Overview of Economic Models

Richard Clayton
richard.clayton@cl.cam.ac.uk

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

ITAT
4th December 2013

Why SHIM6 is likely to fail

Richard Clayton
richard.clayton@cl.cam.ac.uk

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

WEIS
June 2009

How is Internet routing failing ?

- Companies want to be multi-homed for reasons of resilience
  - IPv4 approach: publish specific route in global table
- Global routing table is growing super-linearly
  - ongoing for 20 years ! and so routers need constant upgrading
  - major cause of growth is multi-homing
- Can estimate cost of each route as $23bn / 300000 = $77K
  - $23bn estimate from router count & cost of different size networks
  - ALSO almost exactly twice the annual router industry sales
- Actual cost of obtaining an AS and publishing a route is low
  - RIPE: € 2300 in first year, € 1300 thereafter
- i.e.: local decision has global consequences
  - global cost is $77K, but cost to individual business is low
- viz: a “tragedy of the commons”

How does SHIM6 work ?

- SHIM6 is the chosen way of doing multi-homing in IPv6
  - chosen after lots of technical analysis of competing schemes
  - SHIM6 RFCs finally published in June 2009
- Multi-homed company gets IPv6 address space from each provider and all machines are configured to have multiple addresses, one IPv6 address from each provider
- Nothing special put into global routing table
- When a long-lived connection is made to a remote machine the other end is told “if I happen to disappear, then try this alternative address instead”
  - long-lived => 20+ packets (avoid overhead for short conversation)
  - lots of extra complexity to ensure that machines do not mislead and thereby impose a denial-of-service attack on a third party

Why will SHIM6 fail ?

- Multi-homed IPv6 site has incentive to deploy SHIM6
  - think of this as an incentive to push suppliers for the functionality, as well as doing all the complex issues of configuration
- But site only gets a benefit if remote sites also deploy SHIM6
- These remote sites have no incentive to bother

oops!!!

- So to get the full benefits of being multi-homed the site needs to become an AS and announce routes in the global table
- Hence they no longer have an incentive to deploy SHIM6
- No “first mover advantage” means no movement occurs

No surprise to WEIS attendees

- WEIS 2006:

