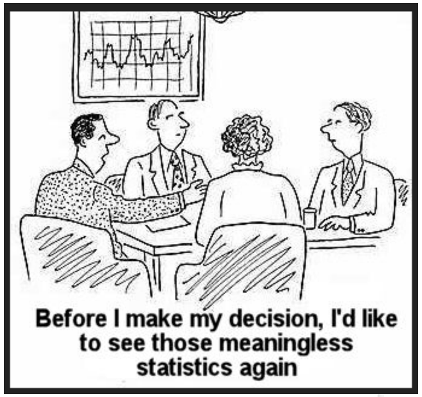
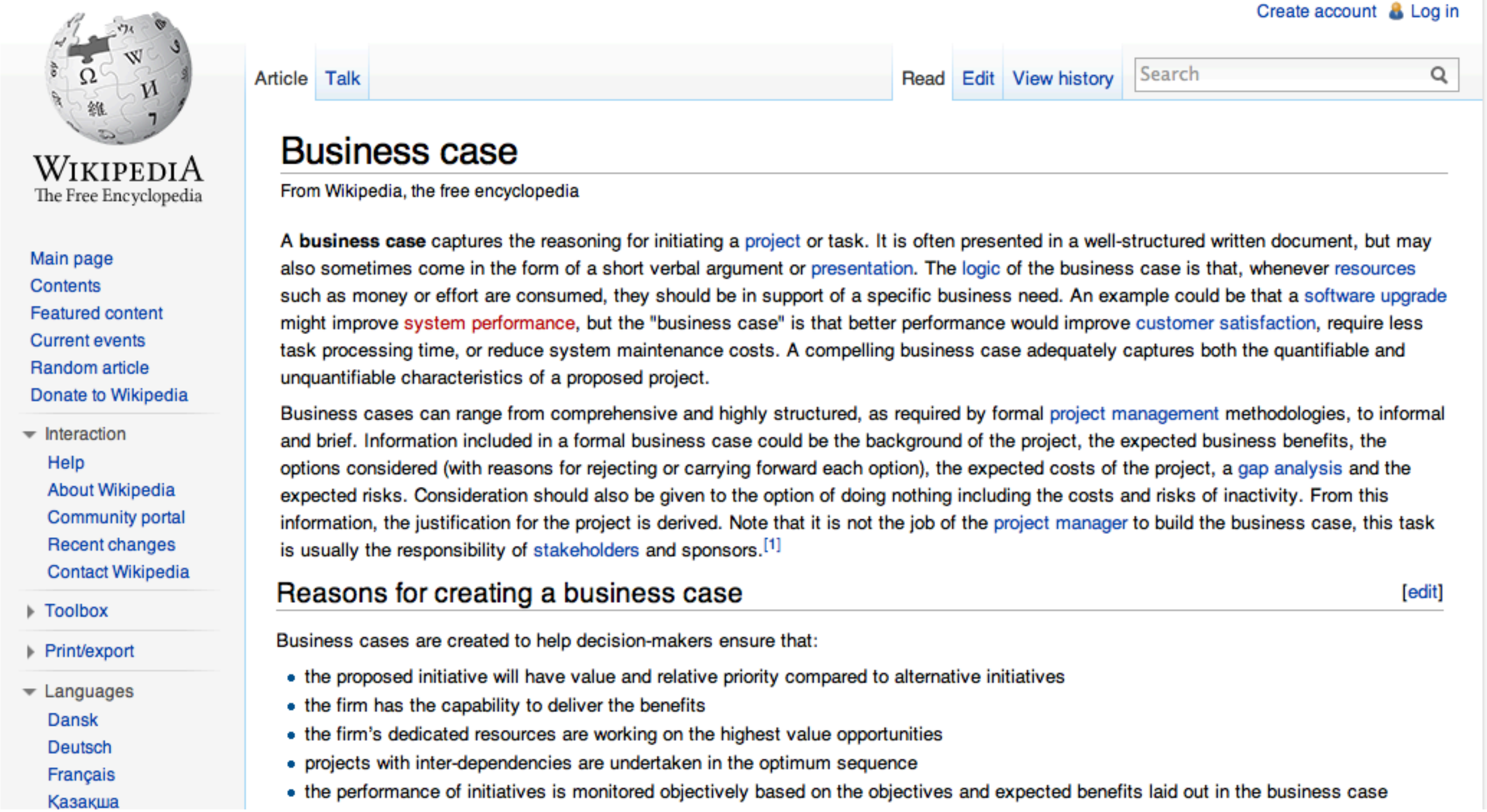
The Business Cases for IPv6 & DNSSEC

A “Business Case”



Before I make my decision, I'd like to see those meaningless statistics again



Business case

From Wikipedia, the free encyclopedia

A **business case** captures the reasoning for initiating a project or task. It is often presented in a well-structured written document, but may also sometimes come in the form of a short verbal argument or presentation. The logic of the business case is that, whenever resources such as money or effort are consumed, they should be in support of a specific business need. An example could be that a software upgrade might improve system performance, but the "business case" is that better performance would improve customer satisfaction, require less task processing time, or reduce system maintenance costs. A compelling business case adequately captures both the quantifiable and unquantifiable characteristics of a proposed project.

Business cases can range from comprehensive and highly structured, as required by formal project management methodologies, to informal and brief. Information included in a formal business case could be the background of the project, the expected business benefits, the options considered (with reasons for rejecting or carrying forward each option), the expected costs of the project, a gap analysis and the expected risks. Consideration should also be given to the option of doing nothing including the costs and risks of inactivity. From this information, the justification for the project is derived. Note that it is not the job of the project manager to build the business case, this task is usually the responsibility of stakeholders and sponsors.[1]

Reasons for creating a business case [edit]

Business cases are created to help decision-makers ensure that:

- the proposed initiative will have value and relative priority compared to alternative initiatives
- the firm has the capability to deliver the benefits
- the firm’s dedicated resources are working on the highest value opportunities
- projects with inter-dependencies are undertaken in the optimum sequence
- the performance of initiatives is monitored objectively based on the objectives and expected benefits laid out in the business case

The Basics of Business

Business is driven by two very fundamental emotional states:

Greed

Where the anticipated return is greater than the investment, and the motivation is to maximize the margins

Fear

Where the absence of investment will erode current returns, and the motivation is to minimize the damage

The Basics of Business

Business is driven by two very fundamental emotional states:

What is the major business driver for iPv6? is it Fear or Greed?

Greed

Where the anticipated return is greater than the investment, and the motivation is to maximize the margins

What about DNSSEC? Fear or Greed?

Fear

Where the absence of investment will erode current returns, and the motivation is to minimize the damage

Lessons from the Past

Why are we discussing this issue of a business case for technology in the context of IPv6 and DNSSEC anyway? As far as I recall it seems that IPv4 never needed a business case!

Economics and Technology

To answer that we need to digress into an examination of macro economics and technology…

