BUILDING FEDERATED RESEARCH NETWORKS IN EUROPE

Lars Fischer
NORDUnet, Kastruplundgade 22, DK2770 Kastrup, Denmark
e-mail: lars@nordu.net

Bartosz Belter, Milosz Przywecki
PSNC, Noskowskiego 12/14, 61-704 Poznan, Poland
e-mail: {bartosz.belter, mprzyw}@man.poznan.pl

Maribel Cosin
RedIRIS, Pza. Manuel Gomez Moreno, s/n, 28020 – Madrid, Spain
e-mail: maribel.cosin@rediris.es

Paul van Daalen, Marijke Kaat
SURFnet bv, P.O. box 19035, 3501 DA Utrecht, Netherlands
e-mail: {Paul.vanDaalen, Marijke.Kaat}@surfnet.nl

Ivana Golub, Branko Radojevic, Srdjan Vukovojac
CARNet, Josipa Marohnica 5, 10000 Zagreb, Croatia
e-mail: {ivana.golub, branko.radojevic, srdjan.vukovojac@carnet.hr

Andreas Hanemann
DFN-Verein, Alexanderplatz 1, 10178 Berlin, Germany
e-mail: hanemann@dfn.de

Paper type: Research paper

Abstract

This paper describes research carried out by the GN3 project into network federation, i.e. sharing resources among multiple independent networks. The aim of the research is to investigate how federated networks can contribute to the research and education networks' goal of improving performance and end-user service and reducing costs. To achieve this objective, we have assessed user demand for federated networks, analysing current and future projects requiring international data transmission, and investigated the three key building blocks for federated networks – network, operations and services – with particular reference to their current status among European NRENs and their potential usefulness or limitations for establishing a federation of research networks. We have used our findings to consider the architectural principles of federated networks and to develop models that optimise the use of shared resources and improve services. We have developed test cases to help refine the models, including one to support the Large Hadron Collider network, and have assessed the implications of a federated approach for both network operations and service delivery. Each of these aspects of our research is described in this paper, prefaced by a summary of the benefits and challenges of network federation and concluding with an outline of future work. The research's originality lies in its exploitation of leading-edge technologies, its innovative proposals for international collaboration, its access to and application of primary data sources. The results are of value not only to GÉANT and European NRENs but also to any special-purpose network and core networks in general.

Keywords: federated networks, multi-domain networks, cross-border fibres, federated architectures, processes

1. Introduction

Networks for research and education, such as the European National Research and Education Networks (NRENs) or the pan-European network GÉANT, continuously strive to improve performance and end-user service, and to reduce the cost of operations. This entails exploiting leading-edge technologies and establishing innovative forms of international collaboration.

Joint Research Activity 1 Task 3 (JRA1 T3) of the GN3 project aims to contribute to these dual goals by pursuing network federation, i.e. networks composed of shared resources contributed by members of a partnership. We are investigating how to combine resources from different networks in an efficient manner and how services can be improved, and detailing the implications of a federated approach for both network operations and service delivery.

As an example, imagine two GÉANT Points of Presence (PoPs), located in different countries and connected by dark fibre leased from a carrier. Now, if the NRENs of the two countries are connected by cross-border fibre, resources offered by the NRENs, either spare wavelengths or completely unused fibres, could be used to connect the GÉANT PoPs. Linking the GÉANT PoPs in this way could provide the same service quality at lower cost.

Such approaches are currently being pursued by GÉANT and some NRENs on a case-by-case basis. The goal of JRA1 T3 is to address the issue from a broader perspective. We are considering the architectural principles for building federated networks, the consequences of changing design parameters such as PoP locations and number, and the implications for network operations. The results are applicable not only to GÉANT and European NRENs but also to any special-purpose network as well as core networks in general.

2. Benefits and challenges of federating networks

This section identifies the key benefits of federated networks, and briefly discusses the main challenges.

The key benefits are:

- Improved services for multi-domain projects by offering enhanced service resilience and also by simplifying the support structures from the user perspective.
- Reduction of capital expenditure and costs of leased circuits for the networks participating in the federation. As these costs dominate the total cost of wide-area core networks such as GÉANT, major reduction of the overall cost is possible.

The main challenges are:

- Management challenges: interconnecting networks through federation requires tight collaboration in network operation. Processes for fault handling, configuration, accounting, performance monitoring, quality of service (QoS), and security management have to be coordinated.
- Technological differences and missing standards: while collaboration at the IP level is based on well-known shared standards, there is a large heterogeneity at the level(s) below IP. Every network has implemented an individual realisation of technologies such as native Ethernet, Ethernet over Multi-Protocol Label Switching (EoMPLS) or Synchronised Digital Hierarchy (SDH). This creates difficulties when a multi-domain link has to be provisioned and further complicates operational collaboration.
- Unified user view: users should experience the federated network as a single network and be unaware of the collaboration within the federation. A unified service desk has to be provided.
- Cost model: federating a network at the European level involves serious costs. It is therefore necessary to agree on a cost-sharing model and also a pricing model for the services on the federated network. The model must take into account how partners are remunerated for the resources they contribute to the federation. This problem has not yet been satisfactorily solved even in the context of cross-border fibres.

