Access Control and Network Administration Resources through a AAA server at the GAD Urcuqui's Municipality using free software based solutions

Carlos A. Vásquez, William E. Vaca

***Abstract*— This project presents the design and implementation of a network's scheme that supplies the authentication service, authorization and accounting (AAA) in the "San Miguel de Urcuqui's GAD Municipality" that access control and network resources administration utilizing free software based solutions. Its user's authentication is done using the EAP-TTLS method. Its own security is built-on digital certificates and a centralized directory that stores access codes thus allowing a dynamic network resources assignment through VLAN. Finally, within a MySQL database, all events generated by AAA system users are stored.**

***Index Terms*— AAA, EAP-TTLS, IEEE 802.1X, RADIUS, LDAP, MySQL, VLAN**

I. INTRODUCTION

DATA networks are essential to the growth and development of companies. They are capable of supporting new technologies easily evolving, facing changes and new applications that are being developed every day. At present, there are many security risks related to communication networks, social engineering techniques, neglecting service attacks, misused apps and even data retention. Those threats can be originated outside the company or by employees who intentionally compromise the entire infrastructure's operability.

At the AAA system's implementation within the GADMU data network, a secure access procedure is guaranteed through authentication methods based on digital certificates and networks resources. Then those resources are administrated y security policies centrally managed from a MySQL database and directed to the authentication server, all events are generated by devices successfully accessed to the system.

II. BASIC CONCEPTS

A. AAA Systems

The AAA standard is used in the data network access control design, providing authentication services, authorization and accounting in a centralized form.

- **Authentication.** Is the most relevant process of the AAA system. It serves as the basis for the entire system due to a direct relation with the authorization and accounting processes. The authentication allows proving a user's identity throughout the following elements: Something known, as a personal identification number (PIN) or password, something had, like an intelligent card (ATM) or something that physically identifies the user in a unique way, like a digital fingerprint, voice recognition, eye retina scanner, etc. Using more than one identifiable factor adds credibility to the authentication process [1].

- **Authorization.** It is the process whereby a user is assigned a predetermined amount of resources or network services based on activities performed and by access polices established by the administrator, who in turn must by related to the authentication process. If one user is not correctly identified, the proceeding steps will be null. In order to comply with the authorization process, AAA systems use solutions like databases or directories allowing the storage of each user's access profiles.

- **Accounting.** Once the authorization process is done, the "accounting" phase is originated, it begins at the time the NAS authenticator approves the suppliant access to the network services. Accounting is the statistical and data collection process located over the connection. Properly used collected data during the authentication/authorization processes allows the network administrator manage system's future demand so that it is able to plan its development.

Document received on December, 2014. This research has been made as a previous project to get the degree in Electronics and Communication Network Engineering, at the Técnica del Norte University.

C.A. Vásquez, Works at the Técnica del Norte University, Ibarra-Ecuador (phone: 0996125270; email: cavasquez@utn.edu.ec).

W.E. Vaca, Graduated in Electronics and Communication Networks, at the Técnica del Norte University (phone: 0986260191; email: william_889@hotmail.com).

B. *Radius*

RADIUS (Remote Authentication Dial In User-Service). Is a protocol where the network's infrastructure is client-server based. Authentication, authorization and accounting are administrated by a resource equipment provider, which in this case, server radius and clients are those who access services offered by the network infrastructure [2].

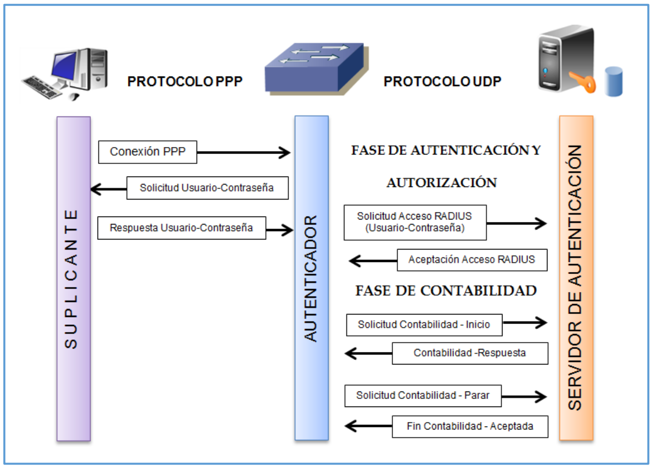

PROTOCOLO PPP
PROTOCOLO UDP
SUPLICANTE
AUTENTICADOR
SERVIDOR DE AUTENTICACIÓN
Conexión PPP
Solicitud Usuario-Contraseña
Respuesta Usuario-Contraseña
FASE DE AUTENTICACIÓN Y AUTORIZACIÓN
Solicitud Acceso RADIUS (Usuario-Contraseña)
Aceptación Acceso RADIUS
FASE DE CONTABILIDAD
Solicitud Contabilidad - Inicio
Contabilidad -Respuesta
Solicitud Contabilidad - Parar
Fin Contabilidad - Aceptada

Fig. 1. RADIUS Communication

RADIUS uses the UDP 1812 port for the authentication process and the 1813 port for information recording (accounting).

