

# Community Connection Service for eScience

(A GN3plus Open Call Project)

R. van der Pol\*, B.M.M. Gijzen<sup>†</sup>, R.J. Strijkers<sup>†</sup>

\*SURFnet

Radboudkwartier 273  
3511 CK Utrecht, The Netherlands  
Email: ronald.vanderpol@surfnet.nl

<sup>†</sup>TNO

Brasserplein 2  
2612 CT Delft, The Netherlands  
Email: bart.gijzen@tno.nl, rudolf.strijkers@tno.nl

## KEYWORDS

GN3plus, SDN, OpenFlow, Network Virtualisation, eScience

## ABSTRACT

In this paper we describe the first results of our work in the GN3plus Open Call project CoCo (Community Connect). CoCo is a proof of concept for a novel on-demand connectivity service for research communities and education communities, connected through participating NREN networks and the GÉANT network.

Conducting eScience based research is a community effort in which the importance of networked services and facilities, e.g. medical databases, genome databases, remote microscopes, render and visualisation facilities, cloud computing and storage, is increasing. Due to privacy, security, and quality of service issues, services and facilities may not always be exposed via the Internet. Currently, the setup of a private and secure virtual network involves manual processes at a NOC or even multiple NOCs if the services and facilities are located in different domains. But Software Defined Networks (SDN) and Network-as-a-Service (NaaS) service models can facilitate end users in eScience communities in the creation and management of virtual networks without needing to contact NOCs.

CoCo enables scientists to dynamically create a private and secure virtual network for sharing services and facilities amongst collaborators. A CoCo service can be setup by an end user through a simple and easy to use web portal, which also includes an API that developers can include in their applications. CoCo automatically sets up and manages a virtual network for a community across multiple domains, considering mobility, redundant paths, and fail-over of network connections. Consequently, CoCo's virtual networks are more agile, efficient, and robust than manually created virtual networks.

CoCo's proof of concept is being developed on existing testbeds, such as GÉANT's and SURFnet's OpenFlow testbeds, and uses existing state-of-the-art open source bandwidth on demand and NaaS frameworks where possible.

The primary objective in this project is to develop a prototype of a novel multi-domain network service, termed Community Connect (CoCo), with functionality far beyond current VPN services and which is also simple and user-friendly. To reach this objective, we have organised a workshop for researchers in various disciplines and interviewed some of them in order to understand the added value of SDN technology and useful applications for eScience and worked that out in several use cases. These use cases are the starting point for the design and implementation of a prototype, in which topics of the GÉANT activity can be further explored, i.e. hardening of network management, deterministic behaviour of networks, and networking without borders.

End users from the research or education community use CoCo to create a secure and private virtual network for sharing their resources and eScience services to which only members of the community have access. Figure 1a shows such a virtual network in blue, which is called a CoCo instance (1). End users, eScience services, and facilities are located and associated with various organisations (2). So, the CoCo service will make sure that the networks of the organisations (3), participating NRENs and GÉANT (4) are properly configured to provide a CoCo instance without manual steps of the infrastructure providers. End users that are associated to the CoCo instance, but have no access via a physical network will be able to connect to the CoCo instance via a VPN access point (5). This option also enables access to the CoCo instance with mobile devices, as long as they are connected via a VPN access point. Consequently, the end users, instruments, and eScience services will only be accessible via the CoCo instance.

