# Response to the consultation of the draft BEREC Guidelines on common approaches to the identification of the Network Termination Point in different Network Topologies

21 November 2019

## INTRODUCTION

The Dutch telecoms operators CAIW, KPN, T-Mobile/Tele2, VodafoneZiggo and the providers united in NLconnect would like to thank BEREC for the opportunity to respond to the consultation of BEREC's draft guidelines on common approaches to the identification of the network termination point (NTP) in different network topologies. Earlier in the process, in May 2019, the Dutch telecoms operators already took the opportunity to informally provide a position paper to the relevant BEREC expert working group. This position paper is attached to this response in an annex.

In this response to the consultation, the Dutch telecoms operators would like to emphasize their standpoint as set out in the position paper and raise a few additional issues related to the draft guidelines, which were published on the 10th of October.

## The guidelines do not seem to contribute to their purpose of consistency

Article 61(7) of the EECC requires BEREC to adopt guidelines in order to contribute to a consistent definition of the location of network termination points by NRAs. NRAs are to take utmost account of the guidelines when defining the location of the NTP.

The current draft BEREC guidelines, however, outline different options for the NTP. In its draft guidelines, BEREC provides an analytical framework for NRAs. BEREC only mentions certain criteria which should be considered by NRAs and how to consider these criteria. BEREC does not recommend or define specific locations of NTPs. There seems to be no peer review or other mechanism included to ascertain that in similar markets and with similar technical standards the same outcome will result. The Dutch telecoms operators therefore find it highly questionable whether these draft guidelines will contribute to a consistent definition of the location of NTPs in the EU/EEA.
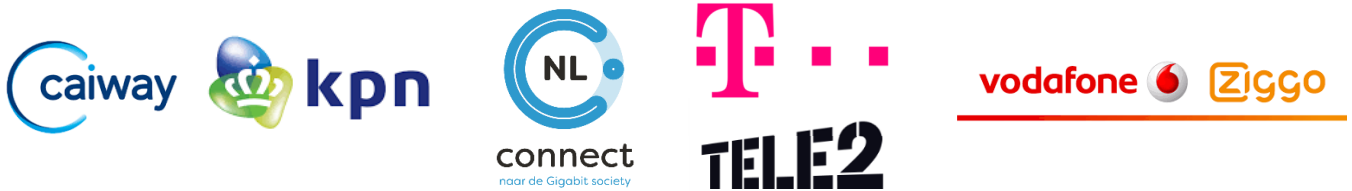
## The boundary should be independent of the service

The NTP represents a boundary of the network. The BEREC Guidelines based on Article 61(7) of the EECC should contribute to a consistent definition of the <u>location</u> of the NTPs. The draft Guidelines seem to imply that all equipment after the NTP should be considered terminal equipment and therefore could be supplied by others than the service provider. In the annex to the draft guidelines BEREC suggests that the location of the NTP depends on the service and may differ for several services. The draft guidelines themselves only seem to analyse example (5) of the annex to the draft guidelines, the internet access service. An end-user can use different services over the same internet access connection. The location of the NTP would however have consequences for the different services, which is complicated already. Flexible NTP locations, depending on the service delivered, could lead to an unclear or unmanageable situation. The Dutch telecoms operators would rather see that BEREC states that there can only be one NTP defined per broadband technology.

In its position paper[1] the Dutch telecoms operators argued that the BEREC guidelines should define the NTP only for broadband access. Realistically, in broadband networks only point A or point B could qualify as the NTP. Broadband networks can be used to deliver all kinds of services (OTT, or 'specialised services') and it may be necessary to deliver associated equipment for specific services. However, that is a consideration for the provider of that specific service.

Given that the examples in the draft BEREC guidelines are only related to broadband services, the Dutch telecoms operators suggest removing the other examples from the annex, such as PSTN, ISDN and leased lines. These are old technologies at the end of their lifecycle. New interpretations of the NTP for these old services could result in inefficient new obligations for telecoms operators.