3. Analysis of user demand for federated networks

A number of current projects within the GÉANT user community require the participation of several parties. Some of these projects are implemented on a European scale, while others are on a global scale. With the evolution of networks and services it is reasonable to expect this kind of collaboration to become more common. Each of the projects features network federation in some manner, and, as users of services delivered by collaborating networks, they provide models for typical users of a future federated network. They were therefore analysed as part of our research. The focus areas of the analysis included network topology, requirements for data delivery, workflow, and cost models. The results were used to develop potential models for a future federated network. The projects analysed were:

- Large Hadron Collider (LHC) http://lhc.web.cern.ch/lhc/
  The LHC project is organised in a hierarchical model, with CERN, as the leader of the project and the site where experimental data will be produced, defined as Tier0. Tier1 participants have been defined in several countries and are connected directly to CERN through an Optical Private Network (OPN). Some Tier1 participants are also connected with each other.
- electronic Very Long Baseline Interferometry (e-VLBI) http://www.evlbi.org/
  In e-VLBI the data from distant radio telescopes is streamed to the central processor through optical fibres, and correlated in real-time. One great advantage of this technique is that the observations are no longer dependent on the availability of disk space at the telescopes, allowing long observations at high data rates.
- Enabling Grids for E-sciencE – Croatia (EGEE-III) http://www.eu-egee.org/
  The EGEE infrastructure in Croatia consists of three grid sites located in the cities of Zagreb and Split. These three sites are part of the global grid infrastructure that consists of 280 sites. The sites in Croatia provide computing power and storage space to grid users. The global infrastructure schema is available on the EGEE-III website.
- Distributed European Infrastructure for Supercomputing Applications (DEISA 2) http://www.deisa.eu
  DEISA is a consortium of national supercomputing centres that currently deploys and operates a persistent, production-quality, distributed supercomputing environment with continental scope. The purpose of this FP7-funded research infrastructure is to enable scientific discovery across a broad spectrum of science and technology, by enhancing and reinforcing European capabilities in the area of high-performance computing. This becomes possible through a deep integration of existing national high-end platforms, tightly coupled by a dedicated network and supported by innovative system and Grid software.

In addition, several projects under the European Strategy Forum on Research Infrastructures (ESFRI) umbrella were included in the analysis. ESFRI is a study of future projects to be conducted in Europe (http://cordis.europa.eu/esfri/roadmap.htm). The ESFRI projects included in the analysis were:

- LIFE WATCH http://www.lifewatch.eu
- European Bio-banking and Biomolecular Resources http://www.bbmri.eu
- INFRAFRONTIER http://www.infrafrontier.eu
- X-Ray Free-Electron Laser (European XFEL) http://www.xfel.eu
- European Extremely Large Telescope (E-ELT) http://www.eso.org/projects/e-elt
- Facility for Antiproton and Ion Research (FAIR) http://www.gsi.de/fair/index_e.html
- Partnership for Advanced Computing in Europe (PRACE) http://www.prace-project.eu
- European Incoherent Scatter (EISCAT) http://www.e7.eiscat.se

4. Contributions and limitations of current building blocks for federated networks

The continuous development of network technologies in NRENs, complemented by a new approach to interconnecting neighbouring NRENs with fibre infrastructure (cross-border fibre (CBF)development), opens new perspectives for federating network infrastructures at the "technology" layer and brings benefits not only to the parties involved (the NRENs), but, most importantly, to end users. However, the advances in technology have not been fully reflected at the operational level. This was identified at an early stage of the GN2 project and addressed during the development phase. The work done by the GN2 project partners resulted in a number of tools to support end-to-end requests from the end users of research networks. These tools supporting multi-domain workflows present an opportunity to analyse how a future federation of research networks in Europe might be built.

This section introduces the three basic building blocks of future federated networks: network, operations and services. Each component is described in detail, with particular focus on existing elements that are potentially useful for building a federation of research networks in Europe. Much of the analysis of networks draws on the responses to a survey conducted on the NRENs taking part in JRA1 T3.

4.1 Network

This section describes several NREN infrastructures as part of a bigger picture representing research infrastructures in Europe. It is based on a survey conducted on the NRENs participating in GN3 JRA1 T3, namely, CARNet, DFN, PIONIER, RedIRIS and SURFnet. The aim of the survey was to get an overview of the current status of networks in a number of countries and investigate the issues involved in a potential federated GÉANT network.

In order to investigate the potential federation of networks in Europe, emphasis was put on the following aspects:

- Network topology: how NRENs have built their networks and what kind of technology is used.
- Network coverage: the current coverage of NRENs in particular countries.
- Network utilisation: the utilisation of links in NRENs.
- Network development: future plans for network development in the countries participating in the survey.

Each of these is discussed below.

4.1.1 Network topology

According to the results of the survey questionnaire, some NRENs have leased or own dark fibre links, based on Dense Wavelength Division Multiplexing (DWDM) and Multi-Protocol Label Switching (MPLS) technologies in the core. On the other hand, there are also core networks based on leased capacities. Some NRENs have cross-border fibres (CBFs) to neighbouring NRENs, and also some point-to-point links dedicated to specific projects. NRENs have one or more connections to the Internet, via the GÉANT network and via other providers. Bandwidth in the core ranges from a few Mbps up to 40 Gbps, depending on the country and on the part of that country. There are differences between countries regarding vendors of the networking equipment used. The vendors mainly mentioned in the survey are Cisco, Juniper, Foundry Networks, Huawei and Nortel.

