Body of European Regulators for Electronic Communications

BEREC

BoR (12) 32

BEREC
Guidelines for Quality of Service in the scope of Net Neutrality

Draft for public consultation

29 May 2012

Table of Contents

1. Executive summary

Background and scope

The increasing importance of electronic communications in general, and the Internet in particular, has spurred the public debate on the open Internet and net neutrality. In the revised European regulatory framework which was approved in 2009, it was explicitly recognised that NRAs should promote the interests of the citizens by, *inter alia*, "*promoting the ability of end-users to access and distribute information or run applications and services of their choice*" (Art. 8(4)(g) Framework Directive).

NRAs are equipped with regulatory tools such as the promotion of competition and enhanced transparency requirements to reach this objective. Furthermore, the revised regulatory framework introduces the competence of NRAs to set minimum Quality of Service (QoS) requirements in order to prevent degradation of service (Art. 22(3) of the Universal Service Directive (USD)). This raises many questions that are discussed in these guidelines: What is the scope and extent of this competence? What purpose does it serve? What is quality of service? What is degradation according to this provision? What considerations are relevant in deciding whether intervention is deemed necessary?

When considering whether to use the minimum QoS powers, NRAs must also consider whether it would be more appropriate and proportionate to use alternative regulatory tools. If traditional competition tools, the enhanced transparency requirements and other relevant tools of the regulatory framework are insufficient to address degradation of service, NRAs may however impose minimum QoS requirements on ISPs.

The strict technical definition of QoS includes parameters which go beyond the control of the ISP. It is therefore necessary to use the concept of "network performance" which can be used for the measurement of the quality of sections of the network. Degradation of network performance of IP-based networks may be due to general congestion in the network or it may be caused by targeted traffic management, e.g. performing throttling or blocking of specific applications.

Regarding use of the transmission capacity over the end user's broadband connection, two kinds of services are provided: Internet access services and specialised services. Internet access services provide connection to the public Internet and thereby connectivity between end points connected to the Internet. Specialised services typically rely on access restrictions and extensive use of traffic management techniques.

Specialised services intrinsically offer contractual terms which ensure quality of the service provisioning. BEREC therefore considers that it should generally not be necessary to apply the Art. 22(3) USD minimum QoS requirements to specialised services. These guidelines consequently focus specifically on quality conditions of the Internet access service. However, in cases where the capacity of specialised services are provided at the expense of the Internet access service, specialised services will be of particular interest to NRAs.

Art. 22(3) USD says that NRAs may set minimum QoS requirements *"[i]n order to prevent the degradation of service and the hindering or slowing down of traffic over network*s". These BEREC guidelines do however not give straightforward answers, but provides guidance for

NRAs to assess the severity of a situation by considering the practice itself and also in the context of the market. When it comes to defining what is reasonable or unreasonable practice by an ISP, and whether an NRA should intervene by imposing minimum QoS requirements, the guidelines provide several criteria of assessment which enable NRAs to perform a regulatory evaluation of the situation.

Main regulatory issues related to QoS in the context of NN

A precondition for a competitive and transparent market is that end users are fully aware of the actual terms of the services offered. They therefore need appropriate means or tools to monitor the Internet access services, enabling them to know the quality of their services and also to detect potential degradations.

Furthermore, NRAs will supervise the development of the market, either proactively or reactively. With the proactive approach, NRAs will monitor the development of the quality of the Internet access service over time. With the reactive approach, NRAs may initiate monitoring on an ad hoc basis, for example when a potential incident is reported by a stakeholder.

BEREC has identified two main categories of degradation of service:

(1) the Internet access service considered as a whole and
(2) individual applications using Internet access service.

In the first category, the quality of the Internet access service would typically be compared to specialised services, and the question would be whether the specialised services were prioritised at the expense of Internet access services. In the second category we typically find cases of differentiation of traffic within the Internet access services, like VoIP blocking, P2P throttling and prioritisation of traffic from specific content and application providers.

When evaluating cases of the first category in particular, the distinction between Internet access services and specialised services is essential. For the purpose of these guidelines, BEREC provides the following definitions of basic concepts:

> *Internet*
> *The Internet is the public electronic communications network of networks that use the Internet Protocol for communication with endpoints reachable, directly or through network address translation, via a globally unique Internet address.*
>
> *Internet access service*
> *An Internet access service is a publicly available electronic communications service that provides connectivity to the Internet.*
>
> *In principle, an Internet access service allows for reachability between all end points connected to the Internet without any form of restriction to the content exchanged. It enables end users to run any application utilising the electronic communication function of the Internet.*
>
> *Furthermore,* unrestricted *Internet access service is defined based on the definition above and the only deviation allowed is the use of reasonable traffic management. If there is any deviation beyond reasonable traffic management, this is defined as a* restricted *Internet access service.*
>
> *Specialised services*
> *Specialised services are electronic communications services that are provided using the Internet Protocol and operated within closed electronic communications networks. These networks rely on admission control and they are often optimised for specific*

applications based on extensive use of traffic management in order to ensure adequate service characteristics.

If the services are provided as vertically integrated services, the specialised service only encompasses the underlying electronic communications service component, and excludes the application layer. Specialised services may interwork with the electronic communication on the Internet through gateways executing the admission control function.

Degradation of the Internet access service as a whole

In order to identify cases of degradation of Internet access service (IAS) as a whole, it is necessary to monitor the service quality, either proactively or reactively. Monitoring can be done by checking the contracts and terms of available IAS offers or by performing technical measurements of the IAS services themselves. Statistical methods are indispensable during technical measurements because of the varying characteristics of today's best effort Internet communications.

Today, quality measurements of the Internet access service are mainly performed for the access leg, and detection of degradation of the service should preferably also include the interconnection leg. Gathering statistical data using a distributed set of measurement servers would give indications of the performance of the electronic communication service beyond the access leg.

Monitoring should include a range of quality parameters: actual vs. advertised speeds, measurements of timing parameters (e.g. latency or jitter), level of congestion in the network, performance of IAS compared to specialised services, quality as perceived by end users, and IAS offers on the retail market (e.g. availability and penetration).

Following a common European approach will contribute to ensuring a consistent implementation of the regulatory framework. A harmonised set of measurement parameters and methods could be ensured through current or enhanced recommendations from standardisation bodies. Common measurement tools and platforms could also be achieved through participation in existing or new initiatives which seek to have a broad coverage of the Internet infrastructure.

Once information is gathered on the quality of Internet access services, an assessment of the situation at the market level need to be conducted. Causes for concern will be identified by comparing several aspects at the national level (e.g. comparison between IAS and specialised services, between packages, ISPs or categories of end user), or comparison between countries.

Issues regarding individual applications on the Internet access

When considering cases of differentiated traffic handling that occurs *within* the Internet access service, for example through throttling or blocking of individual applications, traffic management practices come into focus. Furthermore will congestion management and the protection of network security and integrity be of special interest.

Traffic management mechanisms are used by ISPs to optimise the flow of traffic within their networks. Traffic management can be used to implement both restricting measures (like blocking and throttling) and enabling measures (like routing and traffic forwarding). BEREC uses the concept "traffic management" in a broad sense and includes both technically implemented measures and measures that are not (yet) technically implemented but for example contractually regulated.

Congestion: IP networks can smooth short time traffic peaks by queuing IP packets in routers. Congestion is the situation met in IP networks when traffic increases to a level where routers run out of buffer space and are forced to start dropping some IP packets. By default, this is done randomly. Congestion in IP networks can occur caused by unpredictable/unavoidable situations or caused by a failure of the ISP to provide sufficient capacity.

Network security and integrity is protection against external or internal caused malfunctioning. Network security consists of measures to prevent and monitor unauthorised access, misuse, modification, or denial of networks and network-accessible resources. Network integrity consists of measures to maintain or restore the level of performance during network failures, and mitigation or prevention of network failures.

Again, as a first step, NRAs can take a reactive or proactive approach. In the former case, relevant cases can arise from complaints from stakeholders (including end users), and in the latter case NRAs would actively monitor Internet access services offered in the market.

NRAs will then need to assess whether reported incidents really constitute a "degradation of service". Blocking is relatively easy to verify since this means that the application is not working at all. Throttling incidents will need more detailed measurements in order to distinguish targeted application-specific measures from natural causes of low network performance. In the case of prioritisation of some applications, it will be necessary to evaluate whether this actually results in degradation in the performance of *other* applications.

NRAs will need to take into account which ISP is responsible for the traffic management practice in question, and what its purpose is. Legal obligations regarding the ISP as well as actions controlled by the end user lie outside the control of the ISP, and will often be considered reasonable measures. When it comes to congestion management, this is needed in IP networks, but ISPs should not "misuse" this as a reason to degrade specific applications when application-agnostic methods exist. Maintaining network security and integrity is also necessary, but this should not go beyond the actual need.

Complex situations may arise in the case of differentiated Internet access service offers, e.g. implementation of traffic classes on the Internet access service. In order to evaluate such a situation it may be necessary to compare different traffic classes and assess whether a prioritised class would actually result in the degradation of non-prioritised classes.

As well as assessing the effect of the traffic management practice itself, there is also a need to assess the practice at the market level. It is useful to consider the number of end users affected by the degradation and how easy it is to switch to unrestricted IAS offers. Extensive use of unreasonable traffic management practices leading to widespread restricted Internet access service offers in the market would indicate a situation of degradation.

The assessment procedures outlined in these guidelines do not specify explicit thresholds for when an NRA should intervene, but the more of the criteria that are met, the more serious the situation will be. In the case of restricted access to individual applications, the network effect means that *unrestricted* end users are also affected by the number of restricted users, since they are not able to use the relevant applications to communicate with them.

Determining the regulatory intervention

In situations where regulatory intervention is deemed necessary as a result of the degradation of the Internet access service, the NRA will choose between available regulatory

tools. If market mechanisms do not allow for easy switching to adequate alternatives, fostering competition and promoting ease of switching may be a sufficient response. If offers with adequate quality are still not easily available, it may be appropriate to consider imposing minimum QoS requirements.

Proportionality is one of the general legal principles guiding NRAs when using the minimum QoS requirements tool, consisting of different subtests: effectiveness, necessity and proportionality stricto sensu. Effectiveness requires that the minimum QoS are likely to remove or reduce degradation of Internet access service offers. Necessity suggests that other regulatory tools have been considered and deemed insufficient. Proportionality stricto sensu implies limiting the requirements to the adequate scope, e.g. relevant ISPs, and that the obligation imposed by the requirement is in proportion to the pursued aim.

The wording of Art. 22(3) USD says that "*in order to prevent the degradation of service*" NRAs may set minimum QoS requirements on ISPs. This indicates that when a situation of degradation pursuant to this provision is identified through the comprehensive regulatory procedure, the goal of the requirements is to prevent this degradation. The basic approach to this would be to require the ISP to improve the service quality until the degradation is eliminated.

In the category of degradation of the IAS as a whole, an example could be that the ISP is providing specialised services at the expense of the IAS. Then an NRA could consider requiring a certain performance level of the access speed, which varies over time, but e.g. using statistical mean value would compensate for the statistical variation.

In the category of degradation of individual applications using IAS, a relatively likely case would be blocking and/or throttling of single applications. Then an adequate requirement could be to prohibit restrictions of the relevant application(s). In some cases an NRA may also consider it relevant to prohibit application-specific restrictions on a general basis.

If minimum QoS requirements are to be imposed on ISPs, the NRA will notify the Commission informing about the draft measures, and also make the information available to BEREC. After taking the utmost account of any comments or recommendations of the Commission, the NRA may make a final decision imposing minimum QoS requirements.

1.1 Questions for the public consultation of the guidelines

Respondents are welcome to address any part of these draft BEREC guidelines for Quality of Service in the scope of net neutrality. BEREC is in particular seeking feedback on the regulatory aspects elaborated in chapters 4, 5 and 6.

What are your views on:

1. The criteria proposed for the assessment of degradation of Internet access service as a whole? (Ref. chapter 4)
2. The criteria proposed for the assessment of issues regarding individual applications run over the Internet access service? (Ref. chapter 5)
3. The aspects proposed regarding the conditions and process for regulatory intervention? (Ref. chapter 6)
4. To what extent are the scenarios described in these guidelines relevant with respect to your concerns/experience? Are there additional scenarios that you would suggest to be considered?

2. Background and scope

These Guidelines on Quality of Service in the scope of Net Neutrality follow on from the BEREC Framework for Quality of Service in the scope of Net Neutrality[1], published in December 2011 (henceforth referred to as BEREC's NN QoS framework). The BEREC NN QoS framework was used as a basis for the development of these guidelines for NRAs.

The European legislator, and subsequently (once transposed) the Member States' legislatures, have given NRAs the authority to ensure Quality of Service (QoS) when deemed necessary, under Article 22(3) USD. Although short, this sentence already raises many questions with regard to the background and applicability of the legal framework from which this power is derived:

1. What is the scope and extent of this authority?
2. What purpose does it serve?
3. What is quality of service?
4. What is degradation according to this provision?
5. What considerations are relevant in deciding whether intervention is deemed necessary?

It is necessary to answer the first three questions in order to understand the playing field on which NRAs, market players, end users, and other stakeholders find themselves. This chapter will be a first exploration on these questions, providing a basis from which the following chapters can explore the last two questions, among other issues.

In this chapter, to answer the questions presented above, BEREC will first set out the legal framework. Then the main technical aspects to take into account will be briefly reviewed. BEREC will also look at current and future business models in relation to quality of service. Finally, an overview of past, current and future BEREC projects which are closely related to this document is given.

In chapter 3, the main regulatory aspects of QoS are expanded on, including a process for NRAs to follow. Chapter 4 and 5 then investigates the two different categories of cases to be evaluated by NRAs. Chapter 6 sets out the determination of regulatory intervention, while chapter 7 provides guidance on the notification procedure.

2.1 Legal framework

At the time of writing, national legislation empowering NRAs to use minimum quality of service regulation has taken, or is taking, form across Member States. This legislation itself derives from article 22(3) of the Universal Service Directive[2] (USD), which in turn was introduced by the Citizens' Rights Directive[3]. The EU Framework also provides other tools with which NRAs can pursue their regulatory objectives, and these guidelines will also consider these other tools.

[1] http://berec.europa.eu/doc/berec/bor/bor11_53_qualityservice.pdf
[2] DIRECTIVE 2002/22/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (hereinafter: Universal Service Directive).
[3] DIRECTIVE 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (hereinafter: Citizens' Rights Directive).

Understanding the European legislator's intentions in the legislation is a first step in understanding the scope and goals of the regulation. Therefore, before analysing the regulatory tools at NRAs' disposal, BEREC will first explore relevant passages of the Framework Directive[4] (FD), which provide guidance by setting out some of the objectives to be pursued.

2.1.1 Framework Directive

Net neutrality is a subject in which content and carrier are inherently linked to each other. But as mentioned by the European legislator, the framework covering transmission[5] does not cover the content of services delivered over electronic communication networks using electronic communication services[6]. So, in principle, both areas have their separate regulatory basis.

However, this does not mean that the legislator rejects the idea that carrier and content are indeed connected: "*The separation between the regulation of transmission and the regulation of content does not prejudice the taking into account of the links existing between them, in particular in order to guarantee media pluralism, cultural diversity and consumer protection*."[7]

In this respect it is first important to draw attention to the policy objectives in the Framework Directive, which provide guidance for how the provisions in the four specific Directives[8] of the electronic communications regulatory framework should be understood. Specifically, we are concerned with three overarching goals set out in article 8 of the Directive, some of which were adjusted (Art. 8(2)(b) FD) or added (Art. 8(4)(g) FD) by the Better Regulation Directive[9]:

- To achieve the overarching objective of guaranteeing access to content for the interest of the citizens of the European Union: "*promoting the ability of end-users to access and distribute information or run applications and services of their choice*" (Art. 8(4)(g) FD);

- To ensure that electronic communications networks run smoothly, in other words to guarantee a satisfactory quality of service; this is covered by traditional objectives falling on NRAs, notably: "*ensuring that the integrity and security of public communication networks are maintained*" (Art. 8(4)(f) FD) and "*encouraging (…) and the interoperability of pan-European services, and end-to-end connectivity*" (Art. 8(3)(g) FD). The new power to set minimum quality of service requirements (see 2.1.2 below) may also be viewed in this light;

[4] DIRECTIVE 2002/21/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 7 March 2002 on a common regulatory framework for electronic communications networks and services (hereinafter: Framework Directive).
[5] Regulatory framework: Framework Directive; Universal Service Directive; DIRECTIVE 2002/20/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive); DIRECTIVE 2002/19/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive); DIRECTIVE 97/66/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector. (Hereinafter: Directive on privacy and electronic communications).
[6] Framework Directive, recital (5), more specifically: *"This framework does not therefore cover the content of services delivered over electronic communications networks using electronic communications services, such as broadcasting content, financial services and certain information society services, and is therefore without prejudice to measures taken at Community or national level in respect of such services, in compliance with Community law, in order to promote cultural and linguistic diversity and to ensure the defence of media pluralism"*.
[7] Id. 6
[8] These are the aforementioned: Universal Service Directive; Authorisation Directive; Access Directive; Directive on privacy and electronic communications
[9] DIRECTIVE 2009/140/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services (hereinafter: Better Regulation Directive).

- To enable the long-term development if the networks and services thanks to innovation and the development of the most efficient technical and business models; competition plays a fundamental role here, hence the importance of NRAs' objective of "*ensuring that there is no distortion or restriction of competition in the electronic communications sector, including the transmission of content*" (Art. 8(2)(b) FD).

While drawing on these goals we should acknowledge their nature - as policy objectives, they provide valuable guidance but they do not in themselves constitute a direct ground for intervention, nor are they absolute concepts on which to base any actions.

That said, access to content is an objective which is interlinked with relevant parts of the electronic communications regulatory framework. As content is being made available through networks, there is the inevitable link mentioned at the start of this section between the regulation of transmission and the regulation of content, referred to in recital (5) of the Framework Directive. So, without prejudice to the eventual outcome of a careful and balanced consideration of interests, BEREC does recognise the idea that, according to article 8(2)(b) FD, NRAs shall ensure that *there is no distortion or restriction of competition in the electronic communications sector, including the transmission of content*, as part of the interests at stake.

The ability to regulate content is also contingent on it being accessible, which links with the article 8(4)(g) FD objective of "*promoting the ability of end-users to access and distribute information or run applications and services of their choice*". The objectives pursued by content regulation are of a general interest nature, such as: "*freedom of expression, media pluralism, impartiality, cultural and linguistic diversity, social inclusion, consumer protection and the protection of minors*".[10] Again, these do not constitute absolute and final considerations, but should be taken in account when considering the objective in article 8(4)(g) FD.

These policy objectives therefore play a role in how NRAs approach their discretionary powers under article 22(3) USD: they will have to determine whether specific offers, or the combination of available offers, sufficiently serve the general interests mentioned in the recitals. Again, these are obviously not the only considerations to be taken in account. In fact these might be seen to contradict other notions of the regulatory framework, namely that the market is free to operate and, if there is no market failure, it can be expected that the market will deliver the outcomes set out in the policy objectives. However, in reality, there will be imperfections or failures in the market, hence the relevance of these objectives and the existence of article 22(3) USD and other tools.

