Vendor input draft BEREC Net Neutrality guidelines

Cisco, Ericsson and Nokia welcomed the adoption of the EU Net Neutrality Regulation (the TSM Regulation). We have throughout the process supported a ban against blocking and anti-competitive behaviour and we believe the Regulation as agreed by the European legislators struck a reasonable balance between protecting rights of end-users of Internet access services (IAS) and ensuring freedom to continue to innovate and develop new services.

We are therefore concerned to see some of the language in the draft BEREC guidelines, which could skew this balance and which risks introducing restrictions and conditions above and beyond those contained in the Regulation. Our concerns centre around three key issues:

- technology mandates for how to deliver specialised services
- limitation on the kind of services that can be delivered as specialised services
- additional restrictions for what constitutes reasonable traffic management

Specialised services

The issue: logically separated and strict admission control

Paragraph 106: *"…It is understood that specialised services are offered **through a connection that is logically separated** from the IAS to assure these levels of quality. The connection is characterised by an extensive use of traffic management in order to ensure adequate service characteristics and **strict admission control**."*

How it goes beyond the Regulation: creates technology mandates

- This language was included in the European Parliament's definition of a specialised service. However, during negotiations between the European Parliament and the Council of Ministers, a political decision was taken *not* to include this definition precisely on the basis that there are several ways in which these services can be delivered, thereby avoiding limiting the kind of services that can be delivered as specialised services.
- There is consequently no legal basis in the Regulation for introducing such technology mandates in the BEREC guidelines. The BEREC guidelines should implement what was politically agreed and should not introduce further obligations above and beyond that.

The risk: Limits specialised services to video and real time

- Logical separation and strict admission control are methods used to deliver some specialised services but they are not the only ways.
- Logically separate connections implies a level of demarcation of network resources that may not always be true nor necessary in order to deliver a specialised service without it having a negative impact on IAS. Some services will be delivered through mechanisms that would arguably be "logically separate" connections, e.g. IPTV through multicast.
- However, other in particular future services may be delivered on shared interfaces where it is not clear whether that would qualify as logically separate. For instance, it could be imagined in the future emergency services are delivered as specialised services but as rarely used, there will be no need to implement logically separate connections. In the event the service will be used it will be set up to automatically get priority.

Another example could be online gaming through peer-to-peer (P2P) set up to automatically download resources overnight when there is available capacity.

- Additionally, there is already a trend in current deployments towards "single-IP", using a single IP address per user and a single VLAN construct for the plurality of its services, using Ethernet, IP and TCP/UDP parameters for traffic class differentiation, but not using logical separation.
- Admission control is one specific delivery method for the kind of services that would likely be specialised services under the Regulation. There are two reasons for implementing strict admission control. The first is to ensure the user is authorised to use the service. The second is for network resources. This mechanism is therefore mainly used for services that require specific and/or high rates, namely real-time video and voice.
- Other services which could be delivered as specialised services do not require specific and/or high rates, e.g. home health care, smart grid management and home surveillance, and are therefore not delivered with strict admission control. This does not mean they may not need to be delivered as specialised services for reliability and a mandate to apply strict admission control could impede such services to be offered.

- **Recommendation for alternative wording**

Paragraph 106: delete

Justification

As explained above, there is no legal basis in the Regulation for introducing technology mandates. Such mandates are not necessary to ensure compliance with the safeguards around the provision of specialised services vis-à-vis IAS and could prejudice new ways of delivering services. The paragraph should therefore be deleted.

