FUTURE INTERNET TESTBEDS
EXPERIMENTATION BETWEEN
BRAZIL AND EUROPE

*

Grant Agreement No.: 288356
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***

D3.5 Final report on the

Operation of the facility

Author: WP3
Revised by: Sebastià Sallent (UPC)
Due date of the Deliverable: Month 34
Actual submission date: 07/04/2014
Start date of project: June 1st 2011 Duration: 34 months
version: v.1.0

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 Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

* This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration

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-D3.5-v1.0
Document Title	D3.5 Final report on the operation of the facility
Workpackage	WP3
Authors	Carlos Bermudo (i2CAT) Leonardo Bergesio (i2CAT) Mayur Channegowda (UNIVBRIS) Dimitris Giatsios (UTH)
Editor	Carlos Bermudo (i2CAT)
Reviewers	Sebastià Sallen (UPC)
Delivery Date	11/04/2014
Version	V1.0

Abstract

WP3's aim is to setup and operate the European site of the federated FIBRE testbed facilities. During the length of the project, the FP7 facilities OFELIA and NITOS have been enhanced by hardware and software.

As the facilities or enhancements were operable, they were offered to the public or selected users for experimentation. As usual in a development work, some issues appeared and were reported to the developers and administrators in order to solve them. These issues and their solutions are presented in this document.

Secondly, this document covers any action performed on the infrastructure. In this sense, any change in the configurations along with its motivations and solution are described. General maintenance is the third reported effort of this deliverable.

Finally, all the activities within the operation of the facility related with the establishment of the connectivity between islands and its deployment are described. This last topic is related also with T4.4 in WP4.

This document complements previous reports on the operation of the facilities presented in [1] and [2] with new issues appeared in the period after the publication of the previous document.

TABLE OF CONTENTS

1 Acronyms 6
2 Scope 7
3 Island management and set up 8
3.1 FIBRE's addressing schema 8
3.2 i2CAT island 9
3.2.1 Addressing 9
3.2.2 Management network deployment 9
3.2.3 Island description 10
3.2.4 Deployment of the equipment for QinQ links with other islands 13
3.3 UNIVBRIS island 14
3.3.1 UNIVBRIS network deployment 15
3.3.2 Layer2 VLAN stacking (QinQ) deployment 15
3.3.3 Addition of Media capability 16
3.4 UTH island, NITOS 16
3.4.1 VLANs and addressing 16
3.4.2 Finalization of WiMAX component deployment 16
4 Operation and Maintenance 18
4.1 i2CAT island issues 18
4.1.1 User experience 18
4.1.2 Control framework and monitoring 18
4.1.3 Federation experiments 19
4.2 UnivBRIS island issues 19
4.2.1 User experience 19
4.2.2 Control framework and monitoring 19
4.2.3 Federation experiments 19
4.3 UTH island issues 20
4.3.1 User experience 20
4.3.2 Control framework and monitoring 20
4.3.3 Federation experiments 21
5 FIBRE connectivity 22
5.1 Link i2CAT - UTH 22
5.2 Link i2CAT – UNIVBRIS 22

5.3 Link i2CAT – RNP (Brazil) 23
5.4 Link UTH – UNIVBRIS 24
5.5 Link UNIVBRIS – RNP (Brazil) 25
6 Reference Documents 26

TABLE OF FIGURES

Figure 1: Old i2CAT island configuration and old addressing schema 10
Figure 2: Final i2CAT island configuration with new addressing schema 12
Figure 3: QinQ strategy in i2CAT island 13
Figure 4: UNIVBRIS network setup for FIBRE 14
Figure 5: i2CAT Bristol VLAN trace 16
Figure 6: Topology of WiMAX component at NITOS testbed 17
Figure 7: Link between i2CAT and UTH 22
Figure 8: Link i2CAT- UNIVBRIS 23
Figure 9: Link UTH - UNIVBRIS 24
Figure 10: Link UNIVBRIS – RNP 25

1 Acronyms

BS	Base Station
DVI	Digital Visual Interface
FIBRE	Future Internet testbeds / experimentation between Brazil and Europe
L2	Layer 2 “Data link layer” of the OSI model
L3	Layer 3 “Network layer” of the OSI model
MPLS	Multi-Protocol Label Switching
MS	Milestone
NAT	Network Address Translation
NREN	National Research and Education Network
OCF	OFELIA Control Framework
OF	OpenFlow
OFELIA	OpenFlow in Europe: Linking Infrastructure and Applications
OMF	cOntrol and Monitoring Framework
UPC	Technical University of Catalonia
VM	Virtual Machine
VPN	Virtual Private Network
VT AM	Virtualization Aggregate Manager
WP	Work Package

2 Scope

This deliverable document report keeps a similar structure as previous reports on the operation of the facilities. It starts with a brief description of individual islands describing the enhancements in the facility and the new features since the previous milestone MS11 Second report on the operation of the facility [1]. Then each individual island will report on the issues encountered with respect to the island and the possible solution for the problems faced. It will concentrate on 3 key areas mainly: to host users, install and manage control framework and hardware and also the experiences of federation with other islands. Finally, the status of the links between islands is presented.

3 Island management and set up

This section aims to present the efforts done during this last period regarding the set up of the individual European islands. These changes involve reconfigurations, addition of equipment, connectivity activities, etc.

3.1 FIBRE's addressing schema

In a joint task with WP2 a new addressing schema was designed with the goal of interconnecting both the Brazilian and European sides of the facility. As it was explained in [2], the different islands count with up to 3 different networks:

- Experimental or Data Network. This is an OpenFlow network that connects the OpenFlow switches with the users' VMs available for experimenting.
- Control Network. This network gives users access to the several services hosted in the servers to control and use the facility.
- Management network. This network is not intended to be accessible by users. Management network allows the Island Managers to manage the infrastructure of their islands.

The data network is L2, and the L3 configuration is part of the user's job depending on the experiments he needs to perform. The addressing schema explained in this section targets the Control Network, and in a secondly, the management network.

The addressing schema can be summarized as follows:

- Top level:
  - 10.0.0.0/9 → Europe
  - 10.128.0.0/9 → Brazil
- Once in Europe:
  - 10.E_IID.0.0/16
- Once in Brazil:
  - 10.B_IID.0.0/16

The firs distinction done is to separate European and Brazilian islands. This is done with the first bit of the second octet of the IP address.

Europe: 10.0.0.0/9 → 00001010.**0**0000000.00000000.00000000

Brazil: 10.128.0.0/9 → 00001010.**1**0000000.00000000.00000000

The rest of the second octet (bits 2nd to 8th) is used to name an island in each side. This leads to up to 127 different islands in each side. E_IID stands for European Island ID while B_IID is the same for the Brazilian. E_IID goes from 1 to 127 and B_IID goes from 128 to 254. For example, in the European side, the islands for i2CAT and Bristol have these networks:

i2CAT: 10.1.0.0/16 → 00001010.0**0000001**.00000000.00000000

Bristol: 10.2.0.0/16 → 00001010.0**0000010**.00000000.00000000

This configuration defines the two lasts octets for internal island addressing. This means that each island can map up to 65536 IP addresses inside it (256^2) that can define according to its own needs.

