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***

D 2.4 Report on FIBRE-BR operational plan

Author: WP2
Revised by: Iara Machado (RNP)
Alex Moura (RNP)
Michael Stanton (RNP)
Antonio Jorge G. Abelém (UFPA)
Due date of the Milestone: Month 20
Actual submission date: 03/05/2013
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)	✓

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-D4.2-v1.0
Document Title	D2.4 FIBRE-BR operational plan
Workpackage	WP2
Authors	Daniel Marques (RNP) Alex Moura (RNP) Iara Machado (RNP
Editor	Iara Machado (RNP)
Reviewers	Michael Stanton (RNP) Iara Machado (RNP) Alex Moura (RNP) Antonio Jorge G. Abelém (UFPA)
Delivery Date	03/5/2013
Version	V1.0

Abstract

The purpose of this document is to define how the Network Operations Centre (NOC) for the FIBRE-BR network will work. Besides that, it also points out new requirements that the NOC should meet. This document references requirements described in the sections 11 and 12 from the Deliverable 2.1.

TABLE OF CONTENTS

List of Figures

1 Acronyms

API	Application Programming Interface
CLI	Command Line Interface
CP	Control Plane
FIBRE	Future Internet testbeds / experimentation between Brazil and Europe
FIBRE-BR	
FIBREnet	
GUI	Graphical User Interface
IM	Island Manager
MS	Milestone
NOC	Network Operational Centre
NREN	National Research and Education Network
OCF	OFELIA Control Framework
OF	OpenFlow
OFELIA	OpenFlow in Europe: Linking Infrastructure and Applications
OSPF	Open Shortest Path First
p.	page
SDN	Software Defined Networking
SFA	Slice-based Federation Architecture
VLAN	Virtual Local Access Network
VM	Virtual Machine
VPN	Virtual Private 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

The objective of the FIBRE's NOC (Network Operation Centre) is controlling and monitoring the network assets of the FIBRE-BR and monitoring the services provided by the testbed, supporting its users.

3 Infrastructure

This section presents the infrastructure to be used for NOC operation.

Responsible for the Operation:	RNP
Server Location:	PoP-DF, Federal District - Brasília
Operational System:	Debian 7
Hypervisor:	Xen
Server Specification:	• Dell PowerEdge R620 • (2) Intel Xeon E5-2360 • (2) 16Gb Memory • (6) HD 600Gb 10k RPM

4 NOC Tiered Support

According to the section 12.1, from the Deliverable 2.1, the Support Structure requirements are the following:

[Req OP01] The FIBRE-BR system MUST be supported by a minimum support infrastructure. It is envisioned to have different levels of support to ensure service operations of the islands and its connection.

[Req OP02] The FIBRE-BR system MUST at least offers 3 levels of support:

- Level 1 - To be provided by a centralized team in one of the institutions participating in the FIBRE-BR efforts. The responsibility of this team is the evaluation of the issues raised and being able to redirect all relevant events for each island.
- Level 2 - To be offered in a distributed fashion by a team at each island. The responsibility of this level is the handling of incidents of the local island.
- Level 3 - The third level should be offered in a distributed fashion by the development team. The responsibility of this level is the handling of problems found in the software and/or hardware being used and/or developed.

Based on the requirements presented, the following structure is proposed:

Level 1 : Support Level 1 is the first team to deal with the incidents in the FIBRE-BR system. It acts as a single point of contact (SPOC) for the end user. This level of support should deal with well-known problems, while escalating to Level 2 incidents related to a specific island, and/or to Level 3 incidents that do not have a known resolution and are not related to any particular island. This task is undertaken by RNP and is provided by a centralized team, including two engineers. This level will be operational during Brazilian business hours (8:00 AM to 6:00 PM, Brazil Standard Time). The response time expected should be no more than 1 business day. Support shall be offered in both English and Portuguese. If Level 1 is unable to solve the observed incident, this team will evaluate it and it will be escalated for further levels of support.

