



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*

### D2.7. Report on management operations and monitoring of the FIBRE-BR facilities

Author: WP2  
Revised by: Iara Machado (RNP)

Submission date: 31/03/2014  
Start date of project: June 1<sup>st</sup> 2011 Duration: 34 months  
Version: v.1.0

Project co-funded by the European Commission in the 7 <sup>th</sup> 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)	✓

	<b>Report on management operations and monitoring of the FIBRE-BR facilities</b>	Doc D2.7.FIBRE-v1.0  Date 31/03/2014
---	--	--

<b>FP7 Grant Agreement No.</b>	288356
<b>CNPq Grant Agreement No.:</b>	590022/2011-3
<b>Project Name</b>	Future Internet testbeds/experimentation between BRazil and Europe – EU
<b>Document Name</b>	D2.7.FIBRE
<b>Document Title</b>	D2.7. Report on management operations and monitoring of the FIBRE-BR facilities
<b>Workpackage</b>	WP2
<b>Authors</b>	Tiago Salmito, Daniel Area Leão
<b>Editor</b>	Tiago Salmito
<b>Reviewers</b>	Iara Machado
<b>Delivery Date</b>	31/03/2014
<b>Version</b>	V1.0

	<p><b><i>Report on management operations and monitoring of the FIBRE-BR facilities</i></b></p>	<p>Doc D2.7.FIBRE-v1.0</p> <p>Date 31/03/2014</p>
---	--	---

## Abstract

This document describes the operation, management, and monitoring processes for the Brazilian Experimental Facility, also referred here as the FIBRE-BR. The operation framework covers procedures related to end-users and is divided into three main parts: the usage policy, the experimenter workflow and the FIBRE-BR helpdesk. The management and monitoring processes deal with aspects related to the maintenance of the underlying infrastructure and define tools for monitoring and measuring the quality of service provided by the federated islands in FIBRE-BR.

## TABLE OF CONTENTS

Acronyms .....	6
1 Introduction and Scope .....	7
2 Testbed Operation .....	9
2.1 Acceptable Usage Policy of FIBRE-BR islands.....	9
2.1.1 Acceptable Usage Policy for New Users.....	9
2.1.2 User Requirements.....	10
2.1.3 General terms and conditions for resource providers.....	10
2.2 User Registration Workflow .....	10
2.3 FIBRE-BR Helpdesk .....	13
3 Testbed Management .....	17
3.1 Infrastructure .....	17
3.2 Addressing .....	19
3.3 Monitoring .....	21
4 Conclusion.....	24

## List of Figures

Figure 1. Workflow for user registration.....	11
Figure 2. NOC portal web page;.....	12
Figure 3. User registration form. ....	12
Figure 4. FIBRE-BR helpdesk organization.....	14
Figure 5. RT ticketing system web interface. ....	15
Figure 6. Ticket information interface .....	16
Figure 7. Set of CMFs available in the FIBRE federated testbed. ....	17
Figure 8. FIBRE-BR overlay network topology.....	19
Figure 9. ZenOSS monitored infrastructure list.....	22
Figure 10. List of ZenOSS events.....	23

	<p><b>Report on management operations and monitoring of the FIBRE-BR facilities</b></p>	<p>Doc D2.7.FIBRE-v1.0</p> <p>Date 31/03/2014</p>
---	---	---

## Acronyms

CF	Control Framework
CPqD	Telecommunications Research and Development Centre
FIBRE	Future Internet testbeds / experimentation between Brazil and Europe
L2VPN	Layer 2 Virtual Private Network
L3VPN	Layer 3 Virtual Private Network
LDAP	Lightweight Directory Access Protocol
LDAP	Lightweight Directory Access Protocol
NOC	Network Operation Center
OCF	OFELIA Control Framework
OFELIA	OpenFlow in Europe: Linking Infrastructure and Applications
OMF	cControl, Management and Measurement Framework
RNP	National Research and Education Network
UFF	Fluminense Federal University
UFG	Federal University of Goiás
UFPA	Federal University of Pará
UFPE	Federal University of Pernambuco
UFRJ	Federal University of Rio de Janeiro
UFSCar	Federal University of São Carlos
UNIFACS	Salvador University
USP	University of São Paulo
VLAN	Virtual Local Area Network
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network

	<b>Report on management operations and monitoring of the FIBRE-BR facilities</b>	Doc D2.7.FIBRE-v1.0  Date 31/03/2014
---	--	--

## 1 Introduction and Scope

This deliverable (D2.7) describes the operation, management, and monitoring processes for the FIBRE-BR testbed. The management, operation and monitoring processes are implemented within individual islands and in the NOC for proper operation of FIBRE-BR system. These processes are defined and discussed in this deliverable.

The main goal of the FIBRE project is the design, implementation and validation of a central shared Future Internet research testbed, supporting the joint experimentation of European and Brazilian researchers. To achieve this, four main activities should be undertaken:

1. The development and operation of a new experimental unit in Brazil, including the installation of equipment to support experimentation with various technologies (layers 2 and 3, wireless, optical) as well as the development and implementation of a control framework to automate the use and operation of the testbed.
2. The development and operation of an experimentation facility for the Future Internet in Europe and the Federation of two existing infrastructures: OFELIA and OneLab. Two OFELIA islands (i2CAT and the University of Bristol (UNIVBRIS)) and UTH Nitos testbed will be enhanced by: i) adding more physical resources (servers, switches and OpenFlow-enabled access points) to be able to handle large numbers users and different use cases, ii) improve their control frameworks (based on the control structure of OFELIA and OMF) and iii) the addition of more workforce to operate the facility.
3. The Federation of Brazilian and European experimental facilities, both physical connectivity and control level framework to support the provisioning of resources slices from both sides of the testbeds.
4. The design and implementation of pilot applications utilities that show the power of sharing of experimental facilities Europe-Brazil Future Internet.

The FIBRE-BR infrastructure consists of an expandable collection of components. The set of components chosen for inclusion in the infrastructure at any given time are intended to enable the creation of virtual networks covering the entire range of experiments required for FIBRE user community in Brazil.

The FIBRE-BR includes leading sites (also known as islands) in each of the initial Brazilian partners in this project. These sites are interconnected via private channels (Level 2) for "wide area" and metropolitan networks available to Brazilian research and education community. These include RNP's national backbone network and the GIGA network testbeds held jointly by RNP and contributing authors. RNP own metropolitan networks are used to connect the last mile where necessary, and international connections of RNP provide access to other international Testbeds like OFELIA testbeds and Nitos, for purposes of the federation.

