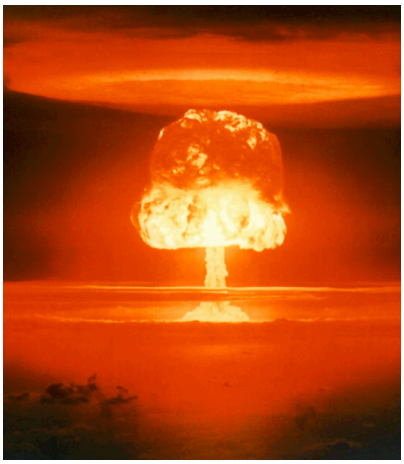
Where-to-Where
(was End-to-End)

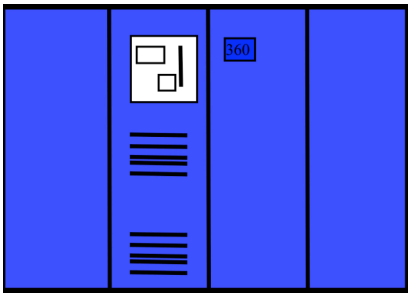
Scott Bradner
Harvard University
20 October 2005

w2w - 1

The Original Reason(s)



or



w2w - 2

Copyright 2005 Scott Bradner - all rights reserved

What to Do?

use self-describing packets

connect existing networks

design for

- survivability
- to support multiple types of communications
- over a variety of network types
- with distributed management
- cost effectiveness
- low cost attachment
- accounting for use of resources

!security
!QoS
!efficiency

The Design Philosophy of the DARPA Internet Protocols - Dave Clark nms.lcs.mit.edu/6829-papers/darpa-internet.pdf

w2w - 3

What Else?

support diverse technologies

use global “internetwork” addresses

w2w - 4

Copyright 2005 Scott Bradner - all rights reserved

Architectural Principle

e2e

let the ends do it

(or control it)

let the user decide

(a.k.a., The Stupid Network)

End-to-End Arguments in System Design - Saltzer, Reed & Clark
http://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.txt
The Rise of the Stupid Network - David Isenberg http://www.isen.com/stupid.html

w2w - 5

But!

no QoS!

no business model!

where is security?

w2w - 6

Copyright 2005 Scott Bradner - all rights reserved

QoS

can you sell better QoS at a higher price?

multiple levels per customer

"the Internet is not reliably crappy enough"

"It fails to fail often enough so it looks like it works."

Mike O'Dell

IAD = IQ test

enterprise VoIP?

w2w - 7

ISP Business Model

service can be provided by 3rd parties - not just by carriers

a quote from an IETF mailing list

Hi Roy,

I still don't understand why it is a "users" choice where the "services" are executed - I would have thought that this would be networks choice

and ISP does not profit from applications using network - i.e., Internet is a commodity

"We do not know how to route money"

Dave Clark

w2w - 8

Copyright 2005 Scott Bradner - all rights reserved

Internet Security

e2e means security is an end system responsibility

end systems under relentless attack

- worms, versus, spyware, ...

Internet infrastructure under occasional attack

- DNS root servers, routers, management systems, ...

