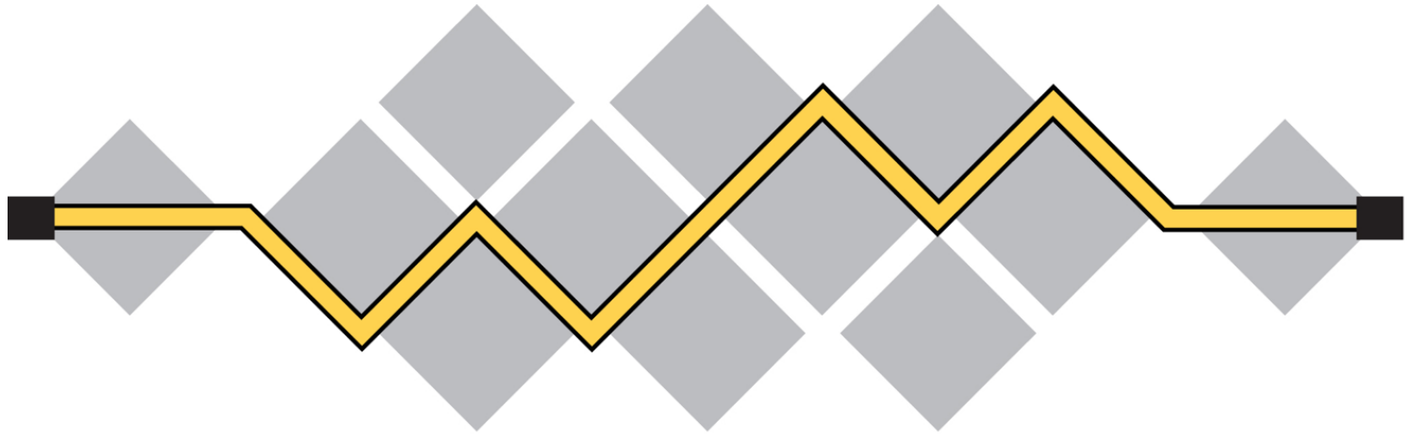


IETF®

Open Standards for an Open Internet

Olaf M. Kolkman

olaf@NLnetLabs.nl

OUTLINE

Open Internet

Open Standards

The IETF as a Open Standards Body

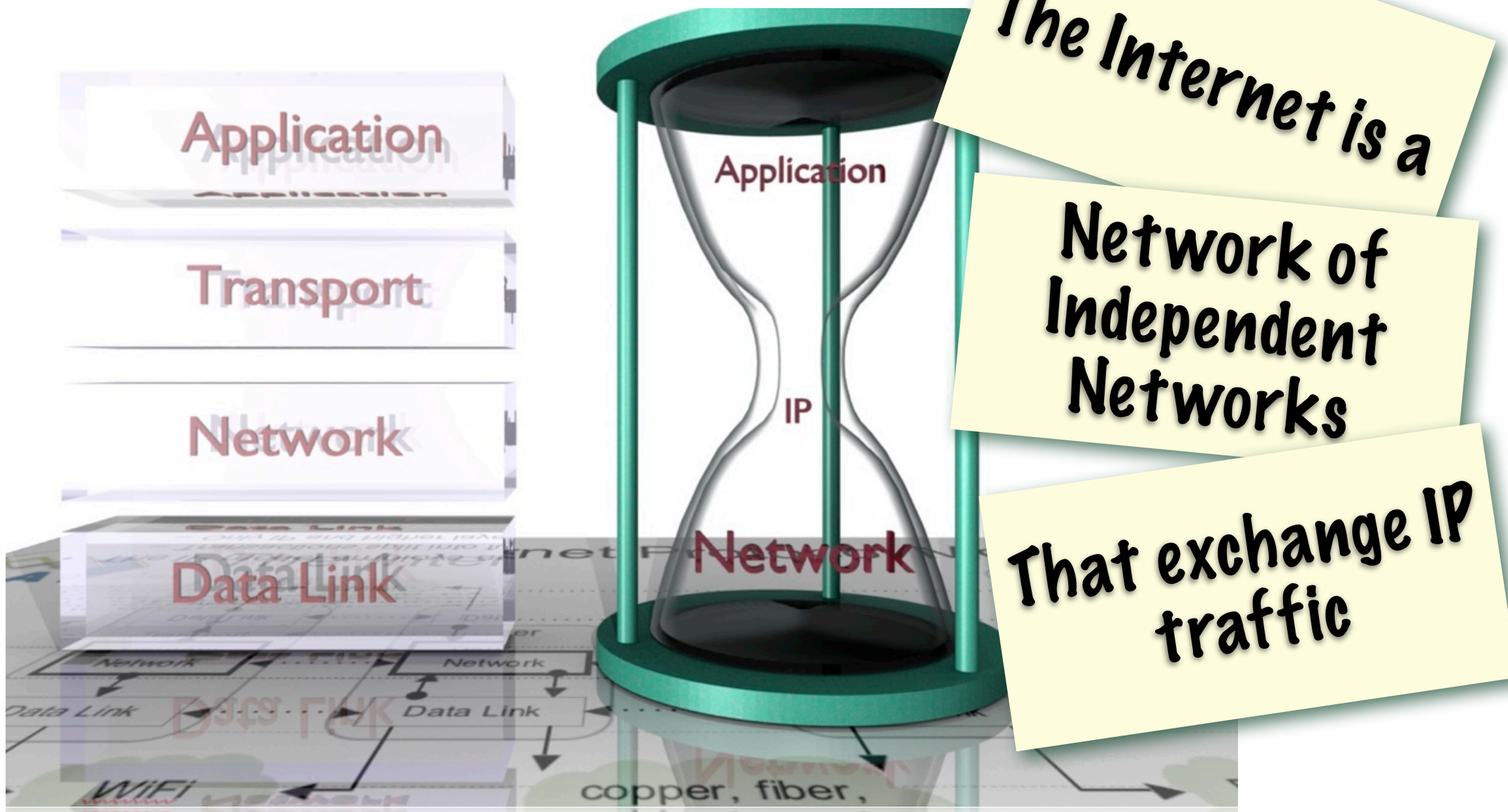
Org Chart

Working Methods

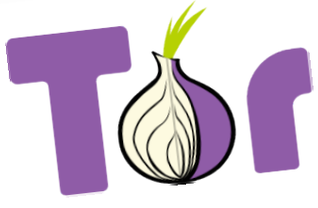
Participation

Work of Potential Interest

Open Internet?



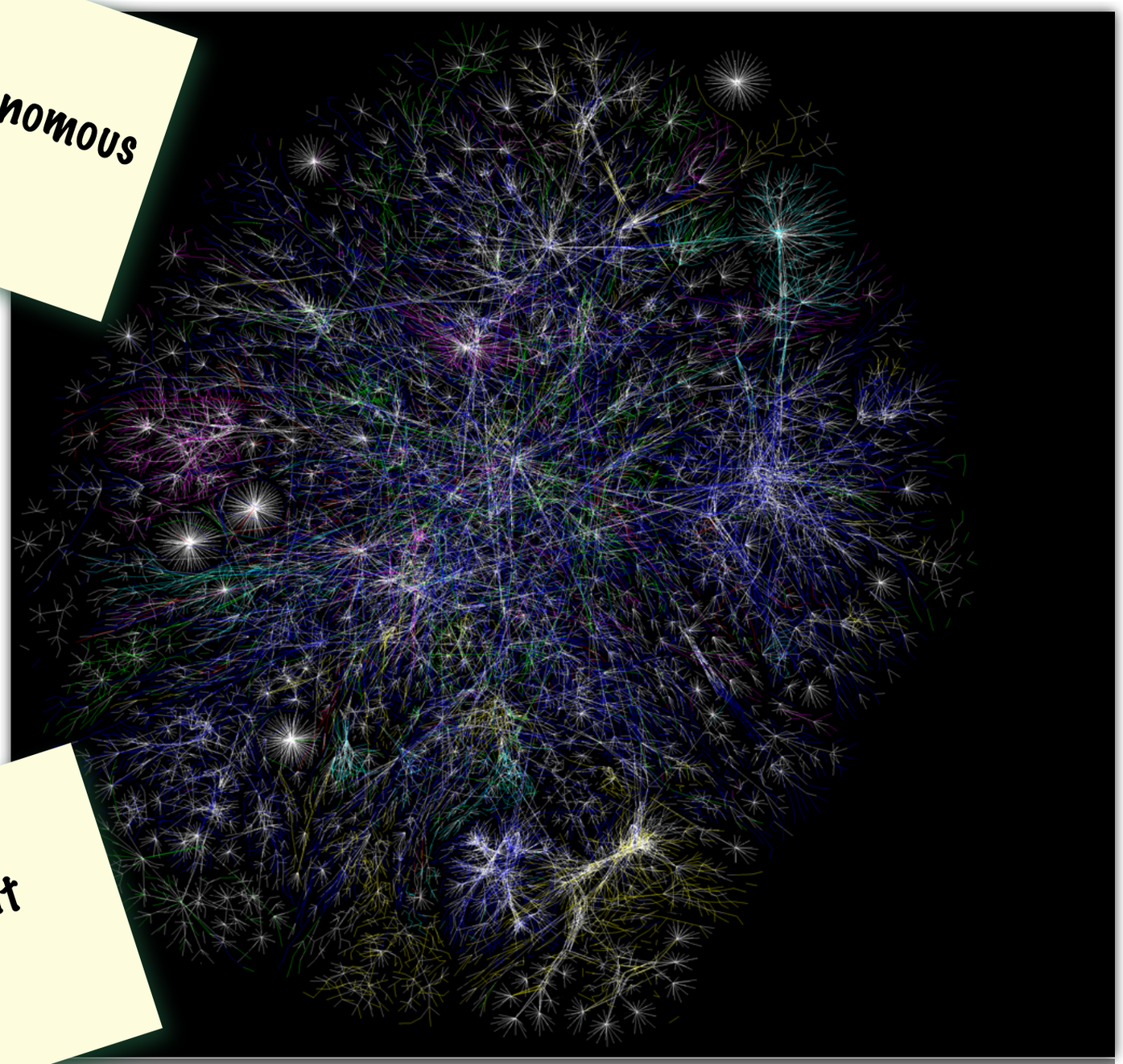
The IP API as the common open interface to the network



Permissionless Innovation

Mini note: HTTP is more and more the de-facto substrate

- Independent Autonomous Networks



- Serving different markets

Image source www.opte.org, creative commons license

Highly competitive

Commodity

The Price of Bandwidth, in bulk, per Mbps

A EUR80 fiber cross connect:	$0.01
Internet Exchange traffic:	$0.25*
Backbone traffic Western Europe:	$0.50
Transatlantic traffic, wholesale:	$1
Internet Transit, wholesale:	$2
Internet Transit, retail:	$15
Broadband Internet, consumer:	$50
National Ethernet service:	$180
3G mobile data, national:	$11,400
GSM voice call, national:	$483,840
3G mobile data, roaming low:	$834,000
3G mobile data, roaming high:	$3,127,500
GSM voice call, roaming:	$3,338,496
SMS Text Messages:	$210,000,000
SMS Text Messages, roaming:	$1,166,400,000