2.1.2 Article 22(3) of the Universal Service Directive

In the revised USD, the legislator expanded on the aforementioned objectives set out in the Framework Directive, expressing the desire for end-users to be able to navigate over electronic networks and services, should they choose to do so: "*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*."[11]

In general, the legislator envisaged that in a healthy functioning market, and with sufficient transparency of the offers made available to end-users by market players, it can be expected

[10] Framework Directive, recital (6).
[11] Citizens' Rights Directive, recital (28).

that end-users will be able to enjoy the quality of service they desire.[12] Nonetheless there may be cases in which it may be necessary for NRAs to intervene: "*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*".[13]

The two policy objectives set out in these recitals are given force by article 22(3) USD, of which the most relevant part reads:

> *"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".*[14]

BEREC understands that the phrase "*an undertaking or undertakings*" means that an NRA has the discretion to decide whether to apply any necessary minimum QoS requirements to one, to several, or to all ISPs. NRAs will want to consider the following questions: if it is the conduct of only one or a few ISPs which has raised concerns, would it be fair to apply the requirements to all ISPs in a market? On the other hand, if requirements were only imposed on one (or several) ISPs, could this be seen as disproportionate, either due to the effect it could have on the one ISP, or if it had the effect of distorting the whole market?

Another issue to explore is the extent to which the provision suggests that quality of service does not pertain only to the end user's experience, but also includes the terms extended by ISPs to content and application providers (CAPs) for the routing of their traffic. Recital 34 of the Citizens Rights Directive[15] notably stipulates that traffic management practices should be subject to scrutiny by the NRA, "*acting in accordance with the Framework Directive and Specific Directives, and in particular by addressing discriminatory behaviour*".

These are issues which will be further examined in chapter 4.

It seems likely that NRAs will mainly be able to impose minimum QoS requirements after having identified an instance or a risk of degradation of service, or hindering or slowing down of traffic. As explained in 2.1.4 below, NRAs are bound to respect the principle of proportionality. In this respect, the imposition of QoS requirements can be considered as an intrusive remedy, and applying these kind of measures pre-emptively would require proving the seriousness of such problem or threat.

2.1.3 Other tools

When considering whether to use the minimum QoS powers in article 22(3) USD, NRAs must also consider whether it would be more appropriate, effective or proportionate to use alternative regulatory tools to achieve the three goals set out above. These additional tools can be divided into asymmetric and symmetric tools.

[12] Citizens' Rights Directive, recital (34).
[13] Id. 12.
[14] The full article includes safeguards for notification of measures to the Commission and BEREC: *"National regulatory authorities shall 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 the Body of European Regulators for Electronic Communications (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. National regulatory authorities shall take the utmost account of the Commission's comments or recommendations when deciding on the requirements".*
[15] Id. 12.

- **Asymmetric tools**

If discriminatory behaviour on the network layer against rival content and application providers become a recurrent feature of the market, NRAs should in principle be able to impose remedies (e.g., non-discrimination) on those providers identified as having significant market power. In particular, the current access regime potentially allows NRAs to impose remedies on ISPs on the basis of article 12 of the Access Directive (AD) (in combination with the 2009 extension of the definition of access in article 2 of the Access Directive).

In practice, there would be significant obstacles to using these remedies in this area. NRAs would have to define and analyse relevant markets, taking utmost account of the Commission Recommendation on relevant markets.[16] As this Recommendation covers neither retail broadband markets, nor an IP interconnection wholesale market, the three-criteria test would need to be fulfilled. This requires a substantial amount of information before deciding to undertake this process, and a high burden of proof if the tools are ultimately to be used.

The Framework does provide a comprehensive approach to identifying the relevant market fulfilled, the operator(s) which may have Significant Market Power (SMP) within that market, and to targeting appropriate remedies[17] However, the extensive timeframe involved in using this remedy may not be compatible with the fast-moving Internet markets. Furthermore, this tool would not be applicable to cases where the operator raising concerns did not have SMP in the relevant market.

In some countries, the provision of data communication services – on mobile and fixed networks – is at the moment characterised by an oligopolistic structure, especially at the wholesale level. The high burden of proof associated with the existence of a joint SMP may again deter NRAs from using this remedy.

Taking into account the Community as a whole, it is likely to often be the case that a multitude of areas (in particular rural regions) will lack suitable competitors for the carriage of any high-speed innovative service, so an existing carrier (and especially an ISP providing access) is in a powerful position. The regulatory principle in article 8(5)(e) FD mandates NRAs to take due account of the variety of conditions relating to competition and consumers that exist within the geographic areas within a Member State. NRAs could indeed take these variations in competitive conditions into account when identifying SMP in the markets mentioned above.

Furthermore, in those cases where ex-ante regulation is not considered appropriate, it always remains possible to rely on ex-post competition law, and in particular the prohibition on abuse of market power contained in Article 102 of the Treaty on the Functioning of the EU.

- **Symmetric tools**

Alongside these asymmetric tools for addressing anti-competitive forms of discrimination, the other provisions of the Framework relevant to Net Neutrality relate to:

- transparency requirements (USD);
- obligations to ensure end-to-end connectivity (AD); and
- dispute resolution (FD).

[16] http://ec.europa.eu/information_society/policy/ecomm/doc/library/proposals/rec_markets_en.pdf
[17] See the Polish case (IP traffic exchange) where the Commission decided that the market had not passed the three criteria test (PL/2009/1019-1020). See also ECJ- Case T-226/10

BEREC looked in detail at the new transparency requirements in articles 20(1)(b), 21(3)(c) and (d), 22(1) and 22(2) of the USD in its December 2011 Guidelines on Transparency in the scope of Net Neutrality: Best practices and recommended approaches[18].

- Article 20(1)(b) places obligations on ISPs to include in contracts with end users specific information covering, *inter alia*, traffic management policies and any limits to services or applications.
- Articles 21(3)(c) and (d) of the Universal Service Directive empower NRAs to impose a variety of information requirements on ISPs.
- Article 22(1) require the providers to publish comparable, adequate and up-to-date information for end users on the quality of their services
- Article 22(2) provides for a transparency obligation regarding quality of service.

Before deciding whether to use their power to impose minimum QoS requirements, NRAs will want to consider whether the EU Framework's transparency obligations are being effectively observed by ISPs. If improvements can be made in terms of transparency, this may complement, or negate the need for, using other regulatory tools.

NRAs can also impose **obligations to ensure end-to-end connectivity** provided by articles 4 and 5 of the Access Directive. The interconnection regime exists independently of any interconnection obligations imposed as a result of finding SMP on a market. The regime protects the integrity of the overall communications sector, by giving the possibility to intervene when end-to-end connectivity is at stake. Following the 2009 revision of the Access Directive, article 5(1) now explicitly mentions that NRAs are able to impose obligations "on undertakings that control access to end users to make their services interoperable".

Separately, the revised article 20 of the Framework Directive on **dispute resolution** now provides for the resolution of disputes between undertakings providing electronic communications networks or services and also between such undertakings and others that benefit from obligations of access and/or interconnection (with the definition of "access" also extended in Art. 2 AD as mentioned above). Dispute resolution cannot be considered as a straightforward tool for developing a regulatory policy, but it does provide the option to address some specific situations, maybe useful in more urgent cases. The potential outcome of disputes based on the transparency obligations can provide a "credible threat" for undertakings to behave in line with those obligations, since violation may trigger the imposition of minimum QoS requirements on an undertaking, in line with article 22(3) USD.

So, the Framework provides indications as to what objectives and ideas should be taken into consideration. Furthermore, it is clear that the revised regulatory framework provides NRAs with the authority to intervene, if appropriate. But what remains unclear is when it is appropriate to do so. The main goal of this document is to provide guidance to NRAs as to how to detect relevant problems, when it is appropriate to intervene, which regulatory tools to deploy, and to identify relevant indicators which will assist with any such interventions.

2.1.4 Proportionality

Following European legal doctrine, BEREC notes that any analysis of QoS requirements must respect the principle of proportionality - measures should be based on a fair assessment that properly balances the relevant interests. Regarding the policy objectives

[18] http://berec.europa.eu/doc/berec/bor/bor11_67_transparencyguide.pdf

mentioned above, the Framework Directive directly calls upon NRAs to operate inside the bounds of proportionality[19].

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, the proposed remedy could be more burdensome than strictly necessary. Likewise there should be a legitimate aim, with an objective justification.

As part of determining proportionality, authorities should usually assess whether the legitimate aim is correctly defined. In the context of the power to impose minimum QoS requirements, the legitimate aim is already extensively described in the regulatory framework. As long as an NRA does not overstep the bounds of these aims, there should not be any problem.

It would also be important, in terms of proportionality, for an NRA to explain how it would monitor and verify any proposed requirements it is imposing, as well as under which conditions, and during which timeframe, they might be lifted.

2.2 Technical aspects to consider

BEREC's NN QoS framework presented how BEREC understands and defines different concepts related to Quality of Service that are particularly relevant to an understanding of Art. 22(3) USD. It also made a first assessment of which aspects are considered to be subject to these new provisions.

2.2.1 The relationship between QoS, QoE and Network Performance

Revisions to the regulatory framework introduced the competence of NRAs to set minimum quality of service requirements in relation to electronic communications services "in order to prevent the degradation of service and the hindering or slowing down of traffic over networks". However, defining the quality of the Internet communication service is rather challenging. It is therefore essential to have a clear understanding of the relevant quality concepts.

Quality of Service (QoS) encompasses all aspects of the service from end to end (i.e. user-to-user or user-to-content). The technical ITU definition of QoS is 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 organisation. QoS is therefore a measure of the performance of a set of functions observable at the user-interface of the service, and measurements are an indication of the performance of a set of functions observable at the user-interface of the service.

Quality of Experience (QoE) additionally takes into account user expectation and context, and is defined as the overall acceptability of an application or service, as perceived subjectively by the end user. It includes the complete end-to-end system effects and may be influenced by user expectations and context, e.g. using Mean Opinion Scores (MOS). 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.

[19] Article 8(1) Framework Directive: *"Member States shall ensure that in carrying out the regulatory tasks specified in this Directive and the Specific Directives, the national regulatory authorities take all reasonable measures which are aimed at achieving the objectives set out in paragraphs 2, 3 and 4. Such measures shall be proportionate to those objectives"*.

Both QoS and QoE, from the broad end user service point of view, include many parameters which are beyond the control of the operator, such as the terminal equipment and local network (e.g. home network) – as opposed to the Internet access service he is delivering. In terms of article 22(3) of the USD, which relates to the practices of operators, it is therefore necessary to use a different concept – that of *Network Performance (NP)*. NP is the concept used for measurement of the performance of network sections, e.g. sections that are under the control of individual operators[20].

Degradation of network performance of IP-based networks may be due to general congestion in the network or it may be caused by targeted traffic management, e.g. 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.

For any further investigation on causes of quality degradation and identification of possible malfunctioning network or terminal elements, a more detailed analysis of the IP infrastructure is necessary. However, this may require access to the network(s) and/or terminals themselves, in order to perform specific diagnostic tests. This report elaborates on possible quality evaluation methods in IP-based networks in the following chapters.

2.2.2 Network and application layers

In the BEREC NN QoS framework report the two-layer model describing how content and applications relate to the underlying IP network was introduced. 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 reference 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).

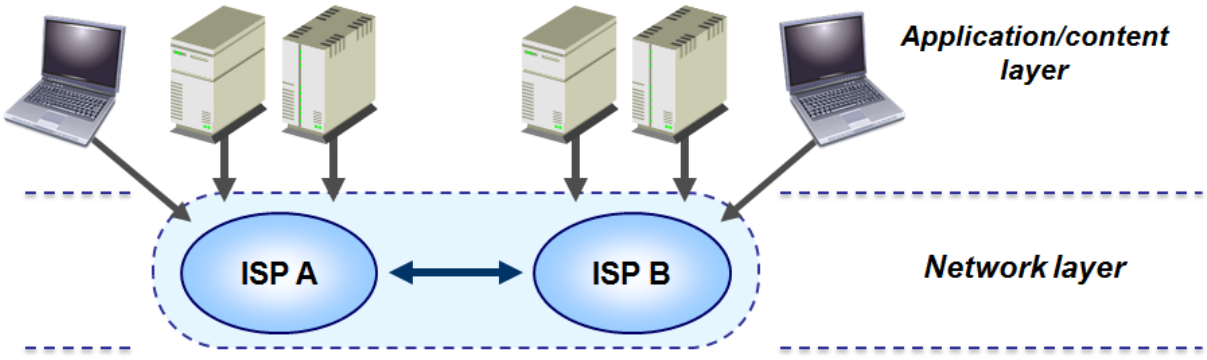

Figure 2.1 – The two-layer model

When running an application, the end user is making use of the electronic communication service at the *network layer*. The application software installed on the terminal equipment (also referred to as the host) executes functions at the *application/content layer* as indicated in figure 2.1. Applications (e.g. telephony, television and web) and content (e.g. videos and web pages) are produced in the endpoints which communicate with each other using the

[20] Note that the quality-related terminology used here is based on ITU recommendations (particularly ITU-T Recs. E.800, E.802 and Y.1540), and the Internet community uses a slightly different terminology.

underlying network layer. In these guidelines, the content/application layer is referred to simply as the *application layer*, while recognising that it actually contains both content and applications.

The net neutrality debate is fundamentally a question of whether transactions which take place at the application layer are independent from the underlying communication function at the network layer of the Internet. Of the two layers, net neutrality relates to the network layer. The electronic communications function should transfer the traffic independent of content and applications. This means that data received from the application layer should be forwarded in a neutral manner by the network layer.

2.2.3 Distinguishing between IAS and Specialised Services

The BEREC NN QoS framework report presented an initial study on the different categories of electronic communications services. Regarding use of the transmission capacity over the user's broadband connection, two categories of end user services are provided: Internet access services and specialised services.

An *Internet access service* (IAS) provides connection to the public Internet and thereby connectivity between end points connected to the Internet. The network performance of the Internet today has no guaranteed characteristics, which is why it is referred to as being best effort, without necessarily implying a low quality.

Specialised services are usually designed to provide guaranteed characteristics (e.g. end-to-end quality, availability and/or security). These characteristics are generally stated in contractual arrangements. Technically, specialised services typically rely on access restrictions and extensive use of traffic management techniques or strictly enforced capacity planning and provisioning.

A central distinction can be seen where capacity limits of a network are reached. In the case of specialised services, a customer's service requests may be rejected or alternatively they may trigger capacity extensions. Best effort networks, on the other hand, will still try to serve all customers' capacity requests, which would logically lead to a decrease in quality when the capacity limit of the network is reached.

Both the general Internet access service and specialised services can implement different traffic management techniques to achieve different levels of reliability. Specialised services are typically able to cover the whole range of guaranteed quality levels, while the open Internet may be less predictable, currently lacking guaranteed levels of performance.

Because specialised services intrinsically offer contractual terms ensuring quality of provision, BEREC considers that the application of minimum QoS requirements according to article 22(3) USD should generally not be necessary for those services. These guidelines therefore focus specifically on quality conditions of the Internet access service. However, in cases where the capacity of specialised services are provided at the expense of the Internet access service, specialised services will be of particular interest to NRAs.

Article 22(3) USD speaks about setting minimum QoS requirements on "*an undertaking or undertakings providing public communications networks*". Since these guidelines focus on Internet access services, they refer mainly to IAS instead of general electronic communications services, and also to ISPs (providers of IAS) instead of providers of public communications networks.

Based on the initial study of the relation between Internet access services and specialised services in the BEREC NN QoS framework, presented in the summary above, BEREC will in these NN QoS guidelines provide more detailed analysis of the two service categories. Definitions of fundamental concepts are presented in chapter 3, while specific concepts related to traffic management are elaborated in chapter 5.

2.3 Relevant market developments

2.3.1 Developments in data traffic and revenues

Internet traffic continues to increase, particularly in terms of mobile Internet access, but the rate of growth is declining.

Cisco estimates that global Internet traffic will increase by 39% in 2011, with the annual growth rate declining to 27% in 2015. For mobile data traffic, the rate of growth is much higher than for fixed, though this is partly explained by the fact that mobile starts from a significantly lower level – it accounts for around 2% of total IP traffic in 2011. The 2011 growth rate of mobile data traffic of 130% is expected to fall to 64% in 2015.

In terms of fixed Internet traffic, the growth is driven more by the increasing amounts of data being used by each subscriber than by the slowing increase in the number of subscribers[21]. The increase in subscriber numbers plays a more significant role in the growth of mobile data traffic. By the end of 2010 there were more than five billion mobile connections, a growth of 629 million in the year, and of the 1.28 billion mobile handsets sold during the year, 23% of them were smartphones, which are specifically designed for the use of mobile Internet applications[22].

It is not just the increase in connections which has driven the higher traffic. The increasing take-up of powerful mobile devices, the availability of fast mobile networks and the ever-growing availability of Internet content and applications (many of which are mobile-specific) means that consumers are downloading and uploading an increasing quantity of data. Smartphone use is growing rapidly: Vodafone reported that smartphones were responsible for 21% of all data traffic on its European networks in September 2011, compared with just 12% in March 2011[23] .

One should however refrain from drawing hasty conclusions from mobile data growth forecasts, which may often be exaggerated[24] and may be compensated, to a certain extent, by larger customer bases and lowering bandwidth costs. Especially when considering that although the overall data traffic is increasing, the growth rate of traffic is declining over time for fixed and mobile networks[25]. Furthermore, prices for transit and content delivery network services have decreased on a per unit basis as a result of decreases in equipment costs[26].

Some nevertheless argue that, at the same time, the revenues of operators are coming under pressure as a result of a range of market developments. . IDATE shows European telecoms revenues stabilising in 2012, after slight falls between 2009 and 2011, with

[21] WIK-Consult (2011), Ch. 2.5, similar Telegeography
[22] IDATE, *DigiWorld Yearbook 2011*
[23] http://www.vodafone.com/content/dam/vodafone/investors/financial_results_feeds/half_year_30september2011/p_halfyear2011.pdf
[24] "The collapse in the value if the mobile gigabyte: myth and reality" http://www.analysysmason.com/About-Us/News/Insight/Insight_collapse_value_GB_Jan2012/
[25] WIK Consult, Network operators and content providers: Who bears the cost?, September 2011
[26] WIK-Consult (2011), Ch. 2.3

continuing decreases in fixed telephony revenues being offset by continuing growth from mobile services, and data and Internet services[27].

Fixed-line voice revenues have long been in decline - mainly from substitution for mobile, but also increasingly from Voice over Internet Protocol (VoIP) telephony in some countries. Fixed broadband revenue growth is slowing as markets become saturated and the service becomes commoditised, Mobile revenues are coming under pressure as increasing data revenues struggle to offset the decline in voice revenues, In addition, SMS revenues are now under threat as some smartphones and applications like WhatsApp offer SMS over Internet Protocol (SMSoIP), enabling consumers to message each other without paying their operator to send SMSs.

While the rising demand for bandwidth has increased traffic and calls for investment in infrastructure, the stabilising revenues of operators threaten to act as a brake on investment. One way that operators have responded to these issues and dealt with the increasing traffic is by managing the traffic that passes through their networks. Another is through the emergence of new business models. In any event, mobile operators usually control both voice and data tariffs and can therefore restructure tariff plans and preserve their revenue.[28]

2.3.2 Emerging business models

ISPs employ a mix of business models across Europe. For example, some ISPs - particularly mobile operators - apply data caps to their tariffs as a way to manage traffic growth, while others have a flat-rate vision or make unlimited data access a selling point of their packages. This is to be considered along with the various solutions adopted by operators to offer Internet access services, in particular the many types of bundling with specialised services.

Some ISPs are using price differentiation based on providing some kind of added value, e.g. through providing faster broadband speeds or “gamer tariffs” which provide the required latency levels to ensure a good gaming experience. In the future, this may lead to other types of differentiation, where end users might be able to pay more for assured quality of service (e.g. for HD streaming) or for a less assured quality of service for end users who only use email and web-browsing. ISPs may also consider the best models to combine such options with the various possible ways for people to access the Internet (home, office, nomadism…).