The issue: verification that specialised service could not be delivered over IAS

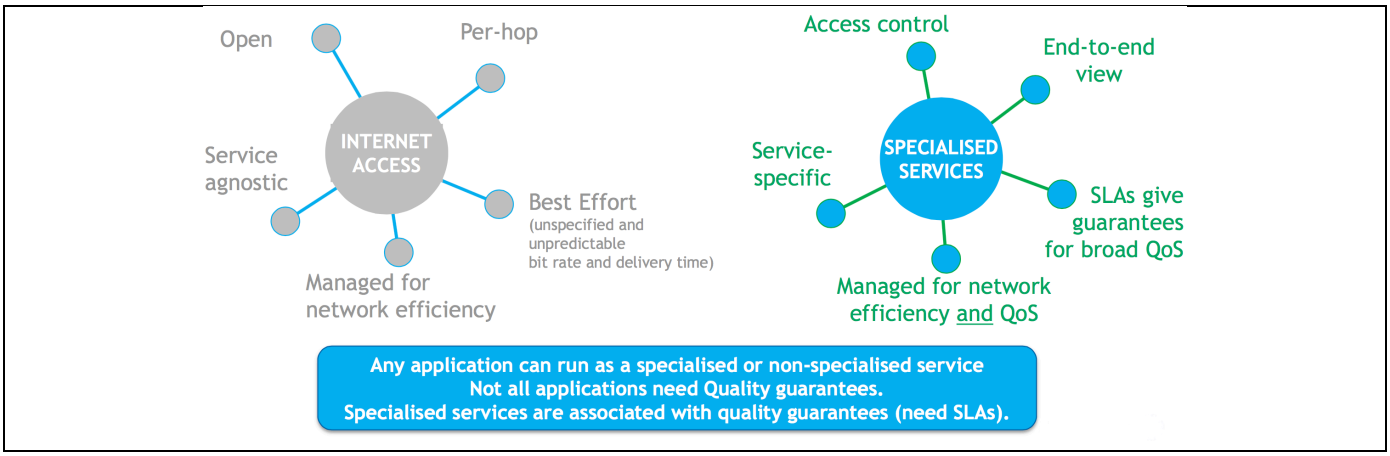
Paragraph 101: "*NRAs should "verify" **whether the application could be provided over the IAS at the agreed and committed level of quality**, and whether the requirements are plausible in relation to the application, or whether they are instead set up in order to circumvent the provisions regarding traffic management measures applicable to IAS, which would not be allowed*."

Paragraph 107: "*NRAs should verify whether, and to what extent, optimised delivery is objectively necessary to ensure one or more specific and key features of the applications, and to enable a corresponding quality assurance to be given to end-users. To do this, the **NRA should assess whether an electronic communication service, other than IAS, requires a level of quality that cannot be assured over an IAS.** If not, these electronic communication services are likely to circumvent the provisions of the Regulation and are therefore not allowed.*"

How it goes beyond the Regulation: creates new condition above and beyond "no circumvention" safeguard

- It interprets the wording that the optimisation has to be necessary in a manner to mean only services where the level of quality could not be achieved through an Internet access service (IAS) can be delivered as specialised services.
- This implies there are some services, which cannot be delivered as specialised services. This is in direct contradiction to the Regulation that clearly says ISPs, and providers of content, applications and services, are free to offer such services.

- It is not about whether there is one level of quality that responds to all end-users' needs and demands. IAS is inherently best effort (unpredictable bitrate and unpredictable time). For many services they could be accessed through an IAS or be delivered as a specialised service. In the former case the end-user may experience a good quality service most of the time. However, if for the end-user reliability or assured levels of quality (specific QoS attached to it) are needed or desired, the service inherently needs to be delivered as a specialised service as this goes beyond the best effort nature of IAS. Moreover, only services delivered as specialised services can offer end-to-end Service Level Agreements to end-users.

