

**Federated E-infrastructure Dedicated to European Researchers  
Innovating in Computing network Architectures**

Co-funded by the European Commission within the Seventh Framework Programme. Grant Agreement No. RI-213107

# Deliverable DSA2.1: User Support

## Version 1.0

<b>Dissemination Level</b>	Public
<b>Contractual Date of Delivery</b>	30 November 2008
<b>Actual Date of Delivery</b>	05 March 2010
<b>Editor</b>	B. Rhoads - KTH
<b>Contributors</b>	M. Potts - Martel J. Mohacsi - NIIFI
<b>Reviewers</b>	M. Campanella - GARR

### Abstract

This deliverable DSA2.1: “User Support” describes the “support tools” that are available to users from the initial contact via FEDERICA’s Web based User Portal to request an IP slice, through to the mechanisms to access the created slice. It also includes a summary of the Use Policies with which users must comply.

The deliverable also describes the associated internal operations that follow the approval of the request, in terms of how the support is organised, the tools that are available (for use by the FEDERICA NOC and the user) and the educational material and training courses that are available.

This document was planned to be the first deliverable from the Service Activity SA2, but in practice, it was found to be necessary to first install the infrastructure with the associated management and monitoring services for providing the IP slices (described in deliverable DSA2.2), before issuing information regarding the procedures, tools and services that enable users to access and use the network.

## Executive summary

This document describes the procedures, tools and services to enable users to access and use an IP slice<sup>1</sup> of the FEDERICA network. It is an output of the Service Activity SA2: “Operational User support and tool-bench development”. The main objectives of this Activity are to implement tools for the FEDERICA infrastructure and provide operational support for the users of the virtual network infrastructure. These software tools allow the creation of the specific network topologies, including the associated addressing and routing.

In a next step, it is planned that some of the tools that are currently used by the NOC to manage the FEDERICA infrastructure will be accessible by users to create and configure their own dedicated and customised network IP slice (ie. *User-Controlled Slice Services*).

The Activity SA2 will also deploy an “accounting system”. It is not intended to charge users, but this mechanism can be used to trace and (if necessary) limit the usage of the FEDERICA resources, as a means to ensure fair resource allocation in the event that demand exceeds the available capacity of any of the virtualised resources. Tracing resources in a virtual network environment involves translating monitoring operations of virtual resources into operations on the physical network (virtual resource monitoring).

The Activity SA2 comprises four Tasks:

- TSA2.1: User support during use
- TSA2.2: Prioritization, policies AAI charging and accounting, gathering user feedback
- TSA2.3: Tools for virtual slicing and network provisioning, e2e monitoring, fault management of virtual resources, AAI, interaction of virtual infrastructures
- TSA2.4: User oriented tools for creation and control of virtual infrastructure

Most of the tools development work related to this deliverable is being performed in the Activity **JRA1**: “Network Control and Management” and the Task **TSA2.4**: “User oriented tools for creation and control of virtual infrastructure”.

Other important inputs relating to users come from the Task **TSA2.1**: “User support during use”, Activity **NA2**: “Building and consolidating the User Community”, the **User Policy Board** and Task **TNA4.3**: “Training end-users on the FEDERICA virtual infrastructure and tool-bench”.

The contributions from each of these 6 main areas are summarised below and described in more detail in the corresponding chapters of this report.

### **JRA1: Network Control and Management**

Partners in this JRA have developed a Web-based *User Portal*, which is the first - and main - contact point for FEDERICA users. It is accessible to all standard web-

---

<sup>1</sup> A slice is defined as a network that has been customised to fit the needs of a specific user, and that is running on top of the physical infrastructure, sharing it with other parallel slices.

browsers supporting FEDERICA's security policy. The User Portal is designed to be reachable from the general Internet after appropriate user authentication and authorisation. Its role starts with supplying preliminary information to the potential users and continues with providing guidance on the account and slice creation - and deletion - procedures and implementing the primary interface between the users and the NOC throughout the life of the slice (e.g. supporting change and failure management).

During the design of the FEDERICA User Portal the following basic requirements were taken into account, based on several discussions and UPB recommendations:

- Users can request their own account.
- Users can request a new slice by providing the following information:
  - From when they need to use the slice
  - Until when they need to use the slice
  - Slice description
  - Slice topology
  - Upload Operating System image files to be started on the virtual hosts
- The user is informed whether the requested slice is accepted or rejected
- The user is informed when the slice is configured in the FEDERICA infrastructure and is ready for use
- The user is informed how to access the created slice
- The UPB representative can enable, disable or remove any user's account
- The UPB representative can approve or reject requested slices
- The FEDERICA NOC Administrator can configure user slices.

#### **TSA2.4: User oriented tools for creation and control of virtual infrastructure**

Users need the appropriate tools for the work they want to perform, which may be either (i) to modify - in a controlled way - an allocated virtual slice, or (ii) simply use a FEDERICA slice to do higher layer (application layer) testing.

The ultimate objective of this Task is the implementation of a *User Controlled IP Slice Service*, via which users can create dedicated IP slices where they can build their customised topology and choose their routing schemes and addressing space.

The implementation of the User Controlled IP Slice Service is divided into three phases:

- Phase 1 (complete): The foundation for the slice infrastructure has been installed. This comprises commercial routing equipment with logical routing and switching capabilities provided by Juniper at 4 core PoPs and 10 non-core PoPs.
- Phase 2 (complete): SUN Workstations operating as virtual computing resources (V-Nodes) have been installed in many of the PoPs. These currently run VMWare hardware virtualisation software. The hardware infrastructure from Phases 1 and 2 can be partitioned into several parallel IP slices, each one running its customised suite of experimental protocols.

- Phase 3 (this feature has been tested with one user): The software developed in Phases 1 and 2 has been enhanced with peering capabilities. Using the software developed in this Phase, users can run an external routing protocol between IP slices, or deploy their customised routing protocol.

### **TSA2.1: User support during use**

In order to maintain a high availability of the virtual network, FEDERICA has installed a full-scale NOC function, equipped with “trouble-ticket” systems so that users can report problems and get feedback on progress. Out-of-band communication channels are provided from the NOC to the physical sites.

The implementation of the user support is passing through three Phases:

- Phase 1: M1 - M9 (complete): The virtual network was designed. In this phase, it was important to include the operational requirements when designing the actual virtual network.
- Phase 2: M10 - M21 (almost complete): Installation, configuration, operation and debugging the user support functions. The user VNC access to the V-Nodes is the main outstanding item.
- Phase 3: M22 - M30 (on-going): Implementation of improved tools for liaising with the users (tracking the progress of requests for slices through the process, providing information about the network status, performance monitoring, etc.).

