FUTURE INTERNET TESTBEDS
EXPERIMENTATION BETWEEN
BRAZIL AND EUROPE

Grant Agreement No.: 288356 (FP7)
CNPq Grant Agreement No.: 590022/2011-3

FIBRE-EU

Future Internet testbeds/experimentation between Brazil and Europe – EU

Instrument**: *Collaborative Project***
Thematic Priority: ***[ICT-2011.10.1 EU-Brazil] Research and Development cooperation, topic c) Future Internet – experimental facilities***

D5.3: Final report on the validation and demonstration of the federated pilots/showcases

Author: WP5
Revised by: i2CAT
Due date of the Deliverable: Month 39
Actual submission date: 29/09/2014
Start date of project: June 1st 2011 Duration: 34 months
Version: v.1.3

Project co-funded by the European Commission in the 7th Framework Programme (2007-2013)		
Dissemination Level		
PU	Public	✓
PP	Restricted to other programme participants (including the Commission	
RE	Restricted to a group specified by the consortium (including the Commission	
CO	Confidential, only for members of the consortium (including the Commission Services)	

FP7 Grant Agreement No.	288356
CNPq Grant Agreement No.:	590022/2011-3
Project Name	Future Internet testbeds/experimentation between Brazil and Europe – EU
Document Name	FIBRE-D5.3
Document Title	D5.3: Final report on the validation and demonstration of the federated pilots/showcases
Workpackage	WP5
Authors	Mayur Channegowda (UNIVBRIS) Roberto Monno (NXW) Natalia Castro Fernandes (UFF) Fernando Redigolo (USP)
Editor	Mayur Channegowda (UNIVBRIS)
Reviewers	i2CAT
Delivery Date	29/09/2014
Version	V1.3

Abstract

The aim of work package 5 is to develop local and federated technology pilots and validate the deployed FIBRE facilities through showcases, which have been pre-selected from a number of use cases (UCs): Seamless Mobility, High Definition content delivery and Bandwidth on Demand through OpenFlow and GMPLS. Previous deliverables of WP5: D5.1 [21] and D5.2 [22] present a global and homogeneous view of these UCs focusing on their overall goals and objectives, requirements, involved technologies, developed building blocks and on the integration of these modules as a whole.

This deliverable, D5.3, utilizes the deployed use cases to evaluate the federated facility capabilities and validates if it meets the requirements set out in D5.1. It introduces to the scope of the validation, briefly introducing the use case, its execution and its flow. It details the user steps that are necessary to execute the use case on the FIBRE facility and also listing the events where the use case was demonstrated. Using the pilot execution process and facility evaluation criteria's, the federated FIBRE facility features are validated against the requirements of D5.1. This document also provides use case results in terms of technical and dissemination activities.

TABLE OF CONTENTS

1 Acronyms ... 6
2 Scope ... 8
3 Reference Documents ... 9
4 Introduction ... 11
5 Validation process and objectives ... 12
6 Implementation of use cases ... 14
6.1.1 UC1: Seamless mobility ... 14
6.1.1.1 Use Case Flow ... 16
6.1.1.2 UC1 demonstration info ... 29
6.1.2 UC2 : High Definition content delivery ... 30
6.1.2.1 Use Case 2 workflow ... 30
6.1.2.2 Use Case 2 Demonstration ... 33
6.1.3 UC3: Bandwidth on Demand ... 36
6.1.3.1 UC3 workflow ... 36
6.1.3.2 UC3 demonstration info ... 39
7 Validation methodology by requirements ... 42
7.1.1 Background on Requirements ... 42
7.1.2 Evaluation criteria ... 42
7.1.3 UC1 Validation Results ... 45
7.1.4 UC2 Validation Results ... 46
7.1.5 UC3 Validation Results ... 48
8 Testbed evaluation results ... 50
9 Conclusion and outlook ... 55
10 Annex 1 ... 56
11 Annex 2 ... 60
12 Annex 3 ... 61
13 Annex 4 ... 62

List of Figures

Figure 1 - Mini-itx based nodes, which are diskless nodes developed in the context of WP5 in order to increase the number of wireless devices. 15
Figure 2 - Mobile node. 15
Figure 3 - Monitoring Node. 16
Figure 4 - FIBRE portal in UFF Island. 17
Figure 5 - Reservation section in the portal, which allows the user to list and reserve the available resources. 17
Figure 6 - Node reservation. More information about hostname, HRN, and control IP is available by passing the mouse over the node name. 18
Figure 7 - List of scheduled times to use OMF testbed. 18
Figure 8 – Detailed list of reserved resources of the selected reservation. 19
Figure 9 - Wireless monitoring system access. 20
Figure 10 - Wireless monitoring system home, which provides access to real-time monitored data and also to a video explaining how the system works. 20
Figure 11 - Access to monitored data in the 11 channels of IEEE 802.11 g. 21
Figure 12 - Channel 1 result for each monitoring node 21
Figure 13 - Example of horizontal handoff [4]. 23
Figure 14 - Search and execution phases in a handoff. [4] 24
Figure 15 - Resource selection 31
Figure 16 - Controller showing discovered switches and switching type 32
Figure 17 - CPU & Memory threshold increase identification 33
Figure 18 - Use Case 2 partial monitoring demonstration at FIA Dublin 2013 34
Figure 19 - negative case where request fails 38
Figure 20 - Successful request 39
Figure 21 - UC3 poster for the 2th open workshop - Barcelona, 5 November 2013 40
Figure 22 - UC3 poster for the FIA meeting 41

List of Tables

Table 1 Results of the delay test in the horizontal handoff experiments 28
Table 2 Facility Validation Table 43
Table 3 UC1 validation results 45
Table 4 UC2 validation results 46
Table 5 UC3 validation results 48

1 Acronyms

AM	Aggregate Manager
AP	Access Point
API	Application Programming Interface
BoD	Bandwidth on Demand
CDN	Content Delivery Network
CDS	Content Delivery Server
CLI	Command Line Interface
CORBA	Common Object Request Broker Architecture
CRUD	Create, Read, Update and Delete
CP	Control Plane
DPID	DataPath IDentifier
DPS	Discovery Packet Switches
E-OFC	Extended-OpenFlow Controller
FIBRE	Future Internet testbeds / experimentation between Brazil and Europe
F-PCE	Flow-aware Path Computation Element
FPGA	Field-Programmable Gate Array
FV	FlowVisor
GMPLS	Generalized Multi-Protocol Label Switching
GUI	Graphical User Interface
HTTP	HyperText Transfer Protocol
IM	Island Manager
LLDP	Link Layer Discovery Protocol
LSP	Label Switched Path
MS	Milestone
NE	Network Element
NMI	Network Management Interface
NOX	OpenFlow Controller
OCF	OFELIA Control Framework
OF	OpenFlow
OFELIA	OpenFlow in Europe: Linking Infrastructure and Applications
OFV	Optical FlowVisor
OMF	cOntrol, Management and Measurement Framework
OML	ORBIT Measurement Library
OSPF-TE	Open Shortest Path First - Traffic Engineering
OSS	Open Source Software
p.	Page
QoS	Quality of Service
ROADM	Reconfigurable Optical Add-Drop Multiplexer
RSVP-TE	Resource Reservation Protocol - Traffic Engineering
SDN	Software Defined Networking
SFA	Slice-based Federation Architecture

SNMP	Simple Network Management Protocol
STA	Mobile station
SSH	Secure Shell
TCP	Transmission Control Protocol
TED	Traffic Engineering Database
UDP	User Datagram Protocol
UNI	User Network Interface
UC	Use Case
VLAN	Virtual Local Area Network
VM	Virtual Machine
VON	Virtual Optical Network
VT	Virtualization Technology
WP1	Project Management
WP2	Building and operating the Brazilian facility
WP3	Building and operating the European facility
WP4	Federation of facilities
WP5	Development of technology pilots and showcases
WP6	Dissemination and collaboration

2 Scope

This report shows the final results obtained with pilots 1, 2, and 3. It also validates all the requirements, correlating them with the building blocks.

3 Reference Documents

1. Olivier Marce, Hoang-Hai Tran, and Bruno Tuffin. 2014. Double-sided auctions applied to vertical handover for mobility management in wireless networks. J. Netw. Syst. Manage. 22, 4 (October 2014), 658-681.

2. Kantubukta Vasu, Sudipta Mahapatra, and Cheruvu Siva Kumar. 2014. A Comprehensive Framework for Evaluating IPv6 Based Mobility Management Protocols. Wirel. Pers. Commun. 78, 2 (September 2014), 943-977.

3. Tomislav Shuminoski and Toni Janevski. 2014. Radio Network Aggregation for 5G Mobile Terminals in Heterogeneous Wireless and Mobile Networks. Wirel. Pers. Commun. 78, 2 (September 2014), 1211-1229.

4. Ajeet Nankani (2005). Horizontal Handoffs within WLANs – A detailed analysis and measurement concerning voice like traffic (Master's Thesis). School of Information and Communication Technology (ICT) , Royal Institute of Technology (KTH), Stockholm, Sweden. 71 pages.

5. A. Mishra, W. Arbaugh, and M. Shin "An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process" ACM SIGCOMM Computer Communication Review., Vol: 32, Issue: 2, Pages: 93 – 102, April 2003.

6. Ryan Izard, Adam Hodges, Jianwei Liu, Jim Martin, Kuang-Ching Wang, and Ke Xu, An OpenFlow Testbed for the Evaluation of Vertical Handover Decision Algorithms in Heterogeneous Wireless Networks, TRIDENTCOM 2014.

7. [FIBRE] http://www.fibre-ict.eu/

8. [OFELIA] http://www.fp7-ofelia.eu/

9. [NOX] http://www.noxrepo.org/

10. [NOX REPO] https://github.com/noxrepo/nox-classic

11. [NOX WIKI] https://github.com/noxrepo/nox-classic/wiki

12. [POX] OpenFlow Controller https://openflow.stanford.edu/display/ONL/POX+Wiki

13. OpenFlow Switch Specification version 1.3.0 - https://www.opennetworking.org/images/stories/downloads/specification/openflow-spec-v1.3.0.pdf

14. OpenFlow Switch Specification version 1.0.1 - https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.0.1.pdf

15. Extensions to the OpenFlow Protocol in support of Circuit Switching - http://www.openflow.org/wk/images/8/81/OpenFlow_Circuit_Switch_Specification_v0.3.pdf

16. FP6 PHOSPHORUS – Deliverable D2.3 "Grid-GMPLS high-level system design"

17. [IETF RFC 4655] – "A Path Computation Element (PCE)-Based Architecture", Informational RFC, Aug. 2006

18. Milestone MS5.1: Report on technology building blocks

19. M. Channegowda, P. Kostecki, N. Efstathiou, S. Azodolmolky, R. Nejabati, P. Kaczmarek, A. Autenrieth, J.P. Elbers, D. and Simeonidou, "Experimental Evaluation of Extended OpenFlow Deployment for High-Performance Optical Networks," in Proceedings of ECOC, Tu.1.D.2 (2012).

20. Okung-Dike Ntofon, Mayur P. Channegowda, Nikolaos Efstathiou, Mehdi Rashidi Fard, Reza Nejabati, David K. Hunter, and Dimitra Simeonidou, "Experimental demonstration of OpenFlow-enabled media ecosystem architecture for high-end applications over metro and core networks," Opt. Express 21, 4811-4816 (2013)

21. [D5.1]: Report on the detailed design and development of technology pilots

22. [D5.2]: Report on integration of local and federated showcases

23. [D5.4]: Content-delivery controller application software

24. [D5.5]: GMPLS as-a-service control plane controller application software

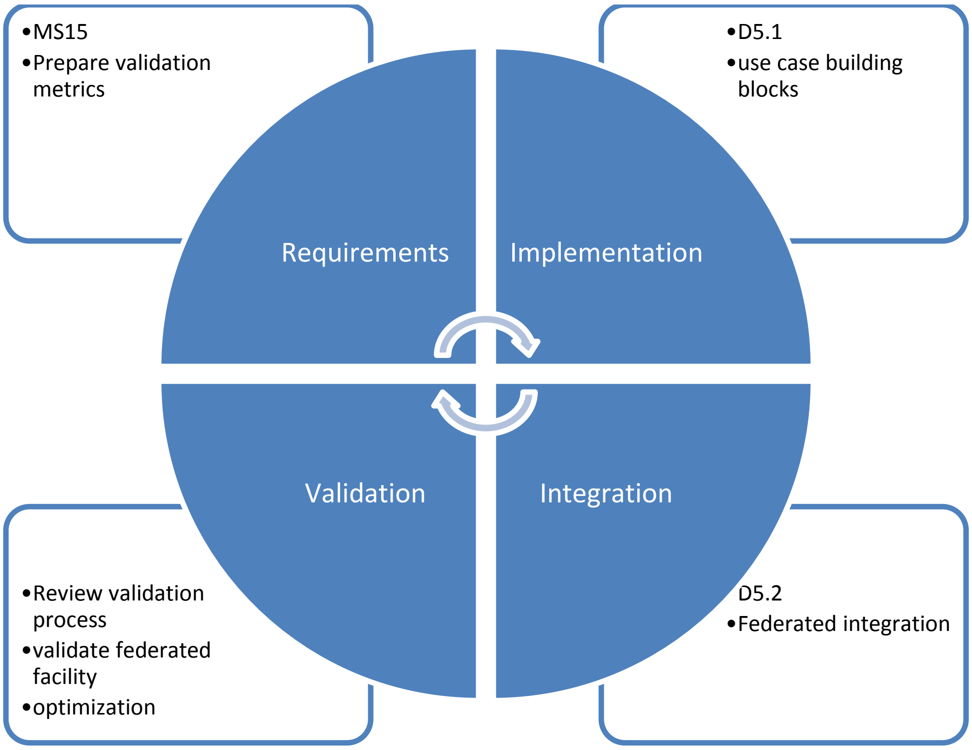
25. [D5.6]: Seamless mobility controller application software

4 Introduction

This chapter describes the validation process beginning from M24 of the project timeframe. In the beginning months of WP5 task technology pilots requirements & validation process was defined (MS15 & D5.1), while the execution of it began when the first results were available. The validation depicted here follows a technical approach, as the main activity of work package 5 was in the development and implementation of use cases. The validation activities here focus on both use cases definition and implementation phase and its validation over the FIBRE federated facility. The goal is to use the use case execution results to validate the facility against the requirements that were defined in the early stages of the project.

