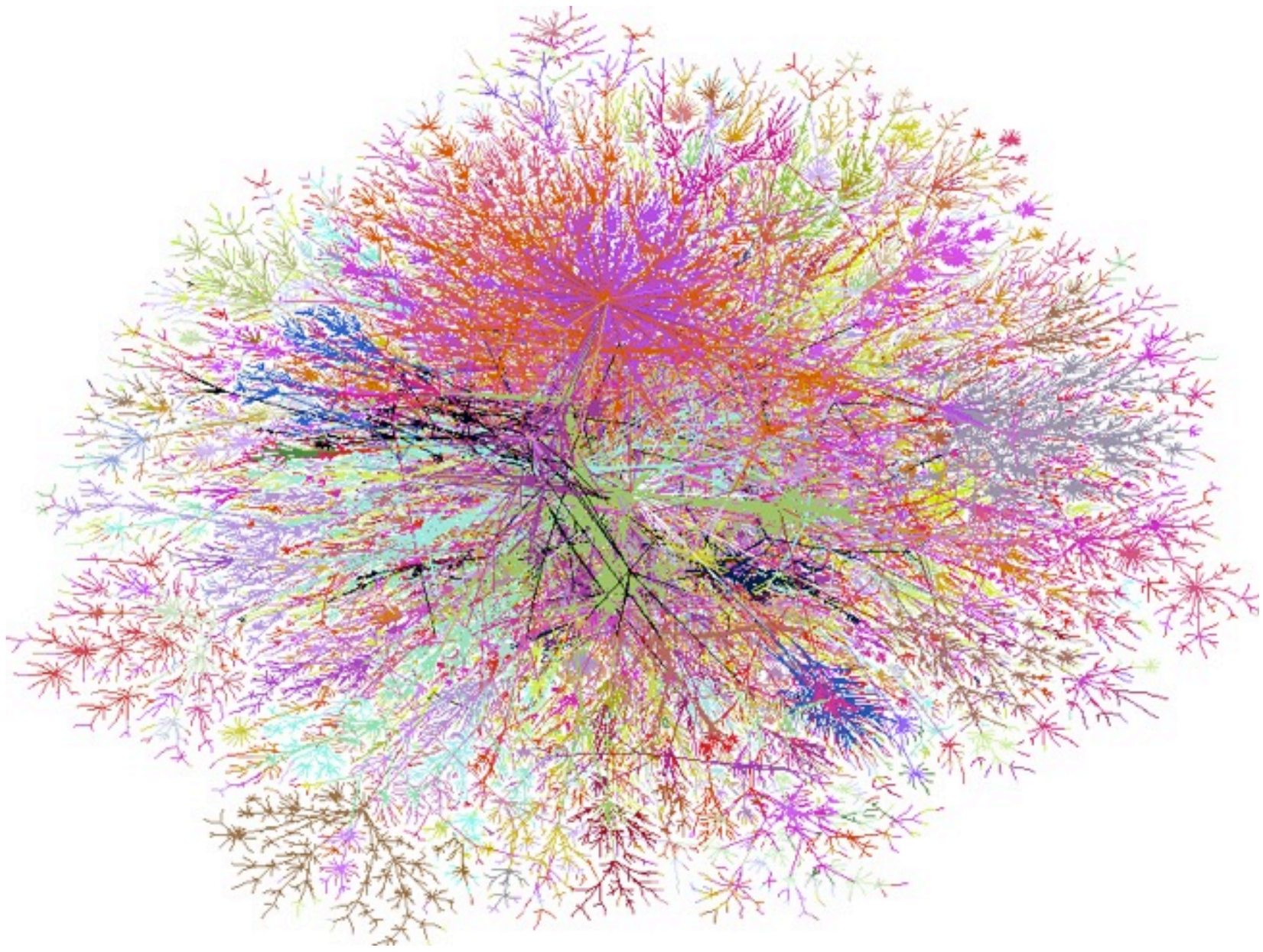
The Internet Spirit

2011-10-11



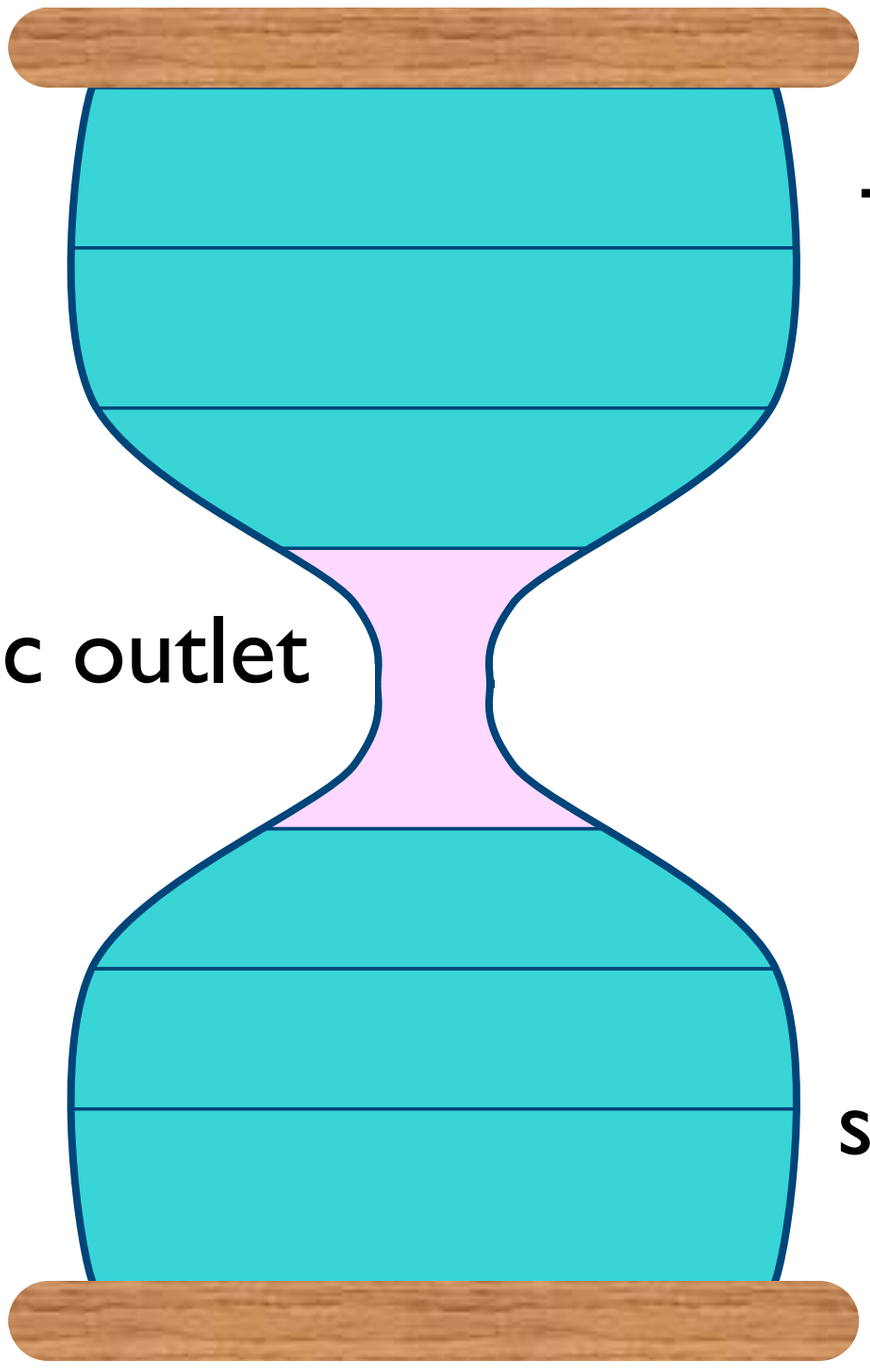
The internet has grown through cooperation and interconnection between countless local networks.

In principle the internet accepts information packets from any source and makes best efforts to deliver them to their destinations.

