Esslingen, 21 November 2019

Input on the draft BEREC Guidelines on CommonA pproaches to the Identification of the Network Termination Point in different Network Topologies (BoR (19) 181)

I strongly support the position of FSFE eV Germany, the Free Software Foundation Europe (FSFE). The NTP should always be at point A, this should be the preferred policy and thereby establish and protect Router Freedom in Europe.

On 3.1: Comply with existing European regulation We welcome that BEREC mentions Article 3(1) of Regulation 2015/2120 as well as Recital 3 of Directive 2008/63/EC. Both unambiguously demand to give end-users the right to use their own terminal network equipment.On the argument of “objective technological necessity” which Internet Service Providers (ISPs) may claim to make TTE part of their network, we cannot find a real case where any incident with customer premises equipment (CPE) would have justified a violation ofthe basic user rights determined in Regulation 2015/2120 and Directive 2008/63/EC.1 / 4

The experiences made in Germany after the legal clarification to set point A as NTP as of 1 August 2016 serve as a positive example that devices chosen by end-users do not cause technological damages for ISPs and other customers although some ISPs and network providers warned against this. A significant number of end-users decided to make use of this freedom, a vital market for CPE is evolving, and there were no such breakdowns in neither the cable nor the DSL network.

On 3.2: Set point A as the NTP We agree to BEREC in the conclusion that the NTP at point A contributes the most to innovation and competition on the TTE market. Furthermore, there are many more arguments that speak in favour of setting point A as the default NTP:• according to Regulation 2015/2120 and Directive 2008/63/EC, end-users must have the right to choose the electronic devices in order to connect to the internet, which includes both the modem and the router. This freedom of choice enables them to choose devices that suit their individual needs best.•Routers and modems as TTE are gatekeepers of most online activity for internet users and businesses alike. Therefore, they need to be able to pick a device that allows them to use certain privacy and data protection features which fulfill their requirements.•
End-users regularly change their ISPs. Only if they can continue using their own device, they can port their settings and existing devices to the new provider. If their TTE was owned by the ISP, the compatibility to other providers and their specific requirements would be drastically limited.•Users profit from the free and fair competition that guarantees free choice and steady improvement of products.

The lack of competition would, eventually, comeat the cost of the user because (security) features would be be continually reduced and the user-friendliness would drop. A vital CPE market will foster innovation that benefits the European industry and citizens.

A lack of Router Freedom increases the probability that large parts of the router market is dominated by only one or a few product families or manufacturers. In those settings, major problems or security holes affect an enormous number of users at once. That is particularly problematic when manufacturers and providers are very slow in the delivery of critical updates and users are not allowed to perform updates themselves. A larger number of available CPE benefits the general security of the complete landscape. It enablesend-users to take own security precautions and/or commission an equipment manufacturer or service provider to take care of updates and preventive measurements.

Instead of trying to create a false sense of security by isolating the public network from TTE not provided by the ISPs, network providers and manufacturers have to work together to maintain the high stability of these networks. Regarding 3.3.3, we would like to point out that the device and network security profits from a more diverse TTE landscape and more competition by manufacturers. The argument that ISPs care best for their clients security has been proven wrong by many incidents where routers did not receive updates for known vulnerabilities and therefore caused massive disruptions for end-users. Only point A as the NTP locations allows for a competition of equipment manufacturers for better security precautions, update service reliability, and complementary features. End-users will then be able to freely choose their equipment and service provider from a range of choices where the ISPs are not the only ones. Regarding 3.3.4 and 3.3.5, we conclude from BEREC's analysis that data protection and the handling of local traffic are best served by point A as the NTP.

Overall, I see the draft BEREC Guidelines going into the right direction. I agree to this position and would like to encourage BEREC to communicate this more strongly.

Sincerely,
[personal data removed]
netzwissen.de
Esslingen/Germany/EU

[personal data removed --] D-73728 Esslingen, Germany, EU *
* Mail: [personal data removed] *
* PGP: [personal data removed]
* Owncloud Federation: [personal data removed]*