3.2 i2CAT island

3.2.1 Addressing

In the i2CAT's case, the internal addressing (the two last octets) is separated in two ranges of addresses: Control and Management. Management range is for internal use only and it is not expected to be accessible from outside of the island, while the Control network offers the access to the Expedient software and public addresses for the created virtual machines.

These ranges are defined by the first bit of the third octet (mask /17). This gives a range of 32768 public available IP addresses (128*256). From these, 26 are reserved for local services (VMs to host Control Framework, FlowVisor, Database, etc.) and the remaining 32742 (32768-26) are reserved for experimenters' VMs.

i2CAT Control: 10.1.0.0/17 → 00001010.00000001.**0**0000000.00000000

i2CAT Management: 10.1.128.0/17 → 00001010.00000010.**1**0000000.00000000

This example of addressing schema can be seen in Figure 2, while Figure 1 depicts the state of the island with the old addressing.

3.2.2 Management network deployment

As it was already explained in previous deliverables and milestones, the i2CAT island's internal management network aims to interconnect the different equipment in the island in order to be accessed and managed from the office by the island managers. As seen in Figure 1, due to a limitation in the number of legacy interfaces in the switches (it is pure OpenFlow), the unique management interface in the switch is isolated from the OpenFlow part and so the switch could not be use for the uplinks between servers. For this reason, the extra interfaces in the network card of the servers had to be used for this objective. Guimera server was connected to the three OpenFlow-enabled PRONTO switches and the remaining servers where uplinked to the first one. Although this configuration worked well, it was not efficient in terms of interfaces used. It required an interface for each OF switch and 2 interfaces on each server to form the uplinks. With such configuration, it was not possible to add more switches to the island in case it was extended.

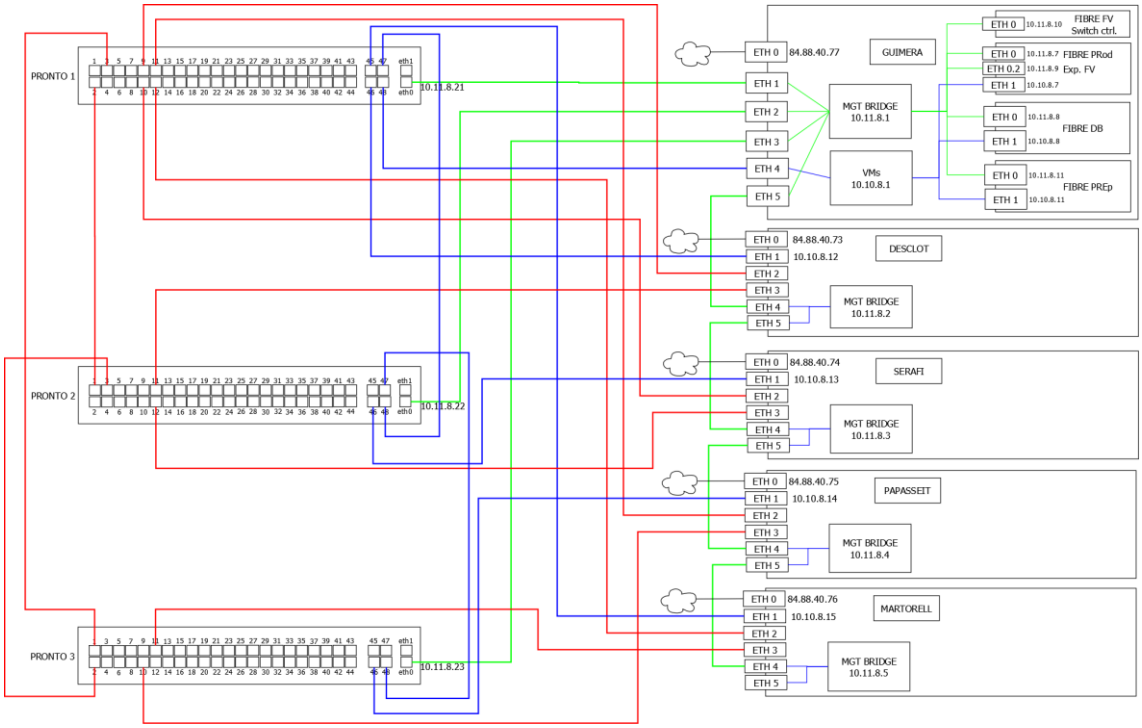

Figure 1: Old i2CAT island configuration and old addressing schema

The solution was to deploy a new simple learning switch 3Com to allow accessing the configuration ports of the OpenFlow-enabled experimentation switches from any of the island servers using only one eth interface in each server, as can be seen in Figure 2 (also showing new addressing schema explained in section 3.2.1). This configuration simplifies the deployment and allows providing more interconnections between users' VMs and OpenFlow switches if needed through making a new connection between a free interface in the server and a free port in any of the OpenFlow switches.

3.2.3 Island description

Although the island has been described in previous deliverables, here is a summary of the different hardware and virtual machines that can be seen in Figure 2. The island is composed by 5 servers: Guimera, Desclot, Serafi, Papasseit and Martorell. Guimera is used to host the VMs where the OCF and required tools (FlowVisor, DB) are deployed. Desclot is used for development, where tests are performed and the rest (Serafi, Papasseit and Martorell) are used to deploy the experimenters' VMs.

The VMs defined inside the Guimera server are:

- FIBRE Prod: this VM contains production environment with the deployed OCF, which manages the users' experiments.
- FIBRE DB: this VM has a MySQL database to store all the required data by OCF
- FIBRE Prep: preproduction environment of the OCF with a smaller MySQL database where modifications to the source code are tested before releasing to the production environment.
- FIBRE FV: this VM was deployed after issue CFM_42_02 related to the OF configuration of the switches explained in section 4.4.1 of [1].

These servers are connected to the three OpenFlow-enabled PRONTO switches through several interfaces. Eth ports of the switches are connected to the servers for configuration using an intermediate 3Com learning switch as explained in previous section.

PRONTO's ports are separated in 2 networks:

- Ports 41-48: management network, it is used for OCF internal management. This network is not user available. They act as a normal learning switch with no OF capabilities.
- Ports 1-40: experiment network, used to define the topology over which the users will deploy their experiments. These ports provide the OF capabilities.

Finally, a CISCO switch is used to connect these switches to other islands to perform the federation. More details about this switch are provided in section 3.2.4.

All hardware characteristics (servers and switches) are described in more detail in [6].