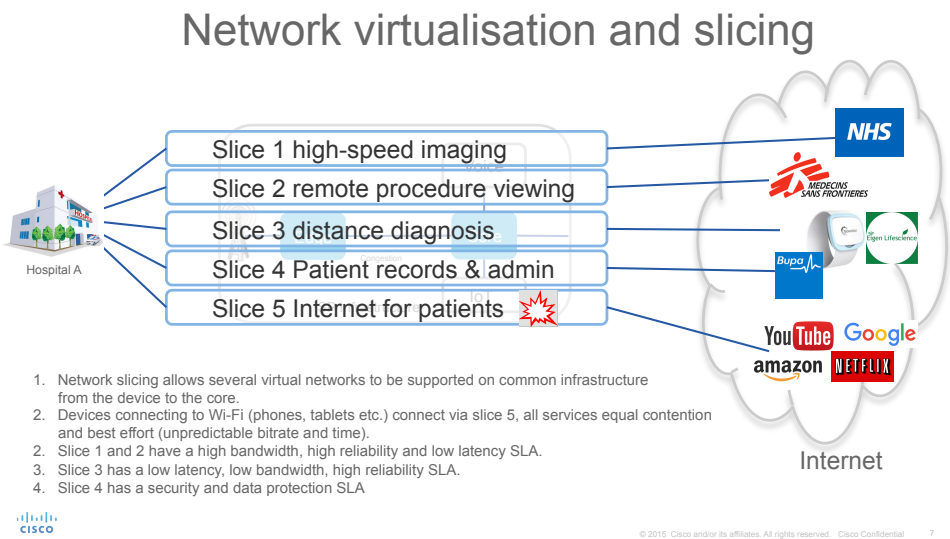


- The language in the Regulation that this optimisation has to be necessary to meet a specific level of quality is explained clearly in recital 16 to be a safeguard against specialised services being used to circumvent the traffic management and non-discrimination rules for IAS: "*…to enable a corresponding quality assurance to be given to end-users, rather than simply granting general priority* over comparable content, applications or services available via the Internet access service and *thereby circumventing the provisions regarding traffic management applicable to the Internet access service*.
- Introducing an additional requirement that only services where the regulator deems the quality is not "good enough" through the IAS creates a significant new restriction on what may be delivered as a specialised service and for which there is no legal basis for in the Regulation.

The risk: limits specialised services to those not already delivered as best effort services

- The restrictive interpretation in the guidelines of this provision not only risks contradicting the Regulation, it risks severely hampering the development and offering of new innovative services, incl. within IoT, for those end-users (consumers and businesses) who would like additional added value, quality, functionality and/or end-to-end Service Level Agreements that they are not able get over IAS.
- Any service which could also be accessed through an IAS risks being precluded from being offered as a specialised service, e.g. audio-visual content. Accessed through IAS, content is delivered sometimes SD, if available capacity and dependent on end-user IAS contract sometimes HD, sometimes there may be buffering. If access as a specialised service, e.g. through IPTV or bundled package, the user will instead get HD or UHD 4K/8K quality, high availability, reliability, fast channel-change.
- Another example is videoconferencing. Through an IAS, video resolution, quality and availability may vary (while meeting many end-users needs). For end-users, in particular professional and business users (like teleworkers), videoconferencing as a specialised service on the other hand provides reliability, higher availability, HD or even UHD video quality and high voice quality.

- VoLTE is another example of a service, which is already an essential part of mobile networks and services today but around which para 101 and 107 create unnecessary uncertainty. This is because in principle an end-user could also use any other VoIP application through its mobile broadband as a best effort service. However and in particular in the mobile space, the quality and availability as a best effort service is variable as opposed to a managed VoLTE service . A VoLTE service offers a significantly higher reliability and voice quality and is also the only IP voice service that can provide emergency calling.
- It is also not clear what the impact would be on services which run over an IAS and which could still require optimisation as a specialised service, mainly in area of home IoT applications. The large majority of these running over the IAS may not need any optimisation in order to deliver the relevant service to a satisfactory level, but others, such as home security solutions, will very likely require optimisation while running over the IAS.
- Further, with network virtualisation through slicing, it is expected in the future that the provision of Internet connectivity will merge with services to accommodate specific needs or business models with predictable service quality per slice (5G and access networks). For instance, through slicing using SDN and NFV, a bank can procure a service that both provides secure access to its IT domains, enables fast trading and transaction systems, bulk load data bases etc., while providing Internet access to employees and customers. Similarly, through same technology, a hospital can secure high-speed imaging, remote procedure viewing and control and patient doctor Internet diagnosis services while providing Internet access to employees and patients.



➢ **Recommendation for alternative language**

Paragraph 101: "NRAs should "verify" whether the application ***is delivered*** ~~could be provided over the IAS~~ at the agreed and committed level of quality, ~~and whether the requirements are plausible in relation to the application~~, or whether they are instead set up in order to circumvent the provisions regarding traffic management measures applicable to IAS, which would not be allowed."

Paragraph 107: "NRAs should verify whether, and to what extent, optimised delivery is objectively necessary to ensure one or more specific and key features of the applications, and to enable a corresponding quality assurance to be given to end-users. ~~To do this, the NRA should assess whether an electronic communication service, other than IAS, requires a level of quality that cannot be assured over an IAS.~~ If not, these electronic communication services are likely to circumvent the provisions of the Regulation and are therefore not allowed."

Justification

As detailed above, the additional test that only services which cannot provide the "assured level of quality" seems to imply there is one level of quality that a service "inherently needs". But the level of quality needed or demanded may depend on the end-user. The wording on the necessity of optimisation is clearly explained in recital 16 to constitute a safeguard against specialised services being used to circumvent traffic management and non-discrimination rules in the provision of IAS. When an end-user asks for a specific level of quality, optimisation is necessary as services accessed over an IAS is inherently best effort. It is then up to the ISP to assess ex ante if the QoS requirements they are selling are plausible. If they are not plausible and they are subsequently not being able to demonstrate that they have delivered to the agreed level of quality, the service may indeed be in breach of the Regulation.

