Body of European Regulators for Electronic Communications

BEREC

BoR (11) 53

A framework for Quality of Service in the scope of Net Neutrality

8 December 2011

Table of content

Executive summary

The debate about the open Internet and net neutrality surfaced among European policy makers and regulators during the political process of the revised regulatory framework, which was approved in November 2009. Net neutrality is a concept related to the objective of an open Internet which can be broadly defined as: "*promoting the ability of end-users to access and distribute information or run applications and services of their choice*", the wording used in article 8 (4) (g) of the Framework Directive.

The revised regulatory framework introduces the competence of NRAs to set minimum quality requirements for the performance of electronic communications networks. This BEREC report elaborates on the wording of article 22 (3) of the Universal Service Directive (USD) that relates to that competence "*In order to prevent the degradation of service and the hindering or slowing down of traffic over networks, Member States shall ensure that national regulatory authorities are able to set minimum quality of service requirements on an undertaking or undertakings providing public communications networks*...".

More specifically, this BEREC report describes a framework for Quality of Service in relation to net neutrality, elaborating on quality related concepts and quality evaluation methods that are relevant to an understanding of USD article 22 (3). Furthermore, a general procedure is presented for NRAs to carry out their functions in relation to this provision. A deeper study will expand on these topics in a BEREC guidelines document to be developed in 2012.

The term quality has different scopes depending on the particular characteristics and the elements of the communication system that is under consideration. The quality of users' interaction with services at the man-machine interface is assessed by the *Quality of Service* (QoS) concept. QoS, which includes both the network and the terminal equipment, is measured end-to-end, per service. This is despite the fact that the terminal equipment (and user-controlled local network, if applicable) is usually not managed by the network provider.

Therefore, for technical purposes the *Network Performance* (NP) concept is used for measurement of the performance of network portions that are under individual providers' control. Given that the strict technical term QoS includes many parameters outside the control of the network provider, BEREC understands that USD article 22 (3) should be limited to network performance.

Degradation of network performance may be due to general congestion in the network or it may be caused by targeted throttling of specific applications. Furthermore, congestion may occur in two different ways, either related to unpredictable situations occurring on an irregular basis, or relatively frequently caused by an operator's failure to meet increased traffic load with sufficient capacity enhancement.

The Internet access service provides connection to the public Internet and thereby connectivity among end users connected to the Internet. Specialized services on the other hand, adopt access restrictions and strict service provisioning, typically implemented in a manner that provides enhanced service characteristics (e.g. end-to-end quality and/or security). These two service models represent an axis of characteristics that demonstrates different degrees of openness and admission control.

One could also envisage another (orthogonal) axis, exhibiting varying degrees of traffic management, with associated performance guaranties that reach from best effort to guaranteed quality levels. This second dimension illustrates that both the general Internet access service and specialized services can implement different traffic management techniques to achieve different levels of quality. Specialized services are typically able to

cover the whole range of quality levels, while the open Internet may be less predictable, currently lacking guaranteed levels of performance.

Because specialized services intrinsically offer contractual terms ensuring quality of provision, BEREC considers that the application of minimum quality requirements according to USD 22 (3) should generally not be necessary for those services. This report therefore focuses specifically on quality conditions of the Internet access service.

Quality evaluation of the Internet electronic communication service is challenging because of the mesh structure of this network of networks, the distributed responsibility of management of the network equipment and the decoupling of applications and content from the network layer. Use of statistical measurement methods is therefore indispensable. Even though an individual ISP is only able to directly control its own network resources, the interconnection arrangements agreed and implemented, are an important part of the service provisioning.

The most relevant quality indicators for evaluation of network performance are throughput, latency, jitter and packet loss. These parameters are today mainly measured over the access leg i.e. from the user-to-network interface to some network internal measurement server. Enhanced methods measuring ISP-to-ISP communication, constituting the interconnection leg, would take into account the fact that Internet access is a service providing access to an interconnected network infrastructure.

Measuring the performance of individual traffic flows originating from specific applications may be a necessary part of any test configuration for detection of blocking and throttling of applications. This is however a challenging test configuration, which will need to distinguish between ordinary congestion situations in the network and targeted application-specific degradation.

BEREC has identified two main phases for ensuring compliance with USD article 22 (3), possibly followed by a third assessment phase:

1. the detection of “triggers” for imposition of minimum quality requirements, and
2. if a trigger situation is detected in the first phase, a subsequent second phase in which the minimum quality requirements are specified, and
3. a third phase, in which assessment of whether the requirements are fulfilled, is also foreseen in some cases.

Each of these *phases* is further subdivided into three generic *steps*:

a) preparation of each phase,
b) quality evaluation and
c) analysis of results.

During the first, trigger detection phase, the *preparation step (1a)* will typically consist of collection of indicators received from stakeholders (including end users) and symptoms detected by the NRA. That preparatory step is followed by the *quality evaluation step (1b)* in order to verify the indicators and symptoms. This phase is typically based on the use of technical quality measurement tools, as described above.

The results of the quality measurements will then be input to the *analysis step (1c)*. During this step, which is the last step in the trigger detection phase, the decision will be taken as to whether or not it is necessary for the NRA to intervene. Frequently occurring degradation of the general Internet electronic communications service or hindering (blocking) or slowing down (throttling) of traffic from individual applications are of particular concern.

NRAs will need to scrutinize the effect of the providers’ traffic management practices. This will include looking into the need to safeguard applications that depend on the underlying

network's quality, prevention of consumer harm, protection of innovation and/or prevention of discriminatory behaviour that restricts competition.

The effect of traffic management practices is categorized into two main groups:

- degradation of the performance of the Internet access service as a whole, and
- degradation of individual applications using the access.

Further work is needed in order to develop detailed recommendations regarding the evaluation of the ISPs' practices in those respects. This will take place during the BEREC work streams on "Guidelines on quality of service in the scope of net neutrality" and "Competition issues related to net neutrality".

During the second, requirement determination phase, the *preparation step (2a)* will typically build on the outcome of the preceding trigger detection phase. This second phase will be entered if the outcome of the first phase is that "triggers" have actually been identified. And the specifics of the degradation leading to this decision will typically point towards the most appropriate quality requirements.

In the next *quality evaluation step (2b)* potential quality requirements are considered. Again there will be two main groups: requirements on the Internet access service as a whole, and requirements on individual applications using the access. BEREC has identified three levels of requirements: Functional, general technical and detailed technical requirements. The determination of concrete requirements during this step will typically require the use of quality measurements made on live communication.

Potential *functional requirements* to be considered could include requirements on the Internet access service as a whole. For example, it could be required that congestion management must be mainly application-agnostic and/or actual access performance could be required to have an appropriate relationship to the advertised speed. Functional requirements regarding individual applications could for example include prohibition of blocking and/or throttling of specific applications and there could be qualitative requirements obliging adequate performance of specific applications.

When potential *technical* requirements are being considered, these could for example include *general* technical requirements, such as obligations regarding typical or minimum actual speed of the Internet access service. NRAs could also consider including the interconnection leg in addition to the access leg in such speed requirements. Applying *detailed* technical requirements to the performance of specific applications could in principle be desirable, but BEREC considers this may not be very feasible on today's best effort Internet.

The *analysis step (2c),* which constitutes the last step of the requirement determination phase, will probably be partly conducted in parallel to the quality evaluation step, in order to analyse the ability of the different candidate requirements to prevent quality degradation. The requirement chosen must be effective while at the same time being the least intrusive.

USD article 22 (3) prescribes a notification procedure that requires information about the proposed decision by the NRA to be provided to the Commission and also be made available to BEREC. Following this, the NRA is obliged to take the utmost account of any comments or recommendations made by the Commission when finally deciding on the requirements.

Further work is needed in order to provide detailed recommendations on the setting of specific minimum quality requirements. The usability of the different options indicated above will be elaborated further during the follow-up BEREC work stream on "Guidelines on quality of service in the scope of net neutrality".

Part I – Introduction

1. The role of QoS with regard to net neutrality

The increasing importance of the Internet for society has led to intense discussions about how to preserve and enhance this shared resource as an open platform for all kinds of electronic communication. End users' and content and applications providers' ability to use the Internet, as well as the Internet service providers' and network operators' ability to build the underlying infrastructure are important aspects of this ongoing debate. The different actors have interests in the performance of the Internet as well as the resulting quality of applications running on the net.

In the strict sense, net neutrality is the principle of equal treatment between packets moving across the IP infrastructure. However, net neutrality has been used more broadly to describe the openness of the Internet. The debate about the open Internet and net neutrality started in the US, and it gained critical mass for European policy makers and regulators during the political process of the revised regulatory framework, which was approved in November 2009. Net neutrality in its broad definition related to the objective of an open Internet is described as: "*promoting the ability of end-users to access and distribute information or run applications and services of their choice*", the wording used in article 8 (4) (g) of the Framework Directive.

In 2010 BEREC started exploring the regulatory aspects of net neutrality. The Commission also initiated a consultation. In its response to the Commission BEREC noted that "*incidents so far remain few and for the most part have been solved without the need for regulatory intervention. BEREC believes that, at present, it would be premature to consider further intervention with respect to net neutrality on an EU level… This, however, does not mean that problems could not arise in the future. For this reason, BEREC believes that it is important that the conditions of net neutrality and the openness of the Internet be monitored over time by NRAs*." In this context quality of service was identified as one of the key issues for further work on net neutrality by BEREC in 2011 and 2012.

The regulatory framework introduces the competence of NRAs to set minimum quality requirements for performance of electronic communications services. In this document the wording of article 22 (3) of the Universal Service Directive (USD) "*In order to prevent the degradation of service and the hindering or slowing down of traffic over networks, Member States shall ensure that national regulatory authorities are able to set minimum quality of service requirements on an undertaking or undertakings providing public communications networks*..." is elaborated on. This document focuses on the issue of quality of service requirements, even though this is of course only one among several aspects of the broader net neutrality theme.

The provision mandates NRAs to set minimum requirements in order to avoid certain situations. These situations are described as "*the degradation of service and the hindering or slowing down of traffic over networks*". This invokes the question: When is degradation of service and hindering or slowing down of traffic of such nature that imposing remedies in the form of minimum requirements is to be considered appropriate? And furthermore, while the article remains agnostic on this matter, what shape should these minimum requirements take?

The answers to these questions ought to be explored within the context of the framework and in line with basic legal concepts. According to recital 34 of the 2009/136/EC Directive, the underlying goals that the legislator wishes to achieve are: [1] to address discriminatory behaviour that could restrict competition; [2] to ensure that services and applications

dependent on the network are delivered at a minimum quality standard; and [3] address service degradation that is to the detriment of consumers.

The framework implies that NRAs need to assess end user indications and symptoms that surface in the infrastructure or application markets, which could indicate that problems have emerged. Different approaches can be used for monitoring these developments, from proactive measurement of communications services to a more reactive response based on incidents reported to the NRAs. Specialized services[1] are usually provided with clear contractual terms related to quality. The Internet access service, being a more general service, will however be a particular subject of interest for quality evaluation. Different markets and countries may also require or prefer different solutions, but it is also necessary to develop some common understanding at the European level.[2]

There are different interpretations of the concept "quality of service" (QoS) depending on the context in which it is used. There is a difference between use of the concept within the provisions of the telecoms package on one hand and the strict technical definition of QoS on the other. In the USD the concept refers to a more general quality perception related to the user's subjective experience when running applications over the network, while the technical specification of QoS consists of well defined performance characteristics of applications.

In relation to this it is important to distinguish between the end user, the terminal equipment and the network itself. Even though it is the end users' perception of the application that is the goal, it is only the network part that is under the operators' control. Varying quality of the terminals used may have a major impact on the performance of the application. Because of this, the end users' perception is an important source of indicators of quality problems, but it will only be the performance of the network itself for which minimum requirements can be set.

It is challenging both to measure and guarantee the network performance of the Internet electronic communication service because of the "best effort" way of working of this global network consisting of several interconnected providers' networks. This also implies that determination of the minimum quality requirements will not be straight forward. Then there is the question about whether to consider individual applications or to look at the performance of the overall electronic communications service provided by the network. Related to this is a question about how to interpret "*degradation of service and the hindering or slowing down of traffic*" which is the wording used in article 22 (3) in USD. These are questions that are discussed in this report.

There will be several steps before, if deemed necessary, the minimum quality requirements can be set. When symptoms of degradation of service are discovered, this situation will then have to be evaluated to make a decision on whether or not this could be considered a "trigger point" for intervention. If it is decided to impose minimum quality requirements, the quality level must be determined based on, inter alia, current technology and the performance level available in the market today. There will also be a need to assess the degree of fulfilment of the requirements after they have been decided on. Then in the longer run there is a need to consider the dynamic aspect of the requirement level, to follow up the evolution of technology and services available in the market.

During the different steps described above there will be a need to investigate in more detail the network performance using technical measurement methods. Measurements may include parameters like throughput rate, network connectivity, packet delay, packet delay variation, packet error, packet loss and support of TCP/IP protocols. In addition to

[1] The concept "specialized service" is further described in section 4.5

[2] See recital 34 of Directive 2009/136/EC explaining the specific use of the notification and response procedure.

measurement of the general network performance, there is also a possibility to measure the performance of individual applications. However, while it will not be feasible to analyse every kind of application, selected applications may be tested for performance and detection of targeted blocking or throttling.

This report is also related to BEREC's "Guidelines on Transparency in the scope of Net Neutrality", and particularly transparency regarding the quality level offered by the ISPs.

2. Scope and structure of the report

The scope of this report is to discuss how to interpret the new provision in article 22 (3) in the Universal Service Directive which describes the NRAs' competence to define and potentially impose minimum quality requirements on electronic communications networks.

After the introduction in part I, the report contains a description of general aspects in part II and a description of the available regulatory tools in part III.

Part II consists of chapter 3 describing the relevant provisions of the regulatory framework, chapter 4 defining quality of service and other related concepts and chapter 5 giving an overview of quality evaluation methods. These evaluation methods are applicable to the different phases of the regulatory process described in part III.

Part III outlines the different stages in a regulatory process. First, the NRA must take a decision on whether there is a need to set minimum quality requirements or not, as described in chapter 6. If the conclusion is yes, the level of those quality requirements has to be determined, which is elaborated in chapter 7. A possible assessment phase is also foreseen, as presented in chapter 8.

Finally, chapter 9 summarizes the findings and gives suggestions for further work. Based on the general framework presented by this report on net neutrality and QoS, BEREC intends to develop more specific and detailed recommendations in a separate follow-up guidelines document.

Part II – General aspects

3. Relevant provisions of the Regulatory Framework

The purpose of this chapter is to present an overview of the legal framework taken into account in this report. Article 22 USD[3] and relevant recitals with respect to article 22 (3) USD are introduced.

The core regulation is article 22 USD, which deals with "Quality of Service". Hence, it is briefly introduced. To simplify the understanding the provisions' texts are shortened and the parts of greatest interest highlighted/ underlined:

Article 22 (1) states that
Member States shall ensure that national regulatory authorities are, after taking account of the views of interested parties, able to

- *require undertakings that provide publicly available electronic communications networks and/or services to publish comparable, adequate and up-to-date information for end-users on the quality of their services and on measures taken to ensure equivalence in access for disabled end-users.*
- *That information shall, on request, be supplied to the national regulatory authority in advance of its publication.*

Article 22 (2) states that
National regulatory authorities may specify, inter alia,

- *the quality of service parameters to be measured and the content, form and manner of the information to be published, including possible quality certification mechanisms, in order to ensure that end-users, including disabled end-users, have access to comprehensive, comparable, reliable and user-friendly information.*
- *Where appropriate, the parameters, definitions and measurement methods set out in Annex III may be used.*

According to article 22 (3),
National regulatory authorities, in order to prevent

- *the degradation of service and*
- *the hindering or slowing down of traffic over networks,*

shall be able to

- *set minimum quality of service requirements*
- *on an undertaking or undertakings providing public communications networks.*

The NRA is obliged to provide the Commission, in good time before setting any such requirements, with:

- *a summary of the grounds for action,*
- *the envisaged requirements and*
- *the proposed course of action.*

This information shall also be made available to BEREC.

The Commission may, having examined such information, make comments or recommendations thereupon, in particular to ensure that the envisaged requirements do not adversely affect the functioning of the internal market.