Therefore, a network able to manage resources at the national and international level to integrate all islands and tools is required. For this purpose, there is the initiative of developing an overlay network on Ipê Network to manage the integration between the islands, dynamically and on

	<p><b><i>Report on management operations and monitoring of the FIBRE-BR facilities</i></b></p>	<p>Doc D2.7.FIBRE-v1.0</p> <p>Date 31/03/2014</p>
---	--	---

demand, and control the resources that will be used by the experimenter, such as bandwidth, topology of the experiment or equipment.

To this end, a backbone called FIBRENet was built to integrate the islands of the institutions participating in the project and offer a way to build experiments at various levels of network and media (wired or wireless). The FIBRENet will follow the model applied to the SDN (Software-Defined Networking) networks, such as programmability, virtualization and split between planes (control and data).

	<b>Report on management operations and monitoring of the FIBRE-BR facilities</b>	Doc D2.7.FIBRE-v1.0  Date 31/03/2014
---	--	--

## 2 Testbed Operation

The testbed operation processes covers procedures related to the operation of the FIBRE-BR facilities, such as events and actions made by users of the FIBRE-BR islands. The operation of the testbed is divided into three main parts: the acceptable usage policy, the experimenter workflow, and the FIBRE-BR helpdesk, which are discussed in the next subsections.

### 2.1 Acceptable Usage Policy of FIBRE-BR islands

The conditions of use described in the FIBRE-BR Acceptable Usage Policy must be accepted by all users during their registration as a user of the FIBRE-BR testbed. Having one common Acceptable Usage Policy for all users regardless of which island they requested an account, eases administrative and interoperability issues between islands.

The terms of the Acceptable Usage Policy are described below:

#### 2.1.1 Acceptable Usage Policy for New Users

By registering as a FIBRE-BR testbed user, experimenters shall be deemed to accept these conditions of use:

1. Users shall not use the testbed resources for any unlawful purpose and not (attempt to) breach or circumvent any administrative or security controls.
2. Users shall respect intellectual property and confidentiality agreements.
3. Users shall protect their access credentials (e.g. private keys or passwords).
4. User access credentials will expire 1 year after your registration. Users can renew your registration at any time after the expiry date.
5. Users shall immediately report any known or suspected security breach or misuse of the testbed or access credentials to FIBRE-BR's Network Operation Centre (a.k.a. NOC).
6. Users must notify the NOC of any changes to their Registration Information.
7. Use of the testbed resources is at their own risk. The resources offered by each island are provided "as is", with no guarantee that the testbed will be available at any time or that it will suit any purpose.
8. Logged information, including information provided by users for registration purposes, is used for administrative, operational, accounting, monitoring and security purposes only. This information may be disclosed, via secured mechanisms, only for the same purposes and only as far as necessary to other organizations cooperating with the FIBRE-BR testbed. Although efforts are made to maintain confidentiality, no guarantees are given.
9. The island administrators and resource providers are entitled to regulate, suspend or terminate users' access, within their domain of authority, and users shall immediately comply with their instructions.
10. Users are liable for the consequences of their violation of any of these conditions of use.

	<b>Report on management operations and monitoring of the FIBRE-BR facilities</b>	Doc D2.7.FIBRE-v1.0  Date 31/03/2014
---	--	--

### 2.1.2 User Requirements

To be accepted as a FIBRE-BR experimenter and be able to setup an experiment, Users must comply with the following rules:

1. To apply to be registered as a FIBRE-BR testbed user, experimenters must provide the following required information:
  - a) Full name;
  - b) E-Mail;
  - c) Institution for accreditation (if not listed, RNP island is used as catch-all);
  - d) Motivation or reasons to use the testbed;
2. Violation of the this Acceptable Usage Policy may result the following actions:
  - a) The respective User will be contacted.
  - b) The slice and/or the account will be deactivated or terminated.
  - c) The administration of the User institution will be contacted and informed.

### 2.1.3 General terms and conditions for resource providers

Any experimental island providing resources to the FIBRE-BR testbed must agree to the conditions below:

1. All islands recognize the FIBRE-BR NOC as the central entity in charge of offering 1<sup>st</sup> level support to the testbed Users.
2. Each island has a seat in the Governance Board (GB) of the FIBRE-BR testbed. The GB shall meet at least every 3 months to analyze pending requests, settling disputes between members and review the testbed policies.
3. Although each island is autonomous to manage local Users and set the rules inside their domain of authority, all federated islands must not discriminate or deny access to any FIBRE-BR registered user.
4. As long as each island is funded by the FIBRE-BR project, it must make available all resources to all registered users.
5. Each island must indicate an administrator to be in charge of managing 2<sup>nd</sup> level support requests. Any change of administrator must be immediately communicated to the NOC.
6. Each island must define and communicate the working hours of its administrative staff, as well as defining the maximum amount of time a support ticket must be answered.

All islands recognize RNP as the “catch-all island” to analyze registration requests from non-member institutions.

## 2.2 User Registration Workflow

This section describes the workflow that potential FIBRE-BR experimenters must follow to request access to FIBRE-BR facilities. Figure 1 shows the user workflow from moment he/she requests a new account to the moment he/she gets access to control frameworks available in FIBRE-BR’s testbed.