5 Validation process and objectives

WP5 activities were categorized into 4 main parts as depicted in the figure below. The process of technology pilots requirement collection, its implementation & integration were performed in the Task5.1 & Task5.2 and are detailed in deliverables D5.1 & D5.3. Based on the requirements collection a set of facility validation goals were envisioned which can be evaluated using use case execution cycle.



Following briefly describes the goals of each use case:

Higher Level Facility Goals:

Use Case 1:

- Analyse and utilize the capabilities of wireless networks to show seamless handoffs experience
- Exploit facility programmability aspects to perform multipath communication to support various levels of mobility

- Extend FIBRE framework (OMF) to share large scale distributed mobile networks to be used by various network/wireless researchers
- Provide environmental monitoring tool to support the analysis of the test results

Use Case 2:

- Exploit enhanced functionalities of a OpenFlow enabled control plane for experimenters
- Apply flow forwarding/routing concepts to load balance traffic to show dynamic infrastructure programmability
- Enable traffic monitoring (network & IT) to enable media application aware (4K) traffic load balance

Use Case 3:

- Exploit flexibility of SDN enablers (OpenFlow, GMPLS) to implement an open and generalized Bandwidth on Demand (BoD) service for heterogeneous resources (optical & packet)
- Integrate existing tools (FlowVisor, BoD application OpenFlow controller etc.) to show facility flexibility

Based on these high level goals WP5 collected requirements in terms of hardware and software which are listed in deliverable D5.1. These formed the basis for the use case design, development and deployment which are described categorically in the next section.

Note: the description of the use cases in the next section includes more details than the deliverable D5.2, D5.4, D5.5 & D5.6.

6 Implementation of use cases

This section includes use case description from a user perspective. It details the steps the user has to follow to run the use case over the FIBRE facility. Demonstrations performed during the course of WP5 is also described in the section.

6.1.1 UC1: Seamless mobility

In the context of UC1, we developed an infrastructure which is auxiliary to the island topology proposed in WP2. In WP2, we developed islands in Brazil that contain both OMF and OCF. Concerning the OMF WP2 related infrastructure, most of the islands are equipped with an OMF virtual server and six Icarus nodes.

The proposal of Use Case 1 was to provide a remote controlled infrastructure that allows experiments of wireless networks and mobility. In this sense, we would need more experimenting nodes, at least one mobile node, and a monitoring infrastructure in order to provide a proper environment for researchers.

To accomplish the observed requirements, we build UFF Wireless Island with the following devices:

- Icarus nodes, which contains two wireless interfaces that allows the use of IEEE802.11 a/b/g/n, and two wired interfaces[1].
- Mini-itx based nodes, which were developed in UFF, containing an IEEE 802.11 b/g/n interface and a Bluetooth interface. Also, it provides a wired interface for both control and experimental traffic. The Mini-itx node is shown in Figure 1.
- Mobile node, also called train, which runs through 100 meters, equipped with a notebook with two wireless interfaces, one for control (IEEE802.11b/g/n) and the other for experiments (IEEE 802.11 a/b/g/n). Also the notebook has a Bluetooth interface. The mobile node also uses two cameras for the experimenter to watch the movement in case this is needed. The developed mobile node is shown in Figure 2.
- Monitoring nodes, which are TP-Link access points equipped with AirView Spectrum Analyzers, as shown in Figure 3.
- Virtual OMF server.

[1] We change the power source of the Icarus nodes due to a high instability of the original power sources in the Brazilian power system.

The main reason for the mini-itx nodes was to develop a low-cost solution to increase the number of nodes that can be used for experimentation in accordance to the project budget. The monitoring system allows the experimenter to choose the best channels to the experiment as well as to observe whether there were strong outside interferences in the experiment. The mobile node is the key platform for creating the mobile scenarios.

Figure 1 - Mini-itx based nodes, which are diskless nodes developed in the context of WP5 in order to increase the number of wireless devices.

Figure 2 - Mobile node.

Figure 3 - Monitoring Node.

6.1.1.1 Use Case Flow

The experimenter accesses the developed infrastructure through the FIBRE portal and, after that, through SSH.

First, the experimenter must visit the NOC or the UFF portal in order to reserve the resources. The NOC portal (https://portal.fibre.org.br) provides access to all OMF FIBRE resources. In addition, each island has its own portal which provides access to the island resources. The following explanations assume the use of the UFF portal (https://portal.uff.fibre.org.br), shown in Figure 4.

Through the portal, the user creates an account, logins, and checks the available resources, as shown in Figure 5. In this page, the user discovers more information about the node by passing the mouse through the node name, as shown in Figure 6. It is important to notice that information about available hardware and position of the nodes is available in Resources section in the portal.

The reservation system allows users to choose nodes, date, and time. The resource will be available to experimenter only in the scheduled times through the OMF virtual server. The user can check his reservation through My Reservation section, described in Figure 7 and Figure 8.

Figure 4 - FIBRE portal in UFF Island.

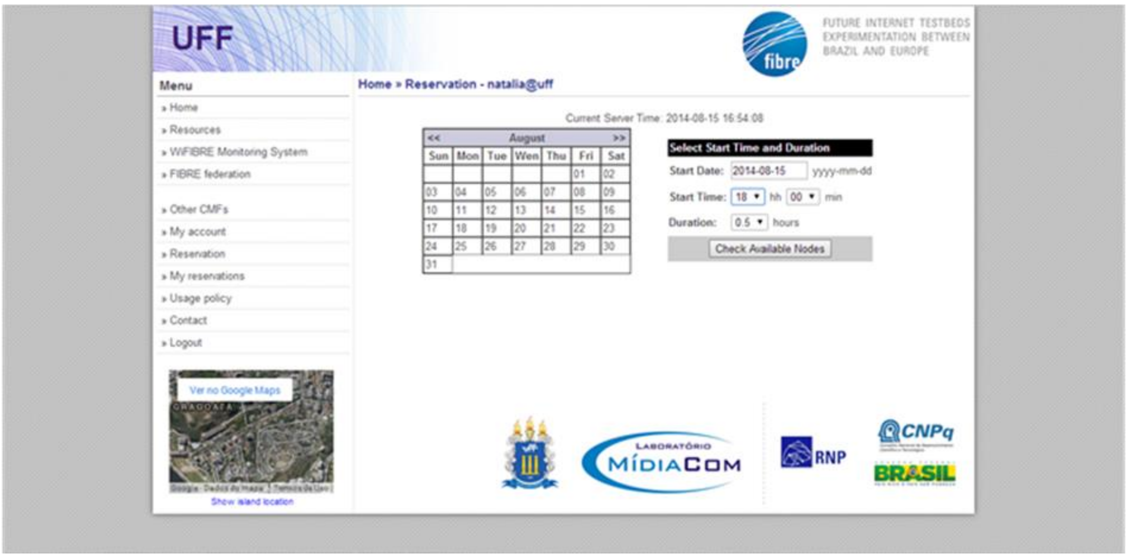


Figure 5 - Reservation section in the portal, which allows the user to list and reserve the available resources.

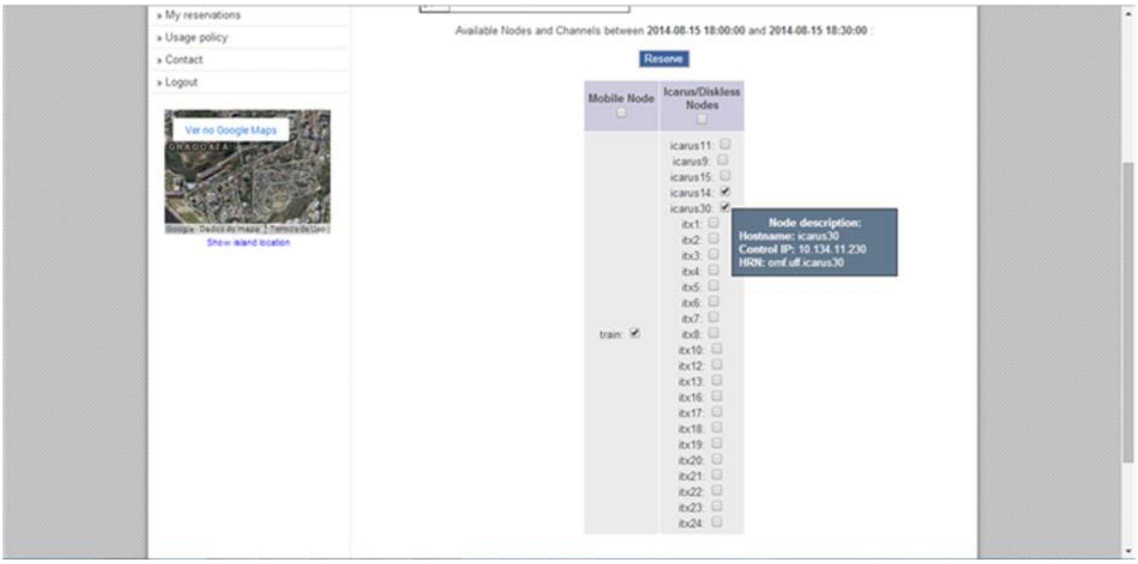


Figure 6 - Node reservation. More information about hostname, HRN, and control IP is available by passing the mouse over the node name.

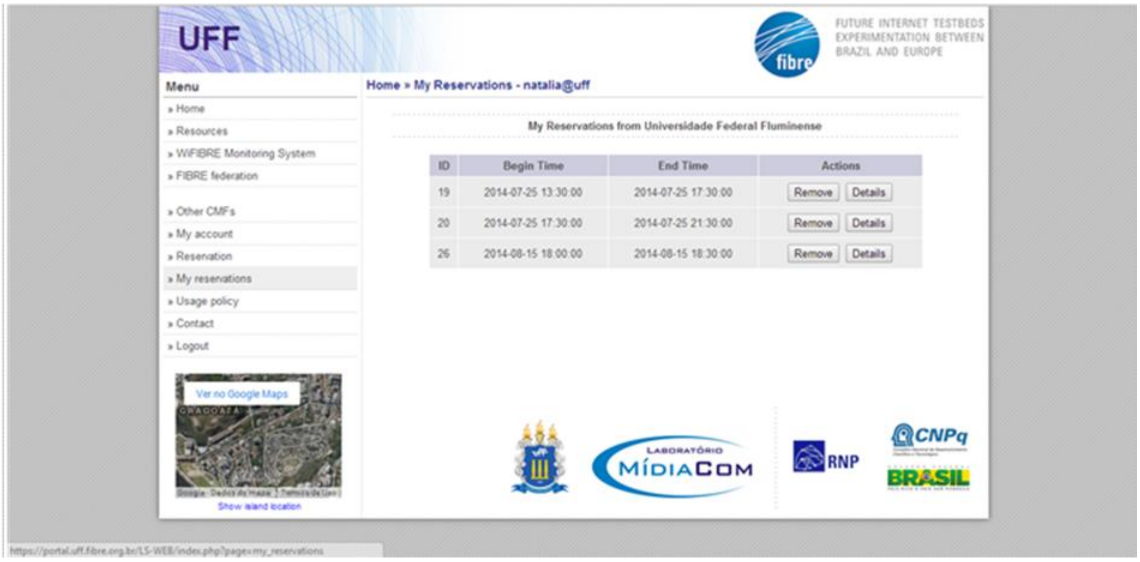


Figure 7 - List of scheduled times to use OMF testbed.