C. *IEEE 802.1x*

It is an authentication standard that allows access control to network services through ports and it operates over OSI model's layer. It secures user's credential interexchange or user's device avoiding any unauthorized access.

An 802.1x infrastructure requires three elements to operate: suppliant, authentication equipment and an authorization server [3].

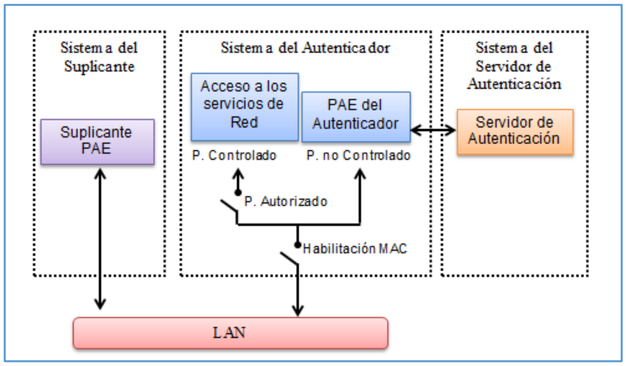


Fig. 2. 802.1x Operation mode

- **Supplicant.** Is a software installed to the client's authenticator equipment, used in wired or not wired environments. Suppliant is charged onto the user's device and is utilized to request access to the network.

- **Authenticator.** Is the component by which the user accesses network services. It is located between the device to be authenticated and the server being used to process the authentication. Examples of authenticators are network switches and wireless access points.

- **Authentication Server.** Is the equipment that receives messages through a RADIUS communication line. It uses this information to prove the user's authentication or the authentication of the accessing device; generally databases are used to perform processes such as SQL, Microsoft Active Directory, LDAP, etc.

D. *Eap-ttls*

The Extensible Authentication Protocol (EAP) is defined in the RFC 3748. It allows multiple authentication methods. One of them is EAP-TTLS transport Layer Security (TLS) and it is the protocol's successor SSL that allows the setting of a secure connection through the creation of an encrypted channel between client and server so that it sends access credentials during the authentication process [4].

Only installation of a digital certificate is required in the RADIUS server so that it reduces its complexity authentication system considerably without the need of installing and managing certificates pertaining to the network devices.

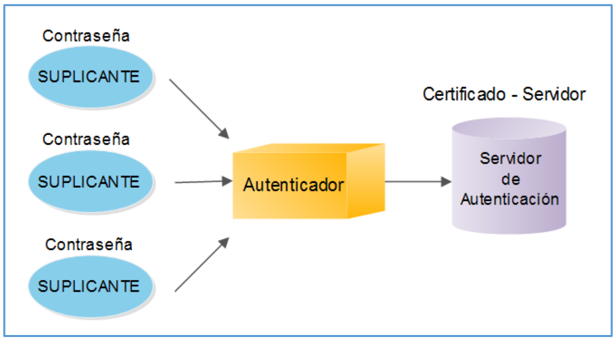


Fig. 3. EAP-TTLS digital certificates

TTLS communication is set in two phases. The first one takes place in the TLS tunnel where the credentials exchange takes place and the client is then authenticated with the server, or vice-versa. This allows the generation of a secure channel using cryptographic mechanisms that will help the information exchange taking place on the following phase.

On the previous phase, the client is authenticated to the server using a less secure mechanism like PAP, CHAP, MS-CHAP so that EAP-TTLS holds authentication database connections keeping at all times secure means for data interexchange.

E. AAA Communication Sequence [5]

Below, the framework process and the Operating System sequencing is described step by step.

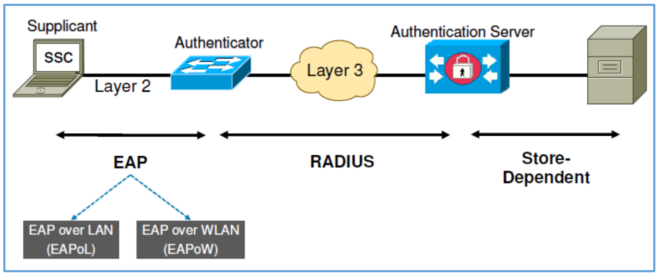


Fig. 4. E. AAA Communication Sequence

1) Communication process begins when the suppliant sends EAPOL – Start package requesting radius client access which means that the “Type” field is a 10 hexadecimal value assigned.

2) In this stage of the process, the authenticator has the access port blocked, it only receives frames 802.1X, and then remaining frames are discarded. At the time the switch receives a EAPOL—Start wave, it requests a suppliant identifier for this process.

3) Using the EAP-TTLS authentication method, an anonymous identity can be used and a secure tunnel is set up so that the user’s name is sent over the device and is protected.

4) The authenticator extracts the received message and it encapsulates it in a RADIUS package. Then data is sent to the server through (AVP) attributes which contain the user’s and equipment information.

5) In this phase, the server initiates the authentication process. In order for the user to identify the authentication method, the server sends the package using the 21 (EAP—TTLS) code and the configured markers are sent by binary numbers that show the message and the TTLSv0 message.

6) Once the EAP process has been initiated, the authenticator stops making decisions and it’s in charge of communicating the user and the server over the EAPOL and RADIUS protocols.