In such a context of complexity, the ability for the end user to switch provider or tariff, and how easy this is, will be a key element when considering whether it is necessary to impose minimum QoS requirements.

ISPs are also interested in securing payment from content and application providers. Incentives for such behaviour, available options for ISPs, and potential impact on the markets are further explored in the BEREC report on competition issues related to Net Neutrality[29], currently under public consultation.

There is a separate question of how commercial and wholesale arrangements might impact on network performance. BEREC is looking separately at trends in the IP interconnection market in the context of net neutrality[30].

[27] IDATE, Le marché mondial des services télécoms 2008-2016, 22ème edition / M11301 – mars 2012
[28] "The future of mobile voice: scenarios for market evolution"
http://www.analysysmason.com/Research/Content/Reports/RRV07_future_mobile_voice_Sep2011/
[29] Draft BEREC report "Competition issues related to Net Neutrality"
[30] Draft BEREC report "IP interconnection in the context of Net Neutrality"

Also, it should be acknowledged that ISPs who purchase their access from wholesale providers are dependent on the networks of others and may have less control of how traffic is managed and on the ultimate quality of service delivered to their end users.

So far we have focused on issues regarding net neutrality that may arise as consequences of the behaviour of electronic communication services providers. However, the ability of end users to access and distribute information and run applications of their choice depends on the totality of the Internet chain, from content and application providers (e.g. search engines) to terminal manufacturers (e.g. smart phones and associated application platforms). The terminal manufacturers could for instance impede the installation of some software on the equipment they provide. In this respect, it is important to take into account the entire chain of stakeholders when monitoring the evolution of markets in general.

Content and application providers may also try to prioritise their data delivery. Without specific agreements with ISPs, they have a limited ability to perform this (despite some techniques available at the application layer). Indeed, due to the design and nature of IP technology, it is in practice the ISP who decides the flow of traffic in their networks. To overcome the problem of effective data distribution, a commercial strategy of large content providers can be to offer their content with better quality by bringing content servers closer to the end users.

This materialises in a comprehensive increase in the use of content delivery network (CDNs), leading to a more efficient aggregation of content in which independent CDN providers offer services to the content and application providers. CDNs as a principle do not raise net neutrality issues, but discriminatory treatment in their favour might well do so, especially since large content and application providers and CDN providers are usually present at both the application layer (which is where the servers belong) and at the network layer. These aspects are outside the scope of these guidelines but are studied in the separate BEREC draft report on *IP interconnection in the context of net neutrality*.

2.4 Main initiatives by public authorities

2.4.1 National legislation

In the Netherlands, specific legislation was proposed and approved by the Parliament in June 2011, and is scheduled for plenary debate in the Senate in May 2012. The proposal aims to prevent Internet service providers from hindering or slowing down end users' applications, as well as preventing price differentiation based on the applications used or offered via the Internet access service. Exceptions apply allowing measures aimed to manage network congestion or preserve security and integrity of the network, and to implement provisions in law or court orders.

2.4.2 Other BEREC projects

It is important to note that these guidelines have not been developed in isolation. Rather, they should be considered in the broader context of BEREC's other work focused on Net Neutrality – on transparency, traffic management practices, competition issues and IP interconnection.

Following its response to the European Commission's 2010 Open Internet consultation[31], BEREC launched several work streams in 2011.

[31] http://berec.europa.eu/doc/berec/bor_10_42.pdf

Of particular relevance to these guidelines was the *Framework for Quality of Service in the scope of to Net Neutrality*[32], which provided a conceptual basis for these Guidelines. The 2011 report evaluates and analyses quality-related concepts and quality-evaluation methods that are relevant to the new Framework provisions on minimum QoS requirements.

In 2011, BEREC also adopted *Guidelines on Transparency in the scope of Net Neutrality: Best practices and recommended approaches*[33], which explored how the new EU Framework transparency obligations would work in practice, and which are relevant in this document when considering transparency in relation to quality. The guidelines set out the type of information to be provided, how it should be conveyed, and which bodies should be involved. They also elaborated on the requirements for a transparency policy to be effective. In 2012, BEREC will hold discussions with stakeholders to understand how the transparency obligations are being implemented across Europe.

In December 2011, BEREC and the European Commission jointly launched *an investigation into the traffic management policies and practices* of fixed and mobile ISPs to better understand the commercial and / or technical practices used by providers across Europe. The preliminary findings[34] showed a great diversity of practices and methods of implementation, both within and between Member States – the most frequently reported traffic management practices being blocking and / or throttling of P2P traffic, on both fixed and mobile networks, and the blocking of VoIP traffic, mostly on mobile networks. A finalised "snapshot", providing further descriptions and quantitative information on the most frequent restrictions, was submitted to the Commission shortly before this consultation.

In parallel with this report, BEREC is consulting on a draft report on C*ompetition issues related to Net Neutrality*. The report looks at the effects of "differentiation practices" - such as traffic blocking/throttling or the prioritisation of traffic - and the circumstances in which these practices could have negative consequences for the level of competition and innovation or have a negative effect on the interests of end users.

Finally, BEREC is consulting on a draft report on *IP interconnection in the context of Net Neutrality*. The aim is to better understand the current IP interconnection agreements (peering/transit) between market parties and how these may affect net neutrality issues. This includes an assessment of competition and technological developments of the IP interconnection market.

[32] http://berec.europa.eu/doc/berec/bor/bor11_53_qualityservice.pdf
[33] http://berec.europa.eu/doc/berec/bor/bor11_67_transparencyguide.pdf
[34] http://berec.europa.eu/doc/2012/TMI_press_release.pdf

3. Main regulatory issues related to QoS in the context of net neutrality

The purpose of this chapter is to give an introduction to the remedies the new regulatory framework provides for regarding network neutrality with respect to quality of service offered to end users. The following chapters will give a more detailed elaboration of the regulatory tools available to assess the market situation.

Articles 20-22 of the USD set out a multi-layered process to enable NRAs to ensure sufficient levels of quality of service. It first details transparency measures and then the power given NRAs to set minimum QoS requirements in order to prevent service degradation.

BEREC's NN QoS framework identified two main categories of cases which may result in degradation of service:

(1) Internet access service as a whole, and
(2) individual applications using the Internet access service.
(3)

3.1 Different roles of QoS in the context of net neutrality

3.1.1 Improving transparency

In the European Directives, transparency is the starting point when it comes to considering network neutrality. A condition for a competitive and transparent market is that consumers have sufficient information to make informed decisions, and in terms of quality of service, this could take the form of contractual terms provided by the ISP.

This information should include the following parameters which are of particular interest for quality of service in the scope of net neutrality:

- information regarding minimum quality of service levels offered as well as other parameters related to the quality offered to the end user
- information on any conditions limiting access to and/or use of services and applications
- information on any procedures implemented by the ISP to measure and shape traffic so as to avoid filling or overfilling a network link, and on how the procedures could impact on service quality

To ensure that end users are fully aware of the actual conditions of the service offered, they should have access to the appropriate means or tools to assess the quality of service their ISP has contractually agreed to provide.

These means or tools should make it possible for the end user to assess the state of service quality, allowing the user to monitor the Internet access service. This would enable end users to detect a clear degradation (for example, the blocking of access to an application), or discover a degradation the ISP had not informed them of (for example, a continued slowdown in the throughput rate).

In this context, the mere possibility of observing quality of service degradations may serve as a preventive measure for avoiding deterioration of quality conditions.

3.1.2 Monitoring of quality

A classification of possible tools to monitor the quality of Internet access is presented below. They contribute to effective transparency by checking factual parameters against advertised or contractual parameters, and detecting degradation of service with respect to the contractually agreed performance.

Two different regulatory approaches can be foreseen, proactive or reactive. With the proactive approach, NRAs will perform monitoring as a more or less continuous activity to see how the quality of the Internet access service develops over time. With the reactive approach, NRAs may initiate monitoring on an ad hoc basis, for example when a potential incident is reported by a stakeholder.

Quality monitoring tools will typically be based on a client/server measurement configuration. At the network side, servers could be deployed at different points of the Internet infrastructure in order to perform monitoring of relevant performance indicators. Test servers could be placed inside ISPs networks and at Internet exchanges for performance monitoring and analysis of IP traffic from different applications, while collecting extensive, reliable and comparable time-series data sets. The test results could be reported on an individual basis for the verification of transparency, as well as in groups, such as different subscriber categories and individual ISPs, in order to aid comparison.

At the end user side, the clients (testing equipment) could be either hardware or software-based. Hardware test probes could be provided either by ISPs or independently, the former with the risk of influence on results by the ISP which knows exactly how the measurements are carried out. Quality testing software could be provided either as interactive tools available to be downloaded from dedicated websites performing measurements at a specific point in time, or as measurement tools that are downloaded and installed by the end user for the purpose of on-going monitoring in the background. Software tests have lower costs but also lower precision than hardware based probes, because they can be impacted by the end user's equipment or operating system.

Although network performance can be measured end-to-end, NRAs will need to recognise that an ISP is only able to exercise control within its own network. It may therefore be necessary for measurements to distinguish between different segments of the complete traffic transmission path, at least separating out the access leg and interconnection leg. The access leg is under the control of individual ISPs, whereas the interconnection leg of the transmission path is normally not under the control of a single ISP but is based on the interconnection arrangements used by the ISP. These circumstances need to be considered when establishing measurement procedures. In this regard, IP interconnection is an area of interest on which BEREC is producing a report in 2012. In particular, BEREC is looking at performance terms in IP interconnection agreements, both current conditions and possible future changes, how they may affect net neutrality matters and whether they need to be considered when NRAs set minimum QoS requirements.

We will return to the different aspects of quality monitoring tools later in these Guidelines. It may also be interesting for BEREC at a future stage to look further into this, for example through exchange of experience and collaboration in defining measurement methods in order to facilitate common grounds for monitoring platforms.

There is also a market dimension which is essential to consider in the evaluation of quality of service. Degradation of service could be a general market situation or an event related to specific providers; it could be related to the popularity of restricted offers or it could happen in the presence of mainly unrestricted Internet offers; providers also have very different market-

shares and some use wholesale offers from the SMP providers while others operate independently, with more control of the quality they can provide. These aspects imply that any minimum QoS requirements need to be tailored to to the specific situation observed. The BEREC report on *Competition issues related to Net Neutrality* examines in depth the effect of differentiation practices (agreements between ISPs and CAPs that involve different treatment of traffic) on competition and innovation, in order to assess potential end user harm.

3.1.3 Imposing minimum QoS requirements

According to Art. 22(3) USD, NRAs shall have powers to set minimum QoS requirements to prevent degradation of the Internet access service and the hindering or slowing down of traffic over networks. In BEREC's NN QoS framework, two types of potential minimum QoS requirements were identified: functional/qualitative and technical/quantitative requirements.

When imposing minimum QoS requirements, NRAs must intervene according to the principle of proportionality, as elaborated in chapter 2, in order to avoid disproportionate measures which are not commensurate with the degradation detected. Thus, to solve these problems, NRAs should impose minimum QoS requirements in a manner proportionate to the regulatory objectives, selecting the most appropriate types of requirement in each case necessary to reach the declared objective(s). Given a particular situation, the NRAs could impose functional/qualitative or technical/quantitative requirements, or a mixture of both.

Functional/qualitative requirements demand certain normative conditions to be met, for example that an application should be allowed to function "adequately". Functional requirements hence allow for a discretionary description that is more flexible and dynamic. However, they may, in some cases, provide limited information to the addressee of the specific content of the requirement, and of its applicability and interpretation. Functional requirements do not exclude the possibility of providing further downstream (technical) specifications of the discretionary requirement in additional regulation.

Examples of possible functional requirements:

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

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 experience an available data transmission rate of at least a specific number of kbps. Detailed technical requirements which specify individual parameters are more demanding on ISPs. On the other hand, they deliver much clearer information in terms of the exact conditions to be met.

Features of possible detailed technical requirements:

- A typical or minimum actual access speed to be required
- Aspects of the interconnection leg to be included in addition to the access leg
- Quantitative quality requirements to be set for different applications (may not be feasible on today's best effort Internet)
-

3.2 Two main categories to be considered

The following sections elaborate on the two main categories identified, where degradation of service would raise concerns. These two categories are:

(1) the Internet access service considered as a whole, and

(2) individual applications using Internet access service.

For simplicity, the two categories will be discussed separately in these guidelines. However, in practice, users can experience a combination of these categories, and it is the concrete situation at hand that has to be examined when considering imposing minimum QoS requirements.

3.2.1 The Internet access service considered as a whole

The first category is where the access to Internet as a whole is degraded. The degradation of the Internet access service considered as a whole can for example be caused by congestion on a regular basis. This will typically occur when the ISP fails to respond to increasing traffic levels with a sufficient increase of capacity.

The dividing line between situations that need regulatory intervention and situations that don't is likely to be difficult to predetermine accurately. However, an example of a rather extreme scenario can be described as what could be called the "Dirt road Internet". Providing this example does not imply that BEREC finds it likely that such a situation easily could develop. The purpose is simply to explore situations that may potentially lead to the imposition of minimum QoS requirements. (Other scenarios are elaborated later in the chapter.)

Scenario A: The "Dirt road Internet"
Most ISPs have moved in a similar direction and have increased the capacity of their specialised services at the expense of the Internet access service. Internet access services have inadequate performance most of the time due to a high degree of overbooking in both aggregation (backhaul) networks and at interconnection points used for traffic exchange. This has the effect that applications using Internet connections receive very low network performance when they run compared to the network performance received by specialised services, where the capacity is provided according to the requirements of each service.

In order to detect a degradation of the general Internet electronic communications services, the performance must be monitored over time. Statistical methods are necessary in order to ensure reliable measurement results. The *congestion level* of Internet access services would be of particular interest as this provides an indication of potential degraded performance. A decreasing ratio of Internet access service speed during peak hours compared to speed at off-peak hours would be a parameter of high importance for such an assessment. Assuming that the specialised services are maintaining their performance level (since they are based on implicit or explicit contractual terms) such a decreasing Internet access performance ratio would indicate a degradation of this service. In cases where the performance of specialised services is actually increasing (e.g. because of technology development) the Internet access service should be assessed based on a similar increase in performance levels.

In order to assess a concrete market situation in this scenario, BEREC recommends that NRAs should assess the access to the Internet at the market level. This assessment may be different depending on whether there are one or several market players and whether there are one or more SMP providers in the market in question. If there is only one provider, or one or more SMP providers control/s the market and has/have caused this situation, the solution might be to impose minimum QoS requirements on the services of only this/these provider/s.

According to Art 22(3) USD, NRAs shall be given the competence to set minimum QoS requirements on an undertaking or undertakings providing public communications networks "[*I]n order to prevent the degradation of service and the hindering or slowing down of traffic over networks".* In the "Dirt road Internet" scenario, this condition would probably be met.

However, according to the wording of this provision there is no requirement that the degradation, hindering or slowing down should be severe. The mere conclusion that there is such degradation, hindering or slowing down seems to be sufficient in to order to impose an appropriate minimum QoS requirement. In that case, conditions for regulatory intervention could be met at a lower level of degradation than that of Scenario A described above. The wording should be interpreted in the light of the legislative goals.

According to recital 34 of the 2009/136/EC Directive, the underlying goals 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. to address service degradation that is to the detriment of consumers.

When setting the minimum requirements, the principle of proportionality should be taken into account. This might, for example, justify stricter or more comprehensive minimum QoS requirements on SMP providers. The principle might also imply stricter and/or more comprehensive requirements depending on the degree of the degradation, hindering or slowing down.

In chapter 4 the guidelines will go deeper into the issues regarding degradation of Internet access service as a whole.

3.2.2 Individual applications using the Internet access service

The second category to consider is the case where individual applications using an Internet access service are degraded. Degradation could be seen from individual applications not working as intended or not working at all. The ISPs may, for example, use different traffic management techniques to “hinder or slow down” traffic to and from specific applications. Again, an example of a rather extreme scenario is provided - describing what could be called the “Cable TV Internet” - with the purpose of exploring potential situations:

Scenario B: The “Cable TV Internet”
Most ISPs have moved in a similar direction and have implemented DPI (Deep Packet Inspection) within their networks. Consequently, Internet access service offers are filtered extensively, and few unrestricted offers exist anymore or they are so expensive that almost nobody subscribes to unrestricted offers. Internet access service offers are increasingly becoming tailor-made to specific usage, such as Facebook, Youtube or Skype. The Internet as an open arena for communication is diminishing as subscribers are increasingly choosing restricted packages.

The focus of this assessment is the functioning of the individual applications, and not the access to the Internet as a whole. The ability to verify service quality is also a precondition for subscribers to be able to make informed choices as well as a tool with which NRAs can detect deterioration of quality, such as blocking (hindering of traffic) or throttling (slowing down of traffic) of specific applications. As an example, verifying quality in these cases can be performed simply by checking that the relevant application is working. If the functioning on this application fails, quality is not verified. The point at which an NRA would intervene based on such verification tests will depend on the availability and penetration of unrestricted offers and to a certain extent on the simplicity of the verification process.

One way to assess a concrete market situation in this scenario would be to assess the access to Internet at product (offer) level. ISPs might choose to have several offers on the market ranging from restricted offers (preventing the use of one or several applications) to

unrestricted offers which enable the end user to run applications of their choice. Such an approach might, as a starting point, be considered to meet the expected level of quality of clearly informed subscribers. However, subscribers of unrestricted offers will in this scenario not be able to use them to the full extent, because in the case of community applications they will not be able to interact with subscribers of restricted offers while using applications hindered at the remote end. This might therefore constitute a "degradation of service". In this scenario, one possible solution could be to impose minimum QoS requirements (possibly in the form of functional requirements) on providers of restricted offers regardless of the market position of said providers.

In the "Cable TV Internet" scenario, the conditions in Art. 22(3) USD for setting minimum QoS requirements are probably met. However, as mentioned above, the condition would already be met at a lower level of degradation than that described in Scenario B. When setting minimum QoS requirements in these cases, the principle of proportionality may - as in the "Dirt road Internet" scenario - imply stricter and/or more comprehensive requirements depending on the degree of the degradation, hindering or slowing down.

In chapter 5 the guidelines will go deeper into the issues regarding degradation of individual applications using the Internet access.

3.3 Definition of basic concepts

As scenarios A and B show, the distinction between the Internet access service and specialised services is crucial in terms of the regulatory issues around QoS in the context of net neutrality. For the purpose of these guidelines, BEREC uses definitions of three basic concepts; Internet, Internet access service and specialised services.

Internet
The Internet is the public electronic communications network of networks that use the Internet Protocol for communication with endpoints reachable, directly or indirectly, via a globally unique Internet address.

The Internet is an electronic communications network according to the definition given in the Framework Directive. The BEREC definition of the Internet is also close to the definition used by the Federal Communications Commission (FCC).[35] Regarding globally unique Internet addresses, these are currently managed by the Internet Assigned Naming Authority (IANA) and related regional and local Internet registries in a structured allocation scheme. Internet-connected computers which are only temporarily and/or indirectly accessible (e.g. through network address translation)[36] are also included in this definition.

Internet access service
An Internet access service is a publicly available electronic communications service that provides connectivity to the Internet.

In principle, an Internet access service allows for reachability between all end points connected to the Internet without any form of restriction to the content exchanged. It enables end users to run any application utilising the electronic communication function of the Internet.

