How to Accommodate Network Slicing & Network Neutrality?

Yassine Hadjadj-Aoul[1][0000−0003−4864−4609], Patrick Maillé[2][0000−0003−1064−5948], and Bruno Tuffin[3][0000−0001−9415−1130]

[1] Univ. Rennes, IRISA, Inria, CNRS, 35000 Rennes, France
yassine.hadjadj-aoul@irisa.fr
[2] IMT Atlantique, IRISA, UMR CNRS 6074, 35000 Rennes, France
patrick.maille@imt.fr
[3] Inria, Univ. Rennes, CNRS, IRISA, 35000 Rennes, France
bruno.tuffin@inria.fr

Abstract. Network slicing has emerged, with 5G mobile networks, as a response to the increasing networks' complexity and the inherent scaling limitations of traditional methods. That technological building block allows, in fact, a very agile orchestration of services, bringing dynamicity, differentiation, and most importantly the fulfillment of various service constraints.
Slicing is therefore seen as a key characteristic of 5G-and-beyond networks, however it seems in contradiction with neutrality principles promoted worldwide. We detail the two contradictory but considered compulsory notions, and discuss how they can be accommodated.

Keywords: Net neutrality · Regulation · Slicing · 5G · Quality of Experience · Specialized Services · Network Operators.

1 5G & Network Slicing

5G stands for the latest generation of wireless networks, coming (as any new network generation) with new capabilities. That fifth generation is in particular expected to increase throughput by a factor up to 100 with respect to 4G, and to allow to connect enormous numbers of devices, from phones to cars and any type of object all over the world. What's more, 5G enables the support of a broad range of services, even the most demanding ones, including real-time interactivity, such as autonomous driving. As of June 2022, around 70 countries had already implemented a 5G network, and it is believed that in 2025, at least 3.6 billion 5G connections will be active. While the first phases of deployment are currently limited to access networks, 5G is designed to go far beyond that, with the ability to provide on-demand guaranteed end-to-end services. This feature is made possible with the adoption of a new concept in 5G and beyond networks, named *network slicing*.

Network slicing consists in creating multiple dedicated logical and virtualized networks over several domains, cutting the infrastructure into "slices" managed

independently (see Figure 1). That approach provides flexible and scalable resource provisioning for applications and services in order to align resources with needs for quality in terms of throughput, latency, reliability and other metrics, by appropriately dimensioning the slices. Slicing allows to simultaneously and efficiently manage heterogeneous traffic and offer tailored solutions to customers and industries, some being demanding such as telemedicine, online gaming, or augmented reality.

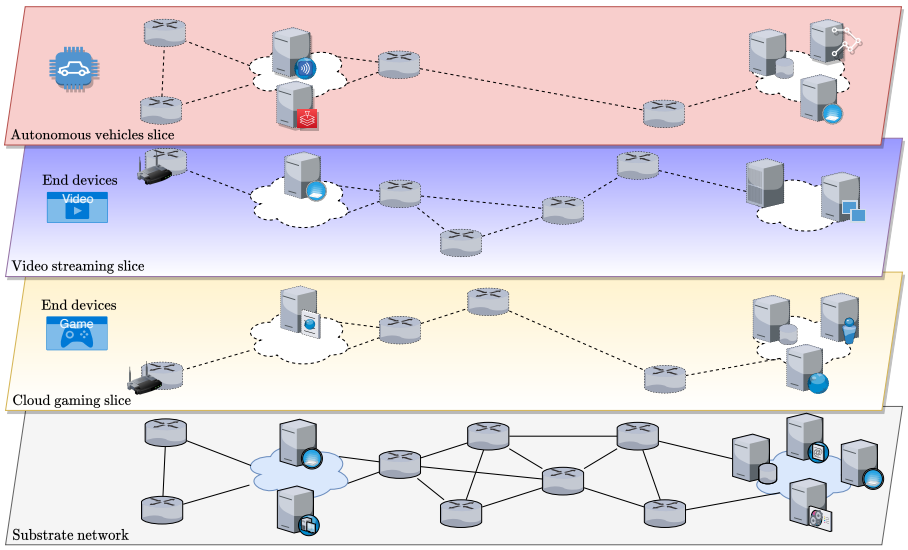

Fig. 1. Typical network slicing architecture

There are several reasons for the adoption of network slicing in 5G mobile networks. One is obviously the support of services with heterogeneous constraints, as described above. In fact, this is an opportunity for Network Operators (NOs) to get more value out of the transport of services, by being part of the content distribution value chain. Indeed, NOs currently have very limited control over their own infrastructure rental revenues, which are currently being determined by national regulators. Network slicing is also seen as one of the most important building blocks for network automation, as it brings more agility in the management of services. It also helps to deal with the growing complexity of networks. For all these reasons, we believe that network slicing will continue to be part of the next cellular network standards.