7) When the user receives the initiation message EAP-TTLSv0, the interexchange process begins using the Handshake protocol. This protocol consists of transmitting a sequence of messages to deal with the security parameters pertaining to the TLS session, which in turn is used to transfer data between the user and the server.

8) The server must respond to the welcoming message with a series of packages to include: the message Server Hello, the RADIUS digital certificate and the message: Server Hello Done.

9) The user sends a secret code message exchange generated from received data. Codes then are calculated using random values generated by the Client – Server Hello messages.

10) Before transmitting the secret code to the server, it is digitized over the server’s certificate public code. Both user and server perform the same process locally and get a private code for a secure session.

11) If the server is capable of deciphering data and completes the protocol, the client will be assured that the server has the correct private code. This step is crucial to prove server’s authentication. Only the server with a private code that matches the certificate’s public code can decipher data and continue the TLS/SSL protocol transaction.

12) Once the tunnel is set up, the suppliant utilizes the TLS/SSL channel to send the user’s access (user + passcode) in a secure way.

13) The RADIUS server verifies internally the LDAP directory, provided that the user’s credentials sent are valid, it responds with a EAP Access-Accept message.

14) Finally, the authenticator configures the port state as “authorized” and sends a EAPOL EAP-Success package to the user, informing him that the authentication has been successful.

F. LDAP

It is a light directory access protocol that allows storing information related to an organization in particular, ie: user names, passcodes, digital certificates, email addresses, etc. technical specifications are defined in the RFC 4510-4519.

LDAP is not a relational database; it is a protocol that regulates access to the stored data, optimizing rapid responses to search operations and information-reading searches [6].

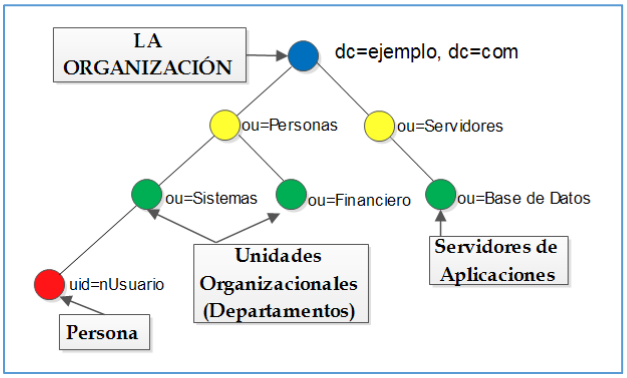


Fig. 5. LDAP Directory

The basic unit within a directory is the entry, which describes real world objects. These objects can be people, departments, servers, printers, etc. an example of a typical directory model may be perceived in Fig 5 that shows some real organization objects.

III. TCP/IP INFRASTRUCTURE NETWORK DESIGN WITH AAA SERVICE

The “San Miguel de Urcuqui’s GAD Municipality” AAA service is designed based on the IEEE 802.1x standard for the network’s access control using the EAP-TTLS authentication method.

A. Technical considerations 802.1x / ttls

The basic components of the 802.1x are: suppliant, authenticator and authentication service. However the raised solution in the GADMU network requires four additional components, a certifying authority, a firewall, a LDAP directory and an SQL database.

- La The CA (certifying authority) is used to generate a digital certificate that the RADIUS server uses during the EAP-TTLS authentication process.
- In the 802.1x architecture, a firewall the plays the router’s function and allows communication between different network zones.
- LDAP directory allows storing of user’s credentials, in fact from al GADMU users and access policies configured over the VLANs assignment.
- The SQL database records authentication equipment and generated information in the authentication process.

B. Supplicant requirements

The installed software in the final-users device is utilized to access wired or wireless networks and it must hold the EAP-TTLS authentication method.

TABLE I
SUPPLICANT REQUIREMENTS

SISTEMA OPERATIVO	EAP-TTLS
Windows XP	SecureW2
Windows 7	SecureW2
Windows 8	Native Client
Ubuntu 12.04 LTS	Native Client
Android OS	Native Client

C. Authenticator requirements

Equipment offering network access service located among user devices on the platform AAA that needs to be authenticated, must comply with the technical requirements specified in TABLE II.

TABLE II
AUTHENTICATOR REQUIREMENTS

REQUIREMENT		DESCRIPTION
RENDIMIENTO		
Ports	▪	48 ports 10/100
	▪	2 ports 10/100/1000
FUNCTIONS		
RADIUS	✓	RADIUS support
Authentication	✓	IEEE 802.1X
VLAN	▪	256 VLAN
	▪	VLAN administration
	▪	Dynamic VLAN assignment by Radius with 802.1x authentication server
Accounting	✓	IEEE 802.1X Acconunting

D. AAA Services requirements

Each one of the AAA services (authentication, authorization and accounting) must comply with the minimum functionality parameters that would allow access and the network resource administration at the GADMU. Requirements are detailed in TABLE III.

