Implementación del servicio federado EDUROAM en los campus de la Universidad Técnica del Norte

Carlos Alberto Vásquez Ayala, Cristian Paúl Espinel Ramos

Facultad de Ingeniería en Ciencias Aplicadas, Universidad Técnica del Norte

cavasquez@utn.edu.ec

cpespinelr@utn.edu.ec

Abstract - ***Connectivity and mobility, is the main aim of EDUROAM, attaining an only space for each user that with so alone his credentials (GO and password) will allow him the access to any dependency inside an institution and even to an external institution in the same federation.***

EDUROAM Is, therefore, an infrastructure based in Free RADIUS that uses like technology of security 802.1X to allow the mobility between the distinct institutions that form it.

Said the previous, pretends offer a service of mobile connection and sure for the students, educational and researchers of the north Technical University what will avoid the constant configuration of the teams every time that they connect to a distinct wireless network and agilitará the educational process and investigativo of the users.

Index of Terms – EDUROAM, CEDIA, Federation

I. INTRODUCCIÓN

EDUROAM (education roaming) Is the world-wide service of safe access developed for the international community of investigation and education.

Initiated in Europe, EDUROAM has won impulse in all the community of investigation and education and now is available in 72 territories.

Permit to the students, researchers and personnel of the institutions participants obtain connectivity to Internet through the campus and when visiting other institutions participants simply opening his portable computer.

Anything user of a to institution participant of the federation can obtain access to the network. Depending on the local politics in the institutions visited, the participants also can have additional resources to his disposal.

The credentials of user keep safe because EDUROAM does not share them with the place that is visiting. In his place, send to the institution of origin of the user, where can be verified and validated.

The system uses a network of servers administered by the institutions and the National Networks of Investigation and Education (NREN, by his acronyms in English) to send these applications of safe way to his institute of origin. All this happens without problems and practically to the instant - All thanks to eduroam. [1]

II. THEORETICAL FOUNDATIONS OF EDUROAM

A. Characteristics.

EDUROAM Offers a service multiplatform, what wants to say that it works on different operating systems such as:

- Windows.
- Linux.
- iOS.
- Android.

To be able to access to this service the wireless user has to have an able device to bear standard IEEE 802.11to, b, g or n, in addition to bearing authentication WPA.

B. Wireless networks.

A wireless network is a network of data in which two or more terminal can communicate without the need of connection by wires. These networks allow to the users mobilize by a specific geographic area while they remain connected.

To attain this mobility the wireless network bases in teams of edge called Access Point, through them the user authenticates to access to the local network [2]

Wireless Local Area Network (WLAN)

A Network Wireless of Local Area (WLAN by his acronyms in groins), is a system of communication of flexible wireless data used like extension of a LAN wired up or like an alternative to this.

It uses technology of radiofrequencies what allows the mobility of the user, is delimited by the distance of propagation, 100m in interiors and several kilometers in outsides.

WLAN Uses technologies as IEEE802.11to, 802.11b, 802.15, etc. For connectivity through the spectrum disperse (2,4; 5 GHz) [3]

C. Management of Users

To make the management of users takes in account the concept of levels of access, awarding privileges for each one of them taking in consideration that can create different accounts.

The management of users inside EDUROAM bases in his instructions for use that will have to be affine to the politics of security of network of the institution, assigning to each user a credential only that will allow him connect to the network when it find in another institution affiliated or in his own institution.

D. Access Point (AP)

It is a device used mostly in WLAN, fulfils the function to cater the resources of the local network to the different wireless devices that request it and can control and regulate the access by means of the standard IEEE802.11. Also it can be used like repeater to serve to stations that find to greater distances [4].

E. FreeRadius

FreeRadius Is a protocol that offers mechanisms of authentication, permission and auditoria, for applications of access to networks. It uses a daemon that derives of the protocol RADIUS, although this, as his name indicates it, is free. [5]

One of the main characteristics of the protocol is his capacity to monitor sessions, catering notifications so much of start of session as of his ending. Uses the ports UDP 1812 and 1813 to send these messages, the port 1812 uses for the messages of authentication and the port 1813 for the messages of administration of accounts.

In EDUROAM FreeRadius will fulfil the role to conceal the credentials of user where, of local way, will be verified in the database and validated to allow the authentication and the access to the service. In case to be an external user to the institution, FreeRadius will link with the National server and this will commission to connect with the server of the corresponding institution.