Figure 8 – Detailed list of reserved resources of the selected reservation.

During the scheduled times, the user can access the reserved resources by executing an SSH to the OMF virtual server. In the case of UFF Island, this is done by accessing IP 200.20.10.88 in port 6622. The port is a standard for all OMF FIBRE islands. Another option is to access FIBRE VPN and do an SSH to 10.134.11.200, also using port 6622. The user must perform the SSH using the credentials created to access the portal. This means that the login is username@institution and password is the same used in the portal.

Once inside OMF server during the reservation time, the user is able to SSH to all reserved resources and configure them accordingly to the experiment. Another option is to develop an OMF script in order to automatically deploy all node configurations. OMF commands, such as omf tell, which tell the current reserved resources, are also available through command line in OMF server.

The access to the monitoring system is open and is available only through UFF portal, by clicking on the WIFIBRE monitoring system, as shown in Figure 9. The home page of the monitoring system (Figure 10) provides access to the real-time monitored data.

All the monitored data is related to the use of the 2.4 GHz spectrum. This corresponds to IEEE 802.11 b/g/n and also to Bluetooth. Even though we also have IEEE 802.11 available, we are not able to monitor the 5GHz spectrum due to hardware limitations. Hence, as shown in Figure 11, we can access data of the monitoring nodes according to the selected channel.

Figure 9 - Wireless monitoring system access.

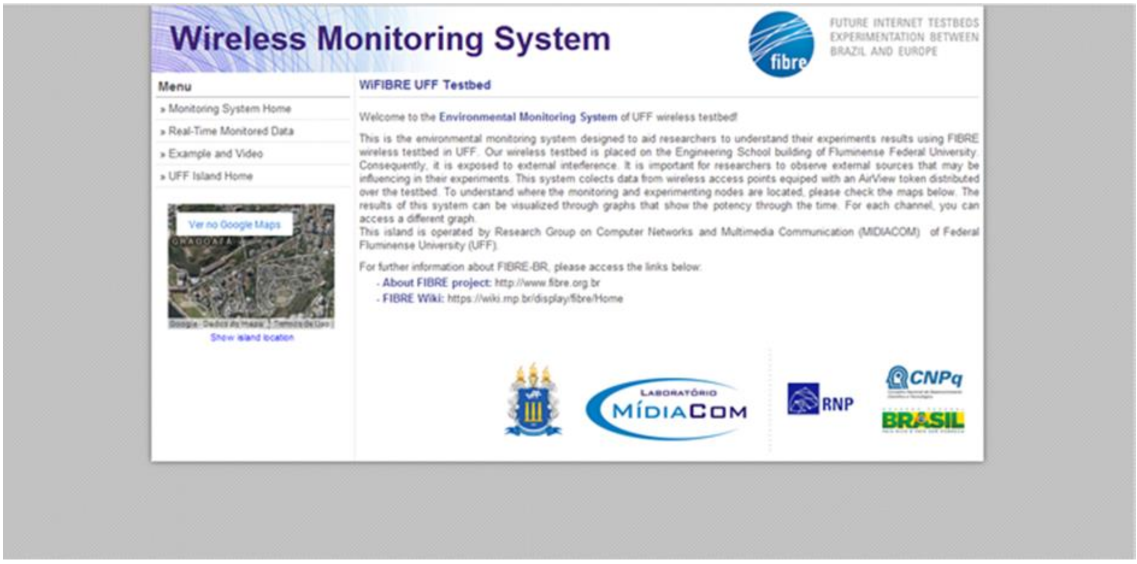
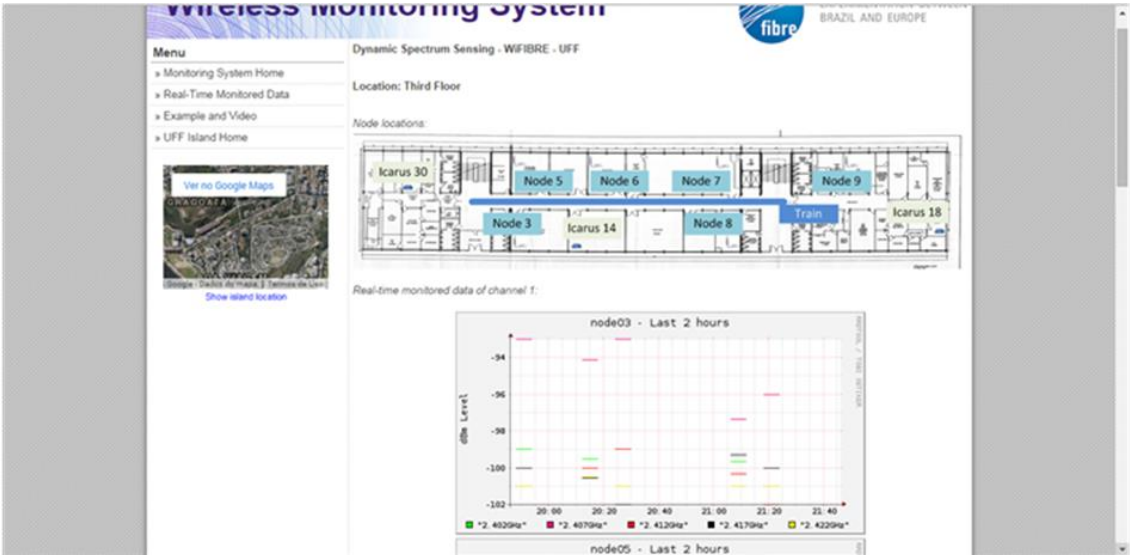


Figure 10 - Wireless monitoring system home, which provides access to real-time monitored data and also to a video explaining how the system works.

Figure 11 - Access to monitored data in the 11 channels of IEEE 802.11 g.

As shown in Figure 12



, for each channel, the system shows node positions and the maximum dBm Level measured during the last two hours for the five main frequencies of the selected channel. Based on this information, the experimenter is able to observe interferences that increase the frequencies power level.

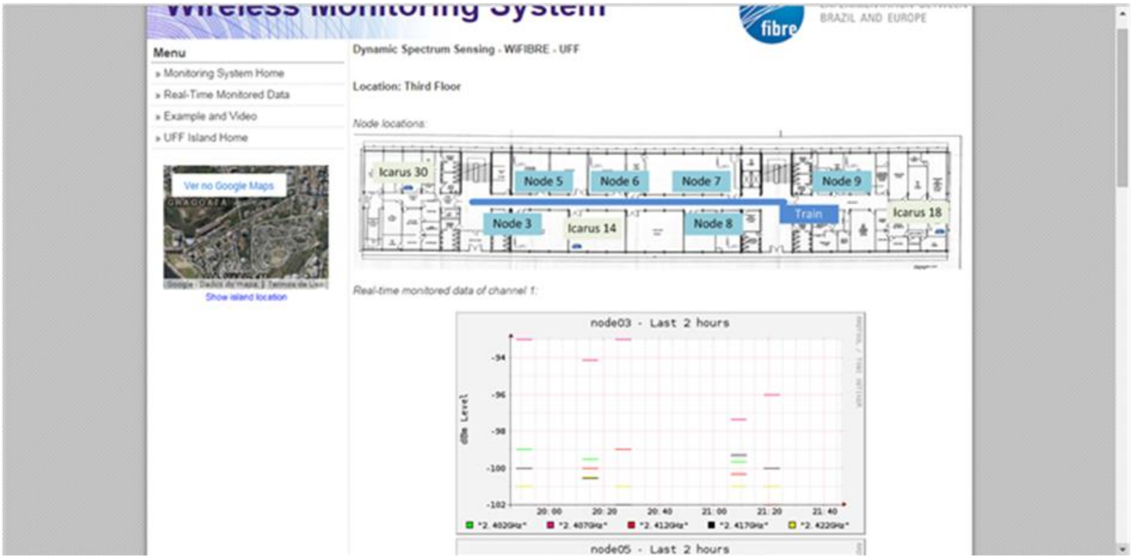


Figure 12 - Channel 1 result for each monitoring node

Vertical and Horizontal Handoff Demonstration

The developed infrastructure may be used to perform different experiments on a variety of wireless network scenarios, such as infrastructure networks, ad hoc networks, sensor networks, delay and disruption tolerant networks, etc. The entire developed infrastructure is also connected through cable in a star topology, which allows the use of Icarus and Mini-itx nodes to perform experiments in wired network. To access and configure the nodes, the users can use the control network, which is a wired network with star topology connecting all experimenting and monitoring nodes to OMF server. The only exception is the mobile node, whose control access is performed through wlan0 interface in a pre-configured wireless network.

Each possible network scenario configured in FIBRE has its own peculiarities and demands the correct configuration of the nodes. In order to create the scenario, the user must know the main characteristics of the technology as well as the main issues of the software implementation.

In the Pilot 1 demonstration, we show how to perform handoff experiments using the FIBRE infrastructure wireless network.

Handoff

In the last years, the use of handoffs as way to allow seamless mobility becomes very important. Indeed, the advent of lightweight mobile phones equipped with Wi-Fi made user mobility very usual and focus of recent researches [1, 2]. New technology proposals about 5G are also correlated to handoffs [3]. Hence, a testbed that provides adequate equipment for experiments with handoffs are of main importance.

Horizontal Handoff

A horizontal handoff is defined as the process in which a mobile station (STA) transfers its physical layer connectivity from one access point (AP) to another, as described in Figure 13. A seamless mobility requires that handoff are transparently performed, without disrupting the user connectivity.

Besides changing physical connectivity, a handoff also transfer state information regarding the association or attachment of an STA to an AP.

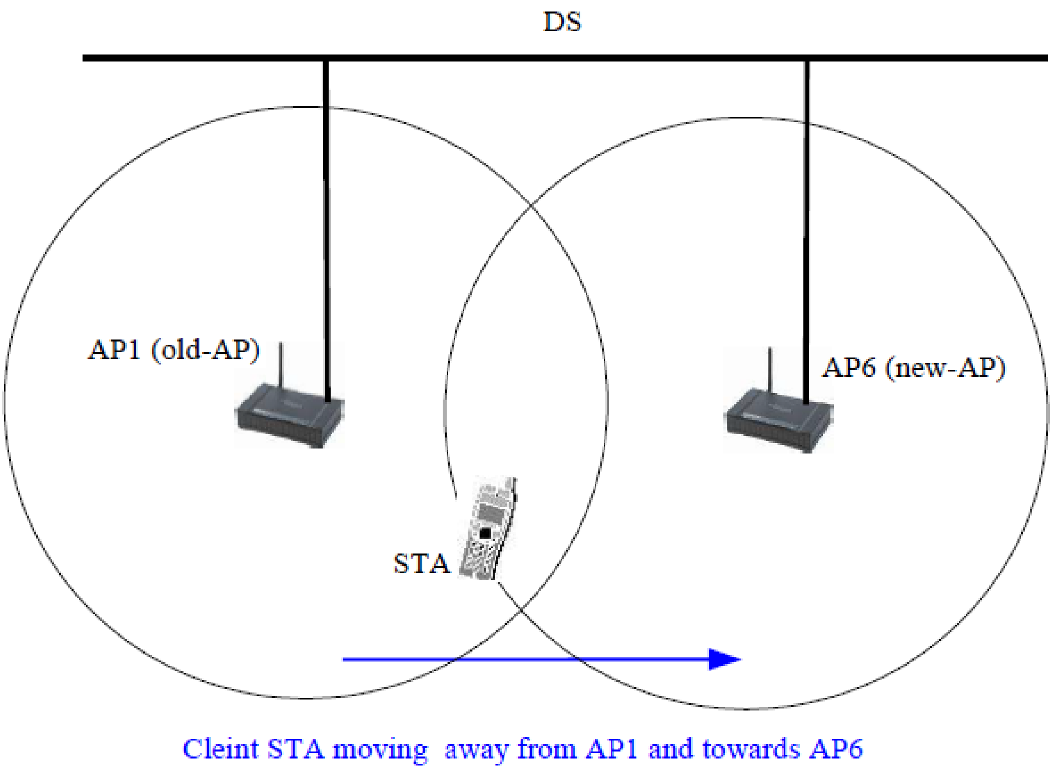


Figure 13 - Example of horizontal handoff [4].

The handoff process is divided into three phases: detection, search, and execution [5]. In the detection phase, the STA checks the quality of the link between the STA and the AP. Once the quality degrades to a certain threshold, the STA will start the search phase. The quality degree is measured in different ways, according to the device manufacture. Indeed, each STA manufacture will probably present a different detection algorithm, which results in different behaviours to perform a handoff. The algorithm to define link quality has a main role in the quality of experience of the user.