## NTP definition for access networks based on a shared medium?

In paragraph 19 of the draft guidelines BEREC considers that in access networks based on a shared medium, the network is not able to establish a clear link between a network address and a defined physical point at customer premises. The implicit conclusion is that these draft guidelines do not apply to access networks based on a shared medium. However, the draft BEREC guidelines lack an analysis of the effect of this conclusion. How do these different types of access networks relate to each other and what would the effect be of defining the NTP in a certain way? Furthermore, the analytical framework does not contain any considerations to review competitive aspects in respect to technologies that are competing in the market. We suggest that in paragraph 3.3 a separate analysis for the competitive aspects should be included.

---

[1] The position paper of the Dutch telecoms operators, which is attached to this response as annex.
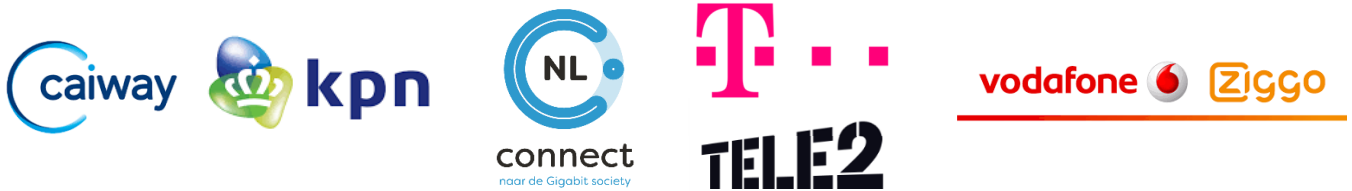
## It is possible to define the NTP at point B in case of modem/router combinations

In paragraph 3.3.5 of the draft guidelines BEREC describes the consequences of the different NTP definitions in case the router includes the modem. BEREC uses graphics as illustration. The Dutch telecoms operators, however, find the descriptions and associated illustrations too simplistic and unsophisticated. ISPs cannot control "local traffic" and local traffic is not part of the service provisioned by the ISP. It would even be impossible for ISPs to control so-called local traffic, such as a print job.

If a modem/router combination is used, it is possible to distinguish the functionalities and to define the NTP at point B. We suggest describing this option also in the guidelines.


## It should be legally possible to disconnect connection when TTE harms the network

If the NTP is defined as point A, the TTE of an end-user could harm the network or cause security incidents. BEREC describes in paragraphs 60, 92 and 93 of the draft guidelines what can be done if this happens. According to BEREC, national legal provisions may be in place which stipulate that end-users are liable for any damages or permit operators to disconnect the TTE in order to protect their networks. In the Netherlands there are currently no sufficient legal provisions in place.

The network continuity and security are of the utmost importance for telecoms operators, as it is a vital sector and providers of public electronic communications networks and services are to take appropriate and proportionate measures to appropriately manage the risks posed to the security of networks and services, according to e.g. Article 40 of the EECC. The Dutch telecoms operators take this responsibility very seriously. There is also a strong commercial interest in this regard. Customers have high expectations of operators. Incidents related to the network continuity and security have a high impact on the operations and competitive position of providers.

For these reasons, the Dutch telecoms providers find it important that BEREC takes a step further and recommends that point A may only be defined as location of the NTP, if legal provisions are in place for network operators to disconnect the TTE in order to protect the continuity and security of the network.
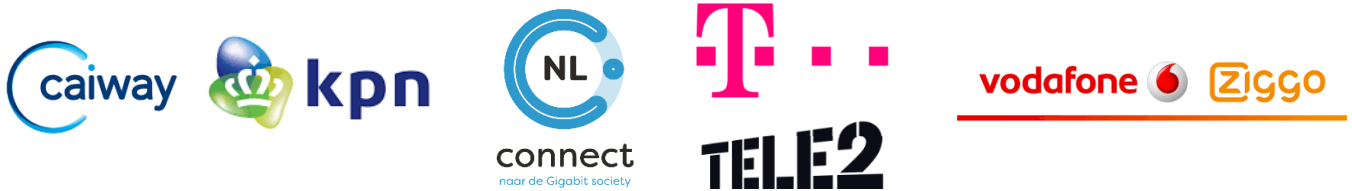
## The promotion of competition on the TTE market is not an objective for BEREC and NRAs

The draft BEREC guidelines greatly emphasize the consequences of the NTP definition on the TTE market. However, the role of BEREC and NRAs is first and foremost to "*promote competition in the provision of electronic communications networks and associated facilities, including efficient infrastructure-based competition, and in the provision of electronic communications services and associated services*".[2] Directive 2008/63/EC does not assign tasks to BEREC and/or NRAs. It may be the case that some NRAs have tasks based on this directive, but that is not due to the EECC, which is the primary source for the BEREC guidelines at hand.

