Study of QoS parameters in IP traffic exchange agreements on the Internet

Master Thesis

Carlos Eduardo Romero G.*
carlosromero15@gmail.com

Tutors: Xavier Hesselbach-Serra, Daniel Ollé♦*

Telematics Engineering Department (ENTEL)
**Technical University of Catalonia (UPC), Barcelona, Spain.*
♦*Comisión del Mercado de las Telecomunicaciones (CMT), Barcelona, Spain.*

Abstract
The Internet has experimented big changes since its conception, the interconnection between Internet Service Providers (ISPs) has evolved as the core of Internet. These interconnections have being growing and becoming more complex in order to support the different IP traffics available on the Internet with certain level of quality. The QoS on these exchanges is present as a key factor on the services provided in the Internet, but also the preservation of the principles of Net Neutrality as an open and neutral environment. Currently there is a debate about Net Neutrality, in which the need to regulate the Internet is discussed.

This document studies the QoS parameters relevant in the IP traffic exchange agreements in the context of ISP interconnection, the way to assure the quality agreed, through establishment and fulfilment of SLAs between the stakeholders. This document includes further discussion/analysis about the possible role of regulation in this scenario; presenting proposals in case they are needed in order to preserve Net Neutrality.

***Keywords*: Internet, ISP Interconnection, QoS, Peering, SLAs, Net Neutrality.**

I. INTRODUCTION

Internet as we know nowadays is the product of an effort by the research and development of governmental institutions and universities around the world, to achieve the "net of nets" or "the Internet", consisting basically in the interconnection of a huge number of network equipment that provide the data flow between computers or any other device. Internet interconnection has been made through agreements between ISPs sharing their IP traffics, establishing strategic relationships between them; sometimes those relationships affect the performance of any other ISP on the net.

As a principle, the Internet had not been regulated by a government or international entity, that is how Internet has grown so fast in the past of years, by the development and collaboration, being the Internet like a big success of "self-regulated" technologic element in our society, reason why the Internet is recognized as "Open and Neutral".

Regarding to preserve "the open and neutral character of the Internet", the declaration on ***Net Neutrality*** by the European Commission [1], arises the need to define clearly the concepts of "open" and "neutral" Internet. Speaking about **Open** Internet is related to the accessibility to any content by the final customers, and **Neutral** is related with the operation of IP-based services in a neutral manner, avoiding discrimination between services and receiving all traffics equal treatment by the ISP (Internet Service Providers).

This document will be structured as follows: Section II provides a set of motivations regarding regulation and net neutrality aspects, for doing this work. Section III defines the background terms to understand the QoS parameters in IP traffic exchanges between ISPs, in others words the context of study;

section IV describes the QoS scenarios in the ISP interconnection. Section V and VI are focused on the agreements established between ISPs through SLAs (Service Level Agreements) and measuring QoS in ISP interconnection, and finally section VII includes proposals for SLA`s and regulation in IP traffic exchanges on the Internet.

II. MOTIVATION AND RELATED WORK

Net Neutrality as a principle suggests no restriction in Internet services providers or governments to consumers' access to networks in the internet, as mentioned before, "open and Neutral".

Need from Regulate Internet

The European regulation started in 1987 with the publication of "the green book of convergence", in 1998 and finished with the total liberalization of telecommunications services in all the countries belonging to the European Union in order to promote the growth of telecommunication sector. From this moment, the European Commission will be in charge of setting the policies for all the EU members in the matter of electronic communications.

In March 2002, a set of Directives were approved conforming a legislative Framework[1], regarding aspects such as access (related to access to electronic communications networks), universal service, privacy and electronic communications (related to personal data treatment).

In November of 2009 reforms of the legislative framework were approved, specially the Directives *2009/140/CE and 2009/136/CE*, which are focused on better regulation and rights for citizens, being those modifications of the past Directives.

These modifications introduce considerations about "Net Neutrality" described in three topics, which are:

- General objectives and principal responsibilities of NRAs (National Regulatory Authorities) and their collaboration with EU institutions.
- Transparency requirements related with *Net Neutrality:* information from SP (service providers) to users about access limitations or use of services and applications and about traffic management.[2]
- NRAs powers related to Quality: NRAs in charge of establishing minimum QoS requirement in SP services provided to clients.

In the same moment, it was proposed the creation of a Body of European Regulators for Electronic Communications (BEREC) [2], in order to enforce relationships between NRAs and improve the collaboration with other EU institutions. The BEREC could make observations or recommendations to the NRAs about their regulations proposals and norms.

The European Commission in June of 2010 launched a public consultation on "The open Internet and net neutrality in Europe" [3], as an attempt to establish a "state of situation of Net Neutrality" in Europe.

The results of this allowed considering the position of Service Providers and Customers associations about the actual state of Internet, market structure, potential issues attempting to net neutrality, and social aspects such as freedom of expression.

In April of 2011 the European Commission expressed its position in the Net Neutrality debate [4], analyzing the results of the public consultation in which issues about net neutrality were analysed, focusing on Traffic Management, ensuring transparency on it, regarding the legislation Framework approved in 2009. The Commission also requested BEREC to study of a list of issues related to: customer-switch of operator, QoS, as well as blocking and throttling of services and similar techniques.

The BEREC had created working groups regarding to Net-Neutrality to deal with the 3 topics considered (according with Directives *2009/140/CE and 2009/136/CE*), previously described.

In May of 2011 the European Parliament pronounced opinions about the net neutrality debate [5]. In this report recommendations were exposed to the entities included in the debate such as:

- Do not impose obligations on net neutrality until the Directives *2009/140/CE and 2009/136/CE* of the European Commission are implemented efficiently.
- Provide support to the investigations related to QoS and transparency to consumers.
- Continue the studies of issues regarding to

[1] These Directives were specifically described by the EU as : *2002/21/CE, 2002/20/CE, 2002/19/CE, 2002/22/CE, 2002/58/CE*

[2] Traffic Management regards of any techniques used to separate, discriminate or limit the use of a service or application in the service provided (e.g. Internet P2P applications blocking, etc.).

Net neutrality analyzed in the claims received on the public consultation such as VoIP and P2P traffic degradation.

As shown above, there is a big interest in net neutrality on access to Internet and customer-provider relationships, but currently it seems that ISP interconnection and IP traffic exchange are not considered as possible Net neutrality`s issues in the initiatives of different bodies to regulate the Internet in this sense.

The ISP interconnection has changed since the Internet conception, new managed services have emerged for clients, constantly increasing and demanding even more content, producing these changes and arising from this the need to regulate QoS on it.

III. Definitions, Assumptions and Notation

This section defines elemental terms in order to be familiarized with some terms related to QoS and the scenario of ISP interconnections.

1. The ISP Interconnection

The Internet was created by ISPs (Internet Service providers) interconnections, an exchange of equal traffic amounts (incoming and outgoing), in others words, symmetric traffic, due to the fact that services provided to the clients had the same behaviour (e.g. web browsing, email, chat).

The constant growing of Internet, reaching all the places in the planet has resulted in a traffic explosion, the increasing amount of hosts or Internet subscribers has incremented traffic, specially types of traffic such as Video (e.g. online video, VoD, IPTV), P2P traffic (e.g. File Sharing), and real time traffic (e.g. VoIP). Figure 1 shows the growth of the Internet traffic from 2010 and their estimation to 2015 by [6].

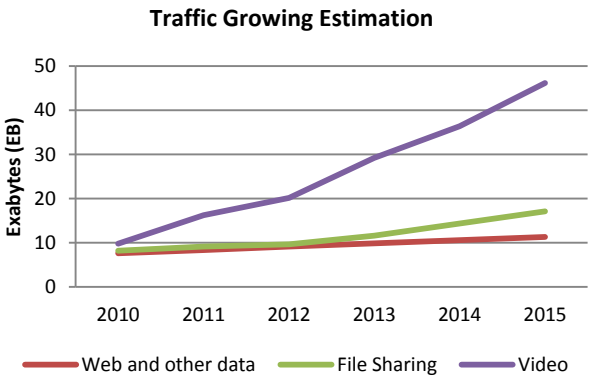

Figure 1 Traffic growing estimation, Cisco VNI [6]

This just indicates one fact: a lot of users are demanding multimedia content and specially video in all their types (VoD, Online, etc.). Services are supplied by Content Providers (CPs), which store these contents and connect to the Internet Service providers (ISPs) in order to achieve their distribution over the Internet to the final users who require those contents. This fact has changed the behaviour of traffic, making it asymmetric due to the clients' demands of contents from CPs through the ISPs.

These connections between CPs and ISPs or ISPs to ISPs and the way these entities are interconnected define and affect the performance of the Internet, because a non correct way of connecting could affect the path length to reach a destination or the speed of content delivery, giving some preferences to services more than others as a strategic or economical action by those entities, affecting in this way to the final users, breaching this the principle of Net Neutrality.

Level 3-Comcast Dispute

The Dispute between Level 3[3] - Comcast[4] is an Example given to illustrate the importance of preserve the principle of Net Neutrality, and also show the possible need for regulation, a perfect scenario in which a suddenly change of ISP interconnection settlement given by business strategies can affect an interconnection relationship (between Level3 and Comcast) from a *free peering connection* to a *Paid peering* by Comcast. Level 3 asked to FCC (Federal Communications Commission) [7], the United States of America regulatory authority, who had released the document titled "Preserving the free and Open Internet" [8], expressing their regulation position, but the FCC could not do anything in order to impose rules in negotiations, due to the lack of power to regulate on Internet, which has been historically self-regulated. This case is widely explained in *Appendix 1: Level3-Comcast Dispute.*

2. Routing strategies related with ISP Interconnection:

Apart from the peering policy or the way of peering with other ISP, there are some routing strategies

[3] Level3 is one of the biggest Tier 1 ISPs on Internet, ranked as one of the best connected ISP, being this a biggest IP transit Provider in America and Europe.

[4] Comcast is one of the biggest media entertainment in the United States, through cable media access technology, providing Internet access and VoIP to millions users in the United States.

involved that have influence in the ISPs operation performance:

Hot-Potato Routing: or *deflection routing*, it's a type of routing which seeks to have a packet in transit through an AS as little as possible, sending immediately to the next neighbour AS to reach its destiny. This routing conduct reduces the need to keep packets in buffers in the AS. Hot-potato routing is commonly used in free-peering agreements.

It works as shown in Figure 2: Supposing there is an end user in Backbone 1 requiring services of a CP located in Backbone 2, so:

1. Backbone 1 exchanges the content request from the end user to backbone 2 through the nearest Interconnection point (IXP1).
2. Hence this traffic will be carried through backbone 2 to the CP.
3. The return traffic will be sent through backbone 1 to the nearest interconnection point (IXP2).
4. Finally backbone 1 carries the traffic back to the end user.

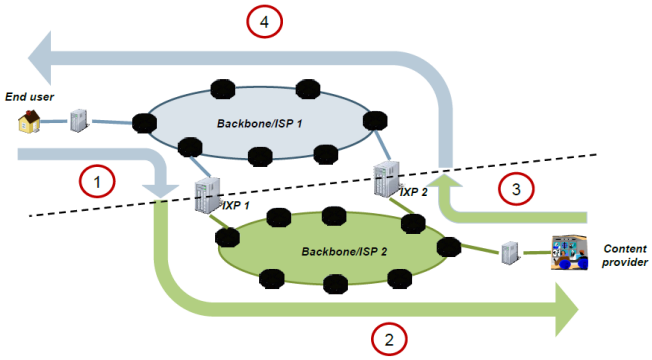

Figure 2 Hot-potato routing [50]

Cold Potato Routing: In this case, packet buffering is performed in an AS carrying them through its AS to get to the next AS destiny. This option is mainly more costly than hot-potato routing, due to the longer transit routes in the origin network. The rationale for this is to have more control of the packets in the network under certain QoS, during the transit of the packet in the network [51]. This type of routing is usually performed in CDNs (Content Delivery Networks).

3. Quality of service (QoS)

The QoS is known as the ability to establish different priorities for specific data flows, or applications through a network (LAN, WAN, or Internet), giving certain guarantees to those who demand it (e.g. real time applications such as, audio and video online, etc.) [9]. This allows differentiating data flows in service classes, truly important in congestion times, when the networks become resource-constrained, and hence QoS has value, prioritising traffic, allowing data flows for those applications.

Different international bodies have proposed QoS frameworks as described briefly below:

- ITU (International Telecommunications Union) E.800 Recommendation described in [9] includes terms and definitions related to QoS and network performance including network dependency, providing a framework for:
  - The QoS concept.
  - Relation between QoS and Network Performance
  - Set of performance measures.

  The framework analyses the QoS in terms of the service provider and the user, remarking the existence of both viewpoints to perform the service delivery. Network performance parameters and measures are consequently terms needed to control the achievement of the service level quality.

- ETSI (European Telecommunications Standards Institute) ETR 003 [10] define a framework considering Networks Aspects, General Aspects for QoS and Network Performance, providing four viewpoints of the QoS:
  - The customer QoS requirements.
  - The QoS offered from network provider.
  - QoS achieved by the Network Provider.
  - The QoS perceived by the customer.

  The relationships between these viewpoints and associate activities in terms of QoS cycles are shown in this framework.