  Bootstrapping the Adoption of Internet Security Protocols

  Andy Ozment & Stuart E Schechter

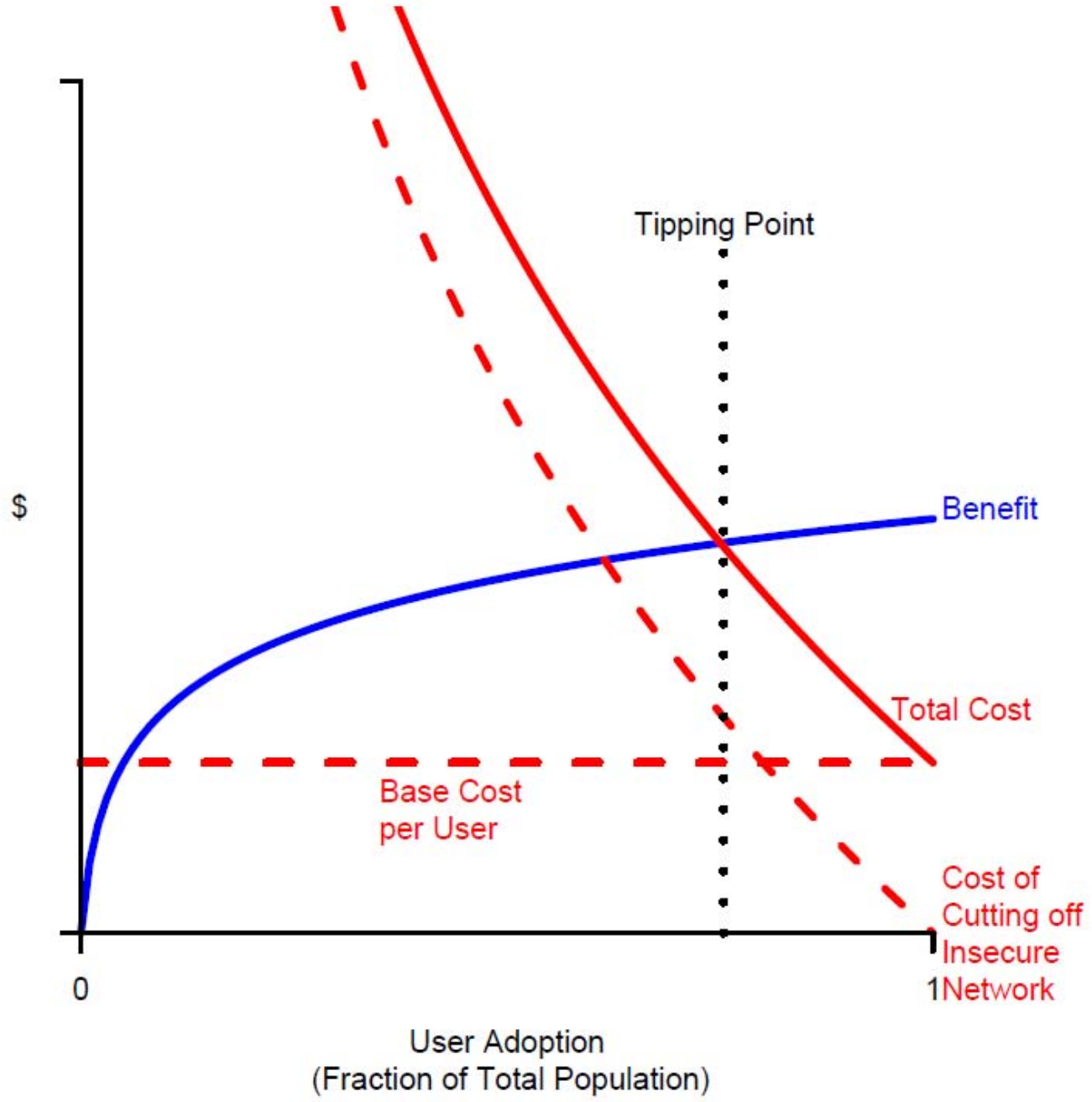
- They started by reviewing the value of networks
  - Metcalfe's law : benefit rises as square of participants; i.e. n^2
  - albeit, Odlyzko & Tilley suggested perhaps just *n log n*
- BUT this is the long term value – so the interesting question for them is how do you bootstrap the growth of the network ?
- If there is an immediate "first mover" advantage then easy!
  - well not quite, they still need someone to talk to!
- So what strategies are available for bootstrapping, especially when benefits do not accumulate for some time ?