TABLE III
AAA SERVER REQUIREMENTS

SERVICES	DESCRIPTION
AUTHENTICATION	
Server	FreeRADIUS
Access control	IEEE 802.1x
Authentication method	EAP-TTLS
Connection	Authenticator (SW CISCO)
AUTHORIZATION	
Server	OpenLDAP
Password storage	MD5 o SHA
Resources assignment	Dynamic VLAN
Connection	FreeRADIUS server
ACCOUNTING	
Server	MySQL
Connection	FreeRADIUS server
FIREWALL	
Zone: wan	Internet Access
Zone: dmz	AAA servers
Zone: local	Supports multiple virtual networks
Inter-VLAN communication	IEEE 802.1Q (Trunk)
Proxy	Transparent mode

IV. AAA SERVER IMPLEMENTATION

In the actual GAD San Miguel de Urcuqui's Municipality's diagram, the AAA service is implemented in a particular way (see figure 6) consisting of equipment with similar characteristics and functions in order to guarantee a feasible solution to the institution's network.

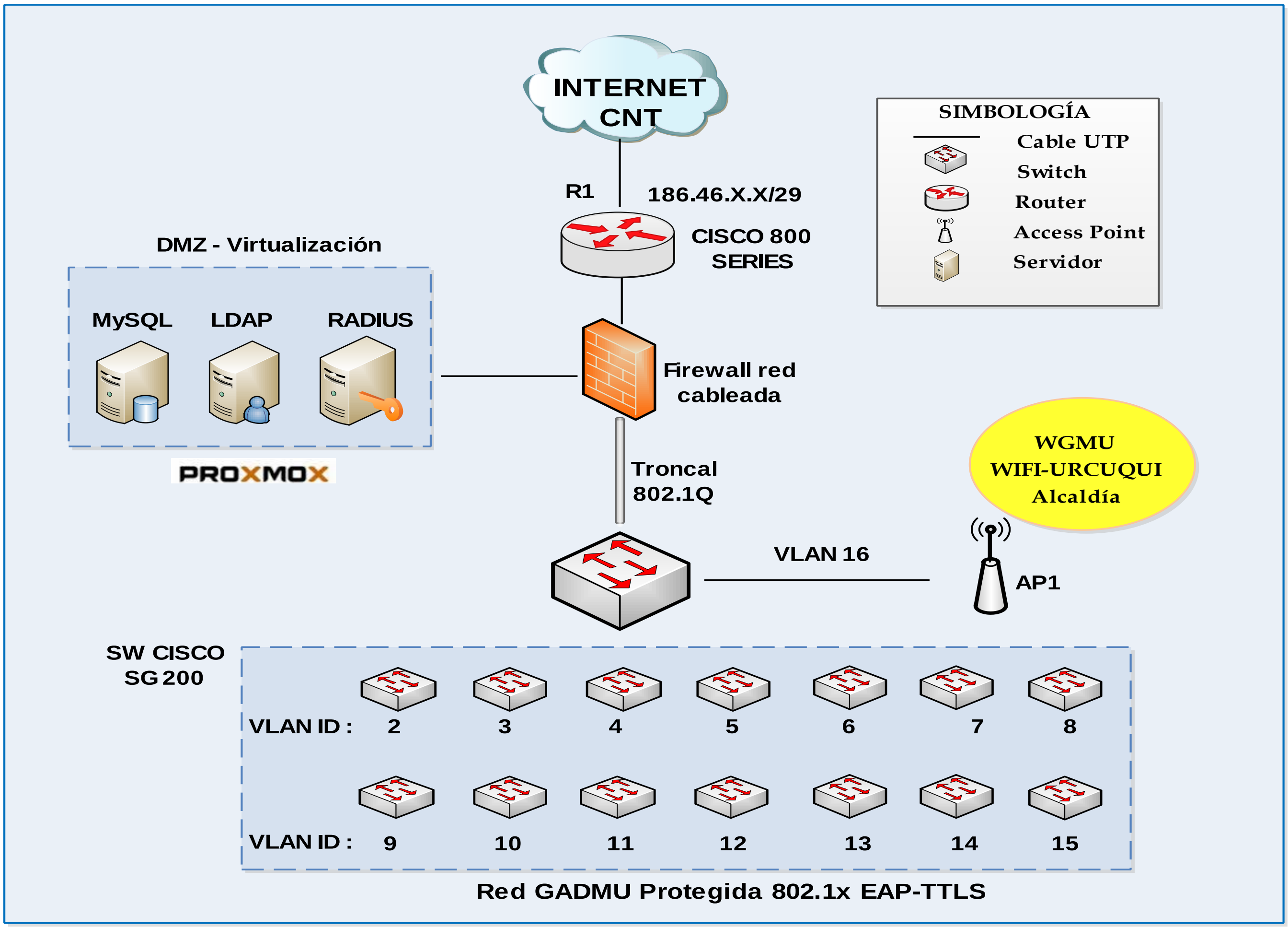


Fig. 6. Integration of the AAA service on the GADMU network

A. AAA Server

It requires three servers installation: Free RADIUS for authentication, OpenLDAP as a directory that stores user's profile, and a MySQL database for client records as well as for the accounting service.

- **Proxmox VE**

In order to optimize hardware use, the Proxmox VE3.0 technology is applied. This technology is one of the best solutions to server's performance. Virtual container technology uses pre-downloaded images able to install Linux operating systems efficiently.