- ISO (International Standards Organization)/OSI (Open System Interconnection) QoS Framework [11] , includes four main concepts in terms of QoS such as:
  - QoS requirements, realized by the QoS management and maintenance entities.
  - QoS characteristics, the aspects of QoS that have to be managed.
  - QoS categories, related to the well know QoS services levels as

requirements specific to particular communications.
    - QoS management functions, combined in various ways in order to meet the QoS requirements.
- Telecommunication Information Networking Architecture Consortium (TINA-C) QoS Framework [12] groups four functional domains:
    - Computing Architecture.
    - Service architecture.
    - Network Architecture.
    - Management architecture.

  All these describing the QoS aspects of distributed telecommunications in the context of computing architecture.
- ETNO (European Public Telecommunications Network Operators Association) working group on QoS, which researched a set of common European parameters (QoS indicators) in order to harmonise the European QoS definitions focused mainly in voice operations, in order to facilitate results in the QoS measurements. [13].

- EURESCOM (European Institute for Research and Strategic Studies in Telecommunications) [14] has developed several projects focused on QoS issues in different study cases such as VoIP, UMTS and other emerging technologies.
  A project of big relevance in this work is the EURESCOM QoS or EQoS framework defined in the study case of Network inter-Provider Environments [15].

All of these bodies present similar structures related with the QoS establishment, their contributions are still work in progress on QoS in the context of networks communications.

QoS performance parameters:

A QoS service class or service level is given by measurable parameters[5] that can be called QoS performance parameters for Internet services (also called IPPM, (IP Performance Metrics) by the IETF [16]):

1. Connectivity: It is the basic facility from which the internet is made, represents the ability of establishing communications between a host and the internet, defined by IETF in [17].

2. Throughput: Rate at which IP packets are transmitted on an Internet Path, per unit of time, defined by the IETF [18]. It can be measured in terms of number of bits per seconds (bps).

3. Goodput: Also known as application level throughput, defined as the number of useful information bits, contained in the data field of IP packets delivered by the network to a certain destination, per unit of time, excluding the protocol overhead bits as a product of packet transmission. It is defined by the IETF in [19] .

4. Availability: Reliability of a user´s connection, it can be measured in terms of proportions of time available to connect [20].

5. One-Way Delay (OWD): also known as Latency, it is represented by the time needed for transmitting IP packets between two reference points through an Internet a path. It is denoted as IPPM (IP Performance Metrics) by the IETF [16] and their specifications are described in [21]. These delays are normally associated to the distance which a packet travels through the Internet, in terms of hops in the network, as well as to the presence of congestion.

6. Jitter: also know as One-way IP Packet delay Variation (IPDV), defined in [22] as the difference in the OWD of selected packets, in a stream of packets. This measure can be performed by the OWD of two different packets between two measure points in a network path. Some definitions as [23], and ITU-T recommendation [20], of measuring jitter are given as the difference between the OWD of a selected packet and the packet with the lowest OWD in the evaluation interval.

7. Packets loss Ratio (PLR): as the ratio of total lost IP packet outcomes to total transmitted IP packets in an IP Path per a certain measuring period, regarding to ITU-T recommendation [20] and [24] by IETF.

Service Class: a service class is defined in [25] as set of traffic flows with specific performance parameters (OWD, Jitter, PLR) requirements of the network. Thus a service class is given by the same treatment of a flow of data in the routers or Hops in the network as PHB (Per-Hop Behaviour) [26] under specific requirements in the domain of the Service provider, in order to ensure these Service class through

[5] Usually Throughput, Connectivity and Availability are not considered as QoS parameters for interconnection services nowadays, due to the reliability provided by the IXPs or NAPs those parameters are seen as ensured by them as service. Goodput measurement is also out of the scope of this work because it is a application level metric.

PDB (Per-Domain Behaviour) [27].

The ITU proposes guidance for IP QoS classes regarding network performance parameters, equivalents to IPPM (IP Performance Metrics, defined by IETF [16]), in which are defined 5 Classes depending on requirements of different applications types [28].

ISPs could have as many classes as they need for differentiating traffic as they wish; this is made possible by QoS methods or PHB techniques (AF Assured Forward, EF expedited Forward, DF default forward) in order to achieve these service levels for their users.

These QoS service classes can be identified by the DSCP (Differentiated Services Code Point), there is a number between 0 and 63, and its placed in a IP packet in the DS (Differentiated services) field, that is intended to replace the ToS (Type of Service) IPv4 field and Traffic class octet in IPv6.

SLA (Service Level Agreements): A SLA is a contract between provider and client, it specifies and defines the conditions of a service that a customer should receive, defined in [29]. The SLA should be as detailed as possible, including a scope of the service provided, performance, tracking reports, problem management, compensation, involved parts duties and responsibilities. All these sections must be detailed in order to define well the service provided.

A SLA besides its technical meaning is a business agreement in economic terms, previously negotiated between the agents involved. It can also be used in any service agreement, beyond the telecommunications scope.

In the ISP interconnection scope, ITU-T has defined initially in 1996 a recommendation for a SQA (Service Quality Agreement) framework between service providers [30], specifying a set of guidelines for establishing these Agreements in order to maintain the service level of the service provided.

An SLA includes a SLS (Service Level Specifications) which is a set of parameters that define the offered service in a Differentiated Service domain (DS domain). In others words, the type of QoS service classes negotiated to be offered ruled by SLS.

The important parameters which describe an SLS for an ISP interconnection SLA are a set of IPPM (IP Performance Metrics), specially OWD, PLR and Jitter, referred in [31]. This topic will be described in detail in the section V, Inter-Providers SLA .

4. Scenario: The Internet and their Interconnection.

The Scenario of internet Interconnection is composed by a set of entities which acts interconnecting each others in certain way in order to exchange IP traffic. Terms to get in the picture of this scenario are developed below, starting with Internet entities, their hierarchies' relationships in the Internet, and how the interactions between these entities are performed.

4.1 Internet: As the Net of Nets, Internet was originated as an interconnection between computers, nowadays there are interconnected more than computers, a huge amount electronics devices (smart phones, TVs, tablets, etc.). All this integration to any kind of devices is provided by the ISPs and their interconnection to each other ISPs. The Internet is based on the IP (Internet Protocol) defined in [32] as a "Protocol for use in interconnected systems of packet-switched computer communication networks". This protocol in their version 4 (IPv4) has allowed a great Internet development and even considered the issue of the QoS, but the actual emerging implementation protocol IPv6 [33] considers specifically the QoS, designating a header focused on it.

The fields used in this IP versions for QoS purposes are the "ToS" in IPv4. IPv6 uses the fields "Traffic Class" (geared for IntServ) and "Flow label" (geared for Diffserv) as QoS aware. Providing this more possibilities of use and implement QoS in a better way.

4.2 Internet Service Provider (ISP) and **Content Provider** (CP): An ISP Offers access to Internet to their customers. This is the main propose of their function, in the different scopes in which it operates with their peers.

In the Internet it can be remarkable the existence of two basic types of providers: Content providers (CPs) and ISPs or *Eyeballs* providers as shown in [34].

Content providers are those in charge of providing hosting and network access for the clients who offer contents, (e.g. Youtube, Google, Yahoo!, etc.). On the other side, the eyeballs ISP provide access to those contents to domestic users and enterprises, all of them supported by the different last-mile access technologies.

4.3 ISP Tiers Hierarchy

The Internet in its conception, development and growing, has been adopting an architecture regarding a tiered hierarchy. This means that ISPs can be classified for the state of the network, e.g. as geographical extension, connectivity facilities, amount of ISPs connected with, their reach in terms of paths to

Internet, that is the reason why a hierarchy using tiers or levels has been defined for this ISP or *Internet Entities.*

4.3.1 Tier 1 ISP, Internet Backbones Providers (IBPs): The entities parts of this tier are represented by the Biggest ISPs, covering great geographical extensions, and being presents in a lot of interconnection points. In others words, they are Global level ISPs (covering a groups of countries or continents), and they are called Internet backbone providers, by the amount of traffic that they manage over their domain.

Those entities are in the top of hierarchy, doing peering connections with their entities in equivalent position (peers), in order to reach and cover the whole Internet and provide *transit* service to lower Tiers Clients, through distribution routers connections to these clients and backbone connections between their belonging equipments, spread in their "footprint" as operation zone.

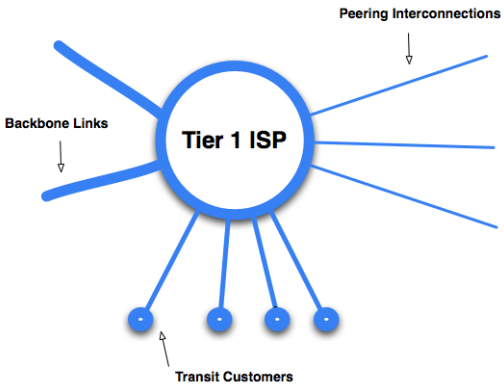

Figure 3 Tier 1 ISP connections [35].

4.3.2 Tier 2 ISP (Transit Providers & Customers): these are Internet entities or ISPs who "buy" Transit to a Tier1 ISP or IBP in order to provide Internet access to their clients, usually cover regional geographic extensions, with presence in some interconnection points to make upstream connections through their transit providers, and also provide transit to lower tiers Internet entities.

Furthermore, some tier 2 ISPs would establish private peering agreements between entities of the same level in order to extend their reach in the Internet, reducing *transit* costs, latency due to long paths or simply have more control in BGP routing.

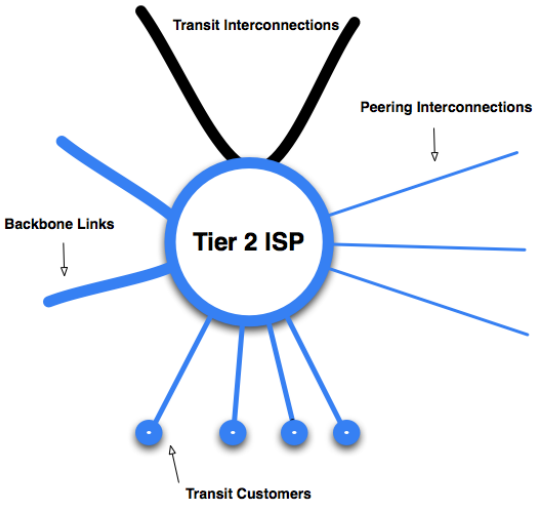

Figure 4 Tier 2 ISP Connections [35].

4.3.3 Tier 3 ISP (Small ISP and Access ISP): Represented by all the ISPs that buy transit to higher hierarchy ISPs and do not sell it again (contrary to the previous case). They cover local scopes and provide Internet access to companies and domestic users. These ISP only have connections to their *transit* providers.

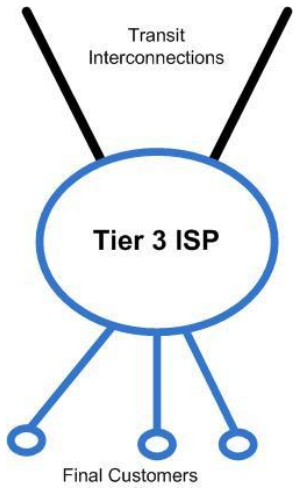

Figure 5 Tier 3 ISP Connections

The architecture achieved by the connection made in a tiered hierarchy of the beginning of internet, in the past 15 years, is shown below in Figure 6:

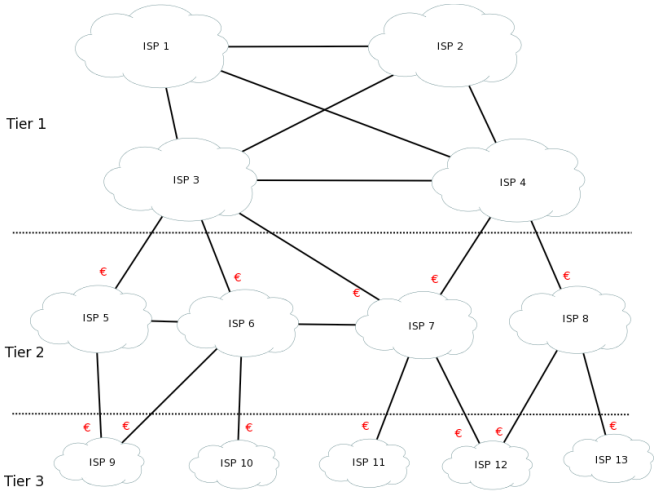

Figure 6 Traditional Internet hierarchy of Tiered ISP [36].

This architecture has suffered different changes due to the evolution of the Internet with the rising of contents providers (CP) as an Internet entity, e.g. Yahoo! in 1995, Google in 1998, Youtube[6] (2005) and this has changed the way how those interconnections are made.

Currently, the scenario is totally different, the following figure give us an idea of the actual architecture with the inclusion of IXP (Interconnection Exchange points), explained also in this section.

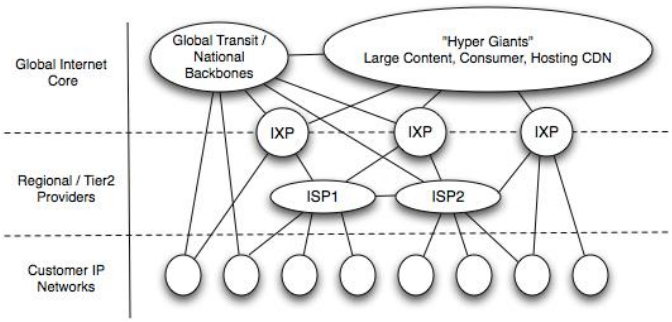

Figure 7 Emerging architecture of Internet [37].

