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

Deliverable 4.5

Report on eduroam preparation deploying an eduroam Federation

A project of the Seventh Framework Programme (FP7)

This project is funded by the European Commission

A project implemented by RedCLARA

Periodical Progress Report

ELCIRA Deliverable: D.4.5 - Report on eduroam preparation deploying an eduroam Federation

Document Full Name	**Report on eduroam preparation deploying an eduroam Federation**
Date	**May, 2013**
Activity	**WP4 (Promoting the deployment of eduroam services)**
Lead Partner	**RNP**
Document status	**Final**
Classification Attribute	**Public**
Document link	

Abstract: Install and configure all infrastructure used by eduroam (LDAP server, RadSec Proxy, RADIUS server, Access points and etc.). Report of technical and administrative agreements obtained through two NRENs of Latin America signing the eduroam Compliance Statement available by Global eduroam Governance Committee (GeGC) to guarantee eduroam interoperability and interoperation.

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 (this website will be available in October 1st 2012).

DELIVERABLE ROUTE

	Name	Member/Activity	Date	Responsible
From	Rodrigo Santiago	WP4		RNP
Revised by	Leandro Guimarães	WP4		RNP
Revised by	Antônio Carlos Fernandes Nunes	WP4	24/05/2013	RNP
Aproved by	Florencio Utreras	RedCLARA/Management	07/06/2013	RNP

A project of the Seventh Framework Programme (FP7)

This project is funded by the European Commission

A project implemented by 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

This document has the objective to present the guidelines to deploy the eduroam[1] service at a federation-level. Its content is based on official documentation elaborated by international groups and institutions like GÉANT, TERENA and GeGC (Global eduroam Governance Committee). The official documents can be accessed at https://www.eduroam.org/index.php?p=docs.

This document is structured in six main chapters, where the next chapter presents an overview of the service, considering its purpose, architecture and technologies involved; the third chapter treats about the guidelines to become a national eduroam roaming operator, focusing on the principal requirements to do so; the fourth chapter is related to documentation that should be developed and published about the service administration; the fifth one presents suggestions about people that may work with client support; the sixth chapter presents a schedule of eduroam implementation and finally, the documents of references are listed.

2.- EDUROAM OVERVIEW

eduroam, stands for *edu*cation *roam*ing, offers users from participating academic institutions secure Internet access at any other eduroam-enabled institution. The eduroam architecture that makes this possible is based on a number of technologies and agreements, which together provide the eduroam user experience: "open your laptop and be online". [1]

The eduroam service started originally as a pilot under the auspices of TERENA, that is the holder of the eduroam® trademark, carries the responsibility for ensuring the correct and secure operations of eduroam at the global level. TERENA also supports the development of technical improvements to the eduroam service, and promotes the deployment of eduroam worldwide.

The European eduroam service is a large-scale collaboration between hundreds of institutions, the majority of which own and operate the service's infrastructure. The national and international coordination of this infrastructure is undertaken by the National Roaming Operators and a central eduroam Operational Team that is funded by the GÉANT project.[2]

[1] https://www.eduroam.org/

[2] http://www.geant.net/Services/UserAccessAndApplications/Pages/eduroam.aspx

The GeGC has the central role in the global eduroam governance structure. The members of the GeGC are senior representatives of confederations and ROs worldwide. If a world region is represented by a confederation, the representatives from that world region are nominated by the confederation. If a world region is not represented by a confederation, then the ROs in that world region jointly nominate their representatives in the GeGC. The GeGC members are officially appointed by TERENA on the basis of these nominations. [2]

2.1 TERMINOLOGY

eduroam

eduroam is a federated roaming service that provides secure network access by authenticating a user with their own credentials issued by their Identity Provider (IdP).

eduroam Identity Provider (eduroam IdP)

An entity that is responsible for user credentials and operation of an authentication server for eduroam access for these users. IdPs are in some regions also known as “Home Institutions”.

eduroam Service Provider (eduroam SP)

An entity that operates an access network on which eduroam users are admitted to access Internet services once they are successfully authenticated by their IdP. Service Provider (SPs) are in some regions also known as “Visited Institutions”.