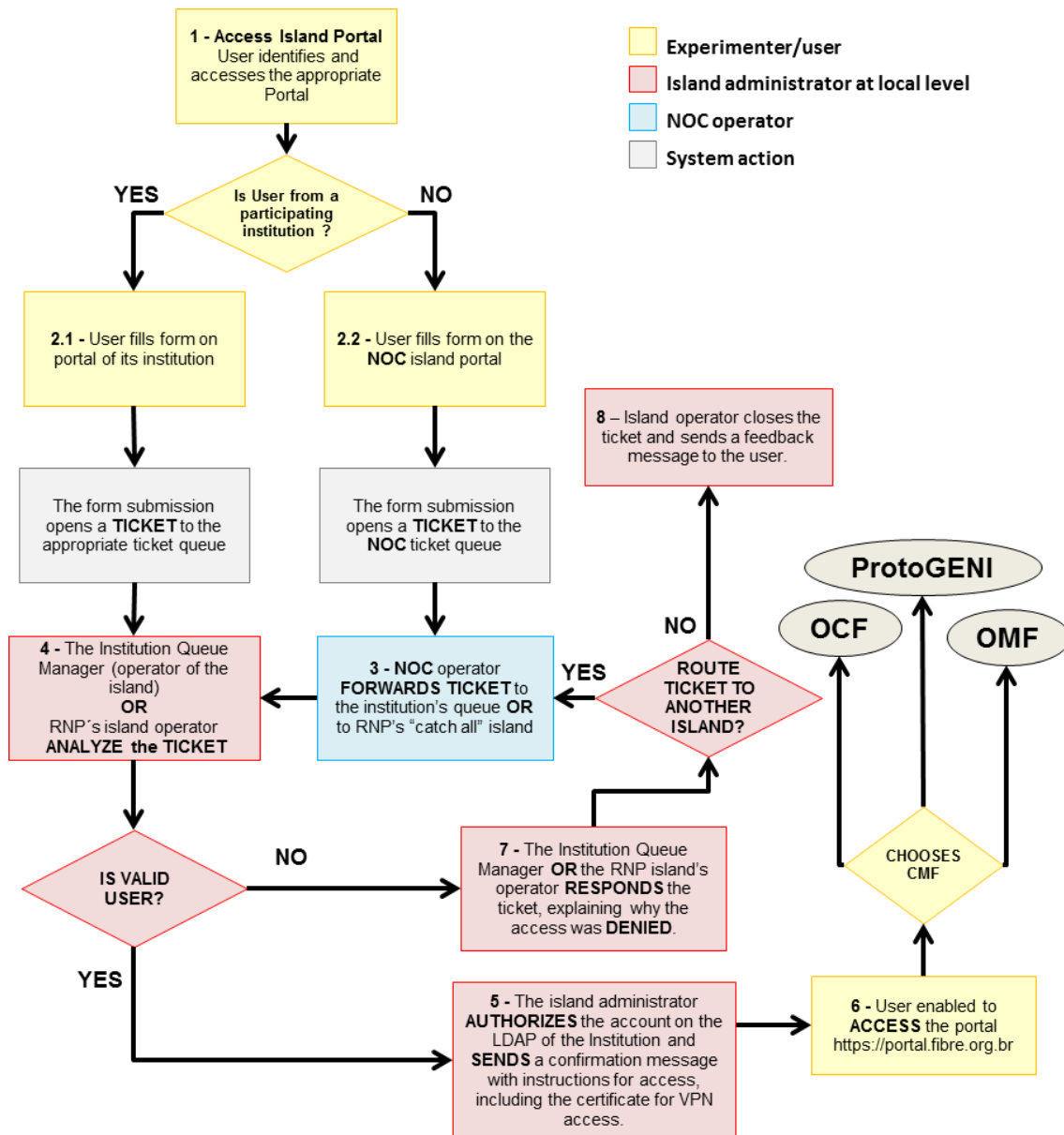


Figure 1. Workflow for user registration.

Each island of the FIBRE-BR testbed maintains a portal web where users can register for an account to access its local control frameworks. Before requesting the account, users must access the portal of its respective institution (step 1 of Figure 1). Users of institutions that host an island of the FIBRE-BR testbed may request access directly in their institution's portal (step 2.1). Users from other institutions can request access through the NOC portal web page (step 2.2), maintained by the FIBRE-BR NOC<sup>1</sup> (Figure 2). The NOC is responsible for controlling and monitoring the network assets of the testbed, monitoring the provided services and to mediate authentication for federated experiments in the FIBRE-BR testbed.

<sup>1</sup> <https://portal.fibre.org.br>

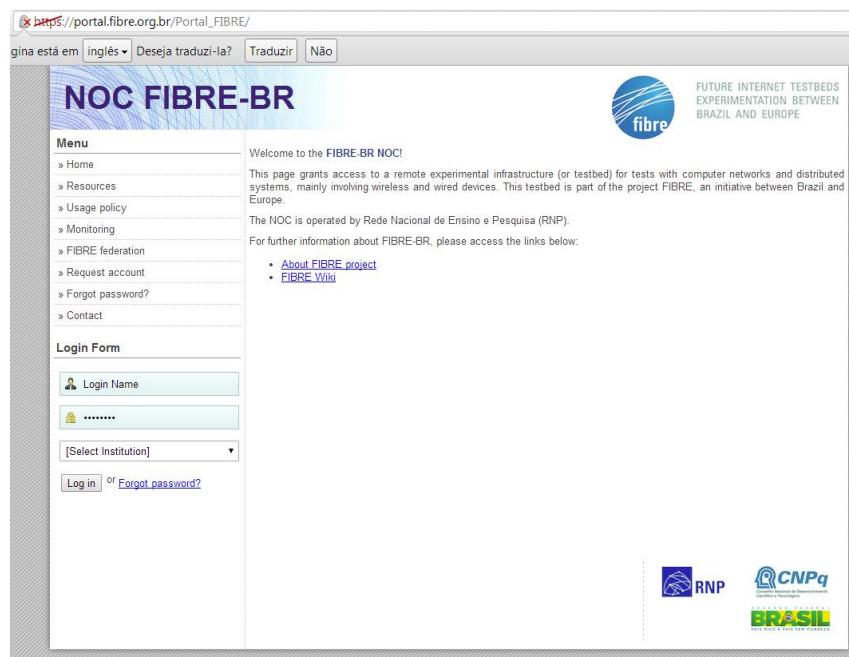


Figure 2. NOC portal web page.

The submission of the “Request account” form (Figure 3) a ticket in the appropriate ticket queue for the target institution. The NOC operator handles requests coming from the NOC portal, forwarding the ticket to a specific institution queue or to RNP’s ticket queue, which acts as a “catch-all island” for experimenters from other institutions (step 3 of Figure 1).

Figure 3. User registration form.

Institution queue managers are FIBRE-BR island operators that are responsible for handling tickets from the queue of their respective institution. Island operators are informed about an incoming request via e-mail. After receiving a registration ticket, the operator must analyze the ticket and decide whether to approve or disapprove the creation of the account (step 4 of Figure 1). Island operators must send a confirmation message with instructions for accessing the

	<b>Report on management operations and monitoring of the FIBRE-BR facilities</b>	Doc D2.7.FIBRE-v1.0  Date 31/03/2014
---	--	--

testbed, including the certificate for VPN and create the account on the LDAP of their institution (step 5). Since user authentication is carried out by a LDAP directory in each island synchronized with a LDAP directory at the NOC, registered users may run federated experiments in more than one island through the NOC portal. LDAP allows authentication with CMFs available in FIBRE-BR testbed (step 6).