Level 2 : Support Level 2 is triggered by Level 1, when it is not able to solve an incident. Level 2 is offered in a distributed fashion, where each island has a team including two engineers, which is responsible for handling the incidents that happen locally. This task is undertaken by the institution responsible for the island, and will be operated during Brazilian business hours (8:00 AM to 6:00 PM). The expected response time should be no more than 2 business days. Support shall be offered in both English and Portuguese. If a particular island is unable to solve the incident, it should be escalated to Level 3 for resolution.

Level 3 : Support Level 3 consists of a development team responsible for fixing software and hardware problems. This kind of support is normally activated by Level 2, but it may be activated by Level 1. Level 3 support is offered in a distributed fashion by the development team, where one specialist per component is allocated. It will be operational during Brazilian business hours (8:00 AM to 6:00 PM). The response time expected should be no more than 3 business days and the team should be staffed by at least two developers. Support shall be offered in both English and Portuguese languages.

The figure below demonstrates the tiered support, representing the responsibilities of each level and how the issue is escalated through the levels.

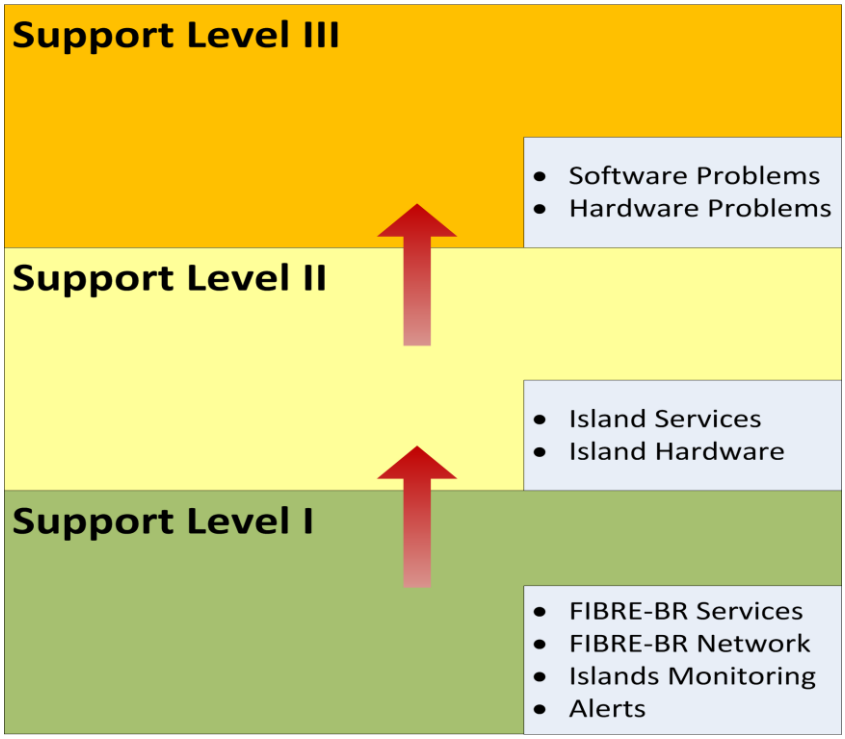
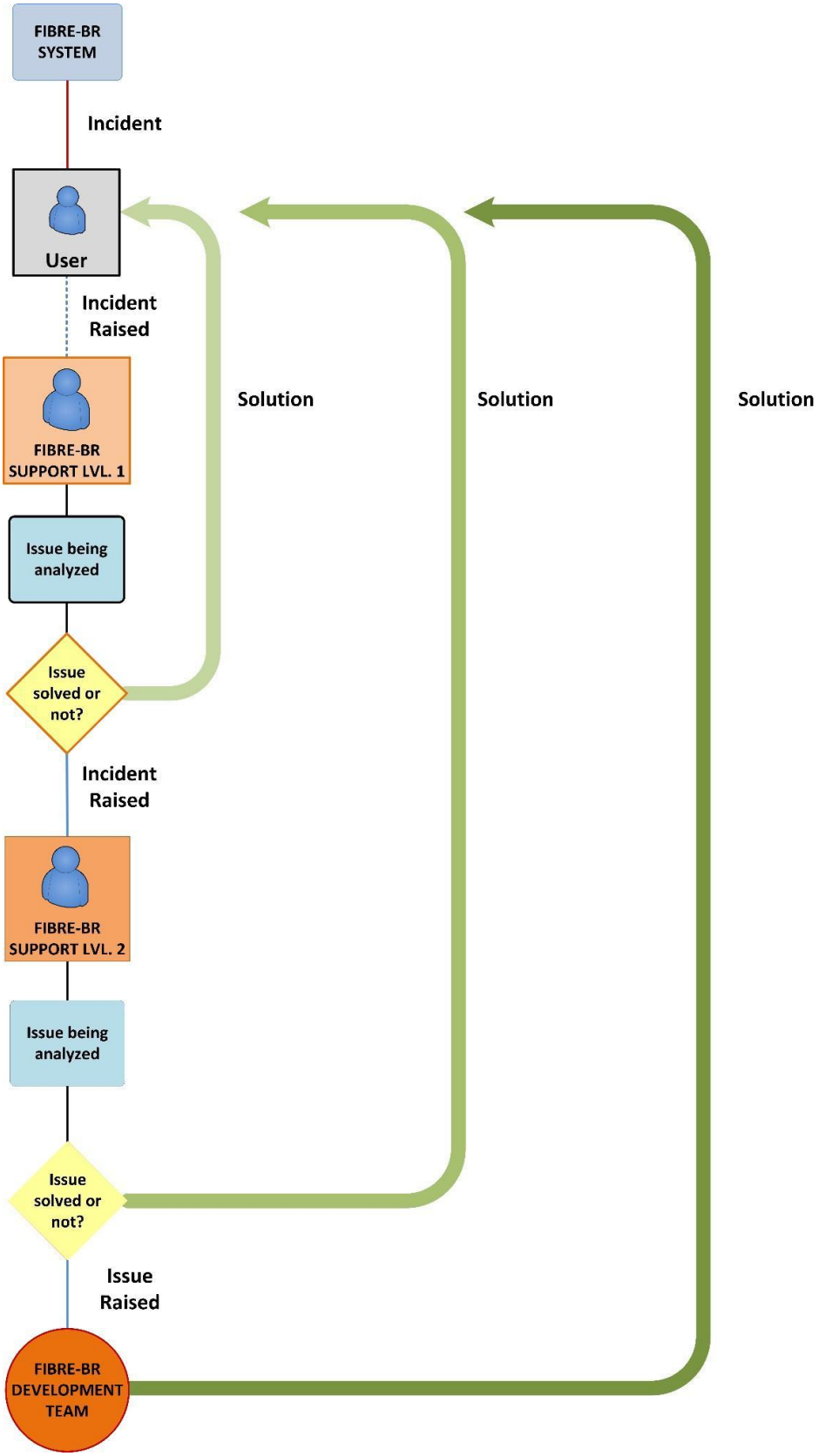


Figure 1 – NOC structure



1.

Figure 2 – NOC levels

Figure 2 gives a graphical description of the tiered support presented and how it works. The FIBRE-BR Support Level 1 is the first level of support that the user will use after have encountered a bug or a failure. In this level the bug/failure will be analyzed and this team will have one business day to solve the issue raised, if the problem is not resolved then, the issue will be escalated to the next level of support.

FIBRE-BR Support Level 2 consists in support teams located in each islands and they have the responsibility to handle the infrastructure problems that happens in their own islands. The issue raised by the Level 1 will be analyzed and this team will have two business days to fix it. If not fixed after two days, the issue will be characterized as a bug and it will be forwarded to Support Level 3.