- *NRAs shall take the utmost account of the Commission's comments or recommendations when deciding on the requirements.*

[3] See Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services

Article 22 describes a multilayered progression of means to secure quality of service, imposing an obligation for member states to ensure that NRAs are able to require providers to publish quality related information and measures taken to ensure equivalence in access for disabled end users (paragraph1). NRAs may specify and provide parameters to providers in this aspect (paragraph 2). In order to prevent degradation of service, NRAs may set minimum quality of service requirements. If doing so, they are obliged to provide information on the envisaged requirements to the Commission and BEREC and to take utmost account of the Commission's comments or recommendations (paragraph 3).

Of relevance in this context is also the amended article 9 (1) of the Access Directive (AD), which now stipulate that NRAs "may, in accordance with the provisions of article 8, impose obligations for transparency in relation to interconnection and/or access, requiring operators to make public specified information, such as accounting information, technical specifications, network characteristics, terms and conditions for supply and use, including any conditions limiting access to and/or use of services and applications where such conditions are allowed by Member States in conformity with Community law...".

Then a closer look into article 22 (3) USD is relevant. To better understand the paragraph it is vital to keep in mind the following excerpts of recitals in the USD[4] (note: these are not quotations and the most relevant phrases in this respect are underlined)

- *End-users should be able to decide what content they want to send and receive, and which services, applications, hardware and software they want to use for such purposes, without prejudice to the need to preserve the integrity and security of networks and services. A competitive market will provide users with a wide choice of content, applications and services.* (Cf. recital 28)

  NRAs should promote users' ability to access and distribute information and to run applications and services of their choice, as provided for in FD Art. 8. Given the increasing importance of electronic communications for consumers and businesses, users should in any case be fully informed of any limiting conditions imposed on the use of electronic communications services by the service and/or network provider. (Cf. recital 28)

- *USD neither mandates nor prohibits conditions imposed by providers, in accordance with national law, limiting end-users' access to and/or use of services and applications, but lays down an obligation to provide information regarding such conditions*. (Cf. recital 29)

- *A competitive market should ensure that end-users enjoy the quality of service they require, but in particular cases it may be necessary to ensure that public communications networks attain minimum quality levels so as to prevent (i) degradation of service, (ii) the blocking of access and (iii) the slowing of traffic over networks.* (Cf. recital 34)

On this background it seems reasonable to conclude that the regulatory power introduced by art 22 (3) has to be executed with thoughtful caution. A discussion seems to be necessary on possible premises for a trigger that alerts the NRA when there might be reason to consider intervention and, as a remedy, to set minimum quality requirements. The provision in art 22 (3) about the Commission and BEREC consultation procedure indicates that other measures (such as strengthening transparency and improving competition) should be taken into account, before imposing minimum quality requirements.

The minimum quality requirements may be imposed on "*an undertaking or undertakings providing public communications networks".* NRAs may therefore also impose such requirements on an individual undertaking and therefore NRAs are granted the right to address one specific provider of public communications networks.

[4] Contained in Directive 2009/136/EC, amending the USD

It should also be noted that the directive does not provide further detail as to what these "minimum quality of service requirements" consist of; should this requirement be interpreted narrowly so as to refer to network performance only, or is it meant to cover the entire 'user experience' of a service? Furthermore, it does not provide clear guidance on what should be the trigger for the imposition of such a minimum quality requirement.

However, recital 34[5] gives some indications in this connection, describing some aspects that could be considered:

> *In order to meet quality of service requirements, operators may use procedures to measure and shape traffic on a network link so as to avoid filling the link to capacity or overfilling the link, which would result in network congestion and poor performance.*

The term "procedures to measure and shape traffic" is what is referred to as "traffic management" in this report.

> *Those procedures should be subject to scrutiny by the national regulatory authorities, acting in accordance with the Framework Directive and the Specific Directives and in particular by addressing discriminatory behaviour, in order to ensure that they do not restrict competition.*

This indicates that the scrutiny by the NRAs should address discriminatory behaviour that restricts competition.

> *If appropriate, national regulatory authorities may also impose minimum quality of service requirements on undertakings providing public communications networks to ensure that services and applications dependent on the network are delivered at a minimum quality standard, subject to examination by the Commission.*

This indicates that NRAs may also take steps to ensure the quality of applications dependent on the underlying network.

> *National regulatory authorities should be empowered to take action to address degradation of service, including the hindering or slowing down of traffic, to the detriment of consumers.*

This indicates that NRAs may address any degradation of service that is to the detriment of consumers.

Summing up, this indicates three sample aspects to consider in the interpretation of USD article 22 (3) regarding traffic management and quality of service:

- discriminatory behaviour restricting competition
- applications' dependence on the underlying network
- degradation that is to the detriment of consumers

There is a potential risk for an adverse effect on the functioning of the internal market if individual NRAs use different legal standards in regard to QoS and triggers for intervention. This could lead to a fragmented market for ISPs with cross-border strategies. For this reason, article 22 (3) USD also provides for a mandatory process of consultation involving the Commission and BEREC where such minimum quality requirements are imposed. However, it is the intention of this report to bring more clarity with regard to the definition of "quality"; quality evaluation methods; when to set minimum requirements; how to determine the requirements; and how to assess the fulfilment of requirements.

Discussions on when and how this new power set out in article 22 (3) USD could be used will be dealt with in more detail in chapters 6, 7 and 8.

[5] Directive 2009/136/EC

4. QoS and related concepts

Although the end user's quality of experience is the final goal, including how it provides a potential indicator for network performance, the main objective for QoS evaluation is to identify degradation of service resulting either from congestion or from operators' practices (e.g. priority given to selected traffic streams over others). Therefore, the approach is not necessarily to use quality of service (QoS) and quality of experience (QoE) concepts as defined in formal standards but to base the analysis on related knowledge in order to achieve pragmatic ways of identifying degradation of service.

4.1 Internet access including interconnection

The Internet consists of thousands of interconnected networks. Each network is operated autonomously and is therefore referred to as an Autonomous System (AS)[6]. Communications paths within an AS are established by the use of internal routing protocols. For end-to-end reachability across several ASes an external routing protocol - an inter-Autonomous System routing protocol called the Border Gateway Protocol (BGP)[7] - is needed. Its primary function is to exchange network reachability (connectivity) information between the ASes for calculating routes and eliminating loops. Routing decisions based on path, network policies and/or rule sets can then be taken.

Internet access service is a service providing an end user with connectivity to the Internet. For doing so an ISP has to operate and maintain an IP network – an Autonomous System as described in the previous paragraph – and connect it to the Internet via BGP. The Internet access reaches from the User Network Interface (UNI) to an egress point of the ISP's AS that is connected to the rest of the public Internet. This egress point can be a direct interconnection to another AS or to an Internet Exchange Point (IXP) where several other ASes may be reached. Any destination on the Internet can be reached either directly (destination is connected to a directly connected network) or indirectly (routing to destination is only possible via transit networks).

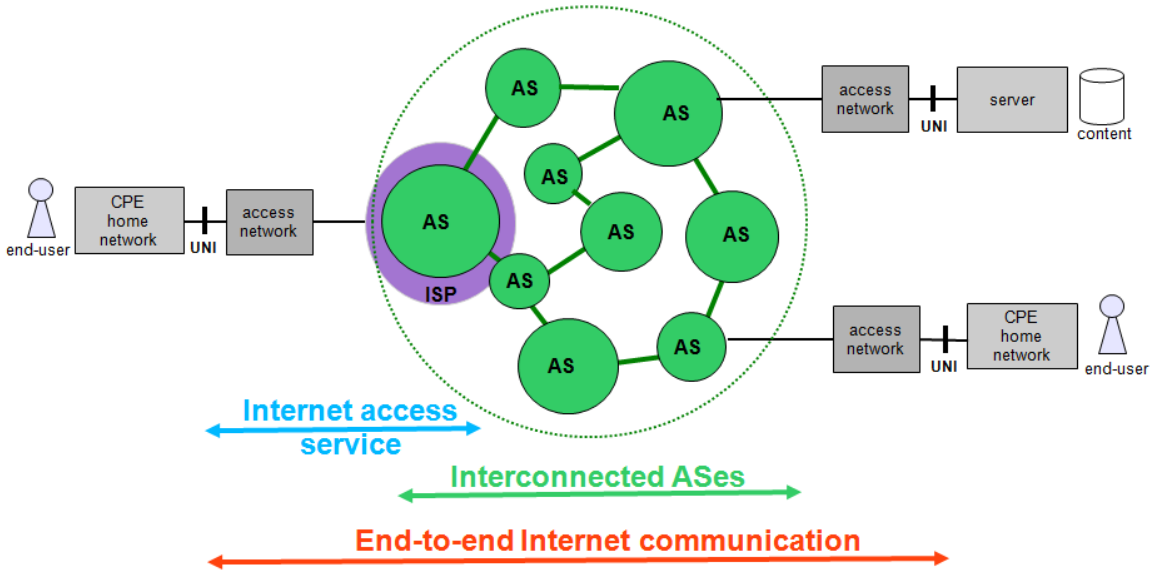


Figure 4.1 – Internet concepts

[6] An Autonomous System (AS) is a set of connected routers under a single technical administration, thus having a single and clearly defined routing policy. Detailed information on the use of ASes is given in RFC 1930.
[7] The Border Gateway Protocol (BGP) is the current de facto standard for inter-AS routing, RFC 4271.

The Internet access service enables the end user

- to communicate with end users connected to the Internet,
- to access content that is hosted on servers connected to the Internet and
- to make use of applications that rely on the communication capabilities of the Internet.

In contrast to traditional circuit-switched networks, applications/services on the Internet are not integrated into the networks. In an IP environment, services are generated at the terminal equipment (the computer), relying on the Internet as a transportation platform (the latter being usually referred to as the “network layer”). The Internet by itself provides only a general electronic communications service.

Applications and content are decoupled from the (physical and logical) network and can only use its available transfer capacity without having any influence on the traffic management mechanisms practised on it. The network does not interact with the applications; its only task is to convey the traffic according to a pre-defined policy. The Internet only provides connectivity between the end points executing the application functionality.

As an example, the use of a VoIP service is shown in the following diagram. There are various sources for impairments that affect the resulting quality of the service and that are attributable to different portions of the network chain. The VoIP application has certain minimum requirements in respect of IP packet transmission that must be met in order to provide good quality. If the network layer quality is low, the end user will only perceive that the VoIP application provides a bad performance. The end user cannot directly identify the specific source of impairment, nor who is responsible for it. This has to be done by objective measurement methods.

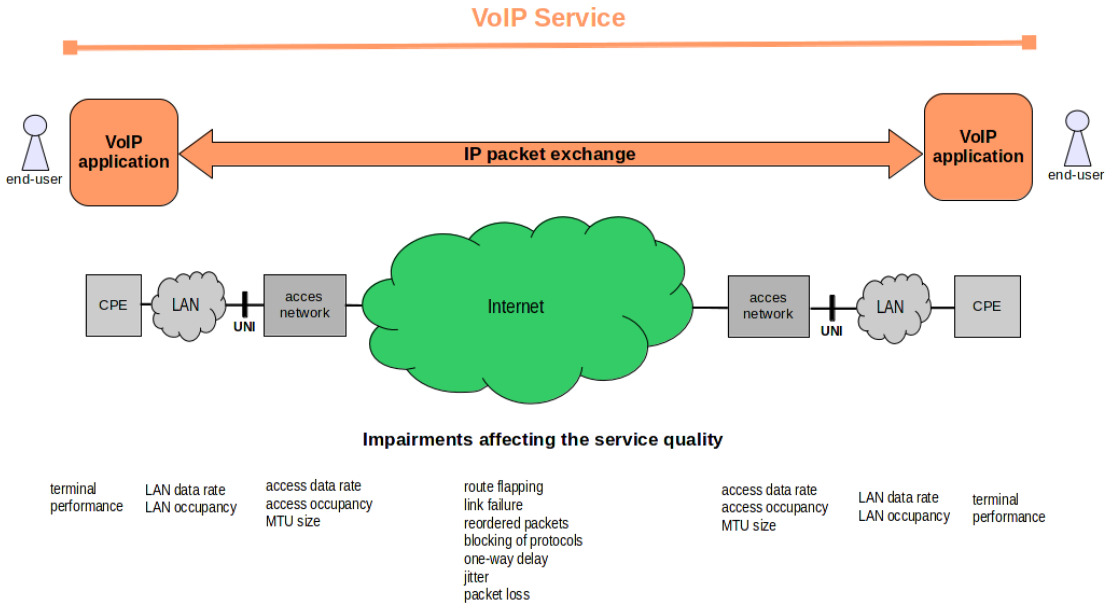


Figure 4.2 – Example application/service: Voice over IP (VoIP)

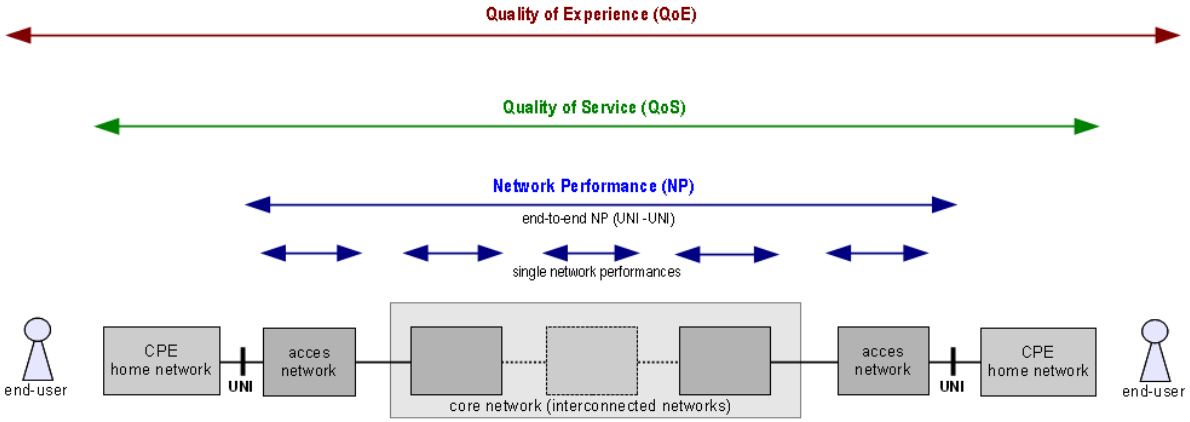
4.2 Network performance, QoS and QoE

The generic definition of quality is "*The totality of characteristics of an entity that bear on its ability to satisfy stated and implied needs*"[8]. Any component of an electronic communications system can be such an entity. Depending on what kind of characteristics and which portion of the communications system is under consideration, the term quality has different scopes. From an engineering perspective the performance of technical elements and functions are of interest. An end user interacts with the communications infrastructure by accessing a service, resulting in a perception of the quality of this service. A user-centric quality perception is given when rating the subjectively perceived service quality and taking into account context of use and user expectations.

Thus, different concepts of quality are used in telecommunications:

- For purely technical purposes, i.e. assessment and analysis of technical functions, the *Network Performance* concept is applied.
- The users' interaction with services at the man-machine interface is assessed by the *Quality of Service (QoS)* concept.
- The overall acceptability of a service as subjectively perceived by an end user is expressed in terms of *Quality of Experience (QoE)*.

The concepts and scopes of application are illustrated in the following diagram.



CPE: Customer Premise Equipment, UNI: User-to-Network Interface

Figure 4.3 – Network performance, QoS and QoE

Network Performance (NP) is the ability of a network or network portion to provide the functions related to communications between users[9]. Network performance is determined by the performance of network elements one-by-one. The performance of the network as a whole (end-to-end) is determined by the combination of the performance of all single elements along with their inter-connections. Network Performance is specified in terms of objective performance parameters, i.e. they are measurable (with instruments or observations) and a performance value is assigned quantitatively[10].