F. Protocol 802.1X

"IEEE802.1X allows to the administrators authenticate users in place of machines and can use so that the users connect to legitimate networks and authorized in place of networks impostors that try to steal credentials" [6] When an user connects to an AP that bears IEEE802.1X begins the exchange of messages of authentication EAP to carry out the authentication of user with the server.

To fulfil the process of connection the protocol IEEE 802.1X has three participants that conform his architecture, the function of each one of them indicates to continuation besides the Figure 1 sample the architecture of the protocol.

- Suplicante.

Generally, it treats of the device applicant of access to the wireless network, generally the user.

- Autenticador.

It treats of the intermediate team that receives the application of the supplicant, an Access Point, for example, this acts like an intermediary in the exchange of traffic of authentication to the server.

- Server of Authentication.

It commissions to check the credentials of the user supplicant, assigns the priorities and privileges established and authorizes the access.

The Figure 1 sample the architecture of the protocol in a diagram of connection between the three participants.

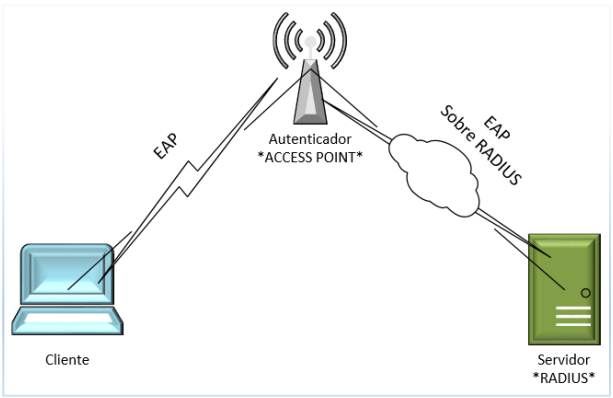

Figure 1. Architecture Protocol IEEE802.1x

The authentication bases in the protocol EAP, which uses several mechanisms of authentication as they are MD5, Kerberos, Passwords of an alone use, among others. It consists in an encapsulated that has to be transported between the Supplicant and the Server, the Figure 2 sample the architecture 802.1X by layers.

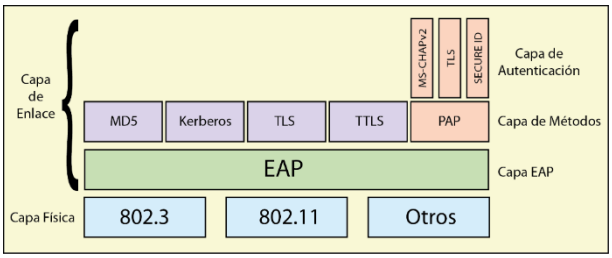

Figure 2.- Architecture 802.1x by layers.

EAP Is a protocol of authentication that carries out the tasks of AAA and when being compatible with IEEE 802.1x can use methods of authentication like digital certificates or identifiers of user and password.

The main mechanisms of authentication of EAP listed below:

- PEAP, Protected EAP consists in a mechanism of validation based in user and password.
- EAP-TLS, based in digital certificates so much in the customer as in the server.

- EAP-TTLS, bases in an authentication of user and password which are transmitted by a tunnel created by means of TLS, unlike EAP-TLS the server is the only that requires certified. [7]

When using EAP-TTLS the Access Point will not sue to implant a concrete method to identify to the users, simply will go in in action like runway between the mobile device and the server, in this case FreeRadius like sample the Figure 3.

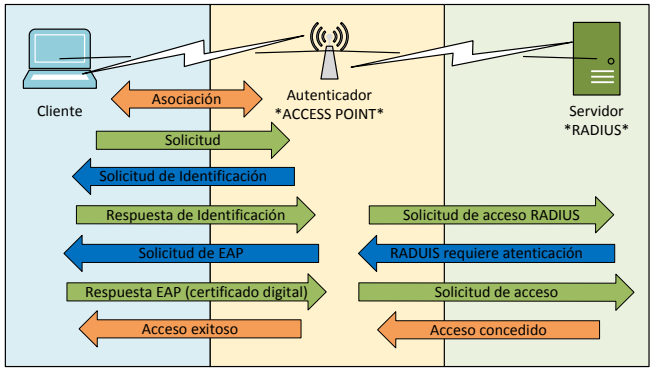

Figure 3. Application of connection.