4.1.2 Network coverage and utilisation

There are differences among NRENs regarding how much of their network is already built and the coverage of their network. Some NRENs already connect all their member institutions, but some connect less than 60% of them. In addition, some NRENs' member institutions are at the university level (universities, research institutions, corporate R&D departments, scientific libraries, teaching hospitals), while others' members also include primary and secondary schools and related educational institutions, hospitals, libraries and other government institutions.

The most demanding users in the five NRENs surveyed are projects like LHC, DEISA, VLBI or LOw Frequency ARray (LOFAR) that are being carried out on a national level as well as on an international level. Apart from projects, NRENs usually have a few member institutions that are more active than others. These are universities or member institutions that are part of a university.

According to the responses, network link utilisation varies from less that 10% of available bandwidth to up to 90%. For a future federated network that might mean that not all links can be treated and counted on equally, otherwise network saturation might result.

For links that are used for EU projects, it was not easy to say how much bandwidth is already utilised, or how much available bandwidth can be counted on for a federated network. Some NRENs do not monitor performance on those dedicated links, while some do not monitor the activities of those projects. However, in one of the NRENs surveyed, such links have a load of 10% – 40%.

4.1.3 Cross-border fibre (CBF) initiatives in Europe

The current direction of development within European NRENs is mainly related to the expansion of optical networks based on leased or owned fibre infrastructure. Optical networks guarantee high capacity and flexibility both in network growth and in the choice of technology used. After covering their own country with optical networks, NRENs started to connect to each other. Cross-border fibres, in addition to standard GÉANT services like GÉANT Plus, have become an alternative way of providing international connectivity.

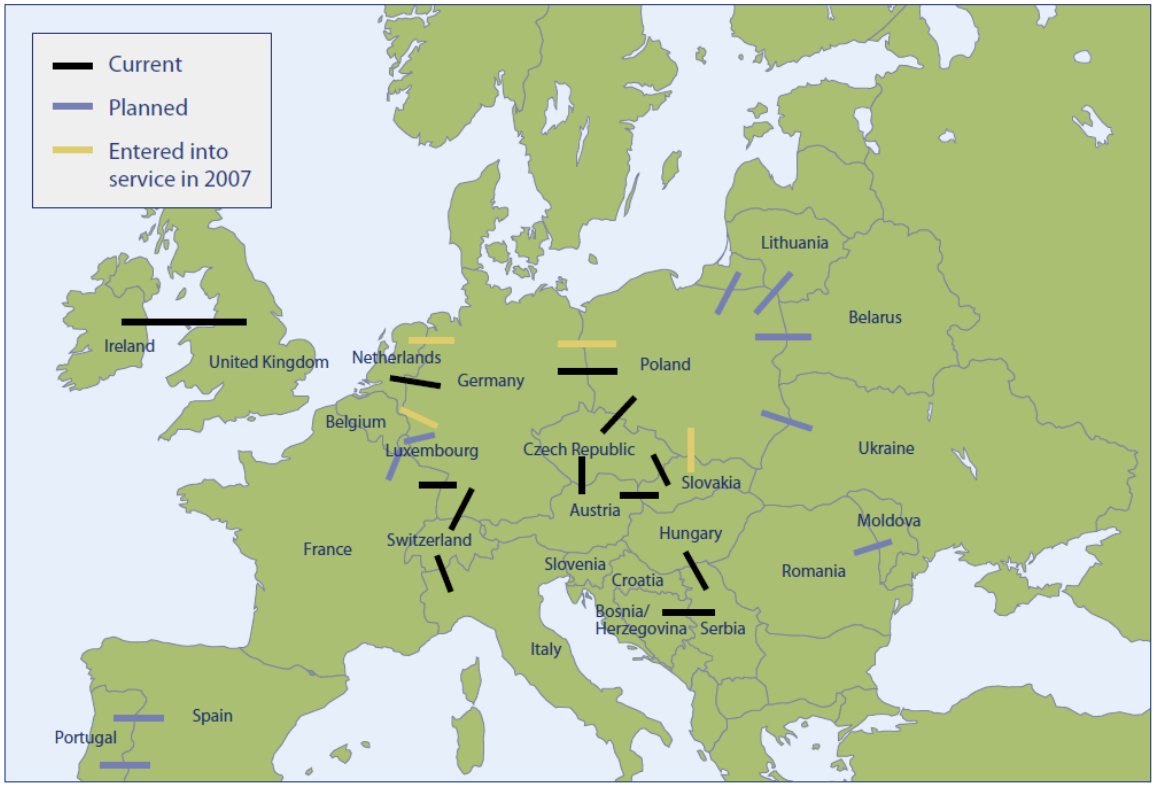
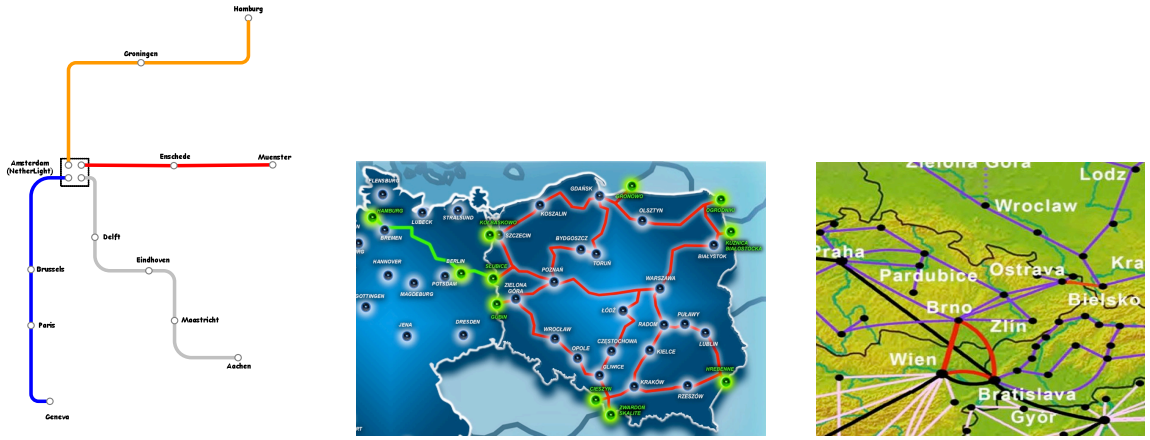