Internet does not protect end system

- makes sure the worm is delivered promptly

end users & regulators may demand that “the Internet” protect the users

carriers may leap to help

- same tools can access to content providers

w2w - 9

Internet Architecture

no regulated architecture or basic design

no regulated interconnection requirements

(in US) no registration/control of ISPs

thus

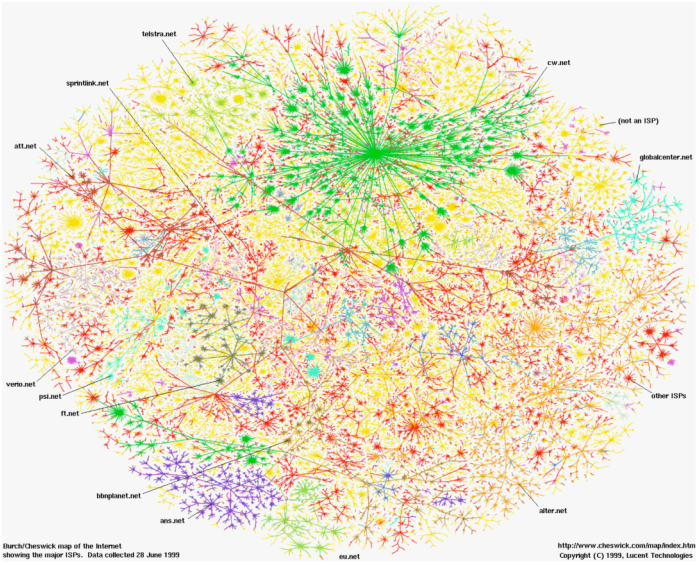
no consistent Internet architecture

may be better from a security standpoint

w2w - 10

Copyright 2005 Scott Bradner - all rights reserved

Internet “Architecture”



w2w - 11

Thus

Internet & IP networks

by definition - to traditional networking folk

w2w - 12

Copyright 2005 Scott Bradner - all rights reserved

What Did It Give Us

e2e Internet, and open computer operating systems, are *generative*

- enable innovation by others

impact society by moving or eliminating control points

The Internet is a “parent revolution”

w2w - 13

Who said this about what?

“*The invention of the [...] is the greatest event in history. It is the mother of revolution.*”

“*In its [...] form, thought is more imperishable than ever; it is volatile, irresistible, indestructible. It is mingled with the air. ... Now it converts itself into a flock of birds, scatters itself to the four winds, and occupies all points of air and space at once.*”

“*A [...] is so soon made, costs so little, and can go so far! How can it surprise us that all human thought flows in this channel?*”

w2w - 14

Copyright 2005 Scott Bradner - all rights reserved

Victor Hugo: Hunchback

"*The invention of the **printing press** is the greatest event in history. It is the mother of revolution.*"

"*In its **printed** form, thought is more imperishable than ever; it is volatile, irresistible, indestructible. It is mingled with the air. ... Now it converts itself into a flock of birds, scatters itself to the four winds, and occupies all points of air and space at once.*"

"*A **book** is so soon made, costs so little, and can go so far! How can it surprise us that all human thought flows in this channel?*"

And the Internet?

w2w - 15

Current Alternative

Intelligent Network (IN)

let the carrier do it

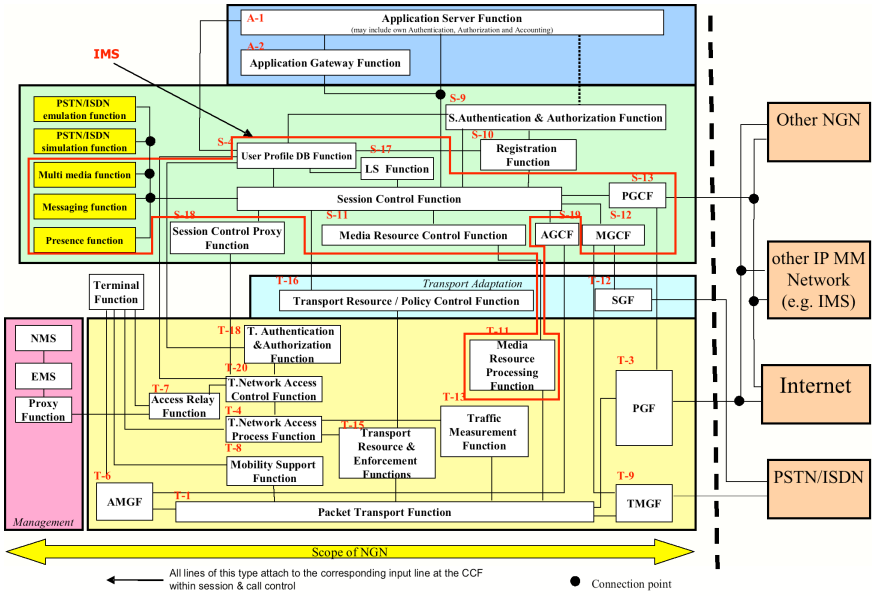
(or control it)

carrier decides

w2w - 16

Copyright 2005 Scott Bradner - all rights reserved

Future Alternative: ITU-T?