4.4 Content providers (CP): is an Internet entity focused on content creation, storage and delivery for the Internet users. To delivery those contents, a CP has to be integrated to the Internet service providers to allow the access of these contents through a BGP peering connection.

Web Caching is also a kind of CP. It usually refers to the storage of web pages requested by clients of an ISP, in order to have an actual copy of them and avoiding request again the same web page content, having a recent version of the content, accelerating the response times, reducing *transit* costs. (e.g. Google Global Cache [38])

[6] YouTube actually belongs to Google since 2006, it has been the biggest video streaming website on Internet. [73].

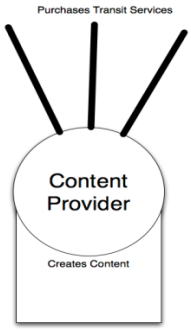

Figure 8 Content Provider Connections [35].

In order to reduce costs through *transit* connections, some ISP establish strategic connections to high demand content providers reducing response times. This arise of CP and their high demand by users to access these contents in the last few years, specially Video services, e.g. Video on demand VoD, Video Streaming (Youtube, Netflix, Vudu, etc.) or video sharing (representing 26.1% of Internet traffic in 2010, according to [6]).

4.5 Autonomous System (AS): is a collection of IP protocol prefixes[7] under the control of a network administrator which represents a common policy especially applicable to EGP (exterior Gateway protocols) to interact with the Internet, defined by the IETF under RFC 1930 [39].

4.6 BGP: Boarder Gateway Protocol is the EGP protocol used to exchange routing information through Internet. It makes possible for ISPs to connect to each other and to share information regarding their connected networks, providing access to their clients.

The information shared between routers belonging to an ISP through BGP, allows the conforming of the "Internet routing table" from a router point of view, hence having paths information to reach any destiny in the Internet.

BGP became a standard of Internet first time in 1989, defined initially under RFC1105 [40], suffering some modifications until the actual version BGPv4 or BGP4 was released in 1995 under RFC1771 [41], and updated to RFC4721 [42].

With upgrades in its 4th version in 1995, BGP4 revolutionized the way of ISP interconnection on Internet (this is due to the *Routing Policies* implementations), producing as consequence the big impulse of Internet in 1996 [43]. A Routing Policy allows an ISP to realize specific prefix announcements to their peers, establishing an efficient way of multi-homing. This allows the definition of specific connections in terms of preferential routes and QoS

[7] Terms "prefix" and "Autonomous Systems" accords with the RFC1930 "Guidelines for creation of an AS" [39].

techniques, Hot-Potato routing implementations, as suitable approaches to multihoming connections.

4.7 Multihoming: is a method in which an ISP can connect to more than one ISP through BGPv4, in order to increase their reliability, having alternative path to reach networks in Internet, load balance, etc. [44].

4.8 Peering: Term used commonly to represent interconnections between two (o more) Internet entities (Usually ISPs), which through BGP protocol those entities exchange route tables and prefix announcements of their Autonomous System (AS).

The traffic exchange in BGP is made by each ISP sending their route tables referred to the networks belonging to their Autonomous System to their neighbour.

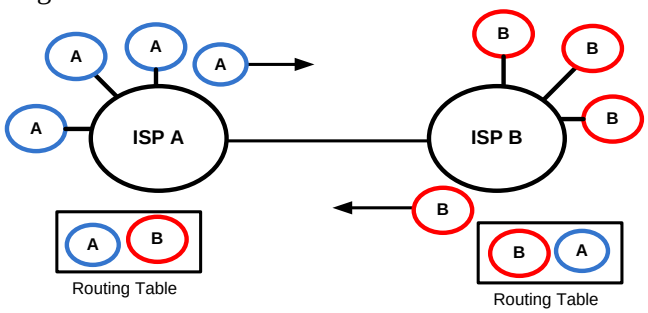

Figure 9 Basic Principle of Peering [45]

The Figure 9 represents an interconnection agreement example between ISP A and B, who exchange routing tables through BGP, allowing each ISP to know how to find routes or paths to reach any user belonging to the other ISP.

There are some different kinds of peering agreements as shown:

a) Free Peering: this agreement is made commonly between IBPs or big ISP. Usually there is no cost involved, this because traffics exchanged between big ISPs is normally symmetric (outgoing and incoming), hence there is no need to charge for traffic incoming if the outgoing is similar, they only have to pay for the physical connectivity cost between their devices (F.O. Carrier, Metro-Eth connection, etc.). Only customer routes are exchanged in this type of connections, which are also called BLPA (Bilateral peering arrangement) [45] or SKA (Sender Keeps All) according to [43] .

b) Paid Peering: this relationship is a peering with compensation from one of the involved parts due to an asymmetry of traffics, here still being exchanged only customer routes, but with an associated charge for the connection.

c) *Transit* peering: regarding to those connections previously mentioned on "Tier 2 ISP" statement, which an IBP "sells" access to smalls ISPs, in order to have access to the whole Internet[8].

These agreements used to be expensive due the reach to Internet path that has the IBP, carrying IP packets from the small ISP to their final destination through its network, reason why these connections are called ***Transit***.

Transit agreements are most common in the Internet environment, due the ability to incorporate Small ISP, companies or any institution with an AS to the Internet, and have increased even more with the presence of the CP, the most important Internet entity in the Internet evolution nowadays.

d) Partial Peering: there is also the option of buying transit in a partial way, this in order to reach regional routes, e.g. in Europe, to reach the routes of specific region or country, it seems a cheaper approach to peer with a country ISP to expand reach area than to purchase costly *transit* to an IBP**.**

This Classification allows representing the peering relationships in terms of routes exchanged and the cost of them, as shown in Figure 10.

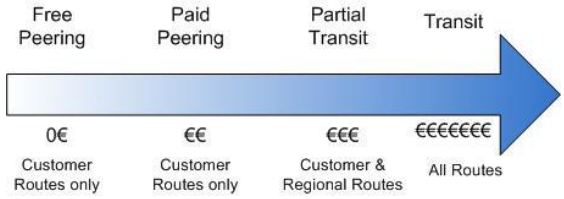

Figure 10 Peering cost classification [46]

Public and Private Peering:

There is also a classification of interconnection Internet entities in terms of the location of physical and logical connection between them as show below:

e) Private Peering: Also known as *Secondary-Peering*, private peering is an agreement between ISP, not usually seen by another Internet Entity, only the involved parts know about its existence, this in order to extend their reach region to the Internet through these peer connection. I.e. suppose two ISPs enjoy transit peers with different IBPs, and each IBP cover different Internet regions, both ISPs agree to make a private peer connection, hence these two ISPs will have now increased their reaching capability to a bigger Internet Extension without pay any more money for *transit* connections. Private peering establishments would take in place at NAPs (Network Access Points) or PoPs (points of presence) through dedicated connections; it would incur some

[8] Referring to "The Whole Internet" as all Internet regions through connections made with IBP that allow reach any destination. It is also called "Global Internet".

associate cost, or could be free of charge, depending on the economical agreement between those parts.

f) Public Peering: Peers performed in public places, usually NAPs or IXPs (Interconnection Exchange Points) after agreement by the interested parts. The main difference with private peering is the place where the connection is made [43] as shown in Figure 11

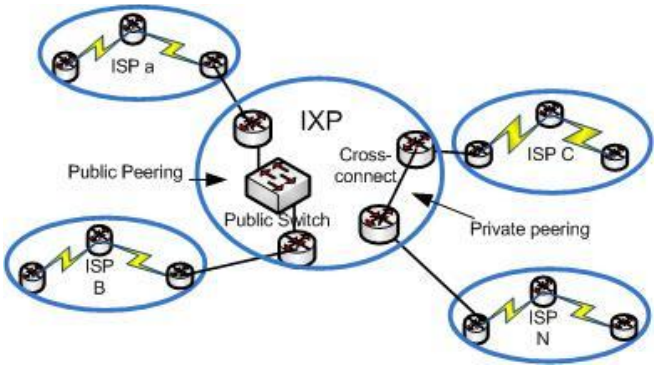

Figure 11 Private and Public peering scenario.

Definitely it can be noted that Free Peering is usually performed between entities on the same tier, Paid peering or *transit* could be performed between different tiers entities, as shown in Figure 12.

4.9 Peering Policies:

Peering Policies are established by an ISP to define how to peer with other ISP o Internet entity with its network. The peering policy will be conditioned by the characteristics of the ISP candidate, if it has presence in IXPs or its tiers Hierarchy, its network extension, amount of prefixes announcement, traffic statics, etc.

There are four types of policies defined to establish a peering relationship according to [35]:

1. **Open:** Be willing to send and receive all the announcements from any ISP
2. **Selective:** Willing to peer under some conditions or pre-requirements.
3. **Restricting:** Not generally interested in peer with any ISP.
4. **No-peering:** No peering intentions (preferences with buying transit from an ISP.)

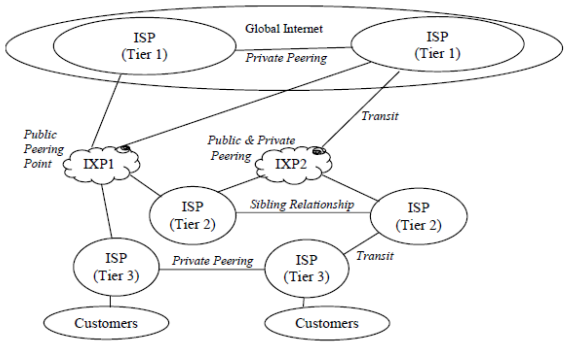

Figure 12 ISP Interconnection relationships [47].

5. Content Delivery Network (CDN):

By the raise of the CPs (contents providers), previously mentioned in this document, there has been an initiative of big CPs in building their own networks of regional or global scope, in order to have better connectivity to their end users. This is achieved by bypassing bigger ISPs and connecting directly to the access ISP (Tier3), reducing OWD, obtaining competitive performance with respect to the alternative of buying transit toTier2 ISP.

These CDN alleviate in part the traffic load in IBPs, but affect their traffic patterns, due to the fact that traffic originating from the CPs to the clients will not be passing through the net of the IBP, traffic that could become asymmetric from the point of view of the IBPs, only receiving the traffic from user as contents requests to those CPs. As shown in the Figure 13 the content requested from a customer to a CP can pass through a CDN and bypass all the transit providers (IBPs) in the Internet on the path to reach the ISP, achieving this more direct communication, sometimes faster and with fewer hops to reach the destination.

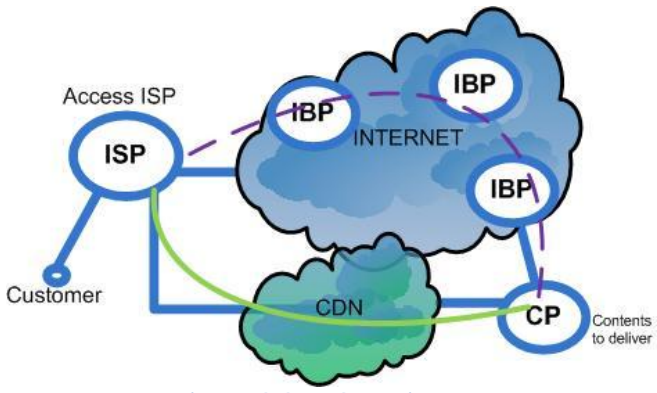

Figure 13 CDN Scenario

On the other hand, CDNs also affect the business scheme on the IPBs or Tier 2 ISPs, because all these traffic alleviated that does not pass through their networks cannot be charged as *transit* when the agreement involved in the business is based on traffic amounts.

The appearance of CDNs has been a milestone on the Internet Architecture, they have literally flattened the Internet architecture, the CDN know as the past as "the growing of WAN links in CPs" in [52] observes and notes the decrease on IBPs traffic as consequence of growing CDNs by the ability of establishment of more peering connections between CPs and access ISP.

5.1 ISPs as a CDN provider

In order to have an important role in the Internet and getting an advantage of their big deployed infrastructure, many IBPs have also promoted CDN services as a market strategy for not losing clients who prefer the services provided by CDNs.

So in these terms, a model for peering agreements with CDN has been presented as an attractive proposal called "CDN peering" for access ISPs, enterprises and others customers willing to purchase those services.

These "*CDN peering*[9]" affects the IBPs business, reason why sometimes an IBP could have a "no-peering" o "restricting peering" policy to any CDN provider (as a possible business rival) or accept only paid peering in order to offer the same service under its infrastructure.

5.2 CDN Interconnection

As a result of these strategies from the IBPs, some CDNs are interconnecting each other, trying to reach more access ISPs and thus more clients. The IETF in [53] describes a model of interconnections between CDNs, mentioning a content interconnection gateway (CIG) as an element term of the model, which is responsible of the peering and connections with others CDNs, all these in the same context of ISPs in order to extend their CDN services.

6. Interconnection Exchange Points (IXP):

Initially called NAP (Network Exchange Point) or MAEs (Metropolitan Area Exchanges) in the 90s, they represent an interconnection model developed in 1995 by NSF (National Science Foundation) [48], with the aim of growing their scientific national network, for educational and research purposes NSFNET (National Science Foundation Network), in which different research agencies of the United States were interconnected in a "NSF Backbone".