FIBRE-BR Support Level 3, also known as FIBRE-BR Development Team, is responsible for correcting hardware and software bugs that were escalated by the FIBRE-BR Support Levels 1 and 2. As explained before this support is only activated when Level 2 and 1 are unable to solve the issue.

5 Requirements for the NOC tools

This section will point out what requirements are needed to accomplish complete monitoring of the FIBRE-BR network.

5.1 Ticketing System

[Req MR-01] The FIBRE-BR system MUST use a ticketing system tool as a communication channel to record issues users meet in using the system.

[Req MR-02] The FIBRE-BR ticketing system SHOULD be accessible to users and to different levels of support, and MUST allow a ticket to be assigned to different teams and/or individuals.

[Req MR-03] The FIBRE-BR system MUST be able to send notifications by e-mail and maintain schedules and other timestamps, such as opening and closing times of events. One desirable feature would be the ability to share maintenance calendars of the different islands.

[Req MR-04] The FIBRE-BR system MUST be intuitive to use and user friendly.

[Req MR-05] The FIBRE-BR system SHOULD allow the recording of important events, the definition of workflows and the customisation of forms.

[Req MR-06] Relevant information that SHOULD be recorded in the ticketing system will include:

- Island information: primary and secondary contact, IP and / or IPv6 address ranges;
- User information: name, e-mail, institution, reason to access the FIBRE-BR system islands and application information;
- Events: Incidents, Information Requests and Scheduled Maintenances;

5.2 Monitoring System

[Req MR-07] Every island of the FIBRE-BR network MUST have a monitoring tool, where their services and equipments are monitored.

[Req MR-08] The monitoring tool MUST be able to monitor Xen Virtual Machines.

[Req MR-09] The monitoring tool infrastructure MUST monitor the following metrics for the virtualization server:

- Server uptime
- Disk Usage
- CPU Usage
- Memory Usage

- Process availability
- Network interfaces

[Req MR-10] The monitoring tool infrastructure MUST monitor the following metrics for the island's equipments:

- Server uptime
- Disk Usage
- CPU Usage
- Memory Usage

[Req MR-11] The monitoring tool infrastructure MUST monitor the following metrics for the virtual machines:

- Server uptime
- Disk Usage
- CPU Usage
- Memory Usage
- Process availability (Depends on what kind of services are being offered)
- Network interfaces

[Req MR-12] This monitoring infrastructure SHOULD monitor the following metrics for each network asset (FIBRENet's Top of the Rack and Openflow switches):

- Availability
- Downtime.
- Number of Failures.
- MTTR - Mean Time to Repair.
- MTBF - Mean Time between Failures.
- Downtime for Maintenance.
- Availability (ignoring downtime during scheduled maintenance).

[Req MR-13] A centralized monitoring infrastructure SHOULD maintain monitoring information about all elements of each island and generate a monthly report, to be made available through the project Wiki.

[Req MR-14] The FIBRE-BR's monitoring tool MUST be able to alert the administrator or the island's responsible about the failure of a service using Jabber or e-mail.

5.3 Netork Monitoring System

[Req MR-15] The FIBRE-BR's island MUST have a network monitoring tool.

[Req MR-16] The FIBRE-BR's island MUST monitor the following metrics for the FIBRE-BR's network:

- PING
- Link Usage:
- Bps (Bytes per second)
- PPS (Packets per second)
- RTT (Round-trip time)
- One way delay
- Packet Loss
- Jitter
- Delay

[Req MR-17] The FIBRE-BR System SHOULD have a weathermap tool, so as to monitor the usage of the FIBRE's network per experiment.

5.4 Security System

[Req MR-18] The FIBRE-BR Islands' and the FIBRE-BR's NOC MUST have a security system so as to detect intrusions against the network.

[Req MR-19] The FIBRE-BR's NOC MUST warn the central operator and Island's operator about the network breach.

[Req MR-20] The FIBRE-BR's NOC MUST log all network security incidents.

