Communications Networks, Content and Technology
European Commission Directorate General

DG CONNECT

European Union's FP7 Programme
DG Connect
Directorate C: Excellence in Science
Unit C1: e-Infrastructure

Deliverable 4.7

Follow up actions and perspectives

A project of the Seventh Framework Programme (FP7)

This project is funded by the European Commission

A project implemented by RedCLARA

Periodic Progress Report

Periodical Progress Report

ELCIRA Deliverable: D.4.7 – Follow up actions and perspectives

Document Full Name	**Follow up actions and perspectives**
Date	**October, 2014**
Activity	**WP4 (Promoting the deployment of eduroam services)**
Lead Partner	**RNP**
Document status	**Final**
Classification Attribute	**Public**
Document link	

Abstract: This deliverable will describe the achievements of the project aligned to the roadmap developed. The managerial aspects of the activities performed and the foreseen follow-up actions will be discussed with specific regard to the Consortium status and perspectives

A project of the Seventh Framework Programme (FP7)

This project is funded by the European Commission

A project implemented by RedCLARA

COPYRIGHT NOTICE

ELCIRA (Europe Latin America Collaborative e-Infrastructure for Research Activities – Call (part) identifier: FP7-INFRASTRUCTURES-2012-1 – Project number: 313180) is a project co-funded by the European Commission within the Seventh Framework Programme (FP7), Infrastructures (DG Connect, Directorate C: Excellence in Science, Unit C1: e-Infrastructure). ELCIRA began on 1st June 2012 and will run for 24 months.

For more information on ELCIRA, its partners and contributors please see http://elcira.redclara.net

DELIVERABLE ROUTE

	Name	Member/Activity	Date	Responsible
From	Leandro Guimarães	WP4	20/10/2014	RNP
From	José Manuel Macias	WP4		RedIris
From	Tania Altamirano	WP4		RedClara
Revised by	Antônio Carlos Fernandes Nunes	WP4	24/10/2014	RNP
Approved by	Florencio Utreras	RedCLARA/CEO	30/0/2014	RedCLARA

TABLE OF CONTENTS

A project of the Seventh Framework Programme (FP7)

This project is funded by the European Commission

A project implemented by RedCLARA

1.- INTRODUCTION

Figure 1 and Figure 2 compare the eduroam coverage in September 2012 and October 2014.

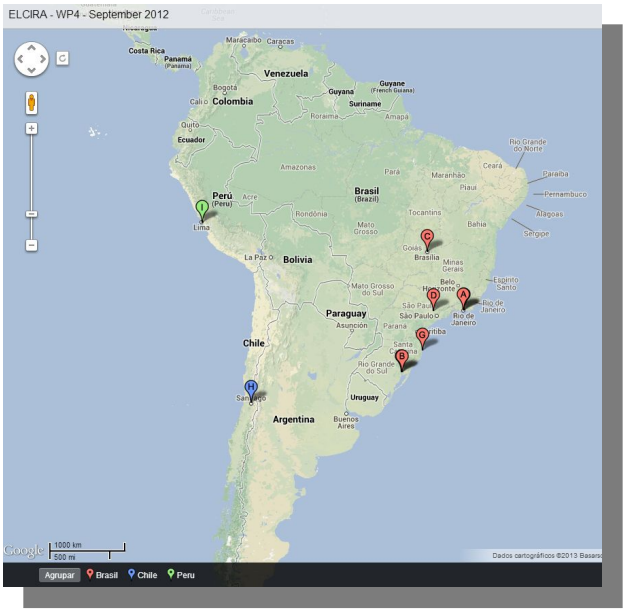

Figure 1: eduroam coverage in September 2012.

Figure 2: eduroam coverage in October 2014.

This shows that with coordination and hardworking is possible to increase mobility level in a short period. For the future, Latin American NRENs will focus on increase the number of hotspot and helping emerging countries to conclude the eduroam adhesion process.