Furthermore, an *unrestricted* Internet access service is defined based on the definition above with the only deviation allowed being the use of reasonable traffic management. If there is

[35] Notice of Proposed Rulemaking, page 65, FCC 09-93, 22nd October 2009
[36] Network address translation (NAT) is an obstacle to innovation, development and deployment of applications (ref. RFC 2993, Architectural Implications of NAT), but NAT is included in the definition of the Internet in order to make these guidelines also cover all end users that today are connected to the Internet through NAT. With IPv6 this problem will diminsh and end-to-end connectivity will be restored on the Internet (ref. RFC6540, IPv6 Support Required for All IP-Capable Nodes).

any deviation beyond reasonable traffic management, this is defined as a *restricted* Internet access service.

In this report the concept of "Internet electronic communication" is used to refer to the general end-to-end communication provided over the Internet, following a similar practice as used in the NN QoS framework, without giving it any further formal definition. However, the Internet access service, which is the service provided by an ISP to its end users, whether in an unrestricted or a restricted variant, is defined as above.

The Internet access service constitutes a segment of the whole end-to-end communication, comprising communication over the access network (fixed or wireless), the aggregation network (also referred to as backhaul) and the IP infrastructure of the ISP[37] – and it also includes access to the Internet infrastructure beyond the ISP's control based on the interconnection arrangements (both contractual and technical) used by the ISP.[38]

By default, an Internet access service is provided with neither contractual nor technical limitations on the use of the service, whether this is in the shape of throttling or blocking of specific content or applications. This kind of limitations is in this report referred to as "restrictions". Deviations from this default rule may be categorised as being either reasonable or unreasonable restrictions.

Restrictions implemented by ISPs constitute a part of their traffic management practices, and therefore traffic management is also referred to as being reasonable or unreasonable. In this report, when discussing whether traffic management is reasonable or not, we are however using the concept "traffic management" in a broad sense including both contractually binding and technically enforced restrictions. Criteria for reasonable traffic management are described in chapter 5.

Specialised services

Specialised services are electronic communications services that are provided using the Internet Protocol[39] and operated within closed electronic communications networks. These networks rely on admission control and they are often optimised for specific applications based on extensive use of traffic management in order to ensure adequate service characteristics.

If the services are provided as vertically integrated services, the specialised service only encompasses the underlying electronic communications service component, and excludes the application layer. Specialised services may interwork with the electronic communication on the Internet through gateways executing the admission control function.

BEREC's definition of specialised services is close to FCC's description of "specialized services"[40] and the Internet Society's description of "IP-based services"[41], and is also sometimes referred to as "managed services".[42]

BEREC's definitions above explain that specialised services and Internet access services are provided over distinct networks. These networks will however in many cases be operated over the same underlying physical infrastructure. Internet access services are operated over

[37] A framework for Quality of Service in the scope of Net Neutrality, section 4.1
[38] A framework for Quality of Service in the scope of Net Neutrality, section 5.2
[39] Specialised services may also comprise non-IP based services like cable television or circuit switched telephony, but the focus in these guidelines is on IP based service provisioning, i.e "specialised IP services".
[40] Communications Commission, Report and order, FCC 10-201, December 2010
[41] Internet Society, Mat Ford, OECD Broadband Metrics Workshop, October 12-13, 2011, Washington, http://www.fcc.gov/events/oecd-broadband-metrics-workshop
[42] Note that "managed services" in this case must not be interpreted simply as "services using service management" since this would overlap with Internet access services which also use traffic management.

the Internet – often referred to as *the open Internet* – while specialised services are operated over *closed IP networks* (without implying closed in any negative sense of the word).

In the Internet access service category, the application and network layers are provided separately, both technically and in many cases commercially, where the network layer (which is more or less equivalent to the electronic communications service) and the application layer are provided by different business entities. In other words, the two layers are *not* vertically integrated in an Internet access service.

In the specialised service category, the two layers are often provided by the same provider and are therefore technically and commercially vertically integrated. One example of this is facilities-based IPTV services[43]. This difference between Internet access services and specialised services makes them difficult to compare. To make comparison easier, for the purpose of this report we define a specialised service as only the network layer component, and we exclude the application layer.

Even though Internet access services and specialised services are provided over different networks, interworking between the two service categories is still possible. Interworking means interconnection though an adaptation function that checks whether admission should be granted according to the service policy (known as admission control). Where different technologies are used in the two networks, interworking may also include transcoding or similar functions.[44]

During regulatory considerations, the two distinct categories of cases described in section 3.2 can be illustrated with figure 3.1 below. When the Internet access service is considered as a whole, its relation to specialised services is of particular concern (as indicated along the horizontal axis) and this will be discussed in detail in chapter 4.

Furthermore, *unrestricted* Internet access services gives access to all endpoints and all applications on the Internet, but may apply reasonable traffic management – while *restricted* Internet access services also apply unreasonable traffic management thereby limiting the access to specific endpoints or specific applications. A description of *prioritised* Internet access services is given in the next section. A deeper study on aspects regarding reasonable traffic management, restricted Internet access and also prioritised Internet access are discussed in detail in chapters 4 and 5.

[43] IPTV can also be provided "over-the-top", i.e using the Internet access service.
[44] An example of interworking between specialised services and over-the-top applications is facilities-based VoIP interconnecting with VoIP provided on the Internet.

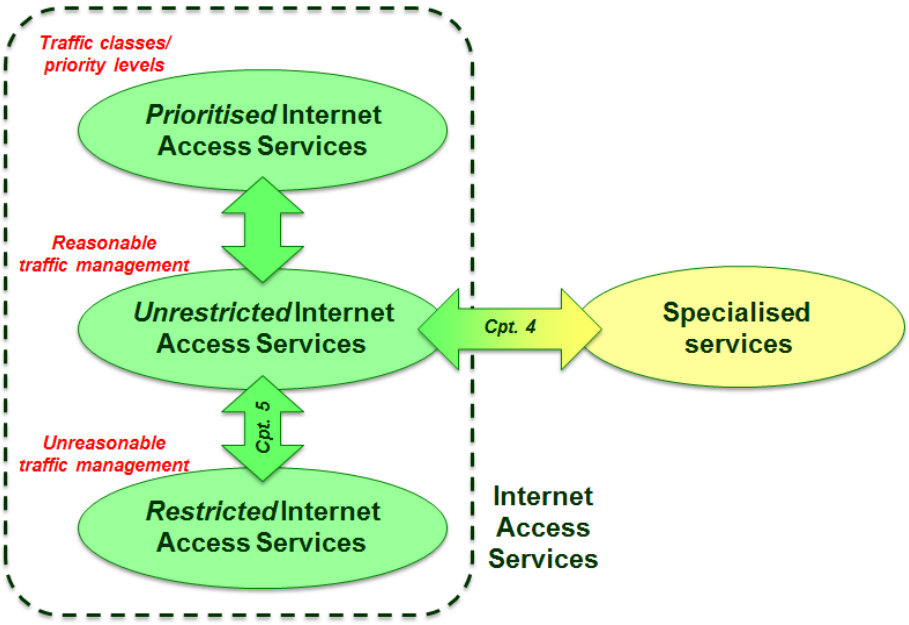

Figure 3.1 – The two dimensions

3.3.1 Differentiation of Internet access service offers

As presented previously, BEREC divides individual cases into two categories - (1) IAS considered as a whole, and (2) individual applications using the IAS. In this section, concepts particularly relevant to category (2) are presented, but methods for regulatory assessment of these practices are covered in chapter 5.

Application-agnostic vs. application-specific traffic management
In this report, BEREC makes a distinction between application-agnostic and application-specific traffic management. A function that is application-agnostic is treating all applications similarly (e.g. IP packets from all applications put in the same forwarding queue) while application-specific functions treat individual applications differently (e.g. VoIP is blocked or P2P is throttled while other applications are not).

When discussing application-agnosticism, the application concept is used in a broad sense. Application could refer to an application layer protocol (e.g. SMTP, NNTP or SIP), a generic application type (e.g. P2P, VoIP or instant messaging) or application software (e.g. Skype, eMule or Firefox).

Network layer traffic classes
Note that the concept of "Internet access service" is not defined based on best effort traffic forwarding, although this is the default way of forwarding traffic on the Internet today. However, differentiated traffic forwarding is becoming increasingly available also for Internet access service offers. (Note that differentiated traffic forwarding is also used for implementation of specialised services, but this section focuses on differentiation of Internet access service offers.)

Traffic differentiation may be targeted at specific applications in an ad hoc manner as mentioned above (e.g. blocking of VoIP), or the differentiation may be based on general *traffic classes* (also referred to as *priority levels*) at the *network layer*.[45]

Traffic classes/priority levels may be implemented based on different principles. The traffic classes may relate to each other as lower and higher priority levels without specific quality guarantees, or they may be defined based on explicit quality guarantees.

Traffic classes without explicit quality guarantees
In the former case, it may become very difficult to define which priority level should actually be considered as the *best effort traffic class*. For example, consider a case with two priority levels, both of them without explicit quality guarantees. The level that is considered to be best effort will depend on the perspective, i.e. from which level the comparison is seen. If the lower level is named best effort, the upper would be better-than best effort. If the upper level is named best effort, the lower would be less-than best effort. There is no specific definition of the quality of a best effort priority level. In a real-life situation it would therefore be difficult to determine whether such a case is an example of a *degraded* service (less-than best effort) or an example of a *prioritised* service (better-than best effort).

Therefore, when it comes to evaluating whether there is any degradation of service in the case of *differentiation of traffic within Internet access service offers*, there may be a need for a more detailed regulatory assessment which is elaborated in chapters 4 and 5.

[45] Network layer traffic classes in an *inter-network case* depends on implementation across networks, which is generally not the case on the Internet today. Traffic that is sent out of a network which supports traffic classess will fallback to best effort.

Application-agnostic traffic classes
Note that *network layer traffic classes* may be application-agnostic in the way that any application may populate any traffic class. In a real-life case, however, specific applications *may* be allocated to specific classes, e.g. real-time applications such as telephony and television will typically have stronger quality requirements than other applications and could therefore typically be prioritised in the network. But the allocation scheme may also be of a more application-agnostic variant where this is dynamically decided independent of application (e.g. per communication session).

An important aspect in such situations would be who decides which traffic that should be transferred by each class. This could be decided by the end user, the CAP, the ISP or some sort of combination. This is an aspect which is discussed in chapter 5.

Furthermore, Internet access services may also be foreseen in the future where end users are offered prioritised delivery of *all* traffic, this is what is referred to as *prioritised Internet access service offers*. Regulatory aspects of such offers are discussed in chapter 4.

Internet access services vs. specialised services
A detailed discussion on the regulatory aspects of traffic management of the Internet access service and criteria for assessing the *differentiation* of Internet access service offers will be presented in chapter 5.

A similar assessment is not needed for specialised service offers since it is not considered necessary to apply minimum QoS requirements to these. However, as will be further elaborated in chapter 4, the assessment of degradation of the Internet access service as a whole will typically be compared to specialised services. Chapter 4 will furthermore discuss regulatory aspects of *prioritised* Internet access service offers.

3.4 High-level regulatory process description

BEREC foresees a regulatory process of up to six steps for determining whether and how to impose minimum QoS requirements, and the steps are outlined in the text below and in Figure 3.2.

Step 1
As a first step, the NRA will typically identify situations that may need further attention. (This corresponds to “indications /symptoms” in the NN QoS framework report.) Examples of such situations could be indications of degradation of the two categories (the Internet access service as a whole, or individual applications using the Internet access service). These indications could be based on complaints from consumer or other stakeholders or be detected by NRAs.

Step 2
If it is considered necessary to follow up situations identified in the first step, this second step will assess whether regulatory intervention is needed. (This corresponds partly to “trigger detection” in the NN QoS framework report.) The NRAs will perform an evaluation of quality indicators to verify the indications/symptoms and analyse the results in order to determine whether to intervene. During this phase, NRAs will assess how severe the degradation is. NRAs will typically have to take into account the extent of the degradation (both from a technical point of view and from the perspective of the end user), the number of end users that are affected by the degradation, and the number of providers that deliver a degraded service.

Step 3
If the decision during the second step is that regulatory intervention is needed, the NRA will have to choose which regulatory remedy to use. (This step corresponds to the last part of the "trigger detection" in the NN QoS framework report.) The different regulatory options include considering whether to impose stricter remedies promoting competition and imposing specific (more comprehensive or more detailed) transparency requirements. The remedy to use will depend on the specific case considered; in particular whether the provider in question has SMP or the situation is a result of a widespread degradation over several providers. If these tools are deemed insufficient to address degradation of service, NRAs may refer to Art. 22(3) USD to set minimum QoS requirements.

Step 4
If the regulatory remedy considered most appropriate in the specific case is to impose minimum QoS requirements on providers, the actual requirements have to be determined. The determination of these requirements will be based on the concrete situation at hand, considering which of the two categories of degradation, or what combination of the two, is relevant. In determining the requirements, the NRA must also adhere to the principle of proportionality.

Step 5
The NRA shall then provide the Commission with information about the envisaged requirements, a summary of the grounds for the requirements and a proposed course of action. This information shall also be made available to BEREC.

Step 6
Finally, after taking the utmost account of any comments or recommendations of the Commission, the NRA can impose the minimum QoS requirements. The NRA may also subsequently need to assess whether the requirements have been complied with.

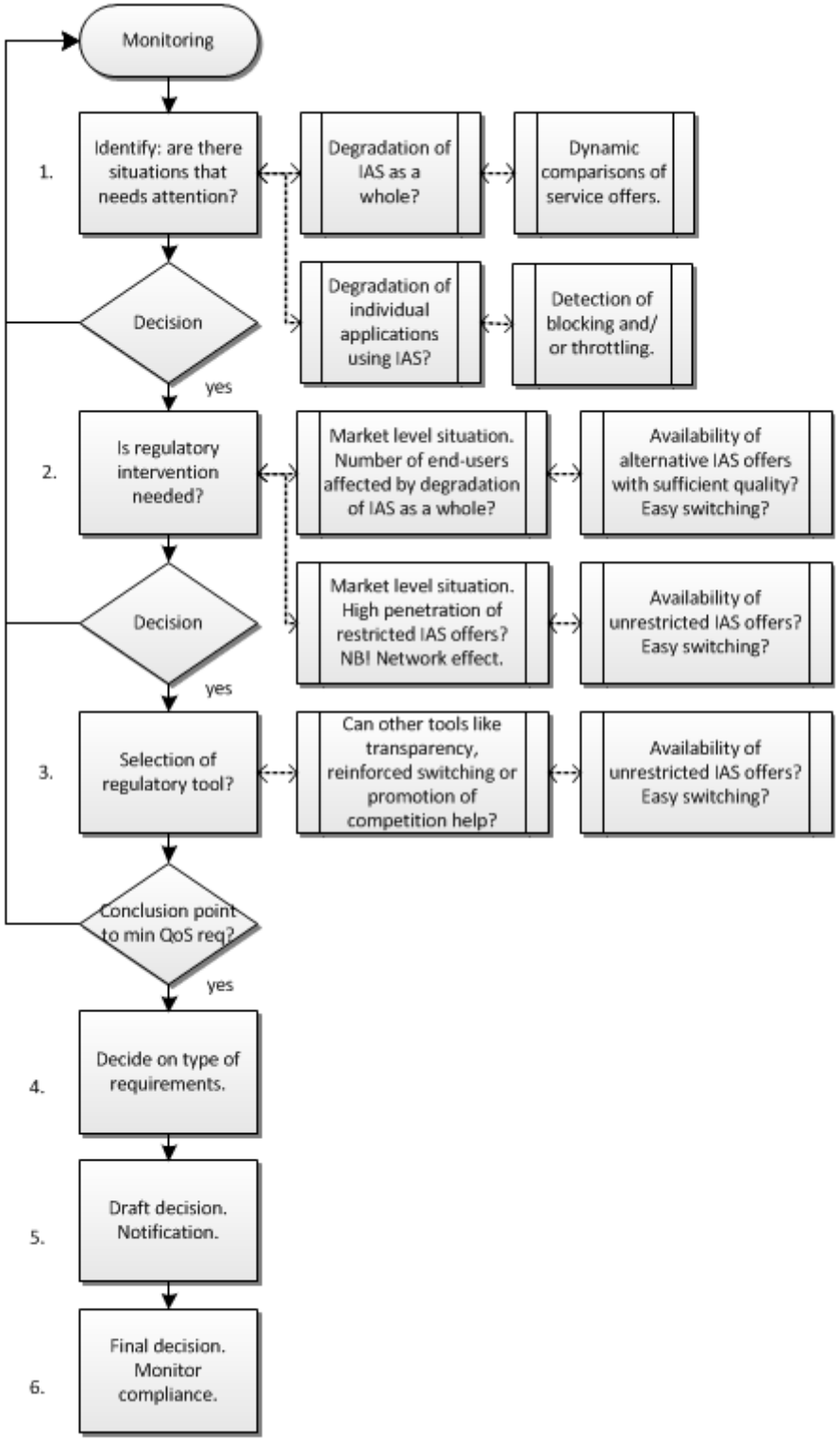

Figure 3.2 – The regulatory process

3.5 Examples of cases to be considered

The “Dirt Road Internet” and the “Cable TV Internet” scenarios mentioned in section 3.2 are rather extreme examples of degradation. In this section, BEREC will list examples of cases that are more likely to occur in reality (the list is not exhaustive).These examples should not be considered as developments of the Internet that BEREC sees as most likely, but simply as possible circumstances in which degradation might occur. Degradation will not, as shown below, necessarily lead to the imposition of minimum QoS requirements: the level of degradation and the need for regulatory intervention will have to be carefully assessed.

3.5.1 Degradation of the Internet access service (IAS) as a whole

Three potential examples of degradation of the IAS as a whole are:

i) ISPs prioritise specialised services on the expense of the IAS as a whole
ii) Internet traffic load grows faster than the increase in available capacity
iii) IAS of sufficient quality is only accessible to a limited number of users

i) One possible business strategy for ISPs could be to prioritise the development of their specialised services, such as facilities based IPTV or VoD. As a result, networks’ resources would primarily be used by these services, which require a high level of quality, and Internet access services would face a severe lack of capacity. The performance of applications through the Internet would decrease or grow at a slower pace than those delivered through specialised services. Thus, with specialised services as a reference point, it appears that the quality of IAS is declining.

If diminishing quality of IAS compared to the specialised services becomes widespread, this could harm both the end users and the CAPs. This could cause end users and CAPs to increasingly opt for specialised services instead of IAS. In the long run this would also reduce the incentive to innovate new content and applications on the Internet. There is also an opportunity for innovation based on specialised services, but this is subject to higher entry barriers.

ii) Another potential example of degradation of the IAS as a whole would typically occur when Internet traffic grows faster than the increase in available capacity, independent of the development of specialised services. Investments would not be sufficient or the business model of the IAS becomes inadequate to allow a smooth conveyance of data in the networks. Congestion becomes more frequent and severe, resulting in a lower quality of Internet access service.

iii) A third example describes a situation where the Internet access service would be delivered with sufficient quality only to a limited number of end users. Other end users would be offered a lower performance and find it (increasingly) difficult to switch to a better service, although they would want to. Barriers to change could be economic, technical, geographical, etc. and explain why a significant proportion of end users would not be able to enjoy a satisfying quality of service.

For each of these three examples, it can be argued that the quality of Internet access service, assessed at a market level, is at risk. These examples do not imply that an NRA should necessarily impose minimum QoS requirements according to the powers given by Art. 22(3) USD. In particular, it must be emphasised that the legal framework does not oblige undertakings providing public communications services to deliver their services with a minimum level of performance. However, the new provisions in Art. 22(3) USD authorise

NRAs to consider the risk of degradation as a legitimate area of concern and a possible ground for action (see chapter 2).