Electricity Hourglass

electrical devices

TV, microwave, toaster, vacuum cleaner, ...



standard electric outlet

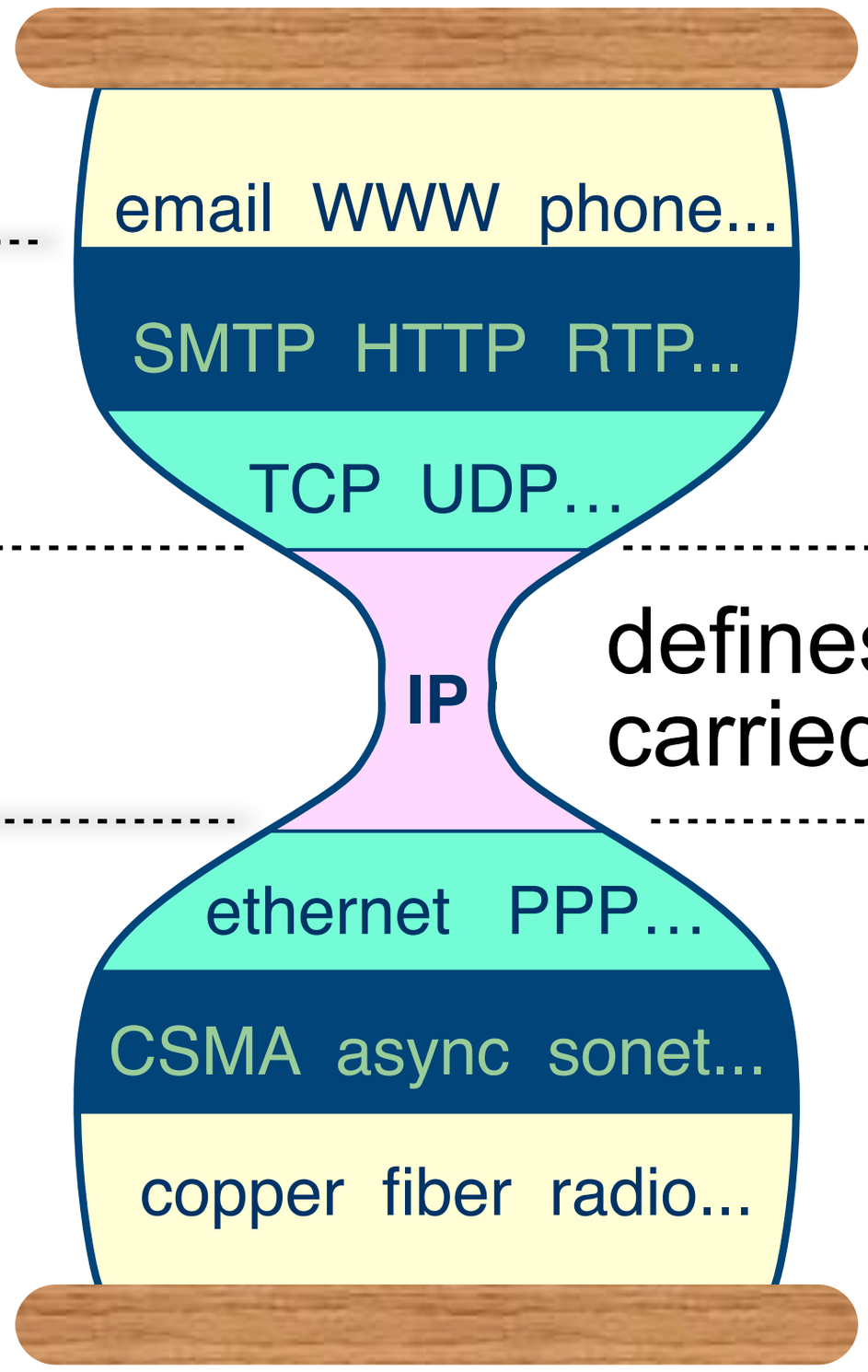
power sources

waterfall, windmill, solar cells, nuclear plants

Saturday, 3 December 2011

- Electric outlet is universal interface between power plants and electric appliances
  - power plants provide 240 V AC to the outlet
  - All devices need plugs that can use current coming from outlet
- Advantages
  - same outlet can be used with any device
  - even ones that haven't been invented! New inventions need only accommodate what the "neck" expects -- plugs. Imagine how inefficient it would be if you had different plugs for each type of appliance! Or different types of wiring for different appliances
- Different countries use different outlets -- makes travelling a pain
- Electric company doesn't know or care if you are using its electricity to do bad things, as long as you pay the bills!

The Internet Hourglass



Steve Deering
IETF London, Aug 2001

Saturday, 3 December 2011

The Internet architecture is also conceptually organized like an hourglass, with the ubiquitous Internet Protocol at the neck, defining the form of the bit packets carried through the network.

A variety of higher level protocols use bit packets to achieve different purposes.

TCP guarantees reliable though possibly delayed message delivery, which is important for text and data.

UDP provides timely but unreliable message delivery (typically used for streaming video).

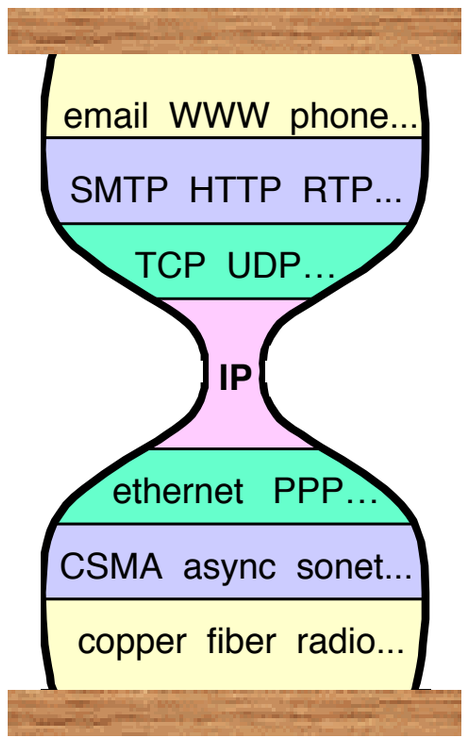
RTP (Realtime transport protocol) also fast, but less reliable (good for things like Skype).

All the higher-level protocols rely on IP to deliver packets.

Once the packets get into the neck of the hourglass, they are handled identically, regardless of the higher-level protocol that produced them.

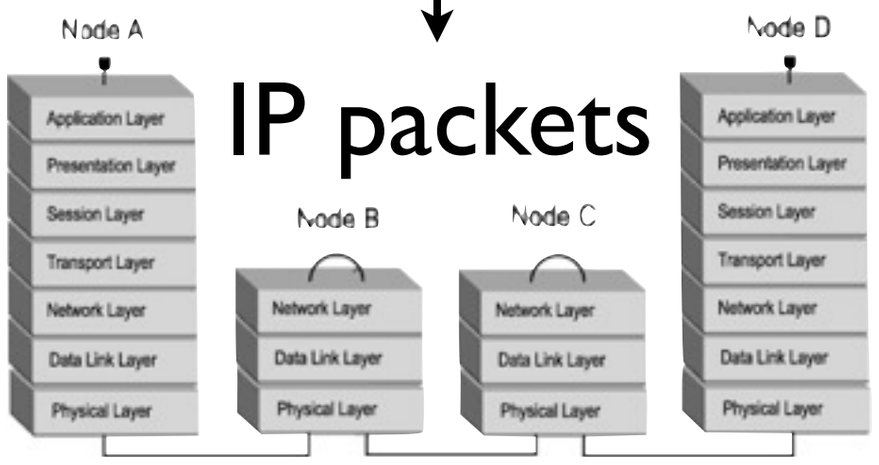
Why the hourglass architecture?

- Why an internet layer?
  - make a bigger network
  - global addressing
  - virtualize network to isolate end-to-end protocols details/changes
- Why a single internet protocol?
  - maximize interoperability
  - minimize number of service interfaces
- Why a narrow internet protocol?
  - assumes least common network functionality to maximize number of usable network



Layers not Silos

mp4 video
jpeg photo
pdf book



In the past there were different industries for processing and communicating different kinds of information. Each industry was an isolated “silo”.

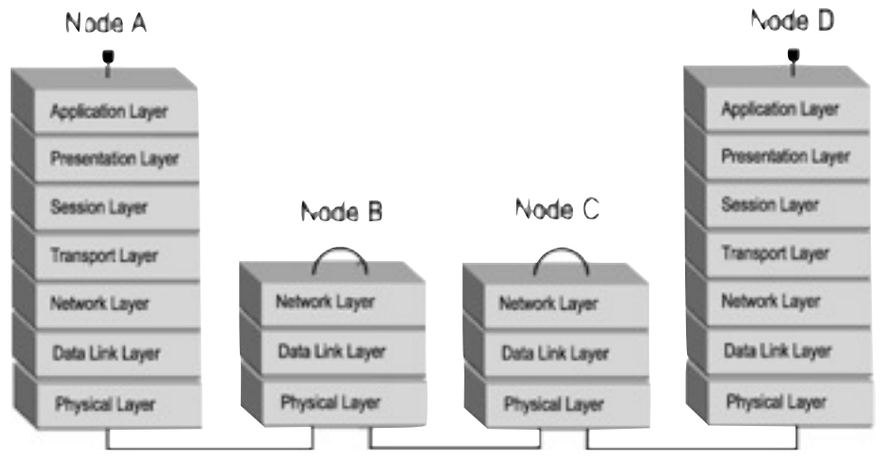
The layered architecture of the internet allows the same infrastructure to serve for all kinds of information.