To explain in which services the NRO (National Roaming Operator) will work on it during the following years, it is explained in the next section, all eduroam central services.

2.- DESCRIPTION OF EDUROAM CENTRAL SERVICES

2.1 INTRODUCTION

The operations team eduroam (hereinafter "eduroam OT") is responsible for the operation of a set of core services, such as service monitoring, statistics, or access to the eduroam CAT tool. Apart from these services, there is a database containing information of all members, which is used in some of the above services.

Furthermore, the service provides an eduPKI *public key infrastructure* that implements a trusted profile for obtaining certificates for use in the eduroam infrastructure servers.

2.2 REQUIREMENTS FOR ACCREDITED AS NATIONAL ROAMING OPERATOR (NRO)

The NRO is the organization in charge of adding new members in a country, as well as manage all information relating to such members, sending it to the governance and operations teams of eduroam. It is therefore, as its name suggests, the operator of the eduroam federation in the country.

On the other hand, people define NRO representatives will be responsible for managing all this information, as well as to bridge in any impacts both within the country and internationally.

The institution that wants to run for eduroam operator in a country, you must apply for membership by contacting the team Global eduroam Governance Committee (GeGC), to which must certify compliance with the following requirements:

- The NRO should preferably be academic network (NREN) constituted in the country. If it does not wish to take over the operation, should in any case be delegated to other body representing the country as GSM roaming. If there were an academic network, the first institution to apply could act temporarily as such if their activity was related to the academic and scientific activity.
- THE NRO must sign the eduroam Compliance Statement, through which is committed to monitoring within their country of recommendations and obligations of members in eduroam. These are contained in document eduroam Service Definition.

• The NRO will also be responsible for managing the information in the database of eduroam, and will be describe in the next section. You need this information to be provided acceptance of NRO as such.

• Finally, the NRO will record the eduroam domain in the country (eduroam.TLD). If this is not possible because there is an academic second-level domain, it should be recorded (eg eduroam.ac.TLD or eduroam.edu.TLD). Under that domain should be a page where is reported the characteristics of eduroam in the country, its members and indeed politics.

2.3 DATABASE EDUROAM

The eduroam database feeds XML files, hanging under the web server with information on eduroam in the country (www.eduroam.TLD). These files contain metadata concerning the following aspects:

• **realm.xml**: includes general information about the NRO, such as the contact person and contact address, web site or its link to politics.

• **institution.xml** contains information about the institutions belonging to the initiative in the country, including the locations of these.

• realm_data.xml and realm_usage.xml (*OBSOLETE*) collects information about the use of the domain (roaming within the federation).

• institution_usage.xml (*OBSOLETE*) collects information on the use of eduroam by institutions.

Specifically, the first two files are used mainly by the database and must be provided from the domain of eduroam already registered in a given country. In addition to providing this information, they should be updated regularly, as they constitute the minimum information to be provided on the NRO federation.

The structure of these files is detailed in the specification document database of eduroam.

There is a tool to check the validity (under the scheme) of these XML files.

There is also DjNRO, an application to perform the above tasks, developed by the Greek academic network, GRNET.

Finally, the information provided is also used to show the locations where there eduroam on an application for mobile devices, eduroam Companion, available for iOS and Android platforms.

The eduroam database is used among other things to establish organizations and representatives face to other services such as eduroam CAT or eduPKI.

2.4 ACCESS EDUROAM CAT

eduroam CAT is a tool that allows installers for different platforms, as well as an interface to perform some kind of check from outside your country eduroam federation.

Access to this tool is by invitation, linking acceptance of the invitation to the identity provider-for single-sign-on using the web-user. Such identity provider may be accessible through any eduGAIN or associated with any of the supported social networks.

Figure 3: CAT Webpage.

To request an invitation federation as administrator, you need to contact addresses match those provided to the eduroam database.

Once you have accepted the invitation, the federation administrator will have access to the tool, which provides:

- An interface that allows you to manage IdPs in the federation;
- Administrators can invite your federation IdPs;
- Landings statistics generated installers eduroam CAT;
- Linking the institution with eduroam CAT institution data in the database of eduroam.