w2w - 17

No E2E

- alternatives assume carrier involvement in application use of the network

w2w - 18

Copyright 2005 Scott Bradner - all rights reserved

Regulations

current list of effective US government regulations on the Internet

- ~~traditional fraud/business regulations~~
- ~~CANSPAM~~
- ~~CDA~~
- DNS squatting
- ~~anti porn~~
- ...

w2w - 19

Regulatory Approaches

openists

- net must be open to enable *innovation commons*
  - require *network neutrality*
    - e.g., power grid does not favor toasters
- to let people at edge/end innovate **e2e**
- *dumb pipe* must be available

deregulationists

- if network is property then companies will innovate
  - note: “property” specifically includes right to exclude
- network owner needs incentive to invest **IN**
- forced *smart pipe* OK

The Broadband Debate: A User's Guide - Tim Wu
http://ssrn.com/abstract=557330

w2w - 20

Copyright 2005 Scott Bradner - all rights reserved

FCC

4 “principles” (5 August 2005)

- *consumers are entitled to access the **lawful** Internet content of their choice*
- *consumers are entitled to run applications and use services of their choice, **subject to the needs of law enforcement***
- *consumers are entitled to connect their choice of **legal** devices that **do not harm the network***
- *consumers are entitled to competition among network providers, application and service providers, and content providers*

http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf

w2w - 21

FCC: CALEA

Internet & interconnected VoIP providers subject to CALEA (wiretapping) law

- VoIP provider "*must necessarily use a router or other server*" thus is facilities-based

logic in FCC Order & principles logically leads to a requirement that the FBI pre-approve applications

- something they requested

http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-153A1.pdf

w2w - 22

Copyright 2005 Scott Bradner - all rights reserved

U.S. House

House Energy and Commerce Committee draft
covers BITS, VoIP & video providers
preempt state & local regulations
all types of providers must register with govt.
requires BITS providers to

> *provide subscribers with access to lawful content, applications, and services provided over the Internet, and to not block, impair, or interfere with the offering of, access to, or use of such content, applications or services*

http://energycommerce.house.gov/108/News/09152005_staff_disc.pdf

w2w - 23

Internet Governance

World Summit on the Information Society - WSIS

- discussing "Internet Governance"

intergovernmental body

- NGOs may watch but ...

e.g., who should control DNS root?

- currently ICANN with US DoC oversight

big push to move to UN (or the like)

- assumptions of other authorities might follow
  - e.g., protect citizens from confusing information

w2w - 24

Copyright 2005 Scott Bradner - all rights reserved

Non Transparent Net

transparency of end2end network mostly gone

- enterprise edge issues
  - NATs, firewalls, proxies, content caches, TCP reshapers
- core issues
  - deregulationists want to let carriers block/impact traffic
- governmental issues
  - e.g., China blocking access to “bad” sites
  - PA law blocking access to “child porn” sites

w2w - 25

Trust-Free Net

mistrust IP address (e.g., NAT)

mistrust privacy (e.g., wiretapping)

mistrust identity of other end (e.g., proxy)

mistrust identity (spoof)

w2w - 26

Copyright 2005 Scott Bradner - all rights reserved

Security in a Trust-Free Net

must be e2e
- as noted in original e2e paper

cannot include network devices/systems in trust envelope and be sure of security

thus e2e identification & encryption is key

secure web browsers often provide this
- some use SSL offload engines so not actual e2e

firewalls do not provide security
- unless firewall is in the end system

e2e encryption is a problem for law enforcement
- Clipper II on the way?

w2w - 27

Tussle in Cyberspace

describes requirement conflicts in today's Internet as "tussles" between needs

advises designing protocols/applications to split along tussle boundaries and to let users express choice
- e.g. tie QoS to packet markings not port #s
- what is good tussle boundary for e2e security?

biggest tussle may be economics
- commodity service vs. compensating non-local ISPs
- "routing money" from service providers to ISPs
- IPR (e.g., music & movie sharing)

Tussle in Cyberspace: Defining Tomorrow's Internet - Clark et al
www.acm.org/sigcomm/sigcomm2002/papers/tussle.pdf

w2w - 28

Copyright 2005 Scott Bradner - all rights reserved

e.g., QoS Tussle

widespread belief that the Internet needs QoS controls

intserv, diffserv & RSVP used in enterprises

MPLS for bulk QoS (traffic engineering) used in some ISPs

but different prices for different service levels is a hard ISP sell

- maybe because today's Internet is not reliability crappy enough to provide business model
  - e.g., VoIP "just works" most of the time - see Skype
- but telcos do not believe that, nor do regulators

w2w - 29

QoS Tussle, contd.

where (if) QoS needed - what should drive it?