5.5 Configuration System

[Req MR-21] The FIBRE-BR's NOC MUST monitor the configurations of the FIBRENet equipments (DATACOM and TOR switches).

[Req MR-22] The FIBRE-BR's NOC MUST maintain a history of changes.

[Req MR-23] The FIBRE-BR's NOC SHOULD have a tool for fast deployment of configurations.

6 NOC tools

In this section, a selection of tools is presented that can be applied by the NOC of the FIBRE-BR project. The analysis of tools dealt with the following fields: Ticketing System, Infrastructure Monitoring and Network Monitoring.

6.1 Trouble Ticketing System Tools

Name:	RT: Request Tracker
Website:	http://bestpractical.com/rt/
Requirements:	• **MR-01 - Trouble Ticketing System tool.** • **MR-02 - Accessible to users and to different levels of and allow a ticket to be assigned to different teams and/or individuals.** • **MR-03 - Able to send notifications and maintain schedules and maintain schedules.** • **MR-04 - The system is intuitive to use and user friendly.** • **MR-05 - Allow the definition of workflows and the customisation of forms.** • **MR-06 - Attended by MR-05**
Observations:	Ticketing System with which RNP is familiar.

6.2 Infrastructure Monitoring Tools

Name:	Zenoss Core
Website:	http://community.zenoss.org/index.jspa
Requirements:	• **MR-07 - Monitoring tool.** • **MR-08 - Able to monitor Xen Virtual Machines.** • **MR-09 - Able to monitor the aforementioned metrics for Xen Hypervisor.** • **MR-10 - Able to monitor the aforementioned metrics for the Islands' equipments.** • **MR-11 - Able to monitor the aforementioned metrics for Xen Virtual Machines.** • **MR-12 - Able to monitor the aforementioned metrics for the network assets.** • **MR-13 - This requirement may not be attended.**

	• **MR-14 - Able to send alarms using Jabber procol or E-mail.**
Observations:	Tool adopted in FIBRE-EU.

6.3 Security System Tools

These tools will be defined and deployed in the next stage of the FIBRE-BR NOC development.

Requirements:	• **MR-18 - Requirement not attended.** • **MR-19 - Requirement not attended.** • **MR-20 - Requirement not attended.**

6.4 Configuration Management Tools

Name:	RANCID
Website:	http://www.shrubbery.net/rancid/
Requirements:	• **MR-21 - Configuration tool able to monitor the configuration of the switches.** • **MR-22 - Able too maintain a history of changes.** • **MR-23 - Requirement not attended.**
Observations:	Configuration tool with which RNP is familiar.

6.5 Supporting Tools

Although these tools maybe were not prescribed by the requirements, there might be a need for supporting tools which will help to manage the FIBRE-BR NOC. A list of these tools is listed below:

- NTP Server
  - Reason: Synchronize servers.
- Web Console
  - Reason: Quick and easy access to the servers.
- Log management tools
  - Splunk - http://www.splunk.com
  - Syslog - http://www.balabit.com/network-security/syslog-ng

- Automated deployment of the configuration
  - Reason: Quick deploy of the configuration in the network assets and reinforcement of these configurations.
  - Requirement: MR-23

7 NOC Policy

7.1 Monitoring Policy

The FIBRE-BR NOC is responsible for the monitoring of all the network assets that compose the FIBRE-BR testbed, including virtual machines created for experiments, services provided by the islands, switches used in FIBRENet and the island's equipments (Servers, Orbit Nodes and NetFPGA servers). Nevertheless, it is expected that each island has a monitoring tool to maintain its own equipment.

When dealing with incidents raised by the users NOC Support will evaluate the problem and will forward it to more specialized teams.The international access to European islands will be concentrated at the RNP PoP in São Paulo, where many of RNP's international circuits are connected.

7.2 About the islands' policies

Each island is responsible for its own policy and processes.