Institutions (IdPs) whose administrators have permissions to edit the data in your organization can perform the following operations from eduroam CAT:

- Manage general organizational data (name, logo, address and phone support, certificate configuration and locations of the organization);

• Create one or more profiles, defining the characteristics there of that "overwriting" the general options mentioned and specify concrete, such as the domain or domains or EAP methods supported in the profile and priority data;

• Download installers and / or to publish their profiles, so that users in your organization can download the installers generated;

• Testing connectivity using the information provided in each profile.

The administrator of an IdP may also invite other administrators in your organization and / or revoke permits.

Tests indicated connectivity are also quite powerful, allowing administrators to verify that your organization can be reached from outside the tool itself.

2.5 MONITORING FROM THE CENTRAL SERVICE

The operating eduroam provides a monitoring service that will alert administrators to any incident is detected for the root servers in a country, and for the root domain of that country.

The monitoring is done based on making proxy requests to a specific server, for which the operations team will provide the connection data (IP and shared secret). The idea is that the requests arrive at the same server as the originating, checking that the proxy server is working properly as.

The operation is very simple: two types of requests, one of Accept Reject type and other types, two different ways also be sent: through the eduroam hierarchy, and directly from the allowed IP.

These tests will go through our proxy, and the total time it took to process the request will be measured.

For reference, is presented below an example of this configuration for a FreeRADIUS proxy nationwide:

```
realm "~ ^ (. * \\.)? eduroam \\. TLD$" {
type = radius
authhost = <IP provided by OT>: 1812
secret = <secrecy provided by OT>
nostrip
}
```

Bold data that should be changed, where TLD is the domain of the country, and the IP and the secret that will give us the eduroam OT. The proxy of the federation must allow for direct access of a client whose IP and shared secret provided by the operations team.

This mirrored configuration is necessary for FreeRADIUS. The configuration for other implementations can easily be deduced from this.

As a result of performing this configuration, the eduroam operator will have access to a service that displays the results of all checks, as well as the time it took to complete the tests. This information is available retrospectively from the website monitoring.

The central monitoring service provides an interface that allows the administrator federation:

- Check the status of eduroam at the level of countries participating in the initiative;
- Know the latest updates that have occurred for a particular domain in a country;
- Know the latest updates that have occurred for a given root server of a country;
- Reporting the results of screening and response time custom date ranges.

2.6 ACCESSING EDUROAM USAGE STATISTICS FOR INTERNATIONAL ROAMING

Another possibility offered by the eduroam OT, is calculated using eduroam for roaming users, offering an array that will allow users to see how many of the same views had a country and how users came domains, or countries from which users have accessed a particular country when they were outside.

For these calculations, the NRO must submit summary information about each access request processing your proxy server or servers. Each of these pieces of information are called F-TICKS. The format of the F-TICKS ticks can be found in deliverable DJ3.1.2,1: Roaming Developments. Furthermore, there is online documentation explaining how to configure F-TICKS using FreeRADIUS as proxy software, RadsecProxy and Radiator.

The interface provides the operations team to consult statistics eduroam, can display data in table format and map format for both access as valid requests accounted for error. These data also can be delimited by date.