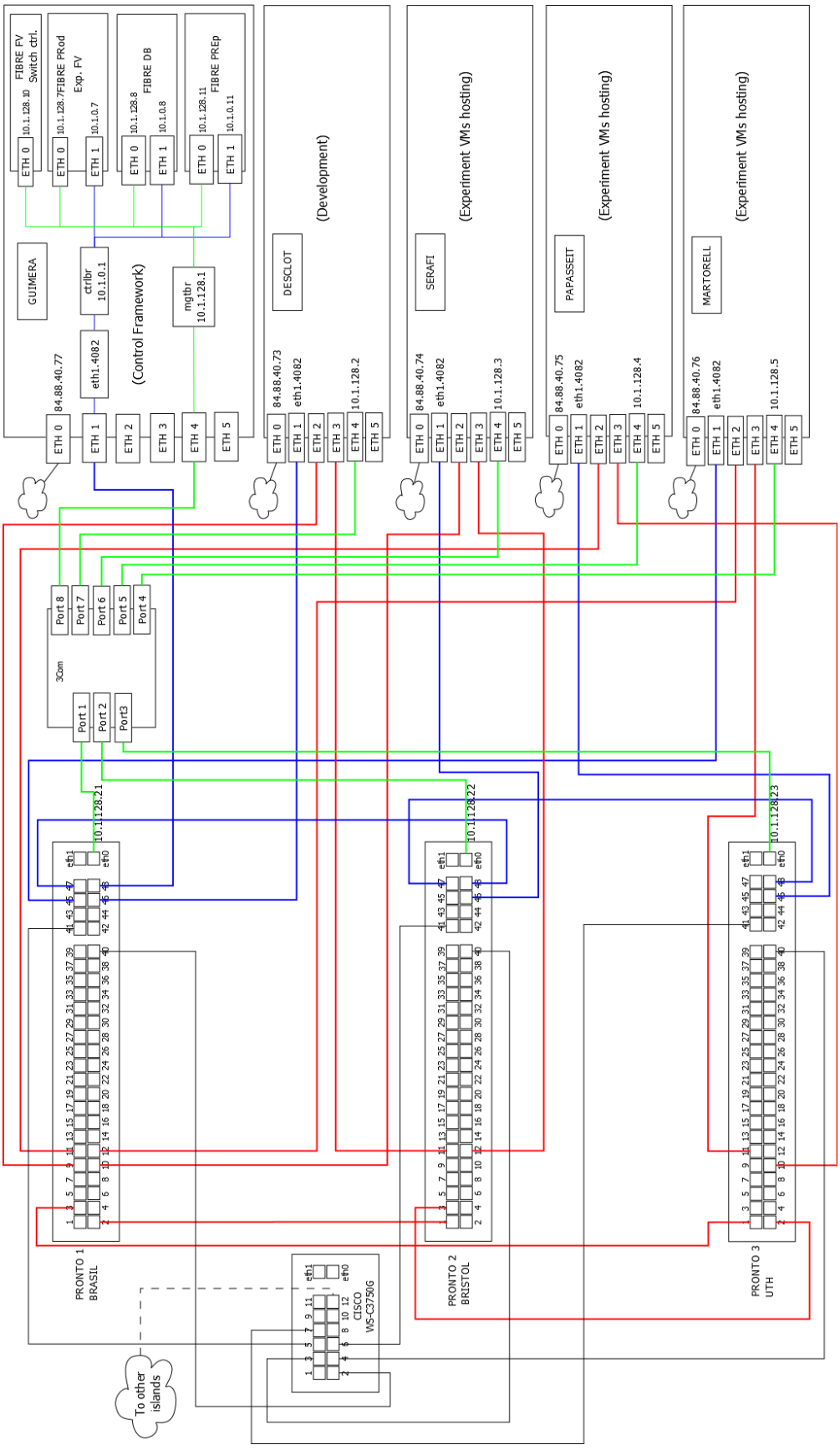

Figure 2: Final i2CAT island configuration with new addressing schema

3.2.4 Deployment of the equipment for QinQ links with other islands

As introduced in [1] in order to support the QinQ links to the rest of the islands in the federation, new equipment was introduced to the i2CAT's island: one switch CISCO WS-C3750G. The deployment is described in Figure 3. The role of this switch is to perform the outer tagging depending on the destination of the packet. The other key element in the deployment is the, also already introduced in [1], stacking of two different FlowVisors. In this period, the configuration and a huge activity of troubleshooting of the links were performed following the design and strategy already reported.

Within FIBRE there are two federated networks: Data network corresponding with the experimental traffic of the users, and Control network corresponding with the traffic of the communication between components of the control framework, controllers and SSH of the users to their VMs. The later uses the VLAN 4082 while the experimental traffic can be tagged with any other VLAN that isolates the slice (except from 4083 which is the local management networks).

The traffic coming from all the islands is double tagged. First it is tagged with the inner VLAN for control or experiment traffic, and secondly with the outer VLAN provided by RedIris/Netherlight/GÉANT to transport the traffic between islands. This traffic arrives to the island via the trunk link in the CISCO switch. It removes the outer tag and forward the inner tagged traffic to two different ports: one aggregating the control traffic, and another three corresponding with the experimental traffic to/from different islands. The lower FlowVisor controlling the Pronto OpenFlow switches discard the non-control traffic in the ports of the control network, while the upper FlowVisor redirects the experimental traffic of each experiment to its corresponding OpenFlow Controller (provided by the user).

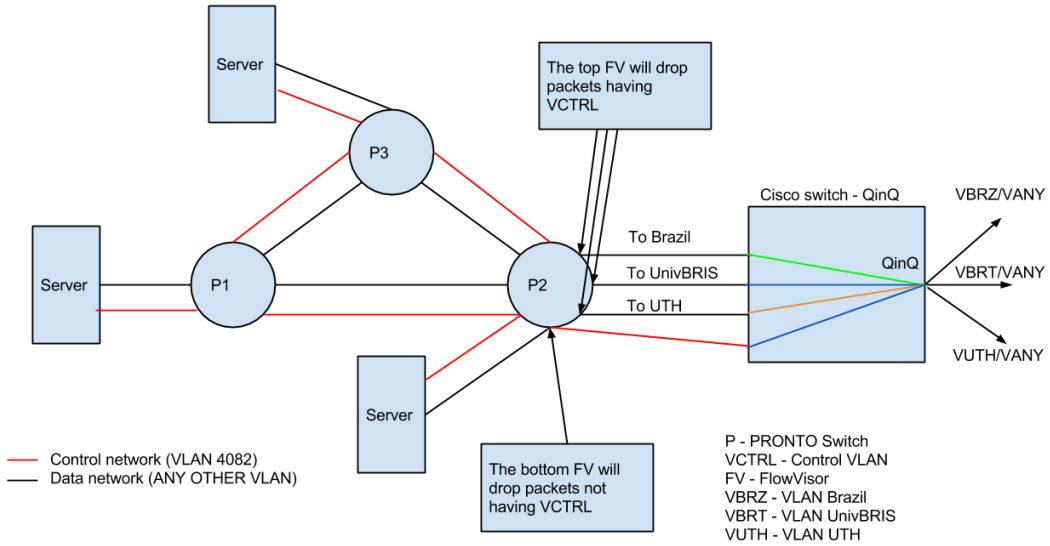

Figure 3: QinQ strategy in i2CAT island

In the inverse direction, the mechanism is the same; the traffic arriving to the CISCO switch from the i2CAT island is tagged with the outer VLAN in the input ports and sent to the trunk link in order to arrive to the destination island.