8 NOC Processes

In this section the processes used in the NOC will be described. These processes vary from the usage of the Ticketing System to the creation of an experiment in the NOC.

8.1 Ticketing process

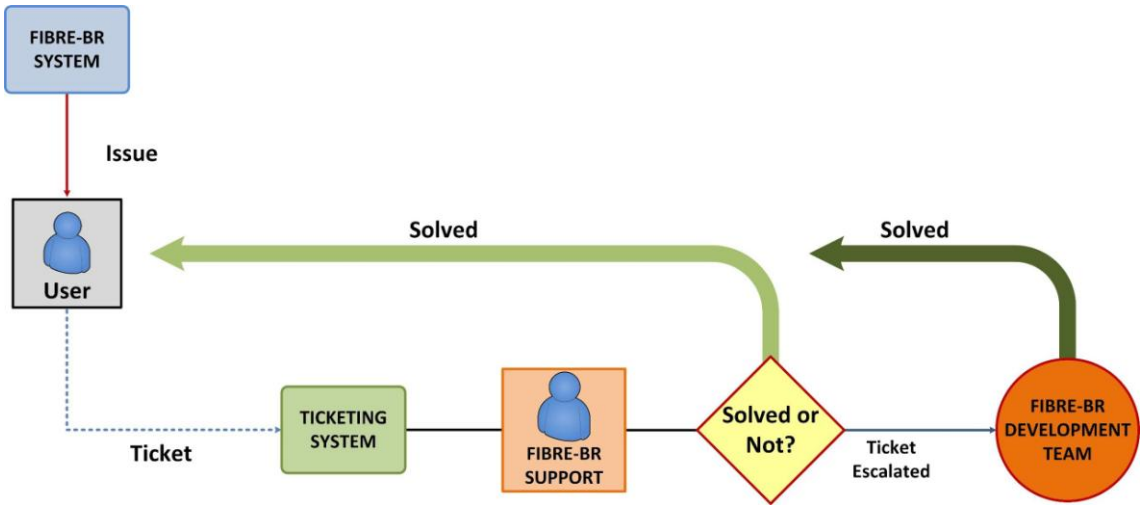


Figure 3 – Ticketing process

Figure 3 shows how the Ticketing System operates. If a a bug or a failure was found in the system, while a user was using the FIBRE-BR system, he/she should report the problem using the Ticketing System. In the Ticketing System, the following fields will be completed:

- Subject
- User information:
  - Name
  - E-mail
  - Instituition
- Problem information:
  - Island where the problem occurred
  - Description of the problem
  - Urgency: Low, Medium and High
  - Reason for the Urgency (Available only for Medium and High urgency)

On receiving this information, FIBRE-BR Support (level 1 and possibly level 2) will evaluate the ticket and will try to solve the issue described. If this is not possible, then the ticket will be escalated to the FIBRE-BR Development Team, where this ticket will be characterised as a bug.

8.2 Monitoring Process

Figure 4 shows how the Monitoring process operates in the FIBRE-BR system. When the Monitoring System perceives that one of the components (services, virtual machines, server and switches) of a certain island changed status, it sends an alarm to the island's administrator, where this alarm can be an email, SMS or a Jabber message. After being notified, the island's administrator will verify what caused the alarm, and if it is a problem he/she will take appropriate measures.