Figure 1: Global view of Cross-Border Fibres in European NRENs [1].

The level of fibre-infrastructure development varies across Europe, with a visible concentration of cross-border fibres in the centre of Europe and a relatively low number of CBFs in Western, Southern and Eastern Europe. The lower number of cross-border fibre connections in those regions may be a consequence of the level of development of the NRENs, regulations that limit the possibilities for owning fibre or creating international connections, difficulties with acquiring dark fibre from network operators, or simply that there are no requirements for creating CBF points.

Three examples of the successful deployment of cross-border fibres in Europe are described below.

- The **PIONIER** network, which is based on optical fibres, has 11 cross-border fibre connection points. It is possible to connect to each of Poland's neighbours: Russia, Lithuania, Belarus, Ukraine, Slovakia, Czech Republic and Germany. Moreover, thanks to new fibre between Słubice and Hamburg, as well as additional connection points to Germany, new possibilities for connecting to the Netherlands and the Nordic countries have arisen. The CBF points include: Germany (Hamburg, Berlin, Kołbaskowo, Słubice, Gubin); Czech Republic (Cieszyn); Lithuania (Ogrodniki); Belarus (Kuźnica Białostocka); Ukraine (Hrebenne); Slovakia (Zwardoń); and Russia (Gronowo) – to be ready in 2010.
- Currently, **SURFnet** has four CBFs – three to Germany (Hamburg, Muenster, Aachen) and one that connects Amsterdam to Geneva through Brussels and Paris.
- Cross-border fibres are also used by NRENs for increasing the reliability of connections. For example, there is a **fibre triangle between the Czech Republic, Austria and Slovakia** running at 10 Gbps, which allows the quick (around 60 ms) redirection of traffic in the event of failure of the CBF connection between two countries. It is achieved using Layer 2 protocols [2].



(a) (b) (c)

Figure 2: SURFnet CBFs (a), PIONIER CBFs (b), and CESNET, SANET and ACONET CBF triangle (c)

4.2 Operations

This section considers the potential usefulness for federated networks of current operational tools and supporting services, and discusses the administrative and procedural requirements of network federations.

4.2.1 Tools and supporting services

This section summarises the existing tools developed in GN2 and which continue to be developed as part of GN3. The requirement to support multi-domain workflows and procedures is one of the tools' basic design assumptions (except for cNIS, which supports a single-domain environment only). eduPERT is the first example of a potentially valuable item that could be re-used when building a federated environment. In contrast to the other examples, eduPERT is already a production service, which started at the end of GN2. It is mentioned here because it is helpful for a general discussion on federation; although eduPERT is not explicitly concerned with federating networks, its findings and results are nonetheless relevant to this activity.

4.2.1.1 eduPERT

eduPERT is the federated Performance Enhancement Response Team (PERT) structure that combines the independent PERTs from the local institutions, NRENs and GÉANT to support end users with performance issues. It should be considered as adding value to a federation of networks, as it actually achieves federation, but at a slightly different level. While it does not address any of the specific challenges involved in federating networks, it does solve a number of general issues related to federation. Any consideration of a future federation of networks in Europe should therefore take into account how federation has been achieved in eduPERT. The administrative structure of eduPERT has given a number of hints to JRA1 T3. For example, a decision was made to keep a central database for eduPERT services, to allow the efficient management of performance investigations across Europe. [3] describes how a fully decentralised model imposed too many constraints on the overall case-investigation process to be realised efficiently in a live environment. In consequence, eduPERT has been implemented as a compromise between fully centralised and decentralised models.

4.2.1.2 perfSONAR MDM

perfSONAR MDM provides a transparent network monitoring capability and has been designed to work in a multi-domain environment – the "MDM" in its name stands for multi-domain monitoring. It allows flexible use of monitoring tools within a domain; depending on the requirements, an organisation can deploy a different set of monitoring tools. Access to the data from other domains is possible because an agreement has been reached between networks on unified data formats and the tools developed for perfSONAR. In this way, an efficient monitoring of paths crossing multiple different domains is possible.