The search phase is responsible for selecting a new AP. In this phase, the STA scans for new available APs, as shown in Figure 14. After the selection of a new AP, the STA starts the execution phase. In this phase, the BSSID (MAC address) of the selected AP is used to try to connect the STA to the AP. Then, the STA sends an authentication message to the AP and waits until it receives a success message in the authentication response. After, the STA sends a re-association message and waits to the AP positively answer the association request. After these steps, the STA finishes the handoff procedure.

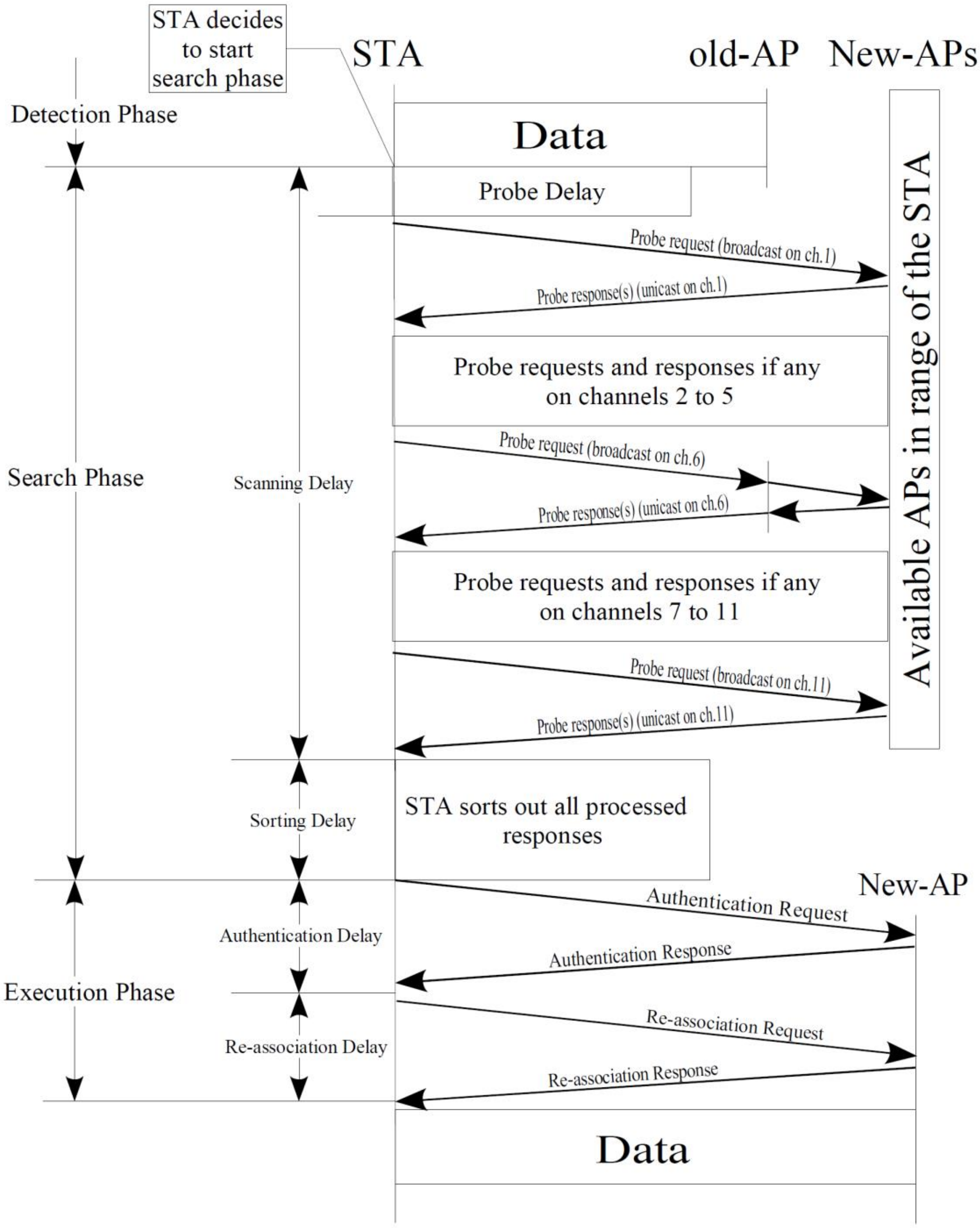


Figure 14 - Search and execution phases in a handoff. [4]

One important issue concerning handoffs is the STA IP address. If the IP address of the STA is changed during the handoff, all the active connections will be dropped. Hence, a mobility management system must be employed to avoid connection losses.

Vertical Handoff

The vertical handoff is similar to the horizontal handoff, but it assumes that instead changing from access points that use the same data link technology, the handoff will be executed between devices that use different data link technologies. Vertical handoff is very interesting when changing from wireless LAN to cellular technologies in order to assure the client access to the Internet. Hence, vertical handoff is defined by the automatic exchange from one wireless technology to another in order to maintain the communication. So, vertical handoff relates to changing the data link technology used to access the network.

Even though vertical handoffs are more discussed between Wi-Fi and cell networks, the exchange between a Wi-Fi and a Bluetooth interface or between a Wi-Fi 802.11b/g to a Wi-Fi 802.11 a is also considered a vertical handoff, because the data link frequency and/or modulation are changed.

In vertical handoffs, the mobility management is also required, but it is more complex, because vertical handoffs usually imply the connection exchange between different domains.

Scripts and Results of the Demonstration

Both the horizontal and vertical handoff demonstrations begin with the same steps. First, the experimenter must access the portal and reserve the train and two nodes that are in different sides of the corridor of the train. We performed the experiment using Icarus nodes 30 and 14. After accessing OMF server, the user should access the CMC of both nodes and turn them on. In these tests, both Icarus will work as access points while the train will work as the STA.

Horizontal Handoff

The experimenting nodes are configured as access points using the Linux software called hostapd2. Hostapd runs based on pre-configured parameters chosen by the user. Hence, it is possible to configure different parameters of the MAC layer, such as SSID, mode, channel, etc. The user may also configure the security in the network access using hostapd.

[2] It is important noticing that this software requires radio devices that are able to run in Access Point mode. This information is available using the command iw list.

In order to distribute IPs, we will also need a DHCP server. We use the isc-dhcp-server also available in Linux distribution. The use of static IP or other addressing server is optional. The experimenter must also configure a bridge in order to interconnect the wireless interface with the wired interface, in case he/she wants to create a connection between the STA and an external point.

We developed a python script to configure all these services. This script, shown in Annex 1, is based on templates for both hostapd and DHCP configuration files. The template files are on Annex 2 and Annex 3. The script assumes some default values, but accepts that the user changes the inputs according to the scenario.

In the horizontal handoff scenario, we use the standard values for the first AP and change the IP input parameter to 192.168.134.110 for the second AP. A script in the OMF server executes an SSH to each AP and automatically runs the script of Annex 1.

The main script that runs inside OMF server performs the following actions:

- Access all reserved resources and run the script of Annex 1 changing the IP of the bridge for each access point.

- Configure the train as a client of the network. To do so:

```
service network-manager stop #turn off the use of network
manager

ifconfig wlan0 up #guarantee that the interface is up

iw dev wlan0 scan | grep SSID # Check whether the Access points
are working properly. In case everything is ok, the SSID teste
must be on the list

iw dev wlan0 connect -w teste #Connect to the network

dhclient wlan0 #Obtain an IP. This step can be performed just
once.
```

- Schedule train movements forward and backward to create the handoffs. The number of movements determines the number of repetitions of the experiment. The train movement is controlled through web service using the following commands:

- To move forward: wget 10.134.11.23/cgi-bin/fwd.cgi
- To move backward: wget 10.134.11.23/cgi-bin/bwd.cgi
- To stop the train at any moment: wget 10.134.11.23/cgi-bin/halt.cgi
- To perform a round trip: wget 10.134.11.23/cgi-bin/rtrip.cgi

- After the end of the train movements, we gather the hostapd logs in each access point, changing the name from temp to temp-AP_IP.

It is important noticing that the use of Wireshark is not recommended to collect this kind of data. Indeed, we need a special hardware such as Airpcap to collect IEEE802.11 control messages using Wireshark. Hence, to observe the handoff, we must use the system log in the APs.

This solution brings another issue correlated to synchronization. The results are obtained in different machines of the testbed and we must correlate the time in the machines. We suggest the use of NTP or the use of a central logging system. In this case, the experimenter must also install the logging server and configure the APs to send the logs to the central server. Our experiments were performed assuming only the use of NTP.

Another way to perform handoff experiments is looking at a specific data flow instead of looking at the control messages, which are difficult to collect. In this case, the use of tcpdump is recommended to observe the number of packet losses during the handoff.

Horizontal Handoff Results

We performed the tests using two different levels of logging in hostapd. To observe the STA associating and re-association, we just need the lower logging level of hostapd. For instance, the log of hostapd after an STA associate to it is:

```
1410055628.739294: Configuration file: temp.conf
1410055628.740938: wlan0: interface state UNINITIALIZED-
>COUNTRY_UPDATE
1410055628.757525: Using interface wlan0 with hwaddr
6c:71:d9:1f:62:85 and ssid "teste"
1410055628.768800: wlan0: interface state COUNTRY_UPDATE-
>ENABLED
1410055628.768809: wlan0: AP-ENABLED
1410055644.059712: 1410055644.059718: wlan0: STA
88:32:9b:85:97:7d IEEE 802.11: authenticated
1410055644.062436: 1410055644.062442: wlan0: STA
88:32:9b:85:97:7d IEEE 802.11: associated (aid 1)
1410055644.062508: wlan0: AP-STA-CONNECTED 88:32:9b:85:97:7d
1410055644.063527: 1410055644.063531: wlan0: STA
88:32:9b:85:97:7d RADIUS: starting accounting session 540BBDCC-
00000000
```

Based on this log, we can observe the reception of Authentication and Association message in hostapd, as well as the moment when the STA is connected to the AP.

In this scenario, we performed a number of experiments and we observed a high variability in the handoff times. The handoff delay was measured as the time since one AP considers that the node has disconnected until the time the other AP considers the node connected. The handoff time varied between 0.34 s and 3.00 s as shown in Table 1. We believe that different results are due to the decision phase of the STA.

Table 1 Results of the delay test in the horizontal handoff experiments.

Test number	Handoff delay (s)
1	0.34
2	3.00
3	0.35
4	2.46
5	2.73
6	0.37
7	2.25
8	0.38
Mean value	1.48

Handoff vertical

The vertical handoff test was performed in a similar way to the horizontal handoff test. We measured the delay to perform a handoff between an IEEE 802.11a AP and an IEEE802.11g AP. Hence, we used the script of Annex 1 changing not only the IP, but also the mode and channel for the IEEE802.11a AP. We used mode=a and channel=36.

For checking the configuration, the user may use iwconfig and iw list. For instance, iwconfig shows if the node is properly configured in Master mode, as shown:

```
IEEE 802.11abgn  Mode:Master  Tx-Power=17 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
```

The results are similar to the results obtained using horizontal handoffs.

Handoff using OpenFlow

The handoff tests can also be performed using OpenFlow. The requirement is to install OpenVSwitch in the mobile node, as well as a controller able to deal with wireless networks. For instance, one could add the 802.11 interfaces as well as the Bluetooth interface in the same OpenFlow switch and control the use of the interfaces by collecting data using the controller.

It is important noticing that the standard OpenFlow statistics and flow control are not enough to take decisions in wireless networks. Additional information about the interface state must be collected in order to take the best decisions about when performing a handoff.

An example of project that developed a Floodlight controller for performing vertical handoff is in [6]. The code is available in https://github.com/rizard/openflow-vertical-handoff. This controller, however, must be adapted to treat Bluetooth.

6.1.1.2 UC1 demonstration info

Prototype demonstration of Use Case 1 has taken place in following events

- 2nd FIBRE open workshop, Barcelona on 5 November 2013;
- Brazil WPEIF/SBRC conference 2014.

6.1.2 UC2 : High Definition content delivery

This use-case takes advantage of the functionalities provided by the OpenFlow infrastructure to create a Content Delivery Network (CDN) controlled by an OpenFlow-based application (i.e. a POX application). The integration of OpenFlow enables the CDN controller to properly distribute the traffic and load balance requests from clients/users of a high-definition video streaming service between delivery sites, by means of re-routing clients to another server located in another site (in UC2 theses sites are located at UK and Brazil). The re-routing is performed by changes in the flow tables of the OF switches under its control

6.1.2.1 Use Case 2 workflow

This section provides a high-level overview of the steps that the experimenter can follow to reproduce the UC2 in the FIBRE infrastructure.

The first step is the creation of a slice using the FIBRE control and management framework. Once the slice has been allocated, the experimenter can allocate the resources for it (virtual machines for the controllers and the hosts, OF switches, select video server and ports, flow-space). For UC2 the experimenter needs to allocate specific OF ports on each site that are mapped to the international Layer 2 circuit linking the two sites.