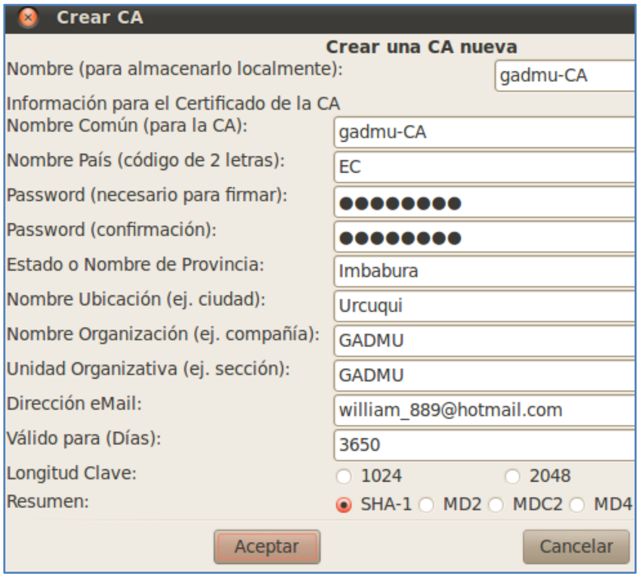
Assignation of hardware resources for Open VZ containers AAA servers is shown in TABLE IV.

TABLE IV
AAA SERVER VIRTUAL RESOURCES

PARAMETERS	FREERADIUS	OPENLDAP	MYSQL
processor	1	1	1
storage	6 GB	6 GB	6 GB
RAM memory	512 MB	512 MB	512 MB
Node	proxmox-aaa	proxmox-aaa	proxmox-aaa
template	Ubuntu 12.04	Ubuntu 12.04	Ubuntu 12.04
swap	512 MB	512 MB	512 MB
vmid	200	210	220

- **TinyCA2 digital certificates**

Using TinyCA2 a main certifying authority is created at the "GAD Municipality of San Miguel de Urcuqui" in order to release and manage the certificate system required by the institution's services.


Crear CA

Crear una CA nueva

Nombre (para almacenarlo localmente):	gadmu-CA
Información para el Certificado de la CA	
Nombre Común (para la CA):	gadmu-CA
Nombre País (código de 2 letras):	EC
Password (necesario para firmar):	●●●●●●●●
Password (confirmación):	●●●●●●●●
Estado o Nombre de Provincia:	Imbabura
Nombre Ubicación (ej. ciudad):	Urcuqui
Nombre Organización (ej. compañía):	GADMU
Unidad Organizativa (ej. sección):	GADMU
Dirección eMail:	william_889@hotmail.com
Válido para (Días):	3650
Longitud Clave:	○ 1024 ○ 2048
Resumen:	● SHA-1 ○ MD2 ○ MDC2 ○ MD4

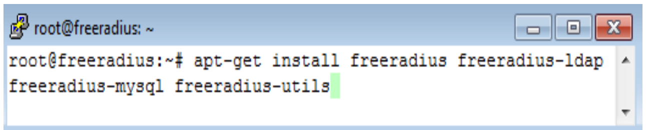
Fig. 7. Certificate Authority TinyCA2

The main gadmu-CA certificate is installed in the clients' reliance certificates repository EAP-TTLS allows the user verify that the authenticating server is real thus avoiding exposure to access codes to just anybody.

- **FreeRADIUS Server**

Free RADIUS is a standard package for multiple operating systems that allows high-scale installations using multiple AAA servers. It holds a variety of database connections, for both the authorization and accounting. It is compatible with a high number of authentication methods which as a set, they form a AAA robust and trustworthy system.

The server and its dependencies may directly download from the repositories over the command shown in Figure 8. One of the great advantages that Ubuntu Server 12.04 presents (as base operating system) is the current repository management which expedites the installation of any software and its dependencies.



```
root@freeradius:~# apt-get install freeradius freeradius-ldap
freeradius-mysql freeradius-utils
```

Fig. 8. Installing FreeRADIUS on Ubuntu Server 12.04 LTS

- **OpenLDAP Server**

The GAD San Miguel de Urcuqui's Municipality does not count with a user directory to store required access credentials for the authentication process directed to the database so a directory must be created using OpenLDAP server [7].

The directory's diagram (see Fig. 9) is designed using as reference the institution's departmental units then a group of users is generated for each VLAN. Passwords will be set up and stored following security policies recommendations.

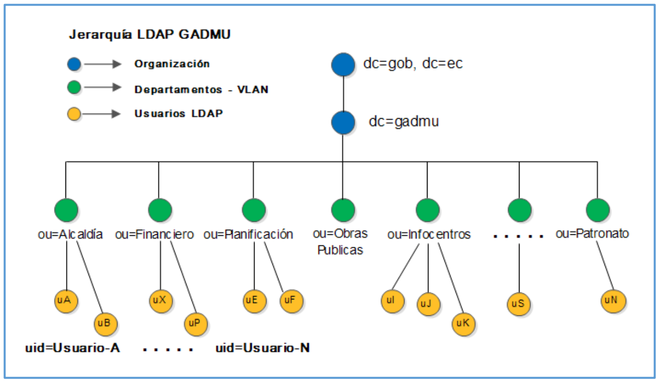


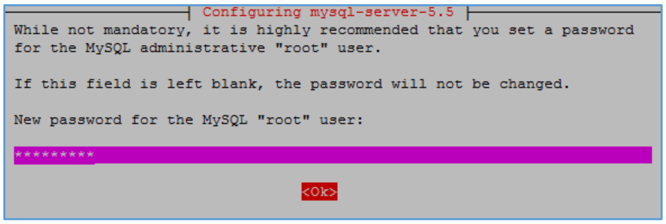
Fig. 9. LDAP GADMU directory structure

- **MySQL Server**

MySQL is an open management system for relational databases. Data is stored in separate tables in order to access to information in a quick and flexible way.

