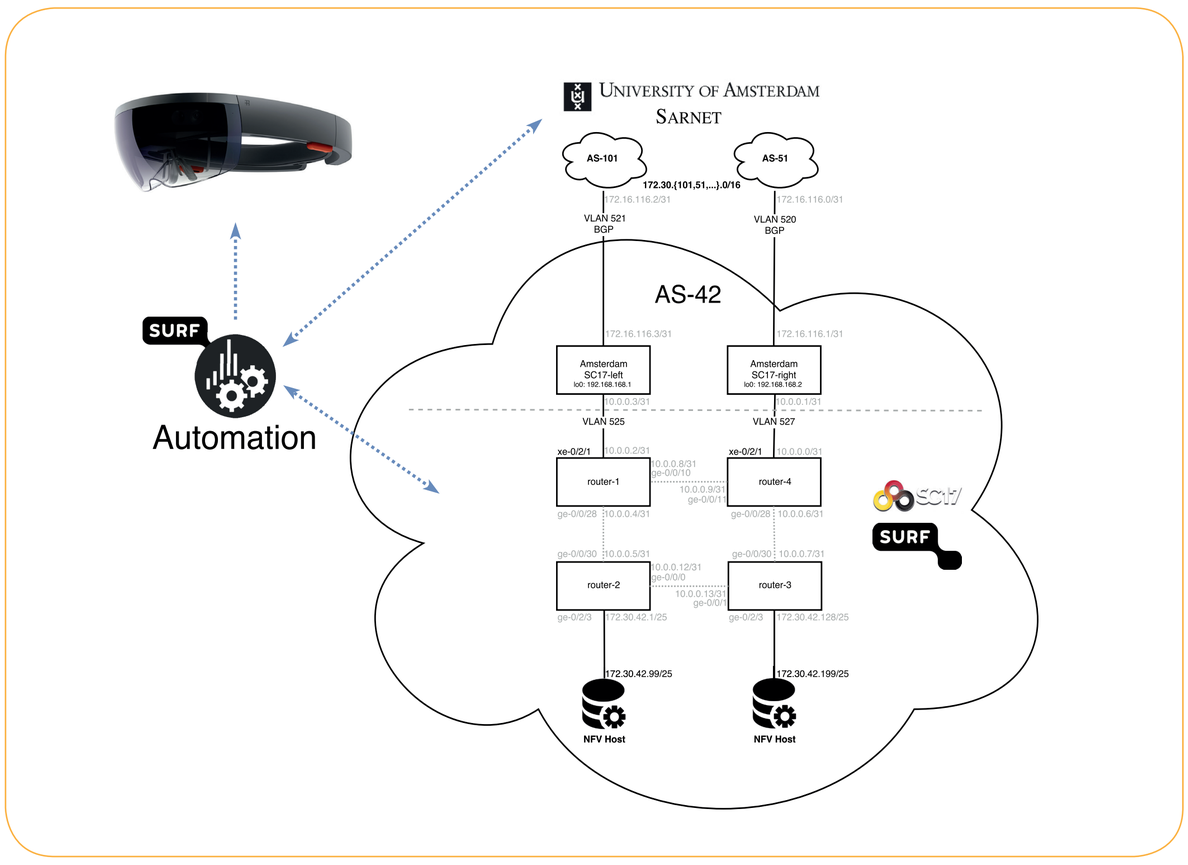
DEMONSTRATION: AUTOMATION INFRASTRUCTURE WITH AUGMENTED REALITY

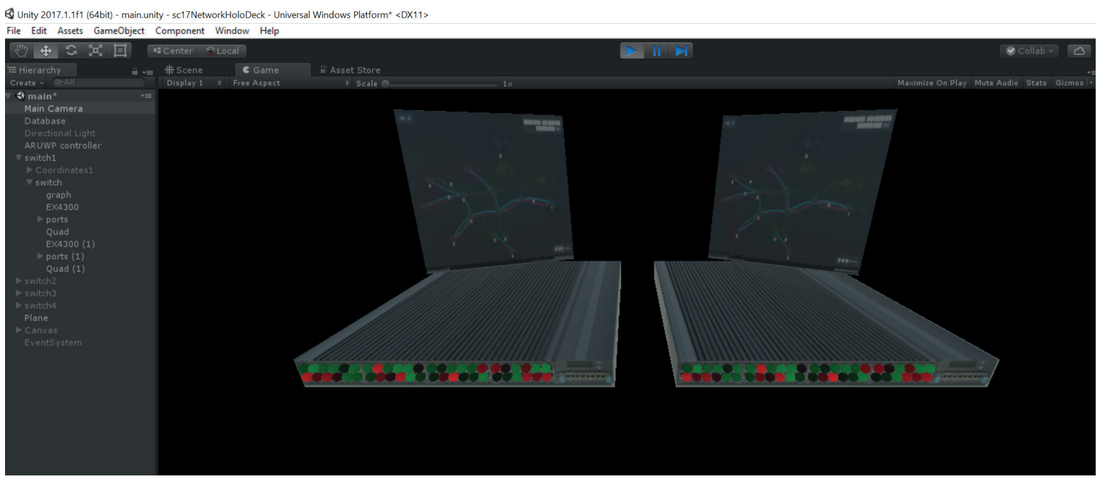
SCENARIO

In this demonstration, we're showing automated and live network (de)provisioning. The network on this booth is part of the international SARNET infrastructure that allows network topologies to be manipulated. Here at the SURF booth, the user wears a Microsoft Hololens and gets instructions from the automation software via the Augmented Reality (AR) graphical interface to plug and pull cables from 4 Juniper routers on-site. The provisioning of all devices at the booth is done real-time in the background. The automation layer can configure devices for different vendors and types underneath the controlling software. This means that the same demonstration can be held with 4 different brand/type routers or switches.