Quality of Service (QoS) is, as mentioned above, the "*Totality of characteristics of a telecommunications service that bear on its ability to satisfy stated and implied needs of the user of the service*" in which "service" is a set of functions offered to a user by an

[8] See ITU-T Rec. E.800
[9] See ITU-T Rec. E.800
[10] The relevant parameters, as defined in ITU-T Rec. Y.1540, are packet delay, jitter, packet loss, packet error (and throughput).

organization. QoS is always end-to-end, i.e. user-to-user or user-to-content. QoS measurements are also carried out end-to-end and are made using objective (quantitative) or subjective (qualitative) parameters. A QoS measurement is an indication of the performance of a set of functions observable at the user-interface of the service.[11]

Quality of Experience (QoE) is the overall acceptability of an application or service, as perceived subjectively by the end user[12]. It includes the complete end-to-end system effects (client, terminal, network, services infrastructure, etc.) and may be influenced by user expectations and context. Hence in principle, QoE is measured subjectively by the end user and may differ from one user to the other. However, it is often estimated using objective measurements through complex algorithms describing a statistical (experience) based relationship between subjective and objective measurements.

Relationship between network performance, QoS and QoE
Network Performance contributes towards QoS. The functions of a service depend on the performance of the network elements and the performance of the user's terminal equipment. Therefore, QoS comprises both network performance and non-network related performance. QoS gives a quality rating of the collective performance of a set of functions that constitute the service. For voice services, for example, the QoS relates to the entire transmission path from mouth to ear.

QoE has a broader scope. It is impacted by the performance of multiple QoS parameters and user expectations and context. In general, there is a correlation between QoS parameters and QoE mean opinion scores (MOS). This relationship (the above mentioned algorithms) is typically estimated empirically and can be used in two ways: either the expected QoE for a user can be predicted by QoS parameter measurements, or the net required QoS can be deduced from a given target QoE for a user.

4.3 Causes and effects of quality degradation

4.3.1 QoS and QoE

As explained in section 4.2, QoS and QoE are end-to-end related, i.e. user-to-user or user-to-content. QoS is a measure of the performance of a set of functions observable at the user-interface of the service. QoE additionally takes into account user expectation and context. QoS and QoE observations and measurements can only reflect the quality as it is perceived by the end user, i.e. as perceived at the service interface. It is not possible to identify the direct cause of quality degradation in technical terms.

The concepts of QoS and QoE are used to validate whether a quality agreement (SLA) has been met or to determine the quality of a given service and the user satisfaction with it. The QoS parameters of each specific service can be specified and measured. By doing so all features of a service can be monitored and verified for compliance against e.g. some reference quality level.

For any further investigation on causes of quality degradation and identification of possible malfunctioning network or terminal elements, a more detailed analysis is necessary. However, this requires access to the network(s) and terminals themselves, in order to perform specific diagnostic tests.

[11] Note that the quality-related definitions referred to in this chapter are based on the ITU recommendations. However, the Internet community uses a slightly different terminology. IETF defines Quality of Service as "a set of service requirements to be met by the network while transporting a flow" (RFC 2386) which is similar to ITU's definition of network performance.
[12] see ITU-T Rec. P.10 Amendment1

4.3.2 Network, terminal and application performance

The user-perceivable degradation of QoS/QoE is related to either an inadequate performance of the IP network or the terminal equipment/end user infrastructure, or a combination of both. Network performance and terminal performance are the building blocks of any end user service. The network(s) provide the connectivity and IP packet transfer capability between network termination points.

The terminal equipment sends and receives packets to and from the network via the network adapter (line card). The adapter is controlled by the operating system of the terminal which includes the implementation of several protocols, the so-called protocol stack. The end-to-end packet transfer performance is influenced by the performance of the hardware and software of the terminal equipment.

The user is making use of the packet transfer capabilities when running an application. The application software installed on the terminal equipment executes functions at the application/ content layer (information processing, content presentation etc) above the network layer as indicated in the figure below.[13]

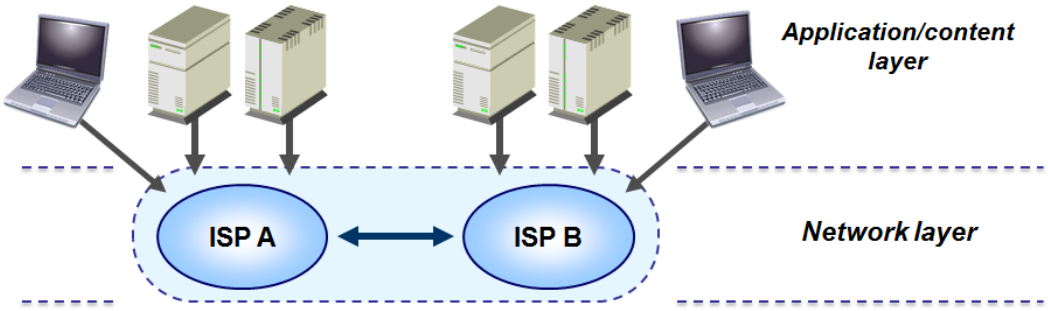


Figure 4.4 – Application/content layer and network layer

At the end user's side of a modern IP environment there may also be a local IP network (home network or corporate network for example) for connection of additional terminals and providing end user and service specific functions.

Network and terminal performance are distinguished because they belong to different areas of responsibility (these areas are separated by the UNI, see figures 4.1 and 4.2). The network operator(s) are responsible for maintaining and operating their infrastructure but they do not manage the end user equipment and infrastructure. The end user uses terminal equipment that is independently chosen and configured by him/herself.

4.3.2.1 Degradation of network performance

A decrease of network performance may be caused by a general degradation in the network, for example due to a general congestion, in which case traffic management or capacity increase may be needed, or it may be caused by a targeted throttling of specific applications.

Congestion can occur in two ways, and it is essential to distinguish between these. One case relates to unpredictable situations that occur on an irregular basis. This is an unavoidable situation, especially in a best effort network, though the amount of such congestion depends

[13] Note that this two layer model simplifies the four layer TCP/IP reference model. The application/content layer in this simplified model includes the upper application and transport layers of the TCP/IP model. The network layer in this simplified model includes the underlying network layer (also referred to as the IP layer) and the link layer (which sometimes also is further divided into data-link and physical sub-layers).

on the degree of over-provisioning of capacity. The second case is congestion that occurs on a regular basis, caused by a failure to meet increasing traffic levels with sufficient capacity enhancement.

In both cases, quality measurements have to be precise enough to evaluate the potential reduction in quality of service caused by the degraded network performance.

4.3.2.2 Degradation of terminal performance

Besides pure network performance, other factors may influence quality of service. For example, the performance of terminal equipment can impact strongly on the QoS, depending on how it has been implemented or due to aging, software incompatibility, or specific configuration issues[14].

The nature of the end user is also relevant. Different types of end users, i.e. private individuals, business customers or content/application providers, have different needs. Depending on the end user's nature and needs, the perceived impact on QoS can be different.

The quality of the local network (e.g. home network) is equally important. Deterioration of the local network linking the terminal equipment to the access point can significantly reduce the performance of applications and services. Consideration of the quality of the local network (ref. figure 4.1 and 4.2) is also necessary when measuring quality of service.

Ignoring these factors can introduce strong biases into any interpretation of QoS measurement results.

4.3.2.3 Degradation of application performance

In economics the network effect (or network externality) describes what effect the number of users has on the value of a certain good or service. Blocking of access to a certain application or content may have an impact on the economic value of that application or content, through the network effect. But the scope of the framework requires us to look beyond that and challenges us to ask the question: could blocking of access to certain applications or content have a negative impact on the functional or social value? BEREC considers this of particular importance because such effects may directly influence the end user's quality of experience.

To illustrate with an example: say an operator blocks a p2p file sharing application. This affects the value of that application, as it becomes less useful. With fewer peers available from whom to retrieve the desired information, the application will lose performance and may eventually lose relevance. Taking a different example: say an operator blocks access to a chat application from some subscription package. This makes the application less valuable, because some people can't use it at all, while others can't reach those for whom this application is blocked. Alongside the economic impact on the value of an application, its functional and social value is diminished in parallel, and for the same reason: less network reach results in less relevance for users.

The numerical expression of the network effect, the so-called Metcalf's law, asserts that the value of an application is proportional to the square of the number of its users. This shows that even though individual users may be able to use an application at their end of the communication path, the usability of the application can *quickly* fall to a low level if users at the other end are hindered.

[14] With most ISPs, the end user can change its terminal equipment configuration so that it favours some characteristics of the network, such as latency, or bit rate.

Regarding the end user's perception of QoS/QoE, a degraded application performance will affect the overall quality of the end user service. When using an application, the performance of the network is involved, including the network effect, and this must be taken into account. Applications, especially those based on user-to-user communication, form a community of application users. They create a virtual network among themselves. This system can be used to exchange information between individual users or to distribute content within the virtual network.

When evaluating QoS/QoE, the application performance, including the network effect, has to be considered. The extent to which negative impact on the network effect occurs can vary from significant to minor impact on economic, functional and social value. While the economic significance is more closely related to the application as a business entity, this report does not primarily focus on that. Following the perspective of the Universal Service Directive, our primary focus will be on the direct effects on the end-user: functionality and social context.

4.4 Traffic management

Traffic management is essential for the implementation of quality measures in IP based networks. This chapter briefly describes the different aspects of traffic management that are particularly relevant to the discussion on net neutrality.

Traffic management includes "*(1) nodal traffic control functions such as traffic conditioning, queue management, scheduling, and (2) other functions that regulate traffic flow through the network or that arbitrate access to network resources between different packets or between different traffic streams*".[15]

Different traffic management techniques can be classified according to which layer they are performed at and which network nodes they are performed in, ranging from internal to external network nodes and from the network to the application layer. An important aspect to keep in mind is that each IP packet can be inspected individually, taking into account all characteristics, and thus implementing any packet forwarding policy.

We use the following three traffic management categories:

1. Traffic management techniques executed at the network layer in the network internal nodes.[16]
2. Traffic management techniques executed above the network layer in the endpoints. (Congestion control which is elaborated on later in the section is an important example.)
3. Traffic management techniques executed above the network layer in network internal nodes.[17]

The last category includes techniques referred to as traffic filtering, traffic shaping and similar terms, and it often uses so-called *Deep Packet Inspection* (DPI). DPI looks deep into the packets' content (beyond the IP header) and classifies packets according to a predefined policy. Based on this, packets may be forwarded, delayed or dropped. DPI is typically

[15] Overview and Principles of Internet Traffic Engineering, RFC 3272

[16] This category includes also traffic management techniques executed below the network layer when the more detailed protocol reference model is used. These techniques can be further divided into two subgroups: (1) Techniques managing packet flows, traffic classes or priority levels (like DiffServ, IntServ and MPLS) (2) Techniques executing in single nodes on a packet by packet basis (like packet scheduling and queue management schemes, e.g. RED, WFQ and PQ)

[17] Layers above the network layer mean transport and application layers.

performed at “traffic junctions” and enables the ISPs to control which traffic is allowed into their networks (from the end users’ access or from the interconnection points).

DPI, originally used as a network security tool installed in firewalls, is nowadays often used for filtering of packets based on the specific application that packets belong to. In this way the ISPs may either limit the capacity used by individual applications, and/or some applications may be blocked completely. Other application-specific treatment may provide improved performance, typically for real-time applications like telephony, streaming and gaming (this is described later in the section).

Because the Internet does not use admission control for traffic flows entering through its access points, congestion occurs from time to time. During congestion, routers run out of buffer space and are forced to start dropping some packets, and by default this is done randomly. Congestion control is used to avoid escalating this situation into total congestion collapse of the Internet.[18]

Congestion control is a feedback-based adjustment of the transmission rate at which data is sent into the network.[19] Using congestion control causes the endpoints (computers connected to the network) to reduce their transmission rates when congestion is encountered, to avert escalation of the situation. This congestion control function in the endpoints may be further supported by the network, based on functionality in the routers.

In many cases when reduction of the traffic load is needed in order to relieve congestion situations, this can be performed in an application-agnostic way,[20] constituting an alternative to the application-specific measures typically performed with DPI.

Another method of managing packets within the network is to establish different *traffic classes* or *priority levels*, allowing specific traffic flows to experience an improved transfer performance. In this case the network configuration typically includes a control function at the edge of the network that limits the traffic within each class, and separate queues per traffic class inside the network.[21]

This report assumes that some traffic management practices are more reasonable than others, even though the scope of this document does not include going into a full scale discussion of this topic. But some main ideas are explained below which will be handled in greater detail in further BEREC work within the net neutrality area.

Aspects which are important when considering reasonableness are; degree of end user control, application agnosticism and full blocking vs. moderate throttling. Traffic management practices that the end user can control may often be seen as more reasonable than measures that are taken unilaterally by the ISP. This is a reflection of the objective of avoiding harm to end users.

Furthermore, practices that are independent of the specific applications that are in use, so-called application-agnostic traffic management, will usually be considered more reasonable in relation to net neutrality than application-specific traffic management. This is a consequence of the definition of net neutrality, which points towards equal treatment of traffic.

[18] Computer Networks – A systems approach, Larry L. Peterson and Bruce S. Davie
[19] Congestion Control in the RFC Series, RFC 5783
[20] For example IETF RFC 6057 Comcast's Protocol-Agnostic Congestion Management System or some newer approach being developed in the IETF Working Group Congestion Exposure (Conex), www.ietf.org
[21] Technologies typically used include DiffServ, IntServ and MPLS

And finally, complete blocking of specific applications is usually considered more severe than moderate throttling, and is therefore more likely to be regarded as an unreasonable practice. All traffic management practices should of course be revealed by the providers as a part of the transparent provision of information.

When specific traffic management practices are being assessed, all aspects of the practice must be taken into account before a conclusion can be drawn as to whether it is considered reasonable or unreasonable. Security and network integrity, legal justification and competition-related considerations are typical examples of additional aspects that need to be included in such an assessment.

4.5 Specialized services

Regarding use of the transmission capacity over the user's broadband connection, two kinds of end user services may be provided: Internet access services on one hand and specialized services on the other hand.

Internet access service provides connection to the public Internet and thereby connectivity between end points connected to the Internet. Since end-to-end communication is usually routed via several IP networks (see section 4.1) with no inter-network traffic management and with each network following its own traffic management strategy (first-come-first-serve, prioritise, throttle or block IP packets) the end-to-end performance is highly variable. Furthermore the Internet is a connectionless[22] data communications network with no guaranteed delivery of data. The network performance of the Internet today has therefore no guaranteed characteristics, which is why it is referred to as being best effort.

Specialized services are usually designed to provide guaranteed characteristics (e.g. end-to-end quality and/or security). These characteristics are generally stated in contractual arrangements. Technically, specialized services typically rely on access restrictions and extensive use of traffic management techniques or strictly enforced capacity planning and provisioning. Whereas in the specialized case customers' service requests may be rejected when the capacity limits of a network are reached or alternatively they may trigger capacity extensions, best effort networks will still try to serve the customers on a constant capacity basis (implying a decrease in quality).

Two independent dimensions differentiate the service offers provided to customers, as illustrated in figure 4.5 below. Along the horizontal axis the varying degree of openness and admission control is indicated, while along the vertical axis the variation from best effort to enhanced quality levels is indicated. The different service offers can be characterized by these two dimensions. Note that the model relates to use of the transmission capacity at the network layer and not to the application/content layer (ref. figure 4.4).

[22] Connectionless data communications means that there is no explicit setup of a connection through the network, and that individual packets are sent independent of each other.