This allows economies of scale – but it also provides more power for those who control the information highway.

End to End

- Network switches should be "dumb"
  - optimized to carry out single, limited function
  - just deliver packets to the addresses they contain
- Complex functions should be responsibility of higher level protocols and applications

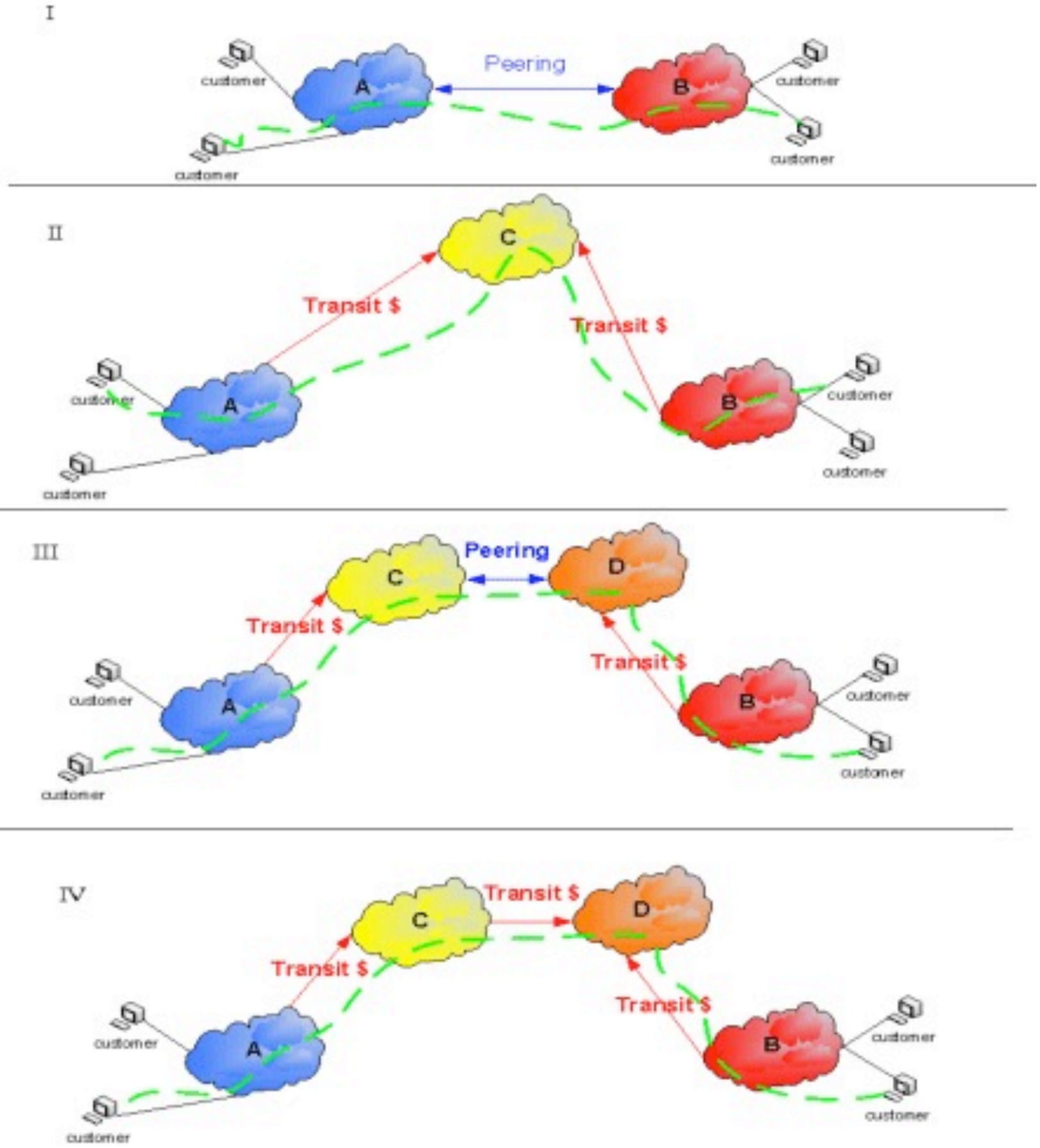
- Advantages:
  - New applications can be added without having to change the core



Saturday, 3 December 2011

Making the network requirements as simple as possible means that we can bring more networks into the internet.

Goods trains are easier to make than lorries and can go faster – they don't need such complex suspension and steering. But they can only run on rails, which are harder to make, and access than roads. Rails require a fixed guage, with precisely engineered wheels. Roads can accommodate vehicles of many different shapes and sizes, with 2 to 20 wheels.



http://arstechnica.com/old/content/2008/09/peering-and-transit.ars

Saturday, 3 December 2011

So far, we haven't talked about money - who pays whom when packets move around the internet?
http://arstechnica.com/old/content/2008/09/peering-and-transit.ars

Customer can be consumers or producers of information – or both at once.

I is simple: both A and B can charge their own customers, and both benefit by connecting to each other. They are equals ('peers'); they exchange traffic gratis 'cos both benefit. This is **peering**.

II is more complex: both A and B pay C for **transit**, the connection provided by C.

III is yet more complex: A and B pay C and D, respectively, for transit, but C and D are equals ('peers'); they exchange traffic gratis 'cos both benefit.

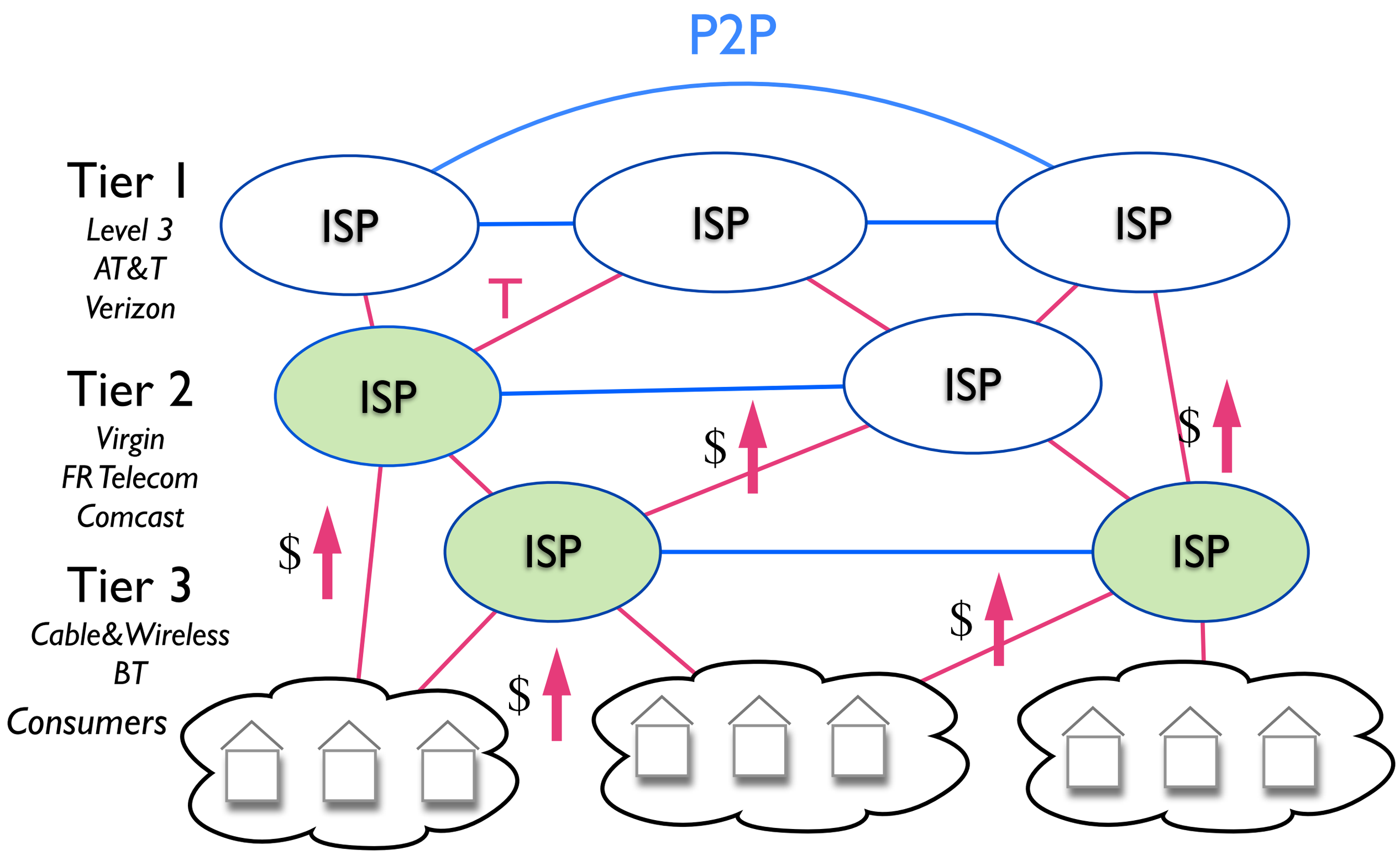
IV the situation in III is unstable: if D is more powerful than C, then D can 'hold C to ransom" and insist on a transit payment, or '**paid peering**'.