### **NA2: Building and consolidating the User Community**

Part of the role of this Activity is to establish the relationship with users. The target users of the FEDERICA infrastructure are those engaged in research “on” networking; ie. researchers who want to use the network not just for the connectivity, but primarily as the “subject” of their work. User groups include other EC projects, research groups in universities or research centres, equipment manufacturers and telecommunications research labs or even individuals (eg. PhD students).

The Activity NA2 began with 2 parallel work items:

- Collecting user requirements (to forward to SA2 for implementing the supporting tools). A deliverable (DNA2.1) reporting on a set of initial user requirements was produced in March 2008, and DNA2.2: “FEDERICA User Community and Requirements” was produced in March 2009
- Defining the policy for the usage of the network (to ensure that the network is not used for commercial purposes). A User Policy Board (UPB) was set up and the basic UPB procedures have been defined. The UPB has created a set of documents that are needed to establish the administrative contact between the potential users and FEDERICA, as well as to efficiently deal with the users’ requests, collect feedback, etc.

### **The User Policy Board**

The underlying philosophy of the project is that usage should be as open as possible and free of charge. However, being based upon a publicly-funded network

infrastructure means that there are some policies, with which users have to comply. The key requirement is that the use must be for non-commercial purposes.

The UPB has written the following set of documents, which are available from the User Information Pack area of the project website: [http://www.fp7-federica.eu/users/user\\_pack.php](http://www.fp7-federica.eu/users/user_pack.php). The contents are summarised in chapter 6.

- Documents for information:
  - D2-FEDERICA-Basic-User-Information
  - D3-FEDERICA-Access-Rules
  - D4-FEDERICA-Acceptable-Use-Policy (AUP)
  - D5-FEDERICA-Resource-Description
- Documents for response or interaction:
  - D6-FEDERICA-Memorandum-of-Understanding (MoU)
  - D7-FEDERICA-Project-Plan
  - D8-FEDERICA-User-Feedback

#### **Task TNA4.3: Training end-users on the FEDERICA virtual infrastructure and tool-bench**

Support is also given to users through the “tool” of training. FEDERICA will transfer technical knowledge produced in the project to network engineers and users of the FEDERICA infrastructure, by means of training and dissemination activities, including tutorials and demonstration labs. The training will be supported by technical presentations, as well as by course material produced by the members of TNA4.3.

Handouts will be provided to the trainees, plus, when relevant existing white papers, cookbooks and CD images.

At least two training events will be organised per year, each targeting about 10-15 participants.

## Table of Contents

<b>Executive summary.....</b>	<b>2</b>
<b>1 Introduction.....</b>	<b>7</b>
1.1 Purpose and scope.....	8
1.2 Document overview .....	9
<b>2 The FEDERICA User Portal (from JRA1) .....</b>	<b>10</b>
2.1 FEDERICA User Portal Architecture .....	10
2.2 Accessing the Portal.....	11
2.3 FEDERICA User Portal Modules .....	12
2.3.1 User Database .....	12
2.3.2 Slice Information Database.....	12
2.3.3 Slice Files Repository .....	12
<b>3 User oriented tools for creation and control of virtual infrastructure (from TSA2.4) .....</b>	<b>13</b>
3.1 Accessing virtual resources.....	13
<b>4 User Support during the use of FEDERICA (from TSA2.1).....</b>	<b>16</b>
<b>5 Building and consolidating the User Community (from NA2) .....</b>	<b>17</b>
<b>6 The User Policy Board.....</b>	<b>18</b>
6.1 D2-FEDERICA-Basic-User-Information .....	18
6.2 D3-FEDERICA-Access-Rules.....	19
6.3 D4-FEDERICA-Acceptable-Use-Policy (AUP).....	19
6.4 D5-FEDERICA-Resource-Description.....	21
6.5 D6-FEDERICA-Memorandum-of-Understanding (MoU) .....	22
6.6 D7-FEDERICA-Project-Plan.....	23
6.7 D8-FEDERICA-User-Feedback .....	26
<b>7 Training end-users on the FEDERICA virtual infrastructure and tool-bench .....</b>	<b>28</b>
<b>8 Conclusions.....</b>	<b>30</b>

## 1 Introduction

FEDERICA is a 30-month EC 7th Framework project to implement a versatile experimental network infrastructure for trialling new networking technologies. This infrastructure is intended to be agnostic in respect of the types of protocols, services and applications that may be trialled, whilst allowing disruptive experiments to be undertaken. The aim is to develop mechanisms that will allow such experiments to be run over existing production networks such as GÉANT and National Research and Education Networks (NRENs) without adverse effect.

The FEDERICA project provides a virtual infrastructure dedicated to network researchers with different profiles. This means that users can make experiments with various types of protocols, including data and control plane-related protocols. It is also possible that some of these experiments challenge the whole structure of the traditional OSI layer of network stack protocols. However, FEDERICA follows a layered approach concept, built upon the virtualisation of Layer 2 and Layer 3 networks.

This deliverable has been produced by the Service Activity SA2 (Operational User support and tool-bench development).

The main objectives of this Activity are to develop tools for the FEDERICA infrastructure and provide operational support for the user of the virtual network infrastructure.

The tools will be used to manage the FEDERICA infrastructure and may let eventually the users create and configure their own dedicated and customised network slice (a *User-Controlled Slice Service*). A slice is defined as a network that has been customised to fit the needs of a specific user, and that is running on top of the physical infrastructure, sharing it with other parallel slices. These software tools will allow to create the specific network topologies, including addressing and routing.

To create this service, a tool from the project MANTICORE is being enhanced to offer the facility to create and manage Juniper logical routers.

Two Phases have been defined:

- Phase 1 will provide logical routing management capabilities
- Phase 2 will provide computer virtualisation capabilities with the objective to create and manage software routers. This will make possible the managing of a server with some virtualisation platform installed; creating and managing virtual machines and resources. A software router will be a virtual machine with an Operating System and some routing software installed that makes it behave as a router.

SA2 will also elaborate the policies and the architectures for prioritisation, and deploy a global “accounting system”. It is not intended to charge users, but this mechanism can be used to trace and (if necessary) limit the usage of the FEDERICA resources, as a means to ensure fair resource allocation in the event that demand exceeds the available capacity of any of the virtualised resources. Tracing resources in a virtual

network environment involves translating monitoring operations of virtual resources into operations on the physical network (virtual resource monitoring).