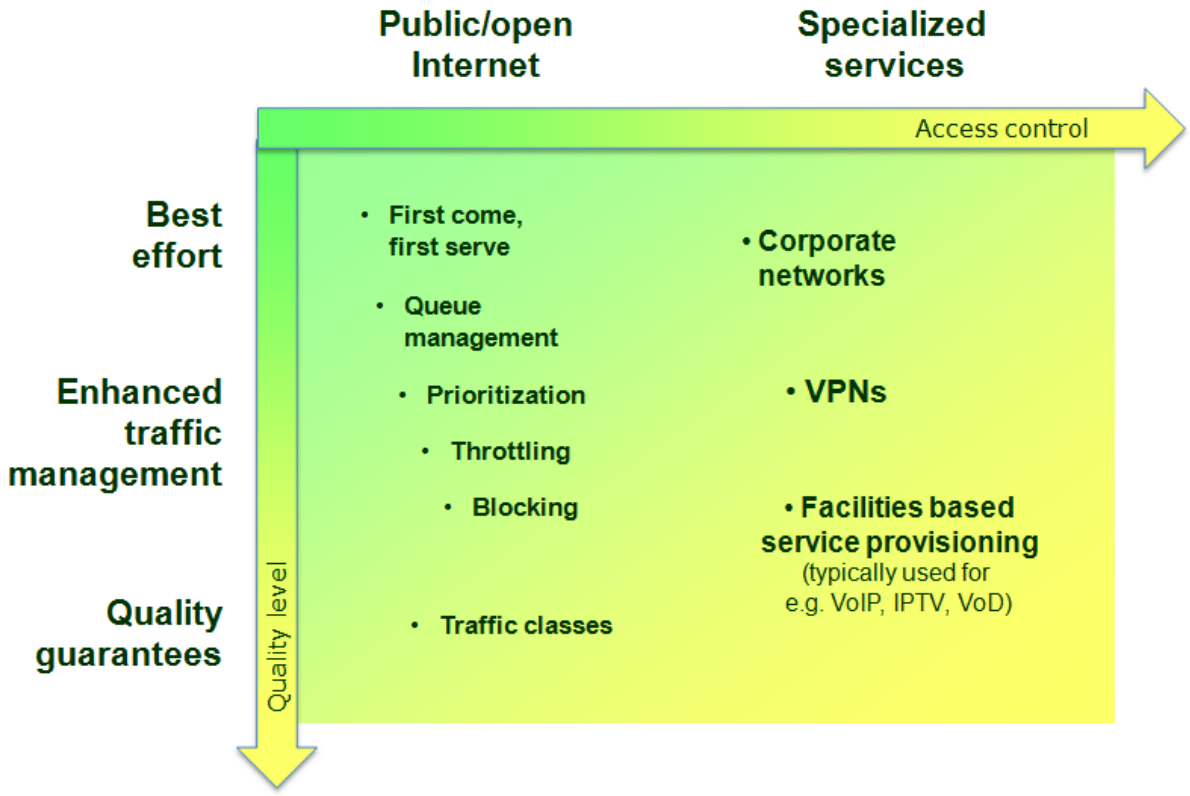


Figure 4.5 – The two dimensional model

Access control dimension

Even though both specialized services and Internet access use the same technology, namely IP, there is a differentiating aspect that enables the operator to achieve stable network performance (IP packet transmission performance) for specialized services:
The specialized services restrict use of those services to specific customers (access control) according to the specific end users' profile (control of IP traffic characteristics). Therefore the operator can calculate the required capacity and can design his network accordingly. He can allocate network resources for the exclusive use of specialized services. This is not the case with Internet access service, as services/applications on the Internet are decoupled from the network. The operator cannot know the amount of capacity required by the user for individual applications. Therefore he has to estimate an average capacity demand per end user, resulting in a variable network performance.

The model describes the operators' implementation at the network layer. This has implications for the services provided at the application layer. In figure 4.5 above, "facilities based service provisioning" indicates example usage scenarios, with VoIP, IPTV and VoD typically offered as vertically integrated services with quality guarantees. Similar services are also available over the Internet as so-called over-the-top (OTT) offers, in this case decoupled from the network layer and delivered with best effort performance.

Note that this way of distinguishing between specialized services and Internet access is also close to the FCC description of specialized services in their report and order from December 2010[23]. FCC describes how specialized services typically share the capacity with the Internet access service at the user's broadband connection to the network. Specialized services are

[23] Federal Communications Commission, Report and order, FCC 10-201, December 2010

separated from the Internet access service and the concept should not be used for services that are substitutes for the Internet access service.

Quality dimension

Another important differentiation between service offers is their capability of providing quality guarantees, varying from best effort to fully guaranteed end-to-end quality. This variation is due to the implementation of different traffic management techniques in the IP network providing the service. These traffic management techniques may include both application agnostic measures (like for example general queue management) and application specific measures (like throttling or blocking of individual applications).

Specialized services and Internet services can both have varying levels of quality guarantee. Today the complete range of quality techniques is used for specialized services, from best effort corporate networks and VPNs to IPTV and VoIP with guaranteed QoS. Internet services however are at present more limited in their use of quality techniques. However, the standardization by IETF of quality architectures could also enable guaranteed QoS for the Internet in the future[24]. The most challenging aspect regarding implementation of these architectures is the IP interconnection between providers.

4.6 The term "quality of service" in Art. 22 (3) of the USD

The new article 22 (3) of the Universal Service Directive states that "*In order to prevent the degradation of service and the hindering or slowing down of traffic over networks, Member States shall ensure that NRAs are able to set minimum quality of service requirements*". Recital 34 of Directive 2009/136/EC clarifies that the "*degradation of service*" can but does not have to amount to the hindering or slowing down of traffic.

Given that QoS can only be specified for individual services, including many parameters outside the control of the network operator, the new provision in Art. 22 (3) USD should be interpreted as limited to the network performance concept since QoS in the sense defined above (in section 4.2) would require the specification of individual QoS levels for a very large list of end-to-end services. It would also require intervention into areas that are not under the control of the operator.

It does not appear necessary to consider the application of "*minimum QoS requirements*" to specialized services, since these intrinsically contain contractual terms relating to quality of provision. The term "*minimum QoS requirements*" could be understood as (ensuring):

- a sufficient performance level of the Internet access service.
- the absence of selective and/or excessive application-related throttling or hindering.

This would be especially needed if that Internet performance was unfairly degraded in order to benefit the development of specialized services.

[24] Several RFCs are standardized by IETF specifying quality architectures like Differentiated Services (RFC 2475 and others) and Multiprotocol Label Switching (RFC 3031 and others) that are used extensively inside individual providers' networks, but that also are applicable to inter-provider solutions.

5. Overview of quality evaluation methods

This chapter gives an overview of the most relevant quality evaluation methods available for networks based on the IP technology. The description starts by highlighting the specific challenges that face any evaluation of the quality of IP networks. It is followed by a description of general methods for evaluation of both IP network performance, and performance of individual applications run over IP based networks. The last section gives an overview of currently available quality evaluation tools.

5.1 The four areas of quality evaluation

Before going into the detailed elaboration of quality evaluation methods, a presentation is made in this first section of how the use of quality evaluation methods fits into the process of determining the minimum quality requirements according to USD article 22 (3). The enforcement of this article will typically consist of three phases which are described in detail in the following three chapters.

1. Detection of situations that could trigger imposition of the minimum QoS provision (chapter 6)
2. Collection of relevant data (e.g. current quality performance) in order to decide minimum quality requirements (chapter 7)
3. Assessment of whether the network under evaluation meets the minimum quality requirements (chapter 8)

The quality evaluation methods are also intended to be used in evaluation of the transparency requirements, as described in the BEREC “Guidelines on Transparency in the scope of Net Neutrality”. This constitutes a fourth area of quality evaluation related to net neutrality.

4. Verification of the information provided by ISPs about the quality level they offer (ref. the transparency requirements, USD article 20 and 21)

The figure below shows these four areas of quality evaluation related to net neutrality as separate flows. Each of these flows is divided into three steps numbered a, b and c. The three generic steps that all four flows consist of are

a) Defining the purpose and setting down the process for the quality evaluation
b) Carrying out the quality evaluation step using tools selected from the toolbox
c) Analysing the results of the quality evaluation step

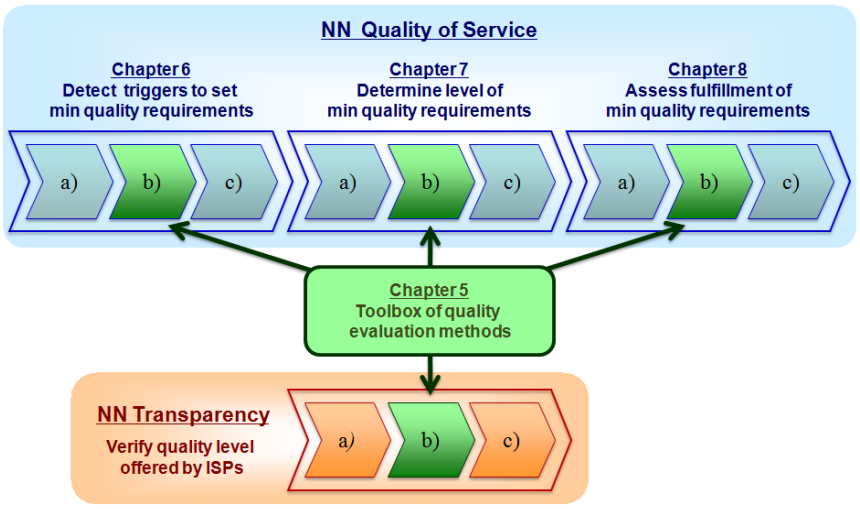


Figure 5.1 – The four areas of quality evaluation

When one flow leads directly into the other, the last step of the first flow will typically overlap with the first step of the second flow. In the figure above, step c) of chapter 6 will typically overlap with step a) of chapter 7, and step c) of chapter 7 will typically overlap with step a) of chapter 8.

In particular, the first step of each flow, where the concrete purpose of that quality evaluation area is used as a basis for the preparation of the process, varies from case to case, as elaborated on in chapters 6, 7 and 8 respectively. The purpose may be to:

1. Evaluate the quality level in the market, for example after indications of quality degradation have been received, to decide whether it is necessary for the NRAs to set minimum quality requirements (ref. chapter 6)
2. Decide if the setting of such requirements is deemed necessary, in which case an additional process may be needed, to determine the level of the quality requirements (ref. chapter 7)
3. Assess whether ISPs fulfil the minimum quality requirements, in the case where such requirements have been set (ref. chapter 8)

And in connection to the transparency requirements:

4. Verify whether the quality level offered by ISPs is in accordance with the advertised and contracted quality (ref. BEREC's "Guidelines on Transparency in the scope of Net Neutrality")

5.2 Quality evaluation challenges in IP networks

The network performance of IP internetworks is challenging to evaluate. The mesh structure of the interconnected networks, the mesh structure inside each network, dynamic routing and dynamic traffic pressure on the networks, all make the use of statistical methods indispensable. Packet switching and connectionless forwarding of the IP protocol results in a variable bit rate best effort performance. Without the assistance of enhanced IP technologies (like e.g. DiffServ and MPLS), it is not possible to guarantee the quality level of end-to-end communication on an IP network.

The ISP will only be able to control its own network resources. However, the ISP will also, based on the service level agreements of the interconnection arrangements, to some extent be able to ensure the performance of the links into and out of its own network. Even if handling of the traffic beyond this point (communications infrastructure and servers at the remote application/content provider end) lies outside the ISP's control in the case of best effort services, the ISP should be responsible for establishing interconnection agreements that are sufficient to ensure a reasonable level of performance to its customers.

A particular concern of best effort IP networks is that they will be subject to congestion from time to time. To cope with this situation the endpoints (users' PCs and servers for example) can execute a congestion control function. This means that some applications running on the terminal equipment reduce their transmission speed when indications of congestion arise. This ability to reduce the traffic pressure on the network depends on which transport layer protocol is being used by the individual application. TCP (Transmission Control Protocol) supports congestion control while UDP (User Datagram Protocol) does not.

However functionality at higher layers can have similar effects, like adaptive media coding which is increasingly being used for modern streaming applications. Adaptive media coding software senses the available capacity between the sender and receiver and adjusts the compression ratio of the media stream accordingly. This is usually implemented through coding at multiple bit rates and the media player clients can then switch between different encodings available from the server, depending on the congestion situation on the network.

A consequence of this is that the individual application under observation, as well as the general mixture of applications in use, will influence the performance even when the network operators don't manipulate the applications' individual performances. In other cases active queue management is performed by routers in the network in an application-neutral way to assist the congestion control function of the end points, or deep packet inspection techniques can be used to manipulate individual packet flows inside the network. (Ref. chapter 4)

In strictly managed IP networks, meaning advanced IP networks configured to handle prioritized traffic classes or even to handle quality guarantees for individual traffic flows, measurement of network performance will of course depend on the specific applications used. Measurement of application performance in such cases is described in section 5.4.

5.3 Evaluating IP network performance

The overall network performance can be described by a set of quality indicators. These are:

- capacity (also referred to as bandwidth, speed or transmission rate)
- latency (also referred to as delay)
- jitter (delay variation indicating small-scale latency)
- packet loss (which is the dominant cause of errors in IP networks)

For practical purposes, these indicators are related to a specific "path", meaning the collection of network nodes and their interconnecting links between the measurement points.

First of all we have the *capacity* itself, also called *throughput*, of the electronic communications service. Because of the varying network conditions described above, the capacity can be best measured by different statistical values such as minimum (or 5% percentile), mean, typical and maximum (or 95% percentile) values. These values will have to be measured separately in outgoing and incoming directions. Furthermore, as these values will change over time, a complete set of measurements performed at different points in time would be necessary to adequately describe the performance.

Other relevant performance aspects, especially for real-time applications, are *timing and error-related parameters*. Timing will typically be measured as a mean latency and variation of the latency (so-called jitter). Errors in packet-switched networks may have several causes, such as loss of packets and bit errors within packets. Packet loss is usually the most significant contributor to data errors. Lost packets are retransmitted for some applications, for example those using TCP as a transport layer protocol. Naturally, this also adds to the observed latency because the receiver has to wait for the retransmitted data. (In the case of TCP, loss of packets leads to reduced capacity).

Network performance can be measured end-to-end for the different packet flows. However, as the control that each individual ISP is able to exercise is limited to its own network resources, measurement of the performance of *segments* of the complete traffic transmission path is needed in order to evaluate individual ISPs. The end-to-end paths can be divided into an *access leg* at each end plus an intermediate *interconnection leg* which binds the two access legs together.

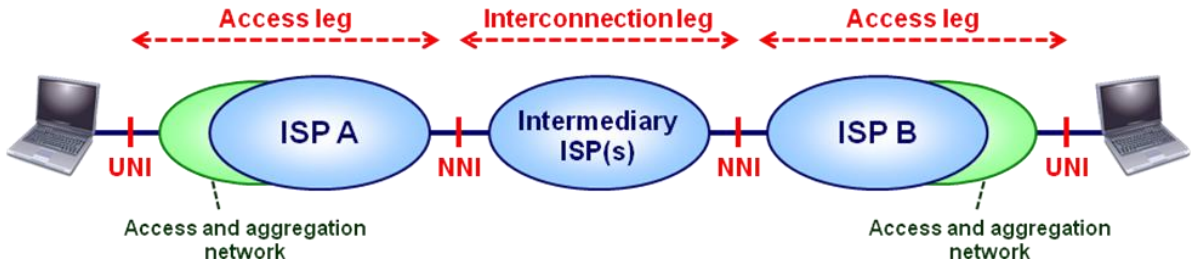


Figure 5.2 – Access leg and interconnection leg

The access leg at each end of the path is under the control of individual ISPs. Measurement systems exist today that are capable of performing access bandwidth measurements fairly precisely. The measurement system is typically configured as shown in the figure below, where the access capacity is measured through the aggregation network plus the IP network of the individual ISP towards a measurement server that is placed at the Internet exchange[25]. For mobile networks the base station will take the place of the aggregator and the radio link will take the place of the access line. Quality measurement for mobile networks is for further study in the follow-up work on net neutrality.

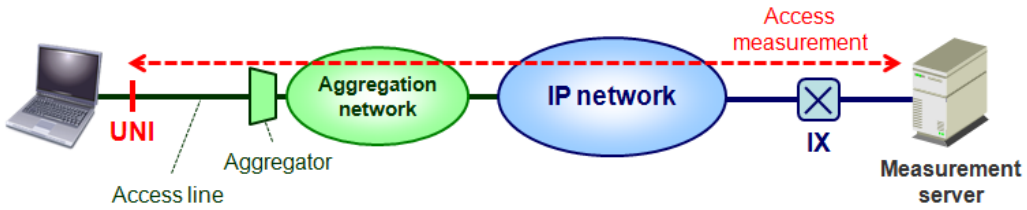


Figure 5.3 – Network configuration of access quality measurements

Because of the mesh network inside the ISPs IP network there will in fact be several different paths from each access to the measurement server. The IP network part controlled by the ISP can easily be configured for high performance tailored to suit the test traffic (e.g. using over-provisioning), so the measurement will in fact usually only measure the performance of the access line plus the aggregation network, as these will constitute the potential "bottleneck".