Firstly, the experimenter should create a slice using the proper CMF portal:

- retrieve the user credentials using the registration form;
- create a project giving a name and a short description;
- create a slice giving a name and a short description;
- add the Aggregate Managers for the computing (VT) and network (OptIn) resources.
- Select option for 4K video server, the admin verifies the request for video server and approves the request

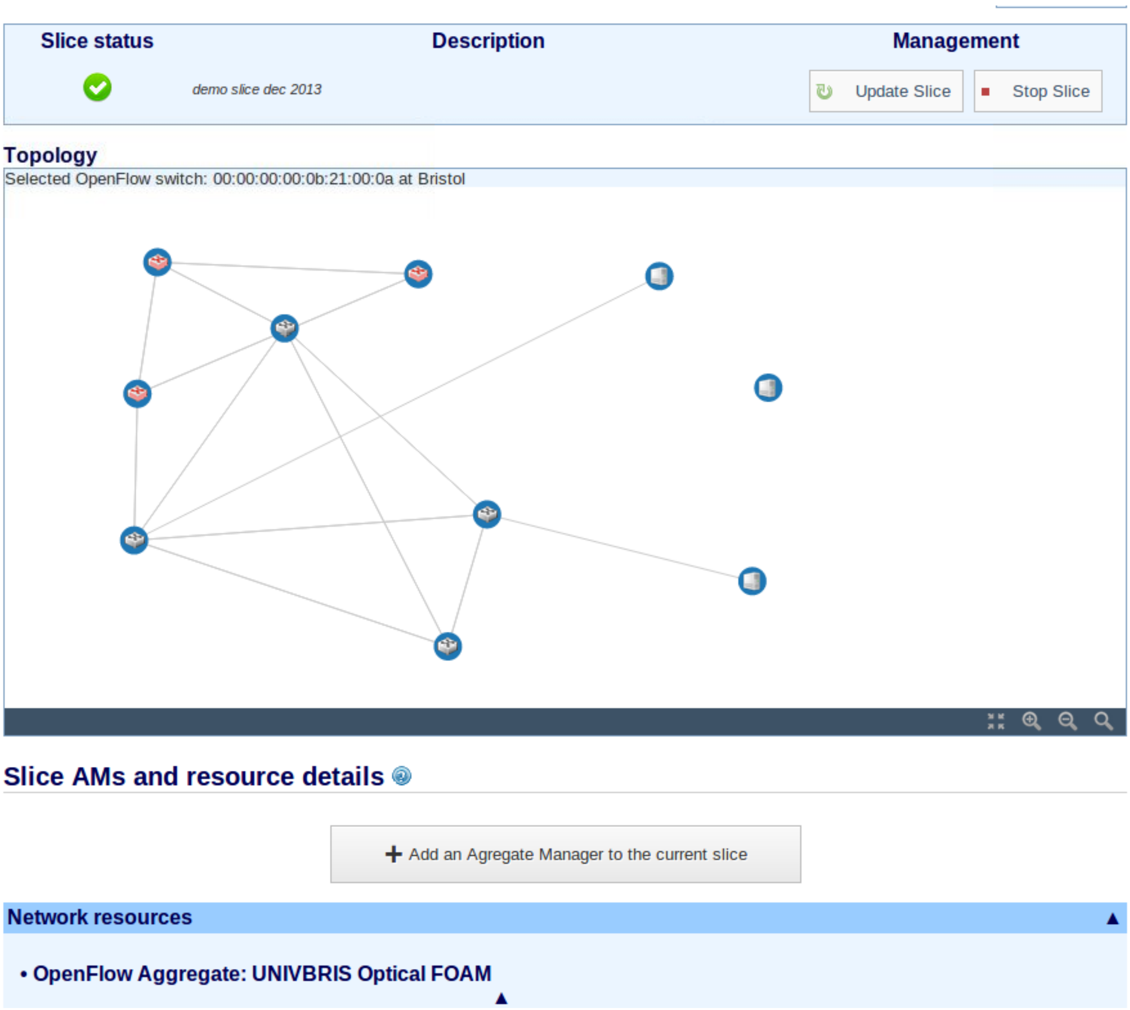


Figure 15 - Resource selection

Then, the experimenter can configure the test environment [refer WP4 documents or the website for guides]:

- create and grant the flow-space (using proper VLAN-ID);
- configure the VMs to send VLAN tagged traffic (using proper VLAN-ID).

After the resources are allocated and machines are deployed, the experimenter can setup the software infrastructure, composed of the CDN controller (OpenFlow-based application) and the video servers (based on the FOGO player).

The users can see the resource on the OpenFlow controller.

http://10.2.9.22:8080/admin/poxcw/poxcw_sw/

Figure 16 - Controller showing discovered switches and switching type

Then the user deploys the media controller application. The application performs identification & modification of flows to prevent congestion caused by high density media flows.

Identification:

- Dynamically detect long lived media flows by maintaining per-flow traffic statistics in the network and declaring a flow to be a congestion flow when its byte count exceeds some threshold.
- traffic sampling (passive-less reliable & active monitoring)
- Collect monitoring data directly from hosts: CPU & Memory

Modification:

- Use OpenFlow to modify flows upon media congestion flow detection
    - end host detection with signalling of congestion flows to the OpenFlow controller
    - Load-balance the congested flows
        - Use Queues on the packet switches
        - Or create Optical Paths

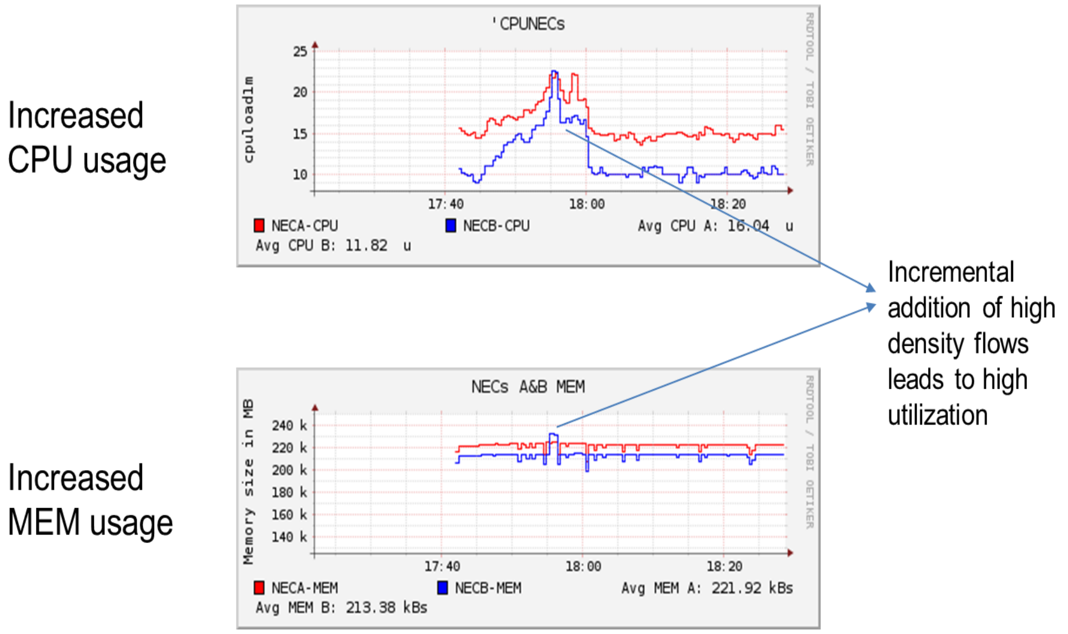


Figure 17 - CPU & Memory threshold increase identification

6.1.2.2 Use Case 2 Demonstration

Use case 2 has been demonstrated in the following events

- FIA Dublin 2013
- 2nd FIBRE open workshop, Barcelona on 5 November 2013;
- USP presented a lecture at the 4th professionals in the state of São Paulo, regarding Future Internet initiatives, presenting the WP5 Use Case 2;
- Demonstration of the application with Optical vendor Polatis in OFC 2014
  - https://www.youtube.com/v/hhHMJ1i6XiQ

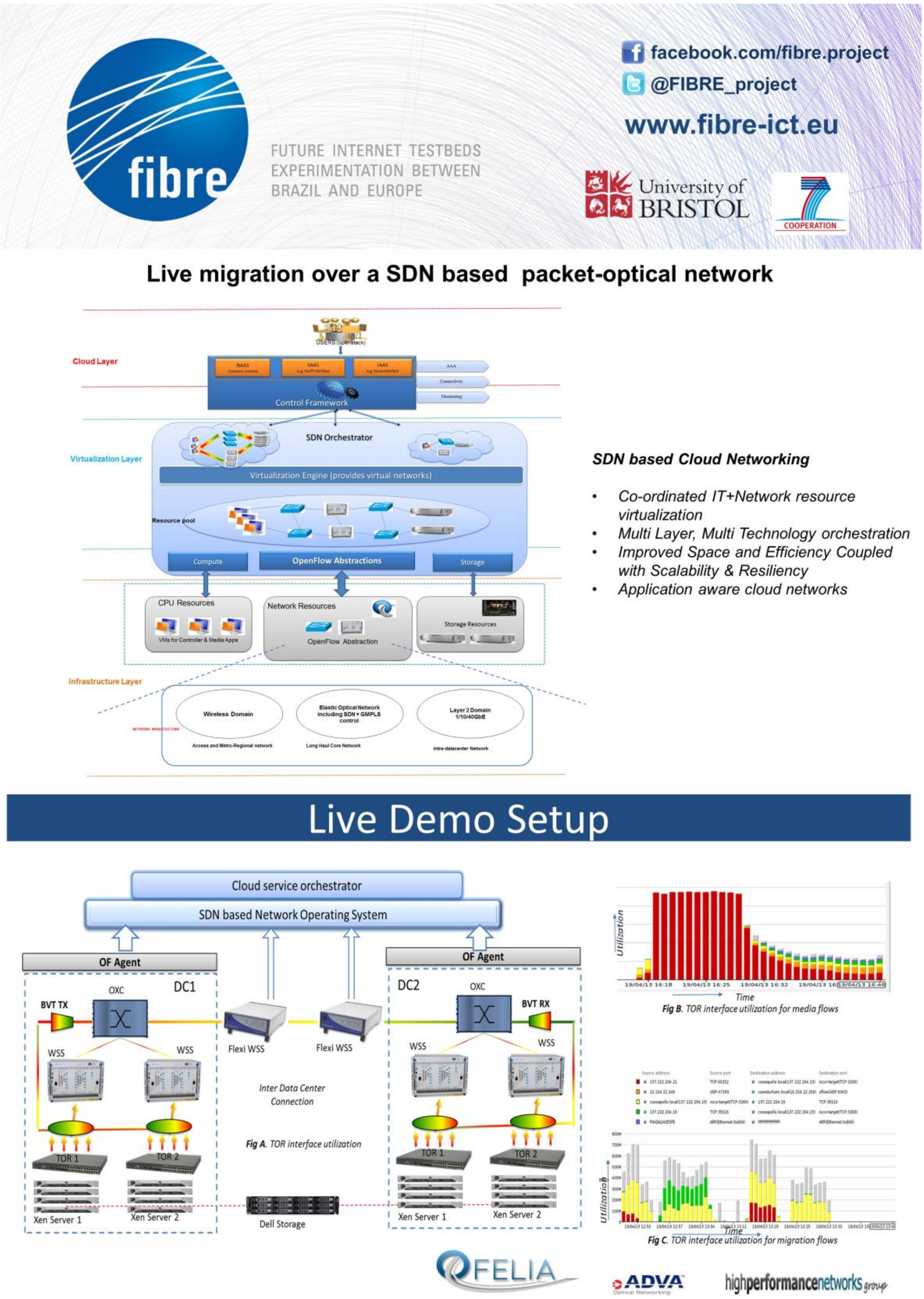


Figure 18 - Use Case 2 partial monitoring demonstration at FIA Dublin 2013

NOTE: Although UC2 servers were deployed in Brazil and UK, it was not possible to test the whole UC spanning the two sites due to problems in establishing the International layer-2 circuit upon which the UC depends.

The problem for establishing the Layer-2 circuit lies on three different issues. The first one is complexity of the circuit setup, as it demands the use of layer-2 circuits on top of another layer-2 circuit (Q-in-Q technology). The second issue is the multi-domain nature of the circuit: it goes from UK to Brazil through the US, spanning different research and educational networks, with different support and visibility for troubleshooting, demanding a significant effort in its setup. Finally, the University of Sao Paulo is undergoing a large strike since may/2014, which has been preventing the researchers to physically access some of the resources in Sao Paulo (specifically the university Data Center, where the international circuit is located), impacting the activities on UC2.