3.3 UNIVBRIS island

UNIVBRIS follows the OCF control architecture making sure it is compatible with FIBRE network scheme. As assigned, the internal addressing (the two last octets) is separated in two ranges of addresses: Control and Management. Management range is for internal administration i.e. for island managers to access and it is not expected to be accessible from outside the island, while the Control network offers the access to the Expedient software and public addresses for the created virtual machines.

These ranges are defined by the first bit of the third octet (mask /17). This gives a range of 32768 public available IP addresses (128*256). From these, 26 are reserved for local services (VMs to host Control Framework, FlowVisor, Database, etc.) and the remaining 32742 (32768-26) are reserved for experimenters' VMs.

UNIVBRIS Control: 10.2.0.0/17 → 00001010.00000001.00000000.00000000

UNIVBRIS MGT: 10.2.22.0/23 → 00001010.00000010.00010110.00000000

This is depicted in Figure 4:

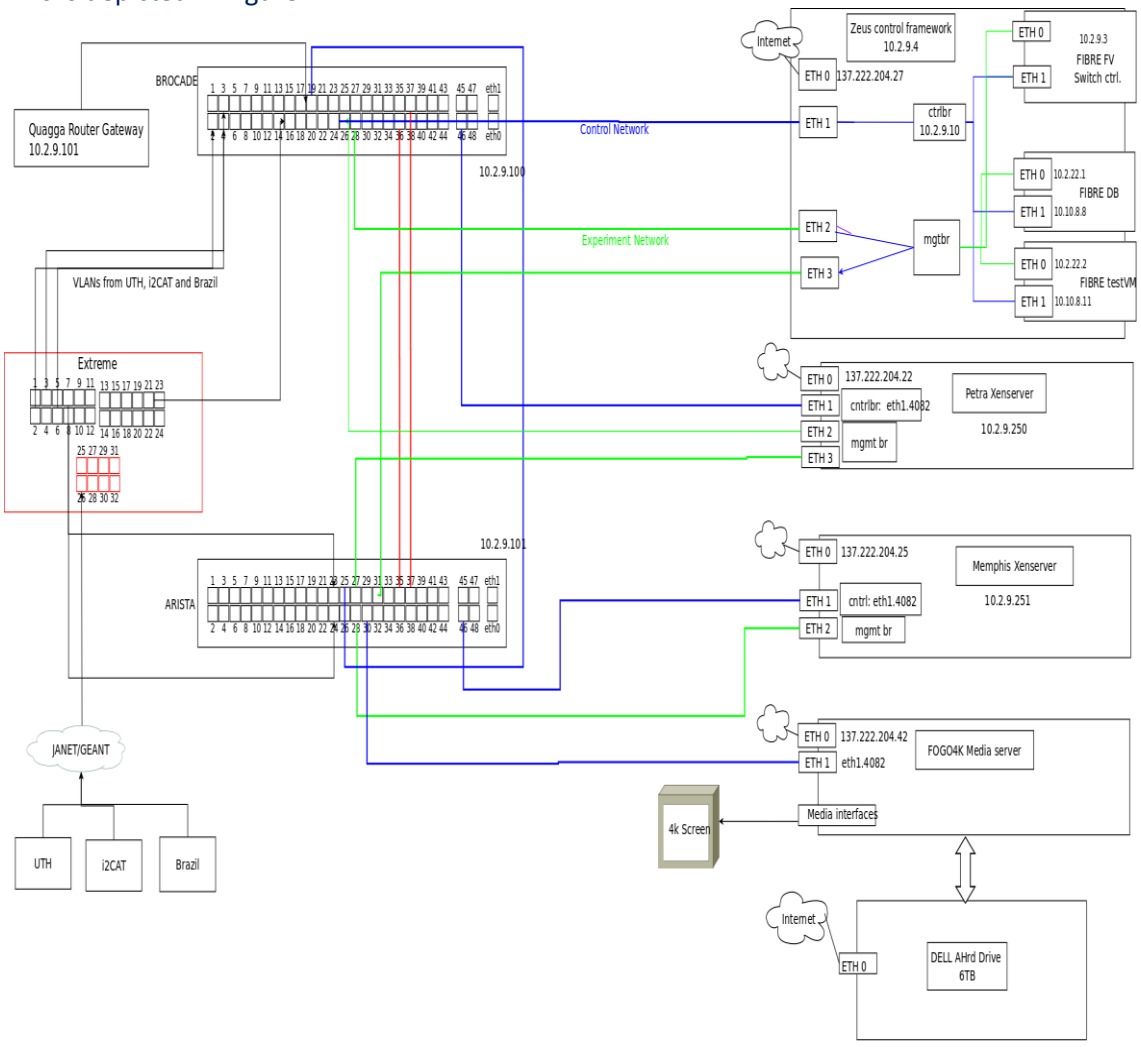

Figure 4: UNIVBRIS network setup for FIBRE

3.3.1 UNIVBRIS network deployment

Following is the description of each of the devices and their network connections.

All devices are connected to the Internet via interface eth1 which is connected to the university network.

Control framework: host Zeus houses the Ofelia control framework (OCF) along with the FlowVisor which provides the network slices for user experimentation. It also consists of the virtualization and OpenFlow resource aggregates and the FlowVisor VM. There is also a testVM which is currently being used to test MySlice plugins from the control framework. The server also acts as a NAT device exposing the aggregates in a private network to a public address which is accessible for MySlice.

Xenservers: Hosts Petra and Memphis are the xenservers providing the user virtual machines. The configuration is based on the available interfaces i.e. both machines have one interface for control and one or many for experimental as in Figure 4. Both machines have a control and management bridge which holds the virtual interfaces of the virtual machines and provides connectivity to them. The control network interfaces on 10.2.22.x network allows users to log into their VMs whereas experimental interfaces participates in the experiments.

Media Server, Storage and Screens: The media server is used for the technology pilot use case 2 in WP5 and its details are mentioned further down in the document.