Measurements on the access leg meet special challenges because of the role of the terminal equipment and local network (e.g. home network) of the end user. These elements will not be under the ISP's control as described in chapter 4. Dedicated test probes may be used to reduce/eliminate this problem, like the European broadband quality measurement study.[26]

When it comes to measurement of the interconnection leg, this is far more complicated. First of all this part of the transmission path is not normally under the control of a single ISP. Secondly, there will be a large number of different transmission paths between ISPs. A measurement system for ISP-to-ISP paths could be envisaged, but it is a highly complex task to achieve reliable measurement results in such a system. Therefore it may not be possible to set up a trustworthy system with currently available technology.

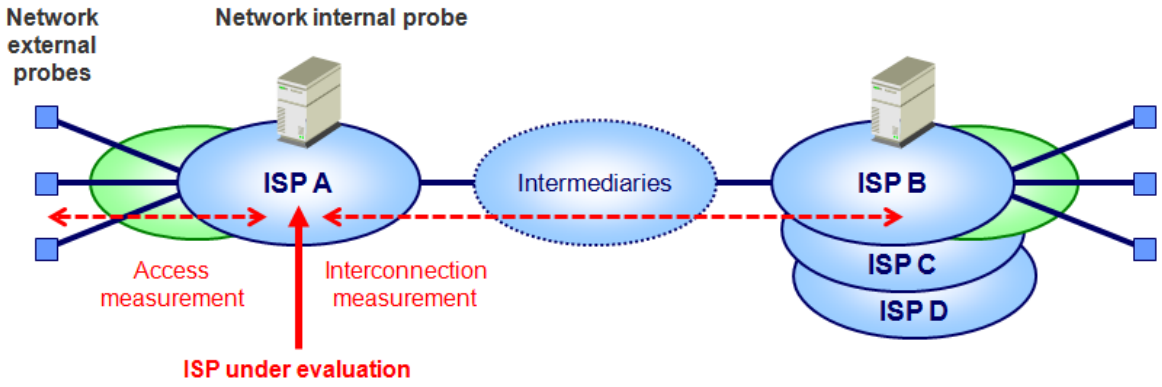


Figure 5.4 – Network configuration of interconnection quality measurements

[25] In ETSI EG 202 057-4, different parameters (login time, data transmission speed, unsuccessful data transmission ratio, successful log-in ratio, delay) are measured between a test PC connected to the access network and a dedicated test PC situated inside the network. The IETF IP Performance Metrics Working Group (www.ietf.org) also provides methodology within this area.

[26] Quality of Broadband services in the EU - SMART 2010/0036

An example of how such an interconnection measurement system could be configured is shown in the model above. Network internal probes (a kind of measurement server) can be configured to measure the performance of ISP-to-ISP traffic. It is also possible to measure from network external probes placed at the network accesses, all the way to probes placed in other ISPs' networks.

Although measurement of the interconnection leg is challenging, it is still possible to use statistical methods to measure for example mean values and follow the development over time, as mentioned earlier in chapter 5. Measuring through the access towards a wide range of network internal probes distributed over the Internet would cover both the access and the interconnection legs and give an indication of the performance of the Internet electronic communication service beyond the access leg. The more distributed probes that are used, the more accurate these results will become.

Several non-standardized measurement tools are also available on the Internet today which allow evaluation of performance parameters (such as capacity and latency) between end users and measurement servers placed in strategic places (ref. section 5.5). However, these tools may not be sufficient to identify where the bottlenecks are in the internetworking scenario.

5.4 Evaluating performance of applications

The performance of the individual applications can be measured by the same parameters as described above for the measurement of the total capacity made available to the end user. However, standardized performance requirements of different applications are usually specified as Quality of Service parameters including the performance of the terminals and higher protocol layers.

By doing measurements of *individual traffic flows originating from different applications* the same test configuration as described in the previous section can be used. This means that the measurement is performed at the network layer as opposed to the application layer as shown in the figure below. Such measurements must necessarily be performed end-to-end, but one of the ends can easily be placed at measurement servers located at strategic places inside the network to simplify the configuration.

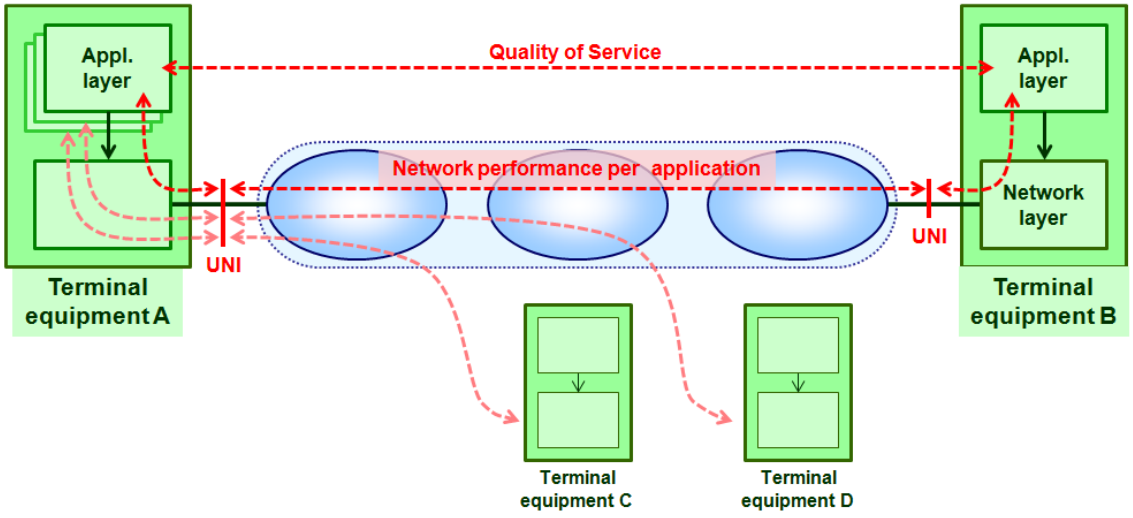


Figure 5.5 – Model showing network performance per application

When the performance of several applications is measured, the results can be compared to detect different treatment of different applications in the network. Blocking of applications can easily be detected and through advanced measurement configurations it is also possible to detect throttling. However, the influence of ordinary congestion in the network (including the congestion control executing in the end points) must be taken into account to be able to detect targeted manipulation of the traffic. Another issue is that even if it is detected that some application is degraded compared to another, it may still be difficult to detect precisely where along the path that degradation is being introduced.

Furthermore, application performance also relies on the specific traffic management implemented by ISPs. Apart from the most obvious cases of blocking (where packets of a specific application are dropped), or throttling (capacity available for the packets originating from a specific application is limited by dropping or delaying *some* packets), modern traffic management techniques permit more sophisticated interventions that are very difficult to detect (such as header forging, modification of IP packets, etc.) in a real environment[27]. In these cases advanced diagnostic tools can be used to detect unexpected network behaviour[28].

This kind of evaluation of application performance does not need to be performed for every application, but it can be a practical method to apply to any individual application when investigating "degradation of service".

Examples also exist of content and application providers offering quality measurement tools on their websites. In the UK, the BBC has developed a traffic-light system for its video on-demand iPlayer to assess users' download performance and inform the user whether their traffic is being throttled. Youtube provides its users with a Video Speed Dashboard which allows people to compare the speed of their Youtube experience with that of other users and with different ISPs. A key issue for the users of the online game World of Warcraft is latency, because a high latency can become a hindrance for gaming with other online users. World of Warcraft provides its users with a colour-coded indicator on-screen of the level of latency being delivered by their Internet access service.

The performance of specialized services is usually specified precisely in the subscriber contract or it is implicitly derived according to the nature of the service. As these services often include dedicated terminal equipment they can be specified by ordinary Quality of Service parameters. If the performance of specialized services is to be compared with Internet based delivery of services, both will have to be monitored in terms of their network performance at the network layer instead of by the use of strict technical QoS.

[27] For instance, until 2007 the American cable operator Comcast implemented a traffic management policy that limited the upload traffic for some peer-to-peer protocols in some specific circumstances by sending "reset" TCP packets in the place of the end user.

[28] For instance, the Glasnost tool (http://broadband.mpi-sws.org/transparency/bttest.php)

5.5 Current quality evaluation tools

In this section the main characteristics of some tools/sites that currently measure the quality of Internet access service are briefly presented. The presentation divides the tools into two categories; tools where NRAs are stakeholders, and tools operated by other organizations.

The tools mentioned are not uniform when it comes to what layer (physical, network, transport or application) of the protocol stack they address. Thus, some of the tools may be better suited to measure specific quality at e.g. the transport layer than others. Due to this, NRAs are advised to seek a thorough understanding of a tool's capabilities before they consider using it.

Tools where NRAs are stakeholders

Network Measurement System (NE.ME.SYS) is the tool of AGCOM's *Misura Internet* project[29]. It measures the performance of each operator in Italy allowing customers to evaluate the quality of their Internet access at a fixed location through a certified system. Measurements are performed using data communication between the user's computer and the remote server which manages the measurements. After completing the measurements, the client can download the results recorded from the *Misura Internet* web page.

Measurement target: Internet download and upload capacity, measurement failure rate, latency, loss and availability
Protocol layer: Network (ICMP), Application (FTP, HTTP)

The Public Utilities Commission in Latvia runs a tool called **SPRK ISPTEST**. Visitors connecting from a Latvian IP address can measure latency, download and upload capacity, loss ratio and jitter. Measurements are made towards servers connected to the Latvian Internet Exchange (LIX). By signing an agreement, ISPs can get access to measurement results obtained by their own customers – but not results from the competitors' customers. The NRA can access all data, while ordinary visitors can choose to save their measurement data to PDF.

Measurement target: Internet download and upload capacity, latency, jitter, loss
Protocol layer: Application (HTTP)

The National IT and Telecom Agency, Denmark runs a tool called **Bredbaandsmaaleren**[30]. This tool allows visitors to measure latency, and download and upload capacity from their computer towards a server located at the Danish Internet Exchange (DIX). Measurement results are saved and the visitor can send a link to the data by e-mail. The tool is based on a measurement engine from Ookla (US).

Measurement target: Internet download and upload capacity, and latency
Protocol layer: Application (HTTP)

The Norwegian Post and Telecommunications Authority (NPT) employ **Nettfart.no**[31], a tool quite similar to the Danish NRA. Measurements of latency, download and upload capacity are done towards a cluster of servers at the Norwegian Internet Exchange (NIX). Visitors can then compare their results against other measurements of comparable broadband products.

Measurement target: Internet download and upload capacity, and latency
Protocol layer: Application (HTTP)

[29] https://www.misurainternet.it/
[30] http://borger.itst.dk/verktojer/bredbaandsmaaleren
[31] http://www.nettfart.no

The Hellenic Telecommunications and Post Commission (EETT) has developed **SPEBS**[32] (System for Performance Evaluation of Broadband Service), an open source measurement tool that integrates and enhances the tools provided by the Measurement Lab (M-Lab) platform (see below). Visitors can measure throughput/capacity (uplink/downlink), latency, jitter and packet loss. Registered users gain access to additional services, including geo-mapping of their broadband connection, graphical representation of historical data and retrieval of such data in CSV format. All visitors have access to geo-mapped statistics. Detection of service performance differentiation and geo-mapping of relevant measurements data is planned for release by end of 2011. All anonymous measurements data are made public and they are accessible by ISPs via a Web Services interface. SPEBS is deployed on the Greek Internet Exchange (GR-IX).

Measurement target: Internet download and upload capacity, latency, jitter, loss, detection of service performance differentiation.
Protocol layer: Application.

Tools run by other organizations

The Swedish **Bredbandskollen**[33] is a tool similar to the above mentioned tools provided by the Danish and Norwegian NRAs – with the exception that the tool is run by an independent organisation (the Swedish national Internet registry). Visitors can choose to carry out measurements towards servers at different domestic locations, as well as avail oneself of the opportunity to install dedicated smartphone versions through iTunes App Store and Android Market. All measurements that are saved by users are available to other visitors.

Measurement target: Internet download and upload capacity, and latency
Protocol layer: Application (HTTP)

SamKnows[34] offers the very comprehensive tool *Test my ISP* providing consumers with reliable statistics of their broadband connection. It has special importance because at present its results are used by regulators to study the behaviour of broadband in the United States and the United Kingdom. The European Commission has, as part of its Digital Agenda for Europe, contracted SamKnows to do a survey of retail broadband services regarding http download capacity, ping performance, DNS lookup time and packet loss.
This tool uses a specific probe supplied by Netgear in order to measure and record the performance of ISP's. Their results provide an insight into the broader practices that can be adopted by ISPs to manage traffic on their networks. The measurement records are delivered monthly to each customer who participates in the project.

Measurement target: Internet download and upload capacity, latency, jitter, availability, loss, DNS query response time, DNS query failure time, Web page loading time, Web page loading failure rate and video streaming performance.
Protocol layer: Network (ICMP), Transport (UDP, TCP) and Application (HTTP, DNS, streaming protocols).

Measurement Lab[35] (M-LAB) is a research platform established by Google, New America Foundation`s Open Technology Institute (OTI) and PlanetLab Consortium (and supported by other institutions such as FCC and EETT), which includes a series of tools designed to measure various Internet communication parameters, allowing researchers to take a broader view of the current behaviour of operators in terms of their quality of service.

[32] http://broadbandtest.eett.gr/?l=1
[33] http://www.bredbandskollen.se/
[34] http://www.samknows.com/broadband/
[35] http://www.measurementlab.net/

Measurement target: The range of tools hosted by M-Labs target a wide range of parameters, including capacity, latency, jitter, loss, availability etc. In addition, some also offer complex diagnoses capable of detecting application blocking, throttling or quality differentiation.
Protocol layer: The available tools address all layers (network, transport and application).

RIPE Atlas[36] is a new measurement initiative from RIPE Network Coordination Centre (the Regional Internet Registry managing IPv4, IPv6 and AS numbers for Europe, the Middle East and parts of Central Asia). Atlas is an active measurement system consisting of small hardware probes that connect to the Internet, and a central management system. As a host for such a probe, a person/organisation can access its measurement results, which currently consist of uptime history, latency to the first and second router hop, and latency measurements to a set of predefined destinations. According to RIPE NCC, future upgrades will add new functionality.

Measurement target: availability (uptime), latency
Protocol layer: Network (ICMP)

Cedexis[37] is a French company that delivers a suite of several performance monitoring tools. Measurements are generated by visitors to websites and infrastructure where small agents (javascript tags) reside. The owner can then get information about a range of performance parameters experienced by his visitors, including results specific to each connecting ISP.

Measurement target: Availability, latency and capacity (throughput)
Protocol layer: Application (HTTP)

Neubot[38] is a free software tool provided by NEXA Center for Internet & Society in Torino, Italy. This tool runs in the background and periodically performs automatic transmission tests. These tests evaluate the Internet performance using various application level protocols, its goal being to quantify network neutrality. The current release (0.3.7) measures latency as well as HTTP download and upload capacity against predefined servers, whereas future releases aim to do multi-protocol testing against other instances of the tool.

Measurement target: Internet download and upload capacity, and latency
Protocol layer: Application (HTTP)

[36] http://atlas.ripe.net/
[37] http://www.cedexis.com/
[38] http://www.neubot.org/about

Part III – Regulatory powers

In Europe, there is a competitive environment for the provision of Internet access services, and a majority of end users have a choice between several ISPs.

In the context of an effectively competitive market, i.e. a market providing complete transparency and easy switching to customers, an ISP delivering poor quality or introducing blocking or throttling of applications could harm its attractiveness and be penalized by subscribers who could switch to rival ISPs. Increasing end user demands put pressure on ISPs to provide adequate quality levels and to invest in supporting more capacity-hungry applications. Moreover, a competitive environment promotes a broader offer that includes services tailored to varying customer needs (for instance, an offer with more capacity but at a higher price, or an offer with less capacity at a lower price).

However, in a scenario where the provision of premium modes of electronic communications services are developed, NRAs will have to assess whether the position of power held by an ISP over its own subscriber base has the potential to negatively affect the performance of the Internet access service. If in the future an NRA considers that the quality available on the Internet is becoming degraded, resulting in harm to end users and/or to innovation, it could envisage the imposition of minimum quality requirements as defined in article 22(3) USD on one or several operators.