Western Europe, early-mid 2011 (based on 10Gbps or 300GB)

Table courtesy of Remco van Mook, Equinix

Open Internet Keywords

Voluntary adoption of technology

bottom-up innovation

Functional Interoperability

Different Players at Different Layers

Global Generic and Universal

Collaboration where needed

Competition where possible

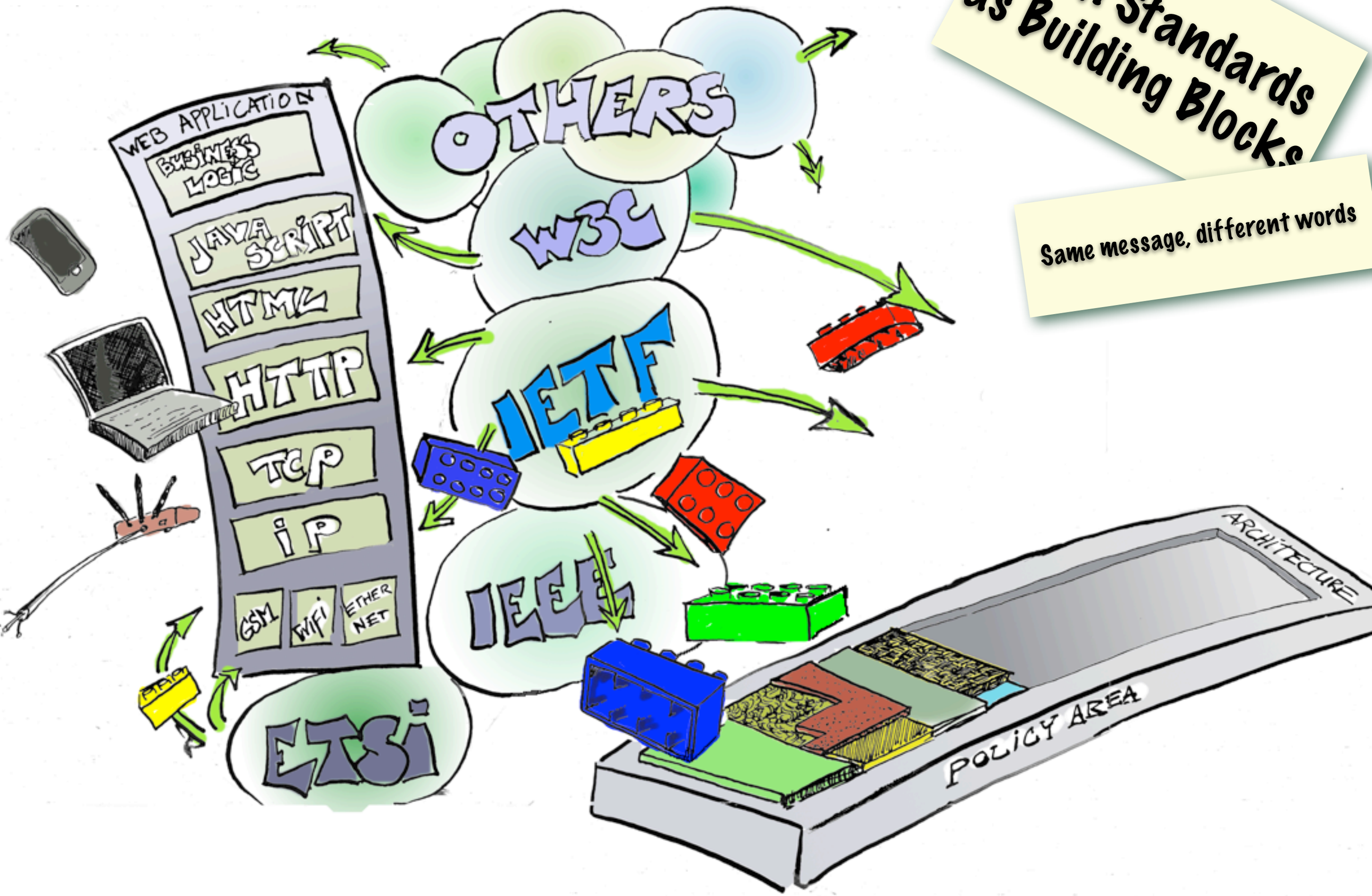
How Do Open Standards Play a Role

Browsing The Web			
802.11	IEEE	TCP/IP	IETF
URI	IETF	BGP	IETF
NAT	No Standard	HTTP	IETF
CSS	W3C	PNG	IETF
HTML	W3C/ISO	MPEG	ISO/IEC
XML	W3C	ADSL	ITU-T

Interoperability

Open Standards as Building Blocks

Same message, different words



Standardization the Internet way

Cooperation

Collective Empowerment

Voluntary Adoption

Adherence to Principles

Availability

driver for innovation

Borderless commerce

Details on:
http://open-stand.org

1. Cooperation

Respectful cooperation between standards organizations, whereby each respects the autonomy, integrity, processes, and intellectual property rules of the others.