The analytical framework in the draft guidelines mentions that particular definitions of the NTP may negatively affect the competition on the TTE market. That may be the case but if an NRA defines the location of the NTP as point A to promote competition on the TTE market, it could be regarded as imposing an access obligation for which a solid market analysis procedure should form the basis.

Furthermore, if BEREC involves the broader value chain in its analytical framework to define the NTP, it should not do so selectively, but should also include the consequences for e.g. the content market, such as the protection of copyrights.

## Reasonable term to implement

As a final remark, the Dutch telecom providers note that it is important that the implementation of the definition of the NTP-location considers a reasonable term for providers to modify their processes as set out in our position paper in the Annex. BEREC should recommend NRAs to investigate what transitional phase is reasonable and proportionate.

*** 

---

[2] Article 3(2) of the EECC and Article 3 of the BEREC Regulation.

## ANNEX: Position paper Dutch Telecoms Providers regarding the location of the network termination point of 13th May 2019

### INTRODUCTION

Article 61(7) of the EECC requires BEREC to adopt guidelines on common approaches to the identification of the network termination point (NTP) in different network topologies. NRAs shall take utmost account of those guidelines when defining the location of the NTP.

BEREC published a report in October 2018 on the location of the NTP to get a deeper insight in the legal provisions of NRAs and other national authorities on the location of the NTP.[3]
In case of an internet access service, BEREC found different locations of the NTP, as illustrated in the figure from the BEREC Report below.[4]
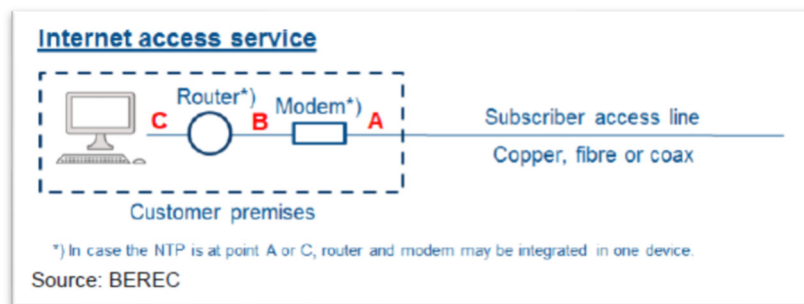


For the Netherlands, BEREC took the intended policy rule of the Secretary of State for Economic Affairs and Climate Policy into account, which defined point A as location of the NTP. However, the Dutch Secretary of State informed the House of Commons in February 2019 that she will not proceed with implementing this policy rule due to the European Electronic Communications Code which authorises the NRAs to define the NTP and requires BEREC to issue guidelines for defining the NTP.

In this position paper the Dutch telecoms operators CAIW, KPN, T-Mobile/Tele2, VodafoneZiggo and the providers united in NLconnect will argue that the expected BEREC Guidelines should focus on broadband access only and why point B is the best suitable location of the NTP.

---

[3] BEREC (2018), Report on the Location of the Network Termination Point, BoR (18) 159.
[4] This figure illustrates the situation of a fixed internet access service. In paragraph 2.2 of BEREC's report it is stated that the situation with regard to the definition of the mobile NTP location is similar to the definition of the fixed NTP location.
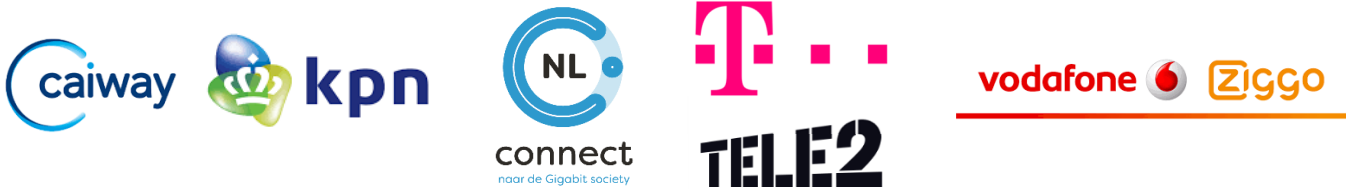
## BEREC Guidelines for broadband access only

