ACCESS NETWORK IMPROVEMENT FOR A WLAN BASED ON 802.1X AND CAPSMAN PROTOCOLS

Fabián Cuzme-Rodriguez[1], Carlos Pupiales-Yépez[1], Mauricio Dominguez-Limaico[1], Carlos Bosmediano-Cárdenas[1] and Walter Zambrano-Romero[2]

[1]Universidad Técnica del Norte, Facultad de Ingeniería en Ciencias Aplicadas, Ibarra-Ecuador
[2]Universidad Técnica de Manabí, Portoviejo-Ecuador

ABSTRACT

This article describes the implementation of a method to access to a wireless network based on Radius with Mikrotik equipment. It is applied EAP-TTLS authentication based on open source software to provide AAA services and a LDAP directory to save user's accounts. This approach allows a better access control and distribution of network resources. As a plus, the work includes the implementation of Mikrotik's CAPSMAN protocol which enablesa centralized control of all access points (AP) emitting the same SSID. This proposal improves the performance of the network and user´s experience.

KEYWORDS

Radius, Mikrotik, EAP-TTLS, 802.1x

1. INTRODUCTION

Since wireless devices showed up, network designers have developed different approaches to guarantee those devices can have access to the services offered by a wireless network. The access to the network is done by a wireless access point which establish centralise and manage the working rules applied in the network. Contrary to a LAN, a WLAN offers several advantages to users and network managers such as nomadicity, deployment reduction costs, and scalability; however, the main disadvantage of wireless networks is the data vulnerability due to RF waves can be detected by anyone at any moment inside the coverage zone. Therefore, it is mandatory to implement access policies to avoid eavesdroppers can steal valuable information of our networks. Currently is common to find wireless networks in public and private spaces that offers free access to the Internet where users enter their personal information; for this reason, it is significant to implement robust and mores trusted access mechanisms such as Radius or Kerberos.

Several works show that wireless networks are unsafe thus it is necessary to implement security approaches to avoid informatics attacks or in the worst case, reduce the effects of those attacks. [1] Proposes the implementation of an open code server, DIAMETER EAP, for authentication and authorization of remote users from the networks of a large corporation. Additionally, [2] states that information security plays an important role in any network because it guarantees the integrity and confidentially of data; in fact, the 802.1x protocol gives the network the ability to

David C. Wyld et al. (Eds) : AI, CSTY, NMOCT - 2018
pp. 43–49, 2018. © CS & IT-CSCP 2018 DOI : 10.5121/csit.2018.81405

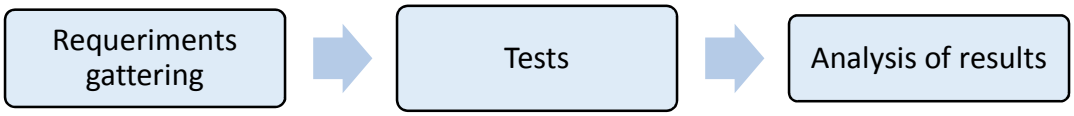
control the access based on ports due to all traffic is denied if users have not been authenticated in the authentication server first.

There are technological solutions implemented in government agencies that try to solve both security and access issues in a wireless network; for instance, [3] has developed a solution based on CAPsCAN and RouterOS which substantially improves the access and security aspects of the networks. Moreover, [4] uses CAPsCAN, WDS, and NDLC to solve similar issues presented in [3], but in this case the offered solutions is implemented in a university campus. Even though network managers implement security policies in wireless networks, the network itself might be still vulnerable due to new and sophisticated methods and tools used in ethical hacking; therefore, it obligates to create stronger and dedicated authentication mechanism that fit to the application and service where it will work. For example, [4] points out that in the authentication mechanism RADIUS the access points are authenticated by a shared static key which is not suitable for wireless networks; for this reason, it is possible to use the approach TPM, Trusted Platform Module, besides the authentication by RADIUS only.

This work is focused on improving the performance and user's experience of FICA's WiFi network which has approximately 2000 users distributed into students, teachers, and administrative personnel who access to the offered services by a simple Hotspot system as the only management tool used to discriminate against traffic, priorities, and bandwidth. This approach is valid for low traffic patterns; however, the number of electronic devices and users that try to access to the network is increasing constantly which cause that the simple Hotspot approach becomes inefficient because of the equipment's overheat, service unavailability in peak hours, 10 am – 1 pm, and a very low performance of the network all day long. Therefore, we propose a scenario where the access to the network is based on a Radius server, 802.1x protocol, and a simple queues to allow users to access to the network with their own credential that makes possible to control the data rate users obtain and can reach.This paper is structured as follows. Section 2 describes briefly the problem this works intents to solve. Section 3 specifies the approach and tools used to improve the performance of the network. Additionally, section 4 shows the results obtained before and after the implementation of the proposed approach and finally section 5 concludes the work with recommendations and future work.