2. Adherence to Principles

Adherence to the five fundamental principles of standards development:

- **Due process.** Decisions are made with equity and fairness among participants. No one party dominates or guides standards development. Standards processes are transparent and opportunities exist to appeal decisions. Processes for periodic standards review and updating are well defined.
- **Broad consensus.** Processes allow for all views to be considered and addressed, such that agreement can be found across a range of interests.
- **Transparency.** Standards organizations provide advance public notice of proposed standards development activities, the scope of work to be undertaken, and conditions for participation. Easily accessible records of decisions and the materials used in reaching those decisions are provided. Public comment periods are provided before final standards approval and adoption.
- **Balance.** Standards activities are not exclusively dominated by any particular person, company or interest group.
- **Openness.** Standards processes are open to all interested and informed parties.

3. Collective Empowerment

Commitment by affirming standards organizations and their participants to collective empowerment by striving for standards that:

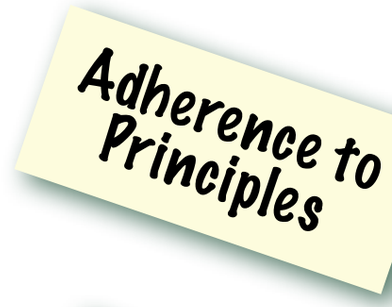
- are chosen and defined based on technical merit, as judged by the contributed expertise of each participant;
- provide global interoperability, scalability, stability, and resiliency;
- enable global competition;
- serve as building blocks for further innovation; and
- contribute to the creation of global communities, benefiting humanity.

4. Availability

Standards specifications are made accessible to all for implementation and deployment. Affirming standards organizations have defined procedures to develop specifications that can be implemented under fair terms. Given market diversity, fair terms may vary from royalty-free to fair, reasonable, and non-discriminatory terms (FRAND).

5. Voluntary Adoption

Standards are voluntarily adopted and success is determined by the market.



OUTLINE

Open Internet

Open Standards

We are here

The IETF as a Open Standards Body

Org Chart

Working Methods

Participation

The Internet Engineering Task Force is
a loosely self-organized group of people
who contribute to the engineering and
evolution of Internet technologies.
It is the principal body engaged in the
development of new Internet standard
specifications.

RFC4677

The mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet.

IETF Universe

Internet Society

RFC Editor

IAB

IRTF

iana
Internet Assigned Numbers Authority

IETF Secretariat

IESG

IASA

IAD | IAOC

IETF Trust

Area	Area	Area	Area	Area	Area
working group	working group	working group	working group	working group	working group
working group	working group	working group	working group	working group	working group
working group	working group	working group	working group	working group	working group
working group	working group	working group	working group	working group	working group
working group	working group	working group	working group	working group	working group
working group	working group	working group	working group	working group	working group

INT

About Packets

RTG

About creating the paths for the packets

OPS

About managing the networks

SEC

About Security Protocols (cross area)

TSV

About the use of the paths to provide the end-to-end experience

APS

About Application Protocols used on the Internet

RAI

About Real Time Applications

IESG

Applications Area
P. Resnick
B. Leiba

- appsawg
- core
- httpbis
- hybi
- jcardcal
- paws
- precis
- repute
- scim
- spfbis
- urnbis
- websec
- weirds

Transport Area
M. Stiemerling

- alto
- behave
- cdni
- ippm
- mptcp
- nsfv4
- ppsp
- rmcat
- rmt
- storm
- tcpm
- tsvwg

Security Area
S. Turner
S. Farrell

- abfab
- dane
- emu
- ipsecme
- jose
- kitten
- mile
- nea
- oauth
- pkix
- tls

Routing Area
S. Bryant
A. Farrell

- bfd
- ccamp
- forces
- i2rs
- idr
- isis
- karp
- l2vpn
- l3vpn
- manet
- mpls
- nvo3
- ospf
- pce
- pim
- pwe3
- roll
- rtwg
- sidr

O&M Area
B. Claise
J. Jaeggli

- 6renum
- adslmib
- bmwg
- dime
- dnsop
- eman
- grow
- ipfix
- mboned
- netconf
- netmod
- opsawg
- opsec
- v6ops
- wkops

RAI Area
G. Gamarillo
R. Barnes

- avtcore
- avtext
- bfcpbis
- clue
- codec
- cuss
- dispatch
- drinks
- ecrit
- geopriv
- insipid
- mediactrl
- mmusic
- p2psip
- payload
- rtcweb
- salud
- siprec
- soc
- straw
- viper
- xmpp
- xrblock

Internet Area
B. Haberman
T. Lemmon

- 6lowpan
- 6man
- ancp
- dhc
- dmm
- dnext
- hip
- homenet
- intarea
- l2tpext
- lisp
- lwig
- mif
- mip-4
- multimob
- netext
- ntp
- pcp
- pppext
- savi
- softwire
- sunset4
- tictoc
- trill