Roaming Operator (RO)

The entity that operates the eduroam service for a country or economy and that is recognized as such by the Roaming Confederation (RC) to which it belongs or, in case the country or economy is part of a geographic region for which no RC is established, by the GeGC. The RO may be a National Research and Education Network operator, for example. ROs are sometimes referred to as the “eduroam operators”.

RADIUS Proxy Server (RPS)

RPSs are established and maintained in order to provide the technical infrastructure (i.e., RADIUS server hierarchy) for the global eduroam service. Top-level RPSs for a geographic region are run by the corresponding RC. In cases where no RC is established for a specific region, the GeGC, advised by the ROs of that region, appoints the ROs that will run the top-level RPSs for the region.

Roaming Confederation (RC)

An entity that consists of a cohesive set of ROs serving a geographical region and that is recognised as such by the GeGC. The “European eduroam Confederation” is one example.

Confederation top-level RADIUS Server (TLR)

The confederation top-level RADIUS Servers, at the time of writing, are located in the Netherlands and Denmark for the European confederation, Australia and Hong Kong for the Asian and Pacific region, and Peru for the Latin America confederation. Each have a list of connected country domains (.nl, .dk, .au, .cn etc.) serving the appropriate National Roaming Operators (NROs). They accept requests for federation domains for which they are authoritative, and subsequently forward them to the associated RADIUS server for that federation (and transport the result of the authentication request back). Requests for federation domains they are not responsible for are forwarded to the proper confederation TLR.

Federation-Level RADIUS servers (FLRs)

A federation RADIUS server has a list of connected IdP and SP servers and the associated realms. It receives requests from the confederation servers and IdP/SP it is connected to and forwards them to the proper server, or in case of a request for a confederation destination to a confederation server.

IdP and SP RADIUS infrastructure

eduroam IdPs operate a RADIUS server which is responsible for authenticating its own users, by checking the credentials against a local identity management system.

eduroam SPs operate RADIUS capable equipment like Access Points or switches (see below). Large SPs typically also deploy an own RADIUS server, which is then responsible for forwarding requests from visiting users to the respective federation RADIUS server. Upon proper authentication of a user the SP RADIUS server may assign a VLAN to the user. Small SPs which do not require VLAN assignments can connect their RADIUS equipment directly to their FLR server, if the FLR permits that mode of operation.

Institutions which opt to be eduroam IdP and eduroam SP at the same time can have one RADIUS server that fulfills both roles simultaneously. This is the most popular deployment model in eduroam.

Note that the IdP RADIUS server is the most complex of all. Whereas the other RADIUS servers merely proxy requests, the IdP server also needs to handle the requests, and therefore needs to be able to terminate EAP requests and perform identity management system lookups.

Identity Management System

The Identity Management System of eduroam IdPs contains the information of the end users; for instance usernames and passwords. They must be kept up-to-date by the responsible IdP. An IdP RADIUS server will query the Identity management system to perform the actual authentication for a user as he tries to log in.

Supplicants

A supplicant is a piece of software (often built into the Operating System but also available as a separate program) that uses the 802.1X protocol to send authentication request information using EAP. Supplicants are installed and operate on end-user computing devices (e.g. notebooks, PDAs, Wi-Fi-enabled cell phones, and so on).

Access Points

Access Points are Wireless LAN access devices conformant to IEEE 802.11 and need to be IEEE 802.1X capable. They must be able to forward access requests coming from a supplicant to the SP RADIUS server, to give network access upon proper authentication, and to possibly assign users to specific VLANs based on information received from the RADIUS server. Furthermore Access Points exchange keying material (initialization vectors, public and session keys etc.) with client systems to prevent session hijacking.

Switches

Switches need to be able to forward access requests coming from a supplicant to the SP RADIUS server, to grant network access upon proper authentication and to possibly assign users to specific VLANs based on information received from the RADIUS server.

2.2 EDUROAM CONFEDERATION INFRASTRUCTURE

The crucial agreement underpinning the foundation of eduroam involves the mechanism by which authentication and authorization works:

- The authentication of a user is carried out at their Identity Provider (IdP), using their specific authentication method.
- The authorization decision allowing access to the network resources upon proper authentication is done by the Service Provider (SP), typically a Wi-Fi hotspot (University campus, etc).

In order to transport the authentication request of a user from the Service Provider to his Identity Provider and the authentication response back, a world-wide system of RADIUS[3] servers was created.