- **Peering**: when two or more autonomous networks interconnect directly with each other to exchange traffic. This is often done without charging for the interconnection or the traffic.

- **Transit**: when one autonomous network agrees to carry the traffic that flows between another autonomous network and all other networks. Since no network connects directly to all other networks, a network that provides transit will deliver some of the traffic indirectly via one or more other transit networks. A transit provider's routers will announce to other networks that they can carry traffic to the network that has bought transit. The transit provider receives a "transit fee" for the service.

- The transit fee is based on a reservation made up-front for the number of Mbps. Traffic from (upstream) and to (downstream) the network is included in the transit fee; when you buy 10Mbps/month from a transit provider you get 10 up and 10 down.

http://drpeering.net/AskDrPeering/blog/articles/Ask_DrPeering/Entries/2011/9/6_Access_Power_Peering.html



Saturday, 3 December 2011

An idealised picture of the global internet. Each ISP is an ‘Autonomous System’ – a network that exists independently, and exchanges traffic with other networks to form the internet.

There is a hierarchy, with larger ISPs providing, and charging for ‘transit’ connections to the global internet, provided to smaller ISPs.

Cash flows upwards from consumers to providers, with each tier (level) paying the level above.

Anyone can create and provide content, and everyone benefits.

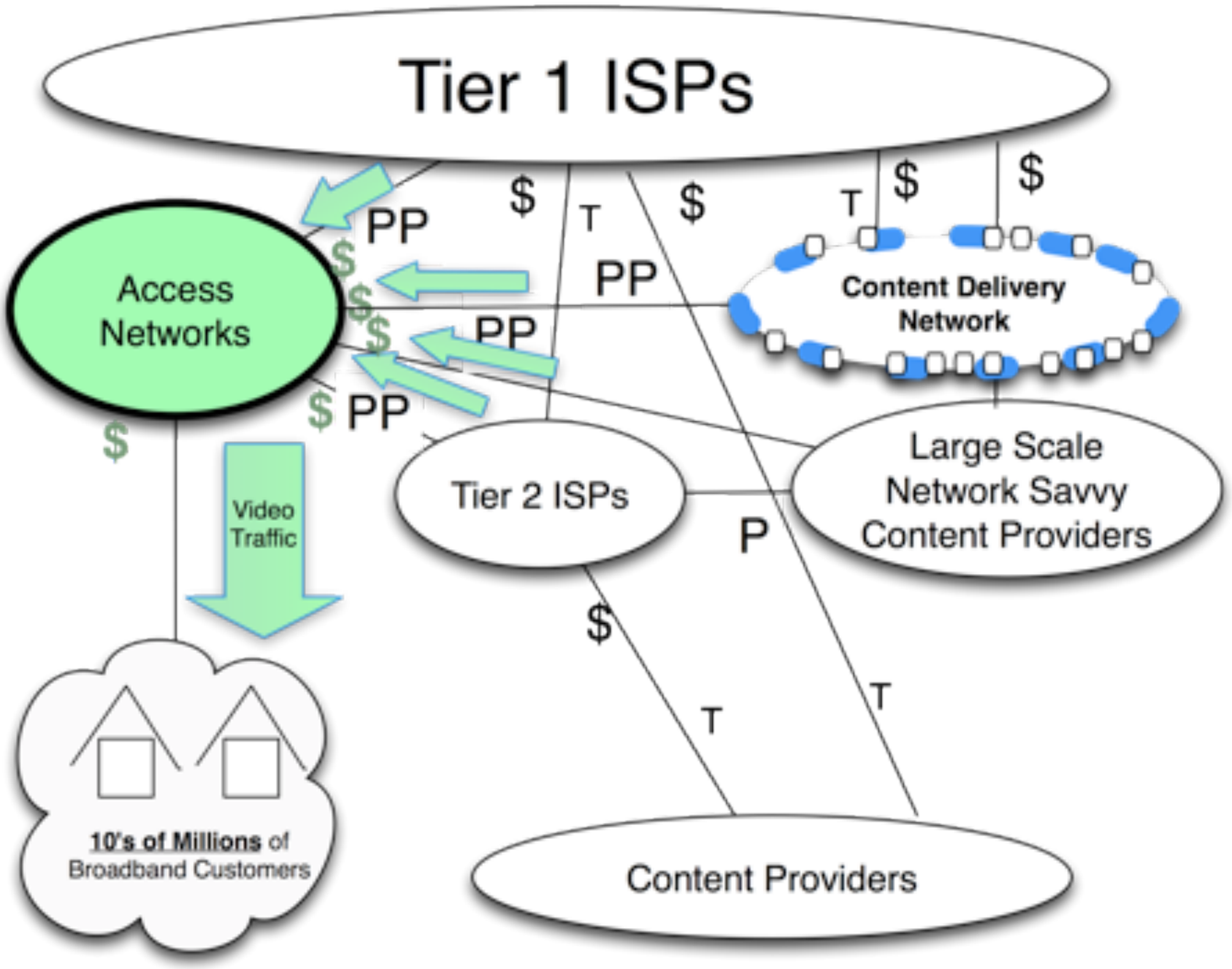
But content providers are an important component missing from this diagram.

Separate content and carrier

- Telegraph was originally not that popular
- First big user of the telegraph was the newswire Associated Press
  - News more valuable if it arrives quickly
- To keep competitive edge, AP made exclusive contract with Western Union (a monopoly)
- Other news organizations priced out of the market
  - AP had a lock on news distribution
  - Threatened Freedom of the Press

To discuss such issues in detail we need to look at the commercial structure of the internet...

http://drpeering.net/AskDrPeering/blog/articles/Ask_DrPeering/Entries/2011/9/6_Access_Power_Peering.html