GENERAL AREA
J. Arko

last update of this slide: march 2013

IETF Standards and RFCs

IETF standards are published as RFCs

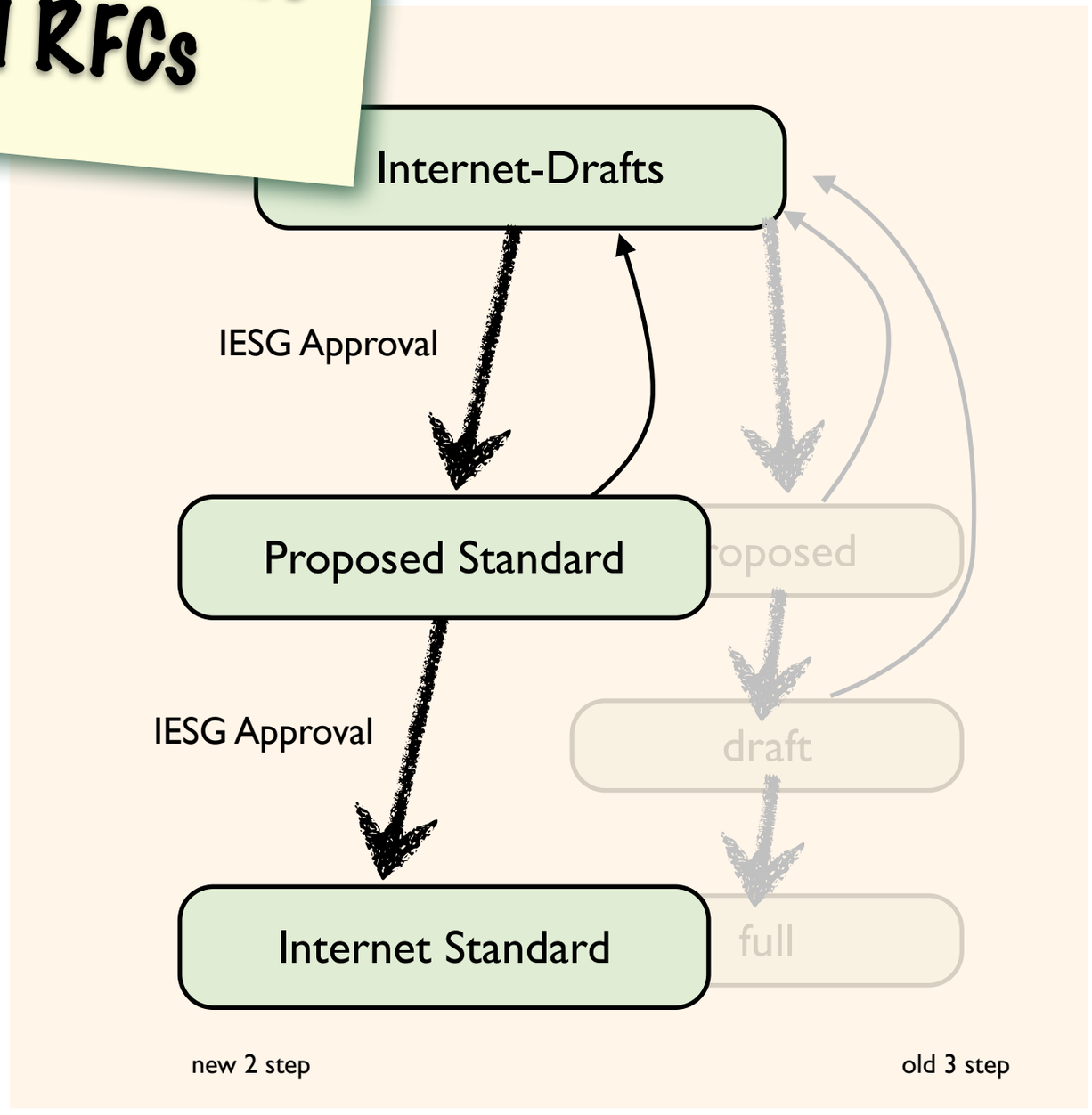
- Standards track
- Best Current Practices (operational)
- Informational and Experimental

RFC series also includes

- IRTF (Internet Research Task Force)
- IAB (Internet Architecture Board)
- Independent contributions