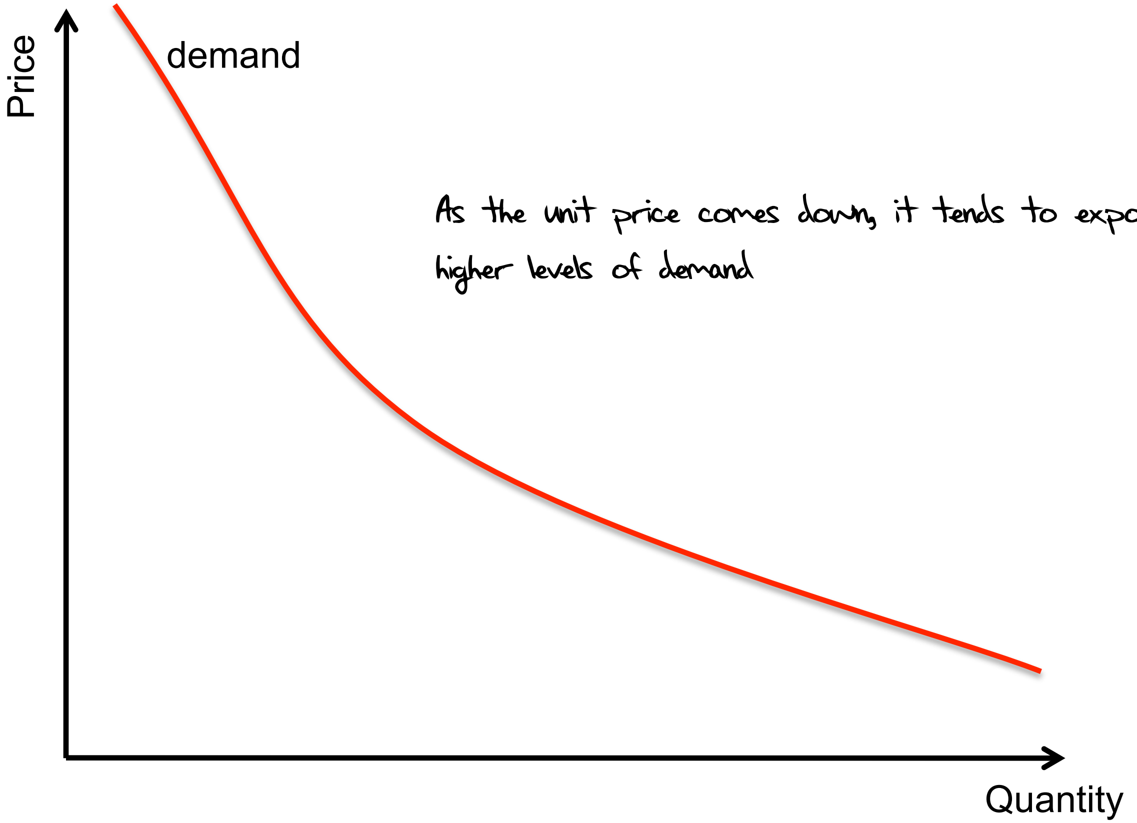
The Rise of the Internet

Technology Shift: From circuit switching to packet switching: transition from network-centric to edge-centric communications model generated displacement leverage

- lower network costs though displacement of functionality and cost to computer-based end systems
- the more flexible service model of a packet-based network exposed a larger set of services that could be replaced by communications-based service models

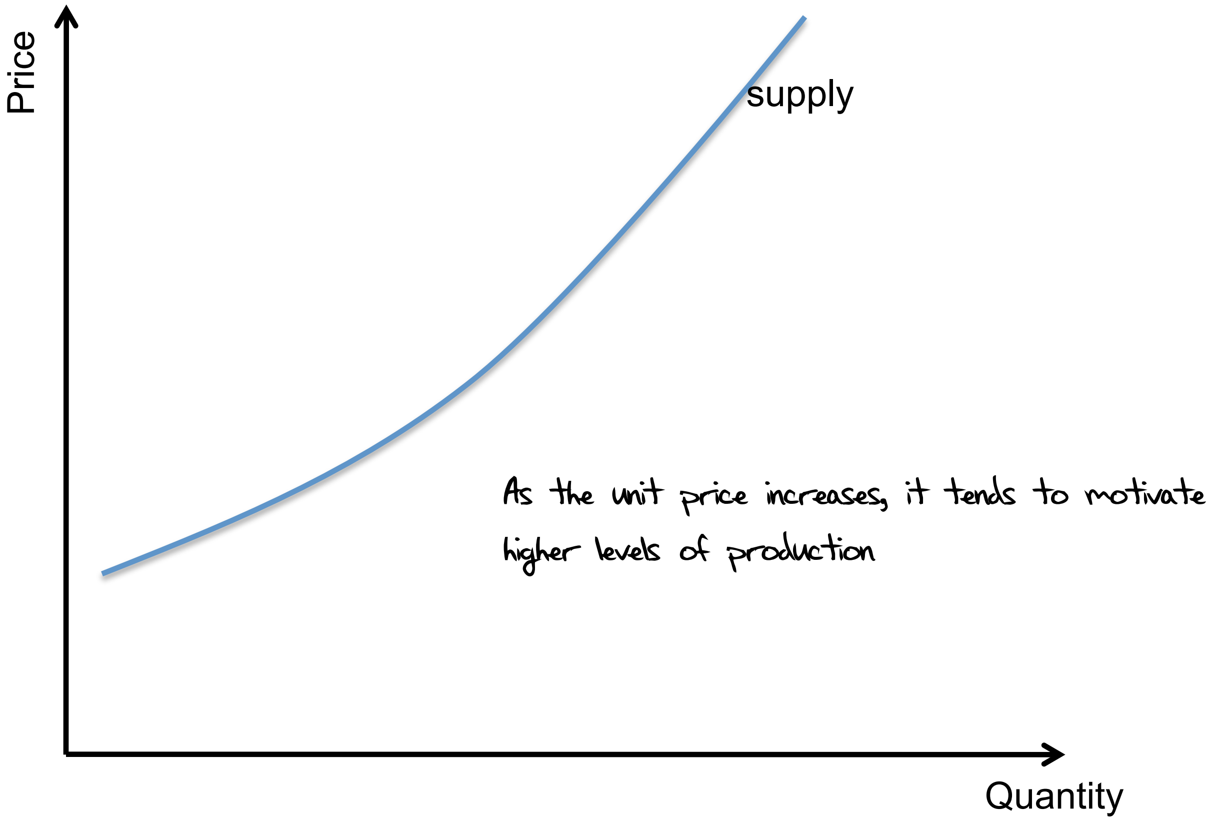
The Demand Schedule

The Demand Schedule: Consumption



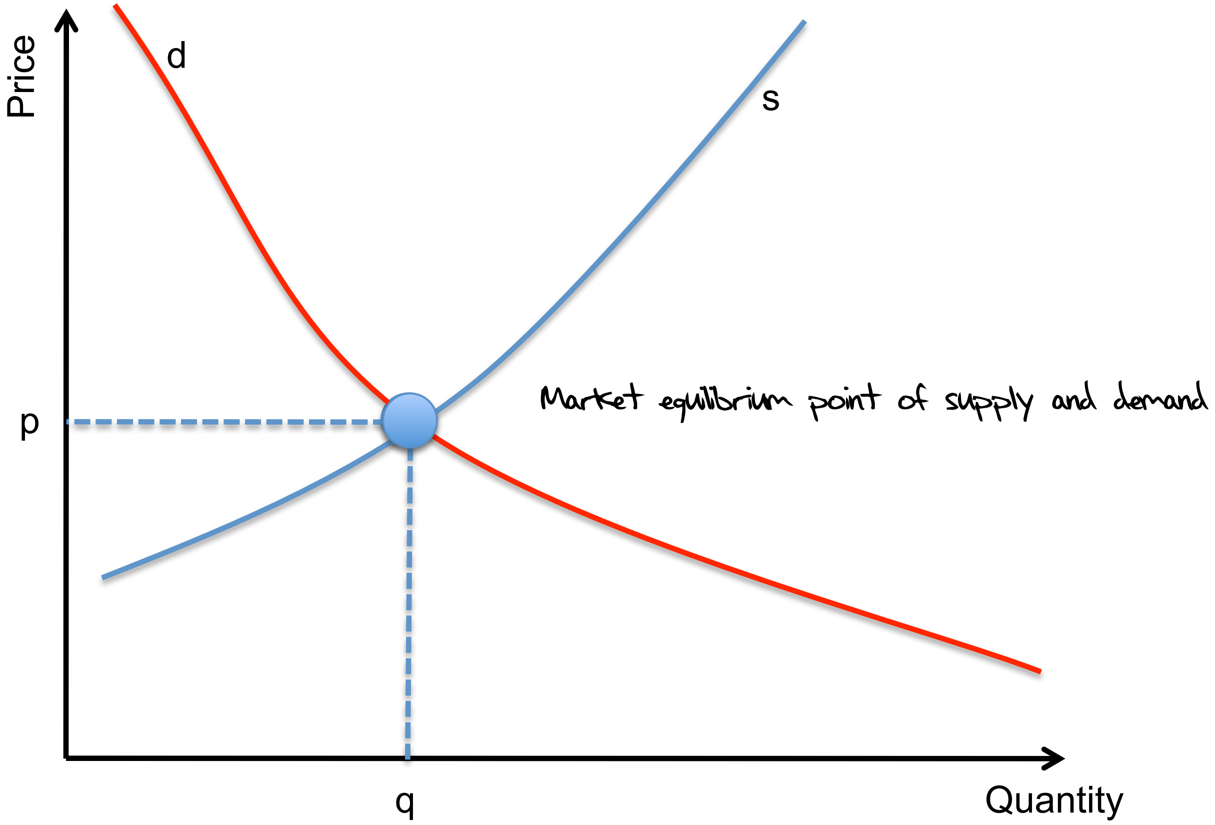
As the unit price comes down, it tends to expose higher levels of demand