In 1993, a lot of commercial firms noted the popularity of Internet, showing interest on interconnecting to the growing Internet. In 1995 the NSF granted contracts for building three NAPs in the United States in order to provide interconnection with commercial networks to the ordered traffic exchange in Internet, producing the dissolution of NSF Backbone.

This in fact enabled the commercial and privatized Internet, because these private companies carried out a faster deployment of interconnection points, called CIX (Commercial Internet Exchanges) or NAPs, which was a milestone in the Internet Expansion those days.

Nowadays the IXPs are denoted as NIX (Neutral Interconnection Points) or NAP, being these as NSF conceived in principle, a unique physical infrastructure (including energy conditions as redundancy, environment conditions, access control security, monitoring, etc.) managed by an unique entity[10] in order to facilitate the Internet traffic through the interconnection of diverse ISP networks based on peering agreements.

In a NIX there are interconnections between peers of the same geographical region, allowing then to carry traffic of local scope (e.g. to reach an Internet service in the same country or continent it is not necessary to reach bigger IBP in others countries to find the path, if the other service can be reached in less hops), producing shorter paths to local destinations, reducing latency, and avoiding international/inter-continental paths that incur in *transit* costs.

An important feature of NIXs is the ability for small ISP (Tier 3 ISPs) to interconnect to bigger ISPs or *transit* providers present in the same IXP, reducing costs related with transport circuits for dedicated links to PoPs in order to make a peering or transit connection, due to the facilities provided being member of an IXP.

IXPs in Europe:

The first IXPs established in Europe were the Finish Commercial Internet Exchange (FICIX) in 1993, the London Internet Exchange (LINX), Amsterdam IX (AMS-IX) in 1994, in Germany DE-CIX (Deutsche Commercial Internet Exchange) in 1995, in Spain ESPANIX (Punto Neutro Español de Internet) in 1997 en Madrid and CATNIX (Catalonia Neutral Internet Exchange) in 1999 in Catalonia.

All of this IXP are members of the European Internet Exchange Association (EURO-IX), founded in 2001 by the principal IXPs of Europe, its main purpose being to promote and enhance the IXP community, sharing experiences and procedures standards coordination related on IXPs management [49].

[9] These concepts of CDN peering also could be seen as peering for specific type of entrepreneurs regarding the service they provide, named as e.g. "Video Peering", "VoIP peering", "Low-Latency Peering".

[10] In IXPs, the NAPs are usually managed by a private company and NIX are managed by a nonprofits organization. In both cases they have the same purpose of administration.

IV. QoS in ISP Interconnection

The analysis of different consultancies in the Internet scope and behaviour of consumers such as [6] [43] [50] has evidenced beyond the big demand of traffic, the need to establish QoS for certain services vulnerable to delay, jitter and packet losses (e.g. VoIP, VoD, etc.).

An ISP can provide an ensured end-to-end QoS inside their AS domain, its own network, managed by their ISP administrators under diff Services techniques [54] such as PHB forwarding, the use of queues to mark and differentiate traffics by QoS classes in each device belonging to that AS (e.g. routers in the AS domain). As noted, this could be seen as a common policy on the AS, in order to achieve the QoS requirements of the service offered to their clients.

So, in this way QoS can be ensured in an AS, supposing then that hosts located in the same network AS can have a guarantee of QoS in their communications.

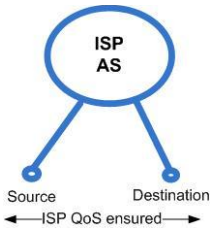

Figure 14 QoS in the ISP´s AS.

But when source or destinations are not in the same AS, the ISP cannot ensure QoS in these communications (see Figure 15.), each ISP or Internet Entity became connected to it could perform different policies for assuring QoS on its own domain, and then there would exist an incompatibility of the implementation of these policies in the exchange of IP traffics.

In fact, it could produce the treatment of a top QoS class treated incoming from an ISP, to be treated as BE (Best Effort) o lower class, contributing this to the service quality degradation.

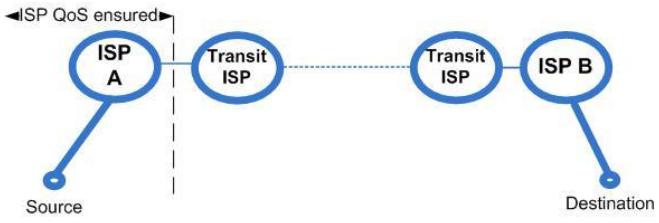

Figure 15 ISP QoS scope in their own AS.

Here it is presented the need to establish some QoS mechanisms in the interconnection between ISPs, in order to assure the end-to-end communication with a certain QoS level.

It technically seems possible to implement QoS inter-providers and inter-AS. An example given to these techniques are the QPPB (QoS Policy Propagation through BGP) described in [55], a technique to propagate QoS policies between different AS or ISPs Domains through Border gateway protocol (BGP), but all these methods can be achieved under some previous agreement between the evolved parts (ISPs or Internet Entities).

The issue of QoS on ISPs interconnection is a little sensitive in the context of partner/business relationships, thus that a set of Internet entities could have QoS preferential treatment for this partner´s traffic. So that leads us to enumerate the biggest Advantages and Drawbacks of implementing QoS in the ISP interconnection scenario:

Advantages

- The ability of ISPs to provide a certain QoS to the user through a multi-provider environment, such as the Internet.
- The opportunity of CDNs to expand their services focused on Video and delay tolerant applications, in the strategic relationships with ISPs or others entities.

Drawbacks

- The QoS essentially differentiate traffics. This could be seen as discrimination for some kinds of traffic flows, e.g. the traffic from a CDN.
- It could be seen as a breach of net neutrality principle in the context of "open and neutral" Internet.

To implement these QoS inter Provider or Internet Entities there should be an agreement between those involved parts as previously mentioned. This agreement is the **SLA** (Service level agreement), specifically in the ISP interconnection context, a ***Peering SLA.***

The IETF propose in [31] a set of considerations for the agreements for Inter-providers QoS in the Internet scope. It describes three scenarios in which QoS could be implemented:

1. **QoS in a single ISP domain** where the source and destination are in the same AS network. There is a quite easy to implement QoS due to the service provider has control of all devices in the transit of the packet for these communication using PDB techniques such as having a policy routing in the whole AS in order to provide the QoS to specific applications or services.

This can be achieved by PHB techniques such as marking packets through setting a DSCP (Differentiated Services Code Point) value on the IP packet to the incoming traffics, in order to differentiate flows such as Expedited Forward (EF), assured forward (AF), Best-effort (BE), etc. This flows can be adjust in order the requirements of these services (e.g. VoIP flow or low-latency) by metrics such as thresholds for jitter, OWD and PLR.

The Figure 16 shows the scenario in which the communication between the Source and destination occurs in the same AS network, in which the packets have the same treatment according to the domain policies for each service.

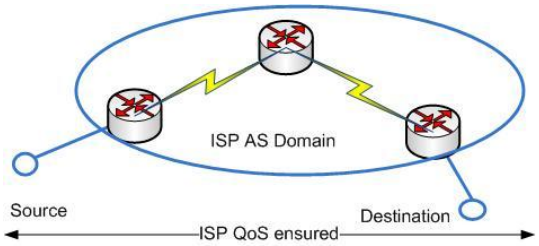

Figure 16 Single Domain ISP QoS

2. **QoS in different domains** composed by a set of small ISPs or Internet Entities with mutual business interests, e.g. SPs focused on VoIP, or video services, or it also could be a set of CPs or CDNs.

   In this scenario, the Internet Entities involved could have similar domain policies regarding the type of traffics they carry in terms of specific parameters, e.g. Video Content Providers which use the same video codec standard should require exactly the same thresholds for OWD, PLR or jitter to ensure the Quality of these video content offered.

   There is a suitable scenario for successful QoS interconnection given the common interest of the stakeholders in delivering their flows with a specific service class, encourage them in business development, being this a good strategy to reach more clients. The more common and profitable case could be CDN interconnection in order to expand their services maintaining their QoS levels (Figure 17).

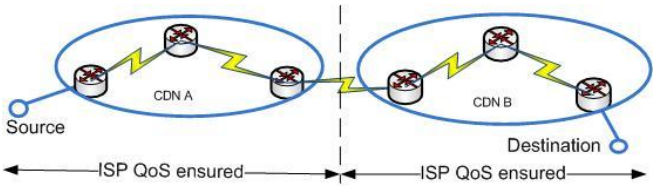

Figure 17 Domain with same interest QoS

3. **QoS in the Internet** in which services can be delivered from any source to any destination.

   In this scenario for an ISP is difficult to ensure the QoS that the neighbours ISPs connected with it can provide or even though know which are the ISPs involved in the path to destination. Besides the initial ISP does not know the exactly path to reach the destination and, as consequence, if the packets would be carried by a QoS aware Internet Entity.

   This scenario is denoted as the most important representing a big challenge due to the huge extension of Internet, their constant changes and the diversity of traffics flows presents on it.

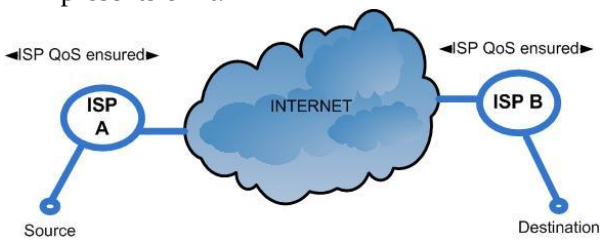

Figure 18 ISP QoS in Internet scenario

It is well known that each ISP can provide a QoS levels under their AS domain, here defined as "local QoS class" (L-QC) for these level of QoS offered by an ISP. E.g. An ISP could perform 3 L-QC such as, Expedited Forward low-latency class, Assured Forward and Best-effort Class which must be supported by their network devices in their AS.

The limits of these QoS parameters values required to achieve a certain L-QC that an ISP should provide in order to interconnect with other ISPs are called Meta QoS Class (MQC).

The MQC is used as exchange label to ensure the Interconnection with an acceptance of QoS to the other Neighbours ISPs and then in the rest of the ISP chain[11], conform by the rest of neighbourhood of ISP interconnected until the destination is finally reached.

In the first ISP, who provides Internet access service, providing an L-QC does not have any QoS control on the ISP Chain neighbours, it only can assure

[11] An ISP chain is the set of connected ISPs that ensure connectivity of the communication once the packet leave the ISP source to the destination.

the ISP in their domain, as show in Figure 19.

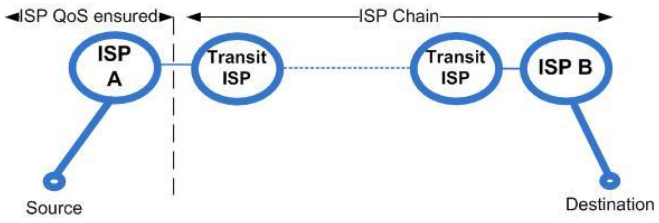

Figure 19 ISP Chain

The approach also notes the vulnerabilities of the MQC exchanges between ISPs if there is a failure in the ISP chain, unexpected changes (physical or failures) or an even more usual issue: **The lack of trust relationship between ISPs**. The trust relationships arises as consequence of SLAs agreements done between those entrepreneurs, in some cases the trust relationship could be interrupted by the not fulfilling of clauses on these agreements.

V. INTER-PROVIDERS SLA

The inter-provider SLA is a document that specifies and defines the conditions to build a trust relationship between two Internet Entities. Usually an SLA creates a win-win situation, in which all the involved entities obtain a benefit of this agreement [56].

The SLAs between ISPs have to include at least the same terms and establishment procedures than SLAs between ISP and Customers have.

In order to establish and manage a SLA between Provider and Customer, there are no standardized procedures but best practices and frameworks exist to deal with it such as ITIL (Information Technology Infrastructure Library)[12], proposing processes regarding with service level Management in IT services, which are roughly similar than Telecommunications services.

The principles on SLA establishment between ISP and Customer require parameters such as minimum conditions of availability[13], reliability and QoS parameters, which the ISPs should provide to their customers after closing these contracts.

To establish an SLA inter-provider it is necessary to define the parameters in which these agreements will be based.

Initially as QoS parameters defined in section II, the IPPM (IP Performance Metrics) [16] give a defined description of these terms to consider, among which One Way Delay (OWD), jitter (IPDV) and Packets loss Ratio (PLR) are the most important regarding the type of service performed between these involved entities (basically Internet Access).

In the scenario of Inter-Provider interconnections, these requirements of QoS parameters should be more specific given the service provided between the involved entities, which are IP traffic exchanges.

As explained before in the *Routing strategies related with ISP* Interconnection:

Apart from the peering policy or the way of peering with other ISP, there are some routing strategies involved that have influence in the ISPs operation performance:

Hot-Potato Routing: or *deflection routing*, it's a type of routing which seeks to have a packet in transit through an AS as little as possible, sending immediately to the next neighbour AS to reach its destiny. This routing conduct reduces the need to keep packets in buffers in the AS. Hot-potato routing is commonly used in free-peering agreements.

It works as shown in Figure 2: Supposing there is an end user in Backbone 1 requiring services of a CP located in Backbone 2, so:

5. Backbone 1 exchanges the content request from the end user to backbone 2 through the nearest Interconnection point (IXP1).
6. Hence this traffic will be carried through backbone 2 to the CP.
7. The return traffic will be sent through backbone 1 to the nearest interconnection point (IXP2).
8. Finally backbone 1 carries the traffic back to the end user.