This power should be used as part of a long-term process, and needs to be based on an open approach to limit the risk of sending negative signals that could adversely affect the markets. The setting of minimum quality requirements is a remedy to avoid degradation of service, which should be executed with thoughtful caution. Prior to defining minimum quality requirements, the following conditions could be considered:

- Whether there is a situation where Internet access services are routinely degraded
- Whether there are no effective alternative ways to cope with the issue (such as strengthening transparency)
- Whether harm is observed for end users and/or innovation
- Whether the benefits of defining minimum quality parameters outweigh the drawbacks.

Different markets and countries may require or prefer different solutions. For example, one NRA could prefer to measure quality on a regular basis, while another could prefer to intervene when investigations are to be launched due to a formal complaint from a content provider or from end users.

6. When to set minimum quality requirements?

This chapter of the report assesses what could trigger the imposition of minimum quality requirements for the performance of electronic communications services according to article 22 (3) of the Universal Service Directive.

As concluded in section 4.6, it does not appear necessary to consider minimum quality requirements with respect to specialized services, since these intrinsically contain contractual terms relating to quality of provision. This chapter therefore focuses specifically on quality conditions on the Internet service.

There will always be a thorough investigation process preceding the potential imposition of minimum quality requirements by NRAs. Different situations may trigger the use of this

regulatory tool. The trigger detection phase will typically consist of three steps, based on the generic approach presented in section 5.1.

a) Indications received from stakeholders or symptoms detected by the NRA
b) Quality evaluation step performed to verify the indications/symptoms
c) Analysis of the results: Is a trigger detected? Yes or no to intervention

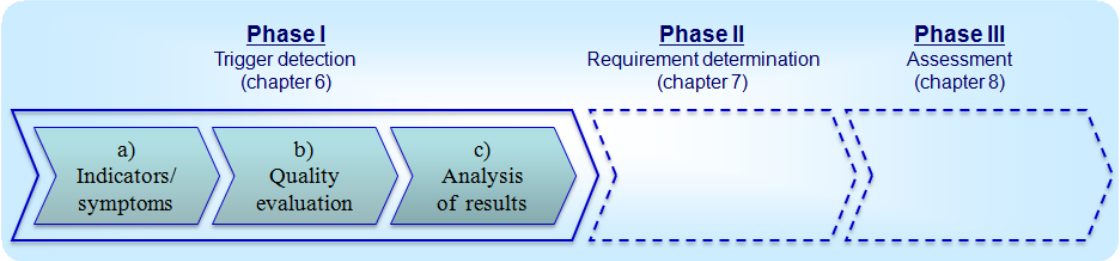


Figure 6.1 – The trigger detection phase is divided into three steps

While it is foreseen that these three steps will enable a decision to be made on whether minimum quality requirements should be set, there will most likely be a relatively large variation between member states when it comes to exactly how each step is performed in detail. This will be further elaborated in a section below describing each of the steps (6.2 – 6.4).

6.1 Degradation of service

Before going into the individual steps, it is useful to look into the kind of situation this regulatory tool is supposed to prevent, as this will also give some idea of the type of actions by ISPs that might fall into the category of indications or symptoms leading to a "trigger situation".

"*[D]egradation of service and the hindering or slowing down of traffic over networks*" can consist of poor performance of the general electronic communications service as a whole (e.g. total capacity) or of specific applications using the underlying communications service, or both. It may result from a general trend in the marketplace or from an individual provider's policy.

As described in chapter 3, recital 28 of the USD[39] states that "*End-users should be able to decide what content they want to send and receive, and which services, applications, hardware and software they want to use for such purposes*". This indicates that there is a need to look beyond the total capacity and consider the users' control over their access for specific purposes.

Different categories of degradation can be identified (not an exhaustive list):

- general congestion due to a high demand for electronic communications services
- general congestion due to prioritization of specialized services at the expense of the Internet access service
- deliberate blocking or throttling of individual applications and/or content
- deliberate blocking or throttling of certain sources and/or destinations

[39] Directive 2009/136/EC

6.2 Step a) Indicators and symptoms

6.2.1 Reactive and proactive approach

Two main approaches could be adopted for this first step: Reactive or proactive. The *reactive approach* is mainly focused on following up complaints from different stakeholders like end users, content providers and application developers. Complaints from end users could for example be caused by problems in accessing specific sites or low performance of individual applications.

Content and application providers are placed at the upstream end of the delivery chain and they usually have a broad user base with which they interact. The servers and content distribution networks (CDNs), if used, provide performance measurements. In addition the providers often receive feedback from their customers. Based on all this information the content and application providers will often be in a good position to monitor the performance of content being distributed over the networks they use.

Application developers and advanced end users are also in a good position to detect degraded operation of the network. These persons often have good insight into the technical details of network and application performance and will in many cases be able to detect blocking and/or throttling of specific communication sessions. Independent organizations concerned about net neutrality may also address their concerns to the NRAs.

If they adopt a *proactive approach*, NRAs will perform some kind of market surveillance of the characteristics of available offers. This could, for example, be based on advertized information available from the ISPs' websites, or it could be based on measurement tools providing performance statistics of the ISPs' networks.

Today technical measurement tools used by some NRAs provide the users with information about the access capacity available to them. This may lead to end users complaining to ISPs and also to NRAs. The results of these user-initiated measurements are then typically stored in databases for statistical analysis that for example could show performance trends for the different ISPs and for the market in general.

These measurement tools usually only cover the access leg because the interconnection leg is not easily evaluated. Detection of blocking and/or throttling of individual applications or of IP addresses is usually not possible using measurement tools currently provided by NRAs, but some independent tools exist, as mentioned in chapter 5.

6.2.2 Example indicators

In both the proactive and reactive approaches it is important for NRAs in step a) to identify and monitor indicators of practices that might violate network neutrality, in order to develop a baseline understanding of the market. This means observing the market over some period of time to prepare the ground for detection of any indicators showing "unusual" patterns, which might indicate that something has changed. As shown in the figure below, at the end of period 2, two of the monitored indicators showed an increase that could mean a change in the market. When this is detected, step b) follows, in which an evaluation and deeper analysis takes place, as explained later in this chapter.

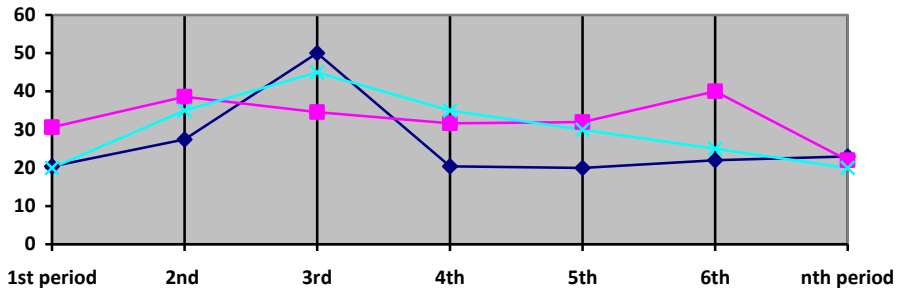


Figure 6.2 – Indicators watched over a period of time

The indicators could be more or less technical, depending on the approach adopted by the NRA. They could for example include the number of complaints characterised as net neutrality issues, or be based on evolution of the mean available throughput rate.

An NRA could monitor quality indicators to compare an ISP's quality at a given time to others in the market or to detect the evolutionary trend of the quality provided by each ISP over a given period. However, comparability between ISPs is more or less crucial depending on the NRA's strategy, especially if measures are to be published (as is the case in some countries).

Examples of technical quality indicators:

- Network performance
  - Throughput
  - Latency
  - Jitter
  - Packet Loss
- Application-oriented indicators
  - Webpage loading time
  - Success rate of a given web surfing scenario
  - Success rate of access to a streaming site
  - Mean time to load a given video from a streaming site
  - etc.

(Refer also to chapter 5 for measurement configurations.)

Examples of non-technical quality indicators

- Availability of unrestricted internet access offers
- Outcomes of disputes settlements handled by the regulator
- Number of complaints from consumers to the regulator or other organizations[40]

6.3 Step b) Quality evaluation

If a large number of complaints is received from stakeholders or severe symptoms of quality impairment are observed by the NRAs themselves, this should lead to a more thorough quality evaluation with the purpose of deciding whether intervention is needed or not. Unless relatively detailed measurements are already being performed, technical measurement tools may now be needed to verify the indications/symptoms.

[40] Example http://respectmynet.eu/

There is however a possibility to use the number of complaints received, especially complaints related to bandwidth performance that is significantly lower than advertized and complaints about blocking and/or throttling of specific applications, as quality evaluation parameters themselves. In particular an increase in the number of such complaints will be of interest to the NRA.

This step could also be partly based on publicly available information about marketplace offers, probably supplemented by dialogues with relevant ISPs to gather more detailed information. Information provided to end users should be transparent, describing all kinds of service degradation mentioned above, but is more likely to only describe deliberate blocking or throttling of individual applications and deliberate blocking or throttling of certain IP addresses.

In order to collect independent information about the different ISPs, an evaluation of the networks performance may be conducted by the NRAs, either directly or with the help of some third party experts.

Quality evaluation should first focus on the total throughput of the access service made available per user. The general test configuration presented in section 5.3 should be capable of measuring statistical values of throughput. More detailed information about error rate (packet loss) and timing (mean delay and jitter) can also be provided. (For a more detailed discussion about the different quality parameters, please refer to section 5.3.)

One should be aware that this test configuration has some limitations when it comes to measuring varying performance as in practice the user communicates towards lots of different destinations on the Internet not covered by this configuration. An advanced test configuration that also covers the interconnection legs between different ISPs would improve this situation, as described in section 5.3.

Regardless of the measurement method used, the performance indicators could easily be applied to calculating aggregated indicators for individual ISPs as well as for the complete market. An important aspect of this aggregation is distinguishing between different subscription packages. The actual performance should be calculated per announced bandwidth class, and Internet access service and specialized services should be calculated separately.

In addition to focusing on the total capacity, the performance of individual applications could also be evaluated as a second step. A simplified model presented in section 5.4 shows the main idea of how this could be performed. Special measurement tools for testing selected applications are however not as commonplace as general tools for measurement of the total capacity.

Verification of specific reported incidents of blocking and/or throttling of specific applications can’t be based on total capacity measurements. Blocking of applications could simply be verified by using the application to see whether it works or not. However, throttling that results in reduced capacity for a specific application is difficult to distinguish from reduced capacity caused by congestion, without a tailor made measurement tool.

One could also consider evaluating a designated portfolio of applications of most importance for end users, like web, voice over IP and video streaming for example. Specific test suites could in that case be developed to address this. The selection of applications for the portfolio would of course have to be adjusted according to the dynamic changes of end users’ behavior.

6.4 Step c) Analysis of results

Once quality evaluation has been performed, the results will be analyzed to decide whether the situation is acceptable or if intervention is necessary. Below, different aspects to be considered during this analysis, without presuming that all these aspects necessarily applies in every case, are elaborated on.

When evaluating the total capacity made available per user, the summarized results for the whole market under investigation could be compared to the performance of the currently available technology, in particular in the access segment. Results for individual ISPs could be compared to their own advertized bandwidth, and the results per bandwidth class of different ISPs could be compared to each other.

By their very nature, best effort services have no end-to-end QoS requirements attached. There are no defined traffic classes (in terms of throughput, delay, jitter or other parameters) that conform to some performance standard for today's Internet service, or indeed for individual applications that depend on it. However, the performance of the Internet access service could be compared to the performance of specialized services, both for the market in general and for individual ISPs.

In particular, *changes* from current performance levels can give clear indications about the situation. Enhanced performance is a positive sign while reduced performance may indicate that degradation is taking place. However, due to continuous technical development, even increased performance is no guarantee of sufficient quality if increased performance of specialized services exceeds that for the Internet access service.

Multiple measurements are necessary to detect changes over time, and analysis based on this method is more easily performed if the NRA continuously and proactively monitors the market developments.

Regarding evaluation of the performance of individual applications, blocking will usually be considered more severe than throttling, but throttling may in some cases be so heavy that the application will not be usable anyway. The relative importance of the actual application(s) being blocked may also be considered during this analysis. Changing application performance over time could also be taken into account.

The analysis will have to take into account whether detected blocking and/or throttling relates to restricted or unrestricted access offers. A restricted subscription (e.g. one which explicitly does not allow p2p file sharing) is of course anticipated to block such use. However, the availability and price levels of unrestricted offers compared to restricted offers may be of relevance during this analysis step. In particular an increasing number of restricted (blocked or throttled) applications is an important indicator to notice.

If developments over time indicate decreasing availability of unrestricted subscription offers with acceptable conditions (i.e. compared to the restricted offers and/or specialized services), this should be considered particularly alarming. This could be evaluated both for the market as a whole and also for individual providers, as not every geographical area will necessarily have several ISPs, from whom users can choose.

Because of the Internet's global connectivity, constraints on particular IP addresses are also an important parameter for detecting limitations on the openness of the Internet. Blocking of individual destinations should be considered a degradation of the Internet service if they cannot be justified as reasonable traffic management.

An important aspect of prevention of application-specific degradation is the network effect. The usefulness of many applications depends on the number of users of that application. This implies that the restriction of specific applications by some providers will also affect users of these applications at other providers.

To reduce the burden on individual NRAs during this process, BEREC could consider the possibility of developing a common quality reference level for the general network performance and the performance of individual applications. Such a common threshold would probably need to contain some variables that facilitate adjustment of the general level to the unique situation in each country.

The minimum quality requirement remedy is, as stated previously in this report, part of a long-term process. Use of this remedy may be considered necessary in cases when other remedies (such as enhanced transparency) do not provide the expected result. Assuming that the quality evaluation step in such a case indicates extensive degradation of service, the analysis step will investigate whether the conditions to impose requirements are present.

The outcome of this analysis step is a decision on whether or not the prevailing situation is considered sufficiently severe that intervention is necessary. If so, close scrutiny of the effect of the providers' traffic management practices should take place. In this examination the need to safeguard applications that depend on the quality of the underlying network, prevention of consumer harm, and prevention of discriminatory behaviour restricting competition[41] would be evaluated.

Safeguarding applications could typically be considered necessary in cases when applications are throttled and/or blocked. Prevention of consumer harm could typically be considered necessary both for the degradation of the electronic communications service as a whole and for differentiated treatment of individual applications. The same applies to prevention of discrimination.

There is a need for coordination at the European level during this step to avoid diverging practices among NRAs, as USD article 22(3) prescribes a procedure involving the Commission and BEREC. The grounds for action, the envisaged requirements and the proposed course of action shall all be notified by NRAs, while the response from the Commission shall in particular ensure that the envisaged requirements do not adversely affect the functioning of the internal market.

When it comes to detailed assessment of how severe these different types of degradations are, this will be subject to further analysis in the follow-up guideline work stream. There will also be a separate analysis performed by the work stream "Competition issues related to net neutrality", which will provide additional input to this discussion, based on economic assessment of potential discriminatory behaviour by providers.

[41] Ref. Recital 34 of Directive 2009/136/EC

7. How to determine the minimum quality requirements?

This chapter of the report describes how minimum quality requirements for the performance of electronic communications services can be determined, with respect to article 22 (3) of the Universal Service Directive. The minimum requirements address the quality aspects already identified in section 6.4.

As concluded in section 4.6, it does not appear necessary to consider the application of minimum quality requirements to specialized services, since these intrinsically contain contractual terms governing their quality of provision. This chapter will therefore focus specifically on quality conditions of the Internet access service.

In the sections below, the aspects to be taken into account when developing minimum requirements will be further elaborated. Quality requirements should incorporate a multi-dimensional approach in order to be effective. If a policy fails to consider all relevant aspects it may end up imposing requirements that fail to achieve their goal of guaranteeing adequate functionality.

In order to determine minimum requirements for networks and services, it is of great importance that the mechanisms and technical interactions of delivering services over IP network infrastructures are well understood. As explained in chapters 4 and 5, different parties, independent technical infrastructures and a range of specific services are involved in an IP environment.

The main part of determining minimum requirements is to identify the key elements responsible for any quality degradation. However, in most cases several different solutions will be possible, involving different undertakings, different infrastructural elements etc. and entailing different consequences. So besides identifying the causes of the quality degradation, another objective of the determination phase is to decide what kind of requirement will be the most effective and advisable.

The whole process of determining minimum quality requirements is described by the three generic steps given in section 5.1 (preparation, evaluation and analysis). Before going into the individual steps in sections 7.2 – 7.4, the general characteristics of requirements to be considered during the process of determining the minimum quality requirements, is discussed in section 7.1.