Typically every Identity Provider deploys a RADIUS server, which is connected to a local user database. This RADIUS server is connected to a central national RADIUS server, which is either in turn connected to an upstream (Latin American/global) RADIUS server or can connect to other RADIUS servers dynamically (using the protocol RADIUS/TLS).

Because users are using usernames of the format "user@realm", where realm is the IdP's DNS domain name often of the form institution.tld (tld=top-level domain; both country-code TLDs and generic TLDs are supported), the RADIUS servers can use this information to route the request to the appropriate next RADIUS server until the IdP is reached. An example of the RADIUS hierarchy is shown in Figure 1.

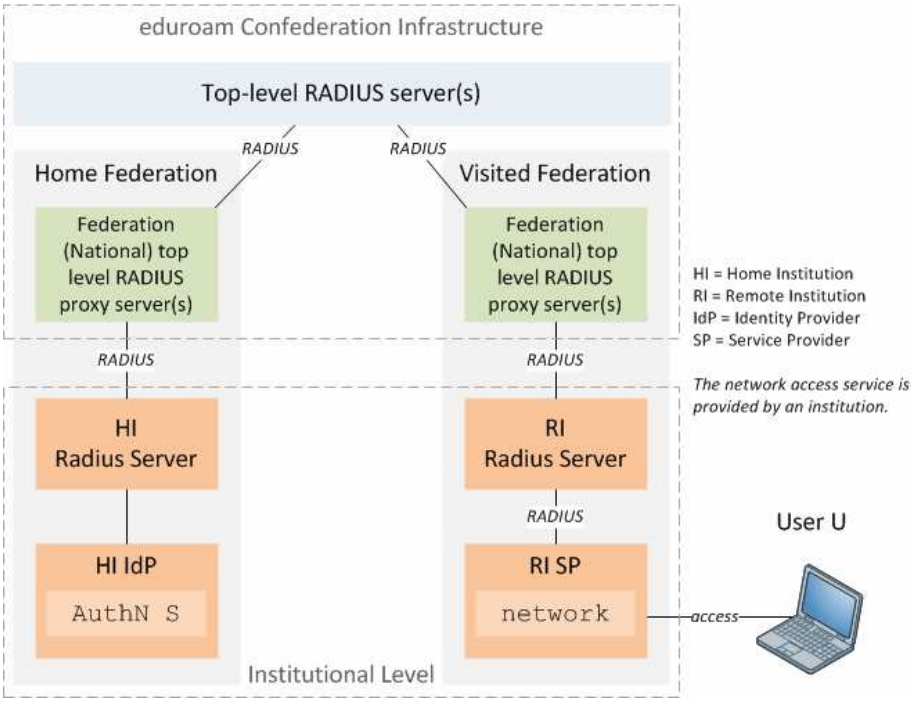


Figure 1 – Current eduroam RADIUS hierarchy.

To transfer the user's authentication information securely across the RADIUS-infrastructure to their IdP, and to prevent other users from hijacking the connection after successful authentication, the

[3] Remote Authentication Dial In User Service.

access points or switches deployed by the SP use the IEEE 802.1X standard that encompasses the use of the Extensible Authentication Protocol (EAP). EAP is a container that carries the actual authentication data inside, the so-called EAP methods. There are many EAP methods an IdP can choose from.

eduroam requires that the chosen EAP method must allow mutual authentication (i.e. the user can verify that he is connected to "his" IdP wherever the user is encryption of the credentials used (i.e. only the user and his IdP will see the actual credential exchange; it will be invisible to the Service Provider and all intermediate proxies).

Some popular EAP methods in use in eduroam are:

- PEAP (Protected EAP) – a Microsoft protocol that establishes a TLS tunnel, and sends usernames and passwords in MS-CHAPv2 hashes inside;
- TTLS (Tunneled TLS) – an IETF protocol that establishes a TLS tunnel, and sends usernames and passwords in multiple configurable formats inside;
- TLS (Transport Layer Security) – an IETF protocol that authenticates users and the IdP with two X.509 certificates;
- FAST (Flexible Authentication via Secure Tunneling) – a Cisco protocol that establishes a TLS tunnel, and sends usernames and passwords in a custom way inside.