A federation of networks should include a monitoring service. We therefore recommend re-using the existing monitoring tools deployed in the GÉANT environment (i.e. GÉANT plus the NRENs) to provide a monitoring facility in a federation.

4.2.1.3 AMPS

From the beginning it was intended that the Advance Multi-domain Provisioning System (AMPS) would work in a federated environment. The provisioning of end-to-end (E2E) premium services in the IP layer may span a number of neighbouring domains and can be established from any of the domains participating in the AMPS pilot programme. Currently, the only administrative domains participating in the AMPS pilot are GÉANT and GRNET. The plans for future expansion are not clear. Currently, no other domain has expressed interest in deploying AMPS.

4.2.1.4 AutoBAHN

Like AMPS, supporting a multi-domain environment was one of AutoBAHN's initial design assumptions (the acronym stands for Automated Bandwidth Allocation across Heterogeneous Networks). It supports a number of technologies, from Ethernet through Synchronised Digital Hierarchy (SDH) to optical switches (Generalised Multi-Protocol Label Switching (GMPLS) is planned in GN3). At the time of writing this paper, the specification for the bandwidth-on-demand (BoD) multi-domain service is being formalised. Based on this specification, AutoBAHN will be deployed and used as an official tool for providing the BoD service to end users.

We recommend considering the BoD service (not AutoBAHN itself) as one of the building blocks for a federation of networks. The first roll-out of the BoD service is expected in the middle of Y2 of the GN3 project.

4.2.1.5 I-SHARe

Information Sharing across Heterogeneous Administrative Regions (I-SHARe) facilitates the management of a multi-domain infrastructure by providing a unified information system for all participating organisations. I-SHARe uses a central server to collect information about the different domains. Each domain can provide information about their links through the I-SHARe Domain Interface. Currently, a fully working prototype of I-SHARe is being deployed in a number of participating NRENs and DANTE [4].

4.2.1.6 cNIS

The Common Network Information Service (cNIS) collects information about single administrative domains and uses separate per-domain databases to store that information. Since the first release of cNIS, the service has been deployed in selected European NRENs. At the end of GN2, four test instances were running. At the beginning of GN3, five operational instances were launched, in Bulgaria, Ireland, Poland, Portugal and Spain [5].

4.2.2 Administration and procedures

In a loosely coupled federation, each federation partner can handle operations and service provisioning autonomously. However, in a tightly coupled federation, network operations for the federation partners' networks become directly interdependent. It is therefore necessary to have an agreed set of known procedures and workflows, e.g. for incident handling and fault management, and to back these with a set of service level agreements (SLAs). The procedures and workflows should detail the interaction between the Network Operations Centres (NOCs) of the federation partners.

For workflows and procedures to be well known, agreed by all partners, and efficient, they must be described in an operations model that details the interaction between the partners, the data sources used, and how data is updated. The operations model should bring together the actions and procedures of all partners. An example of such an operations model is the one used for the LHCOPN [6].

In addition to an operations model, a federation will need intra-federation service level agreements. External SLAs can only be honoured if partners enter into internal, intra-federation SLAs which guarantee the services each partner provides to the federation. These SLAs are similar to those required from sub-contractors in order to deliver end-to-end services in a monolithic network.

In a federated network, both user-network and supplier-network relations can be relations between partners. Such intra-federation relations are often political in nature. A governance structure must therefore be agreed for the

federation, and steering bodies, chains of command, and mechanisms for resolving disputes must be established. The governance structure should be both efficient and fair; it may, for example, assign voting rights and agree cost-sharing principles.

4.3 Services

Resources owned and operated by the federation partners are used to create, provision and operate end-user network services. Some services can be directly composed from the federation partners' network services, while in other situations federated network services are delivered by a core network built as a layer on top of the network components provided by the federation partners.

The essential network services that are required from a federated network are end-to-end circuit services, shared IP transport, and network virtualisation services. End-to-end circuit services and virtualisation services can be provided on a number of network layers, using building blocks at the appropriate layer.

In a federated approach to networks, network services have a dual role: they are both services for end users (e.g. an end-to-end SONET lightpath connecting an instrument to a computational site) and building blocks provided by federation partners to the federated network (e.g. a SONET link between two PoPs provided by a federation partner).

Services can be offered as an aggregation of similar services in the partners' networks. For such aggregation to be successful, a certain amount of glue – control plane, standard interfaces or protocols, etc. – is often needed. Alternatively, services provided by the federation partners might be used as building blocks to construct a core network on top of which the federation will offer a range of services. For example, federation partners might provide transport-level network services to the federation; the federation can then use these services to build and operate an intra-federation transport transit network offering a range of network services, including end-to-end services, shared IP services, and virtualisation.

The choice of how services are offered leads to quite different network designs for the federation. In a core network, operated as a single entity, service provision is no different from that of a traditionally designed network. With this approach, the federated network architecture is not directly visible at the service-delivery level. With the aggregated service approach, on the other hand, the service delivery itself becomes federated, offering services made of composable network elements. This choice is therefore fundamental to the network design.