2. PROPOSAL AND METHODOLOGY

This work uses an exploratory and analytic methodology where we explore new solutions to solve the problem of access control that a real network has. We follow the following process:



To address the inefficiency of access control and low performance of the network, this work proposes to implement the 802.1x protocol and the authentication mechanism EAP-TTLS in a centralized server which will be attached to every single access point, of the brand Mikrotik, in the network. The implementation considers the following features:

- The devices allowed to connect to the networks are laptops, tablets, and smartphones.
- Authenticator devices, APs, must support the management system CAPsCAN, RouterOS, and 802.1x protocol.

- The authentication server will be developed entirely in an open source software.

It's important to remark that we applied a combined protocol which consist of two stages. The first one establish the TLS tunnel with security in the transport layer. The last one, consist of encapsulate the TLS connexion using the EAP method. This approach reduces the system complexity since the radius server requires only one digital certificate to authenticate the user instead of sending several certificates to all the devices attached to the network.

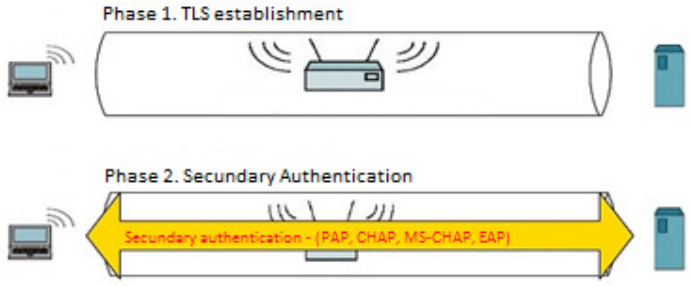


Figure 1. EAP-TTLS Method

2.1. Requirements

2.1.1. SUPPLICANT

The devices allowed to connect to the network must support as operative system at least Windows 8, any distribution of Linux, and Android 1.6. IOS does not need additional software to perform the authentication. For previous and different versions of Windows and Linux it is mandatory an additional software that supports EAP-TTLS. Table 1 specifies those requirements.

Table 1. Technical requirements for Supplicant.

Operative System	EAP-TTLS
Windows 7	SecureW2
Windows 8 / 8.1	Native Client/ SecureW2
Windows 10	Native Client
Ubuntu/Debian/Centos	Native Client
Android OS/ IOS (Iphone-OS)	Native Client

2.1.2. Authenticator (Access Points)

The access points involved in the solution are Mikrotik model CAP-2n and routerOS RB1100. These were chosen because they offer a simple adaptation to a centralized management model such as CAP mode, because routerOS gets along with 802.1x and CAPsCAN mode.

2.1.3. Authentication server

In the authentication server will be running the OS Debian 8, the application FREERADIUS, and the active directory LDAP. The server should has as technical features to respond the requests from all users at least a hard-disk with 10 GB free for storage, processor' speed of 2 GHz, and 1GB in RAM memory. The chosen equipment counts with 3.5 GHz in the processor, 2 GB as RAM memory, 100 GB free in the hard disk, and a Gigabit Ethernet interface.

2.2. Physical and Logical Topology

The initial and the final scenarios have almost the same topology; however, the difference in each scenario is how equipment are connected and configured.

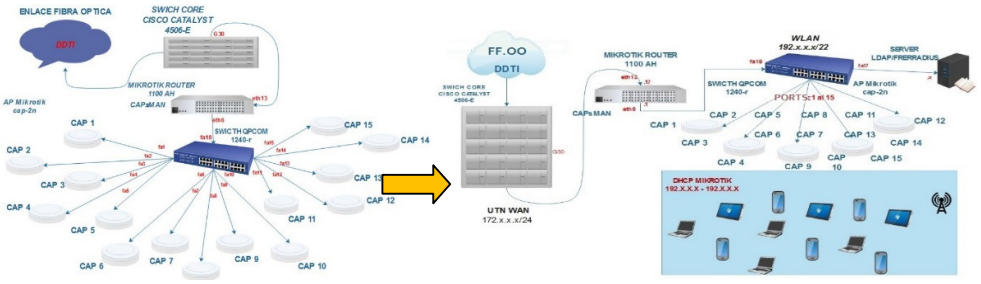


Figure 2. Topologies before and after implementation

2.3. Authentication Server

- **FreeRADIUS:** All dependencies and packets can be extracted from their own data repository using the procedure showed in figure 2. The advantage of using Debian 8 – Jessie as primary operative system is the it is available for both 32 bits and 64 bits architectures which reduces time at the moment of installation and configuration of any software and their dependencies.