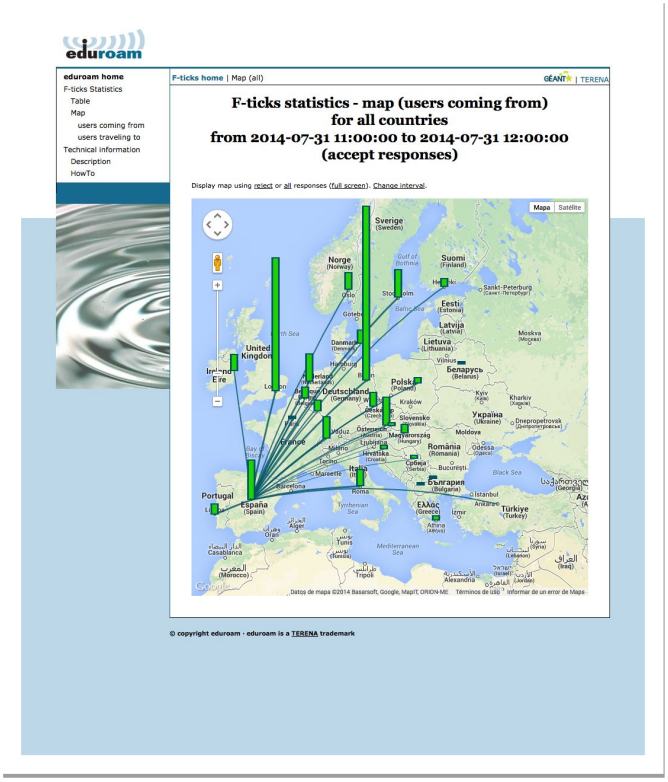

Figure 4: Map showing roamings posted by f-ticks.

2.7 FOR EDUROAM CERTIFICATE REQUEST THROUGH EDUPKI

The certification authority allows, hosted by eduPKI, request the generation and signing certificates for use on servers in the hierarchy. These certificates will be used in the phase of migration from national eduroam proxies to dynamic discovery.

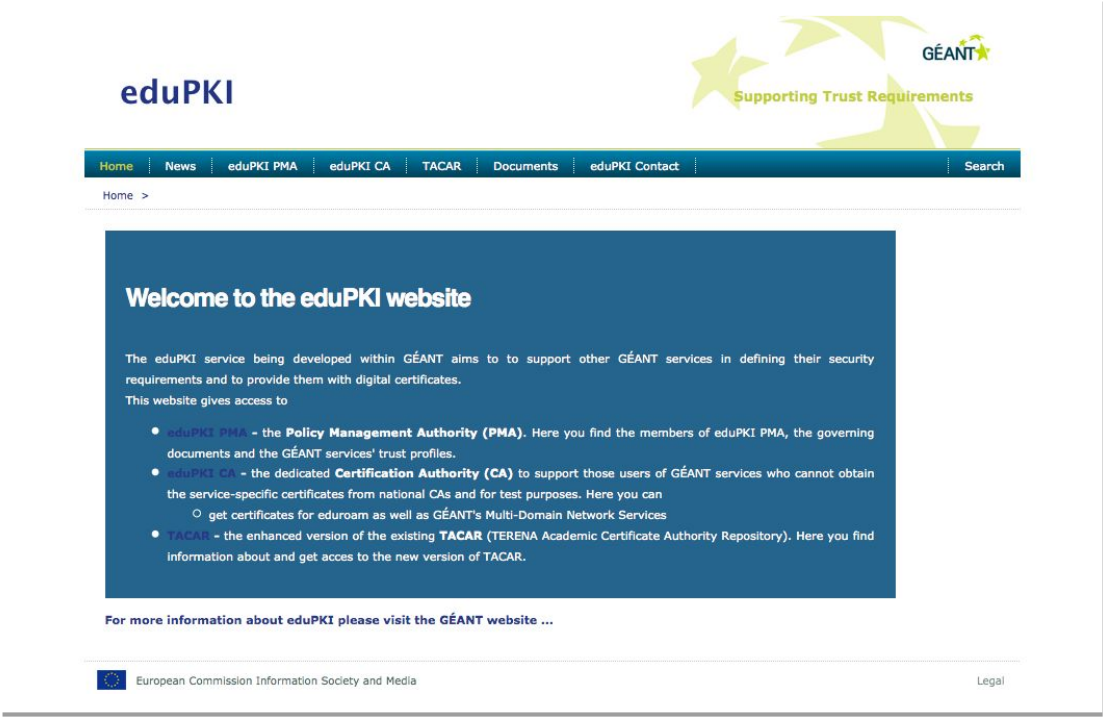

Figure 5: Website eduPKI.

