From: [redacted]
Sent: Thursday, November 21, 2019 2:58 PM
To: NTP_Guidelines; NTP_Guidelines_Notifications
Subject: Freedom issue => Many practical issues
Attachments: OpenPGP digital signature.dat

Hi,

Router and modem should be able to be under users control if users need it.

Being able to control your own router and modem is an essential freedom you shouldn't take away as depending on the hardware and software configuration, that equipment is typically holding the public IPv4 IP address of the user.

If the user equipment cannot hold the public IP addresses:
- It makes self hosting way harder or impossible: Many people still rely on IPv4, especially on cellular network access on smartphones. This would be totally unacceptable as it is a very serious attack on people freedom as freedom of expression also depends on that. It would force people to use centralized services like Google which are US companies that don't respect the European laws (like the RGPD for instance).
- Many ISPs that are part of the FFDN[1] don't provide any modem to the users. It's up to the users to buy a modem.
- It makes the software stack way more complex. This requires ways to traverse nat, requires stun and similar solutions. If the operator controls the equipment that does the NAT, operators could prevent that, leaving users with a completely broken internet. Some have enough market power to impose things like that.

Even if the modem doesn't hold the IP address, this still creates many issues:
- Users can buy modems that can be upgraded[2]. Users buying and operating their modems typically care, directly or indirectly, about freedom and have an incentive to upgrade and maintain their modems.

This means that such modems will get security updates, which prevents most attacks.
Leaving modems prone to attack create issues like Mirai[3] where criminals managed to compromise many of such equipment to build a ddos attack tool that could reach more than 600GB/s.
That blatant lack of security endanger the whole network.
Companies (hardware manufacturers, ISPs) cannot be trusted to keep such equipment secure and up to date as many often try to lower down the cost of maintenance.
- Connectivity problems cannot be investigated and/or solved by users.
- It reduces users trust in technology as someone else is operating the equipment they have in their homes or offices.

References:
---
[1]https://www.ffdn.org/en
[2]https://openwrt.org/toh/netgear/dm200
[3]https://en.wikipedia.org/wiki/Mirai_(malware)