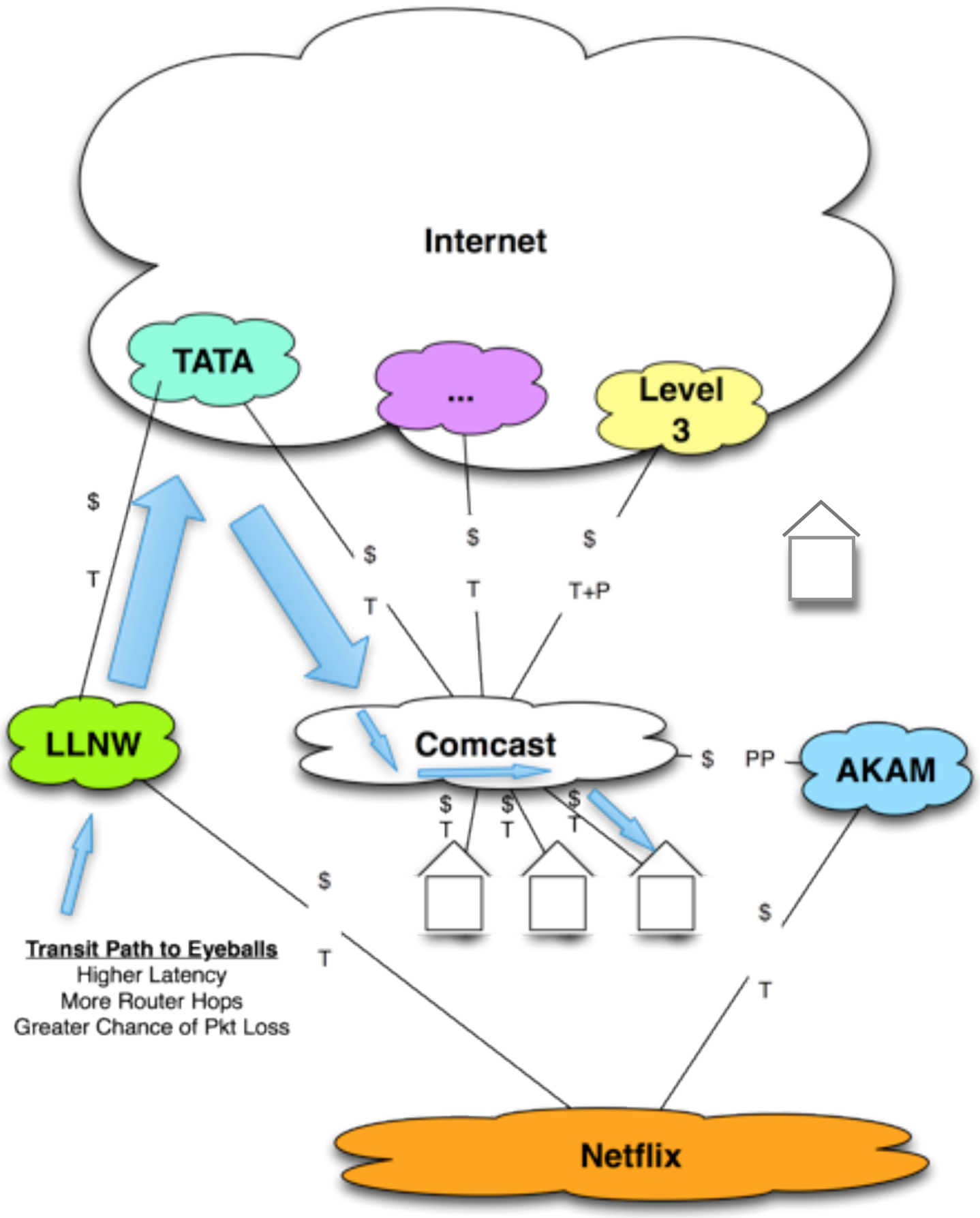
Saturday, 3 December 2011

Real life is more complex. Access networks are the local networks that connect homes and businesses to the internet.
In most of Scotland, BT has a virtual monopoly of the access network.
In much of the USA Comcast has a similar monopoly over access

Some content providers are national or global operators. They don't need to connect via Tier 1. They have Tier 2 peering agreements.

But those who control the access networks control access to consumers. "Why," they ask, "should we pay transit charges to tier 2?" If they want access to our customers, they should pay us.

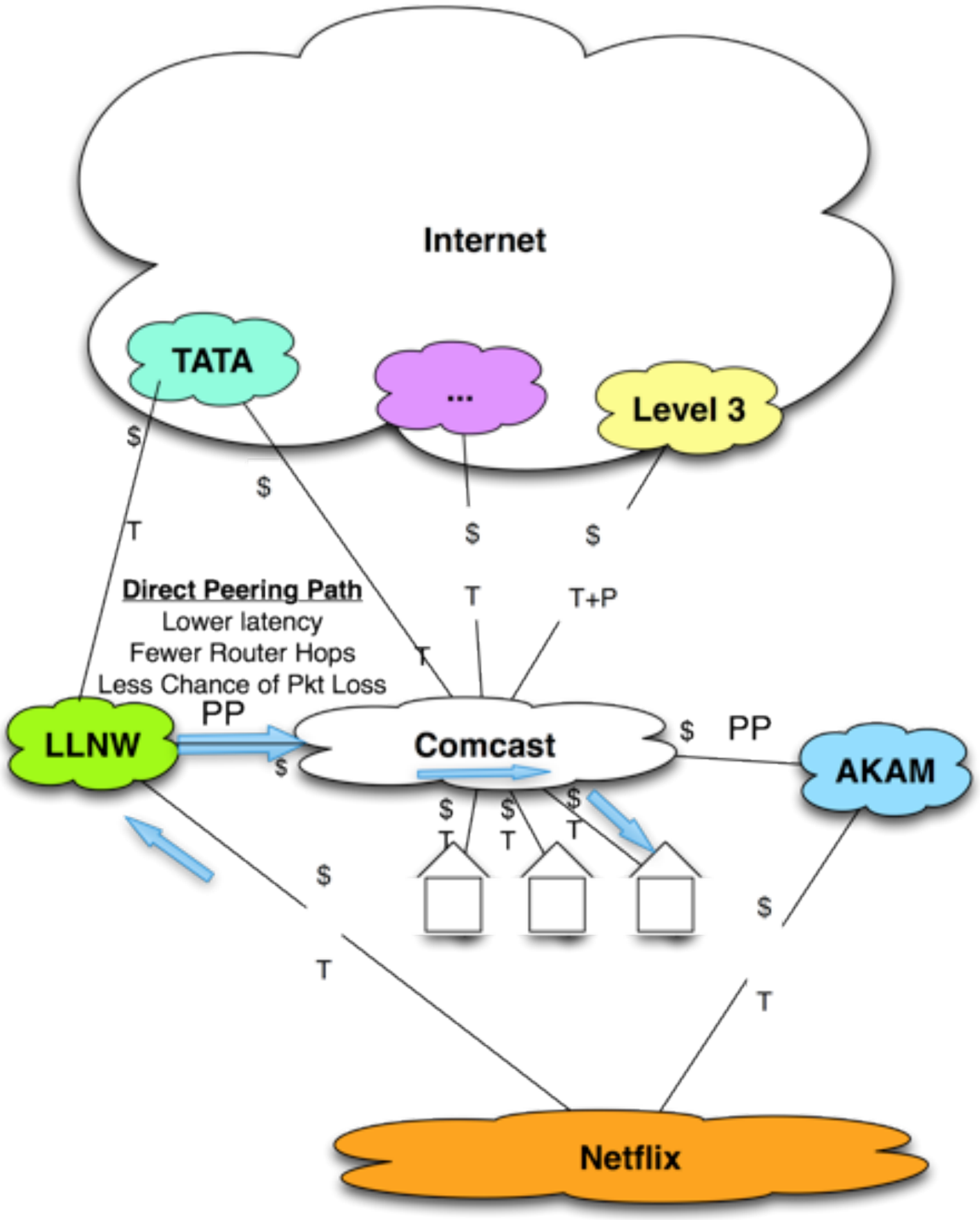
So they see themselves as higher in the pecking order than the content providers – and, although they are already charging their customers for internet access, they also want to charge the content providers for access to these customers.



Akamai was purchasing Paid Peering from Comcast and enjoying low-latency high-capacity access to Comcast customers.

Limelight Networks, a competitor to Akamai had a choice to make. Should it continue to send its traffic through its upstream ISP to reach Comcast customers? By doing so, Limelight traffic will suffer higher latency and potentially greater packet loss than its competitor.

Philosophically, Limelight feels that it shouldn't have to pay Comcast to deliver the content that Comcast customers requested!