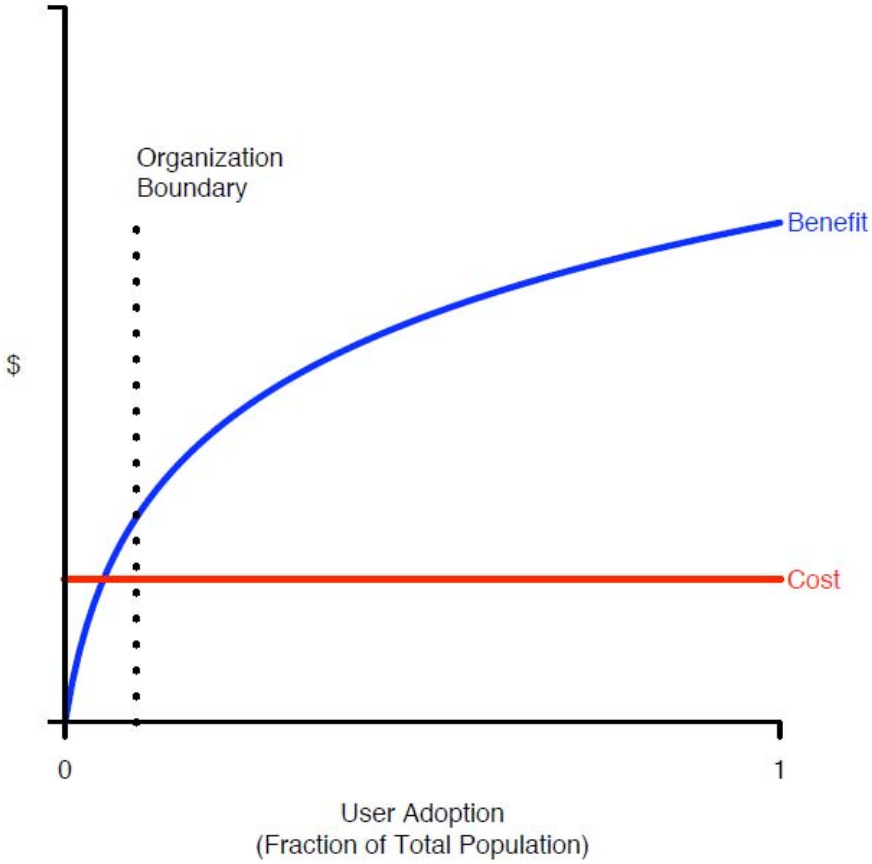
Approaches to bootstrapping I

- #1 Global mandate
  - fine/disconnect people who do not adopt the new protocol
  - TCP successfully replaced NCP on 1 Jan 1983
- #2 Partial mandate
  - force some to adopt, hoping thereby to reach a “tipping point”
  - credit card companies insisted on HTTPS (but no tipping point yet)
  - US .gov mandated the use of DNSSEC
- #3 Bundling complements
  - get something completely different if you adopt
  - e.g. deploying DNSSEC means that you can then use DANE
- #4 Facilitate sub-network adoption
  - can you get a benefit from deploying within an organisation?
  - e.g. fax machines were originally bought to connect offices within each individual organisation

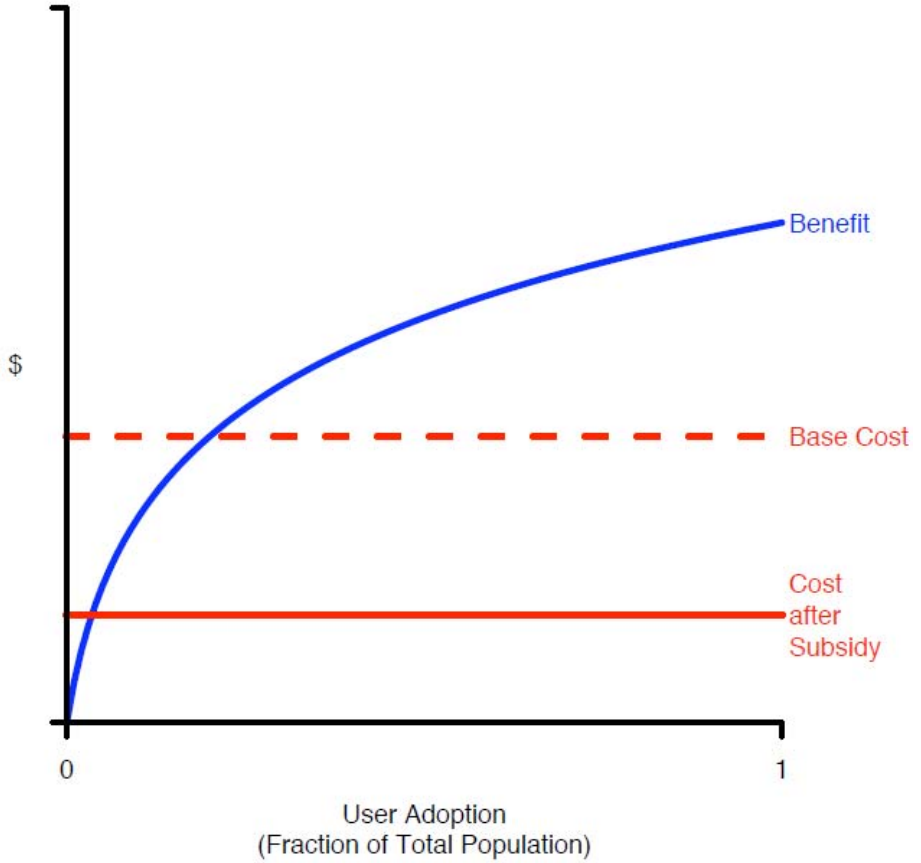
Approaches to bootstrapping II

- #5 Coordination
  - a coalition of the willing agree to use a new approach
  - this is where most of the analysis pre O&S was focussed
    - so still worth analysing this issue BUT NOT solely this issue
- #6 Subsidization
  - a government or similar rewards you for adoption
  - someone finances development (e.g. S/MIME)
  - the .SE registry produced an overnight step change in DNSSEC adoption by charging less for DNSSEC enabled domains
- Original O&S paper has lots of equations and graphs showing exactly why each of these approaches are effective !


