From: [redacted]
Sent: Thursday, November 21, 2019 4:21 AM
To: NTP_Guidelines; NTP_Guidelines_Notifications
Cc:
Subject: Comment reg. different NTP positions

In reference to [0]

Hello,

Since I only read about this draft now, just a few, brief quick comments due to deadline already today in a few hours:

* 3.2.3., NTP at point C, not only affects the CPE vendor market,
  but also the software side:
  - with C it will be a lot more difficult for customers,
    developers and researchers to run an open source router
  - installing an open source router behind an ISP router
    will now need them to follow the rules imposed by the
    ISP router rather than needing to follow a specific,
    technological standard; ISP rules will change during
    runtime via software updates, making it even more hard
    to catch up with; ISP rules might block specific traffic
    types resulting in degraded performance and quality
    for the customer's open source router
  - installing an open source router behind an ISP router
    might unnecessarilly double the electricity and hardware
    costs in certain scenarios

I'm involved in the non-profit Freifunk initiative and the open source software we run on our Freifunk routers. I expect that fixed, ISP enforced, monopolized routers will significantly increase the burden and issues we will have to deal with.

* 3.3.3.1, 89.: "end-user needs to ensure that the software used

in the TTE is no threat for network security"
- I would argue that there is no and should be no obligation
  for the end-user here for threats caused by third parties;
  instead it should be the obligation of the network operator
  to ensure that it is robust regarding network security
- also the end-user will never be able to "ensure" it; and
  even if the end-user were able to ensure it for the router,
  or if the NTP were at C then there are still threats coming
  from the end-user laptops/PCs/phones etc.
  - and then the ISP should provide the laptops/PCSs/phones
    etc. or how would this argument continue then?

* 3.3.6: Fixed line services
- this paragraph is slightly obscur because it is about service
  plans but the conclusions sound more as if there were
  a fundamental, technological necessity for the router to be
  operated by an ISP to allow internet access over a mobile
  network
- the document refers to the LTE connectivity as *mobile*
  network, while trying to enable/enforce a *non-mobile* router
  for "*fixed line* service" contracts - which suggests that
  there is a more fundamental discrepenacy/challenge between the
  intended goal and chosen technology
- even a router provided by the ISP can be turned into a
  "non-fixed line" router by connecting the ISP router to
  a battery pack instead of the grid power
- there might be other, easier, more suitable ways to ensure
  non-mobility other than who is owning/operating the router;
  for instance locking the router to a specific (set of) base
  station(s) - which would work for a customer owned router, too
=> the document should be:
  - more clear that 3.3.6 is about pricing/contract models
    and not about a technological necessity
  - more clear that both an LTE router operated by the ISP
    and an LTE router operated by the customer both cannot
    fully ensure non-mobility / face similar challenges
  - that there might be alternatives to achieve "fixed-line
    like services"

My personal opinion though is that the European Union has no obligation to ensure specific business/pricing models. And that therefore the considerations of 3.3.6. as a whole should be removed.

The document describes the importance of "Data protection" in 3.3.4. Which seems to elaborate on the potential privacy issues in the local network. However it does not seem to elaborate on further, potential privacy issues outside of the local network, which an electronic device in souvereignity and remote accessibility/controllability of a third party imposes:

- With ISPs always providing and operating an electronic device (router or modem) in the customer premises would always provide them a permanent view and access into the private space; they can detect other wireless devices; they can detect/sense when a microwave oven is used (same frequency as wifi, 2.4 GHz, usage is visible in the noise floor of the wifi chip) or when a phone call via a Bluetooth-Headset is made; they are able to estimate how many people are in the customer's (or even neighboring) appartment and how close they are to the ISPs wireless routers; they are even able to triangulate highly accurate positions if a neighbor has a router in control of the same ISP, too
- the ISP may install additional sensors to gain a more accurate view into the customer's premise and a customer's habits, the ISP may demand from the customer to wave certain rights to use its services (similar to how we already have to wave rights to use YouTube, Google, Facebook etc.)
- it may be argued that if the customer did not want to wave its rights that it could choose a different provider - however similar to the large internet platforms, internet providers have monopolized, too, so that pratically the user/customer does not always have a choice
  => and in that case a regulating body needs to restrict the (the reach of) monopolies; and granting a customer the right to:
  a) choose their own router
  b) choose to mistrust and not allow an eletronic device in their premise which they don't have full souvereignity over
  - but without being discriminated/limited/over-prized in

their choices for general internet access
is one means to achieve this
- an ISP could monitor and enforce that only a specfic customer's registered device, but not devices from guests/friends of the customer were allowed internet access, by monitoring the wireless spectrum and blocking traffic that came from a customer device but originated from a different wireless device in the area, for instance
  -> that way an ISP could in theory quite effectively either block users of Freifunk routers, even though Freifunk users usually use an encrypted VPN, or simply cancel a contract if some wifi probings and correlation were detecting a shared internet access
  => this imposes a threat to initiatives like Freifunk which often rely on a shared internet access

These last points might sound a bit dystopic / fictional on first read, but with the current regulations I wouldn't see (m)any legal obstacle(s) for ISPs to implement this. And with networks growing more and more into our lives, especially with the advances in the Internet of Things field, I'm wondering (with the current regulations) why they might not become a reality at some point otherwise.

Regards,
[redacted]

[0]: https://berec.europa.eu/eng/news_consultations/ongoing_public_consultations/5912-public-consultation-on-draft-berec-guidelines-on-common-approaches-to-the-identification-of-the-network-termination-point-in-different-network-topologies