Finally, SA2 will provide an active user support system (NOC) that ensures that the network is operational and provides help for researchers performing experiments. This support activity will itself use the tools developed in the work-package for monitoring and management.

The SA2 Activity comprises 4 Tasks:

TSA2.1: User support during use

TSA2.2: Prioritization, policies AAI charging and accounting, gathering user feedback

TSA2.3: Tools for virtual slicing and network provisioning, e2e monitoring, fault management of virtual resources, AAI, interaction of virtual infrastructures

TSA2.4: User oriented tools for creation and control of virtual infrastructure

Most of the tools development work related to this deliverable is being performed in the Activity **JRA1**: “Network Control and Management” and the Task **TSA2.4**: “User oriented tools for creation and control of virtual infrastructure”.

Other important inputs relating to users come from the Task **TSA2.1**: “User support during use”, Activity **NA2**: “Building and consolidating the User Community”, the **User Policy Board** and Task **TNA4.3**: “Training end-users on the FEDERICA virtual infrastructure and tool-bench”.

The contributions from each of these 6 main areas are described in more detail in the corresponding chapters of this report.

### 1.1 Purpose and scope

This deliverable describes the “support tools” that are available to users from the initial contact via FEDERICA’s Web based User Portal to request an IP slice<sup>2</sup>, through to the mechanisms to access and use the created slice. It is an output of the Service Activity SA2: “Operational User support and tool-bench development”. The main objectives of this Activity are to implement tools for the FEDERICA infrastructure and provide operational support for the users of the virtual network infrastructure. These software tools allow the creation of the specific network topologies, including the associated addressing and routing.

In a next step, it is planned that some of the tools that are currently used by the NOC to manage the FEDERICA infrastructure will be accessible by the users to create and configure their own dedicated and customised network IP slice (ie. *User-Controlled Slice Services*).

---

<sup>2</sup> A slice is defined as a network that has been customised to fit the needs of a specific user, and that is running on top of the physical infrastructure, sharing it with other parallel slices

## 1.2 Document overview

This document was planned to be the first deliverable from the Service Activity SA2, but in practice, it was found to be necessary to first install the infrastructure with the associated management and monitoring services for providing the IP slices (described in deliverable DSA2.2), before issuing information regarding the procedures, tools and services that enable users to access and use the network.

This document contains information regarding:

- How to interface with FEDERICA to request an IP slice
- The FEDERICA support
- The tools that are available (both to the FEDERICA NOC and the user)
- The educational material that is available for the user
- The Usage Policies.

It is structured as follows:

Chapter 1, entitled “Introduction”, is a short introduction describing the background, purpose and structure of this deliverable.

Chapter 2, entitled “The FEDERICA User Portal”, describes the Web-based *User Portal*, developed by TJRA1, which is the first - and main - contact point for FEDERICA users.

Chapter 3, entitled “User oriented tools for creation and control of virtual infrastructure”, describes the work in TSA2.4 towards the development of tools to either (i) modify - in a controlled way - an allocated virtual slice, or (ii) simply use a FEDERICA slice to do higher layer (application layer) testing.

Chapter 4, entitled “User Support during the use of FEDERICA”, the full-scale NOC function operated by TSA2.1 is described. This is equipped with “trouble-ticket” systems so that users can report problems and get feedback on progress. Out-of-band communication channels are provided from the NOC to the physical sites.

Chapter 5, entitled “Building and consolidating the User Community”, describes the role of the Activity NA2 in establishing and maintaining the relationship with users. The target users of the FEDERICA infrastructure are those engaged in research “on” networking; ie. researchers who want to use the network not just for the connectivity, but primarily as the “subject” of their work. However, user groups also include other EC projects, research groups in universities or research centres, equipment manufacturers and telecommunications research labs or even individuals (eg. PhD students).

Chapter 6, entitled “The User Policy Board”, explains the policies, with which users have to comply. The project aims to be as open as possible; the key requirement is that the use must be for non-commercial purposes.

Chapter 7, entitled “Training end-users on the FEDERICA virtual infrastructure and tool-bench”, describes the dissemination activities, tutorials, training course material and demonstration labs that users can take advantage of.

Finally, Chapter 8, entitled “Conclusions”, concludes the document.

## 2 The FEDERICA User Portal (from JRA1)

The FEDERICA User Portal is a web-based user support interface designed to be the main contact point for FEDERICA end-users. It is accessible from all standard web-browsers supporting FEDERICA's security policy. The Portal is designed to be reachable from the general Internet after appropriate user authentication and authorisation. Portal software should be deployed at each User Access Server (currently there is one instance at the PSNC PoP). Its role starts with supplying preliminary information to the potential users and continues with providing guidance on the account and slice creation and deletion procedures and implementing the primary interface between the end-users and the NOC throughout the life of the slice (e.g. supporting change and failure management).

During the design of the FEDERICA User Portal the following basic requirements were taken into account from several discussions and UPB recommendations:

- Users can request their own account
- Users can request a new slice by providing the following information:
  - From when they need to use the slice
  - Until when they need to use the slice
  - Slice description
  - Slice topology
  - Upload Operating System image files to be started on the virtual hosts
- The user is informed whether the requested slice is accepted or rejected
- The user is informed when the slice is configured in the FEDERICA Infrastructure and is ready for use
- The user is informed how to access the created slice
- The UPB representative can enable, disable or remove any user's account
- The UPB representative can approve or reject requested slices
- The FEDERICA NOC Administrator can configure user slices

### 2.1 FEDERICA User Portal Architecture

The figure below shows the architecture of the FEDERICA User Portal:

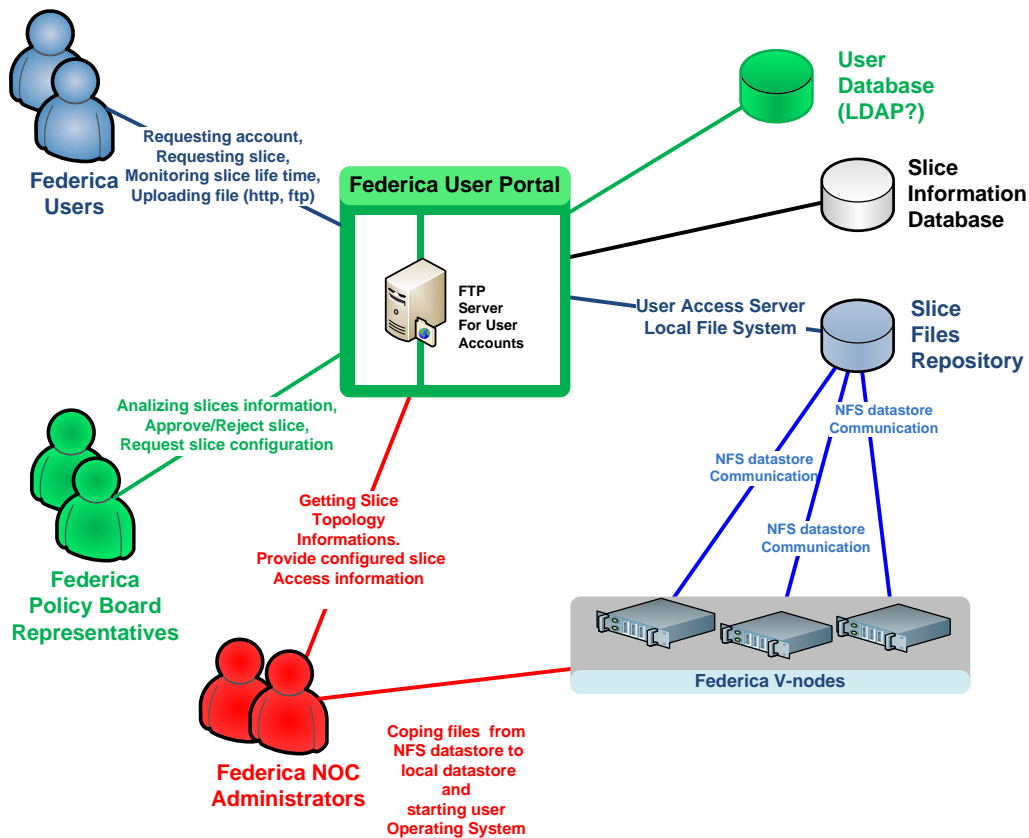


Figure 1: Architecture of the FEDERICA Web Portal

## 2.2 Accessing the Portal

Access to the FEDERICA User Portal is restricted to authorised users. Each user is identified in the system by its own account. This account provides information about personal data and specifies system privileges. It allows a user to log in by typing his user name and password. After login in the user can perform new actions and view history of performed ones. The list of possible actions depends on the user type. In the first version of the FEDERICA User Portal three kinds of users are envisaged:

- FEDERICA User** – The FEDERICA User is the end-user of the FEDERICA Infrastructure. Each potential FEDERICA User who wishes to gain access to the FEDERICA User Portal needs to send a registration request. The user then requests the slice and provides all needed information. The user account is enabled after the approval of the User Policy Board Representative. At this stage, the user can upload Operating System images, etc. and start to use the created slice for experiments. The slice access information is also provided to the user through the FEDERICA User Portal.
- FEDERICA User Policy Board Representative** – The FEDERICA User Policy Board Representative is a member of the UPB who has been designated to this user. The UPB as a whole decides whether to approve or reject the requested slices and initiates the slice configuration at the NOC or (in the future) at the automated slice management system. This group verifies the provided slice

information and assures that creating the new slice will not have any negative effect on the performance of existing slices. The specific User Policy Board Representative is authorised to enable or disable user accounts.

- **FEDERICA Network Operating Centre Administrator** – The FEDERICA NOC Administrator is responsible for creating slices based on the FEDERICA substrate. He allocates the necessary resources and copies the installation images provided by the user from the central Network File System database to the local database of the V-Node. Then the NOC Administrator switches on the virtual hosts and starts installing the Operating Systems. After finishing the configuration process, the NOC Administrator provides the required details to the user so that he/she can start using the newly created slice.

### 2.3 FEDERICA User Portal Modules

#### 2.3.1 User Database

The User Database stores the credentials for the authentication and authorisation of FEDERICA User Portal. The same credential store is also used by the ftp server which is provided to receive the Operating System installation images from the users. Currently, the user database is handled by a relational database management system. An LDAP directory system is under consideration for the upcoming implementation of the credential store.

#### 2.3.2 Slice Information Database

The Slice Information Database stores all information related with a slice. ie.:

- The time when the slice should start.
- The time when the slice should end.
- A short description of the slice.
- Slice topology information. Currently, the user provides an image of the topology and the number of needed resources. In the next stage, the user should use some Java script or Java applet to create the topology diagram in a standardised format that can be mapped onto the FEDERICA infrastructure.
- Slice files (eg. Operating System images).
- Configuration and slice accessibility information.

#### 2.3.3 Slice Files Repository

The Slice Files Repository module allows to store the files associated with the slices and to act as a server from where they can be downloaded to the V-Nodes. Users can upload their files using either an http or ftp upload facility via the FEDERICA User Portal. The uploaded files are reached by the V-Nodes through a Linux Network File System. Each V-Node has an NFS repository configured to access files from the Slice Files Repository. During slice configuration, the NOC Administrator needs to copy files from the remote NFS database to the local NFS database. After this process, the Operating System image provided by the user will boot up on the virtual host.

### 3 User oriented tools for creation and control of virtual infrastructure (from TSA2.4)

Users need the appropriate tools for the work they want to perform, which may be either (i) to modify - in a controlled way - an allocated virtual slice, or (ii) simply use a FEDERICA slice to do higher layer (application layer) testing.

The ultimate objective of this Task is the implementation of a *User Controlled IP Slice Service*, via which users can create dedicated IP slices where they can build their customised topology and choose their routing schemes and addressing space.

The implementation of the User Controlled IP Slice Service is divided into three phases:

- Phase 1 (complete): The foundation for the slice infrastructure has been installed. This comprises commercial routing equipment with logical routing and switching capabilities provided by Juniper at 4 core PoPs and 10 non-core PoPs.
- Phase 2 (complete): SUN Workstations operating as virtual computing resources (V-Nodes) have been installed in many of the PoPs. These currently run VMWare hardware virtualisation software. The hardware infrastructure from Phases 1 and 2 can be partitioned into several parallel IP slices, each one running its customised suite of experimental protocols.
- Phase 3 (this feature has been tested with one user): The software developed in Phases 1 and 2 has been enhanced with peering capabilities. Using the software developed in this Phase, users can run an external routing protocol between IP slices, or deploy their customised routing protocol.