Standards Track documents are maintained by the IETF

- IESG approval: based on consensus process



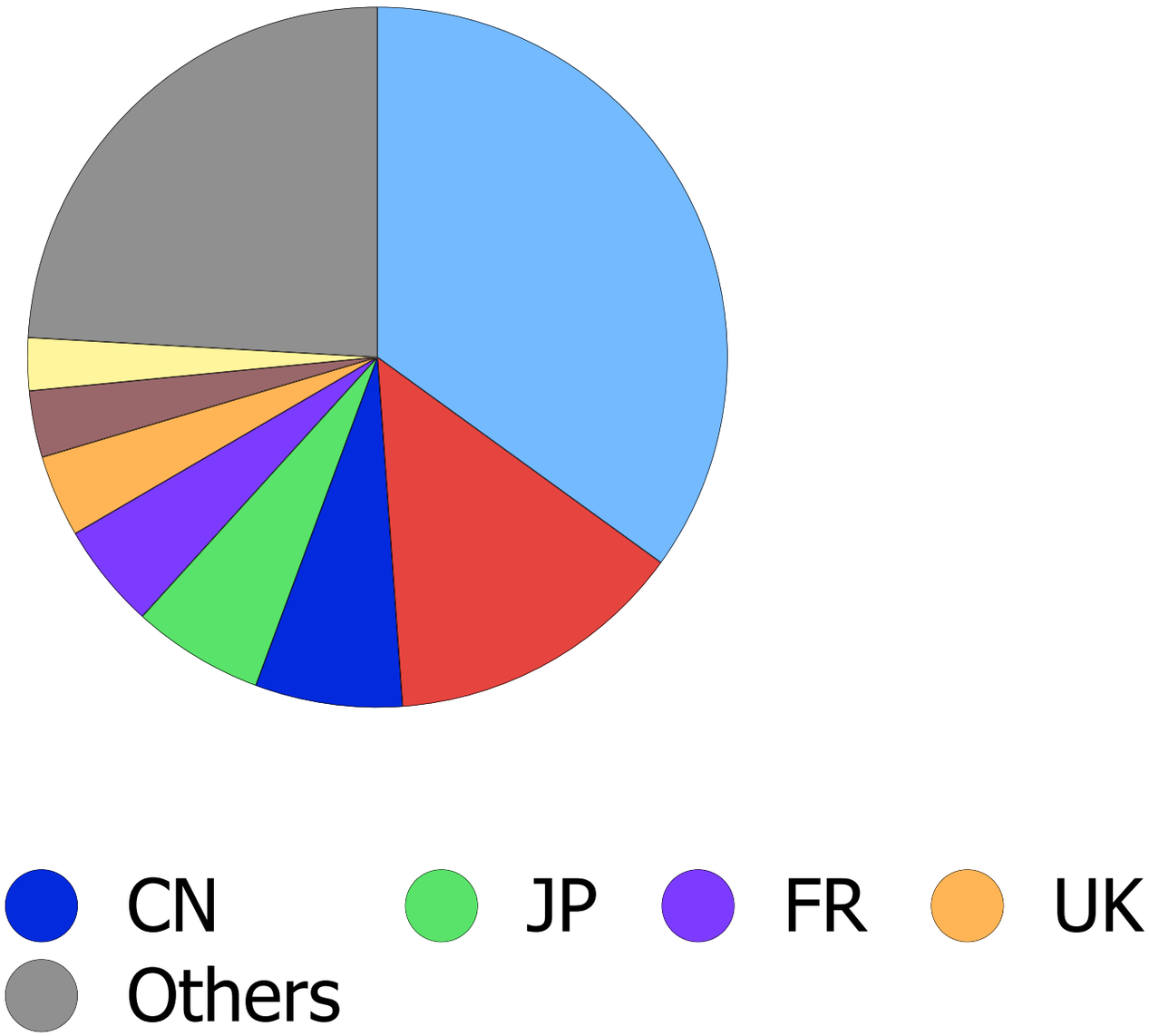
Not al RFCs are IETF standards

IETF 87 Participar

Who Participates

Berlin Meeting Stats

- 1407 people
  - 316 newcomers
  - IETF 84 (Vancouver) was 1199 people
- 62 countries
  - IETF 84 was 52 countries



IETF comes to town

November 3-8, 2013	**Vancouver, CA**
March 2-7, 2014	**London, UK**
July 20-25, 2014	**Toronto, CA**
November 9-14, 2014	**Honolulu, US**
March 22-27, 2015	**Dallas, US**
July 19-24, 2015	**Prague, CZ**
November 1-6, 2015	**Yokohama, JP**

Who Pays

IETF 2012 - 2014 Budget	2012 Budget	2013 Advice	2014 Advice
Revenues			
Registration Fees	$ 2,152	$ 2,101	$ 2,119
Meeting Sponsorship	310	290	590
Network/NOC Host	556	555	605
Hotel Commissions	145	150	150
New Revenue	100	125	125
Miscellaneous	0	-	-
Total Revenue	$ 3,264	$ 3,221	$ 3,589
Expenses	2012 Budget	2013 Advice	2014 Advice
RFC Services	900	$ 933	$ 933
Secretariat Services	1,775	1,788	1,788
Secretariat Costs (Other)	0	-	-
Meeting Space Costs	350	290	590
Network/NOC Costs	600	555	630
Meeting Operations (Secretariat)	912	828	828
Other Meeting Costs	118	124	124
Subtotal Direct Meeting Costs	1,979	1,796	2,171
Transition Expenses	85	60	60
Special Projects	50	50	50
IT Maintenance	50	75	100
Admin (IASA,IETF, IAB, IRTF, NomCom)	415	424	442
IETF Trust	35	37	39
ISOC G&A	120	125	130
Total Expenses	$ 5,408	$ 5,287	$ 5,713
ISOC Direct Contribution Excluding Development	$ 2,145	$ 2,067	$ 2,124
IT Tools Development	215	50	75
ISOC Direct Contribution Including Development	$ 2,360	$ 2,117	$ 2,199

Public Policy Objectives

STANDARDS

Technology

Must Read

Tussle in Cyberspace: Defining Tomorrow's Internet

David D. Clark
MIT Lab for Computer Science
ddc@lcs.mit.edu

Karen R. Sollins
MIT Lab for Computer Science
[illegible]@lcs.mit.edu

John Wroclawski
MIT Lab for Computer Science
jtw@lcs.mit.edu

Robert Braden
USC Information Sciences Institute
braden@isi.edu

1. INTRODUCTION

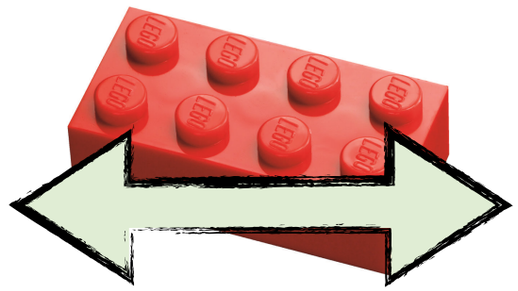
The Internet was created in simpler times. Its creators shared a common goal—they wanted to build a way to hook all the computers in the world. Their own applications could [illegible] other designers, [illegible] common

http://groups.csail.mit.edu/ana/Publications/PubPDFs/Tussle2002.pdf

IETF Technology

Public Policy Aspects

WG Acronym



2 word description of policy area

The design of the building blocks is sometimes triggered by policy requirements and sometimes there are identified public policy aspects.