RADIUS transports the user's name in an attribute User-Name, which is visible in clear text to all intermediate hosts on the way. Some EAP methods allow putting a different User-Name into the RADIUS packet than in the EAP payload. In that case, the following terms are used:

- *outer identity*, that is the User-Name in the RADIUS packet and visible to all intermediate parties;
- *inner identity*, that is the actual user identificator. It is only visible to the user himself and the Identity Provider.

When using such EAP methods, and activating this option, the real username is not visible in RADIUS (it will only see the outer identity). Doing so will enhance the user's privacy, and is encouraged. Outer identities should be in the format "@realm" (nothing left of the @ sign, but the realm is the same as with the actual username). The realm part still must be the correct one as it is used to route the request to the respective Identity Provider. Once the IdP server decrypts the TLS tunnel in the EAP payload, it gets the inner identity and can authenticate the user.

After successful authentication by the Identity Provider and authorization by the Service Provider, this SP grants network access to the user, possibly by placing the user in a specific VLAN intended for guests.

Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:

(a) Does not initiate the transmission;

(b) Does not select the receiver of the transmission; and

(c) Does not select or modify the information contained in the transmission.

3.- BECOMING A NATIONAL ROAMING OPERATOR

This chapter is based on the document [3], which defines orientations to the European community.

The Latin America confederation is composed by NROs administrated by the respective country's NREN that are connected up to the TLR (for RedCLARA) located at Miami (USA), operated by INICTEL-UNI[4] and under administration of RAAP[5].

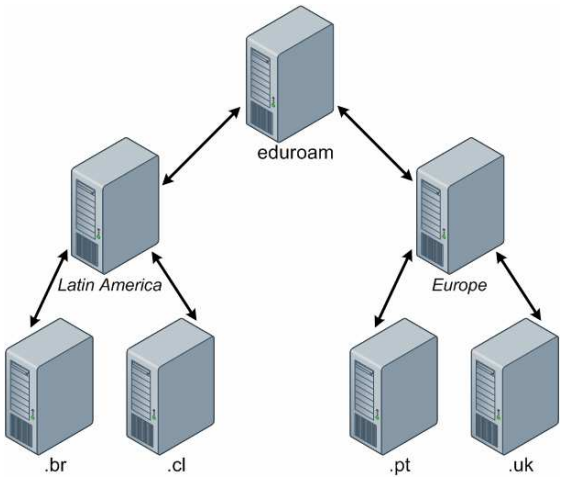


Figure 2 – eduroam international hierarchy.

[4] Instituto Nacional de Investigación y Capacitación de Telecomunicaciones - http://www.inictel-uni.edu.pe

[5] Red Academica Peruana (NREN of Peru) - http://www.raap.org.pe/

3.1 ADMINISTRATIVE REQUIREMENTS

Operating a federation involves managing and supervising eduroam Identity Providers, eduroam Service Providers, as well as keeping authentication logs, fulfilling uptime requirements, etc. Prospect federation operators should read and understand the requirements in DS5.1.1 ("eduroam Service Definition and Implementation Plan") at *http://www.eduroam.org/downloads/docs/GN2-07-327v2-DS5_1_1-_eduroam_Service_Definition.pdf*, particularly sections 4.1.4 ("Roles and Responsibilities - NROs") and section 6 ("Requirements on Confederation Members").[5]

A prospect NRO also needs to commit to the eduroam policy. The European eduroam policy document can be found at *http://www.eduroam.org/downloads/docs/GN2-07-328-eduroam-policy-for-signing-Final2-2.pdf*.

The NRO may outsource the operation of its technical infrastructure (particularly, the Federation Level RADIUS servers) to a third-party, but will remain responsible for eduroam within its service area. [3]

3.2 INFORMATION MANAGEMENT REQUIREMENTS

A National Roaming Operator must maintain a comprehensive overview over eduroam within its service area, and report about its federation's state regularly. The vehicle for such reports is the eduroam database, where contact information about the NRO and all its eduroam SPs and IdPs is stored. The database web interface is open for eduroam operators only; the entry page can be found here: *http://monitor.eduroam.org/db_web/*.

Generic information on how to deliver information to the eduroam database (XML Schema format) can be found here: *http://monitor.eduroam.org/database.php.*

3.3 OPERATING A FEDERATION-LEVEL RADIUS SERVER

Federation-level servers (FLRs) are used to connect eduroam Identity Providers and eduroam Service Providers with each other, and also provide an uplink from the federation to all other eduroam federations. They are managed by National Roaming Organizations (NROs). The NRO may outsource the operation to a third-party, but will remain responsible.