2 Network Neutrality

On the other hand, telecommunication networks have been under the scrutiny of regulators concerning neutrality issues. Network neutrality is the principle that traffic should be treated equally, without discrimination, restriction or interference, independently of the sender, receiver, type, content, device, service or application [7,10]. Due to the historic nature of a free and open Internet, the move to a commercial network ignited fears and threats that some services would not be available to all and/or that some would receive a degraded treatment. According to the rule currently in place in the EU [1], no differentiation is allowed, with exceptions *i)* in case of a legal action; *ii)* to ensure the security and integrity of the network if confronted to attacks; *iii)* in case of temporary congestion if no commercial consideration is taken into account. Those guidelines are in line with the recommendations promoted in the 2010s by the US regulator, the Federal Communications Commission (FCC); see for example [2].

The debate about revenue sharing and the business model of the Internet was raised in 2005 when Ed Whitacre, CEO of AT&T, claimed that distant content providers used the AT&T network for free in order to reach end users, and that architecture maintenance could not be economically sustained if those content providers (who make significant profits) were not charged for that. That period also witnessed cases of traffic management by Internet Service Providers, like the USA provider Comcast blocking P2P applications in 2007, arguing that P2P content is mostly illegal. All this raised a lot of concerns and protests from content providers and user associations, worried about the Internet not being open anymore and about the impact on service innovation if access was not free.

As a consequence, the neutrality principle has been highly debated and laws have been passed in most countries worldwide [7]. But the story (the debate) has not come to an end yet due to the outbreak of new services and economic practices falling in "grey areas" and raising new discussions, such as zero rating and sponsored data[4]; and network slicing seems to also fall into this category. Neutrality rules have even been recently repealed in the USA under the Trump administration [3] to allow more economic freedom, indicating that the regulatory environment is still moving.

3 Contradictions Between the Two Notions and Traditional Propositions

There seems to be a contradiction between the notions of neutrality, now a pillar of the Internet and telecommunication networks, particularly in Europe, and of slicing, a pillar of 5G networks: how to conciliate equal treatment among flows, with reserved resources for *some* traffic flows?

[4] In those practices, for some (favored) applications the operator does not count the corresponding data volume in the data cap, or the data cost is covered by the application provider, respectively.

To address that question, regulators such as ARCEP in France or BEREC in Europe are proposing to define some services, called *specialized services*, which could be excluded from neutrality constraints. This would concern services with strict quality of service requirements, services usually not supported by the Internet network. Typical examples are video on demand, online gaming, autonomous vehicles or telemedicine [4]. The regulation would then allow allocating slices to each of these services, hence guaranteeing a sufficient quality, but potentially at the expense of other "regular" services.

The notion of specialized service and their management open some breaches to the implementation of neutrality principles. Indeed, the definition of a specialized service is vague: what prevents a new service and even an existing one from claiming the "specialized service" label? It would also be tempting for an NO to consider its own services (VoIP for example) as specialized ones in order to obtain a competitive advantage.

This raises a series of key questions: What are then the objective and clear criteria to be part of that category and to define the quality associated to each slice? Who chooses the relevance of pertaining to a slice, and the service levels associated with that slice? Who will ask for a service to be of this particular class? The Service or Content Provider (SCP), the NO? If it is the NO, isn't there a risk to favor commercial partners? What if an NO does not warrant a request from an SCP? How to proceed without economic considerations, which could constitute incentives to favor some services over others, even between slices and specialized services, something excluded by neutrality principles? Those open questions need some clear answers.

The definition of specialized services is therefore surrounded by many grey areas still to be sorted out, otherwise complaints are expected to pop up.

4 An Accommodation Proposition

Given the many unanswered questions, our aim in this section is to propose some high-level guidelines for a solution that could accommodate network slicing and network neutrality. The idea is to define a procedure that is as objective and automated as possible, limiting the holes and antagonist principles between slicing and neutrality.

What we propose is made of the following steps (see Figure 2).

1. First, analyze the traffic flows, their requirements and constraints, and classify them into different "types", or classes. Classification can be either derived from information given by the service provider, or based on packet-level information, through deep packet inspection, or performed using statistical approaches [8], the latter case being possible even with encrypted traffic [6].
2. Define slices, one per traffic type, in terms of a given level of quality of experience (QoE) [9]. QoE "explains" the users' perceived quality for a given service, in general related to quality of service parameters (packet loss, delays, jitter, ...) but in an extremely complex way. Quantifying the QoE has

been the topic of an extensive research activity during the past couple of decades [5].

3. If congestion and consequent degradation of quality of service occurs, differentiate service among slices to offer sufficient or satisfying QoE for each slice as much as possible, while treating all flows equally within each slice (which may imply interrupting service for a whole slice–or several, or uniformly selected flows–if resources are insufficient).