6.1.3 UC3: Bandwidth on Demand

The UC3 exploits the flexibility of the OpenFlow (OF) protocol and the potentiality of the FlowVisor (FV), NOX controller (e-NOX), F-PCE and OSCARS systems in order to provide an open and generalized Bandwidth on Demand (BoD) service upon the network resources grouped into a “slice” of the FIBRE facility.

In short, the OpenFlow protocol allows experimenters to access the OF-enabled devices from the control framework using a standard interface. The UC3 supports the OF version 1.0 [14] with the circuit extensions introduced for the optical switches [15]. Moreover, the FlowVisor enables the creation of a virtual topology composed of multiple slices of the network resources, delegating the control of each slice to a different controller. The UC3 introduces the e-NOX controller (an enhanced version of the NOX) to provide a framework to integrate heterogeneous modules in the standard distribution, i.e. “topology manager” (to discover the network graph), “provisioning manager” (to install the flow-entries for the traffic routing), “statistic manager” (to retrieve the metering information from the devices), etc.

Briefly, other two applications are integrated in this use-case. The F-PCE is in charge of the computation of the path between the source and destination endpoints. The component can also format the commands, i.e. flow entries, to be sent to the managed switches. At the end, the OSCARS web-service allows users to schedule an advance reservation of the resources checking bandwidth and time constraints.

Please refer to [24] for further details.

6.1.3.1 UC3 workflow

This section provides a high-level overview of the steps that the experimenter can follow to reproduce the UC3 in the FIBRE infrastructure.

Firstly, the experimenter should create a slice using the proper CMF portal:

- retrieve the user credentials using the registration form;
- create a project giving a name and a short description;
- create a slice giving a name and a short description;
- add the Aggregate Managers for the computing (VT) and network (Optin) resources.

Then, the experimenter can configure the test environment [refer WP4 documents or the website for guides]:

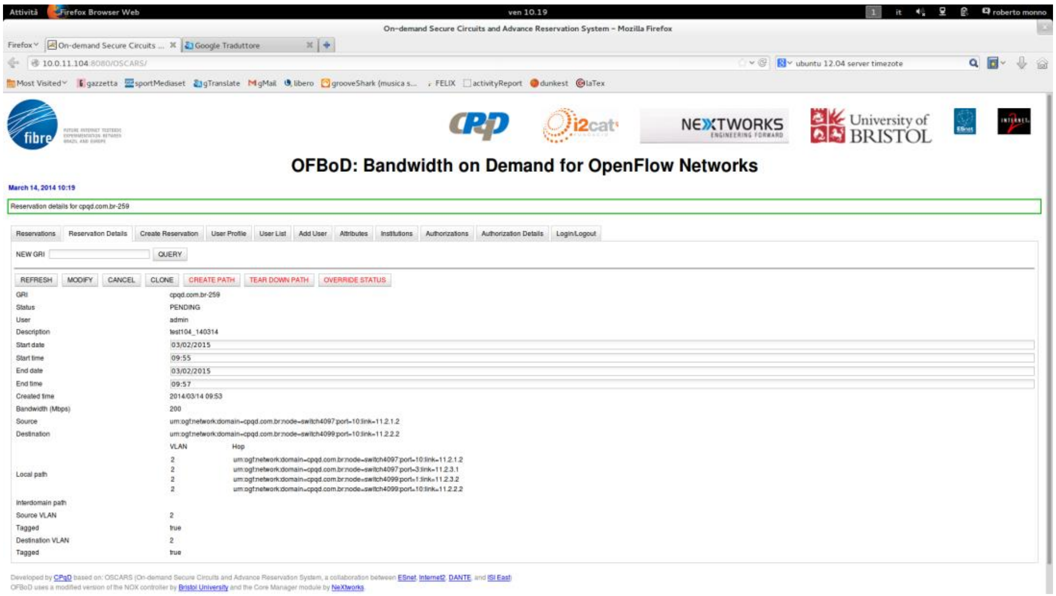
- create virtual-machines for the controllers and the hosts;
- choose OF switches and ports;
- create and grant the flow-space (using proper VLAN-ID);
- configure the VMs to send VLAN tagged traffic (using proper VLAN-ID).

At this point, the experimenter can setup the UC3 control framework:

- deploy e-NOX and OSCARS software, refer to [24];
- start the applications, i.e. F-PCE, e-NOX and OSCARS ,refer to [24].

At the end, the experimenter can manage the network resources creating a virtual circuit using the OSCARS interface:

- retrieve topology information;
- access to the OSCARS web page (admin/admin);



- request an advance reservation specifying proper parameters, e.g. source/destination endpoints, bandwidth, vlan-id, start/end time;
- verify the circuit installation.

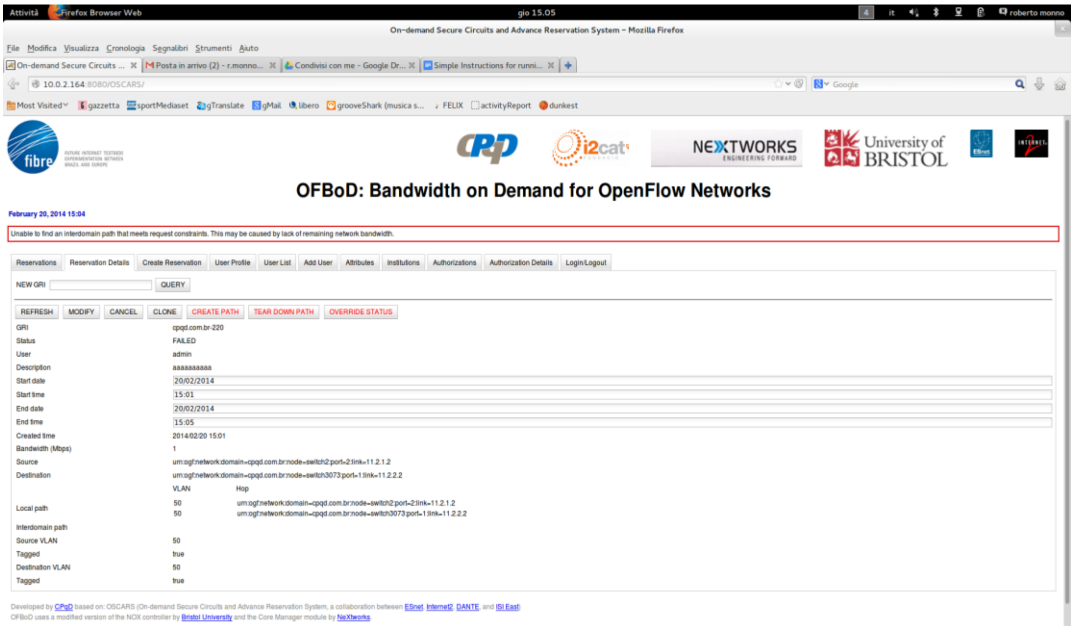


Figure 19 - negative case where request fails

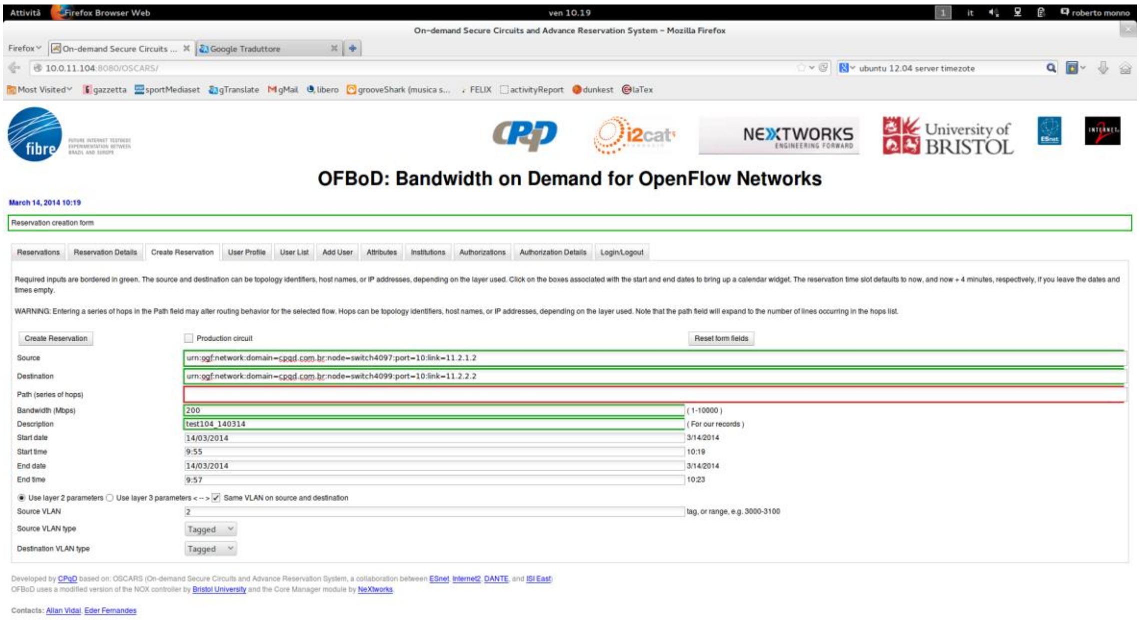


Figure 20 - Successful request

6.1.3.2 UC3 demonstration info

The UC3 has been presented into two public events organized during the 2th and 3th years of the FIBRE project to demonstrate the federated infrastructure:

- 2nd FIBRE open workshop, Barcelona on 5 November 2013;
- Globecom conference 2013;
- Future Internet Assembly (FIA), Athens on 18-20 March 2014;
- Presented FIBRE Use Case 3 pilot at Reunião Semestral da ANSP (RSA 4), on 31/Oct/2013, at USP, São Paulo, Brazil. URL:http://rsa.ansp.br/index.php?option=com_content&view=article&id=100&Itemid=749&lang=us
- Presented "(G)MPLS and OpenFlow: Interworking, Integrating, or Replacing?" workshop at the Pre-FIA Workshops (Dublin, 2013 May 7th).

The Figure 21 and **¡Error! No se encuentra el origen de la referencia.** show the posters used to explain the UC3 architecture, setup and expected results.