The Dutch telecoms operators find it of the utmost importance that the BEREC guidelines define the NTP only for the *network* termination point and therefore only for broadband access. For *services* over the network other than internet access services (in terms of the Net Neutrality Regulation, also called 'specialised services') - such as IP telephony, television and business connectivity – service providers should remain able to ultimately decide what equipment is used, independently whether such service is offered as an OTT service or a 'specialised service'. If end-users are also free to choose this kind of equipment, new problems will occur. E.g. providers will not be able to fulfil their obligations regarding the protection of copyrights anymore. There is also an increased risk of authentication issues, which are more likely to occur with SIP telephony, enabling an abuser to make calls with expensive foreign numbers for free.

## Point B is the most suitable location of the NTP

According to the Dutch Telecoms providers point B is the most suitable location of the NTP.[5] This will be explained below by considering the following topics:
1) Reliability and security;
2) Legal obligations telecoms operators need to comply with;
3) Modifications of operational procedures.

### Ad 1) Reliability and security

Providers have legal obligations, a duty of care and societal responsibility when it comes to the integrity and security of their networks. Telecommunications networks are vital infrastructures and their reliability and security is therefore of the utmost importance. If end-users are completely free to choose their own modem/router combinations, it will make it increasingly more complex for telecoms providers to fulfil the obligations and responsibilities which will be explained further in this paper. The networks will become more easily accessible for external parties and, as a consequence, the number of security breaches will increase, compromising the continuity of networks. This should be taken into account whilst operating the network. If it is clearly known that a certain type of equipment entails irresponsible security risks for the particular end-user or for other end-users, this type of equipment should not be used anymore. It is e.g. also possible that modems, unknown to telecoms providers, are hacked and contain chipsets to track end-users. The question is how these kinds of security breaches are to be detected – as telecoms providers are not always able to do it – and whether it is legally possible to prohibit the use of unknown and possibly dangerous equipment (especially in the case of point A as NTP).

---

[5] Some of the advantages of point B may also apply to point C as location of the NTP. This may especially be the case for devices which combine modem and router functionalities.
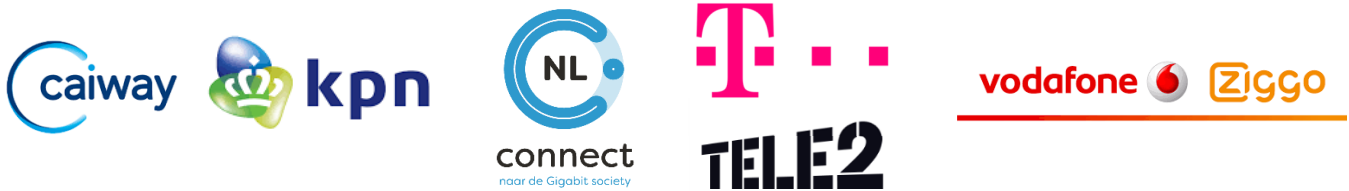
Furthermore, for the integrity and security of networks it is crucial that the maintenance and security upgrades of modems are guaranteed. In practice this is done by telecoms operators for modems they provide through their networks. However, if the end-user has purchased its own modem, it may well be the case that this modem is not up-to-date when it comes to security upgrades.[6] The manufacturer of this modem has to facilitate that end-users are capable of upgrading their own equipment and end-users themselves are responsible for the actual upgrade of the equipment. This increases the risk of endangering the network security. End-users may easily forget to timely upgrade their equipment and even if they do perform an upgrade, they may encounter difficulties. Obviously, there are tech-savvy end-users who are fully capable of keeping their equipment upgraded and safe, but the business model for the provision of modems does not entail any incentive for modem providers and end-users to take care of this. In most cases it is a one-off purchase without a service contract and other safety guarantees.
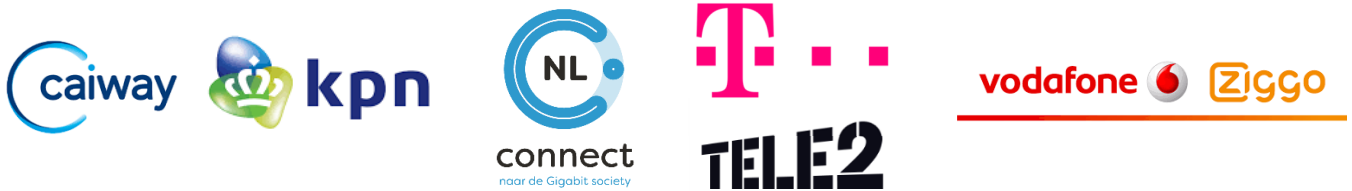
Finally, the presumption is sometimes made that the choice of modem only has operational consequences for one individual consumer. That is true in networks where the connection entails one wire to one receiver. However, this is not the case in shared networks, such as PON networks or hybrid coax-fiber (HFC) networks. In those networks, the quality of the transmitted signal for a whole neighbourhood relies on the functioning of all modems in that neighbourhood. A 'strange', unknown modem could negatively impact all the services provided (not only internet access, but e.g. also television services) to all connected end-users in that neighbourhood. If this situation occurs, it is quite laborious to detect the modem causing the disturbance. In most cases engineers need to physically go to that specific location to detect and resolve the disturbance.