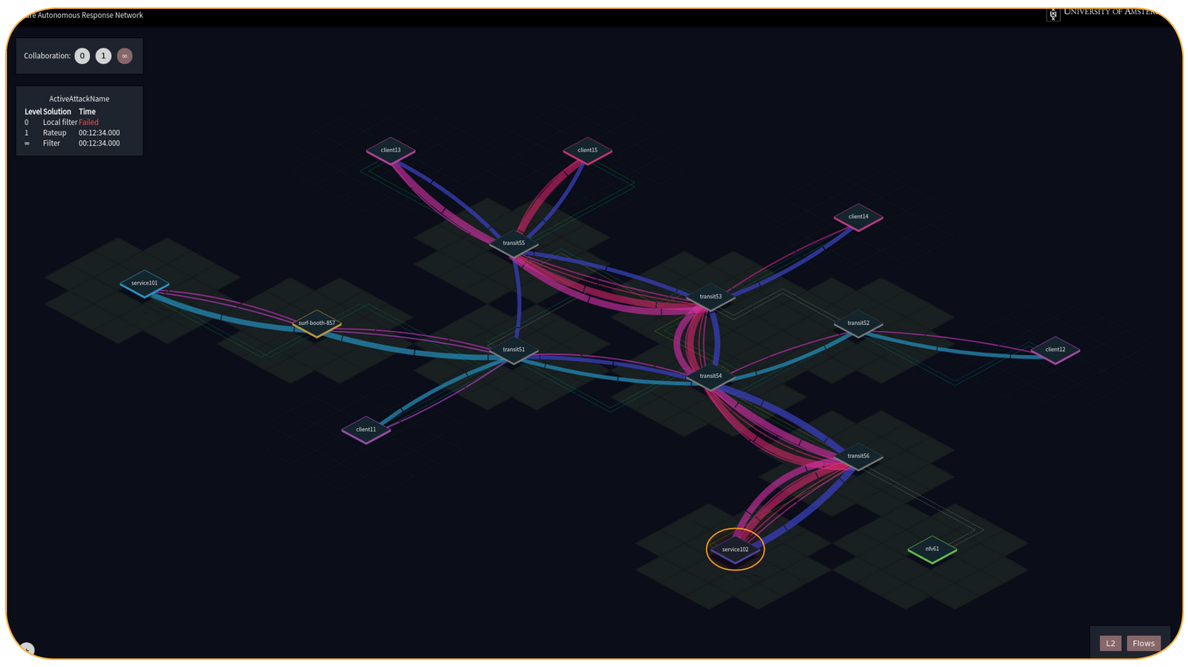
AUGMENTED REALITY

SURFsara created an Augmented Reality application to show the user a real-time overlay of information on the network, such as network topology, data traffic and possible rate limiting. The user is presented (spatial) instructions for network maintenance in order to solve network issues that might arise and need attention. The Augmented Reality application is developed for a Microsoft Hololens (development version), using the Unity3D game engine to build the Augmented Reality environment and the Hololens AR toolkit for tracking markers. The Hololens has a limited amount of processing power: it receives data and instructions via a wireless connection to the network data server, offloading renderings where possible.