#### 3.1 Accessing virtual resources

End-users need to access the virtual hosts and virtual routers residing in their allocated slice. These virtual resources are located in a logically and physically separate private network, which is not part of the global Internet. A gateway mechanism is needed to provide controlled entry to the slice.

To manage the virtual devices all virtual hosts and virtual routers have a management (virtual) interface. The management interfaces are connected by means of an Ethernet VLAN, called the *Service LAN*. To make the Service LAN accessible from the Internet, a virtual host is created for each Service LAN on the User Access Server. This user access virtual machine has two interfaces: one is connected to the Internet the other is connected to the Service LAN. The only functions provided by the user access virtual machines are SSH Server and SSH Client.

End-users login to their respective user access virtual machine using SSH, with the username and password given to them as part of the registration process described in chapter 2. Then, through the Service LAN, they open a new SSH session from the user access virtual machine to the virtual hosts and virtual routers in their slice. The user access virtual machine runs a linux Operating System with a fixed configuration installed by the NOC.

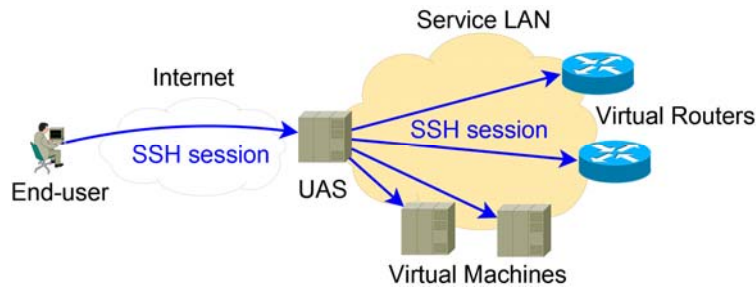


Figure 2 Service LAN and SSH access

To access the virtual hosts and routers in his slice, the user therefore needs an SSH client on his own PC and the following information:

- **Username/password** – created and provided by the NOC Administrator, through the FEDERICA User Portal.
- **Internet reachable IP address of the user access virtual machine** – configured and provided by the NOC Administrator, through the FEDERICA User Portal.
- **Service LAN IP addresses of the virtual hosts** – during the slice design/creation the NOC Administrator allocates a private IP subnet for the Service LAN and gives the details to the user. The user creates the detailed addressing plan for the Service LAN and gives this to the NOC. The NOC configures the virtual resources based on this plan. The NOC also configures a local DNS service (dnsmasq) on the user access virtual machine, which maps IP addresses to the names of the slice's resources. In this way, name-based identification is possible (and preferred).
- **Usernames/passwords of the virtual hosts** – The FEDERICA NOC Administrator installs and configures the Operating Systems on the virtual hosts based on the installation instructions provided by the user. The installation instructions must include the usernames and passwords needed for this configuration.

The fact that the user can access the virtual hosts only through the SSH service, implies that a working Operating System must be present on the virtual host when the user first logs onto the virtual host. This also means that the user cannot install the Operating System on his/her own (not at the first stage of FEDERICA, at least). Therefore, along with the Operating System install image, the user has to provide detailed Operating System installation instructions to the FEDERICA NOC.

More technical details of the (MANTICORE) software that is used to create and manage slices can be found in the deliverable DSA2.2: "IP slice service prototype". The following use case scenarios are described in that document:

- Create a virtual machine
- Copy a virtual machine
- Power On/Off a virtual machine
- Add virtual hardware to a virtual machine
- Modify virtual machine virtual hardware configuration

- Configure Logical Router
- Configure end-interfaces
- Configure internal routing
- Configure external routing

In the later stages of FEDERICA, a virtual console connection to virtual hosts will also be provided for the users.

## 4 User Support during the use of FEDERICA (from TSA2.1)

In order to maintain a high availability of the virtual network, a full-scale NOC has been established within TSA2.1. This chapter describes the NOC functions. Most aspects of operational support for the FEDERICA virtual network with virtual PoPs are equivalent to the case of a physical network setup. For example, the FEDERICA NOC is equipped with “ticket systems” so that users can report problems and get feedback on progress, and staff that are available and educated in the virtual network architecture. Out-of-band communication channels are also provided to the physical sites.

The implementation of the user support is passing through three Phases:

- Phase 1: M1 - M9 (complete): The virtual network was designed. In this phase, it was important to include the operational requirements when designing the actual virtual network.
- Phase 2: M10 - M21 (almost complete): Installation, configuration, operation and debugging the user support functions. The user VNC access to the V-Nodes is the main outstanding item.
- Phase 3: M22 - M30 (on-going): Implementation of improved tools for liaising with the users (tracking the progress of requests for slices through the process, providing information about the network status, performance monitoring, etc.).

Initially, it was important to consider the operational requirements when designing the virtual network, so synchronisation with the network design was necessary. The role of the user support was, to a large extent, educational (see also chapter 7), ie. helping the researchers to get their environment operational.

The second phase was associated with debugging the physical network and fixing operational errors.

The project is now in the last phase, where the user support from the NOC is more related to setting up the slices, monitoring, and liaising with the users. In parallel, new tools and services (eg. AAA, monitoring and management at all levels, automated slice provisioning and configuration, etc.) from the other Tasks in SA2 and the JRAs are being introduced.

## **5 Building and consolidating the User Community (from NA2)**

Part of the role of this Activity is to establish personal relationships with users. The target users of the FEDERICA infrastructure are those engaged in research “on” networking; ie. researchers who want to use the network not just for the connectivity, but primarily as the “subject’ of their work. User groups include other EC projects, research groups in universities or research centres, equipment manufacturers and telecommunications research labs or even individuals (eg. PhD students).

The Activity NA2 began with 2 parallel work items:

- Identifying potential users (from the FEDERICA community, other EC projects, research centres and individual researchers) and collecting their requirements (to forward to SA2 for implementing the supporting tools). A deliverable (DNA2.1) reporting on a set of initial user requirements was produced in March 2008, and DNA2.2: “FEDERICA User Community and Requirements” was produced in March 2009.
- Defining the policy for the usage of the network (to ensure that the network is not used for commercial purposes). A User Policy Board (UPB) was set up and the basic UPB procedures have been defined. The UPB has created a set of documents that are needed to establish the administrative contact between the potential users and FEDERICA, as well as to efficiently deal with the users’ requests, collect feedback, etc. The work of the UPB is described separately in the following chapter.

A useful component of deliverable DNA2.1 was a “User Information Pack”, which gave an introduction to the FEDERICA infrastructure and what it offers to users. This has since been developed by the UPB members into 7 self-contained documents (see chapter 6 below) that are available from the FEDERICA Homepage.