EXAMPLES

IETF Technology

Stir

Ecrit

Paws

Lmap

Mile

Weirds

Eman

Public Policy Aspects

Tel. number authorization

POTS

Emergency Response

Spectrum Management

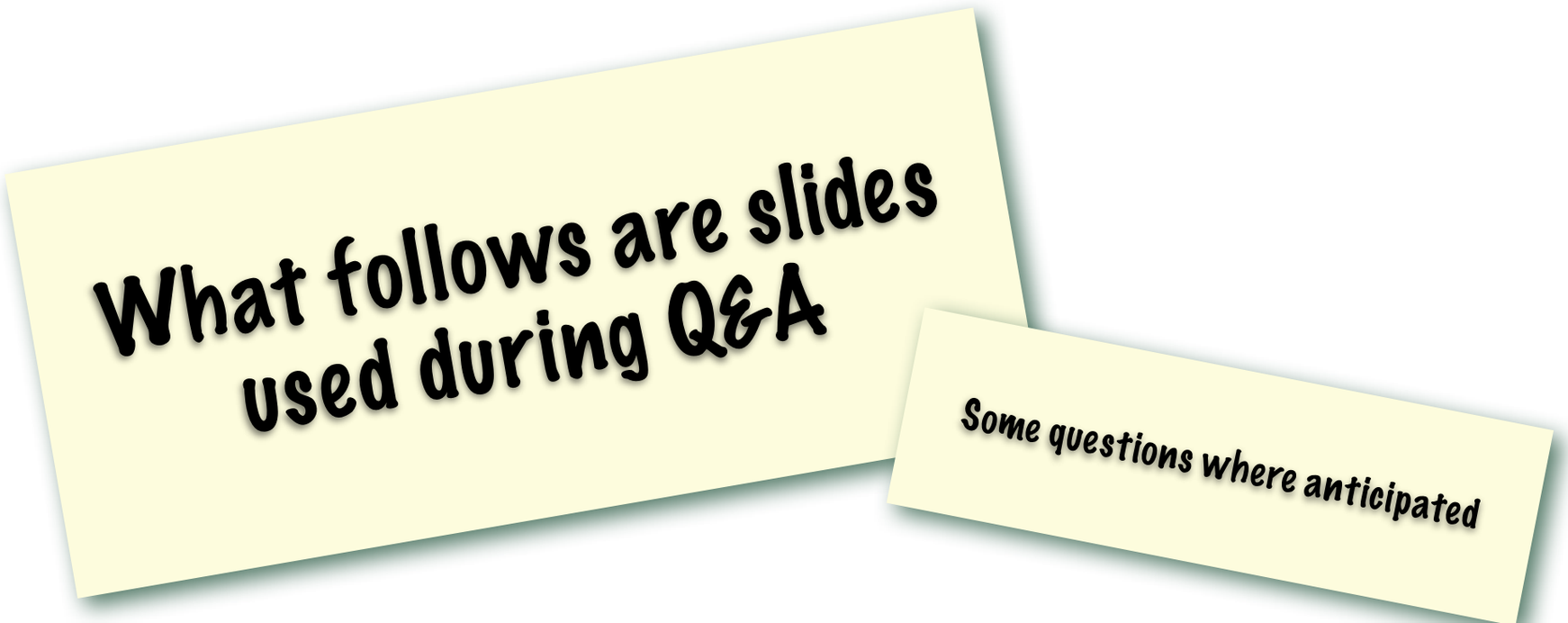
Consumer / Universal Service

ICT trust and security

law enforcement

Energy Management

Question Time



IETF Crypto Support

IETF uses Crypto, does not develop Crypto

IETF protocols are crypto agile

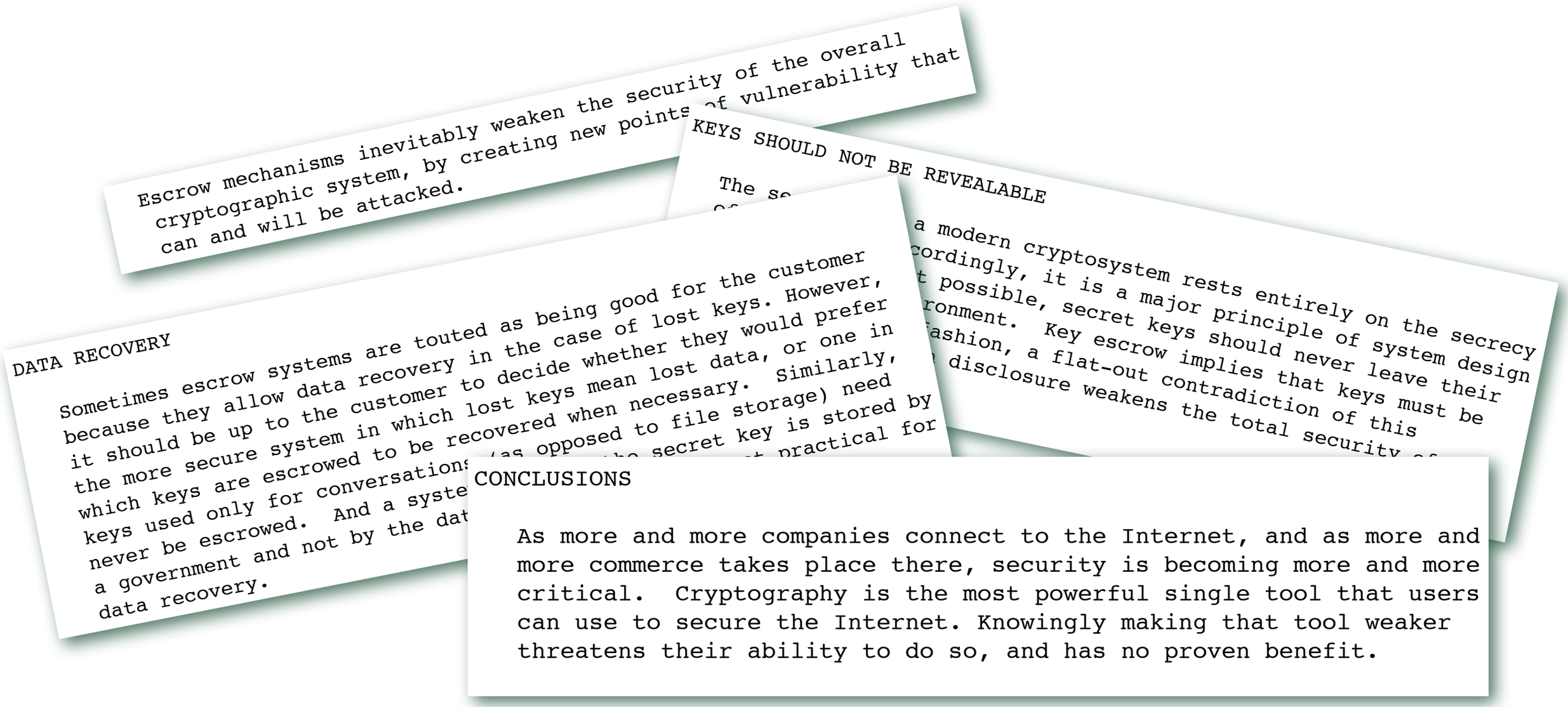
- IETF creates few obstacles to support of national cryptographic algorithms in IETF protocols
  - Public pointer to algorithm definition required, but the documentation need not be an RFC.
  - Easy to publish specifications on algorithm use with IETF security protocols as Informational RFCs
  - Procedures in place to allocate code points
  - Process already used for publication of RFCs specifying use of US, Korean, Japanese, and Russian cryptographic algorithms

USA – Suite B – RFC 5430, 5647, 6239, 6318, 6379, 6380, etc.
Korea – SEED – RFC 4009, 4010, 4162, 4196, 4269, 5669, 5748
Japan – Camellia – RFC 3657, 3713, 4132, 4312, 5528, 5529, etc.
Russia – GOST – RFC 4357, 4491, 5830, 5993, etc.

August 1996

RFC1984

IAB and IESG Statement on Cryptographic Technology and the Internet



Escrow mechanisms inevitably weaken the security of the overall cryptographic system, by creating new points of vulnerability that can and will be attacked.

KEYS SHOULD NOT BE REVEALABLE

The se

a modern cryptosystem rests entirely on the secrecy
cordingly, it is a major principle of system design
t possible, secret keys should never leave their
ronment. Key escrow implies that keys must be
ashion, a flat-out contradiction of this
disclosure weakens the total security

DATA RECOVERY