Tipping Point
$
Benefit
Total Cost
Base Cost
per User
Cost of
Cutting off
Insecure
Network
0
1
User Adoption
(Fraction of Total Population)



(d) Subnetwork adoption



(f) Subsidization

O&S examples: SSH & email signing

- SSH is low cost (many free implementations)
- SSH is easy to learn and does not reduce functionality
- BUT ALSO NOTE
  - could be mandated within organisations (most use is internal)
  - full benefits available once the sub-network has adopted it
  - could use out of band approaches to announce the adoption, and out-of-band bootstrapping of trust (or just TOFU!)
- Email authentication is also low cost (both PGP & S/MIME)
- Authentication is easy to use & functionality basically OK
  - albeit key creation/distribution must be done by someone…
- BUT
  - much email goes external to organisations
  - SO hard to tell if you should expect mail to be signed/encrypted

So let's talk more about email

- Long tradition of reviewing anti-spam proposals from an economic perspective:

  You might be an anti-spam kook if… Vernon Schryver (2003)

  - describes common failure modes of the "FUSSP"
- A common view is that email is impossible to change because it is so widely deployed. Is that actually true ?
- Perhaps you think mail submission looks like this ?

```
telnet smtp.example.com 25
220 mail.example.com at your service
HELO richard.local
250 What can I do for you today ?
MAIL FROM: etc etc
```

Modern email submission

```
openssl s_client -starttls
      smtp -connect smtp.gmail.com:587 -crlf -ign_eof
250 CHUNKING
ehlo richard.local
250-mx.google.com at your service, [128.232.110.14]
250-SIZE 35882577
250-8BITMIME
250-AUTH LOGIN PLAIN XOAUTH XOAUTH2 PLAIN-CLIENTTOKEN
250-ENHANCEDSTATUSCODES
250 CHUNKING
auth plain AGRvSWxvb2tsaWtlPw==
235 2.7.0 Accepted
mail from: etc etc
```

Perhaps you meant the email itself ?

```
Message-ID: <3rHmRHA7+r9vEAo$@turnpike.com>

Date: Sun, 2 Jul 1995 16:48:11 +0100

From: Richard Clayton <betatest@turnpike.com>

To: betatest@turnpike.com

Subject: Turnpike version 1.03

Sender: Richard Clayton <richard@turnpike.com>

X-Mailer: Turnpike v1.03 <U2yaxlNz9m7tpk5wwwfqeW1so7>
```

Today's email is authenticated/traceable...