- **OPENLDAP:** FICA's WiFi does not have user's directory to save the access credentials used in the authentication process, thus we create a directory using OpenLDAP. The structure of the data base implemented in the network "ficawifi" is showed in figure 3.

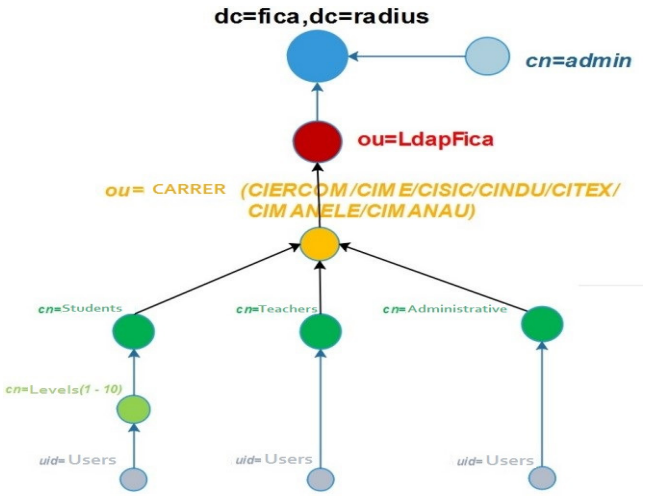


Figure 3. Hierarchical structure LDAP - FICA

Once the service LDAP has been installed, it is necessary to add certain information to its main file by using the command ***dpkg-reconfigure slapd.*** The information filled in the file is:

- Domain name: utn
- Organization name: fica.radius
- Password: ****
- Database engine: MDB

Additionally it is mandatory to enable de purge of ***slapd*** packets and avoid ***LDAPv2*** protocol.

2.4. Authenticator (CAP andCAPsMAN)

There are 15 APs available in the wireless network which must have the same SSID, so every AP is configured in CAP mode. This allows the routerOSMikrotikto manage the APs by CAPsMAN. All APs should be in the same network domain so that every AP can communicate to each other. This can be done configuring a fixed-IP or with a VLAN in CAP mode. Additionally, the mode CAPsMAN must be enabled to have a centralized management of the network. This configuration is presented in figure 4.

Name	SSID	Channel	Datapath	Security
cfg-AP1	ficawifi	channel1	datapath1	RadiusPASS
cfg-AP2	ficawifi	channel11	datapath1	RadiusPASS
cfg-AP3	ficawifi	channel6	datapath1	RadiusPASS
cfg-AP4	ficawifi	channel11	datapath1	RadiusPASS
cfg-AP5	ficawifi	channel6	datapath1	RadiusPASS
cfg-AP6	ficawifi	channel9	datapath1	RadiusPASS
cfg-AP7	ficawifi	channel1	datapath1	RadiusPASS
cfg-AP8	ficawifi	channel6	datapath1	RadiusPASS
cfg-AP9	ficawifi	channel11	datapath1	RadiusPASS
cfg-AP10	ficawifi	channel6	datapath1	RadiusPASS

Figure 4. Configuration parameters for every CAP

According to a first analysis, the occupancy of the network is distributed in 80% for students and 20% for teachers and administrative personnel. This initial analysis would state that students need more data rate than teachers; however, both students and teachers should have the same privileges in terms of data rate and connection. The easiest way to limit the data rate is using simple queues; for this reason, we create two queues for teachers and students.

3. RESULTS

The success of the approach implemented in this work is measured in terms of user's perception and data rate control.

3.1. Perception of the user

To know how users react to the changes in the network, we use the simple approach of interviews. The sample for the analysis is 66 users who are interviewed before and after the implementation of the proposed solution. The period of analysis is from March to August of 2017 and the analysed points are:

- What was the user's experience regarding service unavailability, network coverage, and web browsing?

- Which were the uplink and downlink data rates?

- Conclusion after interviews show that for users the parameters network performance and data rates improved significantly with the implementation of a better network access approach. The results are presented in table 2.