Since the concept of an eduroam federation geographically usually maps to a country, FLRs are central to the deployment of eduroam in a country; there is conceptually only one FLR per country - but for resiliency reasons, it is recommended to provide multiple instances in a failover setup. [3]

3.3.1 Hardware requirements

RADIUS is a very lightweight protocol, and does not require expensive hardware setups. Even the busiest eduroam federations operate their server on a single contemporary hardware or Virtual Machine, without experiencing overload conditions. [3]

As with every other professionally-operated service though, you should keep in mind that service uptime is paramount, and plan your procurement accordingly. Examples:

- In the case of virtual machines, use an underlying infrastructure which enables you to migrate machines without VM downtime, if possible.
- In the case of physical machines, use hot-pluggable parts where possible; and ideally, keep either spare hardware parts at hand or a set up a decent service contract.

4.- DOCUMENTATION AND PUBLICATION

Each NRO should establish and publish one or more documents that describe its policies, practices, and operation. Membership of an institution in the service should be legitimized through an adhesion term elaborated by the respective NRO.

The NRO should publish information about the available points of presence of eduroam (SP sites/hostspots) in its country or economy in an adequate manner defined by GeGC.

The NRO must publish information about eduroam services on dedicated web pages containing the following minimum information [4]:

- Text that confirms adherence (including an URL link) to an RC policy (if applicable);
- A list of IdPs and a list or map showing eduroam access coverage areas with links to each eduroam SPs web page;
- The contact details of the appropriate technical support that is responsible for eduroam services and mailing list(s).

5.- RECOMMENDED PERSONNEL

With a fully operational eduroam NRO, comes the necessity to provide client support. When dealing with IdPs and SPs, the support team must be prepared to guide users on questions about how to set up the provider's rules for authorization and authentication, translation of attributes, attribute collection from different kinds of basis, deployment of new services and many others. This includes knowledge not only of the IdP or SP itself, but also of the available tools that could be used to fulfill the provider's necessities and development possibilities inside the federation. Anyway, NRO may indicate softwares and settings to be used by the institutions while they are in the membership process.

6.- SCHEDULES

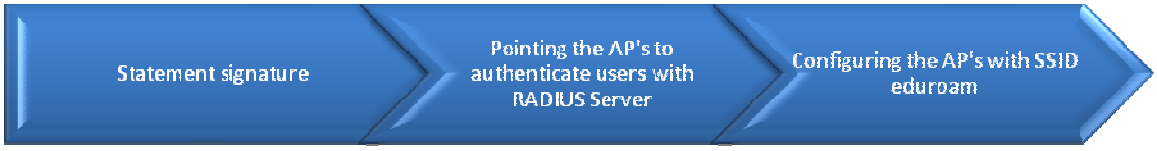
In this chapter is described the phases to implement a national federation for research and education, implement a eduroam Roaming Operator.

The time to run all these phases depends largely of the effort of National Research and Education team ; because of this the schedules consider only tasks, not dates.

6.1 CREATION OF A NATIONAL FEDERATION

6.2 CREATION OF AN IDENTITY PROVIDER (IDP)

6.3 CREATION OF A SERVICE PROVIDER (SP)



7.- REFERENCES

[1] eduroam Policy Service Definition v2.8, GÉANT, 26th July 2012.

[2] Global eduroam Governance, accessed in 24th May 2013 - https://www.eduroam.org/downloads/docs/TSec%2810%29015-GlobaleduroamGovernance-ConsensusVersion.pdf.

[3] How to deploy eduroam at national level, Terena Wiki, accessed in 24th May 2013 - https://confluence.terena.org/display/H2eduroam/How+to+deploy+eduroam+at+national+level.

[4] eduroam Compliance Statement v1.0, Tsec(11)043 – Issued 4th October 2011.

[5] Deliverable DJ5.1.5,3: Inter-NREN Roaming Infrastructure and Service Support Cookbook – Third Edition, GÉANT, 29/10/2008.
https://www.eduroam.org/downloads/docs/GN2-08-230-DJ5.1.5.3-eduroamCookbook.pdf