5. Architecture model development and test cases

This section describes the development of the architecture models together with the test cases that will help to refine the models in the future.

5.1 Architecture models

After analysing existing projects, processes and services that are either potential users of a federation, or feature some element of federation, we have developed a federated network architecture model. The proposed model consists of three main layers: Infrastructure, Operations and Service. Each layer contains elements that are building blocks for federation. Within an architecture layer, element pairs are inter-related, through communication, data transfer flows or some logical relationship. In addition, similar relationships exist between neighbouring layers of the architecture, i.e. between the Infrastructure and Operations Layers, as well as between the Operations and Service Layers.

The Infrastructure Layer consists of networking elements (e.g. NRENs in GÉANT). These elements may vary significantly. This should be taken into account when a decision about new interconnections is being made to create a stable, sustainable, solid and scalable base for the federation. The Operations Layer includes tools and services that are needed in order to provide support for services in the Service Layer. It consists of tools, operations centres and some intra-federation services. All of these elements have the following characteristics in common: they support the upper-layer services, enable communication between the Infrastructure and Service Layers, and are not visible to the end users. The elements in the Service Layer are the various services provided to the end users by the federation.

It is recognised that there are a number of services provided by the end users of the federation, which the federation has to support. However, since providing such services is not within the scope of the federation (but the requirements of those services are), they are represented in an outer box in the figures below.

Two federated network architecture models are presented: Model A (Figure 3) and Model B (Figure 4). The models reflect the two ways communication is performed within and between layers. In order to simplify the figures, a special "Internal communication" box has been introduced, which reflects connections between different elements within a layer.

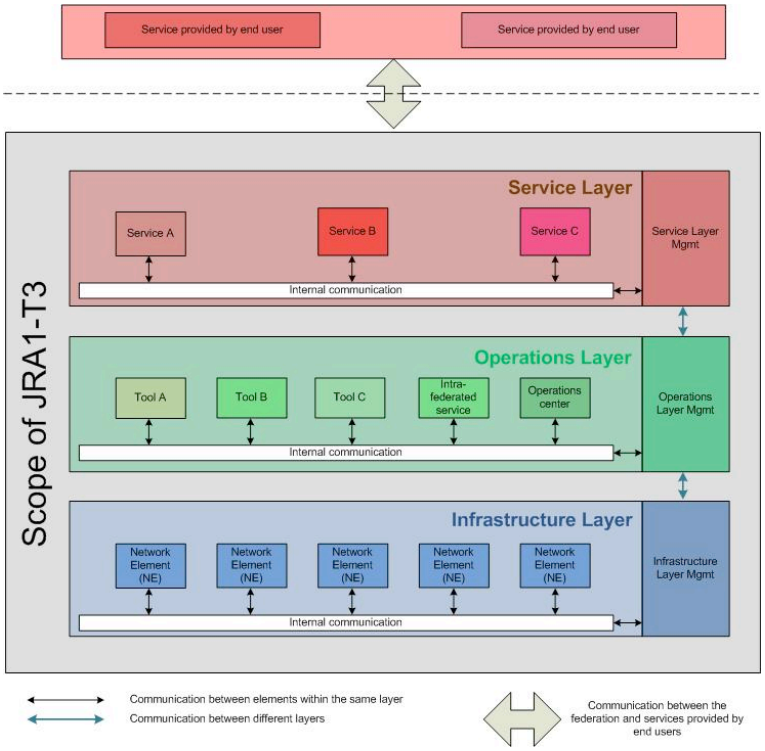


Figure 3: Federated network architecture Model A.

In Model A, all aspects of communication between layers take place only through the Layer Management of neighbouring layers. Communication between individual elements from different layers is not allowed. In addition, all data and information exchange between the Service and Infrastructure Layers has to go through and be performed by the Operations Layer. Communication within a layer is performed via internal communication. Model A is more restricted than Model B.

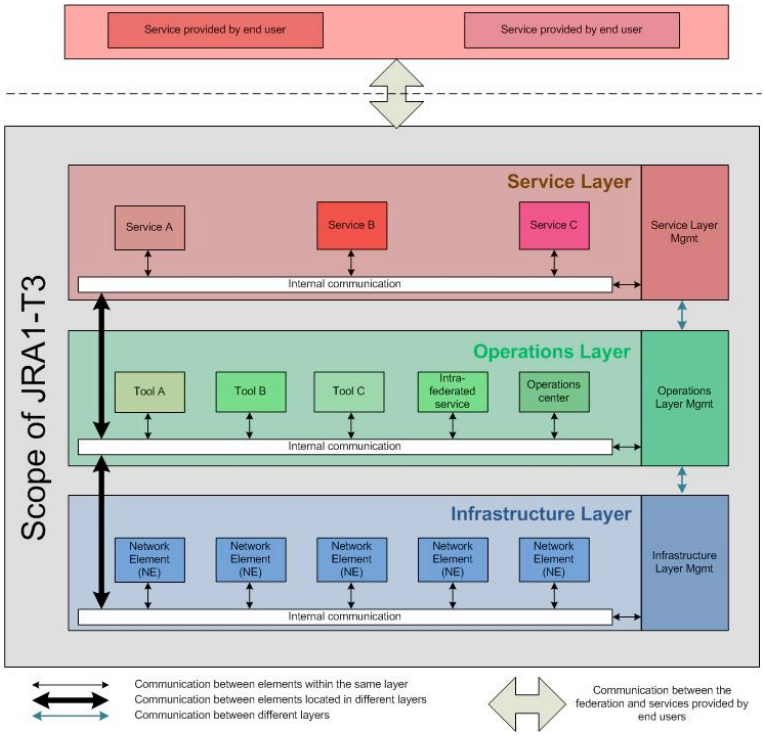


Figure 4: Federated network architecture Model B.