Table 2. User's perception before and after implementation

Parameter	Hotspot			Radius		
	B	G	E	B	G	E
Network Performance	67%	25%	8%	22%	40%	38%
Data rates	57%	38%	5%	10%	54%	36%
B: Bad **G: Good** **E: Excellent**						

3.2. Data Rate Control

In the first stage of the study, between February and March 2017, it is noticeable the inefficient use of resource due to there was not a control for assign data rates. Users used to be able to connect several devices with the same credentials. The effects of this problem was reflected as an uncontrolled assignment of bandwidth for present and future users; in fact, a single user used to use a large proportion of channel bandwidth while others used to be assigned with just few kbps for navigation.

After applying the Simple Queues approach in the Mikrotik router we got excellent results in the period July – August 2017 that can be synthetized as follow:

- The data rate assigned for each user was 6 Mbps in July and the first days of August instead of the 13 Mbps usedin the first stage of the study. Now the average number of users are 150 who are assigned with the bandwidth they request and which is enough for their application thus all users can access to the network and traffic patterns are distributed in a better way.

It is significant to remark that even though the data rate itself decreases, the efficiency in the assignment of it increases being more than enough 6 Mbps. Figures 5 and 6 show the traffic pattern before and after the implementation of simple queues approach, 802.1x, and network segmentation.

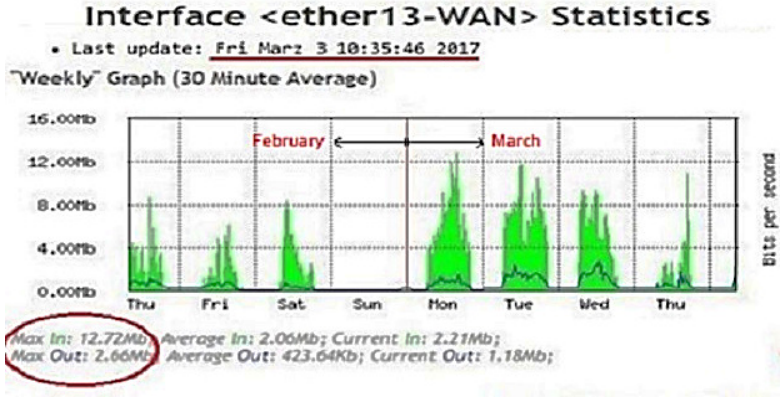


Figure 5. Traffic pattern before implementation

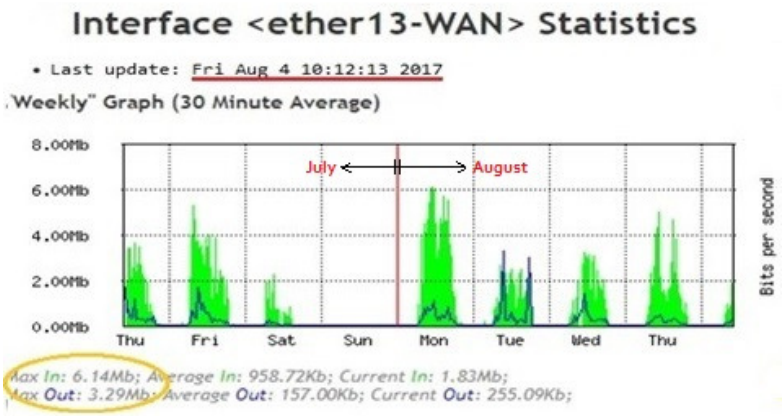


Figure 6. Traffic pattern after implementation

4. CONCLUSIONS

With the implementation of the proposed approach was possible to reach a network performance of 78% comparing to the 34% of performance gotten with the access based on a simple hotspot. Additionally, now data rates for downlink and uplink are assigned more efficiently since users do not share the same credential which used to congest the network. As a consequence, more users can have access to the services offered by the network.

ACKNOWLEDGEMENTS

We would like to thank to Universidad Tecnica del Norte from Ecuador for the strong support for the development of this article.

REFERENCES

[1] Wu, W. T., Chen, J. C., Chen, K. H., & Fan, K. P. (2015, June). Design and implementation of WIRE Diameter. In Information Technology: Research and Education, 2015. ITRE 2015. 3rd International Conference on (pp. 428-433). IEEE.

[2] Qian, Q., Li, C., & Zhang, X. (2013, August). On Authentication System Based on 802.1 X Protocol in LAN. In Internet Technology and Applications, 2013 International Conference on (pp. 1-4). IEEE.

[3] García V. R., (2018). Análisis de implementación de una red CAPsMANMicroTik en el Gobierno Autónomo Descentralizado Provincial de los Ríos. Tesis de pregrado.

[4] Santi DwiRatnasari, E. F., (2017), Implementación de CAPsCAN y Sistema de Distribución Inalámbrica WDS en SMK Integrado al ISHLAHIYAH SINGOSARI MALANG.