Analysis and Implementation of the Authentication Protocol 802.1x

A. I. A. Jabbar, Ph.D
Assistant Professor
Department of Electrical Engineering
Mosul University

Harith G. A.
M.Sc. Student
Department of Electrical Engineering
Mosul University

ABSTRACT
The security of wireless networks against hacker attacks depends on some parameters and special configurations. Authentication is considered as one of the most important security parameter in computer networks [1]. The communication for example between users through the internet must be authenticated by both sides in order to prevent hackers from pretending any one of them [2]. Authentication process has the function to allow or prevent users from accessing the wireless network like IEEE 802.11b or 802.11g, it can be applied also to wired networks [3].

IEEE 802.1X [4] is the famous standard which uses Extensible Authentication Protocol (EAP) to authenticate users before giving them access to the network [5]. The process of authentication is extended to include RADIUS protocol which is designed to authenticate remote users within special organizations, then upgraded to include most of the operating systems and computer networks. It is now the most famous and applicable protocol for authenticating remote users [6].

Recently, the operating system Android has dominated other operating systems, it is based on Linux core and has the capability to support 802.1x and other security protocols [7]. In this paper, 802.1x protocol is applied to authenticate users using windows 7 and Android operating systems, a comparison to show the main differences between them is introduced successfully in mixed (computer & mobiles) network.

Keywords
IEEE 802.1x, EAP, RADIUS, Ubuntu, PEAP, MS-CHAPv2, ANDROID, IOS, Windows 7

1. INTRODUCTION
The first element of the IEEE 802.1X protocol is the supplicant, which is the device that wants to join the computer network. The second element is the authenticator, which is the device or controller that controls access to the network. The third element is the authentication server [8].

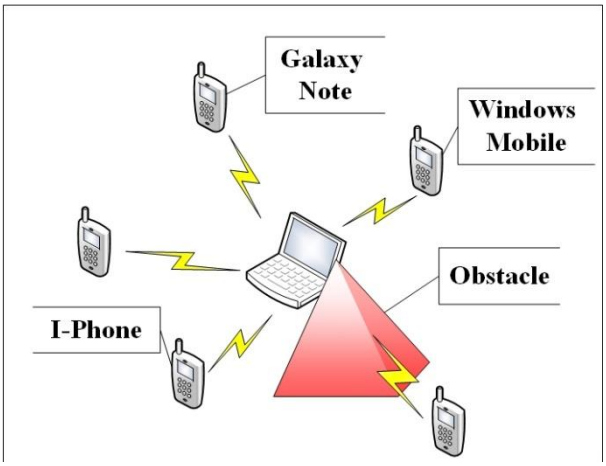
It is worth to mention that the Security Protocol IEEE 802.1X can be obtained by installing FreeRADIUS (the most widely deployed RADIUS server in the world) onto the free operating system Ubuntu server [9].

The rapid deployment of 802.1x in the internet applications generates what is called daloRADIUS which is an advanced RADIUS web platform. It provides efficient user management, accounting, graphical reporting, and can be integrated with Google Maps for geo-locating (GIS). daloRADIUS can be written either in PHP or in JavaScript, It is based on a FreeRADIUS and can support many database systems like the popular MySQL, MsSQL, and many others [10].

Practically, windows 7 and Android operating systems are provided with the necessary software's to authenticate subscribers using 802.1x protocol. Conventionally, if the authentication server is installed on the desktop (stationary server) then it is possible to authenticate users within pure computer networks or within a mixed (mobile & laptop) network reliably. Installing the Android sever software in portable laptop may suffer from some difficulties because of its variable position, this may cause the portable server to be a hidden terminal to the other users leading to a failing authentication process. In this paper, a pure mobile network is designed and implemented practically showing the successful and failing authentication processes.

2. THE PROPOSED MOBILE NETWORK
The mobile network shown in Figure 1 is designed according to the following assumptions: -

1. The number of mobiles is equal to 8.
2. The protocol of authentication provided by Android is installed on a portable laptop.
3. The area of the network is equal to $100m^2$.
4. The hidden terminal problem may be existed according to the positions of the mobiles with respect to the obstacles within the area. Figure 1 shows a possible subscriber distribution within the proposed network.
5. The supporting protocols associated with 802.1x protocol are Protected EAP (PEAP) and MS-CHAPv2.
6. Samsung Galaxy, iPhones and laptops are the types of mobiles being used with the operating systems Android,



3. THE INSTALLATION PROCESS OF 802.1X

Wireless networks provide an alternative networking option when traditional wired networks are impractical. The Ubuntu Server is the operating system which provides secure wireless local area network (WLAN). The flowcharts shown in Figure 2 provide comprehensive guidance on how to install the 802.1X protocol (Successful & Failure Authentication process) onto portable laptop.