Model B differs from Model A in allowing more communication and information exchange channels. In Model B, individual elements within an architecture layer can communicate with another element in a different architecture layer not only via Layer Management but also directly (represented in Figure 4 as direct communication between the internal communication blocks in the different layers). Such direct communication can speed up processes and operations. However, if processes and procedures are not well defined, the greater number of communication channels can create an additional overhead, or bad information flow, both of which should be avoided.

In both models, one element can communicate with another element (including Layer Management) within the same layer directly, or via proxy. For elements in the first case, the figures show a link representing the specific procedure that supports such communication. For elements in the second case, one or more links might be missing from the figures. Important processes will still exist, however, including other elements that act as the proxy for that element for a specific activity.

Links between elements can have different meanings depending on the type of relationship, including physical connectivity, intensity of traffic flows, directions of data and information flows, dependencies in specific projects, and so on. Since each federation has its own specific elements and element connections, it is not useful to limit the definition of the term “relationship” between elements. Any potential federation should be analysed case by case to determine the existing procedures that have specific relationships which will be represented in the architecture model.

To re-emphasise, then: the links in both models represent specific processes and procedures with their respective flows of work, data or information; these should be very well defined and well known to the elements involved. At each different stage of federation – establishment, the addition or removal of an element, or federation restructuring – the relevant processes should be examined for opportunities for enhancement and optimisation.

5.2 Test cases

The two network architecture models described in the previous section appear abstract if not mapped to existing multi-domain structures that are candidates for federation. One approach for future work is to choose one (or more) existing collaborations and analyse their building blocks and relationships from the perspective of the proposed federation model.

A second approach for future work is to analyse the implications of making a change in the federation, and which model is better suited to the new situation. For example, what would be the implications for the federation of adding an element to any of the architectural layers? How would the federation behave if the number of elements was reduced? How would an architecture layer perform if one element were excluded, or joined with another in the same layer, and so on?

Possible test cases include the optimisation of the connection of GÉANT PoPs, and the LHC network. Details of the latter are given below.

5.2.1 LHC test case

For distributing the results of the LHC experiments, an Optical Private Network (OPN) has been built, linking CERN as the Tier0 centre to 10 Tier1 centres around the world. The traffic that will be distributed is regarded as stable over time because it is clear that CERN itself cannot store the huge amount of data that will be generated by the experiments.

One outstanding issue is the connection of Tier1 centres to Tier2 centres for the further distribution of data. The overall topology of these connections is unknown to a large extent. For example, the following aspects remain unclear:

- Which topology is required. In particular, how many Tier1 centres may be contacted by a Tier2 centre.
- Which paths the data flows will take.
- Whether these paths will be more or less the same over time.
- What volumes the data streams are going to have.
- What the quality expectations are in terms of availability and monitoring.

The uncertainty impacts the way a federated network should look in order to provide the best support for the project. There are several alternatives for how the GÉANT consortium might support such connections:

- As with the LHCOPN, static connections can be established between Tier1 and Tier2 centres.
  - These are useful for flows with large data volumes that are always exchanged between the same end sites and where quality expectations (concerning availability, jitter, security) are high.
- A bandwidth-on-demand solution may be provided.
  - BoD is useful for flows with large data volumes where the end sites are changing. This solution should fulfil high quality expectations (concerning availability, jitter, security) once the service is in operation.
  - The implementation of this solution is dependent on technical support from the NRENs, because BoD is a new technology and initial problems due to the newly developed software have to be taken into account.
- No additional infrastructure may be required if plain IP is regarded as sufficient.
  - This option is suitable for flows with low data volumes where no special quality demands exist.

Note that it is not necessary to adopt the same solution for every Tier1-to-Tier2-centre connection. It would even be possible to combine all three.

6. Conclusions and future work

In Y1 of the GN3 project the JRA1 T3 members have investigated the benefits and challenges of federated networks with respect to current and future research projects. Existing tools and services have been analysed to identify possible contributions towards federated networks and to point to areas where additional efforts are required. Based on these investigations, architecture models for federated networks have been developed.

In Y2, refinement of the architecture models is going to be carried out as follows. The team is going to review existing models, such as the one developed by SA2 T1, but also those in the literature, such as the Common Information Model, the enhanced Telecom Operations Map (eTOM)-related Shared Information/Data Model or the MNM Service Model, to check whether additional aspects might be included. The refinement of the models will be validated with respect to the test cases, i.e., the test-case scenarios will be modelled to ascertain whether and how the situation can be improved by the application of the models.