- carrier-run "content-aware" network?
- application request special handling for its packets - per session
- application/site mark packets for special handling - class of service

w2w - 30

Copyright 2005 Scott Bradner - all rights reserved

Thus 1

significant pressures to block end2end

- especially at boundaries (e.g., enterprise or ISP edge)
- but also home NATs & computer firewalls

blocks possible to circumvent

- e.g., HTTP tunnels (see RFC 3093)
- e.g., HTTPS from browser to “server”

enterprise ISPs still mostly open

- but a few “protect” by blocking “dangerous” ports

w2w - 31

Why e2e is(was) Important

customer freedom to access information & content

- psychology important - not clear economically vital

allows widespread innovation activity

- dramatic (and chaotic) innovation using Internet
  - (chaos does bother some people)

non-transparent net restricts ability to innovate

- must get permission of block owner or hide in HTTP

CDA testimony - Bradner - http://www.sobco.com/papers/index.htm
The Future and its Enemies - Postrel - http://www.dynamist.com/tfaie/

w2w - 32

Copyright 2005 Scott Bradner - all rights reserved

MU Rules!

many innovators particularly important when user desires are unclear
- High Market Uncertainty (High MU)

low MU: all implementers know what user wants
- product becomes commodity (low profit)
- implemented in most economically efficient way
  - often centrally

high MU: implementers have to guess
- implementer that gets it right gets high profit
- thus high value in many implementers
- e2e facilitates implementers

A Real Options Metric to Evaluate Network , Protocol, and Service Architecture - Gaynor, Bradner - http:www.sobco.com/papers/ccr-10-2005.pdf

e2e

convinced that the e2e principle is important?
- Google & Skype are

can you get e2e these days?

first - what is an “end”?

Copyright 2005 Scott Bradner - all rights reserved

What is (was) an End?

could be:

- your own desktop/laptop
- 3rd party server somewhere on the net
- enterprise border firewall
- ISP border firewall

for innovation “end” must not be between client & server

- i.e., your client must be able to reach my server

could an “end” be anyplace else?

w2w - 35

Who “Owns” Your Computer?

today enterprise often owns your desktop

- you may not have admin access

you own your home computer

- modulo spyware etc

what about trusted computing?

- Microsoft direction - control what software can run in computer - e.g., to protect intellectual property

where is “end” in these cases?

- are we endless?

The Future of the Internet and How to Stop it. - Zittrain
http://cyber.law.harvard.edu/zittrain/netfuture.pdf

w2w - 36

Copyright 2005 Scott Bradner - all rights reserved

What to Do?

given: end users can not protect themselves

given: something is going to happen

- to protect end users, to protect net, to protect society, to protect IPR, to protect enterprises, ...

what to do

- make liability clear
  - for spam sending, for poor system maintenance, for music sharing, for open WiFi networks, for protecting data
- enable identity assurance
  - when legally needed - anonymity is a real issue
- ...

w2w - 37

Reality

IP-level end-to-end is gone for the average user

- enterprise firewalls, ISP firewalls, personal NATs, ...

IP-level end-to-end for enterprises is still here

- at least for now

thus enterprise sanctioned IP-level innovation can happen

but gone are the days of IP-level e2e being the normal case

w2w - 38

Copyright 2005 Scott Bradner - all rights reserved

IP-level e2e got us here

where can we go without IP-level e2e to individuals?

w2w - 39

Thus 2

with no e2e at IP level for users

must go up a level or two to get e2e

- e.g., run applications over HTTPS

but that creates a tussle at a bad boundary

- at encrypted pipe - allow or not

how long will layer 4 e2e last?

w2w - 40

Copyright 2005 Scott Bradner - all rights reserved

Thank you

&

Good Luck Innovating

w2w - 41

w2w - 42

Copyright 2005 Scott Bradner - all rights reserved