3.3.2 Layer2 VLAN stacking (QinQ) deployment

UNIVBRIS has established 1Gig GEANT connections with UTH and i2CAT and also a similar connection to RNP, Brazil backbone over Internet2. Extreme 10G switch is used to receive all the associated partners' connection VLANs. UTH on 199, i2CAT on 1049 and RNP backbone (Internet2) on VLAN ID (VID) 900 which are received as outer VLAN (SVlan) and the inner VLAN 4082/4083 (Cvlans) correspond to the fibre control/experimental VLANs. The approach is different than traditional QinQ where you have different ethertypes for Svlan (x88a8) & Cvlan (x8100), in the FIBRE case we use ethertype 8100 since the ethertype of 88a8 is not recognised by local NRENs. This is known as VLAN stacking where the outer stacked VLAN is used to switch to different partners and the inner VLANs for the FIBRE project network.

The Extreme X650 switch takes care of en/decapsulating the packets and to tag/untag outer VLANs as shown in Figure 5. The respective VLANs are individually dropped on to the brocade switch which then takes care of switching the inner FIBRE VLANs (4082/4083). E.g. i2CAT incoming traffic (|1049|4082|), shown in trace Figure 5, is received at Extreme port 26 which removes the outer tag of 1049 and then forwards the untagged (4082/4083 VIDs) to brocade's port2 through Extreme port2 (refer Figure 4). Brocade switch then identifies the 4082 control traffic and then forwards it to the control network of FIBRE.

```
Frame 36: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
Ethernet II, Src: IntelCor_36:31:67 (00:15:17:36:31:67), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Source: IntelCor_36:31:67 (00:15:17:36:31:67)
  Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 1049
  000. .... .... .... = Priority: Best Effort (default) (0)
  ...0 .... .... .... = CFI: Canonical (0)
  .... 0100 0001 1001 = ID: 1049
  Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 7, CFI: 0, ID: 4082
  111. .... .... .... = Priority: Network Control (7)
  ...0 .... .... .... = CFI: Canonical (0)
  .... 1111 1111 0010 = ID: 4082
  Type: ARP (0x0806)
  Trailer: 00000000000000000000000000000000000000
Address Resolution Protocol (request)
```

Figure 5: i2CAT Bristol VLAN trace

3.3.3 Addition of Media capability

UNIVBRIS has added the 4k streaming solution to the testbed. A media server with 6TB storage is dedicated for this. Currently 4 display screens are being used to showcase each quadrant of the 4K video but in the coming months there is plan to get a 4k screen (costs not from project). The media server houses the 4K Fogo software developed by the Lavid team in UFPB with co-ordination from RNP. The server also consists of GPU (graphic processor) with 4 display ports having the capability to support single 4k screen or 4 x full HD screens.

3.4 UTH island, NITOS

3.4.1 VLANs and addressing

UTH island, the NITOS testbed, does not use OCF, it exposes a public interface for SFA communication, and provides ssh access to registered users through a public interface (and from there ssh access to their reserved nodes only). Therefore, there was no need to setup any specific VLAN for control messages, nor specify control addresses.

QinQ has been employed in NITOS as well, in order to distinguish among traffic belonging to different experimental slices. Tagging and untagging with the outer VLAN tag is performed in a Linux machine acting as a gateway. The outer VLAN tags for UTH are 691 for the connection with i2CAT and 692 for the connection with UNIVBRIS.

3.4.2 Finalization of WiMAX component deployment

A set of Greenpacket UT WiMAX dongles has been added to the WiMAX component of NITOS, apart from the equipment reported in the MS11 report [1]. Two HTC Evo 4G smartphones with WiMAX connectivity have also been acquired. The latter cannot be into the fixed testbed environment and are mainly being used by UTH volunteers for mobility related experiments.

Additionally, a new server machine has been setup, the WiMAX-RF server, to host the OMF AM service that controls BS parameters (both local BS parameters and subscriber configuration options). The basic topology of the WiMAX component can be seen below.

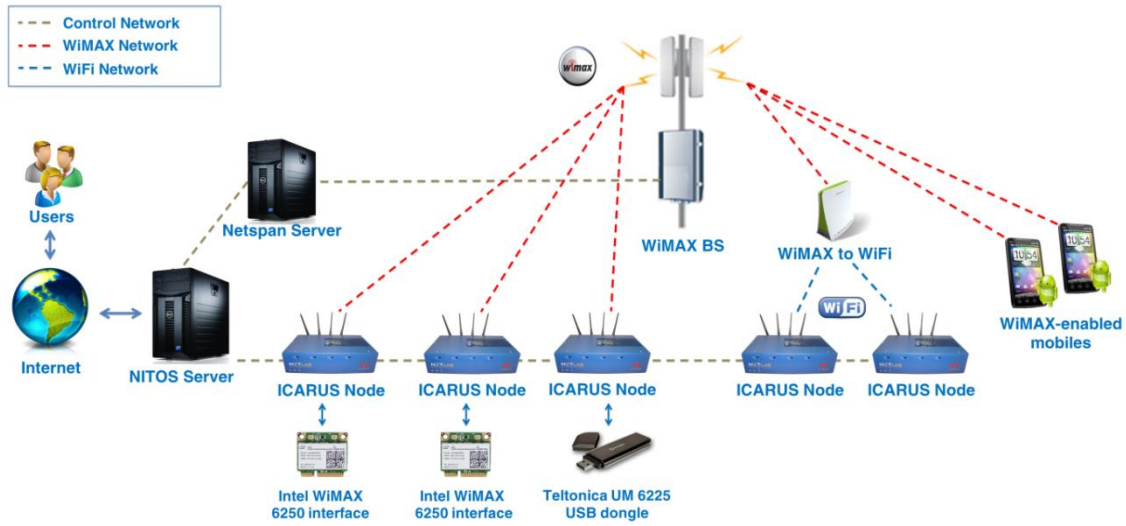

Figure 6: Topology of WiMAX component at NITOS testbed

4 Operation and Maintenance

4.1 i2CAT island issues

4.1.1 User experience

The issues reported in this section were identified during the usage of the facility by users coming from i2CAT, students in UPC and the OFERTIE FP7 project [3].

ID: CFM_41_01	
Issue	Definition of IP ranges with repeated names
Component	VT Manager
Description	The VT Manager supports the definition of IP ranges to be provided by the OCF to the users VMs. During the definition of this range by the Island Manager in the VT Manager, the identification name assigned to the range was the same of a previous existing name. This triggered an unexpected error whose exception was not captured in the code and caused the VT Manager to crash returning an "Internal Server Error" to the browser.
Solution	Once the source of the error was located, the VT AM code was updated to capture the exception and show a warning message to the Island Manager noticing that the chosen name was already used.

