

Research/Implementation plan

We chose the „Project 2 – PI-Hole in P4” with our team. Pi-hole is a DNS sinkhole that can be used to block advertisements and tracking domains at the network level. P4 (Programming Protocol-independent Packet Processors) is a high-level programming language used to define the behavior of network devices such as switches and routers.

If you want to implement Pi-hole in P4, you will need to program your network devices to intercept DNS requests and forward them to the Pi-hole server. You can use P4 to define the packet processing behavior of your network devices, including how to handle DNS packets.

Here are the basic steps to implement Pi-hole in P4:

1. Define a P4 program to capture DNS packets: The P4 program must include a DNS header filter. First, you need to add the DNS headers you want to filter on.
2. DNS header filtering can be applied in several ways. We will extend the filtering by reading from a file and searching in a table. In the file, line by line, there will be the DNS headers and websites that we want to block.
3. To further expand the filtering, we create another file containing the DNS headers and sites we want to allow. This will be a so-called white list. We will then complete our P4 program with a dynamic toggle, which will be used to switch between whitelist and blacklist filters.
4. After completing the previous steps, test the Pi-hole implementation to make sure it works as expected. For this, we will create a script whose task will be to simulate the sending of packets and thus test the correctness of the program.

Based on the examples learned in class and after researching on the Internet, this is roughly how we want to implement it.