Sometimes escrow systems are touted as being good for the customer because they allow data recovery in the case of lost keys. However, it should be up to the customer to decide whether they would prefer the more secure system in which lost keys mean lost data, or one in which keys are escrowed to be recovered when necessary. Similarly, keys used only for conversations (as opposed to file storage) need never be escrowed. And a system in which the secret key is stored by a government and not by the dat practical for data recovery.

CONCLUSIONS

As more and more companies connect to the Internet, and as more and more commerce takes place there, security is becoming more and more critical. Cryptography is the most powerful single tool that users can use to secure the Internet. Knowingly making that tool weaker threatens their ability to do so, and has no proven benefit.

May 2000

RFC 2804

IETF Policy on Wiretapping

Abstract

The Internet Engineering Task Force (IETF) has been asked to take a position on the inclusion into IETF standards-track documents of functionality designed to facilitate wiretapping.

This memo explains what the IETF thinks the question means, why its answer is "no", and what that answer means.

SDO	IETF Liaison Manager	IAB Liaison Shepherd
3GPP	Gonzalo Camarillo	Hannes Tschofenig
3GPP2	Charlie Perkins	Marc Blanchet
Broadband Forum	David Sinicrope	Ross Callon
CableLabs	Ralph Droms	Eliot Lear
ICANN Board of Directors	Jonne Soininen	Andrew Sul
ICANN NomCom	Russ Mundy	Eliot Lear
ICANN RSSAC	Peter Koch	Marc Blanchet
IEEE 802.1	Eric Gray	Bernard Aboba
IEEE-SA	Dan Romascanu	Bernard Aboba
ISO/IEC JTC1 SC2	Patrik Fältström	Russ Housley
ISO/IEC JTC1 SC29	Stephan Wenger	Russ Housley
ISO/IEC JTC1 SC6	Allison Mankin	Russ Housley
ISO/TC46	John Klensin	Russ Housley
ITU-T	Scott Mansfield	Ross Callon
ITU-T, MPLS	Deborah Brungard	Ross Callon
ITU-T, SG15 (optical control plane)	John Drake	Ross Callon
Messaging Anti-Abuse Working Group (MAAWG)	Barry Leiba	Hannes Tschofenig
Unicode	Patrik Fältström	Dave Thaler
W3C	Mark Nottingham	Alissa Cooper
WIPO	Patrik Fältström	
ZigBee Alliance	JP Vasseur	

Formal Relations

Up to date information at: http://www.ietf.org/liaison/managers.html

fin