The Demand Schedule: Production

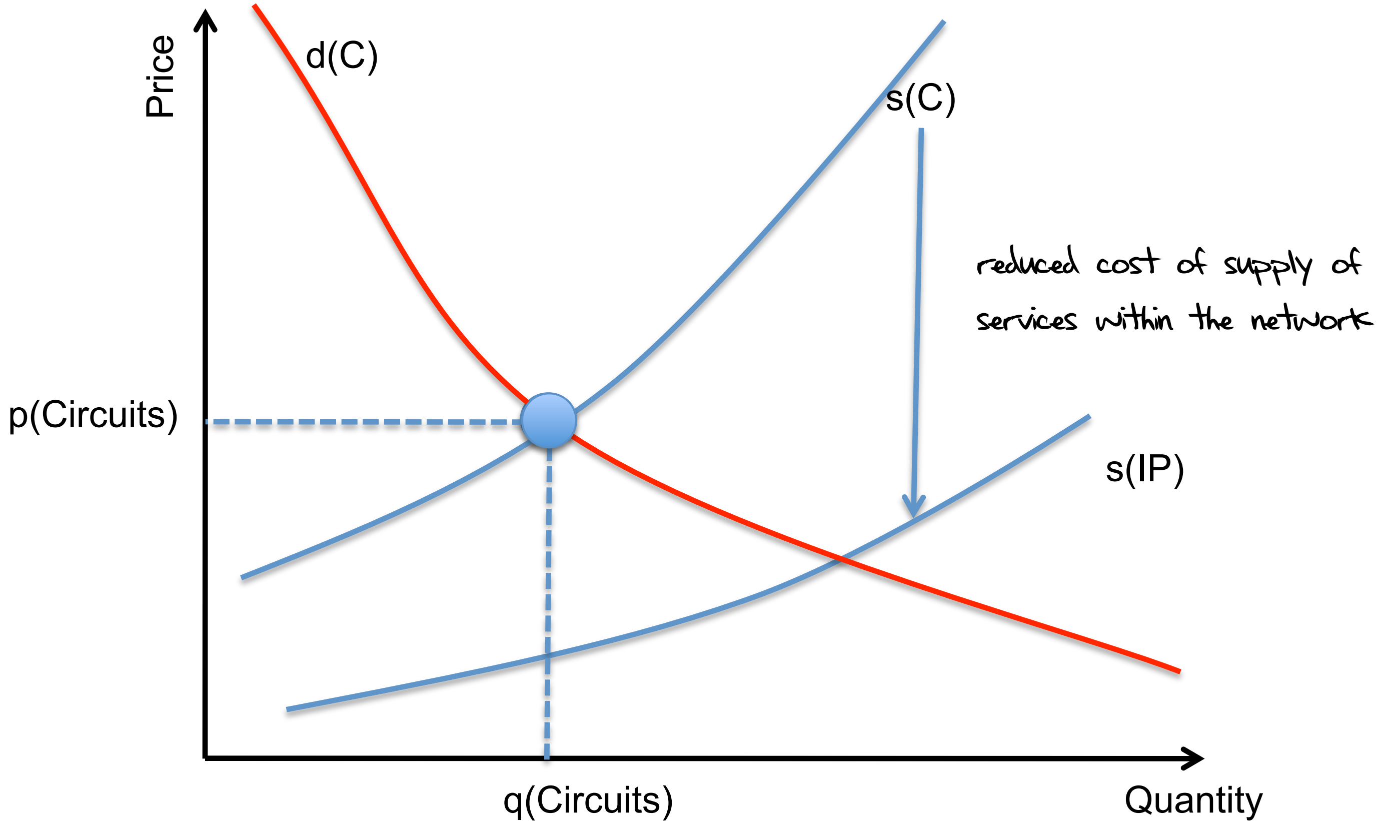


As the unit price increases, it tends to motivate higher levels of production

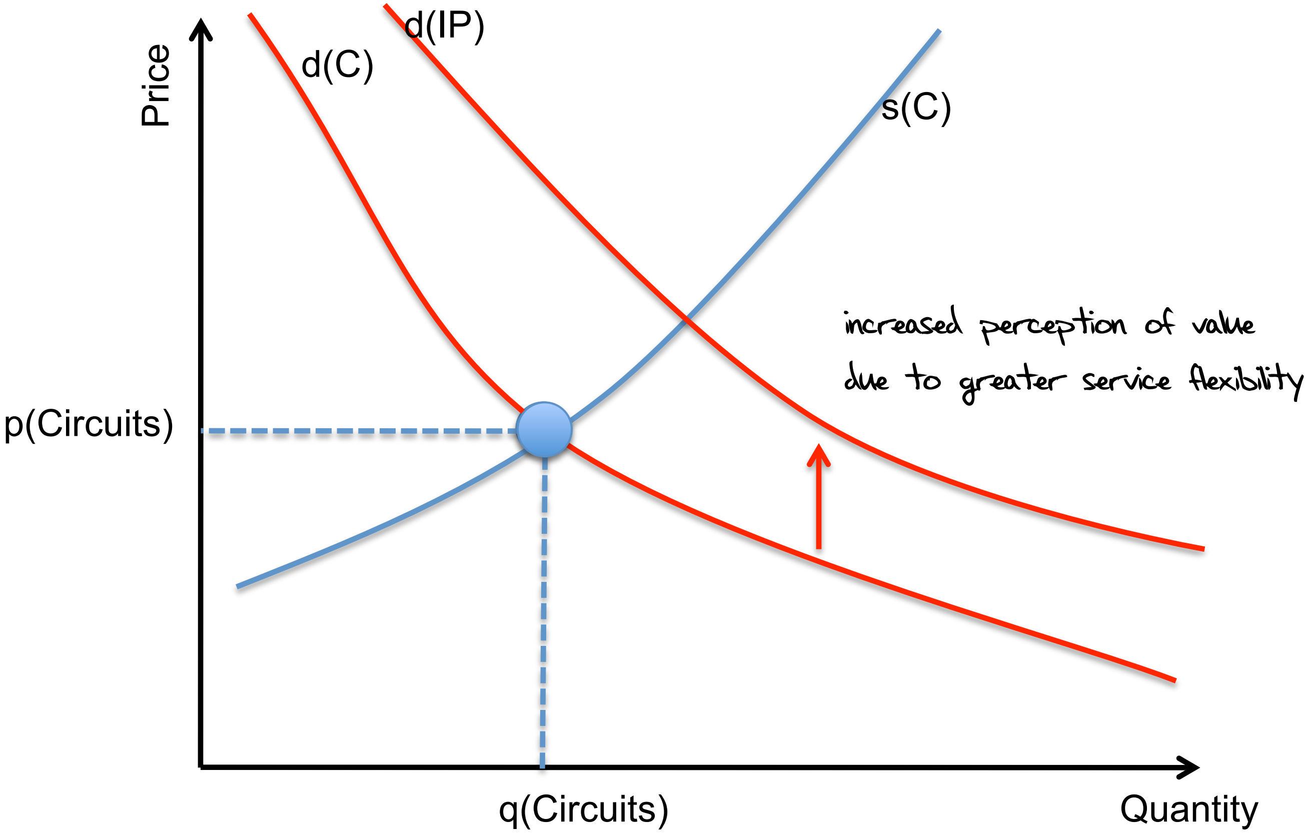
The Demand Schedule: Equilibrium Point



Circuits to Packets: The Demand Schedule Shift

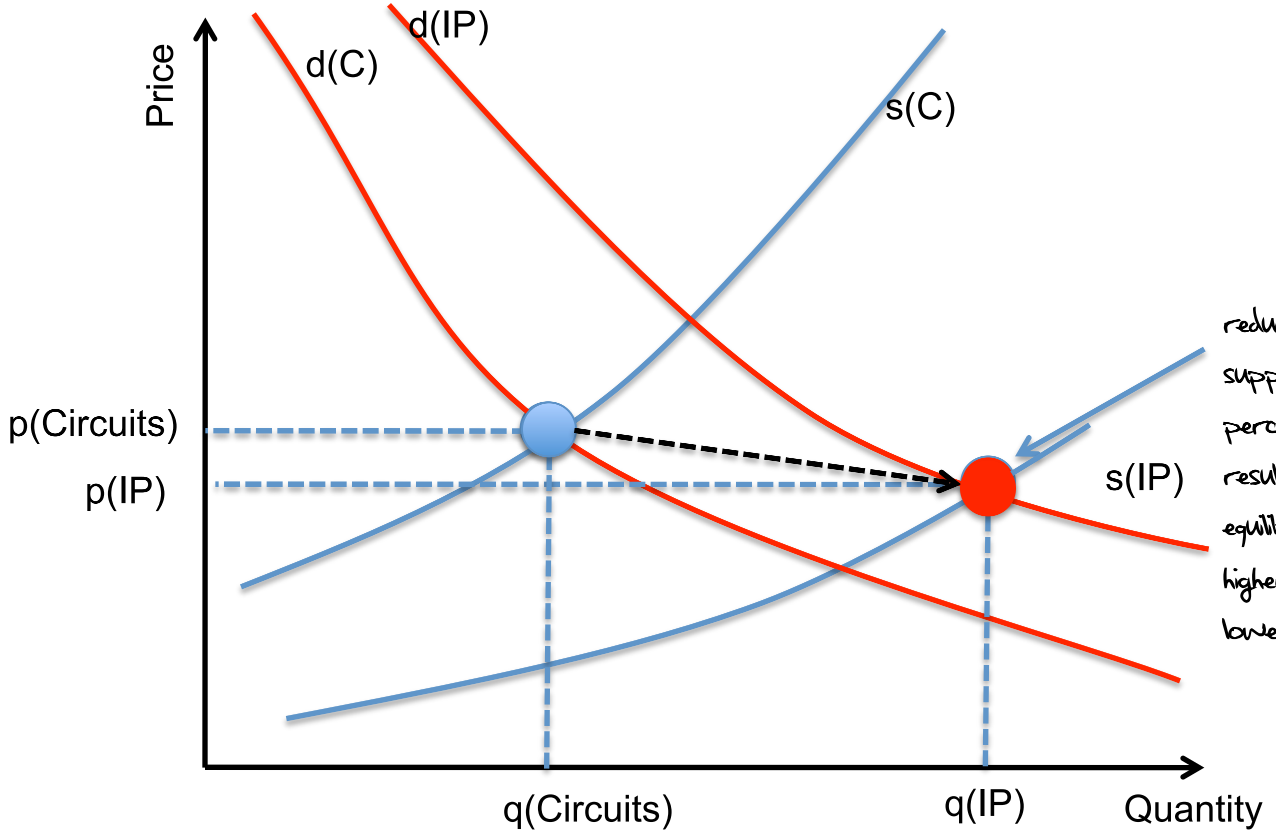


Circuits to Packets: The Demand Schedule Shift



increased perception of value due to greater service flexibility

Circuits to Packets: The Demand Schedule Shift



reduced cost of supply, and increased perception of value, resulting in a new equilibrium point with higher quantity and lower unit price

The Rise of the Internet

Technology Shift: From circuit switching to packet switching

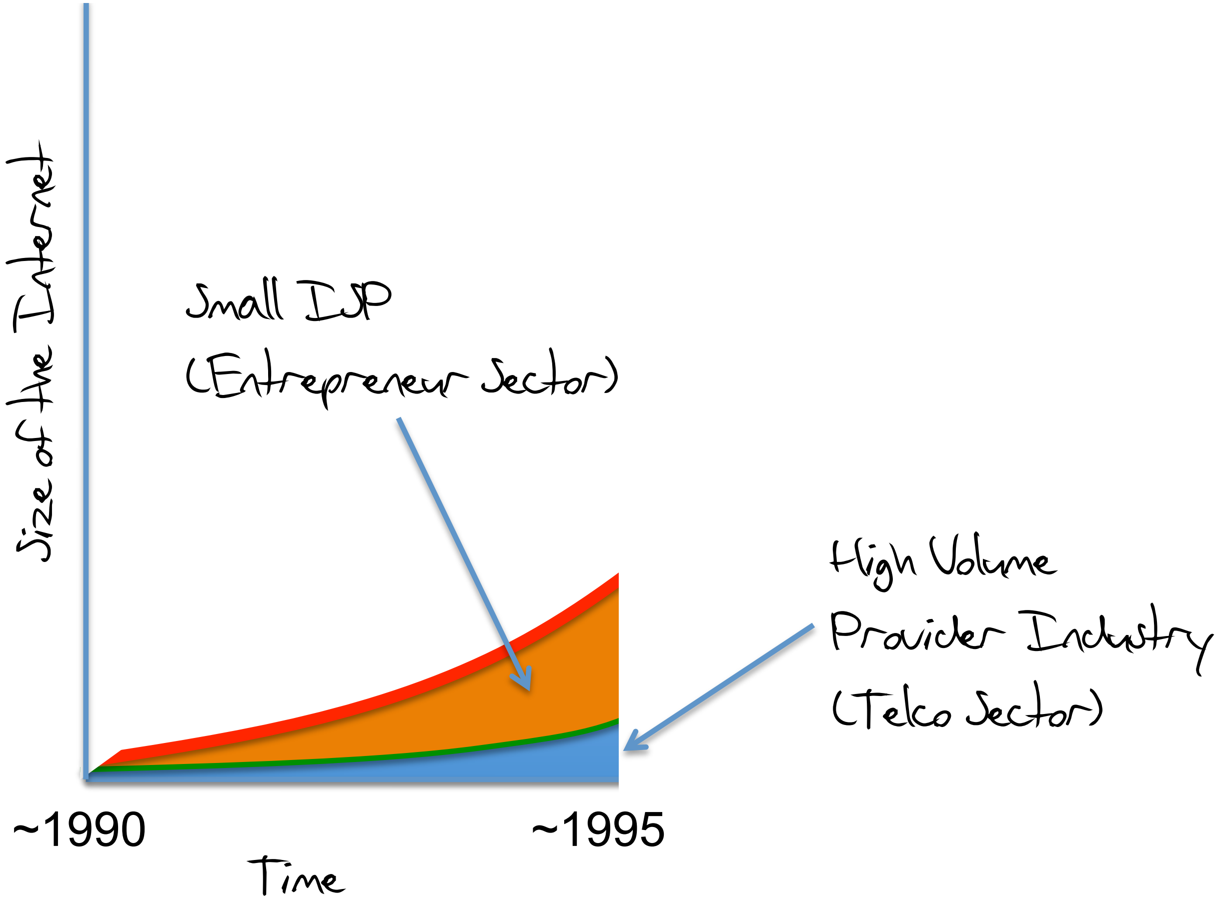
Packet switching is far cheaper than circuit switching. This drop in cost exposed new market opportunities for emergent ISPs

The Rise of the Internet

Business: exposed new market opportunity in a market that was actively shedding many regulatory constraints

- exposed new market opportunities via arbitrage of circuits
  - buy a circuit, resell it as packets
- presence of agile high-risk entrepreneur capital willing to exploit short term market opportunities exposed through this form of arbitrage
- volume-based suppliers initially unable to redeploy capital and process to meet new demand
  - unable to cannibalize existing markets
  - unwilling to make high risk investments

The Rise of the Internet



IPv4 Deployment– First Steps

Greed A small investment by a new entrant could support a service portfolio that has a high perceived value, allowing for a high premium on invested capital

Fear New entrants take market share away from incumbent telcos. Incumbents need to offer similar IP-based services in order to minimize the impact on market share, despite a certain level of unavoidable product cannibalization on their legacy products