In example (i) the question is how the capacity should be divided between IAS and specialised services, while in example (ii) and (iii) the situations may be caused by economic limitations of the ISPs' business model making it more difficult to provide sufficient network resources for high quality services. In the latter cases, setting minimum QoS requirements on such an ISP may not be feasible, and it will then rather become a question about universal service obligations. These guidelines, however, will not cover universal service obligations.

The notion of "degradation" is primarily related to a process of decline which needs to be monitored and evaluated over time. That is why BEREC recommends an on-going approach that allows comparisons over time and may result in the identification of a problematic situation. This is however not sufficient to conclude whether a regulatory intervention is needed. Once this assessment has been made, the appropriate regulatory measure still has to be chosen and, if necessary, minimum QoS requirements may be imposed.

The detailed regulatory assessment of these examples of degradation of the IAS as a whole will be set out in chapter 4.

3.5.2 Differentiated treatment of individual applications on the IAS

Three potential examples of differentiated treatment of individual applications on the Internet access service can be foreseen, as set out in the separate BEREC report on *Competition issues related to net neutrality*:

i) VoIP blocking on mobile Internet access services
ii) P2P blocking or throttling on mobile or fixed Internet access services
iii) Differentiation of traffic from content and application providers (CAPs)

i) Vertically integrated mobile operators may have incentives to block VoIP on the Internet access service, since they will want to protect their traditional voice business. This incentive becomes even stronger when the operator itself offers VoIP as a specialised service. End users could face higher prices (e.g. when the operator chooses to charge extra to use a VoIP application), or alternatively end users could face throttling or blocking practices by the mobile operator to discourage the use of VoIP. The same issues could be experienced with relation to instant messaging applications replacing SMS services.

Even if no mobile operator has SMP, this behaviour may become a problem if the blocking or throttling was to become widespread. The more widespread the practice becomes, the less available unrestricted IAS offers will be. In addition to limiting the possibility of switching, this will also reduce the usability of the VoIP (or messaging) application for users subscribing to unrestricted IAS offers since the potential user base of the application decreases. This will reduce the economic and social value of the application.

When a vertically integrated operator has SMP, the NRA could in principle choose to apply SMP remedies, but this may not always be an efficient way of dealing with the problem (more on this will follow in chapter 6). In non-SMP cases, the new regulatory remedies, including Art. 22(3) USD, could be more directly applicable. Therefore, depending on the outcome of the assessment in steps 3 and 4 of the regulatory process, there may be a reason to impose minimum QoS requirements to remedy the problem.

ii) Another potential case for degradation of individual applications is P2P. This is applicable for both fixed and mobile Internet service providers. Again, vertically integrated operators – in this case ISPs that also offer VoD or IPTV services – have incentives to block or throttle P2P applications because these applications compete with their traditional video business provided as specialised services.

However, P2P applications generate high bandwidth traffic, which can lead to congestion in the network. This may affect other end users of the network if the capacity is not increased to compensate for the increased traffic load. Saving bandwidth cost may be a motivation for blocking or throttling P2P applications, whether the provider is vertically integrated or not. However, the high traffic load may alternatively be handled by application-agnostic congestion management which will give a similar reduction of traffic.

The P2P technology is still subject to considerable improvements, including techniques contributing to significant traffic reduction compared to traditional content distribution. As in the case with VoIP, the network effect is relevant in the case of P2P. This will reduce the value of the P2P applications for end users and CAPs. This will also lead to reduced incentives to further develop the P2P technology.

Therefore, in the case of blocking or throttling of P2P applications on the Internet access service, the assessment of whether the identified case warrants regulatory intervention needs to be closely examined and considered. Today, there is a shift in traffic load from P2P applications over to streaming applications, and similar traffic management practices and related regulatory considerations may become relevant for streaming in the near future.

iii) The third potential case is the most complex one to examine. A practice that has raised debate in the context of net neutrality is whether ISPs are allowed to charge an additional price from CAPs for a higher priority level, or even guaranteed quality, at the network layer[46] of the Internet access service itself. This is sometimes referred to as “two speed Internet”. This must however not be confused with specialised services (e.g. IPTV) provided in parallel to, but separated from, the Internet access service.

Assuming that bandwidth is not unlimited, this practice may automatically lead to a deterioration of the other applications provided over the Internet access service. However, the result depends on how ISPs deal with the situation. They may choose to implement this in such a way that applications of *other* CAPs receive reduced capacity to make up for the capacity that is required by the prioritised traffic. On the other hand, if additional capacity is provided, there is always a question about how this capacity is divided between the different classes of traffic.

An essential aspect of such prioritisation is whether it is made available to all CAPs on the same conditions. In addition, differences in price between best effort and prioritised traffic classes will be of relevance. Regarding the particular assessment of whether the service is degraded, the major parameter of concern is the performance of the best effort traffic class compared to the prioritised classes.

The detailed regulatory assessment of these examples of differentiated treatment of traffic on the Internet access service will be set out in chapter 5.

In addition to cases belonging to the two main categories, market situations may emerge which contain a mixture of practices. This report is mainly focused on clear-cut cases in order to clearly distinguish between different regulatory aspects.

[46] CDN-servers used for distributed caching of content closer to the end users are running at the application layer.

4. Degradation of Internet access service as a whole

Degradation of IAS can generate concern as it may undermine, *inter alia*, the ability of end users to run applications and access and distribute information of their choice. Any degradation of service should be identified in the context of the market: a possible cause for concern could be a declining of quality offered to a majority of end users, but also a low number of IAS offers delivering sufficient quality.

From identifying degradation to implementing regulatory action, several steps must be undertaken, as described in chapter 3. Chapter 4 elaborates on the following two questions:
i) how to monitor quality of the IAS and identify problematic situations in the market?
ii) how to assess those situations and decide whether intervention is needed?

4.1 Monitor/Identify: Are there situations that need attention?

The imposition of minimum QoS requirements is preceded by a period of monitoring of quality of available IAS service offers and evaluation of the market situation, by the relevant NRA. This monitoring may be either preventive – before any concern has risen, or reactive – once degradation has been observed.

Preventive monitoring can have more diverse objectives than simply assessing the need for a regulatory intervention. Preventive monitoring can produce data to be published at regular intervals, thereby contributing to more transparency on the quality of IAS. If this monitoring includes data from different ISPs, it can also act as a comparison tool to promote competition and increase users' awareness of a market's situation.

Reactive monitoring is limited to evaluating a situation when degradation of service is suspected, typically based on complaints about low performance (e.g. speed) of IAS services received by the NRA. It does not aim at providing general data when the market is supposed to deliver sufficient quality to the end users.

Whichever kind of monitoring is implemented, following a common European high-level approach will contribute to ensuring a consistent implementation of the regulatory framework and give visibility to ISPs on decisions and processes that may impact their business. The goal of the subsequent sections is to propose an approach that can be followed by NRAs in the member states.

4.1.1 Quality of IAS over time

In order to determine if there is a degradation of IAS, NRAs would need to monitor the quality of IAS over time. To be able to determine where the potential problems are, monitoring would be performed so that it covers all relevant aspects of the IAS for which ISPs are responsible (including access and interconnection).

Monitoring can be done by checking the contracts and terms of available IAS offers or by performing technical measurements of the IAS services themselves. Complaints from end users, including CAPs, gathered by NRAs, could also give an indication about end users' perception of IAS quality.

As described in the NN QoS framework report, statistical methods are indispensable during technical measurement because of the varying characteristics of the best effort Internet communications service. A measurement platform collecting samples of different

performance parameters spread over a variety of communication paths would provide NRAs with valuable statistical data to analyse the performance of different IAS offers in the market.

One possible approach for monitoring quality of the Internet access service over time according to the QoS remedy in Art. 22(3) USD, could be to collect quality information provided by ISPs to NRAs in accordance with Art. 22(1) USD. The NRAs may, according to Art. 22(2) USD, also specify quality parameters including possible certification mechanism. NRAs using the different QoS remedies of the USD extensively may find synergies between the different aspects of this article.

Platforms allowing end users to carry out quality measurements of their Internet access services themselves are also good sources for information about the general quality level of IAS offers in the market. Several European NRAs provide this kind of measurement platform, and many of them store test results in databases for statistical analysis of results which could be used for monitoring of evolution of IAS speed over time.[47]

Specifying relevant quality parameters and measurement methods for electronic communications services in general, and for the Internet access service in particular, is subject to extensive European and international standardisation and harmonisation. Standardisation organisations like ETSI, ITU and IETF are important sources of quality measurement specifications. Other bodies, for instance CEPT,[48] promote harmonisation across national regulatory practices. It is also possible, especially for NRAs that have direct participation in these bodies, to engage with these organisations in cases where additional specification or harmonisation is needed.

Today, quality measurements of the Internet access service are mainly taken for the access leg. And, as described in the NN QoS framework report, detection of degradation of the IAS communication service should preferably also include the interconnection leg. Gathering statistical data using a distributed set of measurement servers could give indications of the performance of the electronic communication service beyond the access leg.[49]

As illustrated in Figure 4.1 below, the IAS-providing ISPs (ISP1 shown in green) will not be able to directly control the performance beyond its own interconnections to neighbouring networks (ISP2 and ISP3), but ISPs make interconnection agreements after investigating network performance needs and negotiating with peering and transit partners. The resulting performance of the Internet access service is then offered to its end users. [50] If this inter-network service is degraded, this is also an important parameter to include in the quality evaluation.

[47] A framework for Quality of Service in the scope of Net Neutrality, section 5.5
[48] CEPT's Project Team for Technical Regulatory issues (PT TRIS) is working in the area of harmonisation of existing approaches for evaluation of quality of Internet access services offers.
http://www.cept.org/ecc/groups/ecc/wg-nan/pt-tris/page/pt-tris-on-going-work-items
[49] A framework for Quality of Service in the scope of Net Neutrality, section 5.3
[50] A framework for Quality of Service in the scope of Net Neutrality, section 5.2

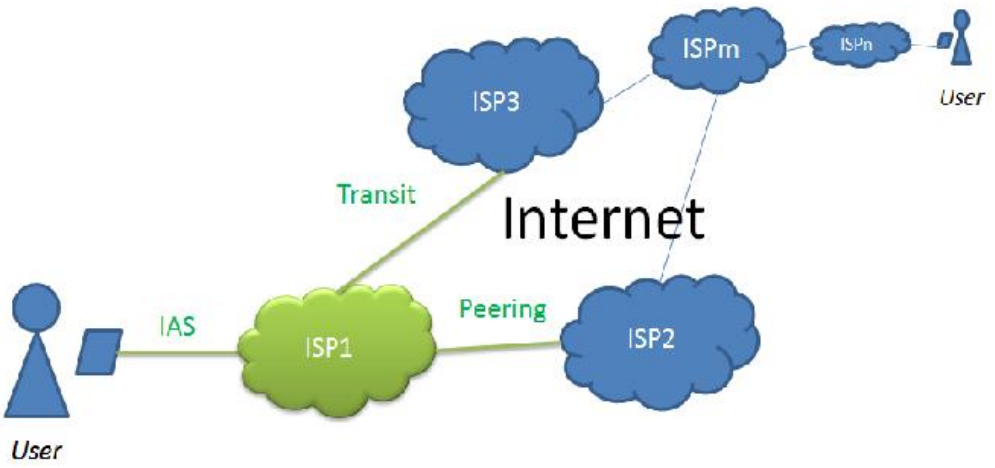

Figure 4.1 – Internet Service Provider (ISP)

4.1.2 IAS speed and congestion

Advertised speed and actual speed of an IAS could be compared. NRA could monitor the development of this comparison over time. It would be important to then also perform tests where the communication path beyond the access leg of the ISP would be tested. Statistical measurement results based on tests performed over a long time period and over a wide geographical area are necessary in order to achieve reliable data.[51]

If the actual speed differs significantly from the advertised speed, this would mostly be a matter of a lack of transparency. However, if the ISP has been sufficiently transparent, significantly lower performance than the contractually agreed speed could instead be an indication of degradation of service. The difference between performance at peak hours and at off-peak hours is one possible method for estimating the degradation in terms of congestion level.

In addition to standardising *methods* of measurement essential to produce comparable measurement results, standardised measurement *platforms* could also be considered in order to increase comparability. This would also contribute to reduced development and operational costs. This could also be an approach for achieving a larger "footprint" of measurement servers spread over the Internet to the extent that stakeholders with different geographical and topological locations are able to participate in, and contribute to, such a platform.[52]

It is particularly complicated to evaluate performance of mobile Internet access service because of the varying conditions for the wireless access links, and because the mobility of the end users causes rather unpredictable loads in different cells. An advanced and robust methodology is needed in order to measure the performance over time and over the coverage area of the individual ISPs' networks. Periodic measurements could be performed based on a statistical sampling plan for the mobile networks, and this could produce geographical as well as accumulated results.

[51] Internet Society (ISOC) response to BEREC consultation on "Guidelines on Net Neutrality and Transparency: Best practices and recommended approaches", Nov 2 2011

[52] Measurement Lab (M-Lab) is an example of an open, distributed server platform for researchers to deploy Internet measurement tools, http://www.measurementlab.net/

The most prominent performance parameter is the data transmission rate (speed) of the Internet access service. However, other performance parameters – such as reliability of service, packet transfer delay, packet delay variation and packet loss ratio – also describe important quality characteristics of the Internet access service. The different parameters should be measured between a representative set of clients (measurement equipment) and a representative set of servers.

The ETSI Guide 202 057-4[53] is one of the most widely used specifications for evaluating the quality of the Internet access service, but there may be a need to assess whether these performance parameters, measurement methods and test configurations should be expanded to incorporate some or all of the elements described above.

4.1.3 IAS vs. specialised services

Specialised services can provide a reference to which IAS may be compared. The two categories of services are deeply different - by definition, the former usually delivers a guaranteed level of quality while the latter is today mainly based on best effort. NRAs could however, monitor the development of both categories of services over a period of time and then observe how various characteristics of the services in both categories change. As illustrated in Figure 4.2 below, one can observe the same characteristics of the services belonging to the different categories in the same time frame:

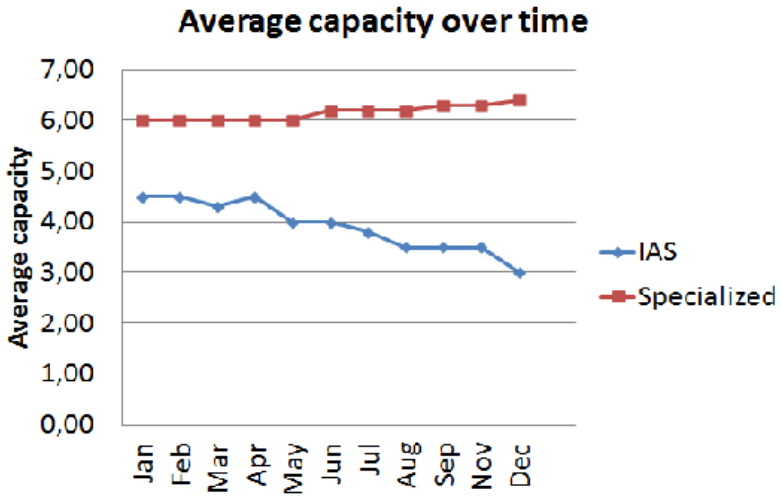

Figure 4.2 – Comparing different service categories

By observing the development over time, NRAs would be able to see the trends and judge if the specialised services being monitored receive preferential treatment on the expense of the development of IAS. NRAs would need to define the recommended characteristics (e.g. capacity, delay, jitter, packet loss) to be monitored over time.

4.1.4 Prioritised IAS

As mentioned in section 3.3.1, Internet access service offers which are given higher priority than best effort – so-called *prioritised* Internet access service – can also be foreseen in the future, sometimes referred to as “gold, silver and bronze” or similar names. (This case concerns IAS offers where *all* traffic is forwarded at a higher priority level and must not be confused with prioritised forwarding of *selected traffic flows* within the IAS, referred to as *differentiated* IAS, which is discussed in chapter 5.)

[53] ETSI Guide 202 057-4, User related QoS parameter definitions and measurements, Part 4: Internet access

Positive prioritisation of IAS offers also needs to be evaluated. It may be difficult to verify whether improved performance for some service offers actually results in a degradation of the performance of the remaining service offers. This is a question about which perspective it is seen from – from the higher or lower priority level. And, as explained in section 3.3.1, if general traffic classes are implemented for IAS, the relative performance of these classes needs to be monitored and evaluated.

4.1.5 Additional methods

Monitoring of quality as perceived by end users
As an addition to technical quality measurements, quality as subjectively perceived by end users (quality of experience) can also be taken into account, for example based on surveys commissioned by NRAs. However, one should emphasise this does not give an accurate measurement on which to base a regulatory decision. The level of quality perceived by end users can either be a trigger that leads an NRA to conduct more detailed measurements, or in addition to them, but it may not suffice in itself.

Monitoring of retail market: availability and penetration
Finally, as the assessment of the need for intervention will combine quality measurements with information about the market situation, an NRA should collect detailed information on availability and penetration of IAS offers in the retail market, together with their terms and conditions. Assessment of practises in the context of the market is expanded below.

4.2 Assess situation: Is regulatory intervention needed?

Once information is gathered on the quality of the Internet access service, an evaluation must be conducted to assess whether and how the situation is problematic and to what extent there is need for concern. The regulatory framework draws the attention of NRAs to the risk of "degradation of service and the hindering or slowing down of traffic over networks". This is considered for IAS as a whole within this chapter, while the access to individual applications is discussed in chapter 5.

Generally, the quality of IAS cannot be synthesised into one single parameter, as a large number of different service offers exist in the market and with varying levels of quality. For example, within one country, ISPs offer different packages, each of them being associated with a certain performance. Separately, even if two subscribers are on the same ISP's package, the quality may vary according to elements specific to each subscriber (whose location may have an impact on the level of performance of the access line, for example). Thus, ISPs, packages and categories of end users, *inter alia*, can be considered as different levels for assessment regarding impact on possible degradation of the IAS.

Generally speaking, meaningful comparisons can be made where there are clear distinctions to draw, such as:

- *between IAS and specialised services:* even though these are significantly different service categories, an assessment could be made as to whether specialised services are provided at the expense of Internet access services;
- If applicable, between *best effort* IAS and *prioritised* IAS[54], since it may need to be assessed whether the implementation of prioritised IAS is provided at the expense of end users subscribing to best effort IAS;
- *between packages:* within one ISP, or across several ISPs, the level of quality delivered by each package can be compared;

[54] Must not be confused with *differentiated* IAS (described in chapter 5), where the traffic *within* the IAS is differentiated, i.e. *some IP packets* (e.g. IP packets belonging to specific applications) are transmitted in traffic classes with higher priority than other IP packets.

- *between ISPs:* an average quality level can be calculated for each ISP, or one specific package that matches some criteria could be used as a reference (e.g. a representative package defined as the most sold package below a maximum price);
- *between categories of end users:* quality can be compared based on end users' situation, such as the area where they live or their other specific aspects;
- *between countries:* average quality level at a national level can be compared with other countries.

It should be emphasised that a static comparison of quality levels often does not allow NRAs to draw conclusions as to the causes of differences, as many parameters vary simultaneously. However, trends and changes over time can be compared more easily, where a significantly lower level of growth over time may help to identify degradation.

It is important to look at the specific situation of end users who are affected by degradation. If affected end users are able to easily switch to an offer with sufficient quality, the situation may not raise significant concern. On the other hand, if end users are bound to a service which is not expected to improve, they are clearly suffering from this degradation.