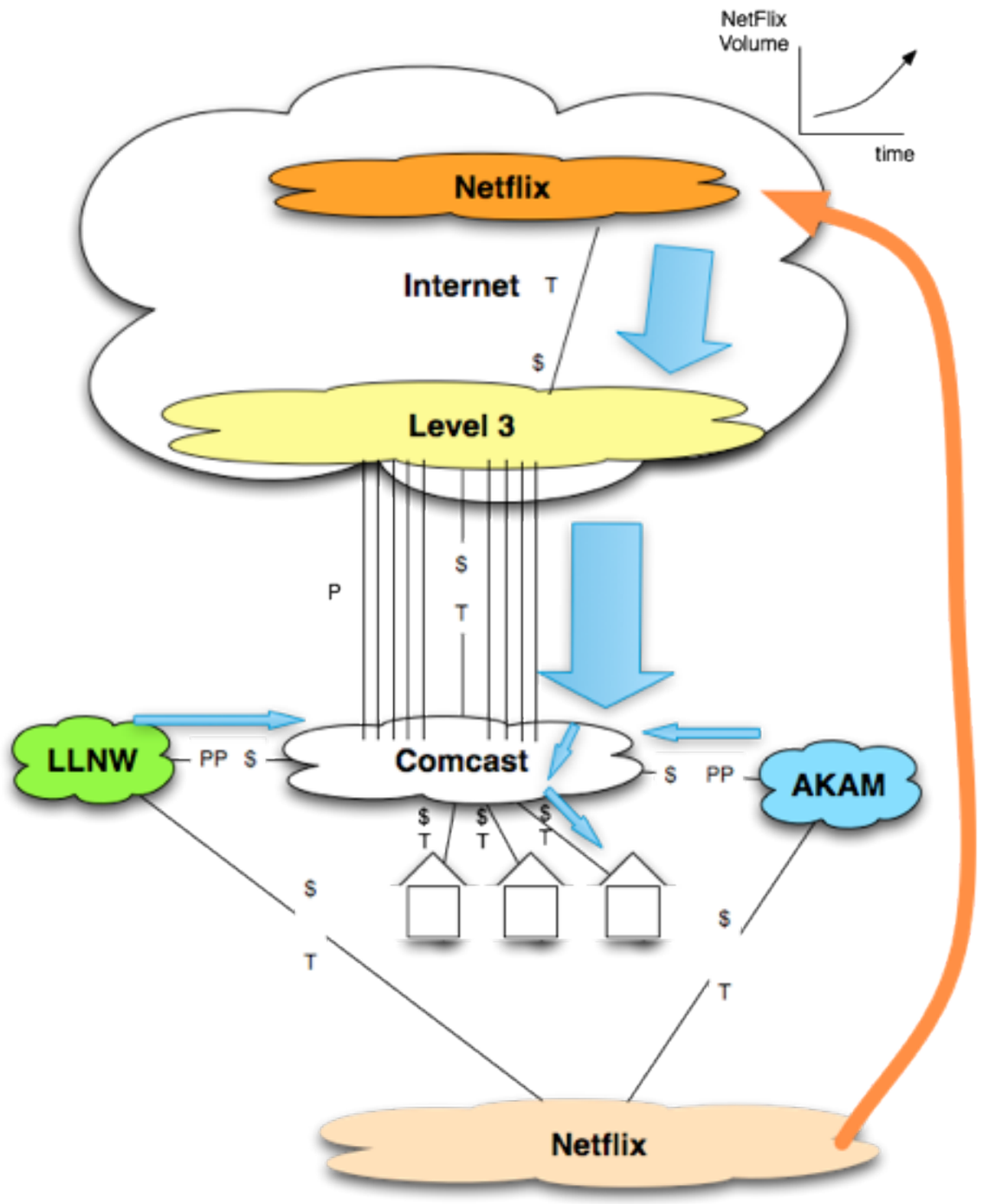


Unfortunately–one wonders why–the links between Comcast and Comcast's upstream transit provider experienced chronic congestion.

Limelight is being paid by Netflix to distribute content, and has to pay Comcast–a 'paid peering' arrangement.

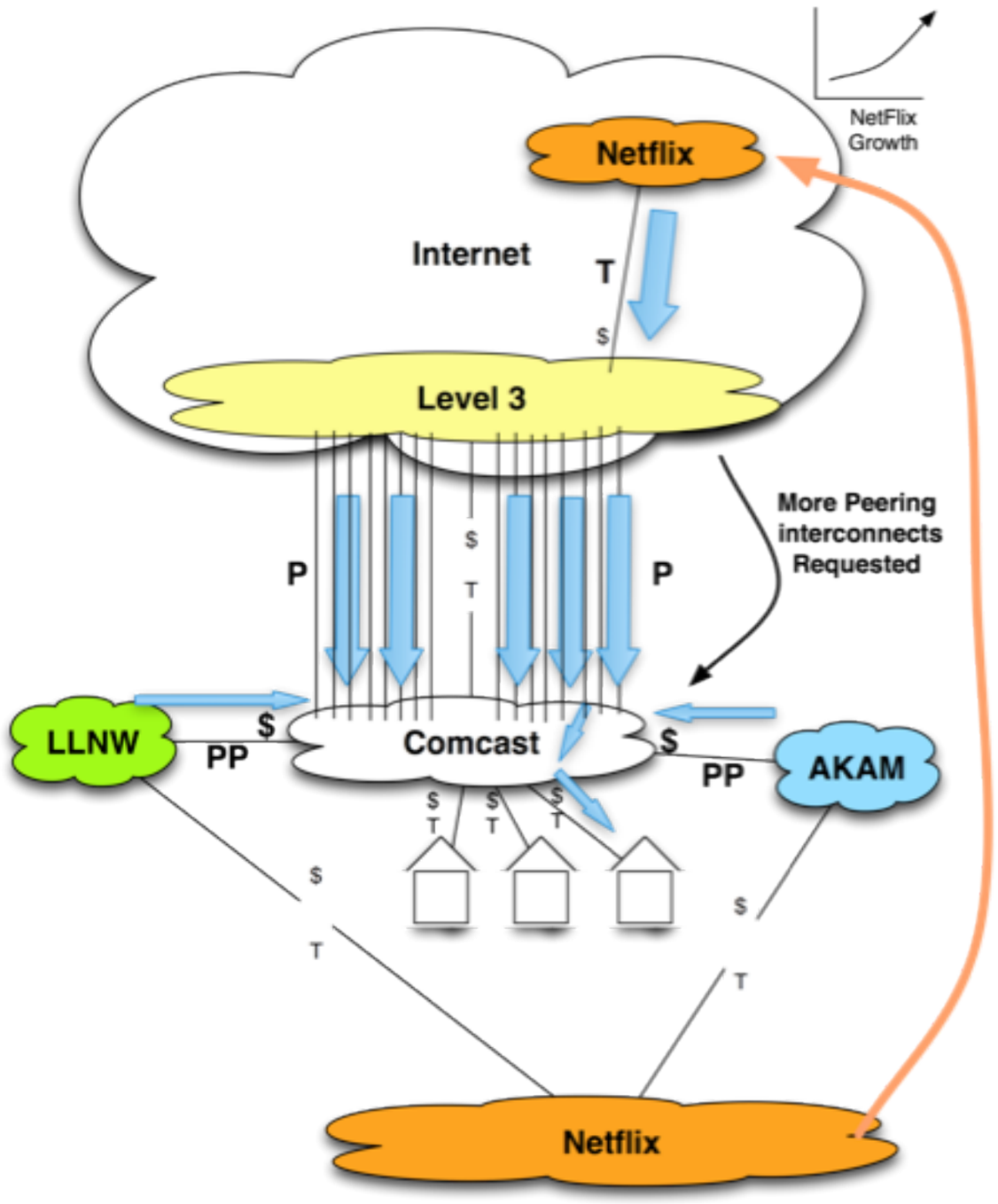
Confusingly, 'Level 3' is the name of a Tier 1 ISP in the USA. Level 3 had a peering arrangement with Comcast. Comcast got free access to Level 3 customers (which happened to include most of the other cable companies) and Level 3 in return got free access to Comcast customers.

The next stage in this game is interesting...



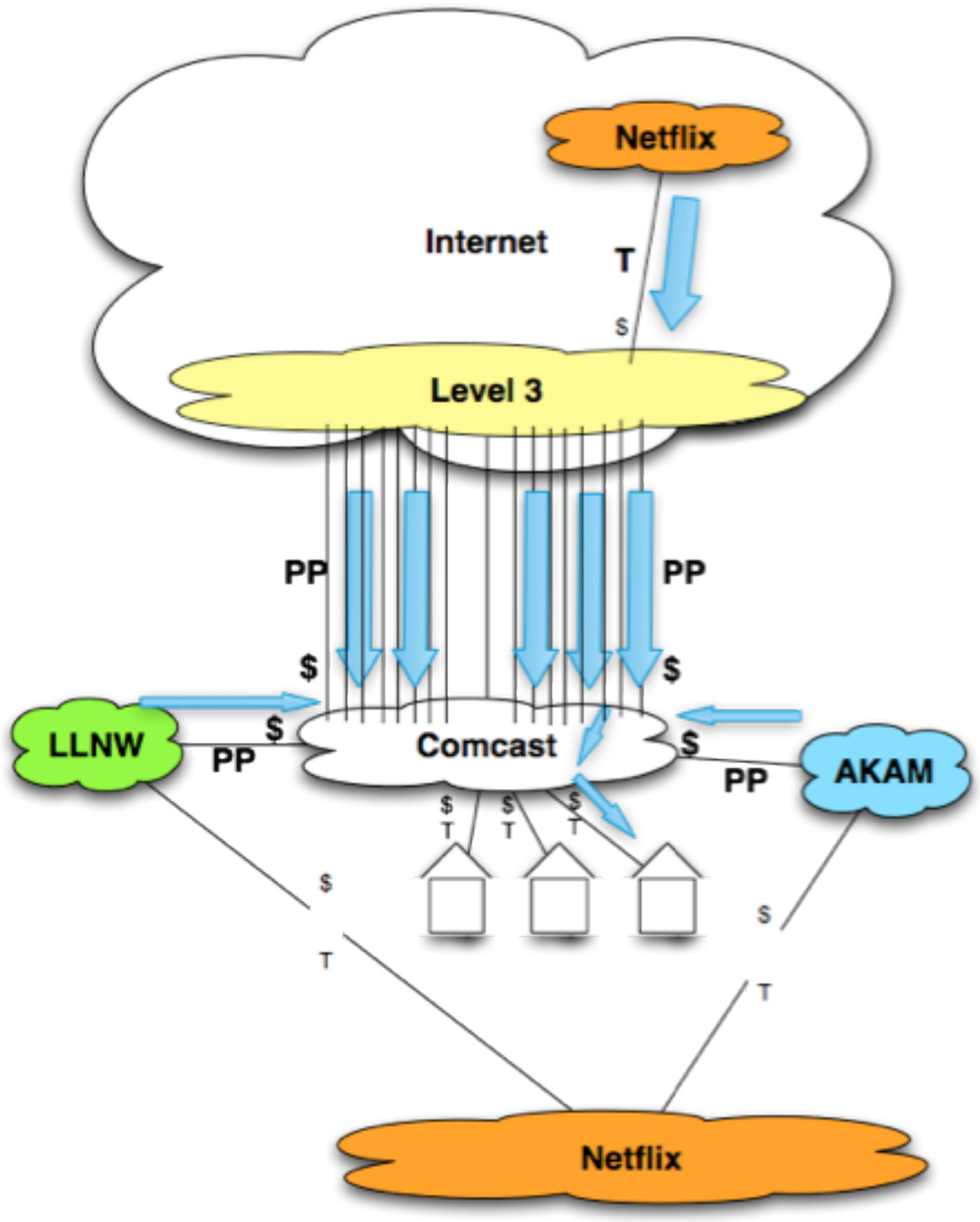
Netflix, the largest video distribution company in the US paid both Akamai and Limelight for internet connections for content distribution. Netflix was experiencing a near exponential growth in traffic.

