and helped consensus.
- Operational involvement needed, otherwise protocol development remains an academic exercise

DNSSEC deployment

- Hampered by ‘Chicken and Egg’ problem
  - No immediate perceived benefit (there are no applications that use DNSSEC yet)
  - Non-zero deployment costs at the server side
- Multiple implementations of DNSSEC code freely available
  - BIND and NSD for authoritative servers
  - BIND for recursive servers (Unbound expected Q1 2008).

Why the effort?

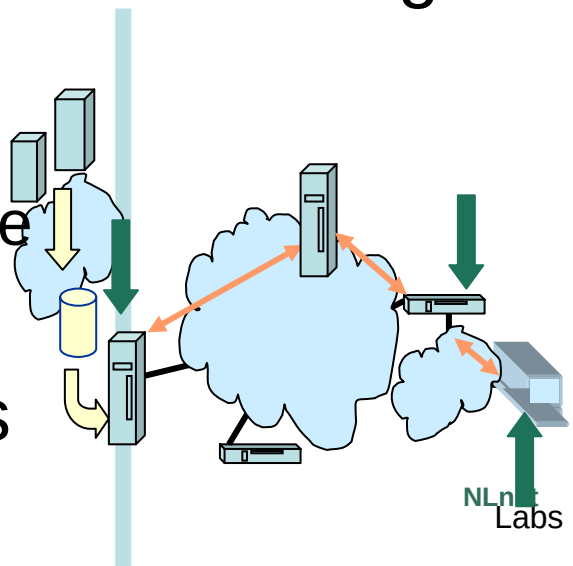
- DNS is a central piece of the Internet infrastructure
- Many applications expect the DNS to hand sensible answers

Deployment order

- DNSSEC deployment at the server side
  - 193.in-addr.arpa, &c, &c…
  - .SE, .BR, BG, e164.arpa (announced)
  - Root zone ?!?!?!
    - ns.iana.org
- DNSSEC in recursive nameservers validating the answers
  - ISPs in Sweden
  - Support for by current design space

…

- DNSSEC support in applications



What can you do?

- Sign your zone
  - NSEC3 is forward compatible, and not needed in many cases
  - TLDs can lead by example
- Implement validation on your recursive nameservers
- Share your experience!
  - MENOG is an excellent forum for that

Questions?

- www.dnssec-deployment.org
- www.dnssec.net
- http://www.nlnetlabs.nl/dnssec_howto/

Acknowledgments

- The IETF description slides came from Scott Bradner's newcommers meeting at IETF 63.
- DNSSEC history from James Galvin: DNS Security: a historical perspective

  IETF Journal, Vol2, Issue 2.