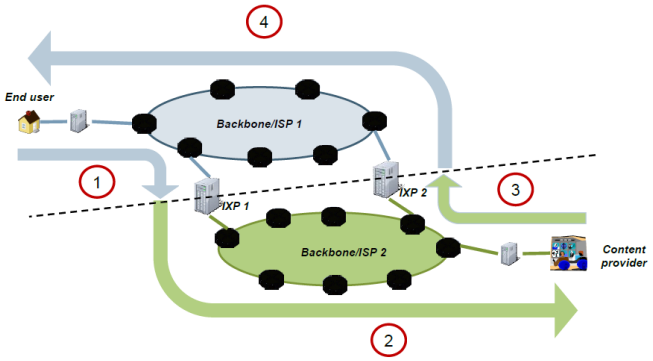

Figure 2 Hot-potato routing

Cold Potato Routing: In this case, packet buffering is performed in an AS carrying them through its AS to get to the next AS destiny. This option is mainly more costly than hot-potato routing, due to the longer transit routes in the origin network. The rationale for this is to

[12] ITIL is the most widely accepted approach to IT service management in the world. ITIL provides a cohesive set of best practice to public and private sectors.

[13] The term of availability is out of the scope of this work, and it is related to an IXP and physical aspects on the ISP interconnection.

have more control of the packets in the network under certain QoS, during the transit of the packet in the network . This type of routing is usually performed in CDNs (Content Delivery Networks).

Quality of service (QoS) statement on Section III Definitions, Assumptions and Notation, the SLA is composed by Service Level Specification (SLS).

The SLS represent a specific set of QoS attributes required from an ISP to others connected with, in order to accomplish the SLA between those entities (ISPs or CPs) that could be specific for certain service.

The relevant parameters included in SLS in the ISP Interconnection are the OWD, jitter and PLR, as QoS parameters required for the wide range of services that can be carried over the Internet, e.g.: SLS for Video transmission will require specific QoS parameters such as Low jitter and OWD thresholds, and minimum rate of PLR, depending of the codec used for that video service requirements, etc.

When the SLS and the services to provide for each involved entities are negotiated, including the economic and business terms[14] of the agreement, then the SLA is closed between these entities, assuring QoS on their interconnection as is shown in Figure 20, but it still remains the issue of ensuring QoS in the ISP Chain interconnection path until the destination is reached.

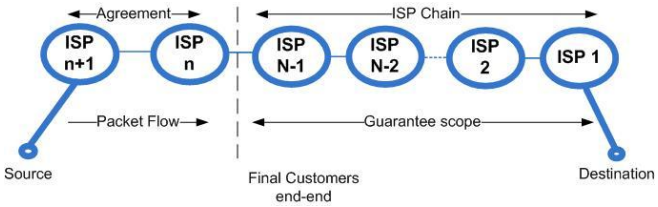

Figure 20 ISP SLA

A new term called pSLS (Provider SLS) is introduced in [57] as an explicit QoS requirements in the ISP interconnection. The authors proposed a proxy QoS distribution systems architecture, located parallel to the ISP AS edge devices (in a Management plane), in order to manage the QoS on Internet Paths. The proposed pSLS advocates the use of concatenating all L-QS of the ISP from the source to conform extended Quality class (e-QCs) in the ISP chain to remote destinations.

The SLS distribution to achieve the SLA requirements in this approach suggests an architecture where the QoS proxy is the key player on it. The QoS proxy play the role of SLS broker, receives the SLS requirements initially from the client (cSLS) to the access ISP, which adapts their QoS service class to provide to a pSLS, which is the SLS that can provide for the incoming flow in their AS domain, then the service provided by the access ISP will become a pSLS to the next QoS proxy of the neighbour AS, the process will be performed on each hop between autonomous systems until the destination is reached.

This recursive method, presents a scalable approach to ensure a QoS level in an ISP chain path from source to destination in order to achieve an approximation of end-to-end QoS.

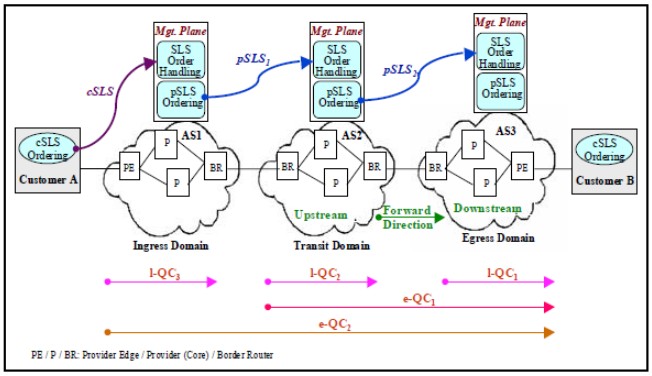

Figure 21 SLS Cascade Distribution Approach [57]

The method described previously is represented in Figure 21 shown as cascade distribution method in attempt to deliver the pSLS assuring a SLA accomplishing up to destination ISP.

Notice that pSLS distribution only can be performed with adjacent ISPs due to the communication that should occur between QoS proxies present on each interconnection. Is to remark, the above figure represents the e-QC conforming to the agreement of SLS (cSLS-SLS or pSLS-SLS) between two entities and their growing up to finally reach the destination ISP.

There are considerations to take in to account due to factors like constant changes in the pSLS by the Internet behaviour, such as Link down failures, BGP route changes, new peering decision policies[15], and others issues. If there are some of these events, the system has to recalculate the pSLS and distribute it through the path to destination, so it requires an up-to-date architecture to give reliability in terms of new QoS ensured paths establishment in case of contingency.

Another remarkable consideration is related with the associated cost to providers by the implementation and

[14] The SLA negotiation as service contract, involves economical and business terms, which out of the scope of this work.

[15] About peering decision policies there are some strategies made by ISPs in BGP peering scope that could affect the performance of others ISPs described in [72].

maintenance of a Proxy QoS infrastructure in a management plane in order to ensure QoS.

The EURESCOM had also proposed a framework for the specific case of CDN interconnection providing recommendations to ISPs about the interconnection SLAs in economic terms in their project p1955 [58]. This project has been oriented in market models[16] scope, about the cycle of money flows when users contract a service through a CDN directly or indirectly on a set of use cases proposed on the project.

Ongoing Works related with Interconnections managing QoS in Internet

It is important to remark the efforts made from research and development bodies on the QoS management on Internet. Specifically, projects developed by the European Commission and private partners; those are part of the Information Society Technologies Programme (IST):

- **TEQUILA Project (Traffic Engineering for Quality of Service in the Internet, at Large Scale)** 2000-2002 [59]. Their main objectives are**:**
  - Specification of static and dynamic, intra- and inter-domain SLSs to support both fixed and nomadic users.
  - Protocols and mechanisms for negotiating, monitoring and enforcing SLSs.
  - Intra- and inter-domain traffic engineering schemes to ensure that the network can cope with the contracted SLSs.
- **MESCAL Project (Management of End-to-end Quality of Service across the Internet at Large)** 2002-2005 [60]. The key objective is to propose and validate scalable, incremental solutions, enabling flexible deployment and delivery of inter-domain QoS across the Internet at large, in order to:
  - To develop business models, based on current commercial practice and emerging business scenarios.
  - To specify a generic, multi-domain, multiservice functional architecture for the flexible deployment and delivery of inter-domain QoS-based services. Develop templates, protocols and algorithms for the specification, negotiation, subscription and invocation of QoS-based IP services between customers and ISPs and between peer ISPs.
  - To enhance existing inter-domain routing protocols and algorithms and to investigate new approaches to convey QoS information to enable scalable inter-domain traffic engineering solutions.
- **AGAVE Project (A liGhtweight Approach for Viable End-to-end IP-based QoS Services)** 2005-2008. [61]. AGAVE's key objective is to develop an approach for open end-to-end service provisioning in order to support added-value IP-based services. The focus is the core networks of the Internet, and "end-to-end" means across these core networks. Quality of service will be enabled through different Network Planes within domains, whose interconnection will form global Parallel Internets that will support the needs of well-defined services, with VoIP being a key service. Specific sub-objectives are to:
  - Specify a business model for the stakeholders, including customers, ISPs and CDN identifying relevant open interactions, e.g. SLSs required, between ISPs for service provisioning.
  - Investigate the inter-domain extension of these planes to form Parallel Internets and the inter-connection of non-adjacent QoS-enabled domains.
  - Investigate how to select and control optimal inter-domain paths. Investigate approaches for parallel plane separation to support QoS-aware networking.
  - Devise intra and inter-domain traffic engineering approaches for the coexistence of the Network Planes and Parallel Internets respectively.

These ongoing works briefly described and the proposed studies in this section represent the of efforts from research bodies, private partners (such as SP`s and technology providers Research + Development centres) and public entities such as the European Commission in terms of the SLA establishment and management on inter-providers as a manifest of the relevance on the improvement of Internet and services supported through it.

VI. MEASURING INTER-ISP QOS

The way to prove that a SLA is fulfilled between the parties is by checking the result of the quality of the service provided; this can be achieved by measuring the parameters in which SLA are based, basically defined on the SLS (Service level Specifications).

These parameters (OWD, jitter and PLR) should be objectively measured (according to ITU-T E.802 recommendation [62]) in order to obtain empiric data to compare with the negotiated SLA, as well as exact conditions about the measurements, time of

[16] The market models in the ISP interconnection is not a included in this work.

measurement, frequency of measurement, data measurement format taken by both involved entities.

In the SLA between ISPs the protocol used to measure the QoS in the Inter-ISP QoS should be clearly described. To measure OWD, Jitter and PLR in one way, a suitable protocol to achieve this is the OWAMP (One-Way Active Measurement Protocol) a protocol that allows to measure IPPM defined by the IETF in [63]. To measure the parameter in the two way path, the suitable protocol is the TWAMP two-way Active measurement protocol [64], based in OWAMP, a little more complex to implement due the need of synchronization clocks in both sides of the measurement path link.

According to [23], the points of measurement could be devices such as edge routers or servers bounding with other ISPs, called Inter-ISP Link (shown in Figure 22), these devices could be dedicated to measurement tasks or can be performing data exchanges operations while being used simultaneously for measurement.

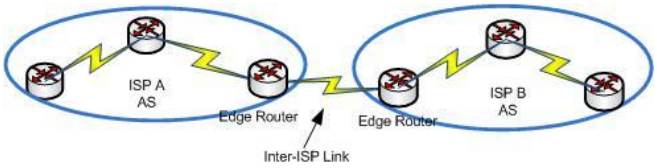

Figure 22 ISP devices involved in QoS measures

Not all providers use the same methodology to measure these parameters, so there are two relevant scenarios that could be present:

1. In which an ISP agrees with other on the methodology for measurement
2. In which the ISPs use their own measurement methodologies, so that both methodologies and devices should be approved by them consequently.

It is also a clear fact that those ISPs should cooperate to define the points of test to perform the measurements, especially if there is one or more Inter provider links between them located in point of presences or IXPs.

An IXP is shown as the most efficiently point of measurement; one of the main advantages of the IXP is their ability to connect to any other ISP present in the same IXP, so it will allow measuring IPPM to the different inter-ISP links of their peers as shown below.

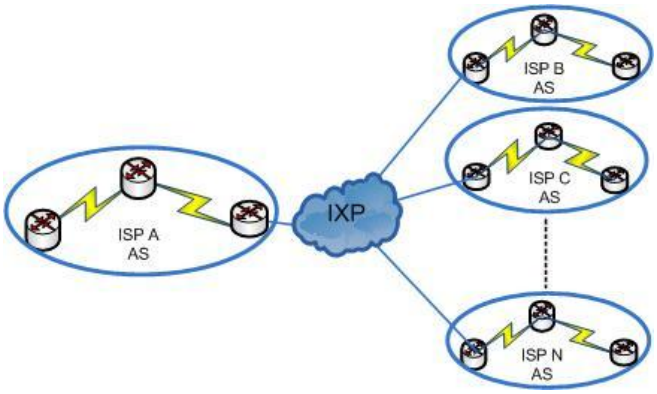

Figure 23 Inter-ISP Links in an IXP

This approach also allows a rapid deployment of measurement mechanisms for a new Inter-ISP establishment.

Regarding the measurement techniques, for the QoS parameters in IP traffics exchanges in a network path there are a lot of equipment and software tools available to perform this task, classically used in LAN (Local Area Networks) and links between devices inside ISP domain, in WAN (Wide Area Networks) links and any other networking scenario.

Procedures for QoS parameters measurement.

As mentioned before, the involved entities should agree the specific measurement procedures of these parameters that compose the SLS.

The IPPM framework proposed by IETF [16] establishes procedures for metric measurement following a set of principles:

- Direct measurement on the link to study through a traffic injection test.
- Projection of a metric from low level measurements.
- Estimation of a constituent metric from a set of more aggregated measurements.
- Estimation of a metric at one time from a set of related metric at other times.

It also refers that a measurement procedure has to be repeatable, in others words, the procedure should be able to be performed in the same conditions.

According to this, there is the need to establish some parameters to perform the measures.

About the **time of measurement**, the IETF in [24] and [65] proposes one-minute time periods for PLR and IPDV measurement respectively, in order to have enough amount to obtain samples, for this case 5 **minutes** is recommended.