Level 3 bid for and won the Netflix video delivery business. Both Akamai and Limelight had paid peering arrangements with Comcast. But Level 3 had free access.



Comcast was not pleased.

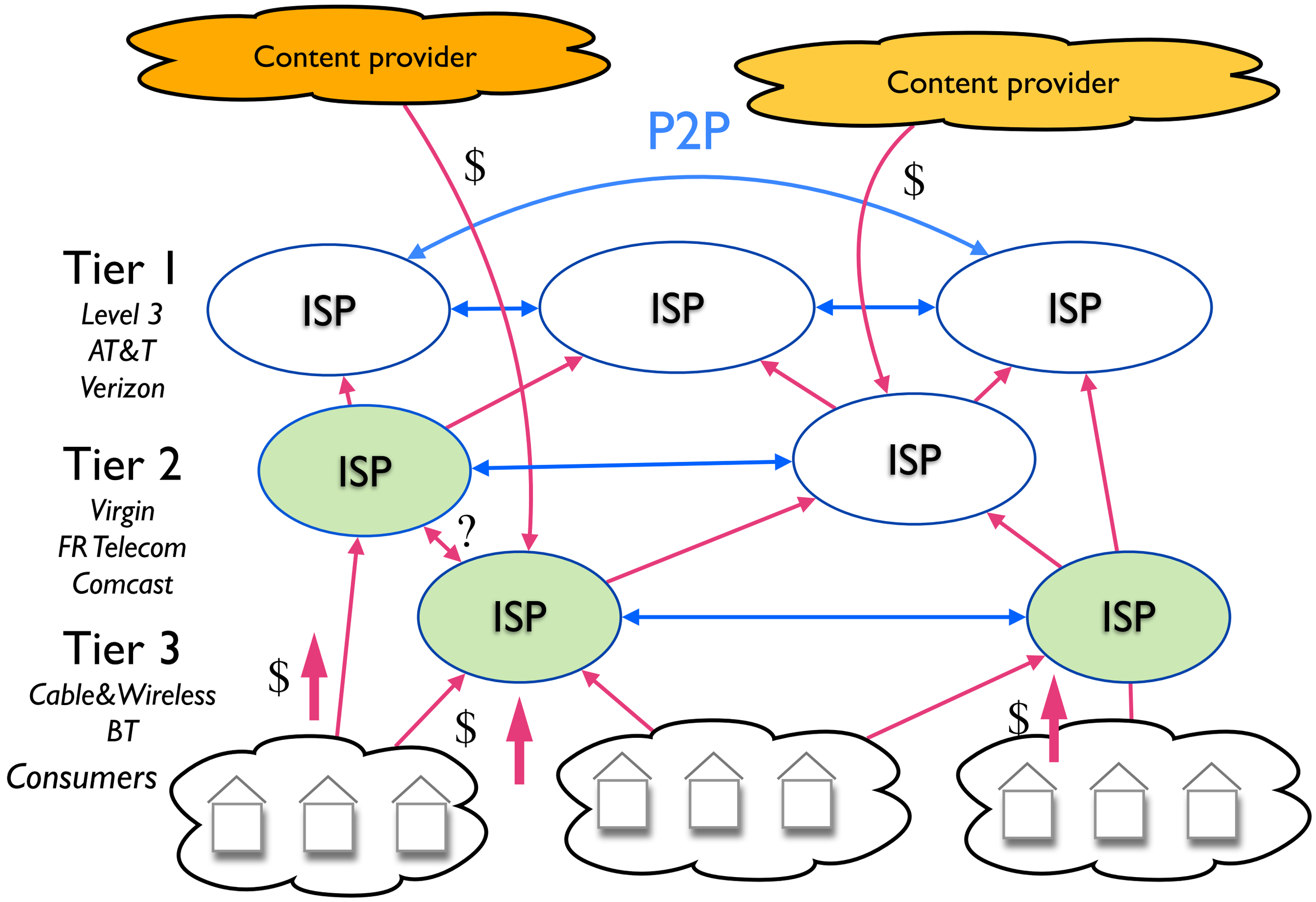
They lost revenue they had been getting from Akamai and Limelight, and had to cope with the increasing video traffic coming from Netflix via Level 3.



Comcast held Level 3 to ransom, by threatening to throttle the connection (or refusing to invest in the hardware required to handle the increased traffic–which amounts to the same thing).

Level 3 now makes payments to Comcast for the Netflix traffic it sends.

http://drpeering.net/AskDrPeering/blog/articles/Ask_DrPeering/Entries/2011/9/6_Access_Power_Peering.html



A logical outcome of such exploitation of a monopoly over customer ‘eyeballs’ would be to reverse some of the flows of cash through the hierarchy of ISPs.

http://drpeering.net/AskDrPeering/blog/articles/Ask_DrPeering/Entries/2011/9/6_Access_Power_Peering.html

Saturday, 3 December 2011

Similar commercial pressures mean that it is often not in your ISP's best interest to give you the best service that is technologically available.

An obvious example is Skype. It is feasible and efficient to use Skype over a 3G mobile connection, but your mobile carrier would rather you make calls via them so they can charge you more.

The Open Internet

http://nextdigitaldecade.com/

Saturday, 3 December 2011

In your essays you looked at the benefits and risks of the internet.

The consensus was that the internet is a good thing and that the benefits outweigh the risks.

The economic example we've just discussed suggests that we shouldn't take the internet for granted.

Now we want to look at the ways that the architecture of the internet makes it vulnerable. One weakness is the underlying economic model.

What keeps the internet open? (Short answer – profit.)
How will it be changed by the changing economics of peering and transit.
Where are the points of control, authentication and trust?

The Open Internet

http://nextdigitaldecade.com/

- Benefits
  - education
  - emancipation
  - internationalisation
  - revolution
  - truth
  - art
  - freedom

Saturday, 3 December 2011

In your essays you looked at the benefits and risks of the internet.

The consensus was that the internet is a good thing and that the benefits outweigh the risks.

The economic example we've just discussed suggests that we shouldn't take the internet for granted.

Now we want to look at the ways that the architecture of the internet makes it vulnerable. One weakness is the underlying economic model.

What keeps the internet open? (Short answer – profit.)
How will it be changed by the changing economics of peering and transit.
Where are the points of control, authentication and trust?

The Open Internet

http://nextdigitaldecade.com/

- Benefits
  - education
  - emancipation
  - internationalisation
  - revolution
  - truth
  - art
  - freedom
- Risks
  - disinformation
  - control
  - cultural invasion
  - repression
  - lies
  - pornography
  - censorship

Saturday, 3 December 2011

In your essays you looked at the benefits and risks of the internet.

The consensus was that the internet is a good thing and that the benefits outweigh the risks.

The economic example we've just discussed suggests that we shouldn't take the internet for granted.

Now we want to look at the ways that the architecture of the internet makes it vulnerable. One weakness is the underlying economic model.

What keeps the internet open? (Short answer – profit.)
How will it be changed by the changing economics of peering and transit.
Where are the points of control, authentication and trust?

Use or Abuse?

"On the Internet, nobody knows you're a dog."

The US military has contracted with a California-based company that makes it easy to create and manage fake identities online.

(see following slide)

Use or Abuse?

"On the Internet, nobody knows you're a dog."

The US military has contracted with a California-based company that makes it easy to create and manage fake identities online.

Ntrepid Corp. will be receiving $2.75 million for spreading pro-US propaganda overseas by making it appear that the sentiments are coming from actual living humans and not digital sock puppets.

Companies, crooks, and some egomaniacs do the same.

David Rose & friends

"David Rose" was an assiduous Wikipedia editor who devoted much time to defending (ex-) Guardian journalist, Johann Hari and attacking his enemies.

In fact, David Rose *was* Johann Hari.