Free RADIUS has the capacity to use MySQL as database for the authentication process and accounting in the AAA service. Free RADIUS installation includes configuration scripts that automatically create tables for data entry.

To install MySQL, lamp-server package is downloaded; a combination of software based on an open code that includes: HTTP apache server, the MySQL database and extra components are required for the building of a database that will be used to process AAA accounting service.



```
                 ┤ Configuring mysql-server-5.5 ├
While not mandatory, it is highly recommended that you set a password
for the MySQL administrative "root" user.

If this field is left blank, the password will not be changed.

New password for the MySQL "root" user:

*********

                               <Ok>
```

Fig. 10. Password MySQL root

Once the MySQL server is prepared, a RADIUS database must be created. FreeRADIUS embodies SQL scripts to atomize this process.

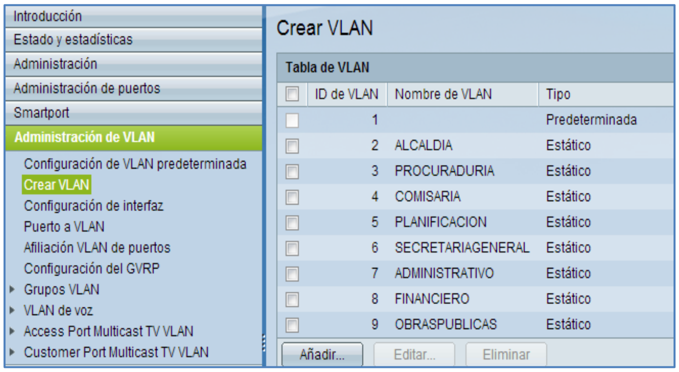
B. Wired authenticator

The 802.1x service implementation is performed in the “Cisco Small Business SF300” switch; network switch that operates as a layer 2 or 3 mechanism according to its own configuration.

- **VLAN**

In order to achieve communication among different hardware, VLANs, the use of a layer three mechanism is required to direct packages of various networks routing processes. The port’s router must abide with IEEE 802.IQ protocol’s mechanism and allow sharing multiple networks with transparency in the same physical environment without causing interference problems among the networks [8].

The IEEE 802.1Q standard implementation is done at the GNU/Linux firewall’s “eth0” port. In order to activate the service, basic requirements must be configured so that virtual interfaces are enabled in the Ethernet’s red card.



Introducción
Estado y estadísticas
Administración
Administración de puertos
Smartport
Administración de VLAN
Configuración de VLAN predeterminada
Crear VLAN
Configuración de interfaz
Puerto a VLAN
Afiliación VLAN de puertos
Configuración del GVRP
Grupos VLAN
VLAN de voz
Access Port Multicast TV VLAN
Customer Port Multicast TV VLAN
Añadir...
Editar...
Eliminar

Crear VLAN

Tabla de VLAN

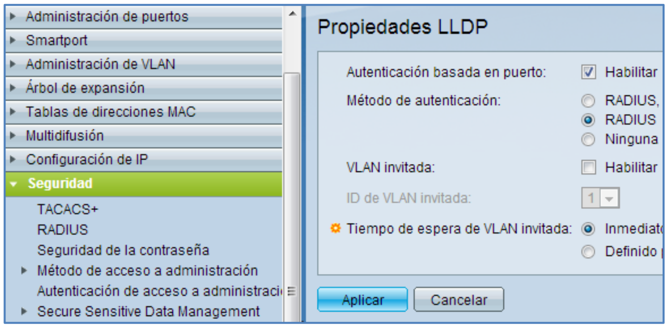
□	ID de VLAN	Nombre de VLAN	Tipo
□	1		Predeterminada
□	2	ALCALDIA	Estático
□	3	PROCURADURIA	Estático
□	4	COMISARIA	Estático
□	5	PLANIFICACION	Estático
□	6	SECRETARIAGENERAL	Estático
□	7	ADMINISTRATIVO	Estático
□	8	FINANCIERO	Estático
□	9	OBRASPUBLICAS	Estático

Fig. 11. VLANs on switch cisco FS-300

- **802.1X**

To activate RADIUS service, first one must go the access menu and type: Security > RADIUS> Add.
On the main page the main parameters must be set up to the FreeRADIUS server which is used as GADMU’s server network for authentication.

After the RADIUS server has been added, standard IEEE 8012.1X parameters must be set up globally and in each port individually in the SF-300 switch.