G. Database LDAP.

Lightweight Directory Access Protocol (LDAP) Is based in a group of open protocols and in the standard X.500 of sharing of directories by what is able to propagate his query to other databases LDAP all over the world, what provides a "global directory". It is also a system customer/server commissioned to organize the information of hierarchical form to way of directory with the end to be able to access to said information by means of a query,

Between the advantages find that one of his applications is the authentication of users based in Radius controlling the access to a network, guarantees besides a fast reading of the registers ensuring that each one of them was only, allows to create multiple independent directories and of hierarchical form for allocation of privileges, simple to install and keep.

Taking in account all the advantages showed, in EDUROAM the database LDAP will conform the directory of the students, educational and researchers since when being flexible allows to deploy the information that the server require to check. [8]

The structure of the database that will implement in the institution and will house to the users of EDUROAM finds in a hierarchical order as it shows in the Figure 4.

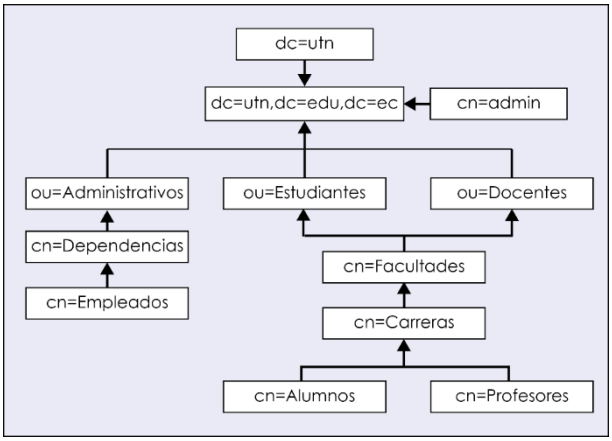

Figure 4.- Hierarchical structure of the Database LDAP UTN

H. Digital certificate.

The digital certificate is a digital document that contains a public key together with the data of the user, all this endorsed by an Authority of Certification, this document has the characteristic to protect the data that the user facilitates, by such reason offers an additional security inside the communications.

EDUROAM Will use the digital certificate to accredit to each user of the institution and to all those of pertaining institutions to the agreement, besides will guarantee the security during the connection to the network federada. [9]

I. Standar ISO/IECE/IEEE 29148.

The standard ISO/IEC/IEEE 29148 for the analysis of requests for development of software, allows the suitable election of an Operating system for the implementation of a service by means of the evaluation and consideration of parameters and specific requirements such as:

- Interfaces of User.
- Interfaces of Software.
- Interfaces of Communication.
- Types of Information.
- Frequency of Use and Access.
- The Entities of Data and his Relations.
- Restrictions of Integrity.
- Restriction of Data.
- Version.
- Licence.
- Performance.
- Interoperability.
- Escalabilidad.
- Security and Reliability.

III. CURRENT SITUATION THE OF THE NETWORK OF THE UNIVERSIDAD TÉCNICA DEL NORTE

A. *Current infrastructure.*

The campus of the Universidad Tecnica del Norte is conformed by the following buildings:

- Central plant.
- University welfare.
- Faculty of Engineering in Sciences Applied.
- Faculty of Engineering in Sciences Agropecuarias and Environmental.
- Faculty of Administrative and Economic Sciences.
- Faculty of Education Science and Technology.
- Faculty of Sciences of the Health.
- Academic centre of Languages.
- Institute of Postgrado.
- Mechanics and Electricity.
- Library.
- Polideportivo.
- Aquatic complex.
- Gymnasium.
- Auditorium Agustín Cave.

At present the wireless network of the north Technical University has 84 Access Point interiors and with 16 Access Point outsides, situated strategically in each building of the campus to attain the maximum coverage.

B. *Physical topology of the network of the north Technical University*

The Figure 5 sample the connection of the teams of core and administration situated in the Data Center of the DDTI and the teams of distribution situated in each faculty and dependency inside and off campus.