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s1024; t=1385997947; bh=/AcAUoW
n+kYTxC0Gexd92FS2H3doRWjNFRP0uFiwWqI=; h=X-YMail-OSG:Received:X-Rocket-MIMEInfo:X-Mailer:Message-
ID:Date:From:Reply-To:Subject:To:MIME-Version:Content-Type; b=6gkqGHO/xdfaCryJx7qGGJSMhqSeJ09+48EX7N
yOFyN1QsiHh3tIoQbT/w+nBnfl8Cnmo27ewcPDJBjMoWNLiCX+fpOU5RNbc99Mqi4R9PBFqjdZdYJ4wHvCCa0EcKBzAkF6Kq6ttV
h3BplymYHUTrqLC1/JmO5vHcgNy49rLsY=
DomainKey-Signature: a=rsa-sha1; q=dns; c=nofws;
  s=s1024; d=yahoo.com;
  h=X-YMail-OSG:Received:X-Rocket-MIMEInfo:X-Mailer:Message-ID:Date:From:Reply-To:Subject:To:
          MIME-Version:Content-Type;
b=wHlytFUSpap954ttCSq4jud92j+Dp9mlQgZnfXvMTItsaowQFebd6otoKp7Qvha4tzLE3CVWKgQWhuUDIDkcMxOiXiFYULxu
Ds+wAJ9uYTsBBf/XadPXRbpKdTczWKmnL6qFDLH1n1CQh7mBPH6R9xPFFRID/zHUOu6f35jTGdg=;
X-YMail-OSG: oh0wTqAVM1n43_fmfoWs1unYe5Mls7nrE6rOUkM3.V_e3wS
 .M0r5espzRJ8_xdg4k8eFPlrUYQQev.u1Fz2QyAnvoxS.P7RhQEtamaHIZSF
 w1ZGafT5hnmVNLyr7nMN8vwtmnz_2NZWqkdu1xg2Dt_vVQF.oSYsEs2GwvTs
 JmU67ziZn58KhneVqWEpFnieuhd_C0bpB78KIqmtriHB4qLOwHX6qrwjkhe1
 XheBNYh0QvKKEGaCR5CPJ34IXNPaYU80GOPtFK5wXuSFTmqLJe9MayiR.T2T
 hdlagn3y8KegfHXolVwTYCG.2NYY_3yXJOjP.AhdV2zun7Dxe8YIaNH0cdOq
 TsJK1WPFy30IyIKlIIgPxuL4mVThAV4TOMh6U8re7XV95XYRqvpJDRmFYt4h
 Sn.EBk6NTDOdt9IkiTjHsWp17JRMo0iUVK9YzpTAXpZwLzyS6NmVFEx7Vt8q
 F_HwQloskgTz7t17Ybsh926LwArBecpcwLv4wSfdfubQAapmblG7I3qX1PQ3
 TA1BAZQutw81qzzDKaMwsUnnRsA--
```

Why has email evolved?

- MIME – richer content
  - works well in sub-networks & within organisations
  - benefits for early adopters
- ESMTP – improved control of SMTP sessions
  - authentication permits mobility
  - benefits for early adopters
- DKIM/SPF
  - (threat of) mandates
  - benefits for early adopters (even the spammers)
- DMARC (“my DKIM/SPF policy is…”)
  - coordination (70% of mailboxes adopted this almost overnight)
  - benefits for early adopters

TCP/IP – the name remains the same

- Compare a classic TCP/IP header from 1990 with what you'll see on the wire today:
  - No IP options (they look like hacking!)
  - MTU discovery (so almost no IP fragments)
  - Carrier Grade NAT
  - Timestamps
  - Window scaling
  - SACK
  - Congestion control (of various interacting kinds)
  - Explicit Congestion Notification
  - Tight windows on RST validity
  - Multipath (deployed in IOS7)
  - All packets in order
  - and all that's before we consider how smart interface cards change how packets look in Wireshark…

Middleboxes – optimise & lose generality!

- The actual ossification issue with TCP/IP is middleboxes
  - many types: NAT, firewalls, proxies, application gateways, VPNs, load balancers, etc. etc.
- Multi-path TCP designers did lots of tests

  Is it still possible to extend TCP? Honda et al. (2011)

  - MP_CAPABLE options removed from SYN packets (14%)
  - servers cannot initiate sub-flows (because clients behind NATs)
  - Initial sequence numbers rewritten (10%)
  - “holes” in TCP data blocks further transmission (11%)
  - ACKs not passed on if data not seen (33%)
  - middleboxes will re-segment data (as will hardware at sender!)
  - NATs can rewrite content (e.g. FTP IP addresses)

Conclusions

- In my SHIM6 paper I recommended that RFCs for new protocols should have an “economic considerations” section (c.f. security)
- Ozment & Schechter have a good template for this:
  1. global mandate
  2. partial mandate
  3. bundling complements
  4. facilitate sub-network adoption
  5. coordination
  6. subsidization
- It is lazy to claim that it’s the installed base that’s the problem, or that nothing ever changes in key protocols
  - but optimising today’s traffic may damage tomorrow’s
- TAKEAWAY: it’s all about incentives – why should people want to use your protocol rather than an alternative (or nothing)

It’s the Economics, Stupid!

http://www.lightbluetouchpaper.org

UNIVERSITY OF CAMBRIDGE
Computer Laboratory