4.1.2 Control framework and monitoring

ID: CFM_42_03	
Issue	VLAN assignment through different islands
Component	OCF
Description	When an experimenter requests a FlowSpace for his slice, the way to isolate it from other experiments is through a VLAN assignment. When the slice is spanned over multiple federated islands, the FlowSpace has to be approved individually by the Island Manager in each island. Furthermore, the VLAN assigned has to be the same in all the approved FlowSpaces, otherwise the experiment will not work. Although the experimenter can suggest a VLAN or range of VLANs for the FlowSpace when requesting it, it is not mandatory; IMs can assign whichever VLAN or range they want depending on the island's policies or availability of free VLANs. In previous deployments of OCF, where the number of islands was smaller, this issue was solved manually via email coordination between the IMs involved in the slice, but in FIBRE, where the amount of islands is bigger, this solution is not feasible.
Solution	The solution was the development of an automatic VLAN assignment module, able to get single VLANs or ranges of VLANs from all the islands of the slice by monitoring the islands' OFAMs to find the intersection of available VLANS and assigning them to the FlowSpace. Technical details of this solution can be found in section 4.2 from FIBRE deliverable document D3.3 [4].

4.1.3 Federation experiments

ID: CFM_43_04	
Issue	Intercontinental link not available for demo
Component	OCF Expedient
Description	To perform a demo during 2nd FIBRE Open Workshop, a link between i2CAT and Brazil was needed to interconnect Aggregate Managers. But the QinQ link with the corresponding VLANs was not fully configured, a temporal solution was needed.
Solution	The temporal solution in order to perform the demo was to set up a VPN over the already deployed GEANT link between Europe and Brazil.

4.2 UnivBRIS island issues

4.2.1 User experience

ID: CFM_51_04	
Issue	Media use case display & Interfaces
Component	Media Server
Description	The media server supported only display ports whereas the 4 screens setup to show the media content had DVI ports.
Solution	Ordered few display port to DVI converters.

4.2.2 Control framework and monitoring

ID: CFM_52_03	
Issue	Virtual Machine Storage
Component	Xenserver and Dell Storage device
Description	Need hard disk storage space for user VMs
Solution	Added support in the control framework to hold virtual machines in the storage. Also enabled replication at the storage device to have redundant backups.

4.2.3 Federation experiments

ID: CFM_53_04	
Issue	Intercontinental link over Internet2
Component	Extreme Switch
Description	AmPath node at edge of Internet2 connection to Brazil upgraded their equipment; they were unable to translate Bristol VLAN 900 to FIBRE VID 3505.
Solution	Notified RNP about the connection problem and the VLAN was extended into RNP domain. Changed the VLAN configuration accordingly in the

	extreme switch.

ID: CFM_53_05	
Issue	MySlice Integration over public IP
Component	Control framework server
Description	For Federation the aggregates needed to be exposed over the Internet using public addresses
Solution	In order to make the OCF aggregates available to MySlice we had to get public addresses for the aggregates. So we ran overloaded NAT to use a single public IP to represent different aggregates with different ports.

ID: CFM_53_06	
Issue	Routing between different islands
Component	Software router
Description	For Federation we needed a router at the Bristol hub to route between EU and Brazil islands
Solution	Installed Quagga soft router in UNIVBRIS island

4.3 UTH island issues

4.3.1 User experience

ID: CFM_61_03	
Issue	Topology Assessment and Experiment Planning
Component	NITOS Connectivity tool, NITOS distance tool
Description	Users need to have a good picture of the node topology in NITOS and of the link quality among node pairs before setting up and running their experiments.
Solution	Two utilities have been integrated in the NITOS website for that purpose, where users can see the physical distances among nodes, and, more importantly, to see the link qualities between pairs of nodes. The latter measurement takes place at real time upon request (for reserved nodes only), so it depicts the current channel conditions.

4.3.2 Control framework and monitoring

ID: CFM_62_04	
Issue	OMF support for controlling WiMAX devices
Component	OMF
Description	As described in the MS11 report, UTH was in the process of building OMF drivers (Resource controllers) for the NITOS WiMAX client devices

	(specifically the RC for the WiMAX to WiFi AP was pending) and an OMF AM service for controlling the BS.
Solution	The development of these OMF interfaces has finished. Now the entire WiMAX component of NITOS is controllable through OMF. More technical details are to be found in D3.4 [5].

4.3.3 Federation experiments

ID: CFM_63_03	
Issue	Participation of WiMAX nodes in federated experiments
Component	NITOS server
Description	The traffic to and from nodes connected to the BS via their WiMAX interfaces needs to be forwarded to the Internet, to allow for experiments involving remote islands.
Solution	As an addition to the wimaxrf service, a Click (modular software router) installation has been employed, that is used to setup the experimentation datapath. The datapath concerns whether the nodes are going to have connection to the Internet over the WiMAX interface or just communicate with each other. The service has been designed in a way that a connection over the GEANT network will be able to be used.

5 FIBRE connectivity

5.1 Link i2CAT - UTH

In order to setup the link between i2CAT and UTH, a petition form was made to GÉANT through CESCA/RedIRIS and GRNET, which are the i2CAT and UTH contact points to GÉANT respectively. Once the petition was submitted, a communication channel was established with the interested institutions to follow the required steps and have a constant feedback in order to set up the circuit setup at the end sites. Once GÉANT confirmed that the whole path was established, point to point tests were performed to confirm the correctness of the installation. The final step was to make the circuit arrived to the testbeds as described in previous sections.