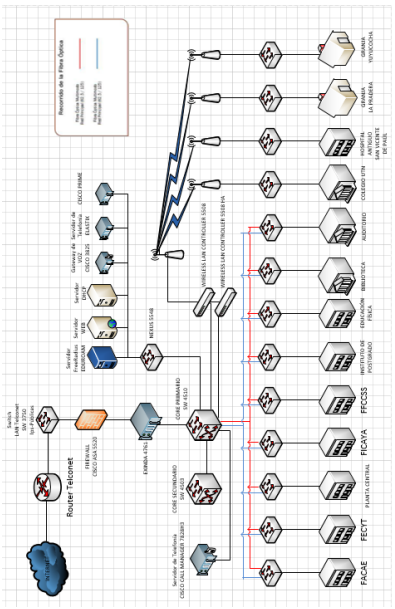

Figure 5.- Physical topology of the north Technical University.

The mechanism of Access for the different networks Wireless of the institution is the following:

- Wireless Administrative

The SSID propagated in the campus is "WUTN.Admin", the access makes by means of password, which is configured in the WLC of the north Technical University.

- Wireless Educational

The SSID propagated in the campus is "WUTN.Educational", the educational make his authentication by means of a password and besides registering the direction MAC of his or his devices (PC, Smartphone, Tablet), what allows that only the device registered can access to the network.

- Wireless Students

The SSID propagated in the campus is "WUTN.Estudiates", considering the high number of users and the availability of connection that requires by the same, the network of students is of free access.

- Wireless Events

The SSID propagated mainly is the Auditoriums of the Institution is "WUTN.Events", the access makes by means of password, which is configured in the WLC of the north Technical University.

C. *Bandwidth*

The north Technical University has a Bandwidth of 600 Mbps, which are distributed priority between the current dependencies of agreement to the need of each one of them, in addition to guaranteeing 55% of bandwidth to each student that connect to the network WUTN.Students, this of agreement to the politics of administration of Bandwidth established in the DDTI by the administrator of Networks.

D. *Equipment*

They installed 49 teams marks CISCO model AIR-CAP3702I-To-K9 exclusive for interiors, 16 teams marks CISCO model AIR-CAP1532And-To-K9 exclusive for outsides, besides relocate 32 teams marks CISCO model AIR-LAP1262N-To-K9 and 5 mark CISCO model AIR-CAP1602And-To-K9 exclusive for interiors, for a total of 84 teams as it indicates in the section III. To.

In accordance with the manufacturer of the respective teams installed at present in the campus of the Institution, determines that:

- Team AIR CAP3702I-To-K9, exclusive for interiors, has the capacity to bear 120 users connected simultaneously.
- Team AIR LAP1262N-To-K9, exclusive for interiors, has the capacity to bear 100 users connected simultaneously.

- Team AIR-CAP-1532And-To-K9, exclusive for outsides, has the capacity to bear more than 150 users connected simultaneously. [10]

For the mark of Access Point that has the north Technical University has of four ways of operation, depending on IOS or his configuration can be:

- **Local way (LIGTHWEIGHT):** An Access Point that works in local way links of automatic form to the Wireless LAN Controller adopting his configuration automatically, in this way the AP's answer to commandos lwap, capwap.
- **Autonomous way:** they Work of independent form, that is to say, do not link to the Wireless LAN Controller, therefore, depend on the individual configurations that the administrator make.
- **Way Mesh:** it Offers the functions of antenna to communicate with another Access Point, uses the frequency of 802.11b and 802.11g, usually uses to cover big distances, however, has to take in account that the bandwidth diminishes.
- **Way Flex Connect:** An Access Point in this way saves the configurations of the Wireless LAN Controller, when the connection with the WLC falls the AP in way Flex Connect turns into a WLC secondary that uses the local resources.

EDUROAM Requires a control centralized to administer his resources, and place that the WLC offers this ease, all the wireless teams that find installed in the campus of the north Technical University have to be configured in *Local Way*.

E. Users

The Table 1 sample the average of users connected simultaneously in a week to the inner teams of the dependencies of the north Technical University.

Table 1
Average Users inner teams

Building	Weekly average
FACAE	331
FECYT	239
FICAYA	168
FCCSS	216
CAI	168
POSTGRADOS	68
UNIVERSITY WELFARE	25
CENTRAL PLANT	83
AUDITORIUM	57
SWIMMING POOL	24
POLIDEPORTIVO	151
LIBRARY	148
ELECTRICITY	40
GYMNASIUM	10

The Table 2 sample the average of users connected simultaneously in a week to the external teams of the north Technical University.