An annex was appended to the deliverable DNA2.1 to collect user requirements and to give users information about the procedure for requesting a slice. However, these forms have now been superseded by the on-line User Portal

## 6 The User Policy Board

The underlying philosophy of the project is that usage should be as open as possible and free of charge. However, being based upon a publicly-funded network infrastructure means that there are some policies, with which users have to comply. The key requirement is that the use must be for non-commercial purposes.

The UPB has written the following set of 7 self-contained documents, which are available from the User Information Pack area of the project website: [http://www.fp7-federica.eu/users/user\\_pack.php](http://www.fp7-federica.eu/users/user_pack.php).

- Documents for information:
  - D2-FEDERICA-Basic-User-Information
  - D3-FEDERICA-Access-Rules
  - D4-FEDERICA-Acceptable-Use-Policy (AUP)
  - D5-FEDERICA-Resource-Description
- Documents for response or interaction:
  - D6-FEDERICA-Memorandum-of-Understanding (MoU)
  - D7-FEDERICA-Project-Plan
  - D8-FEDERICA-User-Feedback

A brief summary of each document is given below:

### 6.1 D2-FEDERICA-Basic-User-Information

Document D2 first gives an introduction to FEDERICA, explaining how it is based on GEANT links and PoPs, but provides virtual ‘slices’ in which users can perform their own experiments, without impacting on users working in other ‘slices’. It identifies the types of organisations and individuals who are expected to use the facilities, and some typical use cases (eg. experiments on networked application, or on new routing protocols).

The services that FEDERICA offers to users are summarised in this document as:

- The possibility to request a virtual infrastructure composed by a combination of circuits (up to 1Gb) and virtual machines (V-Nodes). The default Operating System on the V-Nodes is Linux, and this is the Operating System installed as a ‘placeholder’ until a user supplies his/her ‘image’.
- The slice can contain: routed IP circuits and/or system(s) and/or routers. An optional routed connection to the general Internet is also possible.
- The slice can be a set of L2 circuits and system images (no IP configuration, just Ethernet framing). The GN2+ service provides native 1GbE circuits for FEDERICA. These can be slices using either VLAN technology or MPLS L2 LSPs. In both cases the framing remains Ethernet. (SDH and other transport technologies are out of scope in the first phase of FEDERICA).

- Circuits may have capacity assurances on request. The options for providing capacity assurances are:
  - Dedicated 1 GbE link
  - Up to 4 classes (users) per interface with guaranteed capacity using 802.1p
  - Premium IP (3 classes, but with known capacity patterns so no packet loss can be assured)
  - Characteristics of 2 Line Cards in the Juniper MX240 (Q type) which have up to 4K shapers (this option is only available on the Juniper routers)
- Some basic monitoring of the network and system behaviour in each the slice is provided. The data can be exported raw, or displayed on the web-based User Portal.
- The user will initially access the network and system using SSH.
- The circuits provided should be seen as untouchable pipes. The user can play ‘inside’ his pipes as much as he likes. In that case he/she has to instantiate a virtual node that plays the role of a router or switch (eg. in some cases it is possible to configure logical routers in the Juniper physical routers and provide the user full access to them).

The sequence of events from requesting a ‘slice’ to gaining access to it and uploading software onto the V-Nodes is then described.

## **6.2 D3-FEDERICA-Access-Rules**

This document provides rules and guidelines to be followed by applicants to request access to the FEDERICA infrastructure as well as the criteria that are applied by the UPB, in order to evaluate and prioritise the requests.

The list of documents to be exchanged is identified in this document as:

- Memorandum of Understanding (D6)
- Acceptable User Policy (D4)
- Project Plan (D7)

It is mentioned that the infrastructure is available (normally free of charge) to both the academic and private sector, but that it is not a commercial service and there are a limited amount of resources available (manpower, time, virtual links, nodes, etc.).

It is also mentioned that FEDERICA expects to receive feedback on whatever is non-confidential regarding the experiments that were performed, in terms of the results and also how the user perceived the efficiency of the FEDERICA procedures.

## **6.3 D4-FEDERICA-Acceptable-Use-Policy (AUP)**

The underlying philosophy of granting access to the FEDERICA infrastructure is that usage should be as open as possible and free of charge. However, being based upon the publicly-funded network infrastructure of GEANT means that essentially the same compliance policies have to be applied also for FEDERICA users. The key requirements are:

- FEDERICA may be used to create a ‘slice’ for experimental research, and to connect other resources which are reachable via interworking agreements operated by FEDERICA partners.
- The use of internal, existing FEDERICA resources inside the ‘slice’ is “for free”. Interconnection to external resources using the IP best effort service through the FEDERICA peering is also possible at no cost. Physical interconnection requests that have special requirements may be satisfied according to the real cost. Any provision of service must be authorised in advance.
- FEDERICA may **not** be used for any of the following:
  - the creation or transmission of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
  - the creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety;
  - the creation or transmission of defamatory material;
  - the transmission of material such that this infringes the copyright of another person;
  - the transmission of unsolicited commercial or advertising material either to other user organisations, or to organisations connected to other networks, save where that material is embedded within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe;
  - deliberate unauthorised access to facilities or services accessible via FEDERICA;
  - deliberate activities with any of the following characteristics:
    - wasting staff effort or networked resources, including time on end systems accessible via FEDERICA and the effort of staff involved in the support of those systems;
    - corrupting or destroying other users’ data;
    - violating the privacy of other users;
    - disrupting the work of other users;
    - using FEDERICA in a way that denies service to other users;
    - continuing to use an item of networking software or hardware after UPB has requested that use cease because it is causing disruption to the correct functioning of FEDERICA;
    - other misuse of FEDERICA or networked resources, such as the introduction of ‘viruses’.
  - any breach of industry good practice, or of the Acceptable Use Policies of other networks, that is likely to damage the reputation of the FEDERICA network.
- It is also not permitted to provide access to FEDERICA for third parties without the prior agreement of the UPB.

#### 6.4 D5-FEDERICA-Resource-Description

This document provides a set of definitions for the resources available within FEDERICA at Layer 2, which a user can request. These are:

- **Virtual Infrastructure (VI):**  
A VI is a specific set of Virtual Resources with selected control capabilities. The user can request a VI consisting of selected resources and the capabilities it should offer.
- **Virtual Resource (VR):**  
A VR is an abstraction of a physical network resource which forms part of the Virtual Infrastructure. From the user's point of view a VR appears to function as a physical resource. A VR can represent a single partition of a physical resource (a 'slice'), or a collection of physical resources (cluster). The following concepts are all examples of VRs: Virtual Links, Virtual Nodes, Virtual Switches, Virtual LANs.