Administración de puertos
Smartport
Administración de VLAN
Árbol de expansión
Tablas de direcciones MAC
Multidifusión
Configuración de IP
Seguridad
TACACS+
RADIUS
Seguridad de la contraseña
Método de acceso a administración
Autenticación de acceso a administraci
Secure Sensitive Data Management
Aplicar
Cancelar

Propiedades LLDP

Autenticación basada en puerto: ☑ Habilitar

Método de autenticación: ○ RADIUS, ● RADIUS ○ Ninguna

VLAN invitada: □ Habilitar

ID de VLAN invitada: 1

Tiempo de espera de VLAN invitada: ● Inmediat ○ Definido

Fig. 12. 802.1X on switch cisco FS-300

In the section: Security > 802.1X > Port’s Authentication. Parameters for the standard 802.1X must be defined for each port.

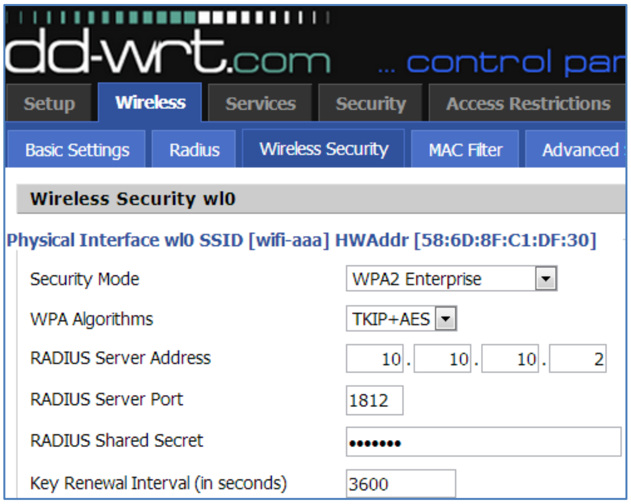
1) Puerto: Port: Select front end’s switch to enable authentication
2) Administrative port control: automatic mode makes the front end change from authorized to not authorized, according to the package exchange between the switch and the user.
3) RADIUS VLAN Assignment: VLAN assignment dynamic works exclusively as the 802.1X mode is set up in “multiple” mode or session. This option links an authenticated port to a VLAN assignation automatically.

The attributes that the server must send to the switch are: Tunnel-Type= VLAN, Tunnel-Medium-Type= 802 and Tunnel-Private-Group-Id = VLAN ID.

C. *Wireless authenticator*

As wireless authenticator, the AP Linksys WRT-54GL router is used. It utilizes a hardware Linux compatible, which allows charging of a firmware different from the original. The Operating System that approves its functionality is DD-WRT, a Linux based firmware released under GPL licensing, and files must be downloaded from its official page in order to install it. . To uploaded to the AP from the menu: Administration > firmware Upgrade > Select file > Upgrade.

In the menu: Wireless > Wireless Security, a “WPA2-Enterprise” is established as a security mode by default to the wireless users, using TKIP and AES algorithms together to reach better compatibility. In Fig 13 all AP WRT-54GL configured parameters can be seen.



Wireless Security wl0

Physical Interface wl0 SSID [wifi-aaa] HWAddr [58:6D:8F:C1:DF:30]

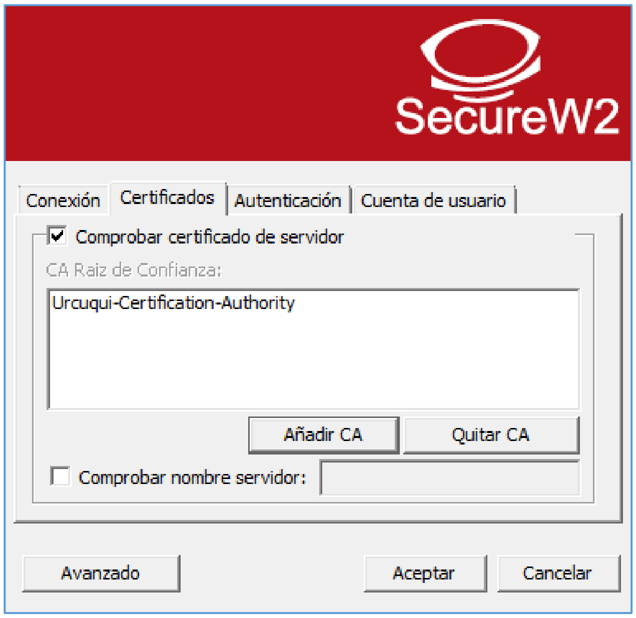
Security Mode: WPA2 Enterprise
WPA Algorithms: TKIP+AES
RADIUS Server Address: 10 . 10 . 10 . 2
RADIUS Server Port: 1812
RADIUS Shared Secret: •••••••
Key Renewal Interval (in seconds): 3600

Fig. 13. RADIUS configuration on AP WRT-54GL

D. *Supplicant*

To access a AAA system’s protected network, users require an additional software (suppliant) that back up the EAP-TTLS authentication implemented method. Any device that does not comply with this requirement will not be able to connect to the network.

Secure W2 is a TTLS client of the Windows platforms. In the case of operating systems as GNU/Linux or Android the TTLS installation is not necessary since it holds its own bearer for this type of authentication; even Windows 8 latest version has it by default.