Table 2
Average Users external teams

Location	Weekly average
FACAE External Bar	49
FACAE External Terracings	27
FACAE External Park	22
FECYT External Park	36
External auditorium Square	2
External auditorium Fields	3
Central plant Outside	28
Postgrado External Park	15
Postgrado External Swimming pool	17
CAI/FICAYA External	29
FICA/FICAYA External	74
FICA/FCCSS External	36
External swimming pool	6
FICA External	128
Gone in North Fields	33
Gone in North Welfare	13

Of agreement to the data collected and in comparison with the data that the manufacturer stipulates for the teams, concludes the following:

The teams Wireless, so much inner like outsides, have the necessary capacity to bear the continuous influx and simultaneous of users.

F. Requests of Hardware and Software

For the installation of the server FreeRadius with database LDAP and administration phpLDAPadmin recommends consider the following characteristics so much of software as of hardware.

Software.

- Operating system: Debian 6.0.7.
- FreeRadius.
- Database LDAP.
- phpLDAPadmin.

Hardware.

- Processor AMD FX(tm)-8320 Eight-Core 3.50 GHz.
- Memory RAM 4 GB.
- Hard disk of 1 TB.

This with the end to bear logs and administer of suitable and fast form the number of users that will be stored in the database.

G. Selection of Software

In base to the standard ISO/IEC/IEEE 29148 that indicates in the section II.I. It makes the comparison between the Softwares CentOS and Debian to select the most suitable based in the already established requests, the T abla 3 sample the qualification by characteristic.

The qualifications describe of the following way:

For each request assigned the levels of characteristics that considered necessary, depending on this, assigned the values: zero (0) to that less apt for the implementation, one (1) for an intermediate or suitable characteristic and two (2) to which considered more adapted for the project.

Table 3
Qualification of parameters for selection of software

Request	Characteristic	Qualification	CentOS	Debian
Interfaces of User.	Compulsory graphic surroundings	0	1	1
	Console of commandos	1		
Interfaces of Software.	It Does not bear Servers and BDD	0	1	1
	It bears Servers and BDD	1		
Interfaces of Communication.	It Does not allow the protocol EAP	0	1	1
	It allows the protocol EAP	1		
Types of Information.	Types of information limited	0	1	1
	Types of complete information	1		
Frequency of Use and Access.	Low availability	0	2	2
	Half availability	1		
	High availability	2		
Entities of Data and his Relations.	It does not classify the users	0	1	1
	It allows to classify users	1		
Restrictions of Integrity.	Administration limited	0	1	1
	Complete administration	1		
Retention of Data.	It is not possible to generate report	0	1	1
	It is possible to generate report	1		
Version.	Previous and stable	0	2	2
	Up to date	1		
	Up to date and Stable	2		
Licence.	Owner	0	1	1
	Free	1		
Performance.	Low performance	0	2	2
	Half performance	1		
	High performance	2		
Interoperability.	Limited	0	1	2
	Two or more Platforms	1		
	Any Platform	2		
Escalabilidad.	It is not scalable	0	1	1
	It is scalable	1		
Security and Reliability.	Low security	0	2	2
	Half security	1		
	High security	2		
TOTAL			**18**	**19**

As it can observe in the previous table the difference between the softwares is minimum, however, **Debian** describes mainly by his interoperability with other platforms, in this case in particular has to integrate the operating system with the Wireless LAN Controller of the institution.

IV. INTEGRATION And IMPLEMENTATION OF EDUROAM

Once that it has selected the operating system on which mounted the services, proceeds in first instance to make the basic configurations to guarantee the connectivity to the network. The following step is the installation of the services.

FreeRadius, the one who does the times of server AAA, making the Authentication, Permission and Auditoria of EDUROAM.

LDAP, is the database where will house the users of the institution.

Schema, that defines the organization of the users, that, in this case, will be of hierarchical form.

phpLDAPadmin, interface web that allows the administration and organization of the users inside the database, all this once that it has defined the hierarchy with schema.

In the Figure 6 observes the process of a request of connection by part of an user of the north Technical University inside his own campus once that they have configured all the services and assigned the credentials of access.

