Future Internet Cross-Domain and Cross-Layer Experimentation

Piet Demeester, Tim Wauters, Bart De Vleeschauwer, Brecht Vermeulen, Filip De Turck
Dept. Information Technology (INTEC), Ghent University - IBBT
Gaston Crommenlaan 8, bus 201, B-9050 Ghent, Belgium

Abstract -- Research on Future Internet technologies requires experimental facilities in order to develop and validate novel ideas and technologies. Today there are many national and international initiatives that build and provide these experimental facilities to researchers and developers. Although many of these facilities are still stand-alone and targeting at rather specific cases, there is a clear tendency to federate facilities in order to provide additional capabilities, otherwise not possible.
Testbed infrastructure federation enable large scale or heterogeneous cross-domain experiments but it can also allow cross-layer experimentation (from physical layer aspects up to the direct involvement of end-users evaluating advanced applications and services). This paper will present some ideas on future internet experimentation from a cross-domain and cross-layer point of view.

I. INTRODUCTION

Testbed federation aims at creating physical and logical interconnections between several independent experimental facilities to provide a larger-scale, more diverse and/or higher performance platform for accomplishing advanced tests and experiments. The ongoing facility prototyping projects in the FIRE [1] initiative, such as Onelab2, Panlab II, Federica, Wisebed and Vital++, already reach very promising results for sustainable federation by offering these mostly independent testbeds to the broader research community. These FIRE prototyping efforts are loosely coupled through the support action FIREworks, whose major role is to orchestrate and stimulate strategy discussions involving the FIRE stakeholder community, the user communities and other related initiatives in the EU Member States and abroad.

II. CROSS-DOMAIN EXPERIMENTATION

Fig. 1 describes a cross-domain experimental facility from a technical viewpoint. The *Core Network* connectivity is offered by existing public networks (e.g. public Internet: commercial ISP's or NREN's), a field deployed experimental Internet (e.g. as provided by Federica) or an emulated experimental Internet (e.g. as provided by Emulab or iLab facilities). Different *Access, Building and Home Networks* can be distinguished, providing public access (e.g. public hot spots), field deployed experimental access (e.g. an experimental wireless sensor network in an office environment) or emulated experimental access (e.g. emulated wireless links). As a consequence, *Computing, Storage and Information Resources* from public (e.g. Amazon or Google resources) or experimental (e.g. Emulab or Grid5000 facilities) origin become available to the *Terminals*. The latter include both public (e.g. 3G terminals or thin clients) and experimental Terminals (e.g. experimental terminals with displays integrated in textiles and voice activation or standard terminals with experimental software).
However, in order to arrive at an open and trusted federated platform, higher levels of interconnectivity, interoperability

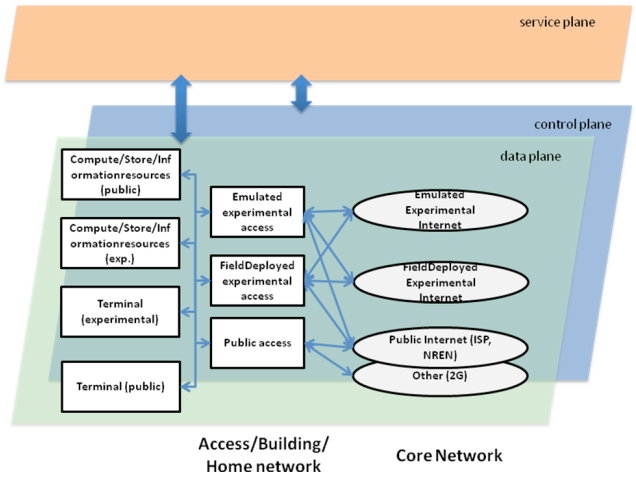

Figure 1. Technical view of the federated experimental facility

and interworking have to be achieved by automated resource reservation and measurement tools, easily accessible through a user-friendly and intelligent portal.

III. CROSS-LAYER EXPERIMENTATION

Adding new capabilities to the existing experimental facilities allows for experimentation at different layers and as well as from a system perspective.
Generic emulation testbeds, such as the iLab Virtual Wall [2], currently support large scale network layer experiments through node virtualization techniques, automatic topology construction mechanisms, generic traffic generators and extensive resource monitoring tools. In order to allow for system level experiments, these environments also need to address similar functionality for the service layer. Such functionality includes automatic install of application servers, generation of service requests (e.g. based on WSDL, IDL, EJB interfaces) for a variety of configurable parameters (e.g. spatial or temporal request distribution, service popularity), monitoring of performance of service instances (e.g. response times, bandwidth/CPU/RAM consumption and availability over time) and generation of service-specific proxy components to shield or modify existing services.
Example use cases include: (i) evaluating large scale eHealth applications by generating client requests (automated secure login) and benchmarking the throughput and response times of the different available operations in an automated way, and (ii) evaluating large scale multimedia content retrieval services based on semantic information by automatic generation of user queries and scalable logging of individual user session response times.

[1] FIRE, http://cordis.europa.eu/fp7/ict/fire/
[2] iLab, http://ilabt.ibbt.be