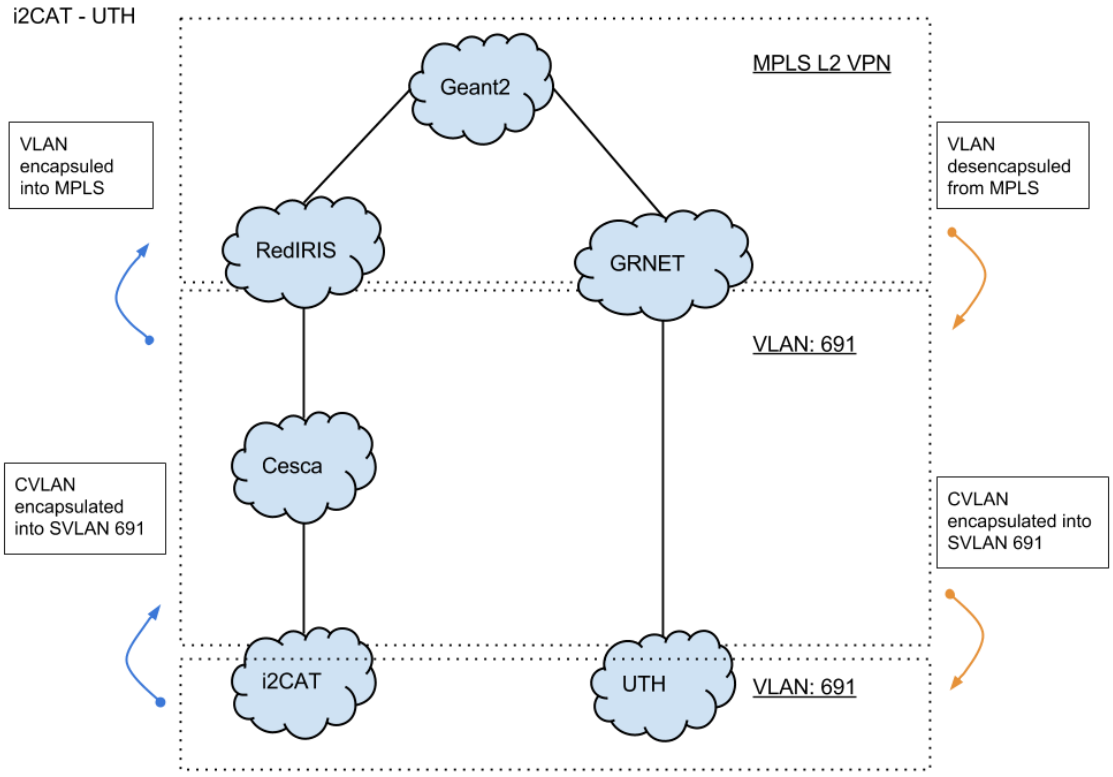

Figure 7: Link between i2CAT and UTH

5.2 Link i2CAT – UNIVBRIS

FIBRE UNIVBRIS' circuit was a migration from University of Essex through JANET. The set up of this circuit is quite different from the usual. It is supported by Netherlight with a native Ethernet connection of 1Gbps. In order to respect the different VLAN domains of the NREN participating on the circuit (RedIRIS and JANET), a PVLAN switch has been performed from Netherlight. This is changing the native PVLAN 195 from RedIRIS to PVLAN 318 from JANET and backwards. This is possible since Netherlight has deployed Carrier Ethernet enabled equipment and use dedicated network interfaces for every institution connected.

This circuit is setup for using QinQ VLAN-Stack, using Cisco equipment at i2CAT and Extreme Networks at Bristol side enabled with this feature.

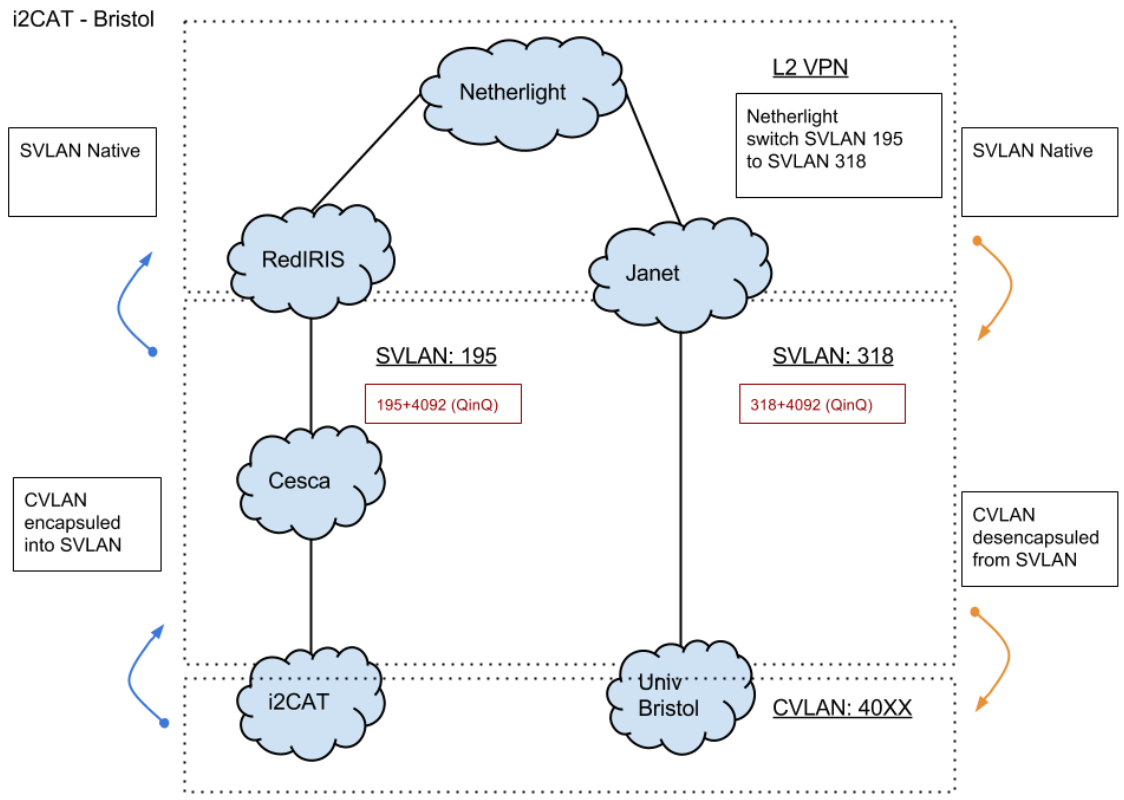

Figure 8: Link i2CAT- UNIVBRIS

5.3 Link i2CAT – RNP (Brazil)

The connection to Brazil is a large setup crossing the Atlantic Ocean where there are a great number of different institutions participating (i2CAT, CESCA, RedIRIS, GÉANT, RedCLARA, RNP). The task requires a huge degree of coordination and collaboration to configure all the intermediate and end equipment and debug the connection.

First steps were administrative and easily achieved. Submitting the petition form and starting the channel communication with the different parts implied was done early. Once the confirmation from the different partners was received, a single test not using QinQ was performed via MPLS L2 VPN circuit successfully.

The second step was to perform the configuration needed for QinQ. This task was not easy since the tests failed, and troubleshooting tasks were required to be performed to find the source of the problem. These activities involved using network sniffers on the different points of the circuit, to search where traffic was dropped, which showed that the problem occurred in some point between RedIRIS-GÉANT-RedCLARA-RNP, but not the exact reason. The QinQ was

dropped on the way from Brazil to Spain, most probably at the MPLS segment. The complex communication with different partners was not clear enough to match the exact problem, since QinQ is not a service provided by GÉANT and the NRENS, and the circuit is working OK without QinQ at the end points.

While the troubleshooting tasks were being performed, RedIris informed us about how the link is configured in order to debug it better. From the last year, after GÉANT changed the equipment in their facilities passing from SONET to Ethernet, the normal way RedIris is delivering traffic to GÉANT is through native Ethernet interfaces in trunk mode using LSPs via the IP trunk link. Nevertheless, for this specific link GÉANT had to maintain the inherited configuration using SONET and so asked RedIris to keep it using LSP. Although intensive testing is still being made in this scenario, RedIris informed us that GÉANT confirmed that at the end of April 2014 they are migrating the connection to RedClara to native Ethernet, then this will imply that the link will have to be completely reconfigured.