The market situation must be evaluated to determine whether the problem calls for an intervention. More precisely, the ability of end users to switch to an appropriate offer depends on (1) the availability of such offers, and (2) the *ease of switching in a broad sense*, including all burdens faced by customers, like the price difference between offers (see figure 4.3 below). NRAs should assess the level of each of these parameters, for different categories of end users they consider to be relevant.

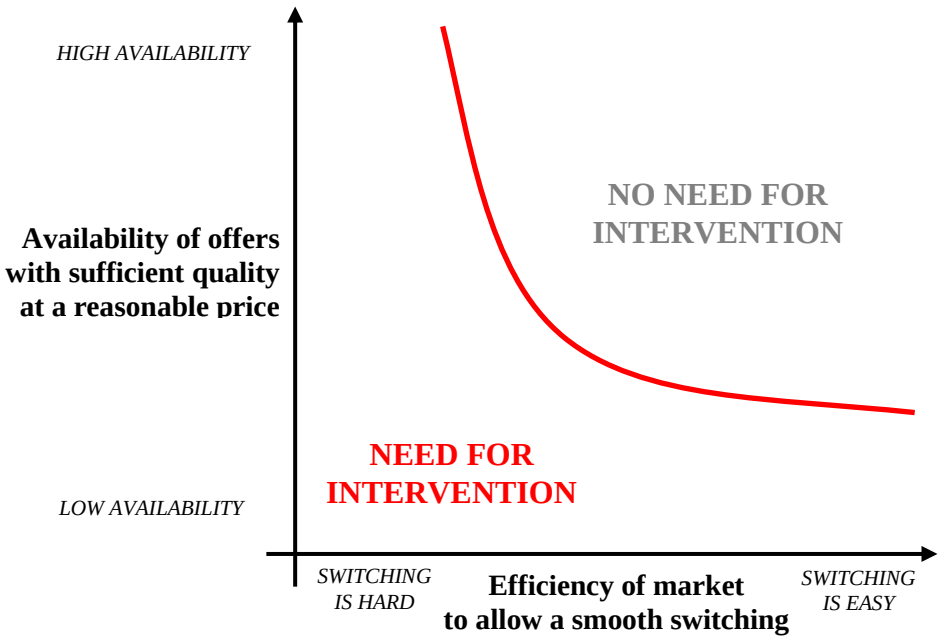

Figure 4.3

As shown in figure 4.3 above, when these two parameters are both at a high level, no intervention is necessary. However, when either or both decrease an intervention may appear useful or necessary. That is, intervention may be justified if the availability of alternative IAS offers with sufficient quality at a reasonable price is low, or if the possibility and ease of switching is limited.

Summary – Degradation of Internet access service as a whole

Identifying if there are situations that need attention

Monitoring *quality of Internet access service – either proactively or reactively –* ***is necessary*** *in order to detect degradation.*

Monitoring can be done by checking the ***contracts and terms*** *of available IAS offers or by performing* ***technical measurements*** *of the services themselves.*

Statistical methods are indispensable *during technical measurement because of the varying characteristics of today's best effort Internet communications.*

There should be ***monitoring of the quality of Internet access service (IAS) over time****, covering all aspects for which ISPs are responsible.*

Monitoring should include a range of quality parameters:
- actual vs. advertised speed
- level of congestion in the network
- measurements of timing parameters
- performance of IAS compared to specialised services
- IAS offers on the retail market (e.g. availability and penetration).
- quality as perceived by end users

Is regulatory intervention necessary?

Once information is gathered on quality of the Internet access services, ***an assessment of the situation at the market level must be conducted****.*

The identification of causes for concern lies in the comparison of several aspects at the national level (e.g. comparison between IAS and specialised services, between packages, ISPs or categories of end user) or between countries. Significant differences in these comparisons may illustrate a cause for concern.

There is ***no need for intervention*** *when there is* ***good availability*** *of Internet access service offers with* ***satisfying quality*** *(i.e. without degradation)* ***at a reasonable price*** *and the possibility and* ***ease of switching is sufficient****.*

If one or more of these elements is not fulfilled, intervention may be necessary.

5. Issues regarding individual applications on the Internet access service

5.1 Introduction

Chapter 4 investigates situations where the Internet access service as a whole is considered degraded. In Chapter 5 it is assumed that the quality of the Internet access service is at a reasonable level. This chapter addresses cases of differentiated treatment of traffic *within* the Internet access service. (Issues related to specialised services are not relevant to this chapter. Such issues are dealt with in chapter 4.)

Since applications depend on Internet electronic communications in order to work as intended, any restrictions to the ability of the application to exchange traffic with endpoints of the Internet will degrade its performance. The traffic exchange characteristics of the Internet access service may show such an application-specific behaviour. The application's traffic may either be blocked or throttled. Blocking prohibits any communication whereas throttling limits the throughput to a certain degree.

The main purpose of this chapter is to identify which kind of cases within this category could warrant the application of minimum QoS requirements according to Art. 22(3) USD.

5.1.1 Network effects and individual applications

The first relevant question to answer in this chapter is: why is it relevant to be concerned with issues concerning individual applications? One can argue that as long as there is no SMP, this is not something to worry about. However, due to the network effects, even the blocking of one single (popular) application can have far-reaching consequences. This mechanism will be explained and illustrated in this section.

Whereas a general degradation of access to the Internet as a whole is generally considered problematic, this may not necessarily be the case for the blocking and throttling of individual applications. And indeed, it could be argued that in a market situation where end users are in the position to choose between several ISPs, an ISP that introduces blocking or throttling of specific applications would harm its own attractiveness to end users. As a result, this ISP could be penalised by end users switching to a competing ISP that offers unrestricted Internet access open to all applications. If the majority of end users were to find such blocking and/or throttling undesirable, then ISPs could presumably no longer choose to continue these practices. The market would therefore correct the unwanted behaviour.

However, what should be done when this market mechanism does not suffice to address this problem? It is possible that a general practice occurs whereby (almost) all providers act in a similar way, especially in markets with characteristics of an oligopoly. If these providers do not have SMP, it will be impossible to address such a practice under the SMP regime that is part of the sector-specific regulation for telecommunications. In order to deal with the practice under competition law, there would need to be proof of a forbidden arrangement, which is generally hard to find.

The problem becomes even more serious because of the network effect that is inherent to the use of applications. When the usefulness of applications depends on the number of users of that application, the blocking or throttling by one ISP also has consequences for end users of a competing ISP that itself does not block the application. For example, if end user A has a subscription with ISP X that blocks a VoIP application, end user B that has a subscription with ISP Y – that does not block the same VoIP application – cannot reach end user A

through that application, regardless of its own subscription. Multiple end users can thus be harmed by the practice of even a single ISP.

In addition, switching generally comes at a cost, a cost which an end user might not immediately be willing to pay because of the throttling or blocking of one single or a few applications. Also, end users often have long(er) term contracts, and can thus not switch immediately when they are confronted with an unwanted practice. The combination of the network effect with an unwillingness or difficulty to switch, can potentially seriously hamper the business of the application provider. This is the case even when only one or a few ISPs block its application (depending on the size of the customer base of the ISP), and despite the fact that there still is a choice for end users to pick an ISP that does not block. Thus, in addition to potential harm for end users, the blocking and/or throttling of single applications could have a serious impact on the business case for application providers. This could have an adverse effect on innovation in the application market.

On a more general level, the argument could also be made that the *unreasonable*[55] blocking or throttling of a single application goes against regulatory objectives and the idea and success of an open Internet, and should on that basis be considered as unwanted behaviour.

5.1.2 Application performance and traffic management

The Internet access service relies on the packet forwarding mechanisms of the IP protocol and is today usually based on the best effort concept, which in general provides relatively good quality through some level of over-provisioning of network capacity. Traditional IP technology is not designed to allocate resources between end user sessions as is usually the case with specialised services.

IP networks can smooth short time traffic peaks by queuing IP packets in the routers.[56] Congestion[57] is the situation met in IP networks when traffic increases to a level where routers run out of buffer space and are forced to start dropping[58] some IP packets. By default, this is done randomly. Congestion in IP networks can occur in two ways:

- on an irregular basis, caused by unpredictable/unavoidable situations
- on a regular basis, caused by a failure to provide sufficient capacity[59]

The ISP uses traffic management mechanisms to optimise the flow of traffic within its network and to mitigate the level of congestion. 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.[60]

As described in chapter 3, BEREC uses the concept “traffic management” in a broad sense and include both technically implemented measures and measures that are not yet technically implemented but, for example, could be activated according to contract terms and conditions. Traffic management can be used to implement both restricting (e.g. blocking and throttling) and enabling (e.g. routing and traffic forwarding) measures.

The general principle used in the Internet is that the network layer should handle packet forwarding irrespective of the application the packets belong to. There are however feedback-based adjustments of the transmission rate at which packets are sent into the

[55] Criteria for reasonable and unreasonable measures are discussed in section 5.3.
[56] Queuing of IP packets will introduce some delay and jitter to the traffic flow.
[57] Computer Networks – A Systems Approach. Larry L. Peterson and Bruce S. Davie, Morgan Kaufman
[58] Applications using TCP at the transport layer will retransmitt lost IP packets.
[59] The NN QoS framework report contains a detailed elaboaration on congestion in IP networks.
[60] Overview and Principles of Internet Traffic Engineering, RFC 3272

network by endpoints, called congestion control.[61] These methods are applied in order to relieve the congestion in the network, but are mainly controlled by the end users.[62]

If an Internet access service is operated according to this principle, there will be no application-specific traffic management within the network. The performance of applications is dependent on the current state of the network, i.e. available transmission capacity. In best effort networks it is normal and unavoidable for the network to reach states of congestion from time to time.

In modern IP networks the congestion control function in the endpoints may be assisted by network-internal congestion management functions. This can be performed in an *application-agnostic* way or in an *application-specific* way. The latter is typically performed with Deep Packet Inspection (DPI) technology and may be used to throttle or block traffic from individual applications.[63]

ISPs also use traffic management to protect their networks from malfunctioning, which may have both external causes (e.g. hacker attacks) and internal causes (e.g. link failures). These measures are usually referred to as "network security and integrity". (N.B. this is not the same as "*information* security and integrity".)

- Network security consists of measures adopted by network operators to prevent and monitor unauthorised access, misuse, modification, or denial of the computer network and network-accessible resources.
- Network integrity consists of measures adopted by network operators to maintain or restore the level of performance during network failures, and mitigate or prevent service outages from network failures.

As described in section 3.3.1, differentiation of traffic has increasingly become used for Internet access service offers in recent years. Differentiation can, for example, be used for traffic *filtering* in order to stop denial of service attacks or to limit high volume data flows. It can also be used for *preferential* treatment of specific traffic categories, e.g. VoIP calls, during congestion periods.

Alternatively, differentiation of traffic can be implemented by general quality architectures[64] providing *multiple traffic classes* throughout the network of an ISP. In the future, it could possibly also be used for interconnection between different ISPs' networks.[65] In principle, these traffic classes can be flexibly populated from any application, since traffic is typically classified in endpoints or at ingress points where traffic enters the network, and routers implement multiple queues giving packets different forwarding characteristics.

5.2 Monitor/Identify: Are there situations that need attention?

When checking for degradation of service, NRAs can take a reactive approach, and choose to let the identification of relevant cases arise from concrete complaints from stakeholders. Or, NRAs can take a proactive approach and actively monitor Internet access services offered in the market to see whether there are cases that need extra regulatory attention. The combination of both approaches is also possible.

With a reactive approach, complaints received from stakeholders may represent an indication of a blocking or throttling incident that may need regulatory attention. Stakeholder complaints could be composed of individual cases of degraded application performance or of

[61] Congestion Control in the RFC Series, RFC 5783
[62] Some routers implement functions like for example Explicite Congestion Notification to assist congestion control.
[63] Detailed inspection of traffic may also concern privacy issues. This aspect is however out of scope of these guidelines.
[64] These quality architectures typically use DiffServ and/or MPLS
[65] The IP interconnection service *IP eXchange (IPX)* provided by GSMA is an example. www.gsma.com/ip-exchange/

more comprehensive reports of observations of blocking or throttling of traffic (e.g. measurement reports).

The proactive approach requires the NRA to have a strategy about what it is looking for. The NRA may predetermine a set of situations that are likely to occur (e.g. blocking of VoIP and throttling of P2P). This set would then be cross-checked against the IAS products offered in the market. Any incidents discovered will form the basis for further investigation (step 2).

The active monitoring can be done by checking the contracts and terms of use of IAS offers or by performing technical measurements of the IAS services themselves. While checking contracts etc. is a fairly easy and straightforward process, executing technical measurements is a rather complex endeavour.

Based on the set of situations defined, relevant measurement parameters (technical trigger points) with respective thresholds can be identified. This will result in specific measurement methodologies and test set-ups that can be applied. The basic principle is described in section 3.1.2.

In order to detect occurrences of application-specific blocking or throttling, the measurement methodology will either focus on the resulting application performance or it will measure the traffic exchange itself inside the network.

When measuring application performance a probe is connected to the IASes under consideration and the performance of a set of applications is recorded (e.g. the speech quality of a VoIP application). Explicit measurement of the traffic exchange of the IAS would typically be based on test traffic generated according to the relevant set of situations to be investigated (e.g. usage of specific protocols).

Irrespective of whether application performance or network performance measurements are used; the basic principle is the same: the performance between two reference points is measured. Probes are connected to these reference points initiating the measurement procedure, i.e. running applications or exchanging test traffic.

In order to avoid costly measurements, NRAs can also participate in broad cooperative measurement platform initiatives managed by third parties. Such platforms enable access to data from measurements performed by highly distributed test platforms.[66]

NRAs can also set-up a tailored proactive permanent monitoring system consisting of a number of measurement probes. These probes can be configured according to the set of situations to be investigated. Alternatively NRAs can involve end users by making measurement software available that can run on their end systems. The pros and cons of hardware and software based systems are discussed in section 3.1.2.

5.3 Assess situation: Is regulatory intervention needed?

In the second phase, the NRA will assess whether regulatory intervention is necessary and justified in the specific case. During this phase, the NRA will first assess whether the incident reported or detected really constitutes a “degradation of a service” and, second, whether this degradation runs counter to the regulatory objectives listed in the Framework Directive.

Art. 22(3) USD itself does not provide clear suggestions as to what criteria should be used when NRAs assess whether an incident needs regulatory intervention. The provision only states that the NRA should use the power to prevent “the degradation of service and the hindering or slowing down of traffic over networks”. Recital 34 of the Citizens Rights Directive

[66] E.g. M-Labs (www.measurementlab.net), SamKnows (www.samknows.com), RIPE Atlas (atlas.ripe.net)

states that NRAs should scrutinise ISPs' traffic management practices, in particular by addressing discriminatory behaviour. It also mentions that criteria for taking action are "detriment to consumers" and to "ensure that services and applications dependent on the network are delivered at a minimum quality standard".

Considering that some form of traffic management is necessary for ISPs to ensure smooth traffic forwarding in the IP network, the question for NRAs to answer is when does traffic management lead to "degradation of service"? This document does not give a straightforward answer but provides guidelines for NRAs to assess the severity of any given situation by considering a practice of itself and also in the context of the market.

5.3.1 Evaluation of monitoring data

With a reactive approach there may be a number of stakeholder complaints that need to be evaluated. It is likely that most complaints will be received from end users (including content and application providers) and that they will consist of reports of degraded application performance. The NRA will have a general understanding on what kind of degradation is considered to be non-critical and can be tolerated, and will filter complaints accordingly.

The NRA will need to check whether the complaints are related to subjective aspects, such as expectations or environmental influences, or whether the application itself actually is affected. Then, for each incident, the NRA will have to check whether the observed degradation is caused by traffic management of the IAS. There are several possible reasons for degraded application performance that are not related to the IAS performance, e.g. end user software and equipment, general unavoidable best effort performance variations or remote end user equipment.

A general method that detects whether application degradation is caused by the IAS can't be given a priori, because this depends on the specific application under consideration and the system it is used within (networks, equipment etc.). During the evaluation it will be important to understand the principle of operation and the interaction between the application and the network. In some cases explicit measurements may need to be performed in order to verify whether the degradation is caused by the IAS.

Complaints received from stakeholders with technical understanding (informed end users, ISPs, content and application providers) will usually be more detailed and may even include sample measurement results. These complaints are easier to handle and will probably only need to be validated to some limited extent.

Monitoring data received by the proactive approach will usually be more directly assessable since the measurements performed are specifically designed for the purpose, and the trigger points to look for are well understood beforehand.

Identifying *blocking* is easy since this will result in a non-working application. If other applications are running under normal working conditions on the same IAS, this clearly demonstrates a case of application-specific blocking. Identifying application-specific *throttling* is more complicated. However, in principle the same approach as with blocking has to be taken – the application under consideration is compared with the performance of other applications using the same IAS.[67]

In the case of application-specific throttling, the IAS is affecting the application performance by limiting the traffic exchange performance. Thus, the throughput of the traffic of different applications has to be measured and compared. It may be necessary to measure the

[67] An example of an exising tool of this kind is Glasnost (http://broadband.mpi-sws.org/transparency/bttest.php)

throughput of similar applications first or there may be reference data available. If the application under consideration receives a significant lower throughput than similar applications, this may signify a case of application-specific throttling.

ISPs will deploy and manage their networks according to the traffic load generated by the end users. The aim is to achieve a performance level that is sufficient to allow end users to run applications with adequate performance. To achieve this, ISPs use various traffic management methods. The basic concept is that transmission capacity is deployed at different network links according to the traffic load that is usually expected. This means that the ISPs need to perform statistical traffic measurements and adapt the capacity according to the continuously developing situation.

ISPs that do not follow up increasing traffic load with the deployment of additional network capacity will necessarily experience decreasing network performance. Some ISPs may let the available network capacity be unequally shared among end users and applications, for example by throttling traffic from applications that may generate high volumes of traffic in order to avoid deploying additional resources. This means that, during network congestion, applications encounter different throughput, i.e. traffic of specific applications may be prioritised or degraded.

From an end user's perspective the application performance is not necessarily severely affected since some applications may to some extent adapt to the limited network resources and give limited perceivable degradation to the end user. Even under heavy congestion when an application that is relatively insensitive to delays is throttled extensively this may be almost unperceivable as long as the overall functionality is not affected (e.g. a P2P file sharing application may be throttled temporarily to very low throughput without the end user being aware of it).

But applications may also be affected severely for reasons similar to the congestion situation described above. The ISP tries to share network resources among end users and capacity is allocated to end users according to a presumed usage profile. Deviation from the presumed profile (e.g. extensive use of high capacity-demanding applications) may be responded to with throttling of the respective traffic. The ISP may even block some traffic (and, in the worst case, also block in times of non-congestion).

Traffic management practices like the ones described above will be subject to thorough scrutiny by the NRA, as elaborated upon in section 5.3.2 "Assessment of the practice itself" below.

Differentiation of traffic

Positive prioritisation of applications also needs to be evaluated. It may be difficult to verify whether improved performance for some traffic actually constitutes a degradation of the performance of the *remaining* traffic. This is a question about which perspective it is seen from, from the higher or lower priority level. And, as explained in section 3.3.1, if general traffic classes are implemented for IAS, the relative performance of these classes needs to be evaluated. (Aspects regarding specialised services are not considered here - these were handled in chapter 4.)