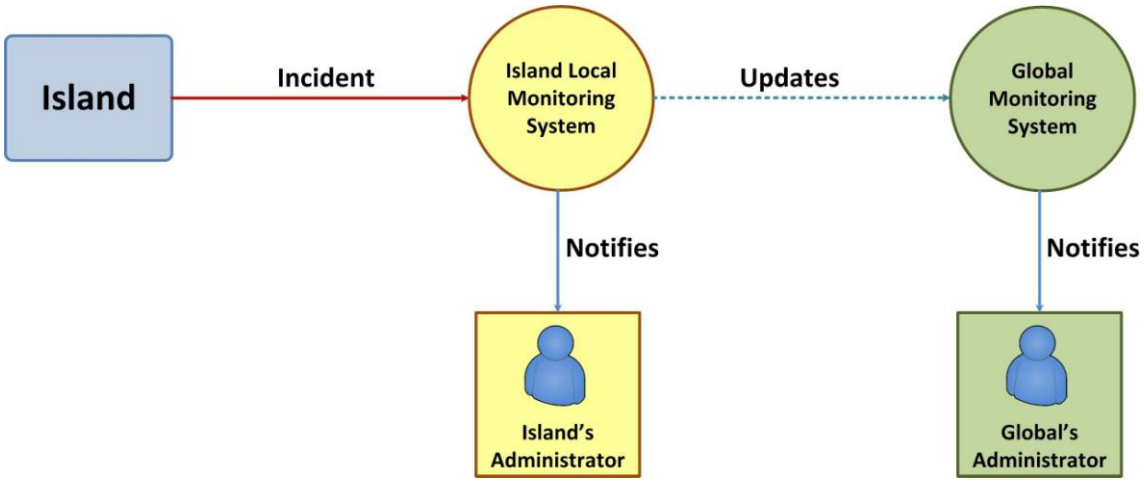


Figure 4 – Monitoring Process

8.3 Authentication

The LDAP directory configured in a FIBRE-BR island should present interoperability between the OMF (Orbit Management Framework), OCF (OFELIA Control Framework) and the CAFe (“Comunidade Acadêmica FEderada”). To do this the LDAP DIT (DIT - Directory Information Tree) must include those attributes which are equivalent in all environments.

Thus, the required attributes for each environment were identified, and a new schema of compatible directories has been proposed.

8.4 Access to the FIBRE-BR Portal - VPN

VPN access is needed for the user be able to use the FIBRE-BR testbed. The certificates needed to access this VPN will be generated by the NOC for authorized users. After that the user will access the VPN using servers deployed in the NOC infrastructure. Figure 5 shows this process.

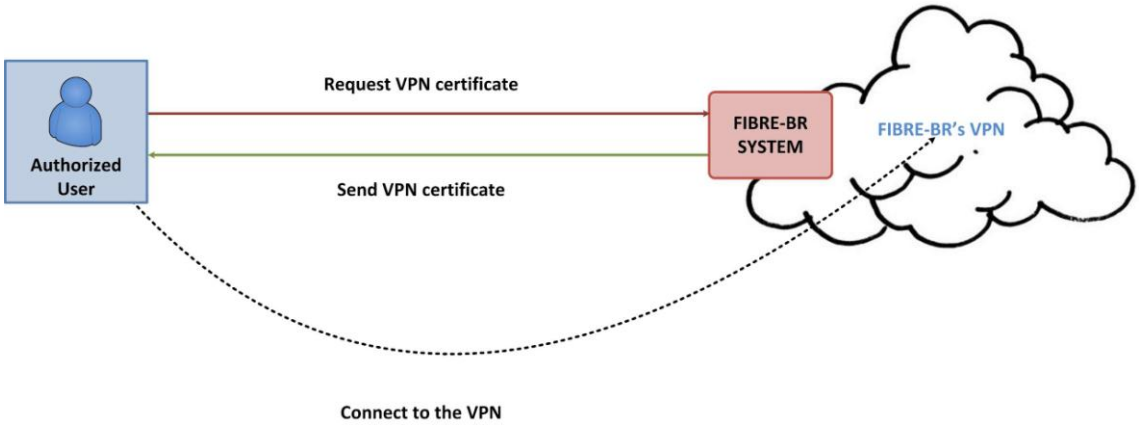


Figure 5 – Access to FIBRE-BR

9 FIBRE-BR Portals

In order to create a single point of access to FIBRE-BR the NOC will deploy the Expedient software and the NITOS scheduler, that provide web interfaces to OCF and OMF respectively.

This is a temporary solution until all islands are federated using the solution under development in WP4.

"*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