The Maturing Internet

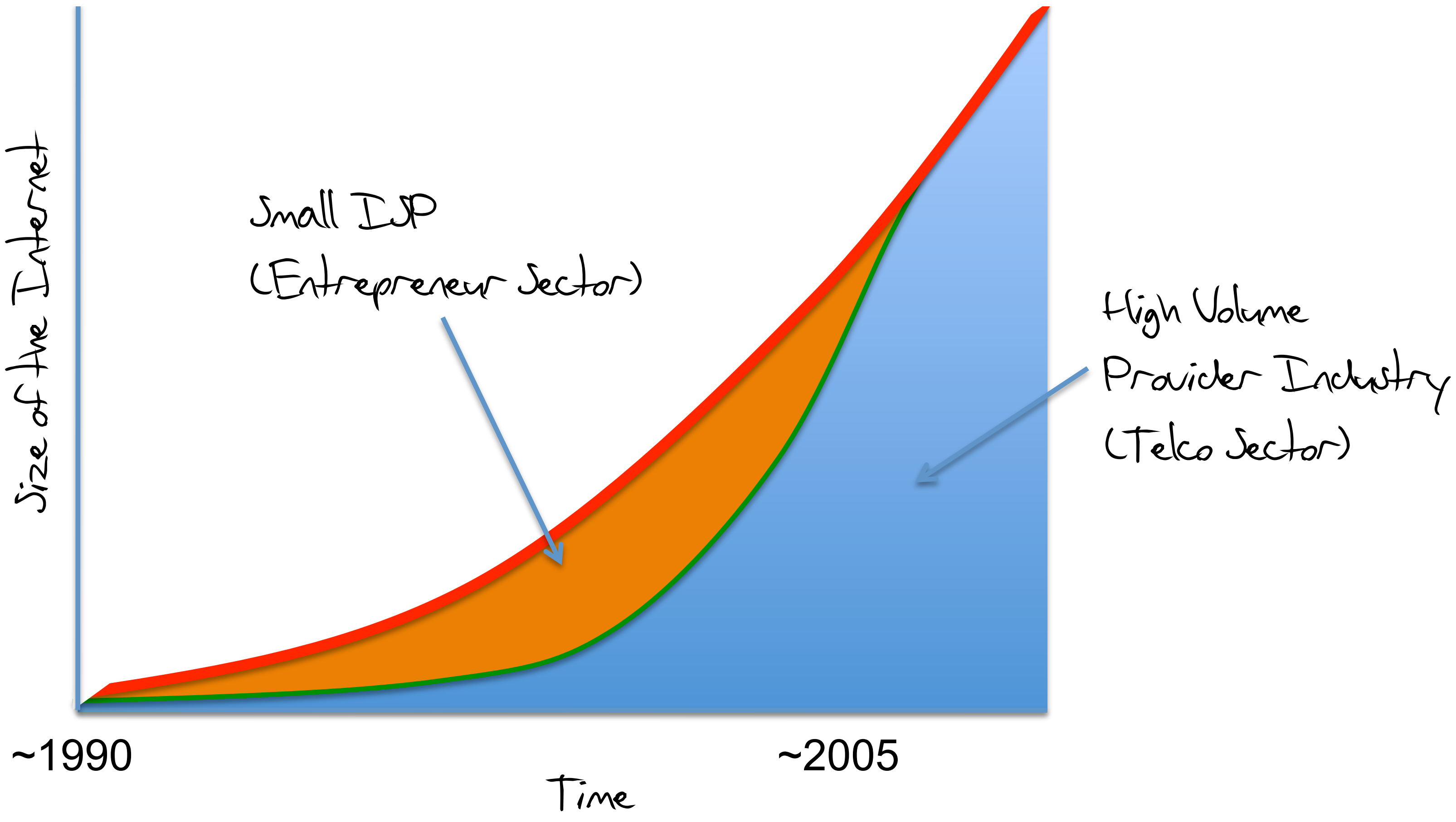
Business: Communications is a volume-dominated activity: higher service volumes tend to drive down the unit cost of service supply

The maturing Internet market represented an opportunity for large scale investment that could operate on reduced cost bases through economies of scale

The Maturing Internet

Maturity: This is a market dominated by volume-based economics. As the market matures the novelty premium disappears, and the market reverts to a conventional volume-based characteristics where the smaller players are squeezed/bought out

IPv4 Deployment



But that was then

And this is now 2013!

And we are looking at the business case for IPv6 deployment!

What about IPv6 Deployment?

Will the same technology, cost and regulatory factors that drove the deployment of the IPv4 Internet also drive this industry through the transition from IPv4 to IPv6?

What about IPv6 Deployment?

- Will the same technology, cost and regulatory factors that drove the deployment of the IPv4 Internet also drive this industry through the transition from IPv4 to IPv6?

Will Greed work for iPv6?

IPv6 vs IPv4

Are there *competitive differentiators*?

✗ no cost differential

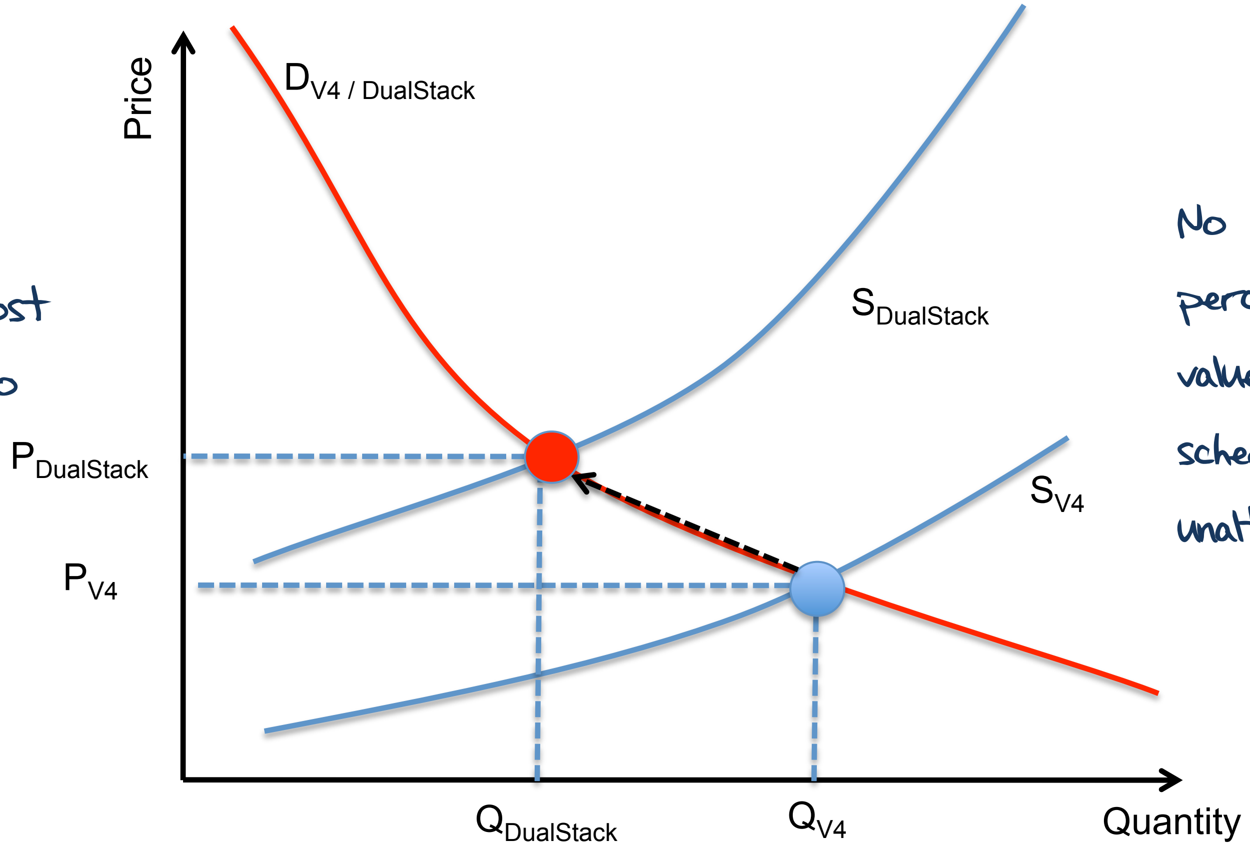
✗ no functionality differential

✗ no inherent consumer-visible difference

✗ no visible consumer demand

IPv4 to Dual Stack: The Demand Schedule Shift

Supply side cost increase due to Dual Stack operation



No change in perception of value, so demand schedule is unaltered

Equilibrium point is at a lower quantity if Dual Stack supply costs are passed on to customers

IPv6

- It won’t make production costs any cheaper – and it may make them slightly higher
- It won’t reduce your customer support loads – and it may make then higher
- It won’t make your network more resilient – it may make the customer experience worse
- It won’t allow you to avoid large scale use of NATs in IPv4

What about IPv6 Deployment?

- Will the same technology, cost and regulatory factors that drove the deployment of the IPv4 Internet also drive this industry through the transition from IPv4 to IPv6?

Will Greed work for iPv6?

What about IPv6 Deployment?

- Will the same technology, cost and regulatory factors that drove the deployment of the IPv4 Internet also drive this industry through the transition from IPv4 to IPv6?

Will Greed work for iPv6?

NO!

What about the Business Case for IPv6?

Its hard to sell incumbent service providers a business strategy involving a quarter-by-quarter expense to improve the strategic outlook over a 5 – 10 year period

Some buy it – its called “the evangelist” business plan, or the “20%” plan

But most have not

And that really should be cause for concern

What is the underlying business driver for IPv6?

future risk.

(and we’re pretty bad at quantifying risk!)

