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

Cisco Technical Leadership Summit

Scott Bradner

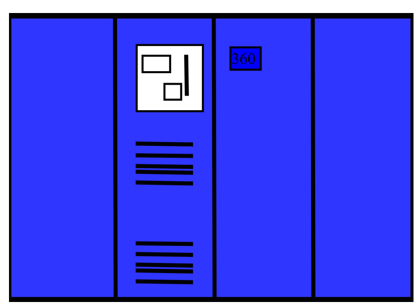
sob@harvard.edu

7 December 2005

w2w:cisco - 1

The Original Reason(s)

or



w2w:cisco - 2

What Existed

The Phone Network from **T**he **P**hone **C**ompany

- **circuit**-based
- **predictable** interconnections between ends
- **assumed** absolute requirement for QoS
- assumption of being **carrier**-provided
- the (only) service was **voice**

TPC

w2w:cisco - 3

What to Do?

use **self-describing** packets

connect **existing** networks

design for

Dest Addr	Src Addr	payload

- **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:cisco - 4

What Else?

global “**internetwork**” addresses

mapping (if needed) to local network address

“**bearer service**” between network(s) and applications

swap in new networks & applications

compare to **ATM**

w2w:cisco - 5

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:cisco - 6

But!

no QoS!

no business model!

where is security?

w2w:cisco - 7

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:cisco - 8

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:cisco - 9

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 control access to content providers

w2w:cisco - 10

Internet Architecture

no regulated architecture or basic design

no regulated interconnection requirements

(in US) no registration/control of ISPs

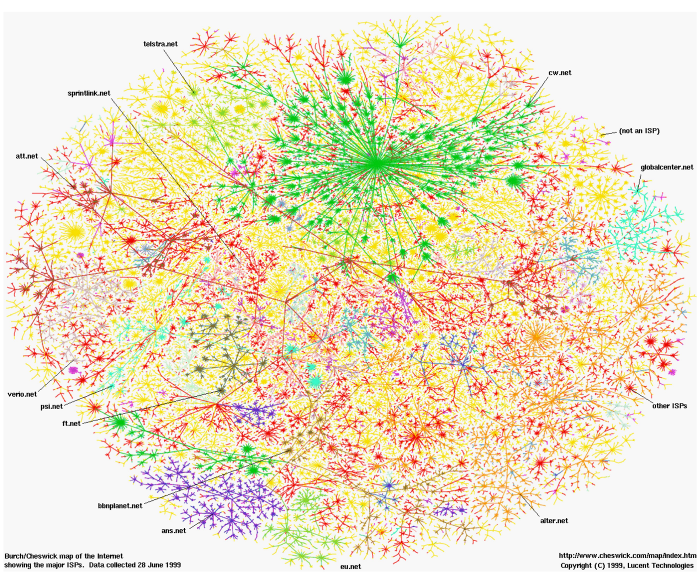
thus

no consistent Internet architecture

may be better from a security standpoint

w2w:cisco - 11

Internet "Architecture"



w2w:cisco - 12

Thus

Internet & IP networks

to traditional networking folk (by definition)

w2w:cisco - 13

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**"

"*The invention of the* ***printing press*** *is the greatest event in history. It is the mother of revolution.*" Victor Hugo: Hunchback of Notre Dame

w2w:cisco - 14

Enterprise Networking

- IP-based enterprise networks benefit from e2e
  - as long as “it” runs over IP “it” will run over the whole enterprise network
- enterprise campus networks generally have plenty of bandwidth
  - less need for QoS
- enterprise WAN nets can & do use QoS
  - enabled by unified management and different business model
  - can get funky over VPNs

w2w:cisco - 15

Current Alternative

Intelligent Network (IN)

a.k.a., SS7

let the carrier do it

(or control it)

carrier decides

w2w:cisco - 16

What Looks Wrong Here?

CISCO SYSTEMS

WHITE PAPER

BENEFITS OF CISCO IP COMMUNICATIONS IN A CISCO INTELLIGENT NETWORK

Adoption of IP Communications accelerated in 2004 as many businesses and organizations embraced this powerful technology. According to Synergy Research, the sales of IP telephony systems, to date the most popular of all IP Communications applications*, grew to US$3.5 billion in 2004—an 85-percent increase over the 2003 figure. Sales are projected to top US$10 billion in 2008. Cisco Systems® alone is displacing 10,800 traditional phones every business day, and more than 28,000 Cisco® customers use an all-IP solution—the largest number of IP Communications installations in the industry.

