Network Neutrality and the IETF

Mark Handley

Why should the _IETF_ care about Network Neutrality?

- An economic and legal issue.
    - IETF doesn't do this well.

- Both sides of the debate present here.
    - IETF can't take sides.

- Issues are different in different countries.
    - IETF must be international.

Tussle in Cyberspace
Clark, Wroclawski, Collins & Braden, SIGCOMM 2002

- "*different stakeholders that are part of the Internet milieu have interests that may be ad-verse to each other, and these parties each vie to favor their particular interests. We call this process 'the tussle'.*"

- "*accommodating this tussle is crucial to the evolution of the network's technical architecture*"

Design for Tussle

"*There is no such thing as value-neutral design*."

- – The choices made by designers shape the Internet, the motivations of the players, and the potential for distortion of the architecture.

"*Don't assume you design the answer.*"

- – You are designing a playing field, not the outcome.

Designing the Playing Field?
An Example

SIP, circa 1996:
- Simple invitation protocol designed around proxies needed for user location.
- We deliberately didn't specify what proxies did, beyond what was needed for interop.

SIP, circa 2009:
- Proxies uses for all manner of intermediation, billing, etc.
- Proxies provide the control point that allows the tussle between the ends and the middle to play out *within* the architecture.

Net Neutrality:
Our playing field?

- Stuck between deep packet inspection, and innovation-inhibiting regulation.

Net Neutrality:
What's the problem?

- Blocking, rate-limiting or prioritizing traffic to or from certain destinations.

- Blocking, rate-limiting or prioritizing traffic from certain applications.

Destination Neutrality

- Not normally an IETF issue.
  - Expressiveness of BGP policies?

- Security
  - We don't have a proper story regarding DDoS defense or spam prevention.
  - Such a story would likely involve technical mechanisms that are not net-neutral.

Destination Neutrality

- In some places, governments dictate some destinations should be blocked.
  - Illegal content.
  - Political reasons.

- Not clear these are technical issues.
  - Technology is used to work around the blocks though.

Application Neutrality

- This is firmly in scope for the IETF.
- The rest of this talk is about this.

It's all just packets

- No, and hasn't been for a long time.
    - RSVP/Intserv
    - Diffserv
    - Firewalls
    - DPI and Traffic shapers
    - VPN prioritization

Question

- Have we provided the right building blocks to allow network operators to manage their networks effectively?

Technical Issues

Broadly, operators control traffic to manage:

– Security

– Congestion

We must provide the tools to do this effectively.

A vicious cycle.

- VoIP and games compete with P2P traffic and lose.
- ISPs use DPI to spot P2P and rate limit it.
- P2P becomes port-agile, encrypted, stealthy.
- DPI gets smarter, makes heuristic inferences from traffic patterns.
- ISPs use DPI to prioritize known "friendly" traffic.
- Innovation becomes hard - needs to look like "friendly" traffic.
- P2P traffic tries to look "friendly".
- DPI needs to get even smarter.
- Strong temptation to use expensive DPI infrastructure for "business optimization".

DPI

- Common in UK, some other countries.
- Not commonplace yet in US, Germany, …

- Seems to be more common where cost pressures are greatest.
  - UK: very competitive market for home broadband.

Outcomes

- Either we end up with a network where innovation can only be within narrow bounds, constrained by yesterday's common applications,

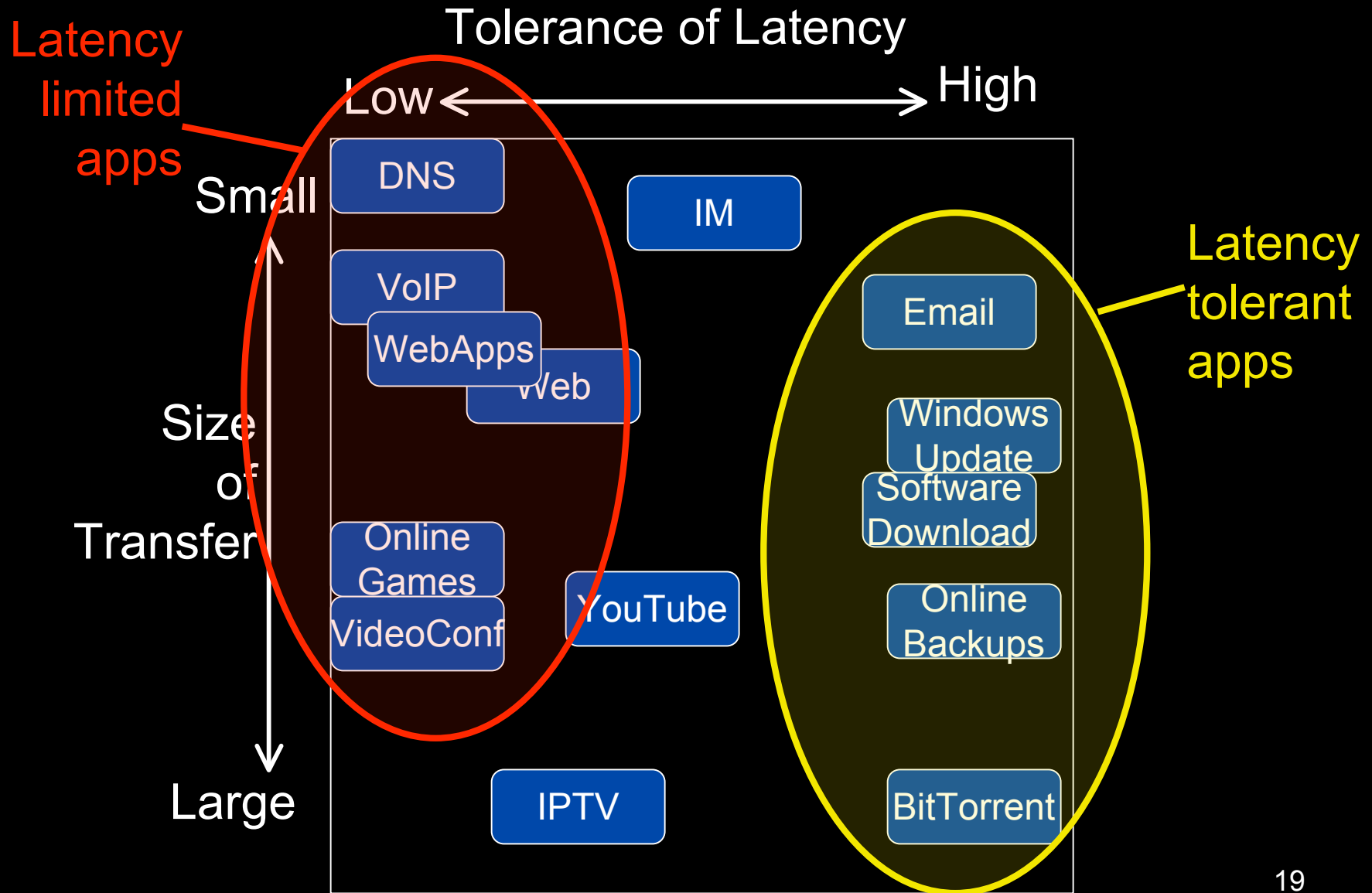- Or the regulators eventually step in and prohibit broad classes of traffic prioritization.