In order to have a constant measurement and consequently a more accurate result, the recommended chosen **packet size** to perform the test should be as small as possible in order to avoid impact on network

performance, in this case the minimum IP packet size of **64 bytes.** The **mean packet separation** is considered of **200ms** according to [23]**.**

A summary of the procedures for QoS parameters measuring is shown below:

OWD:

- **Packet size:** even though an IP packet size could be up to 1500 bytes, for measurement, the minimum size of **64bytes** is recommended.
- **Maximum Evaluation interval of the test:** 5 minutes
- Recommended mean packet separation 200ms.
- One value of OWD will be reported for each result.

Jitter:

- **Packet size** of **64bytes** is recommended.
- **Maximum Evaluation interval of the test**: 5 minutes
- Recommended mean packet separation 200ms.
- The Jitter measurement value is reported in ms, with a minimum value of 1ms.
- The 99^{Th} percentile value of the jitter distribution over the time of measurement [20], chosen as a stable value of 1500 samples of jitter values (5 samples per sec*5minutes*60 seconds) as better and accuracy measure. [28]
- One value of Jitter will be reported for each result.

PLR:

- **Packet size** of 64 bytes.
- **Maximum Evaluation interval of the test:** 5 minutes
- Recommended mean packet separation 200ms.
- The PLR measurement value is reported as percentage, established between 0 and 1.
- One value of PLR will be reported for each result.

After doing the measurements, ISPs should have agreed which information should contain the measurement report and how to exchange these reports between them, as well as the frequency of delivery.

The IETF draft "Reporting Metrics: different point of view" in [66] proposes point of view of the IPPM (OWD, PLR, and jitter) reports, in two point of view: *Network Characterization*, describing condition in IP networks for quality assurance and **SLAs.** *And Application Estimation* Performance, describing network condition in a way of determining values that affects application performance and finally the users.

According to this, focusing on the *Network Characterization* point of view about the manner of results reporting, it is recommended that reports at least content:

- Date of the measurement.
- Time of measurement.
- Location of the ISPs bound devices (PoP or IXP location, measurement devices, etc.)
- Measurement method/report period.
- Measurement type.
- Result statistics.

Monitoring measurement and comparison.

These results obtaining and their respective reports should be retained for some period agreed, in order to support diagnostics on SLA conforming.

The report should be exchange between the entities, to be compared with their own measurement reports to compare the SLS acceptance.

The acceptance of the SLS is provided by accomplish of thresholds levels set under certain QoS service class previously negotiated, the involved entities can choose QoS service class recommended by entities such as ITU [28] or establish their own thresholds for specific services.

In case of discrepancy on reports, an entity can complain and claim about the service provided to the other, supported by statistics or demonstration of certain irregular behaviour on the network reflecting on the QoS parameters degradation.

These issues on the service provided by the involved entities may produce the no accomplish of the SLA, and the provider which is not providing a right service could pay reduction in the charges to the other.

In worst cases, it could provoke consequently their contract rupture, disrupting the trust relationship or even an interconnection interruption, a non-desired event from both entities, which affects clients by the possible lack of reachability.

VII. PROPOSALS FOR SLA`S AND REGULATION PARTICIPATION.

This Section describes proposals for regulation in the context of QoS and SLAs in ISP interconnections.

1. Current developments

Initially, the NRAs or National Regulation Agencies, based their operation mode in terms of analogies to others fields, such as "the customer defence" on commercial activities", usually these

operation modes follows a procedure that starts from the complain from the customer from a illegal treatment form their ISP, study cases, create a register of the event and formulate a decision in order to enforce the correct behaviour from the ISP.

Until now this has been the operation mode from NRAs, regulate internet is totally different due the Internet architecture and the NRA should consider that an illegal treatment to a client not necessarily involve the Access ISP which provides the service, also involve a high-level ISPs interconnections and how they exchange IP traffics.

As mentioned in "Motivation and Related Work" section, regulation authorities are considering the need to regulate Internet; NRAs in the attempt to Some examples of the developments focused on the idea to regulate internet can be found in the "declaration on Net Neutrality" made by the European Commission [1] and from United States of America the FCC with their document "Preserving the Open and Free Internet" [8]. The latter proposes some rules in 3 priority scopes: Transparency, No Blocking and No unreasonable discrimination. Those rules became officially effective on November 20 of 2011 in the US, after the publication on the Federal Register in September 2011 [67].

In the EU, it had been decided to poll the scenario that conforms the Internet in order to have a glimpse of the state of the art and see how much is required a regulation participation in order to maintain the concept of Net Neutrality.

The European Commission in June of 2010 launched a public consultation on "The open Internet and net neutrality in Europe" [3], in which Networks operators, Content Providers, EU members countries and consumers participated in the consultation, related about "*Net Neutrality*" debate. In the report about the results of consultation, there are 5 important topics analyzed:

- **The open Internet – current problems, future problems and the suitability of the EU framework:** the answers reflect that currently there are no problems with the openness of Internet in the EU, but it was difficult to predict future problems. Nevertheless, the BEREC has reported cases of throttling of P2P file-sharing, video streaming, blocking or extra charge for VoIP services. Also as a possible problem expressed was that a managed service such as IPTV could present difficulties, as a product of effects on the best-effort performance caused because some networks could favour certain services more than other, causing degradation the Best-effort service.
- **Traffic management necessity, transparency and managed services:** the answers express that management is needed and essential to operate an efficient Internet, they agree that management is used for congestion and security issues and these are not contrary to *Net Neutrality*, nonetheless some answers criticise the abuse of techniques such as DPI (Deep Packet Inspection)[17], claiming that this technique is not needed to operate in the Internet.

About other forms of prioritizations, several answers regard to CDN (Content Delivery Network) which support the content providers in the delivery of these content to the clients. According to BEREC, CDNs do not arise net neutrality issues, so taking this in to account there is a divided position about whether QoS conditions should be applied to all managed services, arguing that nowadays there no needed additional measures.

- **Market structure:** A lot of responses agreed that the commercial agreement on provision of Internet access, such peering and transit had worked good until now. BEREC also agreed that the market structure is working properly under the needs of the customers, but note the need of being monitored to have a regulatory place when it will be needed.
- **Consumers and quality of service:** the responses consider that a regulatory intervention to set minimum QoS standards for Internet access would be counterproductive and impair the innovation. Some answer suggests establish a conduct code from EU "guidelines" in order to deal with the ability of set QoS parameters and avoid customer´s service degradation.
- **The political, cultural and social dimension:** there were received a few answers about freedom expression, pluralism and cultural diversity on the Internet.

This was an initial very important step in order to have a reference of the actual state of the Internet from all the entities conforming internet in those important 5 scopes, giving birth to a set of groups created by BEREC focused on Net-Neutrality specific key issues: *Transparency, Quality of service Requirements, Discrimination* and started to look in the *IP*

17 DPI (Deep packet inspection) is a technique that consist on computer network analysis of the data section of an IP packet, looking for protocols or patterns of the packets, in IP traffic flows, e.g. to indentify VoIP or P2P communication protocols. Through these techniques a provider can manage their network blocking or constraining traffics becoming from some applications.

Interconnection, these groups will be in charge of investigate these issues and evaluate the possible role of a NRAs in order to regulate them. BEREC started to publish documents about these issues between 2011 and 2012, as described below:

One of these documents is a report of public consultation on the draft ***"BEREC Guidelines on Transparency in the scope of Net Neutrality"*** [68]. For BEREC the transparency is a necessary condition for end-user to have freedom of choice, in this document BEREC elaborated Guidelines on how transparency obligations would work in practice, based on a public consultation which outcomes further developments on the Guidelines recommendations regarding to common terms references, monitoring processes and the option of a co-regulation process as future works for 2012.

The document Titled "***A framework for Quality of Service in the scope of Net Neutrality"*** [69]**,** BEREC introduces the competences for NRAs (National Regulation agencies) to set minimum QoS requirements for electronic communication in possible scenarios about when should NRAs set those minimum requirements and what those should be. It proposes a generic framework of evaluation and analysis for setting the QoS requirements and relates next works in elaborating further methods for NRAs use and promotes tools to end users in order to control and monitor the Quality achieved.

About the issue of *Discrimination and Differentiation*, BEREC had initiated an economic analysis of the potential and theoretical effects of discriminatory behaviour, studying the possible actions that the NRAs should take in the face of potential discriminator issues, under techniques of traffic management. For Discrimination and differentiation issues treatment, BEREC has created a document and public consult about the studies of this kind of IP interconnection issues, denoted as "Draft Report on differentiation practices and related competition issues in the context of Net Neutrality", according to "BEREC public consultations on Net Neutrality Explanatory paper" in the 2012´s midyear[18].

Regarding to the *IP interconnection* issue, BEREC started to look recently in the IP interconnection agreements (peering/transit) between market parties, which could produce net neutrality issues. In order to develop the market, these agreements should be followed closely; preparing procedures, for just in case regulatory actions could be performed when it would be required. For that reason, the BEREC had launched a Public consultation on this topic [70] with the publication of the Draft Report "Assessment of IP interconnection in the context of Net Neutrality" released on May 2012, as made before, in order to check the state of the topic by Internet Service Providers(ISPs).

[18] According to "BEREC public consultations on Net Neutrality" Explanatory paper (june,2012), http://berec.europa.eu/files/news/bor_13_34_public_consultations.pdf

2. Possible future regulation

Analyzing the efforts from these relevant regulation bodies (FCC for the USA and BEREC in the context of the EU), as a result of a progressive and continuous investigation and documentation work, some facts in terms of regulate the internet were evidenced, specially the user protection in terms of allowing full access to internet, transparency on the services provided, throttling of specific applications, blocking or discrimination of services.

Looking at this, is evidenced that regulation bodies had shown the interest on regulate Internet, achieving some progress, specifically on the scope of user-Provider relationship. As e.g. the FCC's Net Neutrality rules neither specify actions explicitly in the scope of the Provider-to-provider relationships, it just describes general actions, focused mainly in the user-Provider relationship scenario.

The BEREC with the formulation of "***Guidelines on Transparency in the scope of Net Neutrality"*** as mentioned before had considered the possibility of establish minimum QoS requirements, but is not described the scenario for ISP interconnections issues, assuming this is not yet included, so there will continue to be an ***absence of regulation,*** and thus neither the possibility of formulate ways to perform procedures in order to set and regulate *SLAs* in ISP interconnections.

Now BEREC until now just has published a document for a public consult in which ask for the wholesale level interconnection between ISPs and others Internet Entities, such as Content Providers [70]. This can be seen as another important step on have a knowledge base in the scope of ISP interconnections, expecting to analyse how Net Neutrality issues can arise by the high level connections among different AS.

In other words, the documents published, and the public consult mentioned before focuses in facts that could gain importance in order to preserve the open Internet, if not the Net Neutrality principle itself.

For regulation bodies this is a challenging task, due to the fact, that they had worked mainly in order to defence the user rights from strategies of providers in the Telecommunications market, looking for the equal competition of the providers and improve the Telecommunication services sector.

The European Institutions have given to the regulators powers for intervention in QoS issues, the BEREC has studied that, but it does not specify the scope of these powers, if it covers Access Providers-Users or Inter-Provider scope, it still not cleared defined, although it will depends of the legislation of the country in which the issue is presented, the type of ISPs involved on the issue and the specifications of the issue presented.

It is important to consider that some actions of regulators were initiated by complaints from users, who after perceive service degradation, had triggered the investigation of non-allowed strategies by providers, and start a regulation procedure in order to assure a suitable service.

As possible future case in the ISP interconnection scenario, the request to a NRA for intervention on IP exchange interconnection could arise from an ISP or CDN by technical issues or discrepancy on the service provided (service degradation) in terms of the QoS offered, that can be measure through methods mentioned on section "VI Measuring Inter-ISP QoS", which specifies explicit conditions of QoS measures in order to have a neutral information about the state of the Service provided/received.

The result of QoS parameters reports will be analysed by the NRA, to be compare with the SLAs conditions performed between the entrepreneurs related for that Interconnection.

Then the NRA will have enough information in order to discover the issue origin, that could vary from unsuitable routing or peering policies, the use of DPI, application blocking, or other reason that cause the SLA breach problem.

At this point the NRA will formulate a sentence about it, which will consist in changes on the routing strategies or peering policies for the guilty entity.

A brief sketch of this regulation process is shown below in Figure 24:

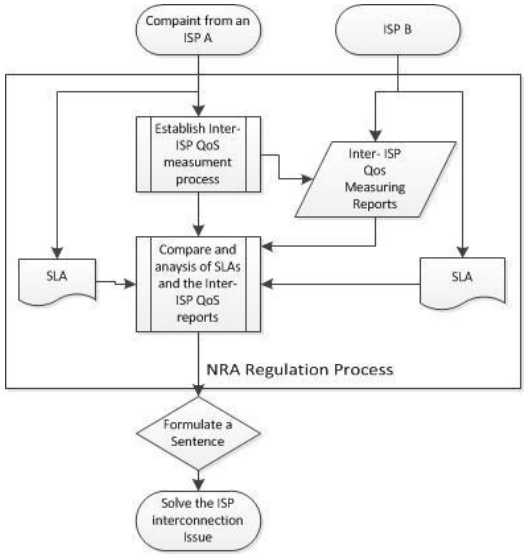

Figure 24 Possible future regulation in ISP Interconnections.