Telecoms providers will be much more capable to protect the reliability and security of their networks, if the NTP will be defined as point B.


### Ad 2) Complying with other legal obligations

Defining point B as the Network Termination Point also enables telecoms providers to continue complying with other legal obligations, such as the net neutrality provisions in the TSM regulation, interoperability obligations, conditions related to the rights of use of radio spectrum frequencies and obligations to ensure security and continuity of their networks and services.

---

[6] Illustrative example in this regard: British research showed that only 14% of 2,205 respondents upgraded the router firmware on their Wi-Fi router, https://www.broadbandgenie.co.uk/blog/20180409-wifi-router-security-survey.
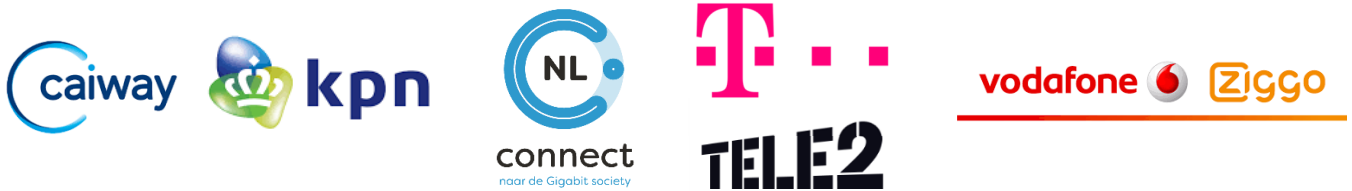
According to Regulation 2015/2120, providers of internet access services need to specify *inter alia* information on the speeds of internet access services. End-users should be able to measure the performance of their connections. It is clear that the speeds need to be measured at the modem. Telecoms providers note that they are not able to specify adequate information regarding internet speeds, if an end-user uses its own modem, as the modem in itself is one of the elements that influence the internet speeds.

Technical standards are complex to manage in practice. Even when different manufacturers apply the same standards in theory, interoperability issues may still occur. Standardisation – often unintendedly – leaves room for different interpretations and manufacturers are also able to add functionalities which are not (sufficiently) supported by standards. The possibilities for telecoms providers to guarantee interoperability are limited in practice. Therefore, consumers should not be given unrealistic expectations that telecoms providers can always guarantee interoperability of all kinds of end-user equipment with the network interface.
It is not obvious that end-user equipment – complying with standards, but without guaranteed interoperability – will function well in practice. Therefore, providers and manufacturers co-operate to certify equipment. During these certification processes, providers support manufacturers to solve potential interoperability issues. The certificate is a guarantee for end-users that this particular device functions as it should on the network of the provider. A number of modem manufacturers seek to enter the consumer market directly (rather than supplying their equipment to providers) and broaden the choice for end-users. The certification process enables modem manufacturers to enter the market in a controlled way.