As stated in the DoW, this is a technological and project execution risk, and the project is taking care of it. Given this situation, four alternatives are considered, sometimes in parallel:

- Continue the troubleshooting of the QinQ approach in order to solve the problem.
- Take advantage of the i2CAT-UNIVBRIS link to bridge the traffic from/to Spain to/form Brazil via Internet2 using the link UNIVBRIS-RNP.
- Wait for GÉANT to migrate the network trunk from MPLS to Ethernet to reconfigure the link and test the QinQ.
- Use another encapsulation technique in order to transport the tagged traffic of the facility via the already established link.
- Keep using the VPN established to perform the first tests. With this option, once GEANT migrates the network, requires reconfiguring the link anyway.

5.4 Link UTH – UNIVBRIS

Connectivity tests, including QinQ functionality, have been performed successfully after the link establishment.

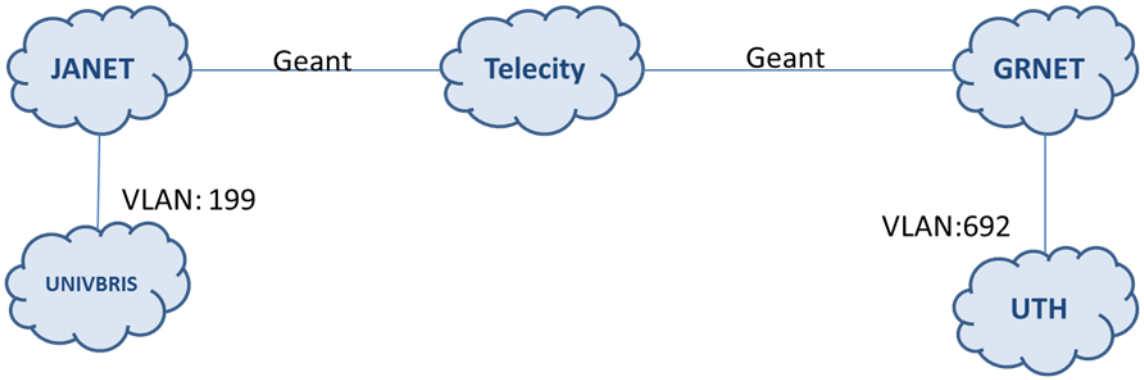

Figure 9: Link UTH - UNIVBRIS

5.5 Link UNIVBRIS – RNP (Brazil)

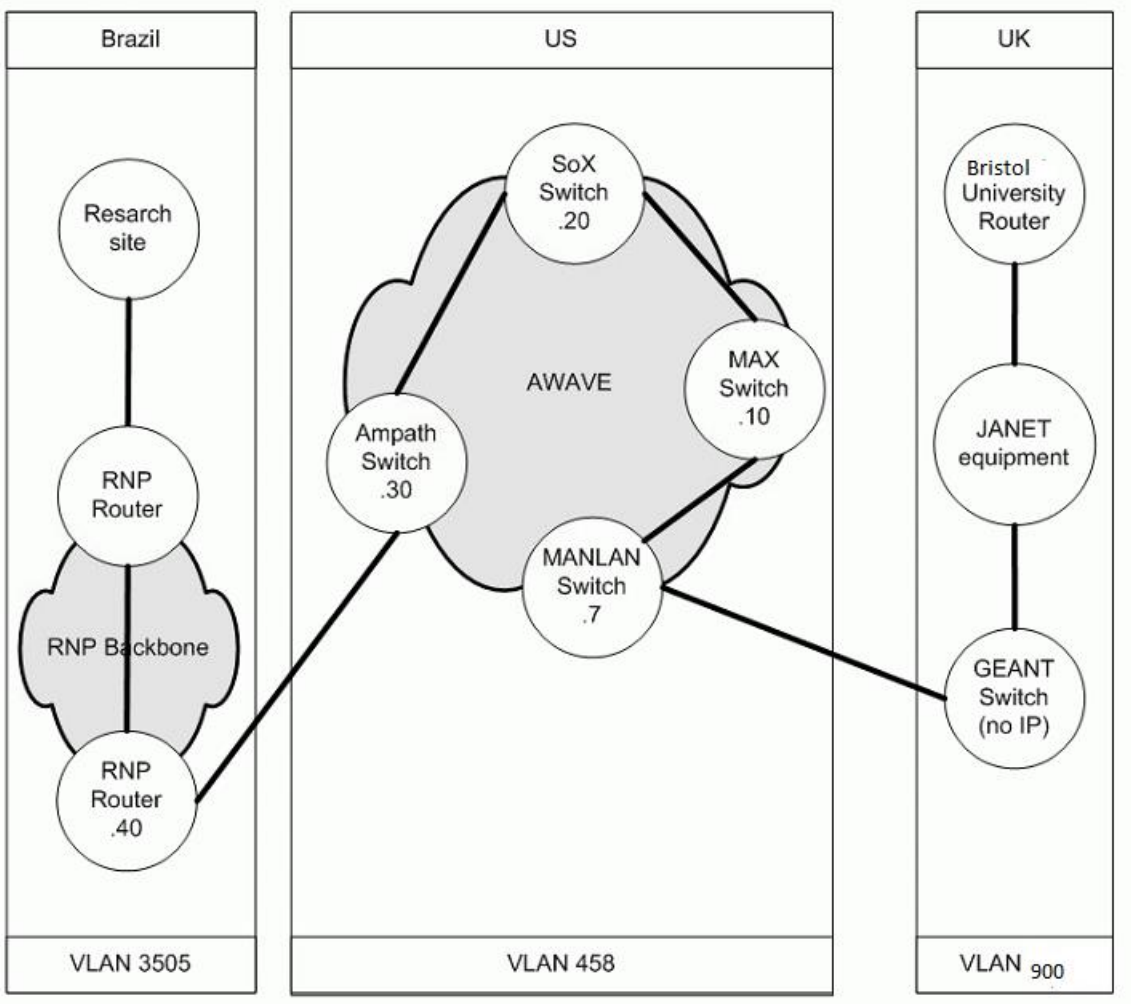

Figure 10: Link UNIVBRIS – RNP

6 Reference Documents

1. FIBRE WP3 MS11 document – Second report on the operation of the facility.
2. FIBRE WP3 Deliverable D3.2 – Report on the European testbeds infrastructure update.
3. OFERTIE (OpenFlow Experiment in Real-Time Internet Edutainment): http://www.ofertie.org/
4. FIBRE WP3 Deliverable D3.3 – Final version of the enhanced OFELIA control framework software.
5. FIBRE WP3 Deliverable D3.4 – Final version of the enhanced OMF control framework.
6. FIBRE WP3 Deliverable MS5 – Report on the list of hardware purchased and expected configuration

"*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