Also in Y2, JRA1 T3 will aim to establish relationships within and beyond the GN3 project that will show how the team's work can deliver real operational benefits as well as help to refine the models further.

References

[1] TERENA Compendium of National Research and Education Networks in Europe 2008 Edition, http://www.terena.org/activities/compendium/2008/pdf/TERENA-Compendium-2008.pdf.

[2] http://www.porta-optica.org/files/kiev/05_Kiev_Sima.pdf

[3] B. Belter, S. Leinen, T. Rodwell, M. Sotos, "GN2 Deliverable DS3.12.1: Description of a Decentralised PERT", http://intranet.geant2.net/upload/pdf/GN2-06-310v5-DS3-12-1_Description_of_a_Decentralised_PERT.pdf.

[4] G. Cesaroni, M.K. Hamm, M. Labedzki, G. Vuagnin, M. Wolski, M. Yampolskiy, "I-SHARe – a Process Support Tool for Multi-Domain Services", TNC 2009, Malaga, 8–11 June 2009.

[5] cNIS website http://cnis.psnc.pl.

[6] G. Cessieux, "Proposed LHCOPN Operational Model", https://twiki.cern.ch/twiki/bin/view/LHCOPN/OperationalModel.

Vitae

Bartosz Belter received an M.Sc. in Computer Science from the Poznan University of Technology in 2002. He works in the Poznan Supercomputing and Networking Centre as a Senior Network Engineer. He has participated in several FP6 IST projects: 6NET, PHOSPHORUS and GN2. He also participated in a number of national initiatives funded by the Polish Ministry of Science and Higher Education (Clusterix, Polish LDAP and others). Currently he is involved in two FP7 IST projects: GN3 and GEYSERS. His main research activities concern the architectural aspects of control and management planes in optical networks and QoS in next-generation packet networks.

Maribel Cosin works in the Network department at RedIRIS, which is responsible for designing, building and managing the RedIRIS network. She completed her B.Sc. in Telecommunications Engineering in 1996, at the Universidad Politécnica de Madrid, and joined RedIRIS eleven years ago. She has participated in the deployment of the current network infrastructure (RedIRIS-10) and is collaborating on the design of the new one (RedIRIS Nova), based on dark fibre. Since January 2005 Maribel has been responsible for the Level 1 Operations Team at RedIRIS. She is also responsible for the DNS service and the RedIRIS Réseaux IP Européens (RIPE) interface.

Paul van Daalen joined SURFnet in January 2009 as a Senior Network Planner. Prior to this he was Director of the Information group at Leiden University for 8 years. During the last 25 years Paul has worked with various kinds of telecommunication and IT systems and structures. As an IT professional he was employed for 17 years by Delft University, where he was responsible for Network Development and Operations.

Lars Fischer is the Chief Technology Officer of NORDUnet. He has spent the past 25 years at ISPs, telcos, and research institutions, and has worked within the areas of systems architecture, network design, network and systems management, software development, and grid computing. Lars was co-author of the GN3 project proposal and is involved in network architecture and federated networks, as well as project governance.

Ivana Golub is a Deputy CEO at CARNet, in charge of the Network Infrastructure Department, which is responsible for designing, building and maintaining the CARNet network and network services. She received her B.Sc. and M.Sc. degrees in Electrical Engineering at FESB, the University of Split. During the last 10 years Ivana has worked in networking, in areas ranging from LAN to WAN, and in positions ranging from architect to manager. Ivana is involved in the GN3 JRA1 activity related to federated networks.

Andreas Hanemann received a Ph.D. in Computer Science from the University of Munich, Germany. In GN3 he is involved in activities related to federated networks, multi-domain service specification and network performance monitoring. After working in a network monitoring project at the Leibniz Supercomputing Centre in Munich from 2002 till 2007, he joined the DFN main office in Berlin in October 2007.

Marijke Kaat works in the Networking Services Department at SURFnet, which is responsible for designing, building and managing the SURFnet network. She received her M.Sc. degree in Computer Science at the University of Amsterdam, Faculty of Mathematics and Computer Science. Since 1992 Marijke has worked in Network Management and Operations, providing technical consultancy on networking, infrastructure, service development, support and training in wide area and local area networking.

Milosz Przywecki received an M.Sc. degree in Electronics and Telecommunications from Poznan University of Technology in 2003 and joined the Network Division of Poznan Supercomputing and Networking Centre as a Networking Systems Analyst in 2005. His main interests are in advanced networking technologies, network protocols and services.

Branko Radojevic is a Deputy CEO at CARNet, in charge of the Applied Systems and Services Department, which is responsible for designing, building and maintaining CARNet's computer and storage infrastructure. He received his B.Sc. and M.Sc. degrees in CIS/MIS from the Columbia Southern University (Alabama, US). Branko is currently leading the national VoIP project in Croatia and is involved in the GN3 JRA1 activity.

Srdjan Vukovojac is Head of the Network Operations Centre (NOC) at CARNet, responsible for day-to-day network operations and maintenance. He received his B.Sc. in Electrical Engineering from the University of Zagreb, Croatia in 1998. Since then he has been working with various information and network systems with a special interest in computer networking, including both network design and maintenance. Srdjan is involved in the GN3 JRA1 activity related to federated networks.