Although for the reasons explained above, point B should be the NTP, if point A is chosen as location of the NTP, operators should be able to guarantee interoperability only for equipment certified for their networks. Operators should also be able to set other conditions regarding the equipment to be used on their networks, such as: (i) the modem is compatible with the standard of the network; (ii) the modem complies with the operator's interface specifications; (iii) the modem is compatible with the frequency plans of the operator; (iv) the firmware is up-to-date, including the correct data for SIP-telephony; (v) the modem is compliant with the security conditions of the operator; and (vi) the modem is compliant with industry standards and European EMC standards. Please note that this list is only indicative and may not be complete.
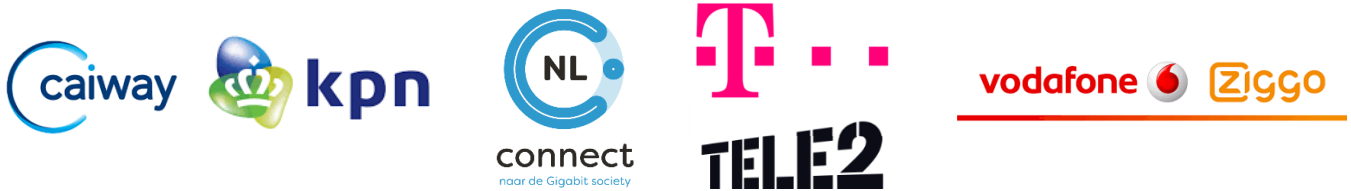
Furthermore, operators would like to note that also in mobile networks there may be equipment used at the location of the end-user that belongs to the domain of the operator. Radio equipment that is meant to provide coverage or services of mobile electronic communication networks which makes use of radio spectrum for which the operators have the exclusive right are part of the domain of the network operator. This is also the case for equipment installed at the location of the end-user such as small base stations or repeaters used to improve the coverage or capacity of public mobile electronic communication within buildings or at business parks. An operator meticulously includes the use of frequencies for these small base stations in the radio planning to ensure that radio frequencies are optimally used and interference between small cells and with the macro network is prevented. This is very important as interference from equipment not included in the radio planning of the macro network may impact the correct functioning of the 112-emergency number, which may lead to life-threatening situations. The Radiocommunications Agency Netherlands ("*Agentschap Telecom*") is very active to ensure these situations are prevented in the Netherlands.

### Ad 3) Modifications operational procedures

The definition of the NTP may impact operational processes. For example: (i) online self-care tools and instructions for call-centres for delivery and disruptions do not work as intended anymore and need to be adjusted, because descriptions and illustrations are not accurate anymore; (ii) national operations centres cannot view unknown modems and are therefore not able to detect and resolve the exact issue; (iii) the deployment of engineers for installation, disruptions and service needs to be adjusted; (iv) other specific company processes (e.g. commissioning services through modems) need to be adjusted; (v) general agreements and conditions need to be adjusted. General agreements and conditions need to be heavily adjusted in case point A is defined as the NTP, to rule out any responsibility for security issues and the quality of service, such as compensation in case of disrupted connection. The question also arises if this major adjustment operation is proportionate for telecoms providers in case of point A as NTP, considering the limited number of consumers that will eventually choose their own modem. In Germany, for example, only 1-2% of consumers use their own equipment (modems and routers).[7]

---

[7] https://www.unitymedia.de/privatkunden/beratung/info/routerfreiheit/ and https://www.vodafone.de/featured/digital-life/freie-routerwahl-vodafone-verraet-was-du-jetzt-wissen-musst/

## Reasonable term to implement

As a final remark, the Dutch telecom providers note that it is important that the implementation of the definition of the NTP-location takes into account a reasonable term for providers to modify their processes. As explained above, the specific period depends on the particular point that will be chosen. NRAs should investigate what period of time is reasonable and proportionate.

<div align="center">***</div>