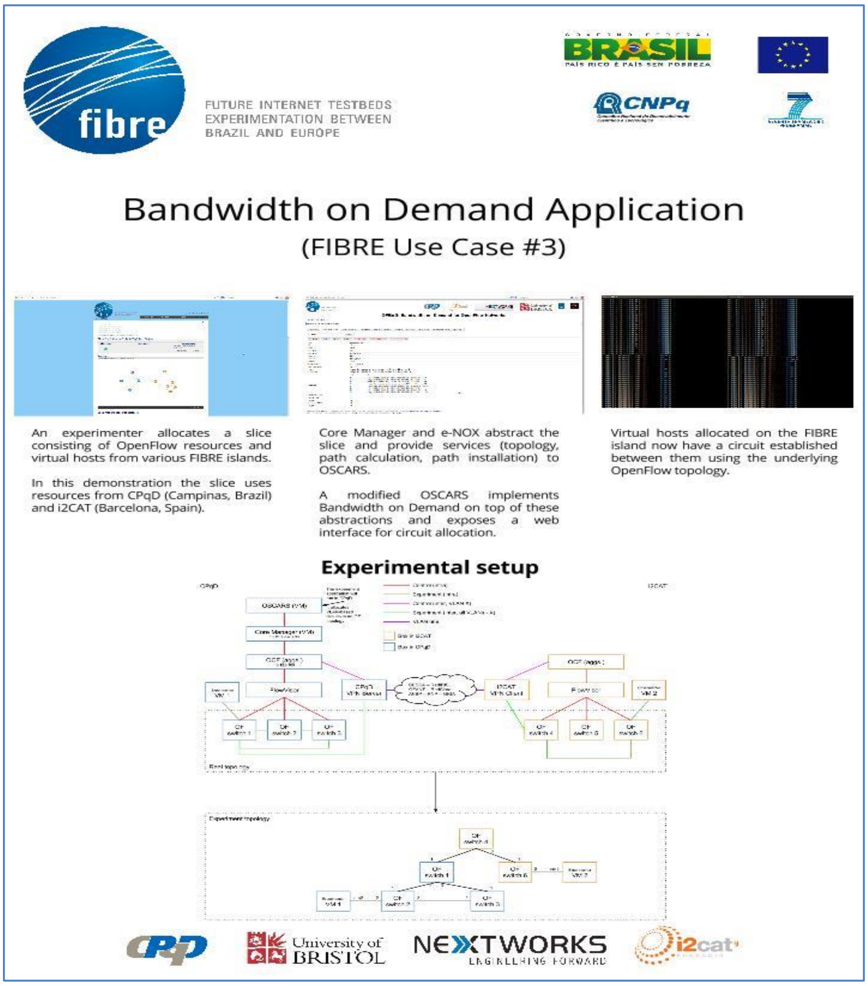


Figure 21 - UC3 poster for the 2th open workshop - Barcelona, 5 November 2013

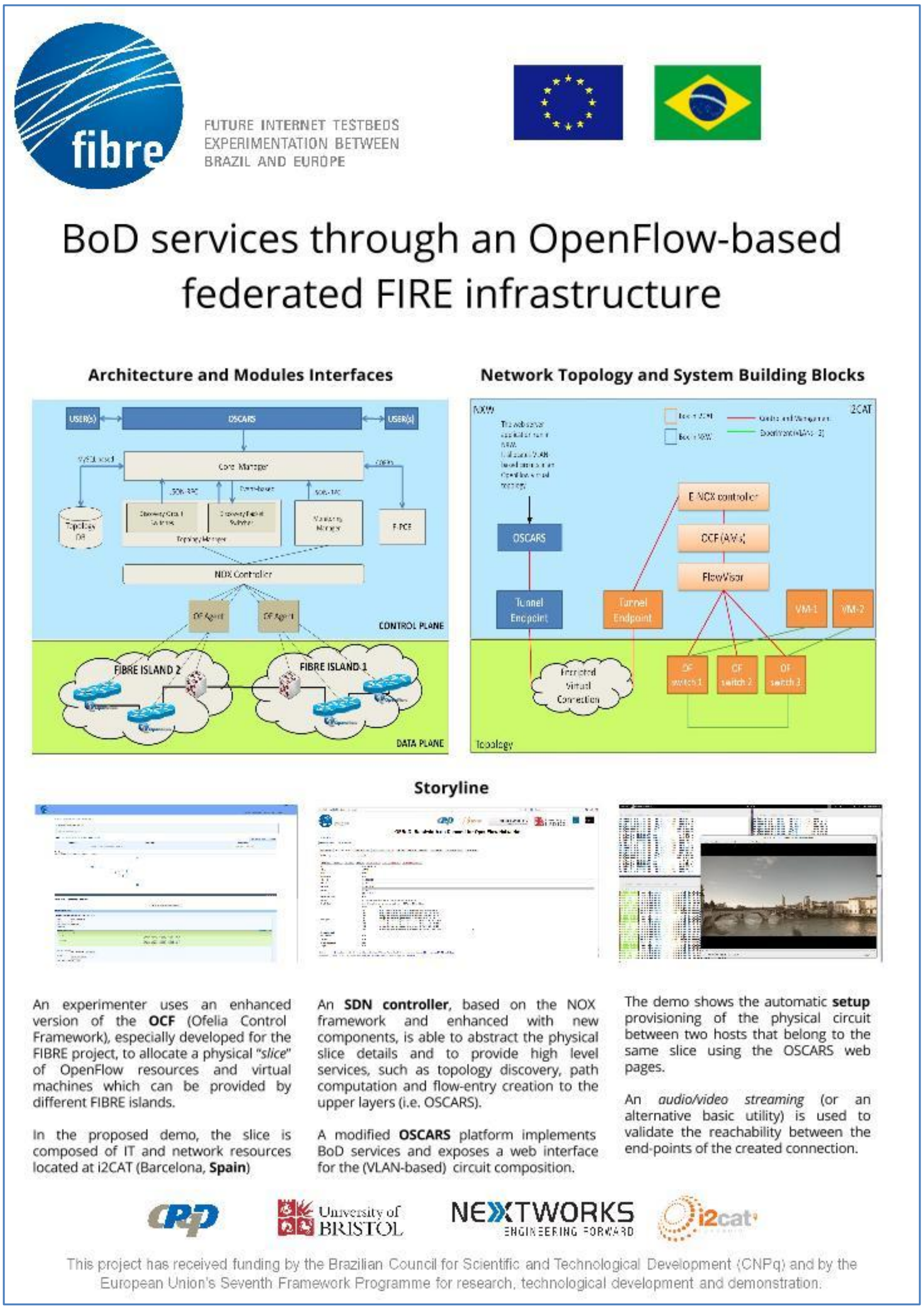


Figure 22 - UC3 poster for the FIA meeting

7 Validation methodology by requirements

7.1.1 Background on Requirements

There are two types of requirements identified in D5.1:

• Functional requirements: are requirements relevant to technological capability and functionality of the technology pilots in FIBRE test-bed.

• Non-functional requirements: are a set of constraints (also known as quality requirements) that define performance expectation and quality of service (QoS) of the technology pilots in FIBRE test-bed.

These are further grouped into following categories:

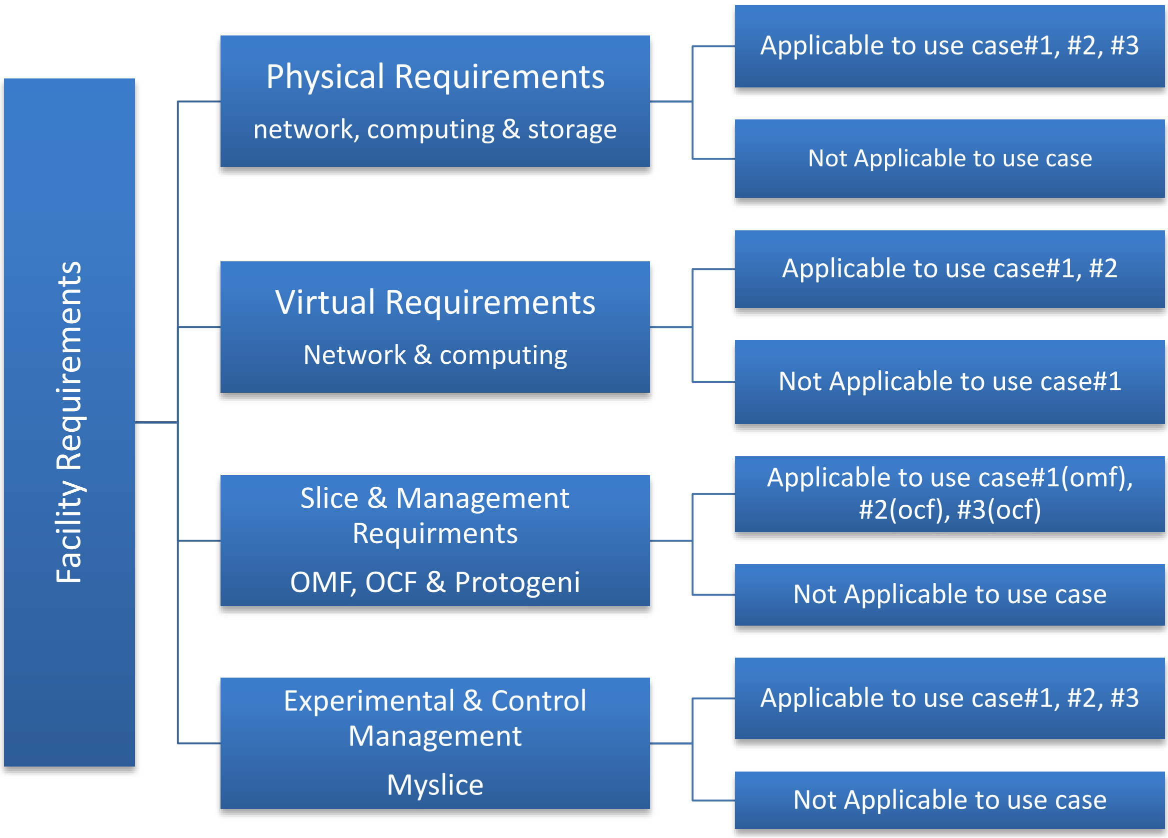
- Heterogeneous physical resources requirements
- virtualization requirements
- Slice and Management requirements
- Experiment control and management

7.1.2 Evaluation criteria

The validation tasks followed the following criterions

- Evaluate which requirements were important to our use case scenes, and which ones were implemented
- Evaluate which pilot requirement validate the facility
- Extent to which the requirement was implemented
- Map requirement to category and use case building blocks
- Document the results of the validation

The validation tasks of WP5 individual categories matched the use cases against the requirement category and verified whether they fulfilled stated requirements. The first task was to match the use case to their respective category which is depicted in the following figure



The following WP5 facility Validation Table evaluate which pilot requirement validate the facility requirement

Table 2 Facility Validation Table

Facility Functionality	Use case	Achieved Validation Results
Interaction between Aggregates	UC#1/2/3	Communication between control frameworks via Myslice
Resource Reservation	UC#1/2/3	Scheduling through Myslice or through the island portals.
Resource Listing	UC#1/2/3	Listing of all the available resources in Brazil and Europe through Myslice or through the island portals.
Resource Availability	UC#1/2	Perfsonar and ZenOSS portals
Monitoring	UC#1	Wireless monitoring system (available in UFF)

resources	island portal)

7.1.3 UC1 Validation Results

The following table summarizes the mapping between the requirements introduced into [21], the referring building blocks, and the achieved validation results.

Table 3 UC1 validation results

Requirements	Description	Building Block	Achieved Validation Results
PR04, PR05, PR06, PR17, PR18, PR19, PR20, PR21, PR22, PR25	Physical infrastructure	Hardware development	Physical infrastructure installed
PR23, PR24	Pilot codes	Horizontal and vertical handoffs	Demonstration
VR02, VR03, AR02, AR04, AR05, AR06, AR08	Island L1/L2 infrastructure	Island development	Interconnection of equipments
ER01, ER03, **ER04**, ER05, ER08, ER09, ER11, ER12	Integration with OMF/OML	Software building blocks	Scripts for the demonstration

7.1.4 UC2 Validation Results

The following table summarizes the mapping between the requirements introduced into [21], the referring building blocks and the achieved validation results.

Table 4 UC2 validation results

Requirements	Description	Building Block	Achieved Validation Results
PR01	OpenFlow L2 infrastructure	CMF	Introduce OF switches into the slice
PR03	Content Delivery Servers	Server	Server connected to OF Switch
PR07	High Definition Media Streaming Server/client	Server	Server connected to OF Switch
PR09	High Bandwidth Application	VM/Server	Application deployed on Island VMs or Servers
PR10	OpenFlow controller	CMF/CDN	Configure the flow-space redirecting the traffic to the OF controller
PR11	Monitoring Manager	CDN / Media Broker	CDN and Media Broker integration for statistics monitoring
PR13	Topology Manager	CDN	Discover the packet/circuit OF switches
PR14	Provisioning Manager	CDN	Install the flow-entries into the OF switches
PR15	Load Balancing Application	CDN	Rewrite flow entries for application
PR16	Replanning Manager	CDN	Rewrite flow entries for application

VR01	L2 network slice	CMF	Create a slice using network resources
VR03	Virtualization mechanism for traffic isolation	CMF	Traffic isolation using a VLAN identifier
AR01	L2 slice creation, allocation, monitoring and release	CMF	Manage a slice with computing and network resources
AR03	Application server and traffic source/sink monitoring, allocation and release	CMF / Perfsonar / Zenoss	Island CMF and management portals
AR04	Island overall L2 resources/network monitoring	CMF / Perfsonar / Zenoss	Island CMF and management portals
AR06	Island overall server resources monitoring	CMF / Perfsonar / Zenoss	Island CMF and management portals
AR07	Monitoring of WAN links	CMF / Perfsonar / Zabbix	Island CMF and management portals
AR08	Authentication, Authorization and Accounting	CMF	Access to the web portals using provided credentials
ER02	Experiment user-to-server monitoring	CDN / Media broker	CDN and Media Broker integration for statistics monitoring
ER03	Experiment network node monitoring	CDN	Retrieve metering information from the OF devices and servers
ER06	Connectivity between federated Islands	CMF	Create on-demand advance reservation into a federated environment

7.1.5 UC3 Validation Results

The following table summarizes the mapping between the requirements introduced into [21], the referring building blocks and the achieved validation results.