The user can request some Class of Service (CoS) characteristics related to the VRs:

- Bandwidth;
  - Burst size;
  - Priorities;
  - Loss probability;
  - Schedulers;
  - Congestion management mechanisms.
- **Virtual Link (V-Link):**  
A V-Link is an abstraction of one or more physical links, seen by the user as a single link between two VRs. The user can request specific demands to these links, such as bandwidth, loss probability, etc.
  - **Virtual Node (V-Node):**  
A V-Node is one or more partitions of a physical node, which can be seen from the user's point of view as a single network node. In other words, this is a Virtual Machine, with the specified user image.
  - **Virtual Switch (VS):**  
A VS is a partition of a physical switch, which the user can configure and use as if it were a physical switch. From the user's point of view, the VS is seen as a physical switch, offering the same functionalities as a physical switch.
  - **Virtual Local Area Network (VLAN):**  
A VLAN is a specific set of Virtual Resources that can be configured so that they appear to be a single network or domain. A VLAN can be offered as a Virtual Resource, if requested by the user, but can also be implemented as a Virtual Service, when implemented by the user on the offered Virtual Infrastructure. A VLAN is an example of a Virtual Network Service (VNS); ie. a service that can be implemented by the user on top of the Virtual Infrastructure.

## 6.5 D6-FEDERICA-Memorandum-of-Understanding (MoU)

The purpose of having an MoU is to formalise the access and use of the FEDERICA infrastructure by the user. It briefly outlines the access policies, the timeframe and any associated conditions. It represents one of the three key documents that describe the collaboration, namely:

1. The Memorandum of Understanding: This formalises the collaboration, the timeframe and lists the mandatory information to be exchanged;
2. The Acceptable Use Policy: This contains the rules defining the responsibilities of each party, the type of traffic that can be carried, the nature of acceptable experiments, respect of private and confidential information from FEDERICA and/or parallel experiments and taking due care not to intentionally disrupt the infrastructure;
3. The Project Plan: This gives a technical description of the planned use of the FEDERICA infrastructure by the user. It details the resources requested in the 'slice', the connectivity requested across the FEDERICA infrastructure and what experiments will be performed. (See the description of the document D7-FEDERICA-Project-Plan in sub-section 6.6, below).

The MOU comprises:

- A short (12-line) description of FEDERICA.
- A short description of the user organisation (at a similar level of detail to the description of FEDERICA).
- A short description of what the FEDERICA infrastructure will be used for (summarised from the Project Plan document).
- A timeline showing the duration for which the resources will be reserved.
- The user obligations, ie.:
  - to comply with the FEDERICA conditions (in particular the Acceptable Use Policy);
  - to share the results of any experiments performed on both their equipment and FEDERICA, to the extent that the information is anonymous and non-confidential. This may be done, for example, through a workshop, or by giving access to the relevant deliverable or publication in journals. The results - and the methodology for sharing them with FEDERICA - will be described in the *User Feedback* document (see the description of the document D8- FEDERICA-User-Feedback in sub-section 6.7, below);
  - to provide feedback on the use of the infrastructure, using the *User Feedback* document template;
  - to acknowledge the use of FEDERICA in any associated publication or presentation.
- A commitment (from both parties) to keep private any user data, experiment details and results.
- A statement that nothing in the MoU implies any partnership between the parties.

- A statement that each party is responsible for financing its own participation in this collaboration, and that (unless stated here otherwise) no charge is made by FEDERICA for the services and resources (bandwidth, equipment, processing resources and personal support).
- The effective start date of the MoU and its predicted date of termination.
- Signatures of both parties.

### **6.6 D7-FEDERICA-Project-Plan**

This document is intended for the user to describe his/her detailed technical project plan. It should include management information, a description of the planned work and a description of the required and available resources.

This information forms the basis for the FEDERICA UPB to assess the eligibility and feasibility of the access to FEDERICA.

The information required is:

- Name and locations of the participating institutions and the contact details of the involved persons (name, phone, e-mail), indicating the person who is overall responsible for the project.
- Planned starting time and duration of the project.
- Project description (1-2 pages of text).
- Description of the usage scenario (1 page text), including a 'slice' topology map.
- Required connectivity to third parties (outside of FEDERICA), eg. to other test environments. (However, such connectivity to third parties is in the responsibility of the user, who has to provide a plan to establish such connectivity).
- Available resources of the user-project partners.
- Required resources from FEDERICA, eg.:
  - V-Nodes as a computing resource capable of executing a system image and which can be connected to one or more circuits;
  - Virtual IP router functionality provided by the network elements;
  - Point-to-point circuits between the V-Nodes or the network equipment;
  - Access points and bandwidth;
  - The likely network properties and service elements.

The following 3 templates are provided to collect this information:

*Service-related requirements*

(Use a separate table for each requested FEDERICA service)

<b>CATEGORY</b>	<b>PARAMETER</b>	<b>DESCRIPTION</b>	<b>REQUIREMENT</b>
Research on network layers / Transparency	Layer 2	Research on what layer?	[choice]
	Layer 3		
	Layer 4+		
Time of usage	Short (hours)	Typical time of usage?	[value]
	Mid (days)		
	Long (months)		
Type of usage	Off-line	Experiments will be performed in the background or live?	[choice]
	On-line		
Response / Provisioning time	Provisioned	Expected service response time?	[choice]
	Scheduled		
	On-demand		
Level of control	No	Control of the service?	[choice]
	Semi		
	Full		
Level of monitoring / measurement	Off-line reports	Monitoring of the elements and/or traffic?	[choice]
	Interactive debug		
Scalability	Number and size of the network slices	Typical number and size of network slices?	[value]
Reliability / Availability	R/A of the network slices	Expected number of nines?	[value]
Security/ Authentication	Internal risks	Importance of security level?	[Y/N]
	External threats		