☑ Comprobar certificado de servidor

CA Raiz de Confianza:

Urcuqui-Certification-Authority

☐ Comprobar nombre servidor:

Fig. 14. Supplicant SecureW2

E. Firewall-Shorewall

Shorewall is an open code tool that allows the creation of hardy firewalls over GNU/Linux firewalls. It is based on the Netfilter/iptables system integrated by default in the Linux kernel. Is in this system where rules and policies are defined and package management takes place.

Configuration and administration of Shorewall is done with the Webmin tool and the general procedure to be followed is detailed above:

- Editing of basic parameters to activate the Shorewall service within the Ubuntu Server.
- Defining network zones: WAN, LAN, DMZ, FW, and VLANs.
- Adding interphases to the network that Shorewall will use for rules and policies for firewall management.
- Setting up default actions for firewall traffic zones.
- Defining rules that allow access to services or ports from and to firewall zones.

V. CONCLUSIONS

With the AAA server’s implementation using free-based software, users’ access control was achieved in a centralized way. Network’s resources assignation was done successfully according to each employee’s role within this institution, obtaining a cost-benefit relation that guarantees project viability.

It was determined that the EAP-TTLS authentication method is the most adequate and safe in which the AAA system may be implemented at ”GAD” Municipality of San Miguel de Urcuqui”. Additionally through a secure channel digital certificates guarantee the authentication process confidentiality.

Integrating the RADIUS server with the LDAP directory, a AAA centralized administration system was created, synchronizing user’s authentication accounts with privileged access for the authorization process.

User Access was denied to those who did not comply with authentication requirements. Eventually they were reassigned using VLAN virtual networks.

The three servers that provide authentication, authorization and authentication in the GADMU were installed over the PROXMOX—virtual environment. This process guarantees significant cost-reductions at the implementation phase.

When a LDAP directory stores user’s credentials, the system automatically stores users passwords using hash algorithms. Since hash are irreversible, it is necessary to select PAP as the internal authentication method inside the TLS tunnel.

Data accounting is registered in a SQL relational database providing the authenticator device (wireless router or switch) is capable of sending data related to the 802.1x server. Otherwise, the network administrator may administrate the service using log records that, by default generates the Free RADIUS server.

The authenticator hardware used in the implementation system hold the accounting service 802.1x server, which allows registration of users to the MYSQL database. Failed connections intents are recorded and dated.

During access code testing, W7 Operating System was used, since it does not have a EAP-TTLS defaulted authentication method, thus a suppliant must be installed to enhance functionality. Software used was SecureW2.

VI. REFERENCES

[1] Fernández, Y., Ramos, A., & García, J. (2008). *RADIUS / AAA / 802.1X : Sistemas basados en la autenticación en Windows y GNU/Linux.* Madrid: RA-MA Editorial.

[2] Rigney, C., Willens, S., Rubens, A., & Simpson, W. (Junio de 2000). *Remote Authentication Dial In User Service (RADIUS).* Obtenido de http://tools.ietf.org/pdf/rfc2865.pdf

[3] *IEEE Standard for Local and metropolitan area networks: Port-Based Network Access Control.* (2 de Febrero de 2010). Obtenido de IEEE Std 802.1X-2010: http://standards.ieee.org/getieee802/download/802.1X-2010.pdf

[4] Funk, P., & Blake, S. (Agosto de 2008). *Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0).* Obtenido de http://tools.ietf.org/pdf/rfc5281.pdf

[5] Nakhjiri, M., & Nakhjiri , M. (2005). *AAA and Network Security for Mobile Access: Radius, Diameter, EAP, PKI and IP Mobility.* USA: John Wiley & Sons Ltd. doi: 10.1002/0470017465.

[6] Howes, T., Smith, M., & Good, G. (2003). *Understanding and Deploying LDAP Directory Services* (2nd ed.). Boston: Pearson Education, Inc.

[7] Butcher, M. (2007). *Mastering OpenLDAP: Configuring, Securing, and Integrating Directory Services.* Reino Unido: Birmingham: Packt Publishing Ltd.

[8] CISCO. (2008). *CCNA 3 Exploration 4.0: Conmutación y conexión inalámbrica de LAN.* Obtenido de http://es.scribd.com/doc/17481738/Cisco-CCNA-3-Exploration-Conmutacion-y-Conexion-Inalambrica-de-Lan-Version-40-Espanol

VII. BIOGRAPHY

Director – Ing. Carlos A. Vásquez A. Born in Quito, province of Pichincha on September 19, 1980. Engineer in Electronics and telecommunications of the “Escuela Politécnica Nacional” in 2008. Currently, teacher of the Electronics and Communication Networks career (UTN), Ibarra -Ecuador, and master degree in Communication and Networks in the "Pontificia Universidad Católica del Ecuador", Quito-Ecuador.

William E. Vaca A.
Born in Ibarra , province of Imbabura on May 7, 1988. Son of Germán Vaca and Guadalupe Aguirre. He studied in the “Teodoro Gómez de la Torre " school, Ibarra - Ecuador.
He studied Electronics and Communication Network Engineer at the Técnica del Norte University”, Ibarra - Ecuador.