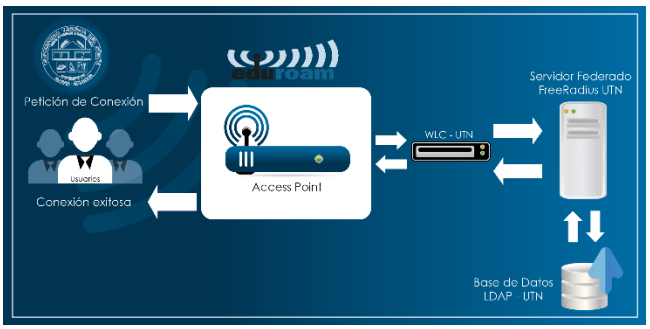

Figure 6. Diagram of local connection.

The process initiates when an user identifies the ssid "eduroam" and requests the access.

The Access point (AP) goes in in operation requesting to the user ingress the credentials.

When the user has ingresado his credentials the AP does the times of tunnel, and through the Wireless LAN Controller (WLC) communicates with the server.

The server FreeRadius makes the process of authentication of the credentials by means of the database LDAP making a comparison of data to validate the existence of the user.

The database answers to the server a "Access accepted" of credentials veridical.

The server assigns the digital certificate to the user that is making the request and answers again through the WLC and of the AP allowing him the access and guaranteeing him the connection.

For a connection between pertaining institutions to the agreement the process is similar, incidentally as it observes in the Figure 7, makes the communication between the servers of the institutions involved and the national server of CEDIA, to what calls federation.

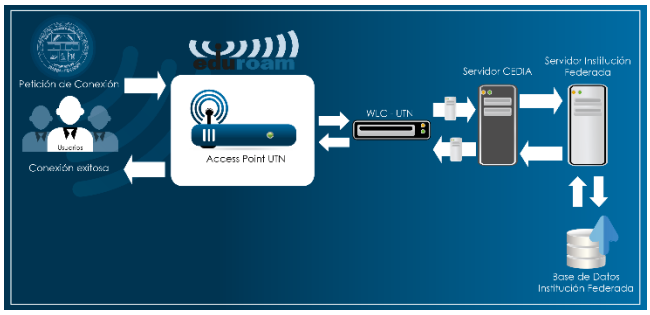

Figure 7. Diagram of connection Interinstitucional.

V. PROOFS And RESULTS

A. *Local proof*

The proof makes afterwards to having configured properly everything in what it refers to the connection between the server of the north Technical University and CEDIA

The first test makes with an user typical of the previously registered institution in the database inside the server and assigned the credentials respective for his correct access, is so executing the commando ***radtest*** together with the user and credentials already mentioned can observe in the Figure 8 the authentication makes successfully and the access is accepted.

```
root@eduroam:~# radtest cpespinelr@utn.edu.ec 1003235213 127.0.0.1 1812 AdminLdap@Eduroam
Sending Access-Request of id 129 to 127.0.0.1 port 1812
        User-Name = "cpespinelr@utn.edu.ec"
        User-Password = "1003235213"
        NAS-IP-Address = 10.24.8.8
        NAS-Port = 1812
        Message-Authenticator = 0x00000000000000000000000000000000
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=129, length=37
        Tunnel-Private-Group-Id:0 = "128"
        Tunnel-Medium-Type:0 = IEEE-802
        Tunnel-Type:0 = VLAN
```

Figure 8. Local proof with commando radtest.

It concludes , dand agreement with the result, that the communication between the server and the database is correct.

B. *Proof Interinstitucional*

The present proof makes with the end to check the correct communication between the Institutional Server and the Server of CEDIA.

For this end the administrator has created the user *utpl@**utn.edu.ec*** corresponding to the north Technical University and requesting the collaboration of the Technical University Individual of Loja, pertaining to the federation, to make the respective proof. The collaborator makes the connection by means of a mobile device with operating system Android, to continuation, the Figure 9 sample how makes the request through the server federado of CEDIA and connects to the Institutional server, is as well as the user UTN connects satisfactorily inside the campus of the UTPL.

```
ptado :) %{User-Name} -> Usuario Aceptado :) utpl@utn.edu.ec
(from client org-federado.cedia.org.ec port 0 via TLS tunnel) Usuario Aceptado :) utpl@utn.edu.ec
section.  Using default return values.
ith from file /etc/freeradius/sites-enabled/inner-tunnel
```

Figure 9. Proof of connection of an user UTN in a pertaining institution to the federation.