The issue: VPNs and specialised services

Paragraph 11: "*Regarding virtual private networks (VPN) network services,* ***these are typically provided by the ISP to anyone that wishes to enter a contract about the provision of such a service, and these would therefore typically be considered to be publicly available.*** *The term 'private' describes the use of such a service which is usually limited to endpoints of the business entering the contract and is secured for internal communications.* ***In accordance with Recital 17, to the extent that VPNs provide access to the internet, they are not a closed user group and should therefore be considered as publicly available ECS and are subject to Articles 3(1)-(4)****. VPNs are further discussed in paragraph 111.*"

Paragraph 111. "*Business customers often request services relating to virtual private networks (VPN), which are also discussed in paragraph 11 above. The term VPN can be used in relation to two different types of services:*

- *"VPN* ***application****": A VPN application is typically used in the context of teleworking****. A computer (e.g. an employee's laptop) uses the public internet*** *to connect to corporate services. In order to protect the information transferred, a VPN* ***application on the client*** *encrypts all traffic* ***between the VPN client and the VPN server and typically sends all traffic to a VPN concentrator*** *located within the corporate network.* ***Both ends - the client and the concentrator - use an IAS, and this would therefore not be a specialised service.***
- *"VPN network service": A VPN network service is typically used to provide a private connection between a number of sites (e.g. different locations of a corporation). Such VPN services are typically implemented over common infrastructure with IAS (e.g. based on MPLS[22]). Such services are provided in parallel with IAS. As long as the services comply with the requirements set out in the Regulation, they are considered to be specialised services.*"

How it goes beyond the Regulation: limits the kind of VPNs that could be delivered as specialised services

- It is <u>not clear what the intention is behind the paragraphs on VPNs. The Regulation does not regulate specific services, including business services such as VPNs</u>.
- If the purpose of paragraph 11 is to clarify recital 17, the paragraph appears to confuse the question whether a service is an ECS or an IAS for the purposes of the Net Neutrality Regulation. Regardless whether VPNs constitute a publicly available ECS or not, it is not an Internet access service even if it does provide access to the Internet. That is clearly stated in recital 17 of the Regulation: "*However, the mere fact that corporate service such as virtual private networks might also give access to the Internet should not result in them being considered to be a replacement of the internet access services…*"

The risk: prejudices the development and offering of new types of corporate VPN offerings

- By taking a narrow and static view of what a VPN is (an application or a service), who provides VPNs, and how they are delivered risks prejudicing developments in new ways of delivering corporate services, incl. VPNs.
- VPN services are for instance not typically provided by ISPs, they are offered by many service providers. They could or could not use the public internet depending on how networks are connected and the routing tables. The assumption there is a clear-cut distinction between VPNs that only use an Internet access service or are delivered in parallel with an Internet access service is not reflective of technological developments.
- VPNs could be delivered as specialised services to ensure higher availability and offer a full end-to-end Service Level Agreement for people to work in the best conditions possible remotely, including over Internet access services e.g. cloud-based VPNs targeted towards SMEs with SLAs.

➢ **Recommendation for alternative language**

Paragraph 11: "Regarding virtual private networks (VPN) network services, ~~these are typically provided by the ISP to anyone that wishes to enter a contract about the provision of such a service, and these would therefore typically be considered to be publicly available. T~~the term 'private' describes the use of such a service which is usually limited to endpoints of the business entering the contract and is secured for internal communications~~. In accordance with Recital 17, to the extent that VPNs provide access to the internet, they are not a closed user group and should therefore be considered as publicly available ECS and are subject to Articles 3(1)-(4). VPNs are further discussed in paragraph 111~~."