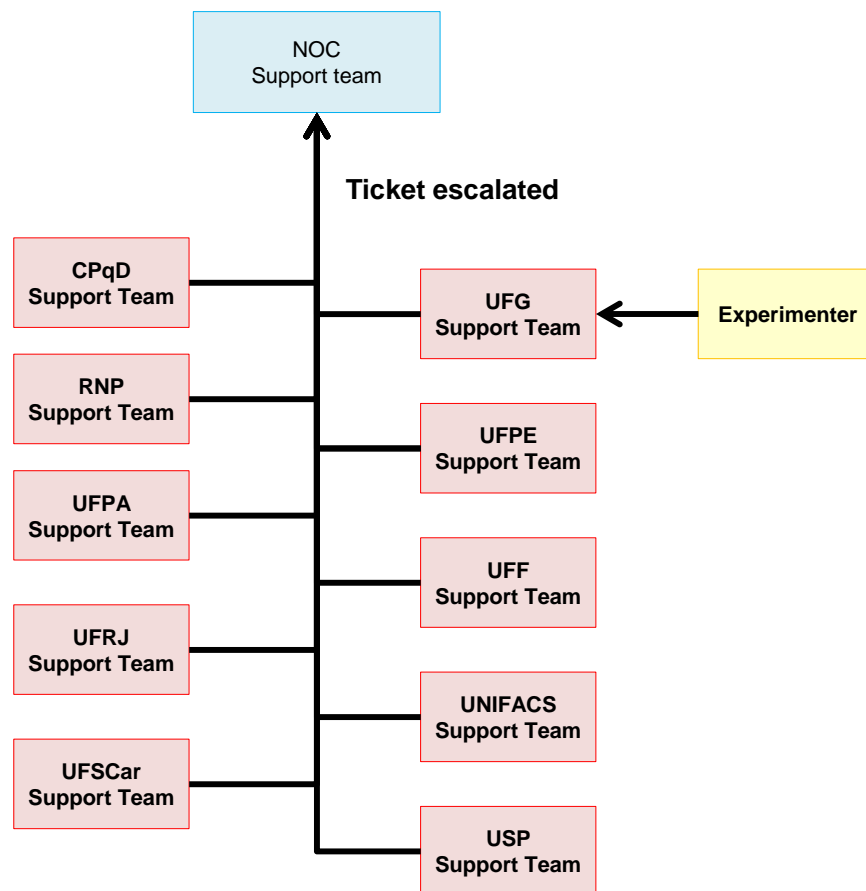
Island operators must respond to the ticket explaining the reason for disapproving user requests (step 7). When a user registration is denied, the ticket may be escalated to the NOC queue to be routed for another island, or closed by the island operator (step 8).

## 2.3 FIBRE-BR Helpdesk

This section describes the FIBRE-BR helpdesk procedures and workflow for contacting staff members for all technical and non-technical issues related to the FIBRE-BR testbed. The ticketing system is the preferred way for users to get support, to report any issues and to notify the personnel responsible for resolving issues reported by the users. The ticketing system is based on RT – Request Tracker<sup>2</sup> – software and is hosted and maintained by RNP.

The FIBRE-BR helpdesk is organized into eleven ticket queues (NOC, CPqD, RNP, UFF, UFG, UFPA, UFPE, UFRJ, UFSCar, UNIFACS and USP), one for each FIBRE-BR island, and an administrative entity, the FIBRE-BR NOC. Figure 4 shows the organization of the FIBRE-BR helpdesk.

<sup>2</sup> <http://bestpractical.com/rt/>



**Figure 4. FIBRE-BR helpdesk organization.**

Each ticket queue has a support team, which is responsible for handling and resolving issues related to their island. The FIBRE-BR NOC operator has visibility to all of the FIBRE-BR issues and will listen for issues related to federated experiments or issues that does not applies to a particular island. To open new tickets, users may send an e-mail for the appropriate ticket queue describing the issue and the ticketing system routes them to the respective island operator. Table 1 shows the e-mail address of the ticket queues of all FIBRE-BR islands.

**Table 1. Island ticket queues.**

Island	Ticket queue
NOC	noc@fibre.org.br
CPqD	fibre-cpqd@rt.rnp.br
RNP	fibre-rnp@rt.rnp.br
UFF	fibre-uff@rt.rnp.br
UFG	fibre-ufg@rt.rnp.br
UFPA	fibre-ufpa@rt.rnp.br
UFPE	fibre-ufpe@rt.rnp.br

	<b>Report on management operations and monitoring of the FIBRE-BR facilities</b>	Doc D2.7.FIBRE-v1.0  Date 31/03/2014
---	--	--

<b>UFRJ</b>	fibre-ufrj@rt.rnp.br
<b>UFSCar</b>	fibre-ufscar@rt.rnp.br
<b>UNIFACS</b>	fibre-unifacs@rt.rnp.br
<b>USP</b>	fibre-usp@rt.rnp.br

Island administrators has limited access on the tickets and can respond only to issues reported to their respective island, whilst the NOC administrators has full access on the tickets, i.e., they are able to reply to open tickets, open new tickets on behalf of other users, change the priority of a ticket, mark a ticket as overdue, close a ticket, ban a user, delete a ticket, post internal notes, transfer ticket to another island and assign the ticket to another member.

Tickets are carried out either through e-mail or by following the link to RNP's ticketing system and accessing the FIBRE-BR helpdesk interface. Figure 5 shows the web interface of the RT ticketing system.