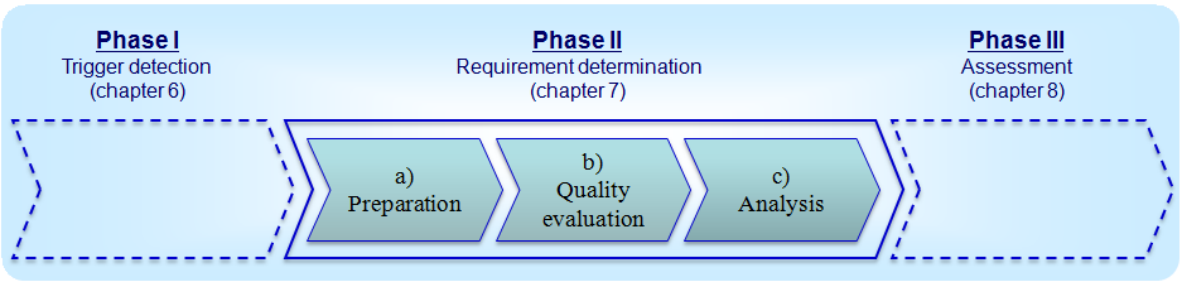


Figure 7.1 – The requirement determination phase is divided into three steps

7.1 General aspects

When setting minimum requirements to achieve the goals identified by the European legislator, an NRA must decide from which angle to address the specific problem. Not every approach is suitable for every situation. While the framework leaves much to the discretion of the NRA in terms of how to shape the desired solution, some common principles can lead to

a successful implementation of these remedies. The goal of this section is therefore to explore the relevant aspects involved.

7.1.1 Proportionality

Following European legal doctrine, BEREC believes that any analysis of quality requirements should respect the principle of proportionality. This principle ensures that adopted measures are based on a fair assessment that properly balances the relevant interests.

According to Article 8 (1) of the Framework Directive measures taken aimed at achieving objectives set out in this Article shall be proportionate to those objectives. One of these objectives is "*promoting the ability of end-users to access and distribute information or run applications and services of their choice",* cf. Article 8 (4) (g). Furthermore, NRAs shall in pursuit of these policy objectives apply "… proportionate regulatory principles"; cf. Article 8 (5). Furthermore Article 8 (4) of the Access Directive states that obligations imposed in accordance with this article shall be *"based on the nature of the problem identified, proportionate and justified in the light of the objectives laid down in Article 8 of … (Framework Directive)".* Article 8 concerns obligations on operators designated as having significant market power.

An application of the principle of proportionality is described in "Commission guidelines on market analysis and the assessment of significant market power, under the Community regulatory framework for electronic communications networks and services (2002/C 165/03)":

"The principle of proportionality is well-established in Community law. In essence, the principle of proportionality requires that the means used to attain a given end should be no more than what is appropriate and necessary to attain that end. In order to establish that a proposed measure is compatible with the principle of proportionality, the action to be taken must pursue a legitimate aim, and the means employed to achieve the aim must be both necessary and the least burdensome, i.e. it must be the minimum necessary to achieve the aim."

In order to avoid disproportionate measures, NRAs should remain conscious of the scope and impact of the remedies they pursue in relation to the envisaged objective. If there is a lack of equivalence between the policy objective and the remedy in that sense, the proposed remedy could be more burdensome than strictly necessary. Likewise there should be a legitimate aim, with an objective justification.

Proportionality in the context of net neutrality can be illustrated by an example. For the sake of clarity a polarized example is used. Let's say the policy objective is an open and accessible Internet: all content and applications should be accessible by end-users. This is the legitimate aim pursued by the policy maker. The chosen solution is to mandate absolute net neutrality: all packets should be treated entirely the same. This is therefore the means employed by that specific policy maker in this example.

The principle of proportionality has been developed in the European context by the European Court of Justice (ECJ) over the last decades, and consists of different subtests: effectiveness, necessity and proportionality *stricto sensu.*

Effectiveness assesses whether a measure is suitable to achieve the legitimate aims pursued[42]. However the European Court of Justice (EJC) has considered whether measures are "manifestly inappropriate in terms of the objective which the competent institution is seeking to pursue".[43] Absolute effectiveness is not necessarily expected however (i.e. in the

[42]This test is often also referred to as a suitability test.
[43] See Case C-189/01, Jippes (2001) ECR I-5689, para. 82

sense of being achieved in its purest form). Following the wording of the ECJ, the test should instead be carried out in an inverted form, so as to arrive at the conclusion that a measure is *not* manifestly *in*appropriate.

In the example presented above, equal treatment of packets is partly effective in achieving the goal of an open and accessible Internet, as it will prevent operators from blocking access in certain ways. On the other hand, it does not entirely prevent degradation of the open Internet. Applications can still be blocked by other means, for example by offering a very low data rate for the upload link or by means of a data cap. One could conclude that the proposed measure in the example is not manifestly inappropriate, and would survive this part of the proportionality test.

The next question relates to *necessity*. Necessity plays a major role in the test of proportionality. It relates to the need to invoke a certain measure but does not have a fixed framework. The standards used by the ECJ in assessing necessity are relative to the circumstances of the case and the relevant area of Community law. Part of the necessity test entails an assessment of whether equally effective alternative options exist that are less burdensome than the proposed measure.

Returning to the example, the question arises whether it is necessary to mandate all packets to be treated equally. For the purposes of the legitimate aim that is being pursued here, that is not *necessarily* the case, as it depends on other options that may be available. The usual situation is that content and applications are accessible, except when specifically blocked or extensively throttled. While treating all packets in an equal manner will probably lead to a situation that attains the desired legitimate aim, it only does so indirectly, as it prevents blocking and extensive throttling to applications and content, which in turn ensures that the policy objective of access to content and applications is met.

As the final part of the test, *proportionality stricto sensu* should be assessed. Part of this assessment entails a determination of the interests being served by the measure taken, and an evaluation of the effects the measure has on interests protected by the EC Treaty. The presence of the latter should at least be acknowledged and considered by the authority invoking the measure. This test also entails an assessment of whether the burdens imposed by the measure are in proportion to the pursued aim; proportionality in the strict sense.

Furthermore authorities should assess whether the legitimate aim is correctly defined. This is relevant in some situations in EU law where there is a predetermined framework for these aims, but for our situation here, the legitimate aim is already extensively described in the relevant directive[44]. As long as an NRA conforms to this aim, problems should normally be avoided.

7.1.2 Classification of requirements

Quality requirements can be classified into two main types: Functional/qualitative and detailed technical/quantitative requirements. Functional/qualitative requirements demand certain normative conditions to be met. For instance a requirement could state that an application should be allowed to function “adequately”. Detailed technical/quantitative requirements on the other hand, demand a performance that satisfies a numerical threshold. An example of such a requirement could be that an application should exhibit an available data transmission ratio of at least x kbps.

Functional requirements can cluster the specific parameters that determine functionality, covering all current and future dimensions. This type of requirement stipulates an end goal to be achieved by the undertaking offering public communications services, and by doing so it

[44] See Chapter 3.

offers important advantages. First, a requirement that clusters these parameters requires less effort to maintain than monitoring a detailed requirement for every single parameter. Instead it just requires the sum of these parameters to perform according to the high level requirement. Secondly, in case future innovations introduce new parameters that are relevant to the functionality in question (e.g. data streams, content or applications), these are automatically incorporated into the functional requirement.

Functional requirements allow for discretionary descriptions, such as 'adequately' or 'sufficiently'. Such descriptions support an approach that incorporates the flexibility and dynamic appreciation described above. Nevertheless they only provide limited information to the addressee, of the specific content of the requirement, of its applicability and interpretation, and of when or whether the requirement has actually been met. However, functional requirements do not exclude further downstream (technical) specification of the discretionary requirement in additional regulation. This can be a useful construction in a system where regulation is layered. For example, the legislator passes an act containing a quality provision with discretionary requirements, which, if necessary, can be further specified or supplemented in regulations or guidelines by (for instance) NRAs.

Technical requirements are more demanding as regards specifying individual parameters, but on the other hand, they deliver much more hands-on information in terms of strict conditions that are easily understood by the addressee. The numerical thresholds are explicit and generally lead to a clear interpretation of whether the threshold is met or not. However, this still doesn't guarantee that the end goal, some desired degree of functionality, is achieved. That depends on the correctness of the ex ante conditions, which can only be confirmed ex post.

It requires more effort to develop and maintain these stricter technical conditions, because each parameter has to be individually set, and then maintained. Future developments and innovations may not be covered immediately, as they may require adjustment of the parameters or incorporation of new relevant parameters. The possible need for this kind of extensive maintenance should be weighed against the resources required to set new conditions, especially in terms of the time required to achieve such adjustment.

7.2 Step a) Preparation

Section 6.4 presented the relevant quality aspects that minimum requirements should address, based on the "trigger detection" process. These aspects are described in rather general terms such as the lack of adequate overall throughput capacity of the underlying electronic communications service or the reported poor performance of specific applications.

Since the provision of electronic communications services over IP based networks, especially the use of applications over the public Internet, may involve the interaction of several providers and network systems, it is difficult to directly identify the cause of any quality degradation. Therefore further investigation may be needed, aimed at identifying the functional elements influencing the observed quality aspects. Relevant measurement methodology for this purpose is described in chapter 5.

Whereas the IP network layer can be directly assessed in terms of its IP packet parameters, i.e. throughput, delay, jitter and loss, applications add an additional layer of complexity. This is because applications are decoupled from the network layer even though the user-perceived quality is significantly influenced by the IP packet transmission function. Thus when setting minimum requirements for applications over the Internet, one needs to be aware of their operating mode.

However, any application or IP network layer or network access service can be analysed with respect to its own functionalities. The quality is determined by a set of functions that depend on various technical processes. The degree of detail needed depends on the service under consideration. Applications also depend on higher layers functions (e.g. higher layer protocols, interworking of networks, terminal performance).

This preparatory step could lead to the identification of two target types for further investigation at the quality evaluation step: either the performance of the Internet access service in general, and/or the performance of individual applications. The first of these addresses the capacity of the provided general electronic communications service, while the second type addresses differentiated treatment of applications, such as throttling and/or blocking.

7.3 Step b) Evaluation of potential quality requirements

The purpose of this quality evaluation is to relate the requirements which are to be determined to the current network performance, in order to reduce or prevent degradation. How comprehensive the quality evaluation step needs to be will depend on the approach already adopted during the “trigger detection” phase (ref. section 6.3). In some cases the results from the preceding phase may be sufficient, and in other cases this “requirement determination” phase may need additional results.

The potential requirements considered during this quality evaluation step will be subject to analysis during the next step in order to test according to the principle of proportionality (ref. section 7.1.1). These two steps (quality evaluation and analysis) may to a large extent be performed in parallel.

7.3.1 Functional requirements

In cases when the requirements to be set are more functional than of a detailed technical nature, the need for measurement procedures may be less comprehensive. As concluded in section 7.2, the two main categories of requirements relate to (a) the performance of the Internet access as an electronic communications service and (b) differentiated treatment of individual applications, like throttling and/or blocking.

A functional requirement for the Internet access service as a whole (affecting the usability of applications) could be to address how congestion management is performed in the providers’ networks. In order to prevent degradation of specific applications, consideration could be given to a remedy of limiting congestion management to mainly application agnostic measures. (Refer to chapter 4 for the classification of traffic management techniques.)

Another functional requirement for the Internet access service could be to address the performance actually provided (for example in relation to the advertised speed). Use of traffic concentration in the aggregation network makes specific throughput at the access service challenging to guarantee. Therefore a qualitative requirement prescribing the performance relative to some target set by the provider could be an approach to consider.

The alternative to such a functional/qualitative approach would be a quantitative approach using technical methods prescribing a specific bandwidth, typically based on statistical parameters taking into account the variable bandwidth. This approach is described below in section 7.3.2.

Functional requirements on the usability of individual applications is another approach to consider. If the degradation is more of the hindering (blocking) or slowing down (throttling) nature, this could be a viable remedy. Similar concerns may also be raised for contractual conditions disallowing use of specific applications, Such requirements could consist of

prohibition of blocking and/or throttling of specific applications, or other qualitative requirements on application performance (e.g. require “adequate” performance level) to limit the throttling of specific applications.

7.3.2 General technical requirements

As mentioned above, as an alternative to setting functional requirements, general technical requirements may be considered. Such a quality requirement would typically prescribe network performance for the underlying electronic communications service provided over the Internet access. A measurement methodology for network performance over the access leg and the interconnection leg is already expanded on in section 5.3.

Current measurement platforms usually cover the access leg only, when measuring between the user access and a measurement server situated close to the ISP under test (e.g. at an Internet exchange). An important aspect to consider in this context is how far the Internet access service actually reaches. Since the ISPs are responsible for their own interconnection arrangements, the Internet access service is regarded as reaching from the user-network interface all the way through to the network-network interface at the interconnections to peering/transit ISPs.

As the Internet electronic communication service is based on many interconnected networks, the quality of this service could only be determined by also taking the interconnection leg into account as described in chapter 5.3. While an individual provider cannot guarantee the quality provided by the other providers, this service is nevertheless the “product” that is sold to the customers. Therefore an important characteristic of this “product” is the quality this complete service has. The quality is, among others, a result of the interconnection arrangements chosen by the individual provider. Technical requirements that include the interconnection leg are complex to determine but, based on statistical methods, this could still be feasible.

Setting technical requirements for the characteristics of different applications running over the Internet presents some complexity, due to the decoupling that exists between the applications and the underlying Internet electronic communication service. Measurement methodology for application performance is expanded on in section 5.4, and considerations regarding such detailed technical requirements are described in the next section.

7.3.3 Detailed technical requirements

In cases when a comprehensive quality evaluation is needed as a background to setting detailed technical requirements, an initial effort can be made by gathering data, i.e. observing the network and resulting quality. A first study of the overall network performance and the relationships involved will provide a rough overview that needs to be further checked.

Based on these results, a detailed evaluation can be performed to determine all relevant quality aspects. The evaluation should start from the end user's perspective by first identifying the user perceivable quality aspects. These can then be related to technical functions at the user-network interface which in turn are influenced by functions taking place at all layers of the IP infrastructure.[45]

In the IP environment several independent undertakings can be involved in providing any specific service. There is a strict decoupling between the application and the network layer of the Internet. Moreover, the network layer consists of several interconnected networks, each

[45] An in-depth explanation and a detailed description of this process are given in ITU-T Rec. E.802. It provides a framework and methodologies for the identification of QoS criteria relevant to users, and guidelines for conversion of these criteria into QoS parameters that can be used to evaluate the QoS of applications. Even though this process is rather complex, it is straight forward and well documented in standardization.

acting autonomously. Therefore the set of quality parameters needed to assess the quality of a service from a technical perspective may spread over the area of influence of several undertakings.

When determining minimum requirements, care should be taken that the chosen quality parameters correspond to those areas of influence. It is important not to burden undertakings with requirements that are outside the scope of their own domains. Requirements can only take effect on those parts of the network or terminal equipment over which undertakings have reasonably sufficient control.

In the end, the whole process leads to a set of quality parameters determining the overall quality of service. By defining specific target values, minimum quality requirements can be set for the allowed values, ranges or thresholds of the parameters.

However, setting end-to-end quality requirements for individual applications is not feasible on today's Internet due to its best effort nature. Furthermore, it is still subject to the general net neutrality debate whether application-specific traffic handling on the Internet is considered acceptable or not.

7.4 Step c) Analysis

This analysis step consists of crosschecking to what extent the selected minimum requirements address the desired effects, i.e. by reducing or eliminating the quality degradations. As there will usually be more than one possible set of minimum quality requirements (ref. the previous section), the different options (which may also be combined) should be tested according to the principle of proportionality.

Note that at this point it is assumed that the decision to set such requirements has already been taken according to the trigger detection procedure described in chapter 6. The task now, at the concluding step of the requirements determination procedure, is to analyse the effect that the requirements will have on the degradations in the light of the regulatory objectives to be achieved.

As described in chapter 3, what has to be scrutinized by the NRAs in this regard is the effect of the providers' traffic management practices. This needs to be done in the contexts of safeguarding applications that depend on the quality of the underlying network, prevention of consumer harm, and prevention of discriminatory behaviour that restricts competition.[46]

The analysis of these aspects depends on the nature of the degradations that triggered the imposition of the quality requirements. The triggers can be categorized into degradation of the performance of the whole electronic communications service and/or degradation of specific applications.