Of agreement to the proofs made so much with local users as with external users to the institution concludes that the service allows the connectivity in all the campus of the institutions that belong to the federation, of the same forms this guarantees the correct configuration of the institutional server of the north Technical University and the communication of the same with the server federado of CEDIA.

VI. CONCLUSIONS

It implemented the service federado EDUROAM in the north Technical University that guarantees the safe connectivity of the users so much in the local campus as in the campus of pertaining institutions to the federation.

The north Technical University has the suitable teams for an administration centralized what facilitates the implementation of the service federado.

Debian In his version 6.07 is the suitable operating system to house the necessary servers, in addition to being compatible with the WLC of the Institution.

The hierarchy used by the database LDAP in the server FreeRadius allows to classify and administer properly the users of the institution.

The use of digital certificates provides to the greater users security to the moment to make his connection with the service federado as it protects his navigation and keeps to except his credentials.

The proofs made guarantee the connection of users of the north Technical University in the campus of the pertaining Institutions to the agreement, besides shows the correct federation between servers.

VII. RECOMMENDATIONS

Previous to the implementation of a wireless service have to make a site survey in the institution to check of coverage and availability of the teams.

In view of the imminent change of direccionamiento IPv4 to IPv6, recommends migrate the server so that it work under the new protocol.

Has to make a periodic analysis of capacity of users of the wireless teams of the Institution, this with the end of dimensioned the daily and weekly connections, with said data will be able to solve the requests of the future users of the service federado, in addition to administering properly the teams of the wireless network to avoid his saturation, by what

recommends create politics of suitable connection for the users.

It is recommended restart the installed services during the implementation with a moderate frequency, this with the end to guarantee the correct operation of the server.

Update the database semiannually, this taking in account that in each period they enter new students to the institution, as well as some abandon it.

To offer the service EDUROAM in the external campus of the north Technical University the installed teams in said dependencies have to change his configuration of Autonomous Way to Local Way.

VIII. REFERENCES

[1] eduroam, «eduroam,» [On line]. Available: https://www.eduroam.org. [Last access: 3 dic 2016].

[2] Definiciones.de, «Definiciones.de,» 2008. [On line]. Available: http://definicion.de/red-inalambrica/.

[3] I. Bernal, «Wireless Communications Generalities of WLAN,» Remove, 2005.

[4] I. Modern, «Modern Computing,» 2008. [On line]. Available: http://www.informaticamoderna.com/acces_point.htm. [Last access: 19 April 2015].

[5] GlosarioIT, «Computer Glossary,» 2003-2015. [On line]. Available: http://www.glosarioit.com/#!FreeRadius. [Last access: 5 September 2015].

[6] S. G. Mattew, Networks Wireless 802.11, vol. 2, Madrid: Anaya Multimedia, S.A., 2006.

[7] P. P. F. Martínez, «dns.bdst.net,» [On line]. Available: http://www.bdat.net/seguridad_en_redes_inalambricas/x80.html. [Last access: 22 March 2016].

[8] RedHat, «Network Hat Enterprise Linux 4,» 2005. [On line]. Available: http://web.mit.edu/rhel-doc/4/rh-docs/rhel-rg-es-4/index.html. [Last access: 21 November 2015].

[9] RedIRIS, «eduroam,» 26 July 2015. [On line]. Available: https://www.eduroam.es/.

[10] Cisco, «Cisco,» 2016. [On line]. Available: http://www.cisco.com/c/en/us/products/wireless/access-points/index.html. [Last access: 17 August 2016].

[11] F. Andreu, I. Pellejero And To. Lesta, Networks WLAN Foundations and applications of security, Barcelona: Marcombo, 2006.

IX. BIOGRAPHIES

Carlos Alberto Vásquez Ayala

It was born in I Remove on 19 September 1981, engineer in Electronics and Telecommunications, National Polytechnical School in 2008, at present educational of the Career of Engineering in Electronics and Networks of Communication of the north Technical University, graduate of the Mastery in Networks of Communication, Pontificia Catholic University of the Ecuador.

Cristian Paúl Espinel Bouquets

It was born on 6 February 1989 in the city of Ibarra, culminated his secondary studies in the School Fisco-Misional San Francisco Physical speciality Mathematician, at present graduate of the career of Engineering in Electronics and Networks of Communication, President of the Student Branch IEEE of the north Technical University period 2016, active member of IEEE from the 2015.