111. "Business customers often request services relating to virtual private networks (VPN), which are also discussed in paragraph 11 above. The term VPN can be used in relation to two different types of services:

- "VPN ~~application~~ **service**": A VPN ~~application~~ **service** is typically used in the context of teleworking~~. A computer (e.g. an employee's laptop) uses the public internet~~ to connect to corporate services. In order to protect the information transferred, a VPN ~~application~~ **service** ~~on the client~~ encrypts all traffic ***between the VPN client and the VPN server*** ~~and typically sends all traffic to a VPN concentrator~~ located within the corporate network. ~~Both ends - the client and the concentrator - use an IAS, and this would therefore not be a specialised service.~~ Such services can be provided using an IAS or in parallel with IAS ***as specialised services***.
- "VPN network service": A VPN network service is typically used to provide a private connection between a number of sites (e.g. different locations of a corporation). Such VPN services are typically implemented over common infrastructure with IAS (e.g. based on MPLS[22]). Such services are provided in parallel with IAS. As long as the services comply with the requirements set out in the Regulation, they are considered to be specialised services."

Justification

There are various VPN services and network services provided by ISPs and service providers. As non-IAS, they provide reliability, higher availability, added value quality and fulfil end-to-end Service Level Agreements.

Reasonable traffic management

The issue: permanent and recurring traffic management not reasonable traffic management

Paragraph 70: *"This does not prevent, per se, a trigger function to be implemented and in place (but with the traffic management measure not yet effective) on an on-going basis inasmuch as the traffic management measure only becomes effective in times of necessity. Necessity can materialise several times, or even regularly, over a given period of time.* ***However, where traffic management measures are permanent or recurring, their necessity might be questionable and NRAs should, in such scenarios, consider whether the traffic management measures can still be qualified as reasonable within the meaning of Article 3(3) second subparagraph****."*

How it goes beyond the Regulation: creates new limitation on reasonable traffic management

- Reasonable traffic management is clearly defined in recital 9: It is transparent, proportionate, not based on commercial considerations but based on the objective technical requirements of different kinds of traffic.
- Stating that permanent traffic management cannot be considered reasonable has no legal basis in the Regulation and it seems to be based on the assumption that traffic management is only in place to deal with congestion that happens due to lack of capacity.
- Reasonable traffic management is about how networks are configured to enable the most efficient use of network resources and to increase overall transmission and throughput rates for the different kinds of traffic. It is not something, which is "switched on and off".
- For that reason, the Regulation does not contain any duration, timing or congestion-based conditions on when reasonable traffic management measures can be put in place. The guidelines should remain within the scope of the Regulation and not create new conditions which risks to undermine the sound language in Art. 3(3) second subparagraph and recital 9.

The risk: creates new restriction that could undermine automated network management

- The need to maintain the Regulation's language is only increasing as networks are becoming more and more automated. Machines will define when network hits levels of congestion that require automated traffic management techniques to be deployed. In mobile networks for example, while developments move to 5G, service differentiation, automation and increased flexibility, new advanced network technologies like multi antenna and device to device communications will only increase the continuous need for network management, independent of network capacity.
- There is no trade-off between capacity and traffic management as implicit in the draft guidelines. While investments into network capacity will be needed to support the exponential growth in IP traffic, more capacity will not reduce the need for traffic management, nor will it address latency, throughput and jitter needs for services and applications. With digitisation and IoT, networks will become more complex as they will be supporting a significantly wider range of services and applications. The technical requirements of packets will become increasingly heterogeneous and management of networks will consequently be imperative to enable delivery of all of these services according to their individual technical needs.
- To enable on-going network management while keeping with the principle of proportionality it should therefore be made clear that the Regulation language that traffic management measures should not be maintained for longer than necessary refers to the *effects* of traffic management.

➢ **Recommendation for alternative language**

70. This does not prevent, per se, a trigger function to be implemented and in place (but with the traffic management measure not yet effective) on an ongoing basis inasmuch as the traffic management measure only becomes effective in times of necessity. Necessity can materialise several times, or even regularly, over a given period of time. However, where traffic management measures are ***implemented in a manner which maintains the effects hereof on a*** permanent ***basis and not just in times of necessity*** ~~or recurring~~, their necessity might be questionable and NRAs should, in such scenarios, consider whether the traffic management measures can still be qualified as reasonable within the meaning of Article 3(3) second subparagraph.

Justification

As stated above, there is no basis in the Regulation for this language and it contradict the technical realities of how networks are managed and operated.

For further information, please contact:

Cate Nymann
Manager, Government Affairs
Cisco
+32 (0)495279886
cnymann@cisco.com

Walter van der Weiden
Director, European Affairs
Ericsson
+32(0)496862233
walter.van.der.weiden@ericsson.com

Florian Damas
Director, Policy & Regulatory Affairs
Government Relations
Nokia
+32 (0)477960544
florian.damas@nokia.com