Minimum quality requirements aiming at prevention of degradation of the whole communications service will typically address prevention of consumer harm and/or prevention of discriminatory behaviour. To be really effective such requirements should, if possible, take into account the interconnection leg as well as the access leg because of the interconnected nature of the Internet.

Minimum quality requirements aimed at prevention of degradation of specific applications will directly address the safeguarding of applications that depend on the quality of the underlying network. But they will also indirectly address prevention of consumer harm, negative impact

[46] Ref. Recital 34 of Directive 2009/136/EC

on innovation and/or prevention of discriminatory behaviour regarding the use of specific applications.

The notification procedure prescribed by USD article 22(3) includes provision to the Commission and to BEREC of the envisaged minimum quality requirements, along with the grounds for action. The response from the Commission will in particular be targeted at ensuring the envisaged requirements do not adversely affect the functioning of the internal market.

The detailed assessment of the different types of minimum quality requirements foreseen by this report and possible role for BEREC during the notification procedure will be handled in the follow-up work stream “Guidelines on quality of service in the scope of net neutrality”. These guidelines will, among others, use tests of proportionality to analyse the effects of different requirements under different scenarios.

8. How to assess the fulfilment of the requirements?

As with the need to verify the information on transparency provisions, submitted by the providers, there is a similar need to assess the fulfilment of any minimum quality requirements imposed on them. This assessment will typically use a similar three-step procedure a) preparation, b) quality evaluation and c) analysis of results, as introduced in the general evaluation procedure in chapter 5.

Step a) Preparation

In this assessment phase, a clearer situation has been reached than what was discussed in chapters 6 and 7. The degradation classified as “a trigger” is identified (chapter 6), and the minimum quality requirements are determined (chapter 7). Once these requirements have been imposed on the providers and have been working for a period, it is time to assess their effects on the providers’ services.

The parameters that need to be checked will now typically be the same as were considered during the previous phases in which the requirements were determined. In many cases the same quality evaluation platform may be used, as this platform may have been maintained to follow up the development on a more or less permanent basis.

Step b) Quality evaluation

The quality evaluation will now be performed along the same lines as for the trigger detection process of chapter 6 and requirement determination process of chapter 7. The details of the quality measurement methods are further elaborated in chapter 5.

If the requirements are based on a technical result-based approach, this quality evaluation will be straight forward. If on the other hand they are based on a functional approach, the process will be more complex. The process will then be relatively open, as the exact parameters to be measured may not be self-evident, and more comprehensive, as the development of the whole market may need to be investigated.

Step c) Analysis of results

This step will analyze the real world effects of any minimum quality requirements imposed on the providers, in contrast to the analysis performed in section 7.4 which adopted a relatively theoretical approach before the requirements had been imposed.

As a result of the analysis of the providers’ fulfilment of the imposed minimum quality requirements, the NRA may conclude that the situation is satisfactory, or the result may be that further requirements need to be considered. In the latter case, another requirement determination phase could be initiated in order to decide on adjusted minimum quality requirements.

Another possibility is that the requirements may be removed at this stage if they are no longer considered necessary. In that case, a procedure along the same lines as the trigger detection phase could be initiated, in order to draw the conclusion to *not* set any minimum quality requirements.

9. Findings and next steps

Having studied the different aspects of the minimum quality requirement regulatory remedy for USD article 22 (3), it becomes clear that interpretation of how to apply this provision has many facets. The BEREC work on QoS in a net neutrality context is divided into two projects consisting of this report which presents a framework for interpretation plus a follow-up guidelines document that expands on this with concrete recommendations.

It may however turn out that competition in the market, along with the provisions on transparency, among others, will make actual enforcement of article 22 (3) unnecessary. In any case, this safeguard article can serve as a useful tool working to prevent degraded network performance (e.g. by ensuring the usability of the Internet access service compared to specialized service offers).

The focus of this report is on the quality aspects of the Internet access service, since it does not appear necessary to consider the application of minimum quality requirements to specialized services. Specialized services intrinsically contain detailed contractual conditions relating to the quality of the service provisioning.

The enforcement of USD article 22 (3) is divided into two main phases:
- What conditions could trigger the imposition of minimum quality requirements?
- And then, how could the minimum quality requirements themselves be determined?

Finding 1: The focus is on the quality conditions of the Internet access service, since it does not appear necessary to consider the application of minimum quality requirements to specialized services.

Detection of trigger situations

During the comprehensive procedure that must be conducted by the NRA prior to setting minimum quality requirements on one or more providers, the task of monitoring the evolution of electronic communications services and detecting triggers as described in chapter 6, must first be addressed.

The trigger detection phase is itself subdivided into three steps: a) Preparation b) Quality evaluation and c) Analysis of results. In this report BEREC identifies alternative approaches for each of these steps, and it thus provides a basis for the guidelines document to further elaborate on the advantages and disadvantages of each option and to draw conclusions on their relative preferences.

National specificities and priorities may lead to different practical solutions on how to handle the two first steps, as these processes will not have to be aligned among member states. On the other hand, the last step that consists of analysis of the situation and where conclusions are drawn as to whether or not a “trigger situation” has been detected, will to a large extent need to be approached from a common basis in order to conform to uniform European market conditions.

During the “Preparation” step, two main alternatives could be envisaged: a reactive and a proactive approach. If choosing the reactive approach, NRAs will base their actions mainly on indications and symptoms reported by different stakeholders, including end users. If choosing the proactive approach, the NRAs will instead monitor developments themselves. A combination of both approaches is of course also an alternative.

As the indicators identified during the first step may be uncertain or even subjective, there will usually be a need for a second step, the "Quality evaluation" step, to verify impressions gained during the first step. In order to detect potential throttling or blocking, a suitable parameter to monitor could for example consist of the complaints received. Alternatively, more technical parameters like Internet access throughput or performance of individual applications could be used.

The last step of the trigger detection procedure is the "Analysis of results" which will lead to a conclusion regarding whether a need exists for NRAs to intervene and set minimum quality requirements, or not. This step may need further co-ordination at the European level, but below general considerations regarding how to analyze during this step are summarized.

The aim of imposing minimum quality requirements is to prevent "degradation of service" etc. Frequent occurrence of degradation of the general Internet electronic communications service or hindering (blocking) or slowing down (throttling) of traffic from individual applications are of particular concern. These situations may in many cases have been detected in the preceding quality evaluation step.

The different considerations to look into during the analysis step can be categorized on the basis of two characteristics: whether the market as a whole or a single provider is subject to analysis, and whether degradation of the whole electronic communications service or degradation of specific applications is being considered. This can be organized into a table to give an overview of the different options (but the cells of the table must not be interpreted as completely isolated, as some aspects from one cell may also be applicable to neighbouring cells).

	Degradation of performance of the Internet access service	***Degradation of individual applications***
Market as a whole	• *Compare with the performance of specialized services* • *Compare with currently available technology*	• *Consider availability of unrestricted Internet access compared to restricted offers* • *Consider the actual penetration of unrestricted Internet access compared to restricted offers*
Individual ISPs	• *Compare with other ISPs' offers* • *Compare with advertised speed*	• *Blocking/throttling of one or more specific applications* • *Restrictions based on source and/or destination*

The outcome of the analysis step is a decision on whether or not the current situation is so severe that intervention by NRAs is necessary. This scrutiny of the effect of the providers' traffic management practices should look into the need to safeguard applications that depend on the underlying network's quality, prevention of consumer harm and prevention of discriminatory behaviour restricting competition.

Safeguarding applications could typically be considered necessary in cases when applications are throttled and/or blocked. Prevention of consumer harm and/or prevention of discrimination could typically be considered necessary both in cases of degradation of the electronic communications service as a whole and in cases of differentiated treatment of individual applications.

Further work will be necessary in order to develop detailed recommendations regarding the different aspects indicated in the table above, and evaluation of this will take place during the BEREC work streams on “Guidelines on quality of service in the scope of net neutrality” and “Competition issues related to net neutrality”.

Finding 2:

Degradation of performance of the Internet access service could be analyzed by

- ***comparing it with the performance of specialized services***
- ***comparing it to the currently available technology***
- ***making comparisons between ISPs’ offers***
- ***comparing actual with advertised speed***
- ***monitoring development over time***

Degradation of individual applications could be analyzed by considering

- ***availability of unrestricted Internet access compared to restricted offers***
- ***penetration of unrestricted Internet access compared to restricted offers***
- ***blocking/throttling of one or more specific applications***
- ***restrictions based on source and/or destination***

Finding 3:

The need to impose minimum quality requirements should be analyzed by the NRA through the scrutiny of the effect of the providers’ traffic management practices. This can be achieved by studying the need to safeguard applications that depend on the quality of the underlying network, prevention of consumer harm, and prevention of discriminatory behaviour restricting competition.

More detailed recommendations regarding this should be subject to further work by BEREC during 2012.

Determination of quality requirements

If the outcome of the trigger detection phase is that minimum quality requirements need to be imposed by an NRA, the next question is to look into how to determine these requirements. First of all, the requirements must address the degradation situation that is triggering the use of this regulatory remedy. Furthermore the proposed requirements should be tested regarding the principle of proportionality.

Again, this second phase of the quality of service remedy is also subdivided into three steps: a) Preparation, b) Quality evaluation and c) Analysis. The “Preparation” step is based on the previous phase where the triggers have been identified, while the specific findings that have caused the decision to impose requirements are typical candidates to be considered.

The results from this first preparatory step should identify the specific quality issues to be addressed by the next “Quality evaluation” step. The quality issues will typically be of two different categories: the performance of the Internet access service as a whole and/or the performance of individual applications using the access.

The potential individual quality requirements can furthermore be categorized into three different levels: functional, general technical and detailed technical requirements. The table below summarizes the foreseen potential individual quality requirements, based on this categorization.

	Quality req. regarding performance of the Internet access service	***Quality req. regarding individual applications***
Functional requirements	• *Application agnostic congestion management (ensuring usability of individual applications)* • *Performance compared to advertised speed (*qualitative *approach)*	• *Prohibition of blocking and/or throttling of individual applications* • Qualitative *requirements on application performance*
Technical requirements	*General tech. requirements* • *Prescribed typical or minimum actual speed (*quantitative *approach)* • *Included aspects of interconnection leg in addition to access leg*	*Detailed tech. requirements* • *Quality requirements including characteristics of individual applications (where feasible on today's best effort Internet.)*

The purpose of the quality evaluation step is to relate the requirements that are to be determined to the current network performance, in order to reduce or prevent degradation. The comprehensiveness of the technical measurements needed for this step will vary from relatively low (functional requirements) to relatively high (detailed technical requirements). The performance of current networks and services will give indications on how to estimate the improvements to be targeted by the requirements.

The "Analysis" step will probably be performed more or less in parallel with the quality evaluation. During this third step, an analysis will be made of the extent to which different requirements may contribute to "preventing the degradation of service and the hindering or slowing down of traffic over networks", seen in the light of the relevant regulatory objectives to be achieved.

At this step it is assumed that the decision to set minimum quality requirements has already been taken, so the question now has to do with the kind of requirements to impose. It is important that the selected requirements are effective when it comes to prevention of degradation. It is also important to be sure that the least intrusive requirements are used.

The notification procedure of USD article 22 (3) states that information about the proposed decision of the NRA shall be provided to the Commission and also be made available to BEREC. The NRA shall then take the utmost account of the Commission's comments or recommendations when finally deciding on the requirements. The purpose of this notification procedure is to avoid fragmentation of the internal market, and prior co-ordination at the European level could therefore reduce the need to adjust decisions retrospectively.

After the "Trigger detection" and "Requirement determination" phases have been conducted, the final decision taken by the NRA will come into play and should be allowed to operate for a period. After that, there will be a need for an additional assessment phase to look into the actual effect of the minimum quality requirements. This phase may lead to: no further action, new enhanced requirements or removal of the requirements.

In order to give detailed recommendation on the setting of specific minimum quality requirements in different scenarios, further work is needed. The usability of the different options indicated in the table above will be elaborated during the follow-up BEREC work stream on “Guidelines on quality of service in the scope of net neutrality”.

Finding 4:

Identified potential minimum quality requirements to prohibit degradation of the Internet access service may be:

Functional requirements such as

- ***Congestion management required to be mainly application agnostic***
- ***Access performance required to be comparable to advertised speed***
- ***Blocking and/or throttling of applications to be prohibited***
- ***Qualitative requirements to be placed on application performance***

Technical requirements such as

- ***Typical or minimum actual access speed to be required***
- ***Include aspects of interconnection leg in addition to access leg***
- ***Quality requirements to be applied to different applications (where feasible on today’s best effort Internet)***

Finding 5:

When potential minimum quality requirements are to be imposed by the NRA, they should be analyzed according to the principle proportionality.

More detailed recommendations regarding this should be subject to further work by BEREC during 2012.

Quality evaluation of the Internet service

The Internet electronic communications service can be challenging to handle from a quality perspective, due to its current best effort mode of operation. Controlling its performance is complicated for the providers, and it is also difficult to measure exact values of application performance over time. As a consequence, it may be complex to determine minimum quality requirements.

In this report BEREC has concluded that, as a technical concept, “network performance” is the best approach for determination of the “quality” of an electronic communications service. The *technical* concept “quality of service” also includes performance of the user equipment which usually lies outside the control of the providers. However, the “quality of experience” perceived by the end users is the ultimate goal.

Internet is the main target of the quality concerns, and the decoupling of the Internet application layer from its network layer is the main cause of this limited control from the providers’ side. At the same time the network performance of the underlying electronic communications service provided by the ISPs is the foundation upon which the performance of the different applications is built.

The interconnected nature of the Internet makes this underlying communications service a distributed responsibility of the individual ISPs that provide the overall service. The interconnection agreements used on the Internet today are without quality guarantees.

However, the capacity provided at the interconnection points determines the ultimate quality of the communications passing through them.

These limitations, decoupling of applications from the network and distributed responsibility for the network performance, makes the use of statistical methods essential to the measurement of network performance. Through long term monitoring of performance, the quality may therefore be measured with a limited degree of certainty.

However, quality evaluation of Internet electronic communication service is currently based mostly on measurement of only the "access leg". This gives an indication of the quality of the Internet access service provided by the ISP, but it does not take into account the interconnection of this ISP to the rest of the Internet, which actually is included in the "product" sold to the end users. For this reason, there is a need to improve the quality evaluation methods to include "interconnection legs" of the Internet.

Increased effort should be put into the promotion of the difficult task of evaluating the quality of the Internet service. One way of achieving this goal is to look into the possibility of achieving a common acknowledged quality evaluation platform.

Finding 6: Decoupling of applications from the network layer and distributed responsibility for the network capacity, makes the use of statistical methods to measure performance of the Internet electronic communication service essential. Increased effort should be put into the promotion of quality evaluation platforms, and the possibility to achieve a common acknowledged platform should be further explored by BEREC during 2012.

Quality of service and net neutrality

Finally, there is a need to evaluate whether the regulatory objective of "*promoting the ability of end-users to access and distribute information or run applications and services of their choice*" is achieved or not. The traditional regulatory remedies including the enhanced transparency requirements should in most cases be sufficient. However, in some cases it may be necessary to use the option to set minimum quality requirements.

That quality requirement remedy is provided in order to prevent "*degradation of service and the hindering or slowing down of traffic over networks*". Such network behaviour based on the providers' traffic management practices should be evaluated by the NRA according to whether they represent discriminatory behaviour restricting competition, their effect on applications that depend on the network performing at a minimum quality standard and finally restrictions on end users ability to run applications they want.[47]

More specific recommendations and guidelines on this evaluation will be elaborated in the follow-up "Guidelines on quality of service in the scope of net neutrality" work stream. This work will build on the general framework presented in this document regarding direct effect on applications and the effect this will have on end users. It will also build on the work stream "Competition issues related to Net Neutrality" particularly regarding discrimination issues.

Finding 7: Finally, there is a need to evaluate whether the regulatory objective of "promoting the ability of end-users to access and distribute information or run applications and services of their choice" is achieved or not. This should be subject to further work by BEREC during 2012.

[47] Recital 28 and 34 of Directive 2009/136/EC