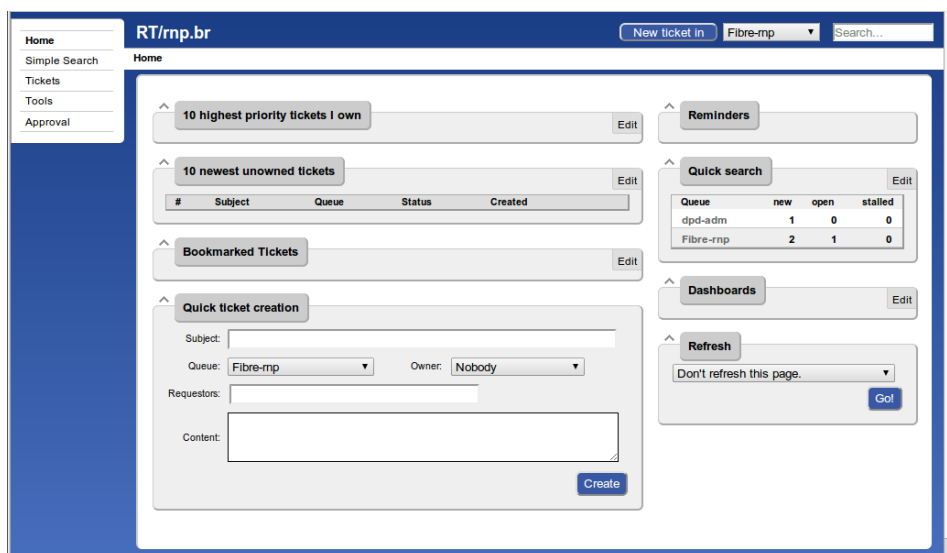
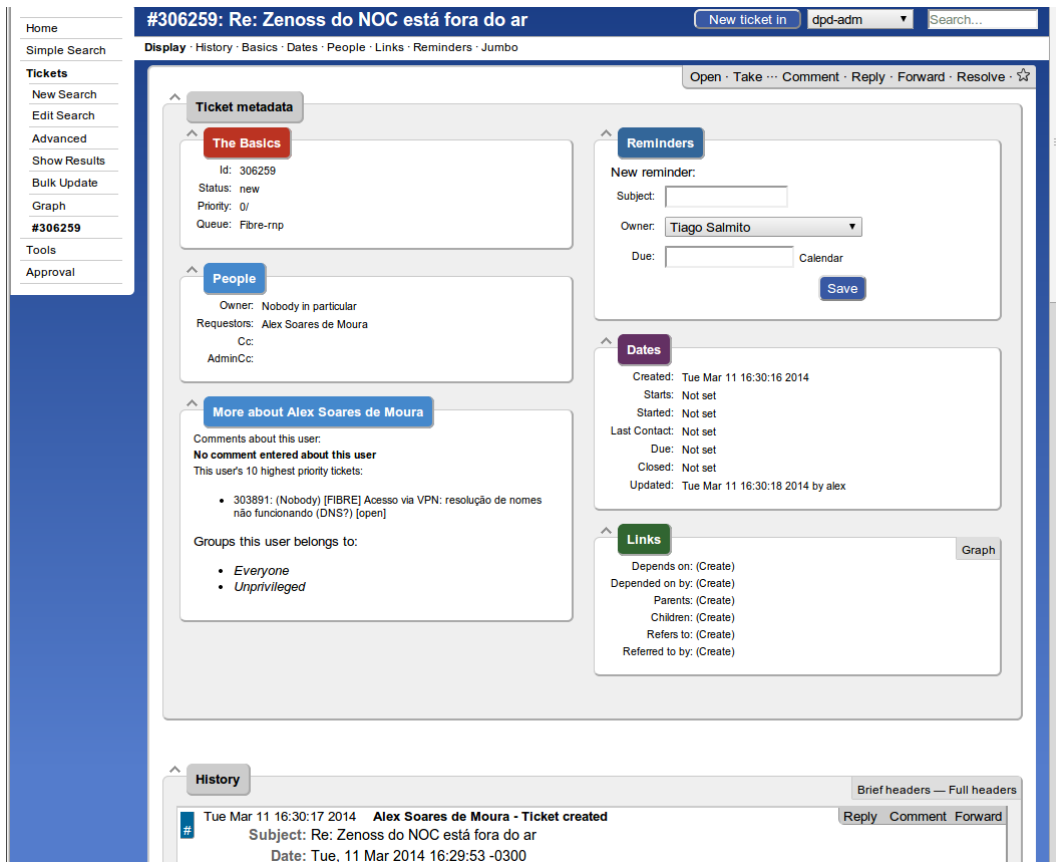


Figure 5. RT ticketing system web interface.

The web interface offers the following operations to island operators: list open tickets, view information about tickets, list answered tickets, list closed tickets, open new tickets on behalf of the end users, list the operators of other islands and modify/change profile settings. Figure 6 shows the interface for viewing tickets.



**#306259: Re: Zenoss do NOC está fora do ar**

Display · History · Basics · Dates · People · Links · Reminders · Jumbo

Open · Take · Comment · Reply · Forward · Resolve · ☆

### Ticket metadata

#### The Basics

Id: 306259  
Status: new  
Priority: 0/  
Queue: Fibre-rnp

#### People

Owner: Nobody in particular  
Requestors: Alex Soares de Moura  
Cc:  
AdminCc:

#### More about Alex Soares de Moura

Comments about this user:  
**No comment entered about this user**  
This user's 10 highest priority tickets:

- 303891: (Nobody) [FIBRE] Acesso via VPN: resolução de nomes não funcionando (DNS?) [open]

Groups this user belongs to:

- Everyone
- Unprivileged

#### Reminders

New reminder:  
Subject:   
Owner: **Tiago Salmato**  
Due:  Calendar **Save**

#### Dates

Created: Tue Mar 11 16:30:16 2014  
Starts: Not set  
Started: Not set  
Last Contact: Not set  
Due: Not set  
Closed: Not set  
Updated: Tue Mar 11 16:30:18 2014 by alex

#### Links

Depends on: (Create)  
Depended on by: (Create)  
Parents: (Create)  
Children: (Create)  
Refers to: (Create)  
Referred to by: (Create)

### History

Tue Mar 11 16:30:17 2014 **Alex Soares de Moura - Ticket created**  
Subject: Re: Zenoss do NOC está fora do ar  
Date: Tue, 11 Mar 2014 16:29:53 -0300

**Figure 6. Ticket information interface.**

In addition to the ticketing system, the FIBRE-BR testbed provides two user mailing lists: [info@fibre.org.br](mailto:info@fibre.org.br) and [fibre-info@fibre.org.br](mailto:fibre-info@fibre.org.br). The former is used from the island managers to inform users regarding any upgrades, downtimes for maintenance or issues in the testbed and the latter is for users to communicate and exchange ideas or common problems regarding their experiments.

### 3 Testbed Management

The testbed is currently composed by ten islands located in Brazil and three in Europe. In this section, we will concentrate on the Brazilian part of testbed.