In order to request certificates from the certification authority (CA hereafter), it must be accredited as defined in the trust profile. In this regard, the applicant should appear in the database of eduroam as the entity responsible for requesting certificates.

Once the country is eligible as applicants, it is generate a key pair and signing request (CSR) using the java application that is offered on the web site eduPKI, which will request the following information:

- FQDN of the server. In the case of a GSM roaming, it will usually be a server name under the rule of the country eduroam (ie eduroam.TLD), or under the control of the academic network (nren.TLD).
- E-mail address in the certificate. It will be included in the certificate itself, and generally be a generic contact address, the group of people associated with the domain name for which the certificate is sought.
- Organization. Generally this will be the name of the NREN, or organization that acts as NRO.
- Profile of certificates. For a national proxy, should be "eduroam IdP and SP," since both receive requests (IdP) or addressed (SP) to any registered domain.

• Country Code. It corresponds to the two-letter country code, as specified in ISO-3166-1 standard.

• Name of applicant. It is the name of the person requesting the certificate, which must be qualified for your application to be estimated.

• Email address of the applicant. It is the address of the applicant. The CA sends the bundle with the certificate to this address once signed.

• Acceptance of the policy. A box in which the applicant agrees to agree with the policy of eduPKI CA.

Figure 6: Application of Certificate Request to eduroam.

3.- DYNAMIC DISCOVERY IN EDUROAM

One issue that always concerns eduroam admins is the architecture of implementation. eduroam is a 12 years old idea, but with no modification so on. During last 2 years it has been discussion the idea of eliminate regional proxies, exchanging this model to a RadSec Proxies with dynamic discovery, with that the resilience of eduroam will be much bigger than it is nowadays.

The implementation is based on RADIUS (standard for eduroam RFCs 2865[1] Remote Authentication Dial In User Service (RADIUS) and 2866[2] RADIUS Accounting) plus RadSec (RADIUS Over TCP – RFC 6613[3]; Transport Layer Security (TLS) Encryption for RADIUS – RFC 6614[4] and Draft -

ietf-radext-dynamic-discovery[5]).