© Bettmann Collection/ Corbis

And the future risk is…

We have no idea how to build the Internet through the coming decade without IPv6 at its foundation *

We have no idea how to scale up the Internet to a network with some 50 – 100 billion connected devices if we have to make intense use of NATS and still preserve the basic attributes of scale, flexibility, security, efficiency and utility

* Actually we don't have all that good an idea of how to do this even with IPv6, but we feel more confident that we can make something work if we have a coherent IP layer at the foundation of the network

The Case for IPv6

It’s all about what made the Internet so disruptive in the first place:

openness

accessibility

permissionless innovation

role specialization

competition

The Case for IPv6

These factors do not necessarily advantage one incumbent over another

But these factors have already facilitated highly valuable new market entrants:

- social nets
- mobility
- grid and cloud
- app innovators
- streaming video
- data analytics

The Case for IPv6

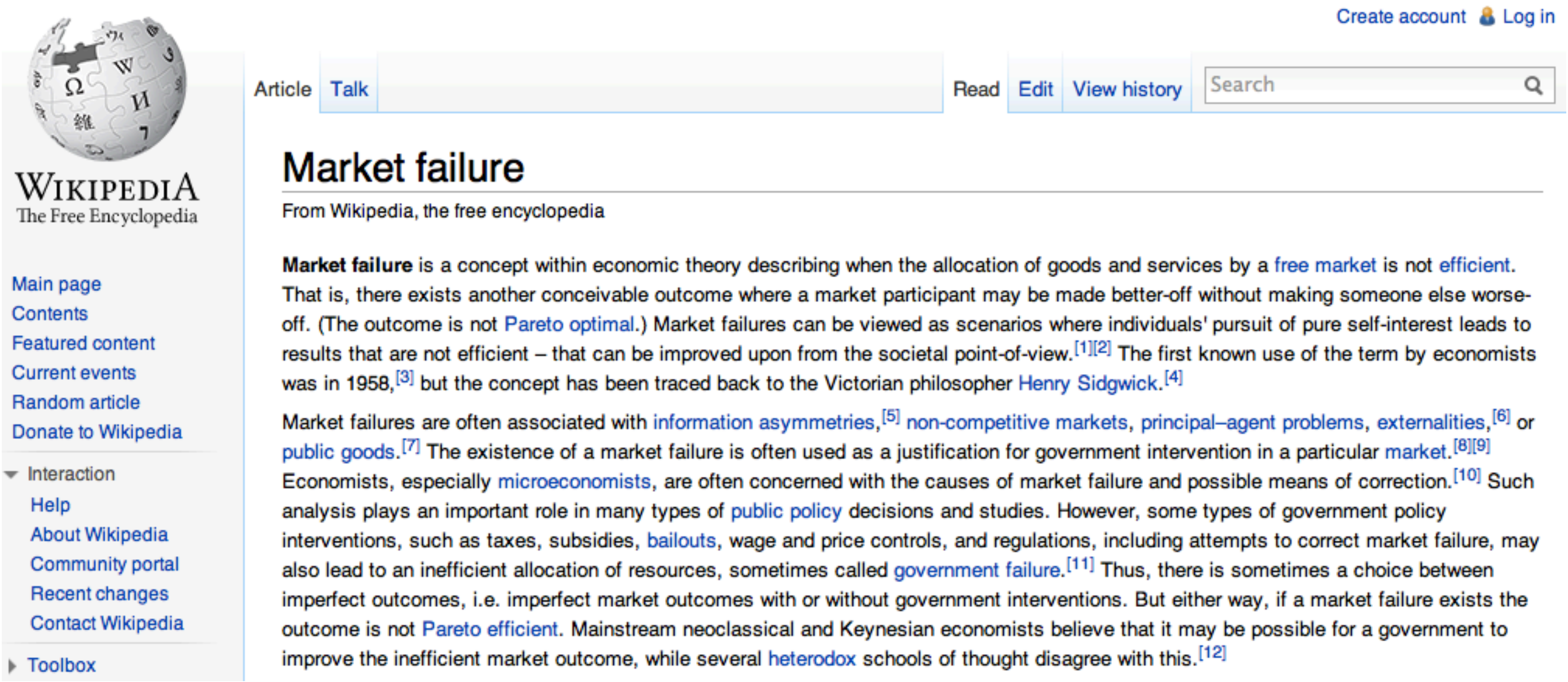
Who benefits:

- ~~The Incumbent Provider?~~
- The Consumer? ✓

The Transition to IPv6

So if there is no immediate benefit to incumbents who elect to deploy IPv6, then in economic terms is this transition an instance of a *market failure*?

“Market Failure”



Market failure

From Wikipedia, the free encyclopedia

Market failure is a concept within economic theory describing when the allocation of goods and services by a free market is not efficient. That is, there exists another conceivable outcome where a market participant may be made better-off without making someone else worse-off. (The outcome is not Pareto optimal.) Market failures can be viewed as scenarios where individuals' pursuit of pure self-interest leads to results that are not efficient – that can be improved upon from the societal point-of-view.[1][2] The first known use of the term by economists was in 1958,[3] but the concept has been traced back to the Victorian philosopher Henry Sidgwick.[4]

Market failures are often associated with information asymmetries,[5] non-competitive markets, principal–agent problems, externalities,[6] or public goods.[7] The existence of a market failure is often used as a justification for government intervention in a particular market.[8][9] Economists, especially microeconomists, are often concerned with the causes of market failure and possible means of correction.[10] Such analysis plays an important role in many types of public policy decisions and studies. However, some types of government policy interventions, such as taxes, subsidies, bailouts, wage and price controls, and regulations, including attempts to correct market failure, may also lead to an inefficient allocation of resources, sometimes called government failure.[11] Thus, there is sometimes a choice between imperfect outcomes, i.e. imperfect market outcomes with or without government interventions. But either way, if a market failure exists the outcome is not Pareto efficient. Mainstream neoclassical and Keynesian economists believe that it may be possible for a government to improve the inefficient market outcome, while several heterodox schools of thought disagree with this.[12]

Really?

Is this IPv6 transition really so hard?

Or is it a collective complacency of the form "we'll move when we have to, but not necessarily until we have to"?

The stories from providers who have provisioned IPv6 is largely positive: low incremental cost, little disruption, no significant service impact

The business case for IPv6 need not be rocket science

The business case for IPv6 need not be rocket science

B ut it does require you to think for yourself, and not just copy your competitor's inaction!

What about DNSSEC?

Why DNSSEC?

The DNS only just works

- that it works at all is a modern miracle!

So why make the DNS

- slower
- a LOT more complex to operate
- more fragile
- more expensive?

What about DNSSEC?

What’s the Business Case for **security**?