1. One of the Stakeholders (ISP A) involved, could complaint to a NRA in order to ask for regulation in their interconnection.
2. The NRA initializes the process of measuring Inter-ISP QoS.
3. Then NRA will compare the QoS measure results with the SLA´s related to the interconnection.
4. Finally the NRA will have enough information in order to formulate a sentence regarding to have a solution for the issue.

An e.g. for this scenario could be a CP complaining to a NRA for regulation through the SLA Measurement reports from a service contracted with other ISP, or by the change of the interconnection agreement model, from Free Peering to Paid Peering (See Appendix 1: Level3-Comcast Dispute).

Due the diversity con type of connections that can be perform between ISPs, regulators should develop methodologies in order to include all the possible cases in which the issues in which ISP Interconnection agreements can be present. One way of analyze those situations could be the verification or auditing of the SLAs between the ISPs.

Is very important to mention that, actually in the case of need for regulation from one of the stakeholders in an ISP interconnection could be present as very unusual cases, this due these interconnection were established by a commercial, strategic or association agreements between them. In high level ISPs and Internet entities, the out-of-service time, represent millionaire losses, in terms of money and clients. Thus the conflicts caused by a discrepancy

on ISP interconnections, usually are solved in a friendly negotiation without regulation intervention.

The ISP Interconnection is a very important topic in the conservation of *Net Neutrality* and openness on the Internet and it will be more evident in the future, where given the *Absence of Regulation* on this field, and the presence of Internet entities associations, the regulation bodies have to be prepared to deal with this issues in case of monopoly or abuse from one of the stakeholders.

To avoid this, Regulators would be present (as a viewer or mediator) in the Interconnections disputes in the scenario of Content provider to ISP, CDN to ISP or inter ISPs, but nowadays it only seems to be possible if one of the stakeholders have presented a complaint or discrepancy to a regulator, regarding the service quality perceived. In the best case, a regulator will have the power to intervene on the dispute, setting the minimum QoS parameters to achieve the Service levels for a proper IP traffic exchange.

VIII. Conclusion and Future Work

This section outlines a set of conclusions after the analysis of the IP traffic interconnection exchanges on Internet in this document.

The Net-Neutrality has been the focus and motivation for this work; as well as the study of the need for Internet regulation.

The actual state of art of the Internet and their interconnection evolution has been explained in detail, describing the rise and growth of new entities in the ISP-eyeball paradigm, the CPs and CDNs due to the patterns of increasing traffic in the Internet, focused in Multimedia application traffic, changing the tiered architecture of the Internet, flattening it. The different ISP interconnection agreements (*Peering, Transit*, etc.) are also described.

Once reviewed the complexity of the ISP interconnection Scenario, the routing strategies and peering policies and QoS were shown as a relevant facts in terms of meeting the requirements of services provided by Internet Entities, denoting at this point the importance of the establishment of SLAs as a key element to ensure the QoS between providers.

To ensure the SLAs fulfilment, methodologies of QoS inter-ISPs measurement are proposed, specifically for the relevant QoS parameters (OWD, PLR and Jitter) in inter-Provider Links, presents in PoPs or IXPs as efficient points of measurement.

Also guidelines were proposed for measurement reporting from each ISP involved, in order to examine performance of the service provided between those entities.

Proposals for Regulation of these SLAs were presented, in which the possible actions to perform to the stakeholders are closely related to changes on routing strategies or peering policies in order to assure the QoS level of the services provided and preserving the Net-Neutrality principle

There is still a research line on Net Neutrality issues from Regulation Bodies who are discovering this issue of the ISP interconnection as one of the most important fact on the Internet development and evolution. On the other hand, historically the Internet has been growing and developing exponentially on the basis of Non-regulation.

The regulation proposals in the scenario of ISP interconnection contained in this study reflect the importance for regulation authorities of being prepared in the field of regulation through the assuring of the QoS for services in a future in which these issues on ISP interconnection could impact on the openness of the Internet.

Acknowledgement

This work was supported by the *Comisión del Mercado de las Telecomunicaciones (CMT)*, in the cooperation contract number 10-230-0265 with *Universitat Politecnica de Catalunya (UPC) 2011*.

IX. References

[1] "Commission declaration on Net Neutrality," Union, European, August 2009. [Online]. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:308:0002:0002:EN:PDF

[2] BEREC. (2011) Body of European regulators for Electronic Communications (BEREC). [Online]. http://erg.eu.int/about/index_en.htm

[3] European Commisssion. (2010, November) public consult European Commission. [Online]. http://ec.europa.eu/information_society/policy/ecomm/doc/library/public_consult/net_neutrality/report.pdf

[4] European Commission. (2001, April) Communication From The Commission To The European Parliament, The Council, The Economic And Social Committee And The Committee Of The Regions. [Online]. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0222:FIN:EN:PDF

[5] Eupean Parliament, "Network Neutrality: Challenges and ResponsesI the EU and the US.," May, PE457.369, 2001.

[Online]. http://www.europarl.europa.eu/activities/committees/studies/download.do?language=en&file=36351

[6] Cisco Systems. (2011, August) Cisco Visual Networking Index: Usage Study. [Online]. http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/Cisco_VNI_Usage_WP.pdf

[7] FCC. (2011, october) Federal Communications commission. [Online]. http://www.fcc.gov/

[8] FCC, "Preserving the Open and Free Internet," FCC, GN Docket 09-191, 2009. [Online]. http://transition.fcc.gov/Daily_Releases/Daily_Business/2010/db1223/FCC-10-201A1.pdf

[9] "ITU-T E.800: Terms and Definitions Related to QoS and Network Performance including Dependability," ITU-T, ITU-T E.800, 1994.

[10] ETSI (European Telecommunications Standars Institute). (1994, October) ETR 0030: Network Aspects: General Aspects of Quality of service and Network Performance. [Online]. http://www.etsi.org/deliver/etsi_etr/001_099/003/02_60/etr_003e02p.pdf

[11] ISO (International Standards Organization) IEC, "ISO Quality of Service Framework. ," UK, ISO/IEC JTC1/SC21/WG1 N9680, 1995.

[12] TINA-C Telecommunications information Networking Architecture Consortium, "The QoS Framework. Internal Technical Report," TINA-C, 1995.

[13] ETNO, European Telecommunications Network Operators' Association. (1995) working group for QoS 07/95. [Online]. http://www.etno.be/

[14] EURESCOM. (2011) EURESCOM. [Online]. http://www.eurescom.eu/

[15] EURESCOM, "A Common Framework for QoS/Network Performance in a multi-Provider Enviroment," EURESCOM, Project Report P806-G, 1999. [Online]. http://ftp.eurescom.de/~pub-deliverables/P800-series/P806/D1/p806d1.pdf

[16] G Almes, J Mahdavi V Paxson, "Framework for IP Perfomance Metrics," IETF, RFC 2330, 1998.

[17] J. Mahdavi and V Paxson, "IPPM Metrics for Measuring Connectivity," IETF, RFC 2678, 1999.

[18] S. Bradner, "Benchmarking Terminology for Network Interconnection Devices," IETF, RFC 1242, 1991.

[19] D. Newman, "Benchmarking Terminology for Firewall Performance," IETF, RFC 2647, 1999.

[20] ITU-T, "Y.1540: IP packet transfer and availability performance parameters," ITU-T, Recommendation Y.1540, 2007.

[21] S Kalidindi… G Almes, "A one-way delay metric for IPPM," IETF, RFC 2679, 1999.

[22] Demichelis C and et al, "Ip packet delay variation metric for ip performance metrics (ippm)," IETF, RFC 3393, 1999.

[23] Nabil Bitar, nils Bjorkman, Ross Callon, Kwok Ho Chan , et al Sane Amnte, "Inter-provider quality of Service White paper Communications Future Program (CFP)," MIT, White Paper 2006.

[24] S Kalidindi G Almes, "A one-way packet loss metric for IPPM," IETF, RFC 2680, 1999.

[25] K Chan J Babiarz, "Configuration Guidelines for DiffServ Service Classes," IETF, RFC 4594, 2006.

[26] k. Nichols, S. Blake, F. Baker, and D. Black, "Definition of the Differentiated Services Field (DS Field)," IETF, RFC 2474, 1999.

[27] k. Nichols and B. Carpenter, "Definition of Differentiated Services Per Domain Behaviors," IETF, RFC 3086, 2001.

[28] ITU-t, "ITU-T Y.1541:Network performance objectives for IP-based services," ITU-T, Recommendation Y.1541, Feb. 2006.

[29] D. Grossman, "New Terminology and Clarifications for Diffserv," IETF, RFC 3260, 2002.

[30] ITU-T, "Framework for service quality agreement," ITU-T, Recommendation E.801, 1996.

[31] p Levis and M Boucadair, "Considerations of Provider-to-Provider Agreements for Internet-Scale Quality of Service (QoS)," IETF, RFC 5160, 2008.

[32] Information Sciences Institute, University of Southern California, "INTERNET PROTOCOL, DARPA INTERNET PROGRAM, PROTOCOL SPECIFICATION.," IETF, RFC 791, 1981.

[33] S Deering and R Hinden, "Internet Protocol, Version 6 (IPv6) Specification," IETF, RFC 2460, 1998.

[34] Dah-Ming Chiu, John C.S. Lui, Vishal Misra, Dan Rubenstein Richard T.B. Ma, "Interconnecting Eyeballs to Content: A Shapley Value Perspective on ISP Peering and Settlement," 2008. [Online]. http://dna-pubs.cs.columbia.edu/citation/paperfile/162/tech08interconn

[35] William B Norton. (2003) The Evolution of the U.S. Internet peering Ecosystem. [Online]. http://www-users.cselabs.umn.edu/classes/Spring-2010/csci8211/Readings/norton.pdf

[36] (2011, January) Internet Exchange Points. [Online]. https://www.euro-ix.net/documents/894-ixp-research-pdf?download=yes

[37] S. Iekel-Johnson, D. McPherson, J. Oberheide, F. Jahanian C. Labovitz. Atlas Internet Observatory 2009 Annual report. [Online]. http://www.nanog.org/meetings/nanog47/presentations/Monday/Labovitz_ObserveReport_N47_Mon.pdf

[38] (2011, August) Google Global Cache. [Online]. http://www.afnog.org/afnog2008/conference/talks/Google-AFNOG-presentation-public.pdf

[39] J. Hawkinson and T. Bates, "Guidelines for creation, selection, and registration os an Autonomous System (AS)," IETF, RFC 1930, 1996.

[40] K Lougheed and Y Rekhter, "A Border Gateway Protocol (BGP)," IETF, RFC 1105, 1989.

[41] Y Rekhter and T Li, "A Border Gateway Protocol 4 (BGP-4)," IETF, RFC 1771, 1995.

[42] Y Rekhter, T Li, and S Hares, "A Border Gateway Protocol 4 (BGP-4)," IEFT, RFC 4271, 2006.

[43] Honnef Bad, "The Economics of IP Networks-Markets, technical and Public policy Issues relating to internet Traffic Exchange," WIK consult, 2002. [Online]. http://ec.europa.eu/information_society/topics/telecoms/regulatory/studies/documents/ip_final_report_execsum.pdf

[44] Louis Lee Lane Patterson, "A How-to Guide to BGP Multihomming," Equinix, paper 2004. [Online]. http://140.116.82.38/members/html/ms03/dclin/Science/Routing%20Protocol/BGP-MHing-HOWTO-whitepaper.pdf

[45] Chris Metz, "Interconnecting ISP Networks," Cisco Systems, IEEE publication 2001. [Online].

http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=914650

[46] william B Norton, "Internet Service Providers and Peering," white paper 2001. [Online]. http://peering.drpeering.net/AskDrPeering/blog/articles/Internet_Peering_White_Papers_files/Internet%20Service%20Providers%20and%20Peering%202.8.pdf

[47] Jörn Altmann and Deepak Goel, "Economizing ISP Interconnection at Internet Exchange Points," School of Information Technology, International University, Bruchsal, Germany, Paper 2006. [Online]. http://iospress.metapress.com/index/17q6ul8bpfnc17k8.pdf

[48] NSF. (2003) A Brief History of NSF and the Internet. [Online]. http://www.nsf.gov/news/news_summ.jsp?cntn_id=103050

[49] EURO-IX. (2011, August) EURO-IX website. [Online]. http://www.euro-ix.net

[50] Analisys Mason, "Overview of recent changes in the IP interconection ecosystem," Analisys Mason, Public Report 17038-93, 2011. [Online]. http://www.analysysmason.com/About-Us/News/Insight/Internet_exchange_points_Feb2011/Related-report-download/

[51] Lakshminarayanan Subramanian, Venkata N Padmanabhan, and Randy H. Katz, "Geographic Properties of Internet Routing: Analysis and Implications," Microsoft Research, Paper MSR-TR-2001-89, 2001.

[52] Martin Arlitt, Anirban Mahanti, Zongpeng Li, and Phillipa Gill. (2008) The Flattening Internet Topology: Natural Evolution, Unsightly Barnacles or Contrived Collapse? [Online]. http://www.hpl.hp.com/techreports/2008/HPL-2008-47.pdf

[53] M Day, B Cain, G Tomlinson, and P Rzewski, "A Model for Content Internetworking (CDI)," IETF, RFC 3466, 2003.