An earlier fanatical supporter of Hari was a blogger named 'Niko', who mysteriously 'went to the Congo' and so 'can't be traced' ☺.

A Gay Girl in Damascus, *an unlikely hero of revolt whose frank and witty thoughts on Syria's uprising, politics and being a lesbian in a conservative country shot her to prominence*,

was, in fact, Tom MacMaster, a 40-year-old Edinburgh University masters student from the USA

Saturday, 3 December 2011

In 2000 Hari was joint winner of the Times Student News Journalist of the Year for work he had done on the Cambridge student newspaper Varsity.

In June/July 2011 Hari was accused of plagiarism in his use of unattributed quotations in interviews, where he had reused previously published quotes in place of his interviewees' recorded answers. The Orwell Prize, which he had won in 2008, was withdrawn. He was shown to have been making misleading edits on Wikipedia under a pseudonym.

Description of Gay Girl in Damascus comes from a Guardian report.

Later in the course we will discuss authentication – tools we can use to verify with whom we are talking.

Use of the Internet

- Criminal — Record evidence of crimes, mobile phones & YouTube
- Political — Participatory democracy (e-petitions), Arab Spring
- Social — Keeping families connected, FaceBook & Skype
- Commercial — Access to global markets, e-commerce

Some of us might like to believe that the genie is out of the bottle and that we all have access to an unstoppable decentralized network.

In reality, the internet is entirely controlled by large corporations and central authorities.

Abuse of the Internet

- Criminal — Phishing (identity theft)
- Political — Terrorist cells communicating via internet
- Social — Man pays $200,000 to save fake girlfriend in online scam
- Commercial — Comcast vs. Netflix, new monopolies

Saturday, 3 December 2011

Some of us might like to believe that the genie is out of the bottle and that we all have access to an unstoppable decentralized network.

In reality, the internet is entirely controlled by large corporations and central authorities. They want to increase profits and prevent abuses.

Of course, one person's use is another's abuse.....

Even if we agree on what is use and what is abuse, some questions remain:

How can we control abuses without destroying the benefits?

Do we need to regulate the internet in order to prevent the benefits being destroyed by commercial pressures?

Open use without abuse?

- Can we censor IP traffic?
  - how do we know where it's from
  - how do we know what it contains
  - ➡ *No border controls*
- Can we control the sources?
  - only if we know where to find them
- Can we control the consumers?
  - only if we watch them closely

Saturday, 3 December 2011

The narrow waist of the hourglass provides an interesting problem.

If all packets really are treated alike, then the bad passes as easily as the good.
If we find ways to inspect, and filter the bad, then these same ways can be used just as well by the 'bad guys', to curtail free speech, eavesdrop on private conversations, etc.

Its a cruel irony in information security that many of the features that make using computers easier or more efficient and the tools used to protect and secure the network can also be used to exploit and compromise the same computers and networks. This is the case with packet sniffing.

A packet sniffer, sometimes referred to as a network monitor or network analyzer, can be used legitimately by a network or system administrator to monitor and troubleshoot network traffic.

But we also have to worry about what types of information could be discerned from the captured data by an evil adversary. Packet sniffers are routinely used by governments – good and bad – Iran, Egypt, Libya, China, USA, UK, ... to detect crimes, terrorists and dissidents.

Later in the course we will discuss data mining, and see how information can be gleaned from seemingly innocuous data.

We finish today with a brief look at what the USA is doing to try to keep the internet open.

Federal Communications Commission (FCC)

Preserving the Open Internet

- **transparency:** fixed and mobile broadband providers must disclose the network management practices, performance characteristics, and commercial terms of their broadband service
- **no blocking:** fixed broadband providers may not block lawful content, applications, services, or non-harmful devices; mobile broadband providers may not block lawful websites, or block applications that compete with their voice or video telephony services
- **no unreasonable discrimination:** fixed broadband providers may not *unreasonably* discriminate in transmitting lawful network traffic

Saturday, 3 December 2011

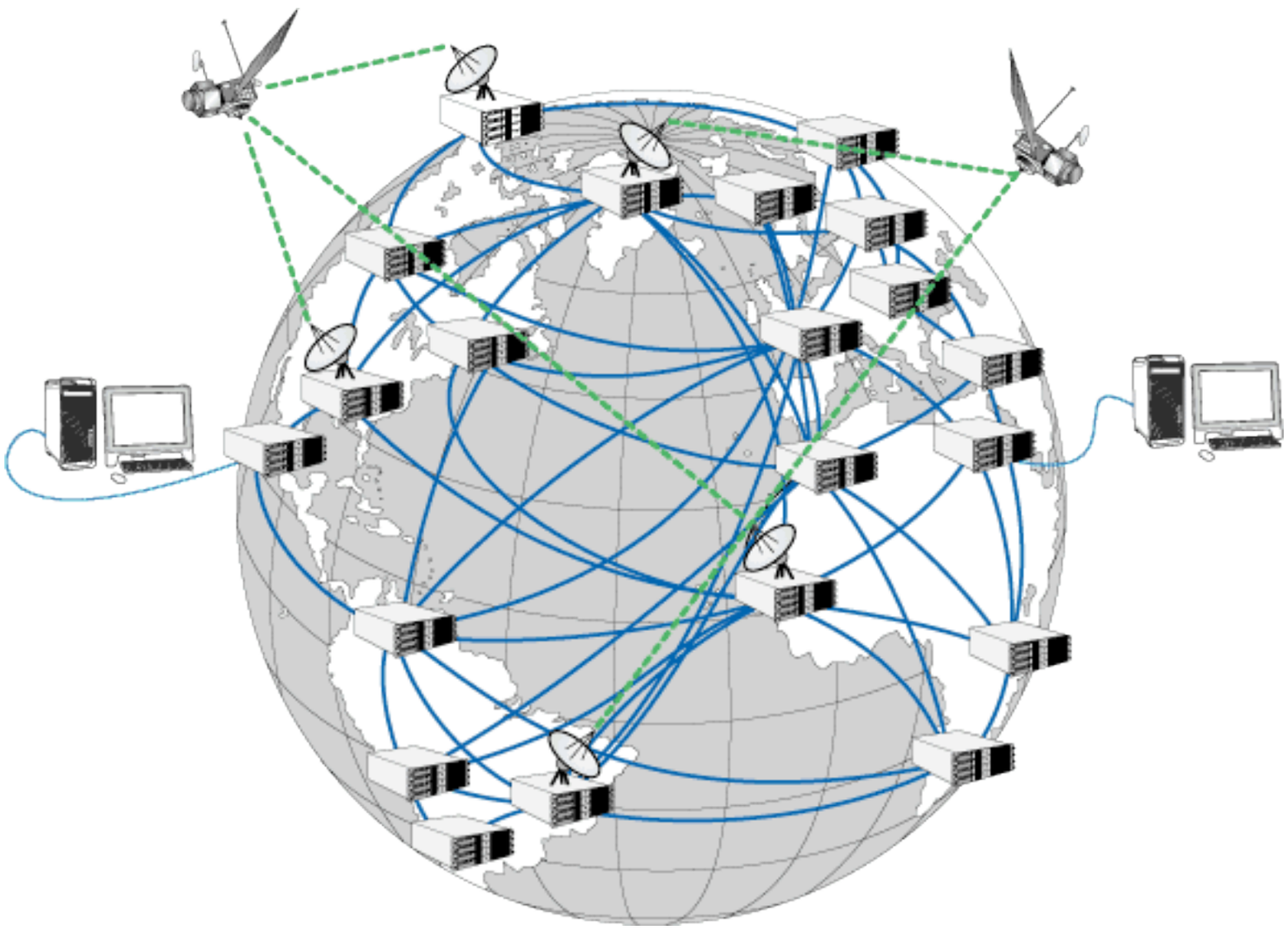
The Federal Communications Commission is the US counterpart to OfCom in the UK. They Recent regulation by the FCC, which regulates communications – telephony, radio, TV, broadband. To try and limit the ability of service providers to impose self-interested restrictions on the service they deliver, to limit the detrimental effects of the providers' monopoly over your eyes and ears, they have recently imposed some regulatory requirements:

transparency: fixed and mobile broadband providers must disclose the network management practices, performance characteristics, and commercial terms of their broadband services

no blocking: fixed broadband providers may not block lawful content, applications, services, or non-harmful devices; mobile broadband providers may not block lawful websites, or block applications that compete with their voice or video telephony services

no unreasonable **discrimination**: fixed broadband providers may not **unreasonably** discriminate in transmitting lawful network traffic

The next Digital Decade



Saturday, 3 December 2011

The internet is a force for good and but can be misused
Criminal misuse : pornography, fraud, defamation
Political misuse : repression, revolution
Commercial misuse : monopoly exploitation
Social misuse: impersonation, defamation