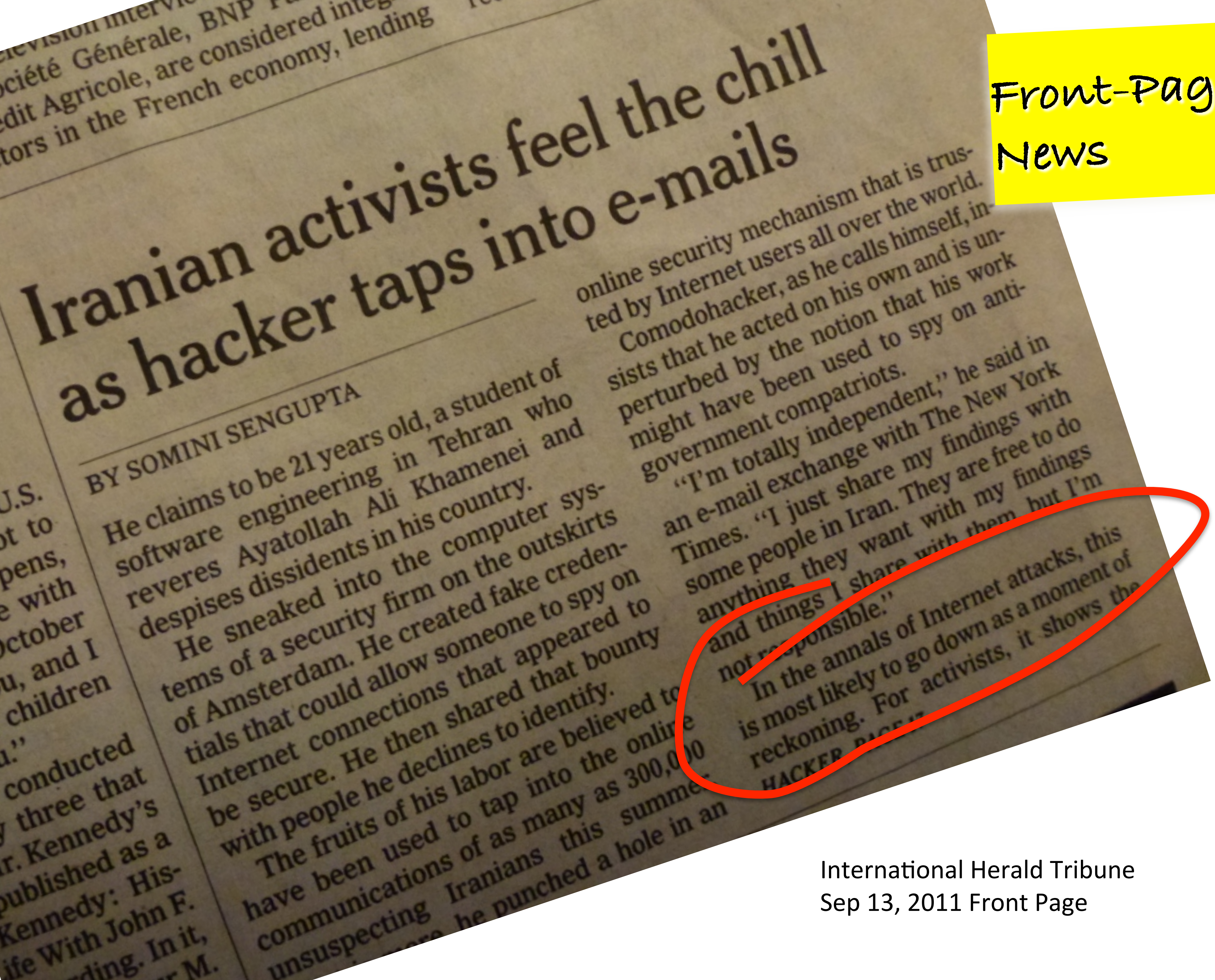
- – If you are an online bank its easy – it’s core business
- – If you are a customer its hard
  - Because its hard to value ephemeral risk
  - And good security often runs counter to simplicity and ease of use
    - – Customers prefer passwords

Why DNSSEC?

Simple:

- The DNS is highly vulnerable to malicious and insidious attack
- And the paraphenalia of today's network security (SSL) has been proved to be highly vulnerable to relatively unsophisticated attacks
- If we were able to secure the DNS we could leverage that to improve the situation with SSL and related service security measures

Front-Page News



...elevision intervie...
...ociété Générale, BNP Pa...
...edit Agricole, are considered integ...
...tors in the French economy, lending

...U.S.
...ot to
...pens,
...e with
...October
...u, and I
...children
...u."
...conducted
...y three that
...r. Kennedy's
...published as a
...Kennedy: His-
...ife With John F.
...ding. In it,
...r M.

Iranian activists feel the chill as hacker taps into e-mails

BY SOMINI SENGUPTA

He claims to be 21 years old, a student of software engineering in Tehran who reveres Ayatollah Ali Khamenei and despises dissidents in his country.

He sneaked into the computer systems of a security firm on the outskirts of Amsterdam. He created fake credentials that could allow someone to spy on Internet connections that appeared to be secure. He then shared that bounty with people he declines to identify.

The fruits of his labor are believed to have been used to tap into the online communications of as many as 300,000 unsuspecting Iranians this summer. [illegible] he punched a hole in an online security mechanism that is trusted by Internet users all over the world.

Comodohacker, as he calls himself, insists that he acted on his own and is unperturbed by the notion that his work might have been used to spy on antigovernment compatriots.

"I'm totally independent," he said in an e-mail exchange with The New York Times. "I just share my findings with some people in Iran. They are free to do anything they want with my findings and things I share with them, but I'm not responsible."

In the annals of Internet attacks, this is most likely to go down as a moment of reckoning. For activists, it shows the

HACKER, PAGE 17

International Herald Tribune
Sep 13, 2011 Front Page

How Did This Happen?

- Because the hierarchy of domain name registration is disconnected from domain name security
  - Your browser has no idea of WHICH Domain Name Certificate Authority to trust to validate a domain name certificate
    - So its trusts them all!
    - And that's not good
    - Because some CA's are not very well secured
    - And get hacked
    - And are used to mint forged certificates
    - For ANY domain name

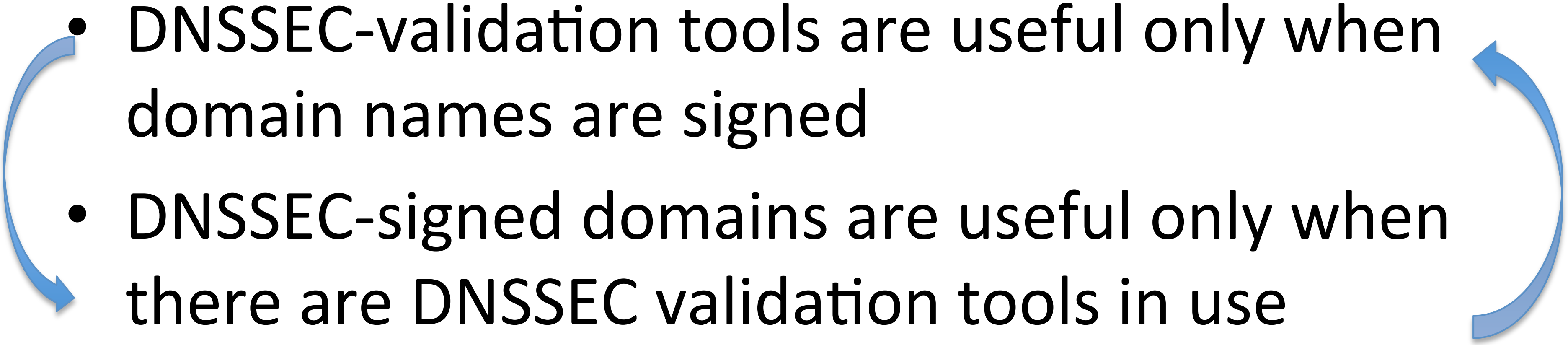
How can we fix this?

- The class of exploit works because certificate validation is independent of domain name resolution
  - The implicit trust model necessarily involves a leap of faith
  - And “trust” and “leap of faith” are conventionally seen as antonyms
- So a robust “fix” should add validation into domain name resolution
  - Which inevitably leads to DNSSEC
  - That allows domain name certificates to be securely placed into a signed DNS (DANE)

Why DNSSEC?

- For clients: avoid being duped or misled through malicious use of forged Domain Name certificates
- For domain name holders: raise the threshold for the attacker