Table 5 UC3 validation results

Requirements	Description	Building Block	Achieved Validation Results
PR01	OpenFlow L2 infrastructure	CMF	Introduce OF switches into the slice
PR10	OpenFlow controller	CMF/e-NOX	Configure the flow-space redirecting the traffic to the OF controller
PR12	Flow-aware Path Computation Element network application	F-PCE	Running the algorithm on the discovered topology graph and compute the flow-entries
PR13	Topology Manager	e-NOX	Discover the packet/circuit OF switches
PR14	Provisioning Manager	e-NOX	Install the flow-entries into the OF switches
VR01	L2 network slice	CMF	Create a slice using network resources
VR03	Virtualization mechanism for traffic isolation	e-NOX/OSCARS	Traffic isolation using a VLAN identifier
AR01	L2 slice creation, allocation, monitoring and release	CMF	Manage a slice with computing and network resources
AR08	Authentication, Authorization and Accounting	CMF/OSCARS	Access to the web portals using provided credentials

ER03	Experiment network node monitoring	e-NOX	Retrieve metering information from the OF devices
ER06	Connectivity between federated Islands	CMF/e-NOX/OSCARS	Create on-demand advance reservation into a federated environment

8 Testbed evaluation results

This section documents the results of the validation tasks

Test-ID: #FV-UC#1-0001 **Execution Status: Executed**	
Test Name	Seamless Handoff
Objectives	Show how to perform horizontal and vertical handoffs using the FIBRE testbed.
Requirements	PR04, PR05, PR06, PR17, PR18, PR19, PR20, PR21, PR22, PR23, PR24, PR25, VR02, VR03, AR02, AR04, AR05, AR06, AR08, ER01, ER03, ER04, ER05, ER08, ER09, ER11, ER12
Related Pilot Use Case	UC#1
Designers	UFF
Test Description	**1. Reserve resources** **2. Configure access points** **3. Start measurements gathering** **4. Connect the model train to closest access point** **5. Move the model train** **6. Finalize measurements gathering**
Expected Results	**Observe the maintenance of the connectivity in case a new access point is found.**
Attachments	Annex 1, Annex 2, and Annex 3
Additional Comments	-

Test-ID: #FV-UC#2-0001 **Execution Status: Executed**	
Test Name	Media slice creation
Objectives	Validate whether the FIBRE facility is ready to provide a slice which includes the media

	delivery servers
Requirements	VR01,VR02,VR03
Related Pilot Use Case	UC#2
Designers	UNIVBRIS, USP
Test Description	**Steps:** • **L**ogin into FIBRE control framework • Choose aggregates for the slice under your project • Create new slice • Add network resource and virtual machines to the slice • Add media server from the virtualization aggregate to the slice • Start the slice
Expected Results	Slice started with media resource
Attachments	Use case 2 leaflet in Annex 4
Additional Comments	

Test-ID: #FV-UC#2-0002 **Execution Status: Executed**	
Test Name	Setup the UC2 Control Framework
Objectives	Validate whether the FIBRE facility is ready to install, configure and run the UC2 control framework into a federated infrastructure
Requirements	PR10, PR11, PR12, PR13, PR14, ER03
Related Pilot Use Case	UC#2
Designers	UNIVBRIS, USP

Test Description	**Steps:** • Login into the slice network controller • Install, configure and run the CDN application • Login to video servers • Install, configure the Media application / Media Broker
Expected Results	UC2 software components configured and started
Attachments	
Additional Comments	#FV-UC#2-0001 should be already verified

Test-ID: #FV-UC#3-0001 **Execution Status: Executed**	
Test Name	Federated slice creation
Objectives	Validate whether the FIBRE facility is ready to provide a slice which includes Computing and OpenFlow network resources into a federated infrastructure
Requirements	PR01, VR01, VR03, AR01, AR08, ER06
Related Pilot Use Case	UC#3
Designers	CPqD, UNIVBRIS, NXW
Test Description	**Steps:** • Login into FIBRE control framework • Create a new Project • Create a new Slice • Choose aggregates from different islands • Add Computing and Network resource to the slice • Start the slice
Expected	Slice started with Computing and Network resources

Results	
Attachments	
Additional Comments	

Test-ID: #FV-UC#3-0002 **Execution Status: Executed**	
Test Name	Setup the UC3 Control Framework
Objectives	Validate whether the FIBRE facility is ready to install, configure and run the UC3 control framework into a federated infrastructure
Requirements	PR10, PR11, PR12, PR13, PR14, ER03
Related Pilot Use Case	UC#3
Designers	CPqD, UNIVBRIS, NXW
Test Description	**Steps:** • Login into the slice network controller • Install, configure and run the E-NOX application (refer to [24]) • Add the OSCARS application to the slice
Expected Results	UC3 software components configured and started
Attachments	
Additional Comments	#FV-UC#3-0001 should be already verified

Test-ID: #FV-UC#3-0003 **Execution Status: Executed**	
Test Name	Create a circuit between Computing resources
Objectives	Validate whether the FIBRE facility is ready to install the flow-entries into the network resources allowing the creation of a virtual connection between Computing resources into a federated infrastructure

Requirements	ER06
Related Pilot Use Case	UC#3
Designers	CPqD, UNIVBRIS, NXW
Test Description	**Steps:** • Login into the OSCARS web-service application • Choose the source and destination endpoints for the circuit • Specify the VLAN identifier for the traffic isolation • Specify the required bandwidth • Ask for path creation
Expected Results	The parameters are evaluated by the OSCARS application in order to check bandwidth availability. The request is forwarded to the F-PCE and the E-NOX applications for the path computation and the flows installation. An up and running circuit is created.
Attachments	
Additional Comments	#FV-UC#3-0002 should be already verified

9 Conclusion and outlook

The pilots present an interesting way to understand how diverse the use of FIBRE can be. They also show how to develop experiments, helping new users. The simple existence of videos and demos are an attractive for potential users who come to know the FIBRE experimental facility.

The development of the pilots also helped to understand the main issues for the experimenter in the original plans for the testbed. This allowed the development of improvements to make it easier to use FIBRE.

10 Annex 1

```
#Code to configure experimenting nodes as access points:

import os

import sys

class ap:

	def __init__(self, wlan='wlan0', ip='192.168.134.100', mask='24', mode = 'g', channel='6', cable = 'p3p1', dns='8.8.8.8', mask_ext='255.255.255.0', net='192.168.134.0',dhcp_begin='192.168.134.101',dhcp_end='192.168.134.200',ssid='teste'):

		self.wlan=wlan

		self.ip = ip

		self.mask = mask

		self.mode = mode

		self.channel = channel

		self.cable = cable

		self.mask_ext = mask_ext

		self.dns = dns

		self.net = net

		self.dhcp_begin = dhcp_begin

		self.dhcp_end = dhcp_end

		self.ssid = ssid


	def configure_hostapd(self):

		'''Configure hostapd'''

		f= open('ap-template.conf')

		ap = f.read()

		ap=ap.replace('$WLAN', self.wlan)
```

```
        ap=ap.replace('$CHANNEL',self.channel)
        ap=ap.replace('$MODE', self.mode)
        ap=ap.replace('$SSID', self.ssid)
        f.close()
        f = open('temp.conf','w')
        f.write(ap)
        f.close()

    def create_bridge(self):
        comando = '''service network-manager stop
        ifconfig br0 down
        brctl delbr br0
        brctl addbr br0
        brctl addif br0 ''' + self.cable +'''\n ip addr add '''+ self.ip + '/' + self.mask + '
dev br0'+ ' \n ifconfig br0 up'
        os.system(comando)

    def configure_dhcp(self):
        f=open('dhcp-template.conf')
        conf = f.read()
        conf = conf.replace('$DNS',self.dns)
        conf = conf.replace('$MASK_EXT', self.mask_ext)
        conf = conf.replace('$IP', self.ip)
        conf = conf.replace('$NET', self.net)
        conf = conf.replace('$DHCP_BEGIN', self.dhcp_begin)
        conf = conf.replace('$DHCP_END', self.dhcp_end)
        f = open('/etc/dhcp/dhcpd.conf','w')
```

```
        f.write(conf)

        f.close()


    def configure_forwarding(self):

        comando = '''iptables -t nat -A POSTROUTING -o internet0 -j MASQUERADE

            iptables -A FORWARD -i ''' + self.wlan + ''' -o internet0 -j ACCEPT

            iptables -A FORWARD -m conntrack --ctstate
RELATED,ESTABLISHED -j ACCEPT


            service isc-dhcp-server restart

            sysctl net.ipv4.ip_forward=1

            hostapd -t -d temp.conf > temp-result'''

        os.system (comando)

    def execute(self):

        self.configure_hostapd()

        self.configure_dhcp()

        self.create_bridge()

        self.configure_forwarding()

    def __del__(self):

        os.system('killall -9 hostapd')

        os.system('rm temp.conf')

        os.system('service isc-dhcp-server stop')

        os.system('ifconfig br0 down')

        os.system('brctl delbr br0')


if __name__=="__main__":

    print "Usage: python configura.py"
```

```
    print "Options: wlan=wlan0, ip=192.168.134.100, mask=24, mask_ext=255.255.255.0, net=192.168.134.0,mode=g, channel=6, cable=p3p1, dns=8.8.8.8, dhcp_begin=192.168.134.101, dhcp_end=192.168.134.200, ssid=teste"

    parameters={}

    sys.argv.pop(0)

    for input in sys.argv:

        parameters[input.split('=')[0]]=input.split('=')[1]

    ap_conf = ap(**parameters)

    ap_conf.execute()
```

11 Annex 2

#Template for hostapd configuration file. We did not use any security mechanism.

ssid=$SSID

#wpa_passphrase=Somepassphrase

interface=$WLAN

bridge=br0

auth_algs=3

channel=$CHANNEL

driver=nl80211

hw_mode=$MODE

logger_stdout=-1

logger_stdout_level=2

max_num_sta=5

#rsn_pairwise=CCMP

#wpa=2

#wpa_key_mgmt=WPA-PSK

#wpa_pairwise=TKIP CCMP

country_code=US

12 Annex 3

#DHCP configuration file template

```
option domain-name-servers $DNS;

option subnet-mask $MASK_EXT;

option routers $IP;

subnet $NET netmask $MASK_EXT {

  range $DHCP_BEGIN $DHCP_END;

}
```

13 Annex 4

CNPq Co-funded by the European Union

fibre

FUTURE INTERNET TESTBEDS EXPERIMENTATION BETWEEN BRAZIL AND EUROPE

Pilot Use Case n.2

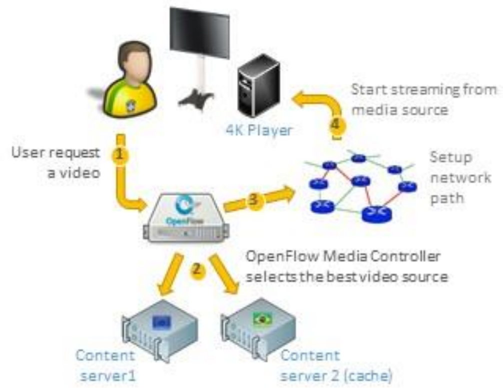
High definition content delivery across different sites

Media aware SDN network

This use case focuses on steering media clients to appropriate content servers based on various network and streaming server load characteristics. The use cases make use of the FIBRE monitoring facility to discover high density traffic flows and re-route such flows through optical networks.

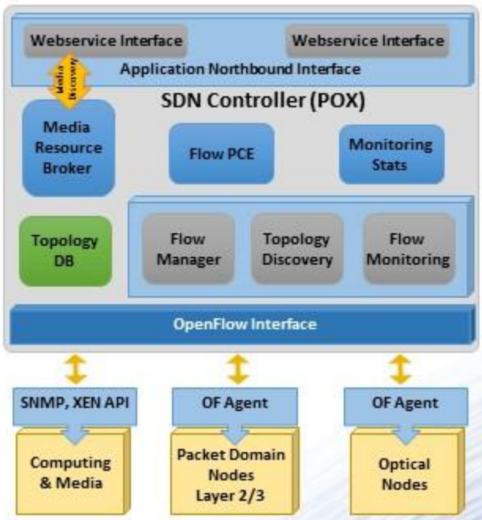
An OpenFlow-based application (i.e. a POX application) is interfaced to one or more **Content Delivery Servers** (CDSs) that form a Content Delivery Network (CDN). The POX application monitors the CDS performance by retrieving the related status, load and failures. When certain thresholds are exceeded (e.g. the load on CDS or its energy consumption), NOX application will re-route one or more clients to another CDS located in another site.

It is important to note that the focus of the use case is not only to serve media requests but also to **adapt request to changing network and media server conditions**. A monitoring module in the POX controller collates all server and network resource information, evaluating if there is any possible problem (e.g. congestion, under/over utilization etc.) and then re-routing users to appropriate media content streamers.



How it Works

1. Request a slice containing optical and media(pre-configured) resources from the FIBRE control framework.
2. Run a SDN controller with the media broker and monitoring application. The monitoring module will utilize both OpenFlow monitoring and FIBRE facility monitoring.
3. Run multiple media clients. The monitoring app detects server or network flow threshold crosses and requests media broker for reroute
4. Client are migrated to new server over rerouted paths



Content Delivery Software architecture

Underlying Components

Topology Discover: It uses the OpenFlow abstractions to read device information and construct the network topology. The discovered topology is stored in the MySql **Topology DB** and it is represented via the **DJANGO** web application.

Monitoring Stats: this function gets monitoring stats from two places one from the flow stats of OpenFlow and from the zenoss/sFlow stats.

Flow Manager and Monitoring: these functions assist in pushing flows and then set the intervals to receive the flow stats (packet and byte counts).

Media Broker: Uses the REST API to receive media server and client requests. It has information on the location of the media servers along with their capabilities. Along with the PCE it finds the best path for rerouting clients.

www.fibre.org.br | info@fibre.org.br

"*This work makes use of results produced by the FIBRE project, co-funded by the Brazilian Council* for Scientific and Technological Development (CNPq) and by the *European Commission within its Seventh Framework Programme.”*

END OF DOCUMENT