[1] http://tools.ietf.org/html/rfc2865

[2] http://tools.ietf.org/html/rfc2866

[3] http://tools.ietf.org/html/rfc6613

[4] http://tools.ietf.org/html/rfc6614

[5] https://tools.ietf.org/html/draft-ietf-radext-dynamic-discovery-11

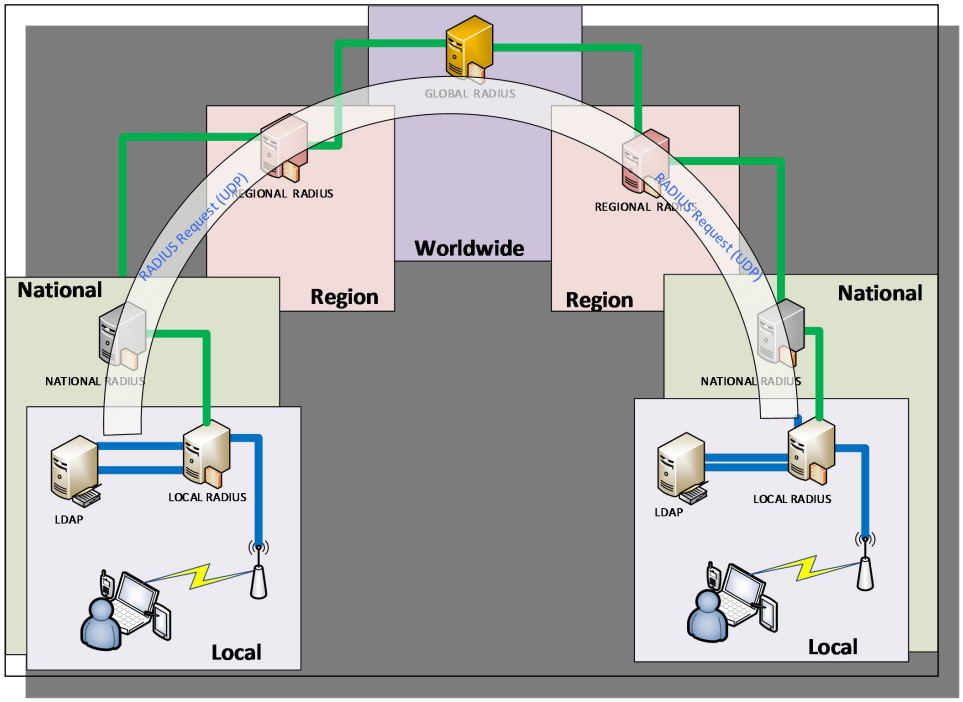

Figure 7: Actual eduroam architecture.

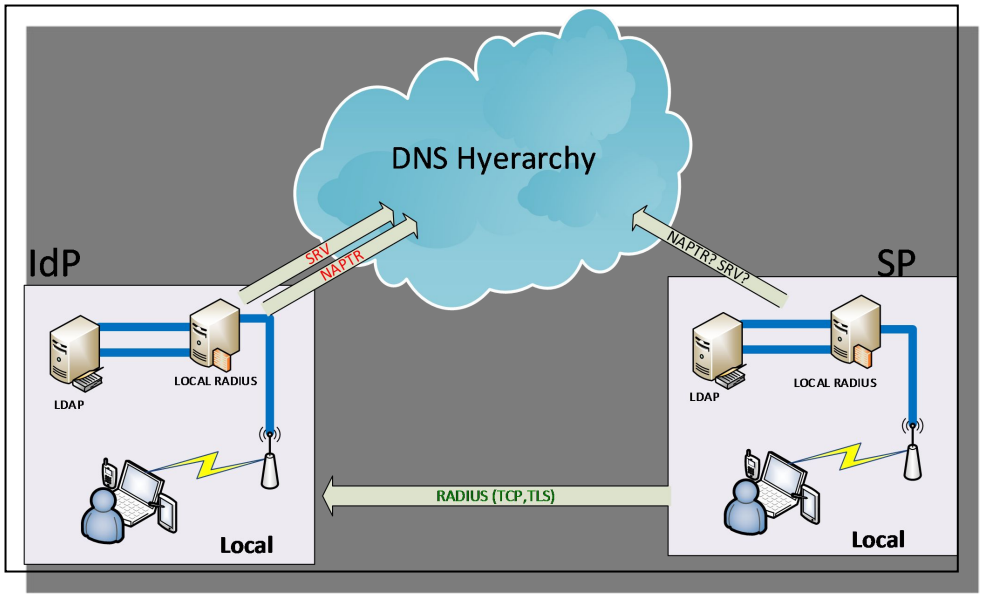

Figure 8: Proposal eduroam architecture.

Some issues was raised during these years and they are solving one by one. The first was regarding trust between NRO (National Roaming Operators). This was solving using eduPKI

(http://www.edupki.org). Only NRO authenticated in eduroam database can request certificates or through GeGC members.

Another problem was how user requests would get to LDAP servers. That was solved using DNS architecture. The SP or an intermediate server makes a DNS query discovery

If there is a NAPTR [6](*Naming Authority Pointer DNS Resource Record*) record from an eduroam user that wants to authenticate, a second question (SRV record) will be send to the server which safely route the request authentication, if not, the authentication request follows the usual hierarchy of RADIUS.

Inside CLATe (Latin America eduroam Comitee – Comité LATino-americano de eduroam), is discussing how, when and who is going to run a pilot of this change.