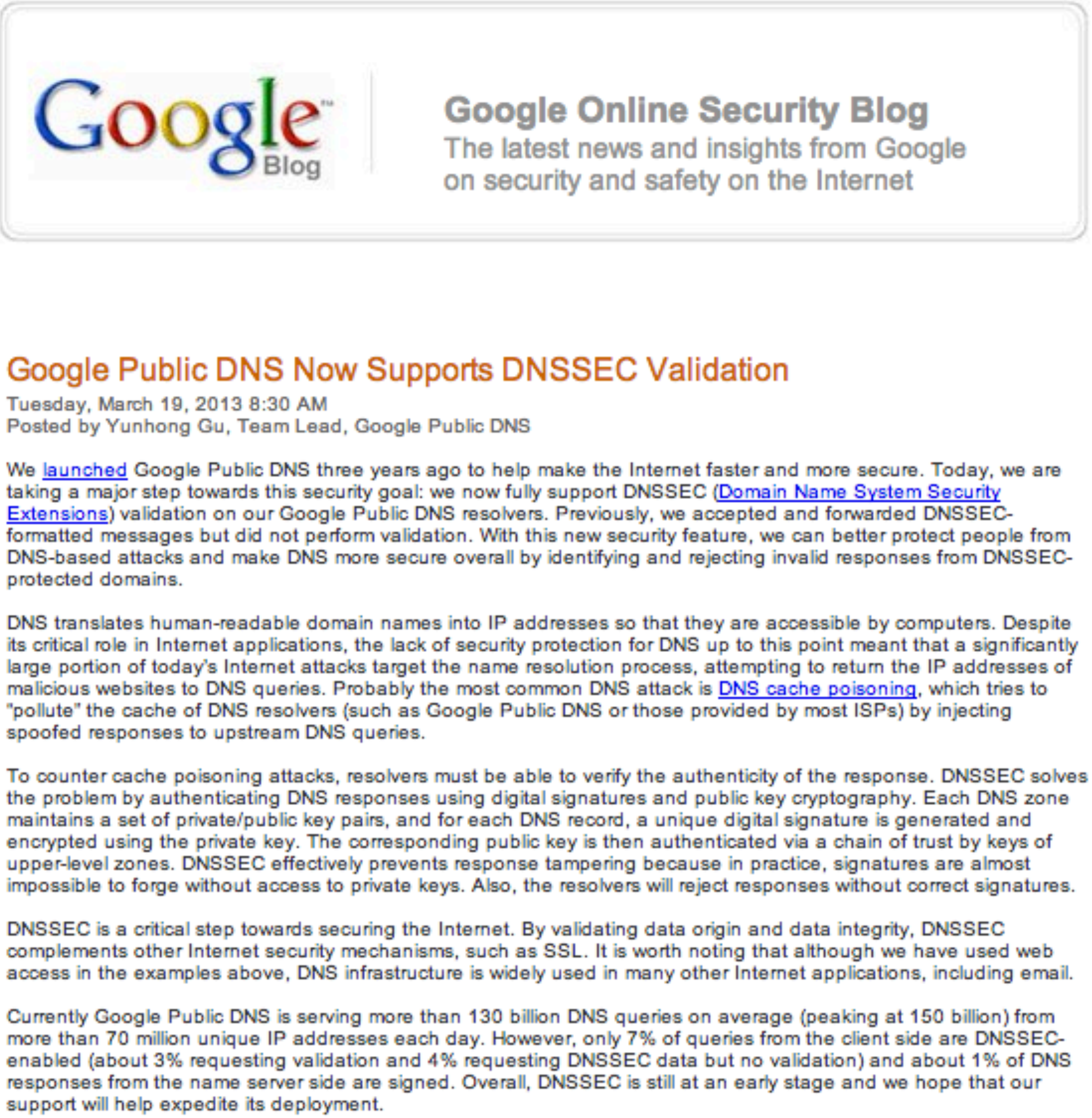
From Here to There



- DNSSEC-validation tools are useful only when domain names are signed
- DNSSEC-signed domains are useful only when there are DNSSEC validation tools in use

What changes this deadlock?

A circuit breaker?



Google Online Security Blog
The latest news and insights from Google
on security and safety on the Internet

Google Public DNS Now Supports DNSSEC Validation

Tuesday, March 19, 2013 8:30 AM
Posted by Yunhong Gu, Team Lead, Google Public DNS

We launched Google Public DNS three years ago to help make the Internet faster and more secure. Today, we are taking a major step towards this security goal: we now fully support DNSSEC (Domain Name System Security Extensions) validation on our Google Public DNS resolvers. Previously, we accepted and forwarded DNSSEC-formatted messages but did not perform validation. With this new security feature, we can better protect people from DNS-based attacks and make DNS more secure overall by identifying and rejecting invalid responses from DNSSEC-protected domains.

DNS translates human-readable domain names into IP addresses so that they are accessible by computers. Despite its critical role in Internet applications, the lack of security protection for DNS up to this point meant that a significantly large portion of today's Internet attacks target the name resolution process, attempting to return the IP addresses of malicious websites to DNS queries. Probably the most common DNS attack is DNS cache poisoning, which tries to "pollute" the cache of DNS resolvers (such as Google Public DNS or those provided by most ISPs) by injecting spoofed responses to upstream DNS queries.

To counter cache poisoning attacks, resolvers must be able to verify the authenticity of the response. DNSSEC solves the problem by authenticating DNS responses using digital signatures and public key cryptography. Each DNS zone maintains a set of private/public key pairs, and for each DNS record, a unique digital signature is generated and encrypted using the private key. The corresponding public key is then authenticated via a chain of trust by keys of upper-level zones. DNSSEC effectively prevents response tampering because in practice, signatures are almost impossible to forge without access to private keys. Also, the resolvers will reject responses without correct signatures.

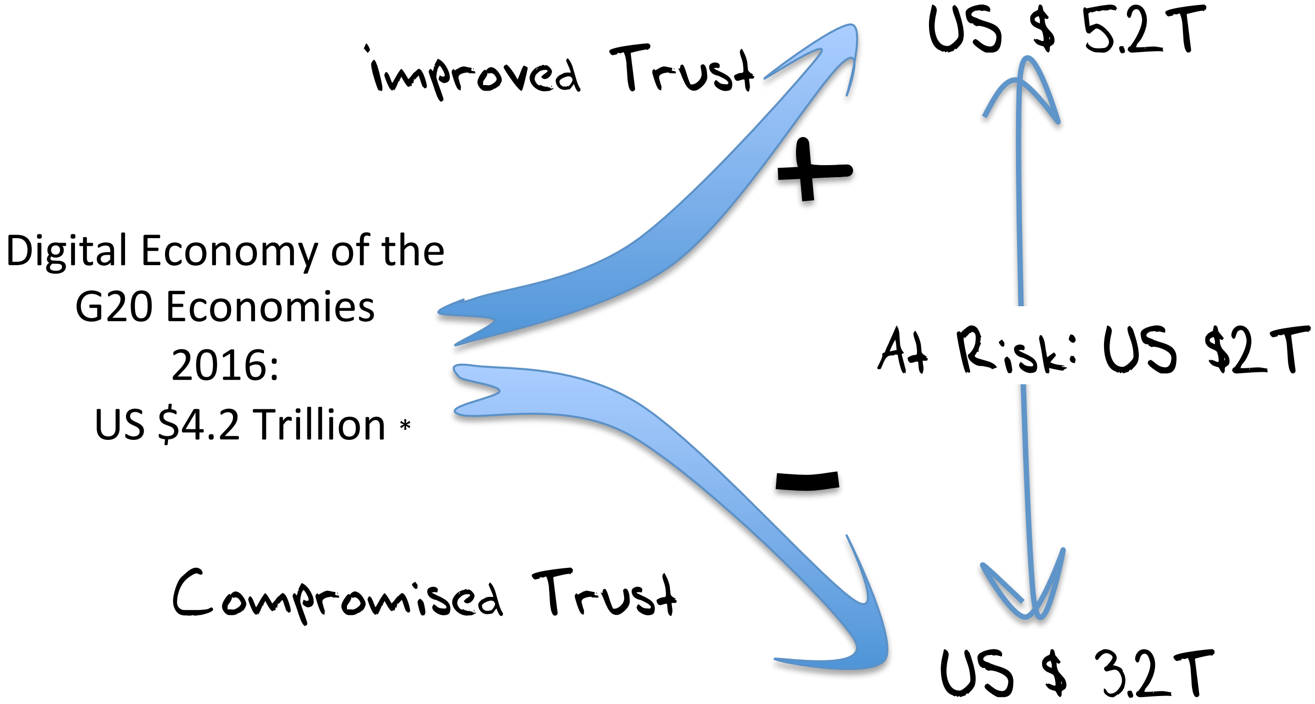
DNSSEC is a critical step towards securing the Internet. By validating data origin and data integrity, DNSSEC complements other Internet security mechanisms, such as SSL. It is worth noting that although we have used web access in the examples above, DNS infrastructure is widely used in many other Internet applications, including email.

Currently Google Public DNS is serving more than 130 billion DNS queries on average (peaking at 150 billion) from more than 70 million unique IP addresses each day. However, only 7% of queries from the client side are DNSSEC-enabled (about 3% requesting validation and 4% requesting DNSSEC data but no validation) and about 1% of DNS responses from the name server side are signed. Overall, DNSSEC is still at an early stage and we hope that our support will help expedite its deployment.

What’s the Business Case for DNSSEC?

What’s the Business Case for security and trust in the Internet?

The Worldwide Digital Economy in 2016



Digital Economy of the G20 Economies 2016: US $4.2 Trillion *

* Boston Consulting Group, January 2012

The Case for DNSSEC

Are there *competitive differentiators*?

- ✗ higher cost
- ✗ more complex operation
- ✗ no overt consumer-visible difference
- ✗ no visible consumer demand

The Case for DNSSEC

Are there *competitive differentiators*?

- ✗ higher cost
- ✗ more complex operation
- ✗ no overt consumer-visible difference
- ✗ no visible consumer demand

But:

- ✓ this is the only way we know to secure the operation of the DNS in the face of known exploitation vectors
- ✓ Securing the name infrastructure then allows us to improve the a suite of security tools that are triggered by name-based rendezvous mechanisms

Thank You!

Questions?