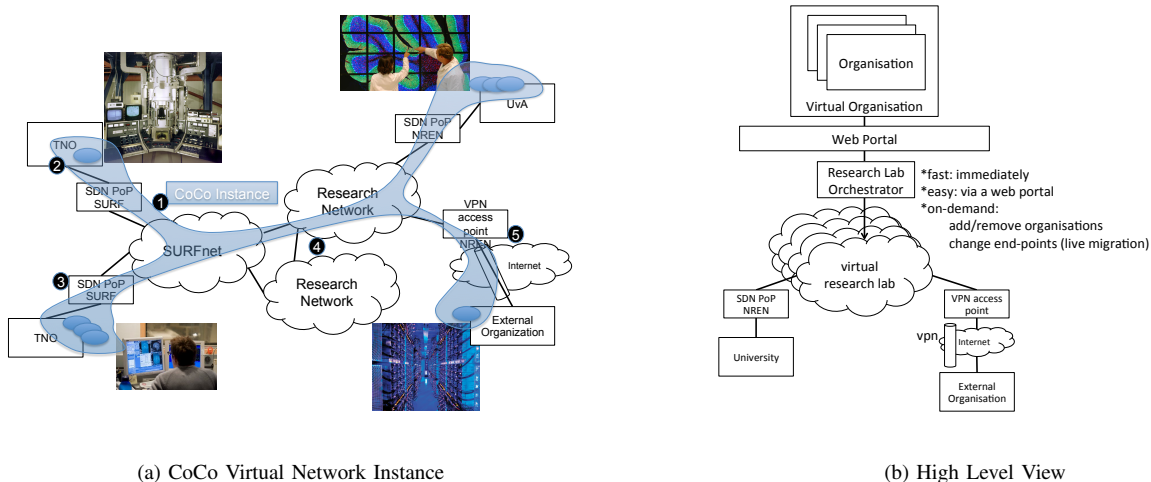


Fig. 1. CoCo Architecture

The CoCo web portal will allow end users to access and modify the properties of the CoCo instance on-demand. End users can add end points to the service via a web interface. End-points can also detach from the network infrastructure, move to another physical location and reattach without any additional configuration steps.

Because the CoCo web portal is used by end users from different organisations, federated identity frameworks are used to implement authentication and authorisation. So CoCo will assume that end users are part of a federated authentication infrastructure. This simplifies the authentication and authorisation framework for CoCo, infrastructure providers, and end users.

The CoCo service automates the configuration of networks that result in a CoCo instance, which is shown in Figure 1a. There is no need for any further manual configuration by either the end user or the infrastructure operator. Automating the network configuration leads to less mistakes, more deterministic behaviour of multi-domain networks, and easier to use services. In order to reap these benefits the CoCo service provides:

- A layer 2 network (CoCo instance) only accessible by members of that community,
- Federated authentication and authorisation,
- A web interface to create and manage CoCo instances (including migration),
- And optionally choices in terms of performance, security and stability.

The CoCo service creates an on-demand layer-2 service that connects the end-points in a CoCo instance across multiple domains. Figure 1b shows a high level view of the CoCo architecture and its interface to end users. End users use a web interface to the CoCo service for creating and managing CoCo instances and to associate users with the instances. The CoCo service exploits SDN infrastructure of each network domain, including the campus network, to negotiate, reserve, and provision network resources. For this purpose, the CoCo service communicates with agents that expose the network services, resources and features of each specific network domain. Because each network domain runs its own CoCo agent, they remain in control over their own network resources. Part of the to be developed architecture is the discovery of the multi-domain topology and how to interconnect the end-points across those domains. Scalability aspects of the discovery and management functions of the multi-domain CoCo service are explicitly addressed during the architecture development.

#### ACKNOWLEDGEMENTS

The CoCo project is one of 21 beneficiary projects of the GÉANT Open Call research project initiative, which is part of the wider GÉANT Innovation Programme. The Open Call initiative brings fresh ideas to the GÉANT project and supports new uses of the network.

#### REFERENCES

- [1] Open Networking Foundation, OpenFlow Switch Specification, Version 1.4.0 (Wire Protocol 0x05), October 14, 2013
- [2] OpenNaaS, <http://www.opennaas.org>
- [3] SURFnet Software Defined Networking, [http://www.surfnet.nl/nl/Hybride\\_netwerk/software\\_defined\\_networking/Pages/default.aspx](http://www.surfnet.nl/nl/Hybride_netwerk/software_defined_networking/Pages/default.aspx)
- [4] A Framework for the Establishment of Inter-Domain, On-Demand VPNs, A. Matos, F. Matos, P. Simoes, E. Monteiro, IEEE, 2008
- [5] Are we ready for SDN? Implementation Challenges for Software-Defined Networks, S. Sezer et al., IEEE Communications Magazine, July 2013
- [6] Towards Cloud-Ready Transport Networks, L. Contreras, et al., IEEE Communications Magazine, September 2012

## VITAE

*Ronald van der Pol* MSc has been working in the field of Education and Research Networks for more than twenty years. Since 2012 he is working on network innovation projects at SURFnet. His former employers include VU University Amsterdam, SURFnet, NLnet Labs and SARA. His current interests are in new network technologies and how these can be applied to next generation networking. This includes Software Defined Networking, OpenFlow, multipathing, load balancing and other forms of traffic engineering and optimisation, network management and monitoring, transport protocols, carrier Ethernet and end-to-end performance of demanding applications. He holds masters degrees in both Physics and Computer Science and is a frequent speaker at networking conferences.

*Bart Gijsen* MSc. After receiving his MSc. degree in both computing science and mathematics Bart joined KPN Research in 1996 as a researcher in the field of performance analysis of Internet technology based information and communication systems. From 2003 till present day Bart is employed at TNO as a senior innovator in the expertise group Performance of Networks and Systems. One of his focus areas is quantitative modelling and impact prediction of Internet security and stability. Among the 20+ journal and conference publications about performance and robustness of information and networking technology was his work on "A Global Reference Model of the DNS", for which he received the best paper award. Since 2010 Bart is also part-time director of the Dutch ICT Innovation Platform "Critical ICT infrastructures".