#### 3.1 Infrastructure

Each island has a common nucleus of OpenFlow-capable switches, as well as a cluster of compute and storage servers, appropriately virtualized, and a set of wireless nodes. Each Brazilian island will propose its own possible extensions, integrating site-specific resources to FIBRE-BR, such as wireless access testbeds (WiFi, WiMax, 3G/4G), OF-enabled equipment, optical networks or even more complex testbeds with heterogeneous resources and their own control framework (e.g.: the Emulab cluster at USP). Figure 7 illustrates a typical FIBRE-BR island, with its common facilities and external connectivity.

The distribution of FIBRE-BR islands shown in Figure 7. The integration of these resources creates a large-scale network. In Europe, there are three islands: one at Fundació i2cat (Spain), one at the University of Bristol (UK), and one at UTH (Greece). The Brazilian part of the testbed is composed by ten islands widely spread across seven Brazilian states. Each island is controlled by one or more CMFs. Figure 7 shows the set of CMFs available in each island, and the network that connects them, the FIBRENet, FIBRE-BR's backbone.

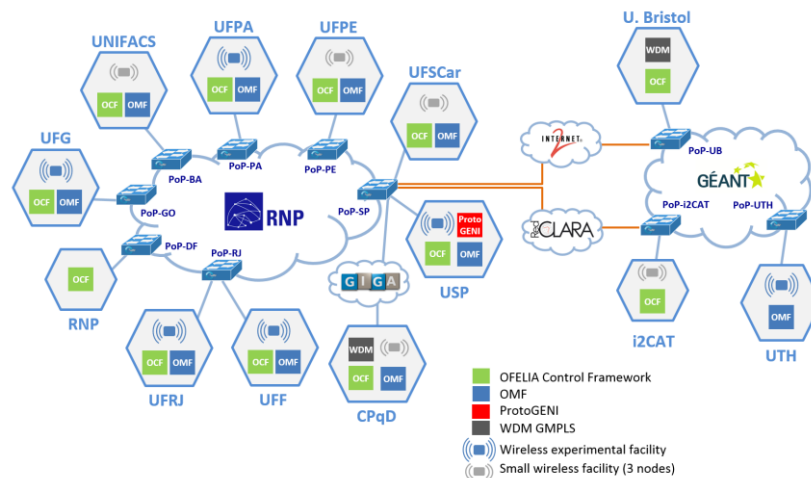


Figure 7. Set of CMFs available in the FIBRE federated testbed.

The FIBRENet is a VPLS overlay network created upon the RNP's backbone (Ipê network), in which the data plane is divided in two parts: an experiment plane and a control plane. The control plan in FIBRENet is prepared to offer control to the central FIBRE-BR NOC. Thus the experimenter can manage and monitor control information among FIBRE-BR islands. In other words, this channel allows communication between control frameworks of all islands and to collect monitoring information. For this an overlay network was built on the backbone of the RNP.

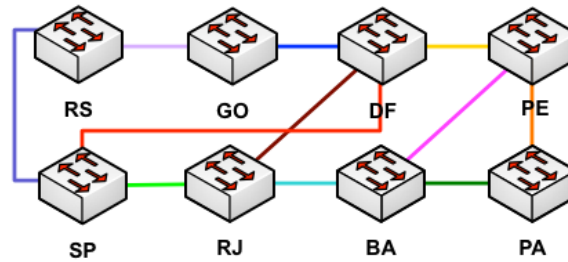
	<b>Report on management operations and monitoring of the FIBRE-BR facilities</b>	Doc D2.7.FIBRE-v1.0  Date 31/03/2014
---	--	--

Virtual Private LAN Service (VPLS) is a way to provide an Ethernet multipoint-to-multipoint communication over IP / MPLS networks. It allows geographically dispersed sites to share the same Ethernet broadcast domain by connecting them through pseudo-wires. The technologies that can be used as Ethernet over MPLS pseudo-wires are, L2TPv3 or even GRE. There are two IETF RFCs (RFC 4761 and RFC 4762) describing VPLS establishment.

The control plane is an overlay mesh network and is used to traffic the data corresponding to the communication of the control frameworks, like OCF and OMF, and the gathering of monitoring information from the components used in the testbed.

The network overlay data plane is used to route traffic between the participants of the experiments using dedicated circuits islands between PoPs. The use of each circuit is determined by identifiers - VLAN IDs - to be defined by administrators.

The network overlay control plane will be used to control data sharing between islands such as monitoring information, OpenFlow control messages between device and controller or remote access for management equipment FIBRE-Net. Furthermore, the control plane network includes the NOC FIBRE-BR, which will operate and control of FIBRE-Net backbone, used by the experimenters during the construction of their inter-island topologies. The topology of the ongoing phase of the FIBRENet overlay network is depicted in Figure 8.



**Figure 8. FIBRE-BR overlay network topology.**

The experiment plane is used to route traffic among participants of the experiments using an overlay point to point network. In this plane, the Flowvisor is the component responsible to segregate the experiments from each other, through the creation of circuits, where each circuit is determined by identifiers, known as VLAN IDs.

In the current phase of the FIBRE-BR deployment, the islands are interconnected through L2VPN overlay network, though some islands are interconnected through L3VPN overlay network, implemented using OpenVPN at FIBRE-BR's NOC.

## 3.2 Addressing

**Table 2. Top Level Routing Table**

Europe	Brazil
10.0.0.0/9	10.128.0.0/9

**Table 3. FIBRE-BR Internal Address ranges**

Institution/Island	ID
NOC	128
UFRJ	129
UFPA	130
UNIFACS	131
UFPE	132
USP	133
UFF	134
UFSCar	135
RNP	136
UFG	137
CPqD	138
New Institutions	N + 1

The following address schema is used to organize the integration of the FIBRE-BR testbed. The first part of this organization it's to separate the Brazilian part from the European. The Table 2 represents this idea, where the range of the second octet from 0 to 127 is used for the European side and the range of 128 to 255 represents the Brazilian side.

	<b>Report on management operations and monitoring of the FIBRE-BR facilities</b>	Doc D2.7.FIBRE-v1.0  Date 31/03/2014
---	--	--

Also, this address schema is used to identify the institution, where the second octet represents an Island. The example below demonstrates the organization:

Address Scheme: 10.X.0.0/8

Examples:

- UFRJ's network: 10.129.0.0/8
- UFF's network: 10.134.0.0/8
- RNP's network: 10.136.0.0/8

For further information about this schema, observe Table 3.