Differentiation of traffic can be categorised as application-specific differentiation or application-agnostic traffic classes (priority levels). Application-specific differentiation involving *degrading* (blocking and/or throttling) of individual applications is the "standard category" and has already been extensively dealt with in this chapter. Application-specific differentiation involving *preferential treatment* needs to be evaluated based on the effect this may have on the rest of the traffic. If the performance of the rest of the traffic in fact

decreases over time, then such a practice may effectively constitute a *degradation* of the other traffic that does not receive preferential treatment.

Providing access with application-agnostic *traffic classes* (priority levels), need to be evaluated based on the effect higher priority traffic classes may have on lower priority classes. Like in the application-specific category above, decreasing performance over time for lower level classes may indicate that the existence of higher level classes effectively constitute a *degradation* of these lower level traffic classes. Another way of describing this is that higher priority levels may "squeeze" lower priority levels.

Furthermore, it is also important to consider who controls the differentiation practice. As described in section 5.3.2, *end user control* will often be seen as more reasonable than measures taken unilaterally by the ISP.

Priority marking of traffic may be performed in the broadband router (also referred to as "integrated access device" and similar terms), based on the contract between the end user and the ISP.[68] The end user's control will in such cases depend on the availability of different IAS offers to choose between; including conditions like pricing structure etc. (Pricing aspects are related to the assessment at the market level and are discussed in section 5.3.3.)

In the case of implementation of traffic classes on the content and application providers' side of the network, the BEREC draft report on *Competition issues related to net neutrality* provides a deeper analysis and some of these findings are referred to in the next section.

5.3.2 Assessment of the practice itself

The first thing an assessment should do is to help determine whether the practice in question significantly restricts the Internet access service. Several aspects have to be taken into account: the initiator of the practice and the goal that is pursued, and then the implementation and effects of this practice. These aspects must be strictly separated, as they highlight the difference between the motivation behind a practice, and the effect it has on the service offers.

Motivation for the practice

For the assessment criteria for reasonable traffic management practices, a distinction can first be made between objective and subjective justifications for traffic management, depending on the motivation of the initiator.

- Legal justification

  Objective justifications can be considered outside of the scope of control of the ISP. For example, a *court order* that requires an ISP to block specific content (e.g. because of copyright infringement) will qualify as an objective justification for an ISP to block. Similarly, a *legal act* (e.g. to block child pornography) will also deliver a justification to resort to traffic management, and hence not warrant regulatory intervention. Since the legal justification in these cases is normally apparent, these cases will not require a thorough investigation by the NRA.

- End user control

  An end user who asks their ISP to block some content, for example through parental control, also provides an objective justification for blocking, as long as this user's decision is well informed, can easily be rescinded and does not affect other end users. Traffic management practices that the *end user can control* will often be seen as more

[68] In the future detailed end user control may be performed by selecting which application software to install and run (and possibly also by configuring these applications). The software can mark the generated traffic with appropriate priority level in order to utilise the traffic classes offered by the ISP.

reasonable than measures that are taken unilaterally by the ISP, in light of the regulatory aim of avoiding harm to end users. However, the fact that an end user subscribes to a restricted service does not necessarily imply that these restrictions are approved or controlled by the user. Assessment of whether the end user really is able to control these measures depends on criteria such as what are the default settings and how easily can the settings be activated and deactivated?

Subjective justifications, on the other hand, lie within the scope of control of the ISP. As a result, they will require a more in-depth assessment by the NRA to be able to conclude whether the practice is problematic. Subjective justifications for traffic management could be, *inter alia*: congestion management, network security and integrity, spam control, but also incentives such as degradation of competitors' content. Despite the fact that all these reasons are within the control of the ISP, some can be more obviously considered legitimate than others.

- Congestion management

Congestion management is something ISPs have to do at times of high traffic peaks in the network, and could therefore even in some cases be qualified as having an objective justification. However, how the congestion management is implemented in practice, e.g. application-specific or application-agnostic, can result in different regulatory outcomes. ISPs should not be able to claim the use of congestion management as a reason to degrade a specific application if application-agnostic methods can be used instead. For that reason, ISPs should be transparent about their congestion management and, in case of a conflict, be able to show that their approach is proportionate, meaning that it remedies the congestion but does not go beyond that. Also, congestion management should not result in undue discrimination between content and application providers.

- Network security and integrity

Network security and integrity is another objective that in many cases could be considered legitimate, since the availability of the Internet access service depends on traffic management measures which protects the network. However, ISPs may try to claim that this objective also includes measures that in fact go beyond real network security and integrity, e.g. measures that are discriminatory or not proportionate. As with congestion management, any subjective justification would need to pass a proportionality and non-discrimination test.

In the absence of an objective or subjective justification, as mentioned above, NRAs could still come to the conclusion that a degradation of a specific application does not warrant intervention on the basis of Art. 22(3) USD, because this intervention would run counter to one of the other regulatory aims mentioned in Art. 8 FD, or because the imposition of minimum QoS requirements would not be proportionate considering the limited impact of the incident.

It is essential to determine which traffic management practices can be considered reasonable in order to verify which Internet access service offers can be categorised as unrestricted when the overall market situation is evaluated by the NRA. Measures justified along the lines elaborated above may in some cases give sufficient background to draw a conclusion. However, more complex situations occur, such as when ISPs provide *differentiated Internet access services* where some IP packets are transmitted in traffic classes with higher priority (ref. section 5.3.1).

When evaluating traffic management practices, they can be categorised based on *legal justifications, degree of end user's control, network security and integrity, congestion management and differentiation of services*, as discussed above. In addition to this, some

general principles are helpful when assessing how intrusive traffic management practices are in specific cases. In all situations, ISPs are bound to be transparent, according to the USD.

Implementation and effects

BEREC's draft report on *Competition issues related to net neutrality* underlines the fact that practices that restrict or prioritise traffic should, in general, be application-agnostic. In any case, they should not discriminate between content and application providers and should be based on objective criteria, such as consumption of resources. Otherwise, practices may have anti-competitive effects, harm end users or deter innovation.

The *efficiency* of the practice, regarding its goal, should also be assessed: it should be finely tuned so as to achieve exactly the pursued objective. It should also be *proportionate*, leading to as few side effects as possible. For example, if it is possible to manage congestion by throttling traffic, then it is less proportionate to block it, and if it is possible to use application-agnostic methods, then it is less proportionate to use application-specific methods.

These criteria help determine whether a traffic management practice appropriately pursues a legitimate goal or, on the other hand, if it is likely to be an anti-competitive tool or an inefficient response to a situation that could be dealt with another way. They are, however, not always sufficient to assess the need for a regulatory intervention.

The *effect* of the practice is also of great importance when assessing its impact. For example, blocking is a more severe degradation than throttling. Its frequency and its reach (i.e. the ratio of affected content among all content available) are also essential to define its intensity. However, intensity should be considered in a broad sense and with a long term perspective. BEREC's draft report on *Competition issues related to net neutrality* has emphasised indirect mechanisms that affect innovation, such as increased entry barriers that may prevent new applications from emerging on the Internet.

5.3.3 Assessment of the practice at market level

A traffic management practice that is suspected to lead to unjustified degradation when examined, must also be assessed at market level. Traffic management practices which do not fit the criteria mentioned above may lead to a restricted Internet access service, but it may not always be a problem at the market level if unrestricted offers are easily available.

Thus, it appears useful to consider the number of end users that are affected by the degradation, and their possibility to opt for an alternative unrestricted service, i.e. an offer with no unreasonable traffic management. For example, when the number of affected end users is low, the extent of degradation is lower, the imposition of minimum QoS requirements may not be proportionate. On the other hand, low penetration and/or low availability of unrestricted Internet access service offers indicates a more serious market situation.

BEREC's draft report on *Competition issues related to net neutrality* shows that, in a competitive market, ISPs also have incentives not to degrade their end users' traffic. There are however situations in which degradation may occur.

A provider with SMP, for example, may have an interest in slowing down its competitors' content. A vertically-integrated provider, which provides applications or content on the Internet, also has incentives to block or throttle competing offers. On the other hand, if this provider has limited market power in the retail market, then end users may easily switch ISP. However, there may also emerge a market situation where restrictive practices become widespread among ISPs, effectively limiting the possibility of end users to switch to alternative ISPs.

The market situation will be of serious concern when few unrestricted offers exist, or when switching from a restricted offer to an unrestricted offer is difficult. In particular, the price difference between the restricted and unrestricted offers must also be assessed as an element of the switching cost. If extensive use of unreasonable traffic management practices leads to restricted Internet access services with few available unrestricted alternatives in the market, then this will signify a serious degradation.

In the case of differentiated IAS offers, the price difference between these offers is of particular importance. If a very high price difference is found, this may *effectively* lead to unavailability, e.g. of unrestricted IAS offers. End users may also choose not to switch simply because of some kind of inertia (for example getting access to an application that is blocked is not considered a sufficient reason to switch when the hassle of the switching process is taken into account). Such situations would typically be reflected in low penetration compared to the availability of unrestricted IAS offers.

Taking all of these considerations into account provides the following set of questions for NRAs to look at when deciding whether there is a need for intervention:

List of criteria to assess the need for intervention	
Criteria to assess a practice *(Does the practice restrict Internet access?)*	**Criteria at market level** *(Is the practice a concern in the market?)*
• Level of end user control *(Who decides, and how? Is the restriction transparent?)* • Justification and implementation *(Is the motivation legitimate? Is it efficiently and proportionately implemented?)* • Discrimination *(Does the practice discriminate between CAPs?)* • Intensity *(Is the impact serious? Could it have long-term consequences?)*	• Availability and penetration of unrestricted alternatives *(Are there unrestricted IAS offers?)* • Easiness to switch *(Are end users effectively able to opt for an unrestricted IAS offer? Is the cost difference high?)*

Table 5.1 – Summary of assessment criteria

5.3.4 Decision on the need for regulatory intervention

Once a traffic management practice is suspected to constitute a situation of severe degradation, the process described above and summarised in Table 5.1 helps determine whether the degradation is problematic, by using two levels of assessment (i.e. the practice itself and the practice at the market level).

While this process does not specify explicit thresholds, it provides guidelines as to which criteria should be considered to assess the severity of the situation. There are no exact rules, but a higher number of criteria being met (*e.g.* low end user control, missing justification, discrimination, etc.) would indicate a higher severity.

If the outcome indicates a severe situation, both of the practice itself and within the wider market context, a regulatory intervention may be needed. At this point, there could be an

assessment of whether end users are no longer sufficiently able to run applications or access and distribute information of their choice with adequate quality.

An aspect that distinguishes evaluation of issues regarding *individual applications* on the Internet access service (chapter 5) from issues regarding the Internet access service as a whole (chapter 4) is the network effect. If the use of an application is restricted for some end users, this affects also the other users that are not directly affected themselves, because the latter will not be able to communicate with the former. The network effect therefore needs to be taken into account in cases covered by this chapter.

Comparing data on availability versus penetration of unrestricted Internet access service offers in the market may give an indication of whether unreasonable traffic management practices are clearly perceived by end users. While end users may not be sensitive to this situation in the short term, it actually reduces the incentives to innovation and in the longer term may lead to fewer new applications and content.

Summary – differentiated treatment of traffic within *IAS*

Blocking or throttling of specific applications by one ISP will also have consequences for end users of other ISPs who may face problems using these applications to reach end users of the restricting ISP (the network effect).

It is also important to understand how and why traffic management is being used?
*- What is its **true purpose**?*
*- Is it done in an **application-specific or application-agnostic** way?*
*- Is it done for reasons of **network security and integrity?***
*- Is there any **differentiation of traffic** and, if so, how? (i.e. through restrictions on specific applications, through preferential treatment, or by providing multiple traffic classes)*

Identifying if there are situations that need attention

*NRAs might take a **reactive approach**, acting on complaints from stakeholders such as end users or content and application providers, or they might take a **proactive approach to monitoring** situation(s) of particular interest.*

*NRAs need to monitor relevant situations. They can do this by checking the **terms and conditions of service offers available in the market** and by using **technical and statistical measurement methods**.*

Is regulatory intervention necessary?

The NRA will first assess whether the incidents reported or detected constitute a "degradation of service" and, if so, whether this degradation runs counter to the objectives set out in the regulatory framework.

In case the degradation of the IAS service is caused by a specific traffic management practice, the NRA will assess whether the practice should be considered reasonable or not, by considering:
- whether the motivation for it is legitimate
- whether the practice is proportionate to its objectives, and has any side-effects
- its impact in the context of the market, availability and penetration of unrestricted IAS

6. Determination of regulatory intervention

6.1 Introduction

In these guidelines BEREC has discussed technical, economic and legal aspects of net neutrality. It is fair to say that net neutrality is a set of dynamics covering much ground in these areas. It is at play in lively, interdependent but separate markets, subject to new usage patterns, and to expectations from end users. It is a moving target.

It is therefore very difficult to come to an exhaustive conclusion in these guidelines as to which specific situations constitute problems and which do not. Situations will often differ slightly, leading to different outcomes and effects. What has been done so far is drawing attention to which aspects should be kept in mind. It is up to NRAs to take these aspects into account and make an assessment of the situation. The outcome of such assessments should be the basis for [1] the decision to intervene, and [2] the type and extent of such intervention.

Again, as there cannot be an exhaustive ex-ante overview of all the situations requiring attention in their own respective ways, there is no way to specify every single relevant intervention in advance. Instead, the focus is on the preconditions that should be met before intervening. The situations could come in various types which are discussed below.

First, NRAs will have to establish which regulatory power(s) should be used. For the same situation, more than one power might be valid. Once a decision has been made to use minimum QoS requirements the substantive measure has to be drawn up. When doing so, NRAs must rely on general legal principles, policy objectives, and the implementation of article 22(3) in their Member State.

The goal of this chapter is to detail these legal aspects and discuss the specific application in light of net neutrality.

6.2 Proportionality

Proportionality is one of the general legal principles guiding NRAs in shaping any minimum QoS requirements. Following European legal doctrine, BEREC notes that any analysis of minimum QoS requirements must respect the principle of proportionality. This principle ensures that adopted measures are based on a fair assessment that properly balances the relevant interests. Regarding the policy objectives mentioned in the previous parts of these guidelines, the Framework Directive directly calls upon NRAs to operate inside the bounds of proportionality.

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, the proposed remedy could be more burdensome than strictly necessary. Likewise there should be a legitimate aim, with an objective justification.

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. However, the ECJ has considered whether measures are “manifestly inappropriate in terms of the objective which the competent institution is seeking to pursue”. Absolute effectiveness is not necessarily expected however (i.e. in the sense of being achieved in its

purest form). Following the wording of the ECJ, the test should instead be carried out inverted, so as to arrive at the conclusion that a measure is not manifestly inappropriate.

The next part of the proportionality test relates to necessity. This is a major part of the test, and assesses the need to invoke a certain measure. However important, it does not have a firm application framework though. Instead, 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.

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 measures 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 usually assess whether the legitimate aim is correctly defined. In the context of the power to impose minimum QoS requirements, the legitimate aim is already extensively described in the regulatory framework. As long as an NRA does not overstep the bounds of these aims, there should not be any problem.

6.3 Choosing regulatory tool

Once intervention is deemed necessary as a result of the degradation of the Internet access service observed and the context in which it occurs, NRAs should consider whether alternatives exist or imposing minimum QoS requirements is justified:

- If market mechanisms do not allow for easy switching to adequate alternatives, fostering competition and promoting ease of switching may be a sufficient response;
- If offers with adequate quality are still not available, it may be appropriate to consider imposing minimum QoS requirements.

The different regulatory tools may act independently or complementary to each other. They are detailed below.

6.3.1 Increasing competition and market efficiency

In a case where a provider holds SMP in the retail market and degrades Internet access service offers to its customers, the outcome may be that a large number of end users see their service degraded and have little to no possibility to change provider. In such situation, promoting competition, in particular through the specific SMP regime and measures dedicated to making switching easier, would be appropriate tools and may generate the greatest benefit to end users if these tools have not already been used to their full extent. However, in a clear SMP situation the NRA will probably already have exhaustively applied these tools.

In a competitive market some ISPs may invest in order to distinguish their offers from the competition. Market mechanisms will be all the more efficient to promote sufficient quality as end users are effectively able to opt for it. NRAs may promote such competition by increasing transparency about the quality which is effectively delivered to end users. The regulatory framework (articles 20 (1) and 22 (1) USD) allows NRAs to determine how this transparency should be ensured. This could help end users identify the offer delivering the level of quality that suits them best. Additionally, barriers to switching should be lowered to allow users to opt for the offer they prefer.

It may also be needed to consider whether there are other relevant tools available to the NRA under national law, for example, in terms of general quality requirements.[69]

6.3.2 Imposing minimum QoS requirements

Regardless of how well a retail market is functioning across several aspects, some situations may still require attention. The relevance of imposing minimum QoS requirements should be assessed based on its effectiveness, necessity and strict proportionality.

- *Effectiveness* requires that the minimum QoS requirements can reasonably be implemented by undertakings and are likely to remove or reduce degradation of Internet access service offers being available to end users.
- *Necessity* suggests that regulatory objectives are challenged because degradation of service has materialised, and other regulatory tools have been considered and deemed either insufficient or not able to be used fast enough to remedy the situation.
- *Strict proportionality* implies limiting the requirements to the adequate scope, and that the obligation imposed by the requirement is in proportion to the pursued aim. In particular, if specific ISPs offer degraded IAS services, then the proportionate requirements may focus on these ISPs in particular.

Also, in some cases it might be considered that fully implementing other regulatory tools will take too much time. Some risks identified in the previous chapters may need immediate response from the NRA. In those cases it may be necessary to establish minimum QoS requirements relatively quickly as a temporary measure.[70]

The first criterion when evaluating whether to impose minimum QoS requirements is the number of affected end users. No specific threshold of significance seems to be appropriate, *a priori*, but a relatively higher number may reflect a general failure of preventing "degradation" of the Internet access service to the market according to the criteria described in chapters 4 and 5.

Second, the level of degradation of IAS has to be evaluated. This assessment combines the availability of service offers with sufficient quality (in the case of IAS as a whole) or availability of unrestricted IAS (in the case of individual applications) and the price of these offers. Their price should be considered in comparison to the "degraded" offers, to identify the barrier faced by end users. In an extreme case, very expensive offers could be considered as equivalent to inexistent offers, although actual situations may be temporary.

Third, should ease of switching not be effectively offered by market mechanisms (in particular if minimum QoS requirements are seen as a temporary measure to cope with insufficient competition), this must be taken into account in the assessment of the availability of sufficient quality of IAS according to the criteria in chapters 4 and 5.

Combining these evaluations will enable an NRA to identify what are the grounds for imposing minimum QoS requirements. The NRA should assess the level of threat the situation poses to regulatory objectives: in particular, end users being offered a degraded Internet access service may have difficulty in accessing information of their choice, which impedes USD Art. 8(4)(g). As most applications provided on the Internet are designed to suit a majority of end users, it could be expected that they would evolve at the same pace as the global increasing of network performance, thus disadvantaging end users who do not benefit from this improvement. Here, in general, it can be underlined that a quality which is

[69] Example: There is a provision in Italian national law which allows the NRA to impose minimum quality requirements on all operators by a general regulatory act for the purposes of ensuring consumer protection. (Ref. Italian law no. 481/1995, Article 2, para 12, letter h.)

[70] Notwithstanding the fact that the Access Directive also provides for more immediate measures i.e. art 7(9) Framework Directive.

significantly lower than the level delivered by standard technologies is likely to undermine an end user's ability to access information of their choice.

6.4 Three dimensions of remedies

As shown before, there is a wide variety of issues that could occur in relation to net neutrality. At the same time, in order to achieve reasonable and proportionate measures, it is necessary to tailor regulatory remedies to the specific circumstances of the case. It is therefore important to set out several different dimensions along which remedies can be shaped. Three dimensions can be identified that seem to be useful in this regard.