[6] https://www.ietf.org/rfc/rfc2915.txt

4.- GOVERNANCE IN LATIN AMERICA

In the framework of TICAL2014: Countries of the region signed an agreement for the creation of the Latin American Confederation of eduroam. On May 27, in the city of Cancun, Mexico, representatives of national networks that participated in the Fourth TICAL Conference meet to initiate the activities for the establishment of the Latin American Confederation of eduroam. Due to the widespread and growing use of eduroam in the region, the objective of the Confederation is to create a stronger basis for the governance of eduroam all over the world.

The agreed responsibilities include choosing the representatives of Latin America in the Global eduroam Governance Committee (GeCG); evaluating the service availability in the region and setting the strategy to follow. In addition, the members of the Confederation shall implement dissemination activities in Latin American countries through online or onsite training.

Figure 9: CLATe members.

The agreement was signed by (in the picture):
- Argentina (Julián Dunayevich – Innova|Red) – *Changed to Javier Martín – Innova|Red*;
- Colombia (Javier Enrique Lizarazo Rueda - RENATA);
- México (Hans Reyes - CUDI);
- Brazil (Leandro Marcos de Oliveira Guimarães – RNP);
- Costa Rica (Danny Silva Bermudéz - CONARE);
- Ecuador (Claudio Chacón - CEDIA);
- Perú (José Luis Quiroz Arroyo - INICTEL-UNI);
- Gustavo García, RedCLARA Technical Manager.

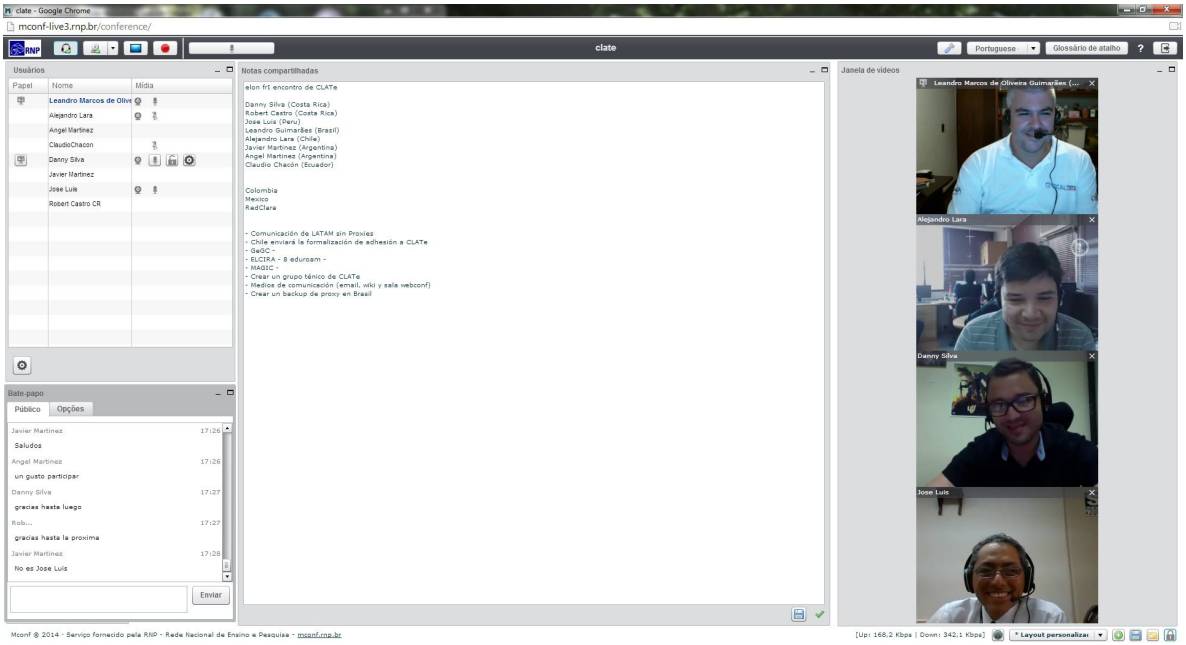

Figure 10: First CLATe meeting.

The first meeting (virtual) was performed in September 30th, with maximum quorum, demonstrating the interest and engagement of representatives from Latin America.