There is a need to create an address schema for each control framework, since they need a range for experiments and a central operation point for the framework. Tables 4 and 5 bellow represents this idea for the OMF and OCF frameworks, respectively:

**Table 4. OMF address schema**

Address schema for OMF	
OMF Portal:	10.X.11.200/8
OMF's nodes:	10.X.10.0/8~10.X.11.0/8
CMC's range:	172.16.X.0/16

**Table 5. OCF address schema**

Address schema for OCF	
OCF Portal:	10.X.0.100/8
OCF's nodes:	10.X.12.0/8~10.X.13.0/8

To help the organization in the Brazilian side of the testbed, a standard addressing schema was used to identify the services and equipment within an Island. Tables 6 and 7 shows the addressing standard adopted for each island equipment:

**Table 6. Island addressing standard for services**

Service	Address
LDAP Server	10.X.0.50/8
Perfsonar1 (eth0)	10.X.0.60/8
Perfsonar1 (eth1)	10.X.0.62/8
Perfsonar2 (eth0)	10.X.0.61/8
Perfsonar2 (eth1)	10.X.0.63/8
OCF framework	10.X.0.100/8
OMF framework	10.X.11.200/8
VPN Server	10.X.0.70/8
ZenOSS/DNS Server	10.X.0.80/8

**Table 7. Island addressing standard for equipment**

Equipment	Address
NetFPGA1	10.X.0.10/8
NetFPGA2	10.X.0.11/8
NetFPGA3	10.X.0.12/8
Pronto Switch	10.X.0.13/8
Virtualization Server	10.X.0.30/8
Top of Rack Switch	10.X.0.1/8

### 3.3 Monitoring

Monitoring of the components is essential to keep a track of the state of the network and service availability, and all the available resources (routers, switches, servers). Network availability comprises the link connectivity among islands and service availability covers the services provided by the end nodes and the state of these nodes. To reduce the complexity of monitoring the whole system, the network monitoring is done by a dedicated central monitoring component located on the NOC and the service availability is done individually by the control frameworks. If strictly necessary, a distributed deployment may be done based on the requirements of the islands to load balance the work on the centralized monitoring component.

The FIBRE-BR monitoring component uses ZenOSS monitoring tool to monitor network, system availability and services that the end nodes provide (e.g VPN connectivity). This component is also used in the OFELIA project. At the moment ping is used to identify the status of the devices and SNMP is used to collect statistics and status of the device according to the monitored resources and memory load or network statistics per interface.

Figure 9 shows the infrastructure list that is monitored in the FIBRE-BR testbed. ZenOSS is able to categorize and group devices in different ways. On the left side the infrastructure is categorized into three different categories; Devices Classes, Groups and Locations. On the right side all the monitored devices and events are listed. Each device is grouped according with their respective island.

The ZenOSS notifies perceived events to the NOC staff via e-mail alerts. Furthermore, it allows for each island administrator to specify custom notification email alerts when an event occurs involving its specific island.



## Report on management operations and monitoring of the FIBRE-BR facilities

Doc D2.7.FIBRE-v1.0

Date 31/03/2014

The screenshot shows the Zenoss CORE interface with the 'INFRASTRUCTURE' tab selected. On the left, a tree view shows 'DEVICES (26)' expanded, listing various categories like AWS, HTTP, KVM, Network, Ping, Power, Printer, and Server. The main area displays a table of 26 devices. Each row includes the device name, IP address, device class, production state, and a status icon. The status icons indicate different levels of health, with red icons for critical issues and green for healthy states. The table is sorted by IP address.

Device	IP Address	Device Class	Production State	Events
ibm.cpqd.fibre.org.br	10.12.0.30	/Ping	Production	1
ibm.noc.fibre.org.br	10.0.0.30	/ServerLinux	Production	1
ibm.mmp.fibre.org.br	10.9.0.30	/Ping	Production	1
ibm.ufpa.fibre.org.br	10.10.0.30	/Ping	Production	1
ibm.ufpa.fibre.org.br	10.3.0.30	/Ping	Production	1
ibm.ufpa.fibre.org.br	10.5.0.30	/Ping	Production	1
ibm.ufpa.fibre.org.br	10.1.0.30	/Ping	Production	1
ibm.ufscar.fibre.org.br	10.8.0.30	/Ping	Production	1
ibm.unifacs.fibre.org.br	10.4.0.30	/ServerLinux	Production	1
ibm.usp.fibre.org.br	10.6.0.30	/ServerLinux	Production	1
ldap.noc.fibre.org.br	10.0.0.50	/ServerLinux	Production	1
ldap.uff.fibre.org.br	10.7.0.50	/Ping	Production	1
ldap.usp.fibre.org.br	10.6.0.50	/ServerLinux	Production	1
mod.noc.fibre.org.br	10.0.0.3	/ServerLinux	Production	2
mon.noc.fibre.org.br	10.0.0.80	/ServerLinux	Production	1
mon.usp.fibre.org.br	10.6.0.80	/ServerLinux	Production	1
netpqa1.usp.fibre.org.br	10.6.0.10	/Ping	Production	1
netpqa2.usp.fibre.org.br	10.6.0.11	/ServerLinux	Production	2
netpqa3.usp.fibre.org.br	10.6.0.12	/ServerLinux	Production	2
ocf.noc.fibre.org.br	10.0.0.100	/ServerLinux	Production	1
ocf.usp.fibre.org.br	10.6.0.100	/ServerLinux	Production	1
omf.noc.fibre.org.br	10.0.11.200	/ServerLinux	Production	1
perfsonar.noc.fibre.org.br	10.0.0.60	/ServerLinux	Production	1
evalqa.noc.fibre.org.br	10.0.0.81	/ServerLinux	Production	1
vpn.noc.fibre.org.br	10.0.0.70	/ServerLinux	Production	1
vpn.usp.fibre.org.br	10.6.0.70	/ServerLinux	Production	1

Figure 9. ZenOSS monitored infrastructure list.

Events tab lists all the events for all monitored devices and shows the error details when selected by the user (Figure 10).