[54] S Blake et al., "An Architecture for Differentiated Services," IETF, RFC 2475, 1998.

[55] Cisco Systems. (2011) QoS Policy Propagation Through the Border Gateway Protocol. [Online]. http://www.cisco.com/en/US/docs/routers/10000/10008/configuration/guides/qos/10qqppb.html

[56] Gerard Blokdijk, "“Service Level Agreement 100 Success Secrets - Sla, Service Level Agreements, Service Level Management and Much More”," 2008. [Online]. http://books.google.com/books?id=msLAn7D7yQYC&dq=sla+toolkit&hl=es&source=gbs_navlinks_s, 2008

[57] Jason Spencer, David Griffin, Takis Damilatis, Hamid Asgari, Jonas Griem, George Pavlou, Pierrick Morand Panos Georgatsos, "Provider-level Service Agreements for Inter-domain QoS delivery," Algonet SA, Athens, Greece, University College London, UK, Thales Research and Technology Ltd., Reading, UK, University of Surrey, Guildford, Uk, France, Paper 2004. [Online]. http://www.springerlink.com/index/vbgumfwxfu990x5j.pdf

[58] EURESCOM, "CDN interconnection," EURESCOM, Presentation P1955, 2010.

[59] (2000-2002) Tequila Project, Traffic Engineering for Quality of Service in the Internet, at Large Scale. [Online]. http://www.ist-tequila.org/

[60] (2002-2005) MESCAL, Management of End-to-end Quality of Service Across the Internet at Large. [Online]. http://www.mescal.org/

[61] (2005-2008) AGAVE, A liGhtweight Approach for Viable End-to-end IP-based QoS Services. [Online]. http://www.ist-agave.org/

[62] ITU-T, "Framework and methodologies for the determination and application of QoS parameters," ITU-T, Recommendation E.802, 2004.

[63] S Shalunov, B Teitelbaum, A Karp, J Boote, and M Zekauskas, "A One-way Active Measurement Protocol (OWAMP)," IETF, RFC 4656, 2006.

[64] K Hedayat, R Krzanowski, A Morton, K Yum, and J Babiarz, "Two-way ay Active Measurement Protocol (TWAMP)," IETF, RFC 5357, 2008.

[65] A Morton and B Claise, "Packet Delay Variation Applicability Statement," IETF, RFC 5481, 2009.

[66] A Morton, G. Ramachandran, and G Maguluri, "Reporting Metrics: Different Points of View," IETF, Draft draft-ietf-ippm-reporting-metrics-05, 2011.

[67] Federal Communications Commision. (2011, September) US federal register. [Online]. http://www.gpo.gov/fdsys/pkg/FR-2011-09-23/pdf/2011-24259.pdf

[68] BEREC, Body of European Regulators for Electronic Communications, "Guidelines for Quality of Service in the Scope of Net Neutrality, Draft for public consultation," BEREC, Report BoR(12) 32, 2012. [Online]. http://www.erg.eu.int/doc/berec/bor/bor11_66_transparencyinput.pdf

[69] Body of European Regulators for Electronic Communications BEREC, "A framework for Quality of Service in the scope of Net Neutrality," BEREC, Report BoR (11) 53, 2011. [Online]. http://www.erg.eu.int/doc/berec/bor/bor11_53_qualityservice.pdf

[70] BEREC, "BEREC public consultations on Net Neutrality , Explanatory Paper," May 2012. [Online]. http://berec.europa.eu/files/news/bor_13_34_public_consultations.pdf

[71] William Norton. (2011, august) The Internet Peering Play book, Interconnecting to the core of the Internet. [Online]. http://books.google.es/books?id=MPe9CLhQhqsC&printsec=frontcover&hl=es&source=gbs_atb#v=onepage&q&f=false

[72] William B Norton, "The Art of Peering: The Peering Playbook v1.2," Dr peering, paper 2010. [Online]. http://www.blogg.ch/uploads/peering-playbook.pdf

[73] http://www.techsupportalert.com. (2011, November) top 5 video Streaming sites in Internet. [Online]. http://www.techsupportalert.com/top-5-video-streaming-websites.htm

[74] EURESCOM (). (2000) EQoS – A Common Framework for QoS/NP in a multi-Provider Environment. [Online]. http://ftp.eurescom.de/~pub/deliverables/documents/P800-series/P806/D4/p806d4.pdf

X. COMPLEMENTARY REFERENCES

ISP Peering:

Geoff Houston Paper “Interconnection, peering and Settlements”.

http://www.potaroo.net/papers/index.html

About CDNs:

CDN Taxonomy.

http://www.cloudbus.org/cdn/reports/CDN-Taxonomy.pdf.

IXP Operations. (CATNIX):
Interview with María Isabel Gandía Carriedo
Network Service Manager. Centre de Serveis Científics i Acadèmics de Catalonia (CESCA). http://www.cesca.es/en

APPENDIX 1: LEVEL3-COMCAST DISPUTE

The following example evidences the scenario of complexity present in the ISP interconnection mowadays. To get the general picture of the issue, here is a briefly description of the involved entities in this scenario.

Level3[19] is one of the biggest Tier 1 ISPs on Internet, ranked as one of the best connected ISP, being this a best option as an IP transit Provider in America and Europe.

Comcast[20] is one of the biggest media entertainment companies in the United States, through cable media access technology, providing broadband Internet access and VoIP to millions users in the United States. As seen Comcast is a big Tier2 and access ISP, carrying huge amounts of IP traffic from its customers to the rest of Internet and vice versa.

Netflix[21] is the biggest VoD and video distribution provider in the United States, with over of 20 million subscribers.

Limelight Networks[22] **(LLNW) and Akamai Networks**[23] **(AKAM):** these are bigger CDNs (Content Delivery Networks) companies present on the Internet.

The usual connection between Comcast and Level3 was a *free peering* agreement, (until late 2010) having them an IP traffic exchange in symmetric way, incoming and outgoing, allowing this the Internet access to Comcast´s users as shown in the figure below. Limelight and Akamai had paid peering connections agreements with Comcast in order to reach multimedia contents provided by Netflix to its customers.

Netflix purchases Transit to CDNs and IBPs in order to be reachable to their customers in the Internet.

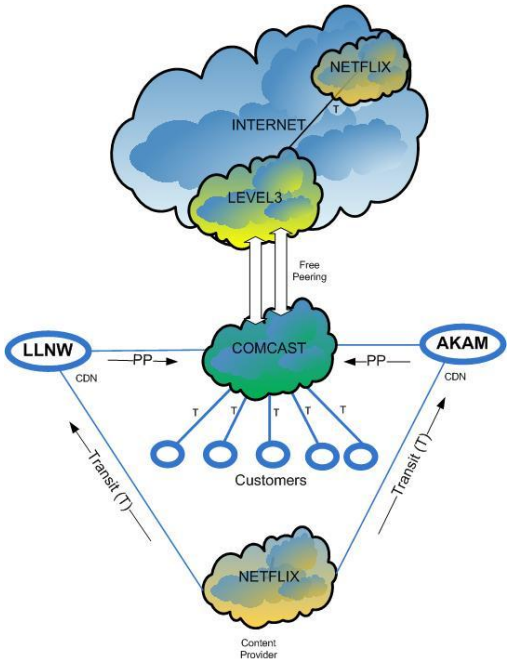

Figure 25 Initial scenario on Level3-Comcast interconnection. [71]

Then some events provoked the changes on the ISP interconnection (Level 3 -Comcast) as shown below:

Act 1: Netflix has gained considerable customers with its VoD service, increasing its IP traffic consequently on the CDN connections (Limelight and Akamai), and as a result also the revenues from Paid Peering that Comcast receives from these CDNs to deliver the Netflix service.

Act 2: In late 2010, Level3 bid and won the Netflix Video delivery business, by offering a CDN service, with more competitive prices than Limelight and Akamai offers.As a consequence, Netflix moves to the cheaper Level3 CDN service and decrease the capacity of *transit* agreements with Limelight and Akamai.

[19] Level3 communications http://www.level3.com/en/about-us/
[20] Comcast Corporation http://www.comcast.com/
[21] Netflix https://signup.netflix.com/MediaCenter/Overview
[22] Limelight Networks http://www.limelight.com/network/
[23] Akamai Networks http://www.akamai.com/html/about/index.html

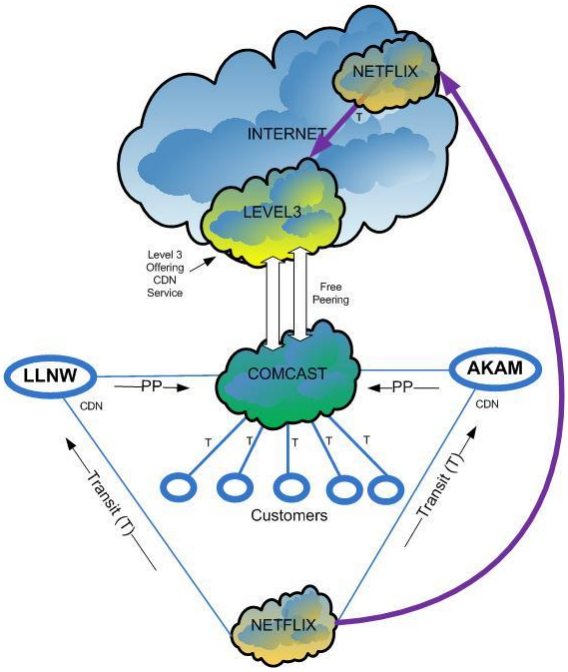

Figure 26 Netflix moves to Level3 CDN service

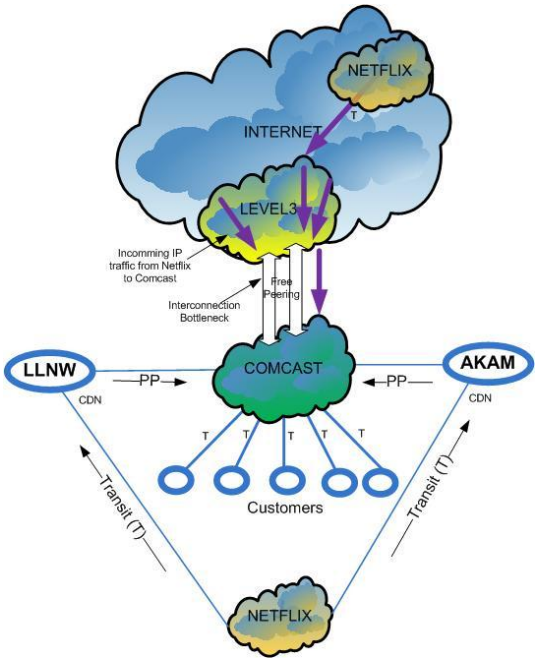

Figure 27 Bottlenecked Interconnection in the scenario

Act 3: Level3 in a prevision of the big amount of traffic that will carry from Netflix informs to Comcast of the need of expand the interconnect capacity between them.

In this moment Netflix was winning the business game, having obtained a cheaper video delivery cost, Limelight and Akamai lose the Netflix business, Comcast obviously loses the revenues from paid peering from the CDNs, and Level3 wins the Netflix business.

Comcast loses again, with related cost from their *free peering* capacity extension asked with Level3.

Act 4: Comcast refuses to extend their interconnection capacity complaining that Level3´s traffic is "out of ratio", in other words, the traffic will not be part of the free peering and Level3 has to pay for a paid peering agreement. Comcast also argue that would not be fair not to charge Level3 for this activity since they charge to other CDNs for the same Service.

So Level3 made this issue public and complained to the FCC, presenting an accusation against Comcast of breaching the Net Neutrality principle. But the FCC was not in a pro-regulation position, arguing that from the Net Neutrality principle, the Internet should be self-regulated.

In the mean time of this dispute, there could be present a bottleneck (see Figure 27) in these interconnection that only could be solved between the involved ISPs.

Finally Level 3 after much discussion, aware of the scenario, agreed to pay Comcast´s Paid peering as shown in Figure 28.

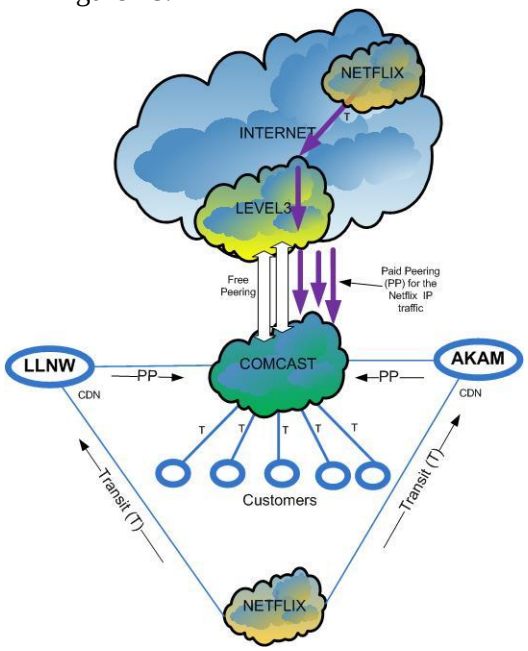

Figure 28 Paid peering agreement from Level3 to Comcast.

This case has shown, beside of the representation of the evolution of the actual Internet architecture, the diverse interconnection ways present on the Internet. Furthermore, there remains the question, about the self-regulation of Internet or the need of regulation authorities' participation.