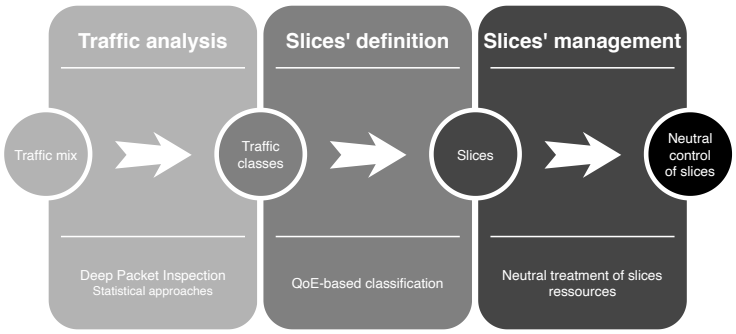

Fig. 2. Methodology.

Proceeding this way, flows with similar quality requirements and perceptions will be treated neutrally, and differentiation will be made possible at the benefits of end users. Users and service providers will be served in an optimal way according to the conditions, and NOs will be allowed to manage services.

Of course, this requires monitoring from regulators to verify that the behavior of actors corresponds to what is expected, here in terms of sufficient QoE. Specific procedures have to be designed toward that goal.

The proposed method allows to respect a new vision of neutrality, oriented toward classes of service, but aiming simultaneously at offering the best possible experience to users, at providing a sufficient quality to SCPs, and at leaving flexibility to NOs. It seems to us a reasonable trade-off for accommodating slicing and neutrality. This obviously requires some knowledge about service requirements and the ability to measure quality of experience, whether flows are encrypted or not. In an over-provisioned system, the operator will have the ability to meet the targeted quality criteria.

In the case of an under-provisioned system, the proposed slicing technique presents some challenges. First, what is the share of resources to be dedicated per class of service? Once we have partitioned the resources, how do we guarantee the quality of the supported services? What incentive is there for a network operator to set up several solutions (i.e., traffic classification, QoE measurement, service monitoring, etc.)? The answers to these questions are not necessarily unique,

but several directions and accommodations exist to achieve these goals while respecting the principles of neutrality.

On the issue of resource sharing, there is the simple possibility of fixed sharing, prior to service deployment and which might be up to the preference of the operators and their interest in favouring one slice or another. But a better solution could be, instead, to have a dynamic sharing of resources that maximizes the satisfaction of the users belonging to the different slices. This would remove a bit of decision power from ONs, but seems to use a balanced solution to let them perform differentiation.

To guarantee the quality of the flows in a particular slice, there is a clear need to monitor the traffic of that slice in order to provide a fair intra-slice resource sharing (i.e., offering the same QoE). In the case where resources are insufficient to reach the minimum QoE, we can include an admission controller, that could act by randomly selecting some flows which will be blocked on this slice to reach the QoE objectives for those served. The selection would be according to a uniform law to ensure a form of neutrality/fairness.

Finally, the proposed solution allows the NOs to offer differentiation in their network, an option they do not have today, even if depriving them from differential control within a slice.

Acknowledgement

The authors acknowledge the support from France 2030 program, operated by the Agence Nationale de la Recherche (ANR), under the grant ANR-22-PEFT-0002.

References

1. BEREC: Berec guidelines on the implementation by national regulators of european net neutrality rules. Document number: BoR (16) 127 (Aug 2016), available at `https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/6160-berec-guidelines-on-the-implementation-by-national-regulators-of-european-net-neutrality-rules`
2. Federal Communications Commission: Protecting and promoting the open internet. available at `https://www.federalregister.gov/documents/2015/04/13/2015-07841/protecting-and-promoting-the-open-internet` (April 2015)
3. Federal Communications Commission: Restoring internet freedom. available at `https://docs.fcc.gov/public/attachments/FCC-17-166A1.pdf` (Jan 2018)
4. IETF: Network Slicing Use Cases: Network Customization and Differentiated Services. https://tools.ietf.org/id/draft-netslices-usecases-00.html (Jun 2017), [Online; accessed 26. Jun. 2022]
5. Khokhar, M.J., Ehlinger, T., Barakat, C.: From network traffic measurements to qoe for internet video. In: 2019 IFIP Networking Conference (IFIP Networking). pp. 1–9. IEEE (2019)

6. Liu, C., He, L., Xiong, G., Cao, Z., Li, Z.: Fs-net: A flow sequence network for encrypted traffic classification. In: IEEE INFOCOM 2019 - IEEE Conference on Computer Communications. pp. 1171–1179. IEEE (2019). https://doi.org/10.1109/INFOCOM.2019.8737507
7. Maillé, P., Tuffin, B.: From Net Neutrality to ICT Neutrality. Springer Verlag (2022)
8. Nguyen, T.T., Armitage, G.: A survey of techniques for internet traffic classification using machine learning. IEEE Communications Surveys & Tutorials **10**(4), 56–76 (2008). https://doi.org/10.1109/SURV.2008.080406
9. Rehman Laghari, K., Connelly, K.: Toward total quality of experience: A qoe model in a communication ecosystem. IEEE Communications Magazine **50**(4), 58–65 (2012). https://doi.org/10.1109/MCOM.2012.6178834
10. Wu, T.: Network neutrality, broadband discrimination. Journal of Telecommunications and High Technology (2003)