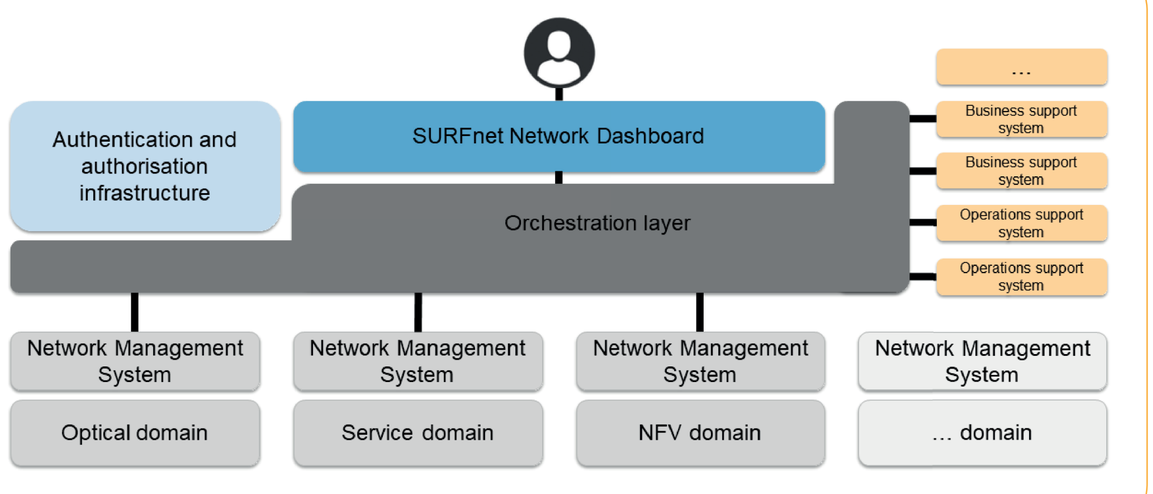
SECURE AUTONOMOUS RESPONSE NETWORK

The automation infrastructure also acts as a physical SARNET (Secure Autonomous Response NETwork) domain. SARNET is a project funded by the Dutch Research Foundation. The University of Amsterdam, TNO, KLM, and Ciena conduct research on automated methods against attacks on computer network infrastructures. This year we will show multi domain autonomous responses to cyber-attacks, and how adjusting the amount of collaboration between the domains can improve the effectiveness of countermeasures. The SARNET part of the demo will be shown at the Ciena booth #1281.



AUTOMATION & ORCHESTRATION AND NFV

SURFnet works on an automation & orchestration framework that offers provisioning across multiple domains in a uniform way. We investigate specifications of relevant standards, as well as standardized open and programmable interfaces (e.g. OpenConfig and P4) so that new components can be added or modified easily into our system in the future. Using data from our internal systems, we create separate workflows to deliver network services (products) to our institutions. We expect that in the near future, all management and technology domains in a carrier grade network will have open and standardized APIs, so that various tasks can be automated in each domain ('automation'). The combination of these actions allows us to connect systems and to manage them intelligently as a whole ('orchestration'). A well-documented workflow and good information architecture with known authoritative sources is key to ensure that the systems exchange information correctly.



Network Function Virtualisation (NFV) allows us to replace some of the network's physical hardware components with an unlimited number of virtual, software-based components. Virtual network functions perform the same tasks as traditional network hardware, such as switches, routers and firewalls, but are infinitely scalable and can be provisioned just in time. This demo includes a proof-of-concept environment with mainly firewall functions, delivered by SARNET, as virtual network functions. These functions can be scaled up or down at any given time, depending on the wishes and requirements of the research and education institutions. The first function we are currently testing in our experimental environment is a virtual firewall.

Nikhef · University of Amsterdam · Juniper Networks · SURF