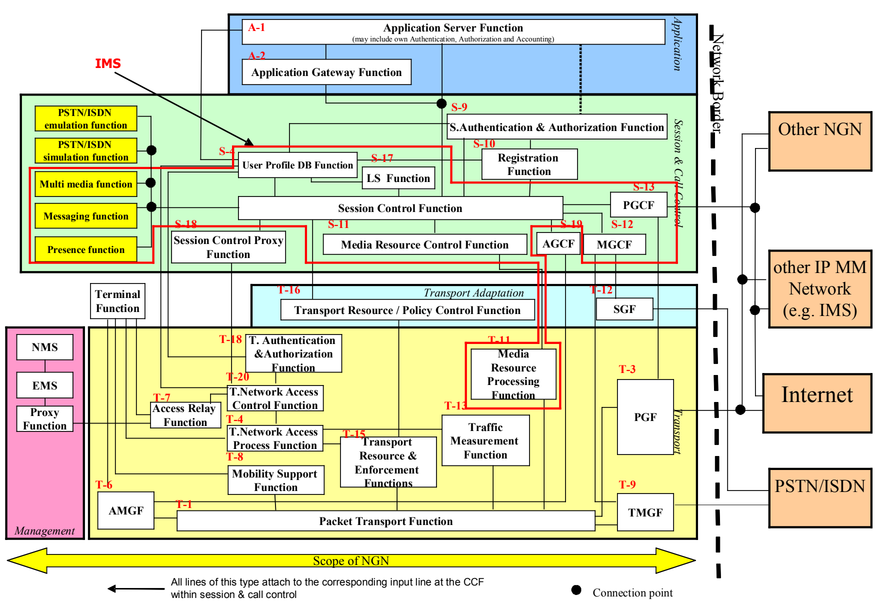
The significant design advantages, flexibility, and real-world successes of all-IP deployments have given this option an edge over the hybrid approach in the market. In a hybrid design, IP telephony is essentially bolted onto a core time-division multiplexing (TDM) architecture; therefore, only the IP-enabled endpoints have access to the rich capabilities of IP Communications. Also, because the TDM endpoints still exist on a separate network, companies do not realize the benefits of single management, and they may also lose the benefits of convergence that allows video and other IP-based applications to be easily added to the network and enables easy conferencing with voice, video, Web, and presence services.

A CONVERGED, INTELLIGENT NETWORK

Organizations that choose the all-IP option face another choice: whether to run IP Communications applications from one vendor on a different vendor's infrastructure, or choose IP Communications applications from the same vendor that built the infrastructure.

Cisco began developing IP telephony applications in 1997 and has provided IP Communications applications longer than any other vendor. From the start, Cisco's focus has been on the most efficient ways to create a modular, resilient, adaptive, and secure converged infrastructure as well as integrated applications for data, voice, and video. Cisco employs a *systems approach* that uses intelligence in the network to deliver cost advantages, productivity gains, industry-leading security, and a higher return on investment. A higher level of integration advantage is realized when Cisco IP Communications runs in a Cisco network.

Future Alternative: ITU-T?



No E2E

- alternative technologies assume carrier involvement in the application use of the network
  - knows what applications are running over network & “helps” them, “un-helps” them, or blocks them
- carrier is assumed to be in the picture on applications using running over the network

w2w:cisco - 19

Regulations

current list of effective US government regulations on the Internet

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

w2w:cisco - 20

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

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

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

may apply to universities

- FCC asked for comment on application to higher ed

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

w2w:cisco - 23

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/11032005_Broadband.pdf

w2w:cisco - 24

Carrier View

it's my wire, I'll do what I want with it

Edward E. Whitacre - CEO AT&T

'Google, Vonage & Skype are using **my** network for **free**'

William L. Smith - CTO Bell South

'we should be able to charge Yahoo to let their web page load faster than Google'

Internet Governance

World Summit on the Information Society - WSIS

- discussing "Internet Governance"
- started by ITU looking for a role

intergovernmental body

- NGOs may watch but ...

world summit
on the **information society**
Geneva 2003 - Tunis 2005

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

fought to a standstill - maintain status quo

- plus Internet Governance Forum (IGF)

ITU post WSIS

- ITU Secretary-General Yoshio Utsumi
  - *"the Internet need not be one net controlled by one centre"*
  - domestic networks are *"more efficient and economical"* (because much traffic is local)
  - *"telephone networks are made up of regional, domestic networks united together in agreement with ITU framework. A similar situation may start with the Internet"* - if so the ITU will be called upon to fix things (within 5 years)
- end-to-end? what is that?

http://www.theregister.co.uk/2005/11/21/utsumi_rejection/

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

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:cisco - 29

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:cisco - 30

Why e2e is(was) Important

allows widespread innovation activity

- dramatic (and chaotic) innovation using Internet
- *"What achieved success was the very chaos that the Internet is. The **strength** of the Internet is that **chaos**."*
  - (chaos does bother some people)

non-transparent net restricts ability to innovate

- must get permission of block owner or hide in HTTP

customer freedom to access information & content

- socially important - not clear economically vital

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

w2w:cisco - 31

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

w2w:cisco - 32

e2e

convinced that the e2e principle is important?

- Google & Skype are

can you get e2e these days?

first - what is an “end”?

w2w:cisco - 33

What is (was) an End?

could be:

- your own desktop/laptop
- 3rd party server somewhere on the net
- enterprise border
- 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:cisco - 34

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

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
- ...

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

IP-level e2e got us here

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

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 HTTP/HTTPS

how long will layer 4 e2e last?

Real (Non-Internet) World

- patents
- copyrights
- web services
- service-oriented architecture
- dream of content as king
- telephony business models

Internet of Things:
http://www.itu.int/osg/spu/publications/internetofthings/

Future(s)