The screenshot shows the Zenoss CORE interface with the 'EVENTS' tab selected. The 'Event Console' view is active, displaying a table of events. The table columns include Status, Severity, Resource, Component, Event Class, Summary, First Seen, Last Seen, and Count. The events are sorted by 'Last Seen' in descending order. The table shows 24 rows of events, with the first row being a critical event (red icon) for 'ibm.cpqd.fibre.org.br' with the summary '10.12.0.30 is DOWN!'. The last row is a warning event (yellow icon) for 'ocf.usp.fibre.org.br' with the summary 'Problem while executing plugin zenoss.snmp.HRSWRUnMap'. The table is filtered to show only events from the last 24 hours.

Status	Severity	Resource	Component	Event Class	Summary	First Seen	Last Seen	Count
1	Critical	ibm.cpqd.fibre...	/Status/Pi...	/Status/Pi...	10.12.0.30 is DOWN!	2014-03-24 14:...	2014-03-25 06:...	974
1	Critical	ibm.unifacs.fi...	/Status/Pi...	/Status/Pi...	10.4.0.30 is DOWN!	2013-11-28 15:...	2014-03-25 06:...	130703
1	Critical	vpn.usp.fibre...	/Status/Pi...	/Status/Pi...	vpn.usp.fibre.org.br is DOWN!	2014-02-05 12:...	2014-03-25 06:...	33734
1	Critical	ibm.ufscar.fib...	/Status/Pi...	/Status/Pi...	ibm.ufscar.fibre.org.br is DOWN!	2014-02-15 08:...	2014-03-25 06:...	19633
1	Critical	netpqa2.usp...	/Status/Sn...	/Status/Sn...	SNMP agent down - no response received	2013-11-10 08:...	2014-03-25 06:...	7461
1	Critical	netpqa3.usp...	/Status/Sn...	/Status/Sn...	SNMP agent down - no response received	2013-11-05 11:...	2014-03-25 06:...	14258
1	Critical	ocf.usp.fibre...	/Status/Sn...	/Status/Sn...	SNMP agent down - no response received	2013-12-16 15:...	2014-03-25 06:...	4779
1	Critical	vpn.usp.fibre...	/Status/Sn...	/Status/Sn...	SNMP agent down - no response received	2014-02-05 16:...	2014-03-25 01:...	67
1	Critical	ibm.unifacs.fi...	/Status/Sn...	/Status/Sn...	SNMP agent down - no response received	2013-11-28 15:...	2014-03-25 01:...	273
1	Critical	mon.noc.fibre...	/Status/Up...	/Status/Up...	Problem while executing plugin zenoss.snmp.HRSWRUnMap	2013-11-24 17:...	2014-03-24 19:...	197
1	Critical	vpn.noc.fibre...	/Status/Up...	/Status/Up...	Problem while executing plugin zenoss.snmp.HRSWRUnMap	2013-11-24 17:...	2014-03-24 19:...	196
1	Critical	ocf.noc.fibre...	/Status/Up...	/Status/Up...	Problem while executing plugin zenoss.snmp.HRSWRUnMap	2013-11-24 17:...	2014-03-24 19:...	197
1	Critical	omf.noc.fibre...	/Status/Up...	/Status/Up...	Problem while executing plugin zenoss.snmp.HRSWRUnMap	2013-11-24 17:...	2014-03-24 19:...	194
1	Critical	perfsonar.noc...	/Status/Up...	/Status/Up...	Problem while executing plugin zenoss.snmp.HRSWRUnMap	2013-11-24 17:...	2014-03-24 19:...	185
1	Critical	ldap.noc.fibre...	/Status/Up...	/Status/Up...	Problem while executing plugin zenoss.snmp.HRSWRUnMap	2014-03-17 19:...	2014-03-24 19:...	15
1	Critical	ibm.usp.fibre...	/Status/Up...	/Status/Up...	Problem while executing plugin zenoss.snmp.HRSWRUnMap	2013-11-04 02:...	2014-03-24 19:...	109
1	Critical	ldap.usp.fibre...	/Status/Up...	/Status/Up...	Problem while executing plugin zenoss.snmp.HRSWRUnMap	2013-11-04 02:...	2014-03-24 19:...	66
1	Critical	mon.usp.fibre...	/Status/Up...	/Status/Up...	Problem while executing plugin zenoss.snmp.HRSWRUnMap	2013-11-04 02:...	2014-03-24 19:...	54
1	Critical	ibm.mmp.fibre...	/Unknown	/Unknown	...	2014-02-13 09:...	2014-02-13 09:...	9
1	Critical	vpn.usp.fibre...	/Status/Up...	/Status/Up...	Problem while executing plugin zenoss.snmp.HRSWRUnMap	2013-11-04 02:...	2014-01-24 16:...	44
1	Critical	ocf.usp.fibre...	/Status/Up...	/Status/Up...	Problem while executing plugin zenoss.snmp.HRSWRUnMap	2013-11-04 02:...	2014-01-24 16:...	30

	<p><b>Report on management operations and monitoring of the FIBRE-BR facilities</b></p>	<p>Doc D2.7.FIBRE-v1.0</p> <p>Date 31/03/2014</p>
---	---	---

Figure 10. List of ZenOSS events.

The following services are currently monitored in the NOC:

- FIBRE-BR main portal;
- DNS server;
- VPN server;
- LDAP server;
- NOC OCF Expedient;

The following services are being monitored in each island:

- Local island portal;
- Island OCF Expedient, optin and vt-manager services;
- OMF services;
- LDAP server;

The network interfaces of the following equipment are monitored in each island:

- Top of Rack switch (DATACOM 4100);
- Virtualization server;
- Openflow Switch (Pronto Pica8);
- Icarus nodes (when available);
- NetFPGA servers;

	<b>Report on management operations and monitoring of the FIBRE-BR facilities</b>	Doc D2.7.FIBRE-v1.0  Date 31/03/2014
---	--	--

## 4 Conclusion

This deliverable described the operation, management, and monitoring processes for the FIBRE-BR testbed. The management, operation and monitoring processes. The NOC has weekly meeting with island local administrator to discuss problems and solution for it. However, due the FIBRE-BR not open yet for external users, we not have many use case to discuss only deployment problems like tracking change management, due a firmware upgrade, or new version for a CMF.

The next step is announce it to Brazilian research during the National Brazilian Conference on Distributed System and Computer Network that will be on May. FIBRE-BR is ready to connect to FIBRE-EU in a federation way.



***Report on management  
operations and monitoring of  
the FIBRE-BR facilities***

Doc D2.7.FIBRE-v1.0

Date 31/03/2014

*"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