The first distinction is between result and effort-based regulatory remedies. Result-based remedies specify a certain absolute criterion to be met. Effort-based remedies require the ISP(s) addressed by the remedy to comply so that the objective of the remedy is fulfilled as much as reasonably possible. Result-based remedies are relatively straightforward and compliance with them is easy to assess. However, in their strictness they could become too harsh, and no longer proportionate. In those cases, choose an effort based remedy could pose a viable alternative.

The next variation concerns the specific type of behaviour that is sought from the ISP(s). NRAs can require undertakings to either commit to a certain action, or to refrain from it. Instead of requiring an ISP to commit to a detailed set of actions, the opposite (requiring them to refrain from a few specific actions) may be much more efficient. In that respect, it is necessary to consider which way leads most effectively to the desired result.

Lastly, to enable NRAs to consider the substantive basis of the remedy, there is a distinction between qualitative and quantitative measures. Qualitative measures are requirements that propose a certain normative threshold to be met, while quantitative measures are generally of a numerical nature.

The proportionality test resonates in these three proposed variations. Setting the appropriate type of measure helps in making sure that the desired effect and perceived outcome of the remedy is in balance with the legitimate aim it is supposed to serve. Furthermore, necessity and effectiveness are served by making sure the leanest and most straightforward measures are being taken.

This overview is not intended as exhaustive, or as final. As a first guidance, these dimensions serve their purpose in guiding NRAs to tailor their remedies to the needs of the circumstances of the case. That is not to say that there may be other relevant dimensions that NRAs will be able to distinguish and successfully apply. BEREC welcomes the development of best practices and encourages NRAs to keep an on-going dialogue between them to share their insights.

6.5 Concrete examples of minimum QoS requirements

The wording of Art. 22(3) USD says that "in order to prevent the degradation of service" NRAs may set minimum QoS requirements on ISPs. This indicates that when a situation of degradation is identified through the comprehensive procedure described in these guidelines, the goal of the requirements is to prevent this degradation. The basic approach to this would be to require the ISP to improve the service quality until the degradation is eliminated.

The NRA could decide to impose minimum QoS requirements on just one undertaking or to more than one. It may also in some cases be reasonable to impose such requirements in general to all the ISPs in the market; or, at least, to those involved, in a direct or indirect way, in the degradation. In cases where requirements are imposed on more than one ISP there is an absolute need for a balanced, non-discriminatory and proportionate action.

Since the two categories - (1) the Internet access service considered as a whole and (2) individual applications using Internet access service - are very distinct, the appropriate requirements would need to be decided independently between these two categories.

In the category of degradation of the IAS as a whole, the most likely case would be that the ISP is providing specialised services at the expense of the IAS. An over-simplified approach would be to require ISPs to provide a similar increase in speed of the IAS as experienced with the specialised services has experienced. However, there may be specific reasons for improving the speed of specialised services, such as the introduction of new capacity-demanding services leading to a steep increase of network capacity. This kind of effect should of course be taken into account when setting the requirements.

The most prominent quality parameter is the access speed, which varies over time. But using statistical values, such as mean value and the 5 % and 95 % percentiles, would compensate for the statistical variation. The speed during peak hours is of particular interest, since this is when congestion is met in the network. Depending on how the degradation appears during the monitoring which takes place prior to the decision to intervene, it may be essential to specifically address performance during peak hours. Also, it may be necessary to specify other quality parameters, such as latency, jitter and packet loss, in the requirements.

Depending on which measurement tools are available to the NRA, it may be appropriate to require that the fulfilment of the minimum QoS requirements by the ISP is to be verified through a specific measurement platform. As discussed previously in this report, exact measurement of quality parameters in IP networks is complex, and referring to one specific set-up for verification increases the predictability and the comparability in cases where more than one ISP receive the same requirements. Depending on the footprint of the measurement platform, both the access and interconnection legs may be covered.

In the category of degradation of individual applications using Internet access service, more diverse cases are foreseen. In the case of blocking and/or throttling of single applications, a natural requirement could be to prohibit restrictions of the relevant application(s). However, the incentive for the original restriction by the ISP is probably related to the success of specific applications. Since all applications start as new and unknown, it is likely that some may grow to a similar success as those that may be restricted today. Therefore it may be relevant to prohibit application-specific restrictions on a general basis.

There is currently intense development within the area of application-agnostic congestion management[71], and such technologies are becoming more available and more effective as time goes on. Therefore, it may gradually become more and more relevant to consider requiring this kind of general application-agnostic measures from the providers.

As described in section 5.3.1, checking application blocking is straightforward, while checking application throttling is rather complicated. Therefore compliance with this kind of requirements may need specific measurement tools. In order to verify compliance with general application-agnosticism, it will be necessary to check of random applications (i.e. port numbers) and random destinations (i.e. test servers).

Another relevant case within the second category – differentiation within IAS – is the provisioning of restrictions and/or prioritisations of traffic for individual CAPs. (N.B. this case does not include specialised services.) If degradation is identified in such a case, there may be different options.

[71] For example IETF RFC 6057 and IETF Working Group Congestion Exposure (Conex), www.ietf.org

On the one hand, if the degradation identified consists of *blocking or throttling* of traffic from specific CAPs (traffic arriving on general transit or peering connections), it would be natural to require these restrictions to be removed. However, if it relates to the peering agreement of a direct interconnection between a CAP and an ISP, this is an aspect not considered within the scope of this report.[72]

On the other hand, if the degradation relates to traffic from specific CAPs as an indirect consequence of *prioritisation* of traffic from other CAPs, it may be appropriate to require that the performance of the degraded traffic (which most likely will be traditional best effort traffic) is improved to a sufficient level.

Intervention in the case of degradation of traffic from specific CAPs (one or more) will most probably be a result of a regulatory evaluation of a situation originally reported by the CAPs themselves. Experiences from these CAPs after the imposition of the requirements will give therefore valuable information to the NRA regarding compliance. However, a full regulatory evaluation may be needed in addition if the complaints from the CAPs are maintained.

Summary – Determining the regulatory intervention

Choose a tool *- once intervention is deemed necessary, NRAs need to select the regulatory tool most appropriate to the problem identified, choosing from among else* ***transparency*** *remedies,* ***competition*** *tools and Art 22(3) USD* ***minimum QoS requirements****.*

Criteria to help NRAs make this assessment:
- the number of impacted end users
- the availability of alternative packages on the market
- the ability for end users to switch easily to alternative packages

An NRA should apply the three-part proportionality test *(effectiveness, necessity and strict proportionality) to ensure that any obligations imposed by the requirement are proportionate to the pursued aim.*

Questions for an NRA to consider:
- should the requirements be imposed on ***one, several or all ISPs?***
- do the requirements relate to the ***IAS as a whole or differentiated treatment of traffic within the IAS?***
- in terms of the IAS as a whole, which aspects of QoS should be considered, e.g. average transmission rate (speed) or congestion level?
- in terms of differentiated treatment of traffic within the IAS, is it sufficient to prohibit the specific restrictions or should a more general application-agnostic requirement be used?
- how will the NRA ***measure QoS and verify compliance?***

[72] More information on this in the separate BEREC draft report on IP interconnection in the context of net neutrality

7. Notification of minimum quality of service requirements

7.1 The notification procedure pursuant to Article 22(3) USD

As elaborated in the previous chapters, if an undertaking or undertakings providing public communications networks causes the degradation of service, or the hindering or slowing down of traffic over networks and if the usage of alternative regulatory tools or measures is not/does not seem to be effective or applicable, NRAs are, pursuant to Art. 22(3), first sentence) USD, able to "…*set minimum quality of service requirements*…".

Furthermore Art. 22(3) USD stipulates a so-called 'notification procedure' vis-à-vis the Commission and BEREC. Thus, before setting any such minimum quality of service requirements NRAs shall provide the Commission, in good time 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 they impose.

Minimum quality of service requirements pursuant to Art. 22(3) USD have – at the time of publication - not been set by any NRA. Neither does a formal (legal) nor an informal detailed *modus operandi* in regard to the notification procedure (yet) exist. Hence a number of questions, taking into account the application of objective, transparent, non-discriminatory and proportionate regulatory principles, need to be clarified and agreed upon:

- How should the notification procedure be applied in practice?
- What is the scope of the notification procedure? Should it only apply if specified/individualised minimum quality of service requirements relating to a particular operator/particular operators are to be set? Or should/could it be applied as well when drawing up general minimum quality of service requirements that would affect every single provider of public communication networks?
- Should it be based on an already existing and well-established procedure, such as the Art. 7/7a FD-procedure?
- Should the notification procedure be of a more formal (legal) nature, e.g. established via a recommendation or guidelines of the Commission? In this case, what would be the concrete legal basis for such a recommendation or guidelines? Or should the procedure stay rather informal, e.g. staff working paper, and be adapted in due course, e.g. with a review and reassessment in two to three years' time?
- Irrespective of the nature of the notification procedure itself, what ought to be the (minimum) formal and material contents and requirements of the notification?

In order to ensure that these envisaged minimum quality of service requirements do not have an adverse effect on the internal market and on the objectives of the regulatory framework, as well as to ensure the effectiveness of cooperation between NRAs, the Commission and BEREC, it would seem appropriate to develop a clear, consistent and transparent regulatory practice with regard to the notification procedure.

BEREC notes that:

- so far, it has not proved necessary to set minimum quality of service requirements pursuant to Art. 22(3) USD and thus no experience/know-how in regard to the formalities and contents of the notification procedure yet exists;
- the wording of Art. 22(3) USD does not provide explicit details concerning the formal and material contents of the notification itself[73];
- such a notification is only to be expected if the setting of "*any such minimum requirements*", using Art. 22(3) USD as the legal basis, is considered the most appropriate regulatory remedy regarding the respective undertaking or undertakings providing public communications networks (at least for the time being); thus in other words, where the usage of alternative regulatory tools or measures is not/does not seem effective or (immediately) applicable;
- an NRA should be able to respond to an undertaking or undertakings efficiently.

Bearing these factors in mind, BEREC proposes an uncomplicated, short, transparent and uniform *modus operandi* for all NRAs to observe with regard to the notification procedure.

Such a pre-established *modus operandi* would not only ensure the development of a consistent regulatory practice in terms of setting minimum quality of service requirements and the timely implementation of regulatory measures; it would also enhance certainty for NRAs and market players as well. Furthermore, it seems clear that the initially established, notification procedure should be jointly reviewed and adapted by NRAs, the Commission and BEREC in due time.

BEREC's views of the necessary minimum formal and material requirements of the Art. 22(3) USD notification procedure shall be elaborated in more detail under 7.2.

7.2 BEREC's proposal for a notification procedure

BEREC suggests the establishment of a 'standard notification form', which shall, in its introduction part, provide a brief and clear summary of the formal and material issues of the notification procedure and which shall further encompass a pre-structured form-sheet, to be filled out by the respective NRA.

7.2.1 Minimum requirements in regards to formal issues

In regards to formal notification issues Art. 22(3) USD outlines that:

- NRAs shall provide the Commission, in good time before setting any such requirements;
- this information shall also be made available to BEREC;
- the Commission may make comments or recommendations thereupon;
- NRAs shall take the utmost account of the Commission's comments or recommendations when deciding on the requirements.

The wording concerning the formal aspects of the notification procedure is rather vague and non-specific. In particular, it does not put forward any exact timeframes or obligations for the respective NRA and/or the Commission. Therefore, this leaves room for various interpretations such as:

- How should the respective NRA inform the Commission?

[73] In contrast to the procedure outlined in Art 22(3), see the much more detailed notification procedure of Art. 7/7a FD: The formal and material contents of the procedure itself are defined to a large extent within the respective legal article. In addition, this notification procedure is further elaborated in the *Commission Recommendation of 15 October 2008 on the Notifications, Time Limits and Consultations Provided for in Article 7 of Directive 2002/21/EC of the European Parliament and of the Council on a Common Regulatory Framework for Electronic Communications Networks and Services, C(2008) 5925 final*.

- How, when and by whom should BEREC be informed? What, if anything, is further expected from BEREC - material contributions, such as technical expertise, or 'merely' keeping an eye on the notification procedure itself?
- What is to be understood by the term "in good time"? In other words, what would be the absolute shortest timeframe for an NRA to inform the Commission before setting the envisaged requirements?
- What is the (maximum) time-limit if the Commission decides to make comments or recommendations? How long should an NRA wait for a response from the Commission? Could a lack of response from the Commission within the given timeframe be given to mean that the Commission has no concerns or comments and the NRA can thus impose its minimum quality of service requirements?[74] Does an NRA actually need to wait until it gets a response from the Commission before setting the requirements, i.e. should there be some kind of stand-still-time? Or may a NRA set (draft) measures (e.g. in response to an urgent situation) before the Commission makes comments or recommendations?

Since there exists no practical experience for the setting of minimum quality of service requirements, BEREC suggests a prudent approach regarding the formal issues of the notification procedure:

- The communication between the respective NRA and the Commission should take place via the Communication and Information Resource Centre for Administrations, Business and Citizens (CIRCABC)[75]. CIRCABC is a well-established communication tool and since it works as point-of-contact for the Art. 7/7a FD-notification procedure all NRAs are familiar with it. Also, BEREC should be informed via CIRCABC of the envisaged minimum quality of service requirements and CIRCABC could be the means to do this.
- Regarding the timeline between providing the Commission "in good time" with the necessary material information (see 7.2.2) for setting minimum quality of service requirements and finally setting/deciding on the envisaged minimum quality of service requirements (having taken utmost account of any comments or recommendations of the Commission) BEREC suggests a flexible approach for the time being - BEREC recommends that the respective NRA should explain in the second part of the standard notification form (see 7.2.2) its timeframe for implementing the minimum quality of service requirements and give reasons (e.g. the urgency of the case). After gaining some experience, it may be possible to review the procedure and set standard timeframes, e.g. one month as a standard timeframe.

  In this context, it should be pointed out that – in comparison to the notification procedure of Art. 22(3) USD – the much more comprehensively Art. 7/7a FD-notification procedure distinguishes between timeframes to adopt the resulting draft measure from one month to a maximum of three months (according to Art. 7) or six months (according to Art. 7a). BEREC believes that at this stage such a demanding procedure and timelines are inappropriate in the scope of the Art. 22(3) USD notification procedure.
- The respective notification should be in any official language of the European Community. Any comments or recommendations made by the Commission should be in the language of the notified quality of service requirements.[76]
- With regard to BEREC's position/role during the notification phase, BEREC proposes a pragmatic policy. Besides being informed via CIRCABC, BEREC could for example

[74] Similar to the *modus operandi* of the Art. 7/7a-FD-procedure.
[75] See also the CIRCABC website for more information: https://circabc.europa.eu.
[76] Regulation No. 1 determining the languages to be used by the European Economic Community: http://eur-lex.europa.eu/LexUriServ/site/en/consleg/1958/R/01958R0001-20070101-en.pdf.

contribute, if it deems this necessary and depending on the concrete circumstances of the specific notification as well as on the evolving situation during the notification phase itself, via a non-binding opinion. Such an opinion could in particular analyse whether the guidelines on minimum quality of service requirements, elaborated in this document, are (correctly) applied.

7.2.2 Minimum material elements of the notification

As stated in Art. 22(3) USD, NRAs shall provide the Commission *"…with a summary of the grounds for action, the envisaged requirements and the proposed course of action.*"

These material requirements of the notification procedure that should be made available to the Commission shall be structured accordingly and encompass the following details:

1. The relevant facts and circumstances of the respective case that have led to the minimum quality of service requirements on an undertaking or undertakings providing public communications networks.
2. An assessment of the case, shall be given and especially its effects on the policy objectives pursuant to Art. 8 FD (*ergo* legitimate aim)[77].
3. A description of the proposed minimum QoS requirements and a justification for why they do not adversely affect the functioning of the internal market (*ergo* minimum intended effect);
4. An explanation of how the proposed minimum QoS requirements meet the so-called 'proportionality test'[78], stating clearly how the proposed minimum quality of service requirements:
    - constitute an effective means to realise the aims pursued by the requirements (*ergo* test of effectiveness);
    - are necessary to achieve the relevant aims – i.e. that no alternative and less intrusive measures are available (*ergo* test of necessity and subsidiary); and
    - a reasonable/fair balance has been found between the aims pursued by the proposed minimum quality of service requirements and any interests impacted by them (*ergo* test of proportionality in the strict sense/ proportionality *stricto sensu)*.
5. The provisional timeframe for implementing the minimum quality of service requirements and the method to enforce/control them.

Additionally – although not foreseen by Art. 22(3) USD - BEREC suggests that the respective NRA communicates the final measure to the Commission. This seems reasonable and could be regarded as a form of 'good practice'.

In order to ensure a clear, consistent and transparent regulatory practice BEREC believes that it could be helpful for NRAs to rely on these elaborated minimum requirements in regards to material issues when notifying the Commission of the to be set minimum quality of service requirements.

---

[77] Art. 8 FD states: "*...Member States shall ensure that in carrying out the regulatory tasks specified in this Directive and the Specific Directives* [= USD]*, the national regulatory authorities take all reasonable measures which are aimed at achieving the objectives set out in paragraphs 2, 3 and 4. Such measures shall be proportionate to those objectives. ...*"

[78] *"… 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 aim. …*": *Commission Guidelines on Market Analysis and the Assessment of Significant Market Power under the Community Regulatory Framework for Electronic Communications Networks and Services*, 2002, para.118.
For more detailed information regarding the principle of proportionality see also: BEREC, *A Framework for Quality of Service in the Scope of Net Neutrality*, December 2011, pp. 40 cont.

Glossary

Art	:	Article
AD	:	Access Directive
BEREC	:	Body of European Regulators for Electronic Communications
CAP	:	Content and Application Provider
CDN	:	Content Delivery Networks
CEPT	:	European Conference of Postal and Telecommunications Administrations
CIRCABC	:	Communication and Information Resource Centre for Administrations, Business and Citizens
DiffServ	:	Differentiated Services
DPI	:	Deep Packet Inspection
ECJ	:	European Court of Justice
EC	:	European Community
EU	:	European Union
ETSI	:	European Telecommunications Standards Institute
FCC	:	Federal Communications Commission
FD	:	Framework Directive
HD	:	High Definition
IANA	:	Internet Assigned Numbers Authority
IAS	:	Internet Access Service
IETF	:	Internet Engineering Task Force
IP	:	Internet Protocol
IPTV	:	Internet Protocol Television
ISOC	:	Internet Society
ISP	:	Internet Service Provider
ITU	:	International Telecommunication Union
ITU-T	:	International Telecommunication Union – Telecommunications
kbps	:	Kilo Bits Per Second
M-Lab	:	Measurement Lab
MOS	:	Mean Opinion Scores
MPLS	:	Multiprotocol Label Switching
NN	:	Net Neutrality
NNTP	:	Network News Transfer Protocol
NP	:	Network Performance
NRA	:	National Regulatory Authority
P2P	:	Peer-to-Peer
OECD	:	Organisation for Economic Cooperation and Development
QoE	:	Quality of Experience
QoS	:	Quality of Service
RFC	:	Request for Comments
SIP	:	Session Initiation Protocol
SMP	:	Significant Market Power
SMS	:	Short Message Service
SMSoIP	:	Short Message Service over IP
SMTP	:	Simple Mail Transfer Protocol
TCP	:	Transmission Control Protocol
TV	:	Television
UK	:	United Kingdom
US	:	United States
USD	:	Universal Service Directive
VoD	:	Video on Demand
VoIP	:	Voice over Internet Protocol