*Network-related requirements (Network slices)*

<b>CATEGORY</b>	<b>PARAMETER</b>	<b>DESCRIPTION</b>	<b>REQUIREMENT</b>
Traffic matrix / Connection topology	Point-to-point	Typical usage?	[choice]
	Point-to-multi point		
	Multi point-to-multi point		
Bandwidth	High capacity./ Narrowband	Typical bandwidth?	[value]
QoS level	Best Effort	Level of QoS?	[choice]
	Quality of Service		
Delay		Expected delay?	[value]
Jitter		Expected jitter?	[value]
Loss rate		Expected loss?	[value]
Fairness		Expected fairness?	[value]
Type of IP network	Close network	Are public IP addresses required?	[choice]
	Open network		
Network management	Fault	Importance of network management?	[Y/N]
	Performance		
	Topology		
Traffic management	Bandwidth	Importance of traffic management?	[Y/N]
	CAC		
	Policing		
Accounting		Importance?	[Y/N]
Cost		Importance?	[Y/N]

*Application-related requirements (Virtual Machines/software packages)*

<b>CATEGORY</b>	<b>DESCRIPTION</b>	<b>REQUIREMENT</b>
Processing power	Typical processing power?	[value]
Memory	Typical memory?	[value]
Storage resources	Typical storage?	[value]
Operating Systems	Are you interested in a particular Operating System?	[Y/N]

## 6.7 D8-FEDERICA-User-Feedback

As mentioned in the documents D3-FEDERICA-Access-Rules and D6-FEDERICA-MoU, in exchange for providing its facilities and support, FEDERICA expects to receive feedback from the users regarding the experiments that were performed, in terms of any (non-confidential) results and also how the user perceived the efficiency of the FEDERICA procedures.

This document provides the templates for obtaining the user feedback. There are two sets of questions: *General questions* and *Service-specific questions*.

### 1. General questions

- What do you think about the whole communication process with FEDERICA?  
Please explain further and if possible provide suggestions to improve.

### 2. Service-specific questions

- Were the FEDERICA services up to the expected level/standards?  
If “no”, please explain further and if possible provide suggestions to improve:

- Would you have expected a Service Level Specification?  
If “yes”, for which services? All/Layer1/2/3/applications  
Please explain further and if possible provide suggestions to improve:

Were you able to manage your slice properly?

If “no”, please explain further and if possible provide suggestions to improve:

Was extensive help from FEDERICA needed?

If “yes”, please explain further and if possible provide suggestions to improve:

- Were there gaps in the operational management of the FEDERICA service?  
If “yes”, please explain further and if possible provide suggestions to improve:

- What results of your project were achieved mainly due to FEDERICA service?

- Were the peering arrangements with other slices satisfactory?  
If “no”, please explain further and if possible provide suggestions to improve:

Were the isolation arrangements between other slices satisfactory?

If “no”, please explain further and if possible provide suggestions to improve:

Was the Commodity Internet connectivity satisfactory?

If “no”, please explain further and if possible provide suggestions to improve:

What other services should be provided by FEDERICA?

- Was the physical connectivity towards the FEDERICA service easy to implement?  
If “no”, please explain further and if possible provide suggestions to improve:

## **7 Training end-users on the FEDERICA virtual infrastructure and tool-bench**

Support is also given to users by partners in the Task TNA4.3 through the “tool” of training. FEDERICA is transferring technical knowledge produced in the project to network engineers and users of the FEDERICA infrastructure, by means of training and dissemination activities, including tutorials and demonstration labs. The training is supported by technical presentations, as well as by course material.

FEDERICA organises four main types of events:

1. Dissemination Workshops
2. User community consultation workshops
3. Tool-bench training
4. Dissemination by the NRENs (National Research and Education Networks) within the project, at the national events they organise for their constituencies.

### *Dissemination Workshops*

These are held during each of the annual TERENA Networking Conferences. They are organised as sessions within the conference programme, and are used to present the activities and results of the project, whilst raising awareness of the infrastructure within the research and education community.

### *User Community Workshops*

These are workshops targeted at communities that do not normally participate in activities coordinated by NRENs. These not only aim to raise awareness about the project, but also to gain feedback from users about their experiences.

### *FEDERICA Training Workshops*

Two training workshops have been organised during 2009 and two more will be held in 2010. These are used to transfer technical knowledge to network engineers and users of the FEDERICA infrastructure, based on training course material produced by the project participants.

### *National Research and Education Networking Events*

Most of the NRENs within the project (namely GARR, CESNET, DFN, HEAnet, HUNGARNET, NORDUnet, PSNC, Red.es and SWITCH) organise national events (typically, annually) for their networking communities. They will use these opportunities to raise awareness of the FEDERICA project.

### *Other Events*

Other dissemination is undertaken at EC concertation meetings organised by the Directorates D1 (Network of the Future), F3 (Research Infrastructures) and F4 (Future

Internet Research and Experimentation - FIRE). Dissemination is also being undertaken at relevant networking conferences and seminars held within Europe, and similar events will be attended outside of Europe where this can strengthen collaboration with projects that have similar goals to FEDERICA (e.g. PlanetLab, GENI, AKARI).

The first step in the dissemination/training process was to develop the course curriculum and training material. The training material contained in deliverable DNA4.2: “Course curriculum” is intended to familiarise users with the FEDERICA concepts and components, how to utilise the infrastructure and how to fully exploit the functionality and features. The course structure is comprised of presentation modules which include:

- An introduction to the project.
- An overview of virtual machines and network virtualisation.
- How to connect to FEDERICA and use ‘slices’.
- How authorisation and authentication is handled.
- A practical demonstration of how users can request and manage ‘slices’, whilst offering pointers as to the different types of experiments that can be undertaken.

## 8 Conclusions

This deliverable has collected together, in one document, the tools and procedures that are relevant for potential users of FEDERICA. These can be summarised as:

- the Web-based FEDERICA User Portal, developed by partners in the Task TJRA1, which is the first - and main - contact point for potential users.
- the tools for the creation and control of virtual infrastructure, provided by partners in the Task TSA2.4 for either (i) modifying - in a controlled way - an allocated virtual slice, or (ii) simply using a FEDERICA slice to do higher layer (application layer) testing.
- the support given to users, while they are setting up their 'slice' and/or making their experiments, by the NOC function operated by partners in the Task TSA2.1.
- the mechanisms that have been established for initiating and maintaining relationships with users.
- the role and rules of the User Policy Board" for ensuring that users comply with the conditions imposed (mainly) by GEANT. The project aims to be as open as possible; the key requirement is that the use must be for non-commercial purposes.
- the training that is available for users on the FEDERICA virtual infrastructure and tool-bench, in the form of dissemination activities, tutorials, training course material and demonstration labs.

This document also gives references to where more information can be found on any of the specific aspects identified above.