# Network Neutral Traffic Classification and Management

Telecommunication networks, the Internet, is not just the infrastructure. As much as hardware is necessary, the proper management and control of the network is required to provide services with high quality. Network operators are generally hesitant to use any service differentiation methods, for several reasons. One such reason is they fear of being accused of favoring one application over the other, or one company over the other. **Another reason is that there are no efficient mechanisms to provide traffic classification.** Therefore, the whole Internet still mainly operates in a best-effort manner, which means that traffic is transmitted without any guarantees and each packet is treated the same way, regardless of its actual requirements.

The Internet mostly operates well; however, there are times and events in which at least certain Internet users observe degradation of their commonly used applications or services. The recent Covid-19 pandemic situation created a sudden and massive demand for online meetings. Online meetings, as well as other interactive applications, usually require special treatment. This means that applications need low latency, but also some reserved bandwidth to operate decently. In a normal situation, the application works fine. However, during the pandemic most people observed degradation of the service, at least occasionally. **Proper service management could, e.g., prioritize online meetings over other Internet activities to solve the problem. To do that; however, efficient service-aware traffic classification is necessary.**

Service-aware traffic classification is a technique that allows network operators to better analyze network traffic composition as well as manage and schedule efficiently network resources to facilitate a sustainable network. It involves identifying different services carried out by different applications in the Internet traffic. Recently, more and more traffic is encrypted, which makes traffic classification even more difficult. Moreover, even for unencrypted traffic, scanning its contents is criticized for invading people's privacy and violating network neutrality principles. In most countries, the telecommunications law does not prohibit such actions; however, they are publicly frowned upon. Net Neutrality means that the telecom operators should not be allowed to differentiate the traffic based on its content, application, source, or destination. The reasons for such statements lie in the fact that telecom operators might manipulate the traffic in their networks for their benefit.

The research hypothesis of the project is as follows:

***It is possible to provide Quality of Service differentiation based on efficient and reliable traffic classification which follows the Network Neutrality concept.***

To prove the hypothesis, the following questions need to be resolved.

1. How to design service-aware traffic classification which: a) is efficient, b) is quick, c) is able to classify encrypted traffic, d) follows the network neutrality principles.
2. How to design characteristic-aware traffic classification which: a) is able to detect elephant flows based on the first packet, b) operates at line speed.
3. How to design an architecture which provides guarantees for traffic classified by 1. and 2.

Each presented above question cannot be resolved by the current state-of-art knowledge, hence research need to be carried out. The project's goals are therefore interesting from the perspective of science. Moreover, what is even more interesting, is that by solving these problems we will contribute to the public welfare, as the outcomes will be highly usable and desirable by every Internet user.