Timely

- It isn't just P2P.
- Internet TV is already taking off.
    - Won't be long before time-synchronous TV broadcast will be obsolete for everything except sport.
    - My 8-year old son watches more TV on the BBC's iPlayer than he watches broadcast TV.
    - Huge shift in usage patterns, but no extra money to pay for carrying the traffic.
- Games, VR, video walls, wearable cameras, ….

Congestion

- TCP-style congestion control has brought us a long way.
  - Prevent congestion collapse
  - Match offered load to available bandwidth

- No longer sufficient, by itself.

Applications

Tolerance of Latency

Latency limited apps

Latency tolerant apps

Low ← → High

Size of Transfer: Small → Large

DNS, IM, VoIP, WebApps, Web, Email, Windows Update, Software Download, Online Games, YouTube, Online Backups, VideoConf, IPTV, BitTorrent

19

Latency, latency and latency

- Traditional TCP-style congestion control and large router buffers:
  Disaster for VoIP, games, etc
  $\Rightarrow$ Need low latency packet forwarding

- Large file transfers (eg BitTorrent, software download, Flikr upload) very latency tolerant.
  – Prioritize short web transfers, and everyone would be happier.

But…

- Giving low latency using DPI is deeply flawed.

- Conflict between privacy and service
  - VoIP over IPsec should work properly.
- Arms race of masquerading apps and detectors.
- Lock in to today's apps.

The sky is falling!!!

- No

- But if we don't actively try to address these problems…

- IPTV may force the issue.

What could the IETF do?

Better congestion handling:

- **Multipath TCP**
  - Improve TCP's ability to move traffic away from congested paths.

- **Multi-server HTTP**

- **LEDBAT**
  - Improve the ability of BitTorrent, etc to play nice with low-latency apps.

- Encourage less-than-best-effort diffserv class?

Path Congestion Visibility

- Shaping on application type is a proxy for what ISPs really want to shape on:
    – The congestion caused by an app,
    – vs the value of that app to the customer.

- Re-ECN provides visibility into the former.
    – Allows shaping based on what causes the problem, in an application-neutral way.
    – Enabler for more sane economics of congestion.
- How to capture the value of an app is still open (or even if it should be done)

What could the IETF do?

- Queuing: do we really need $RTT*bw$ of buffering in routers?
  - No, except in a very few places.

- DDoS defense.
  - Work on effective mechanisms to shut down unwanted traffic.
  - Re-ECN might help here.

What could the IETF do?

- Should IETF design protocols so that layering is hard to break?
  - Mandating encryption?
  - Making obfuscation & randomization a design feature of protocols?

- Or is it a feature that middleboxes can optimize based on content?

What could the IETF do?

- Your suggestion here…

IETF Goals?

- Mechanisms to handle congestion better.
  - Low latency apps should just work, not need explicit QoS.

- Economics of congestion need to make sense.
  - Theory says charge for congestion.
    - Only then does traffic displace other customers' traffic.
  - But end customers don't want to know.
  - Indirect mechanisms will be needed.

ISPs

- In a very difficult position.
  - Don't have the tools to match costs to revenues within the Internet architecture.

- The IETF must provide those tools in a way that lets the tussle between apps and ISPs play out in different ways in different places.

- Not IETF's place to decide the outcome.

Summary

- Network neutrality is (mostly) an economic problem.

- The IETF has not given the ISPs effective tools to make the economics work properly.

- We must fix this. Otherwise:
  - Bad legislation and architectural stagnation, or
  - Ubiquitous DPI and architectural stagnation.

- Even with effective tools, might still need legislation?

What should the IETF do?

Extra slides

Limitations of TCP-style congestion control

- Application must be elastic.
- Needs external feedback loop
  slower transfer $\Rightarrow$ fewer requests
- Cannot move traffic to uncongested paths.
- Builds queues, imposes latency on competing traffic.
- Implicit signal $\Rightarrow$ no economic feedback for sending too fast.
- Fairness questions.