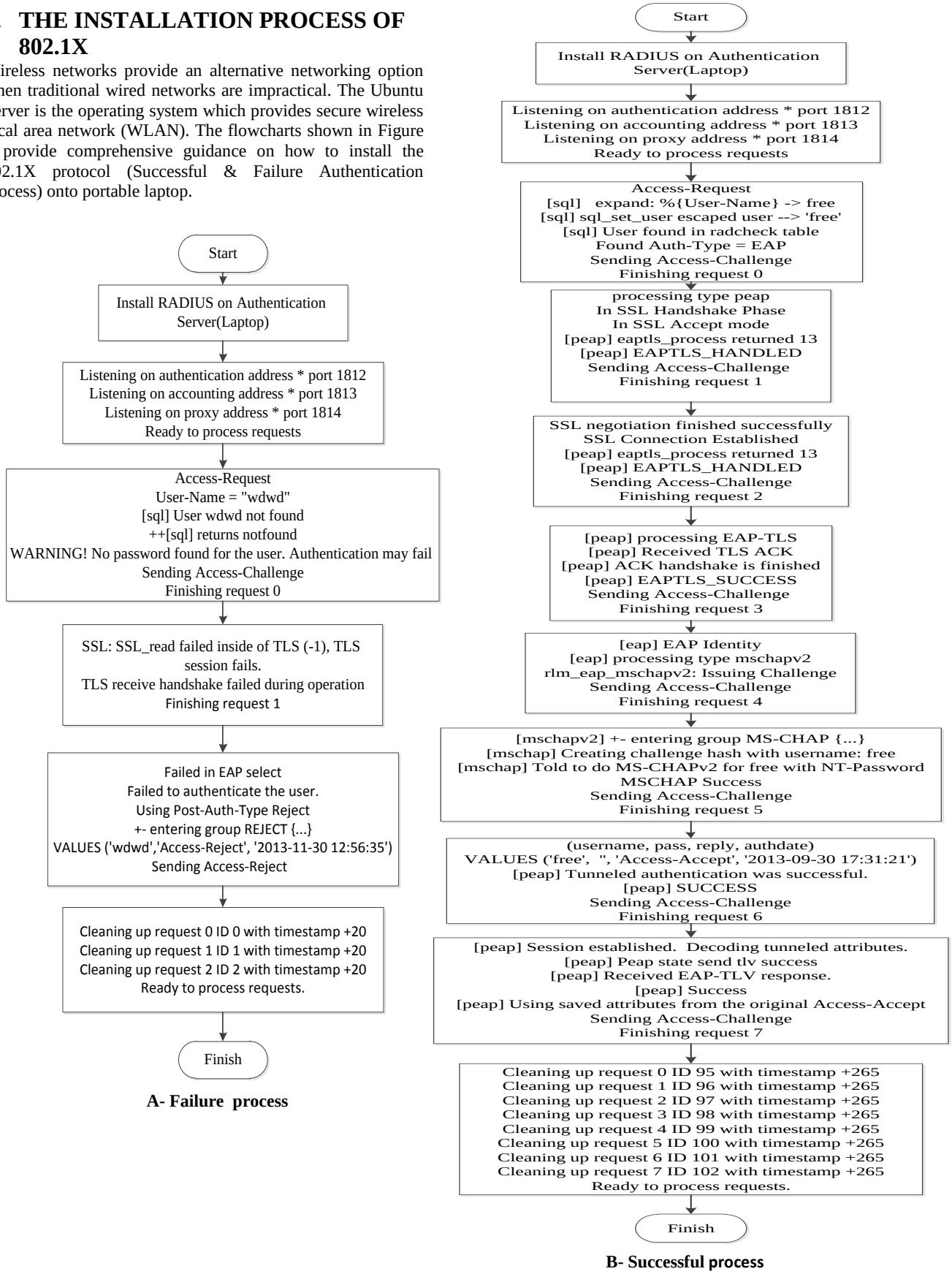


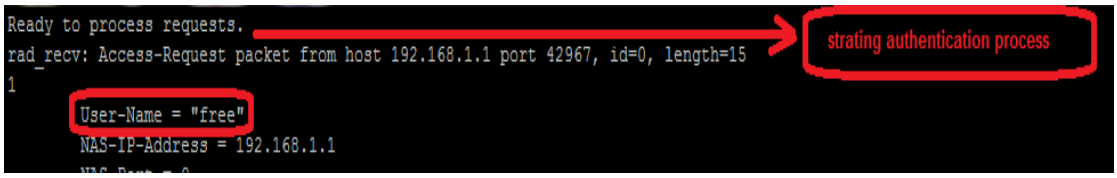
Fig 2: Successful and Failure processes according to the 802.1X protocol

4. PRACTICAL RESULTS

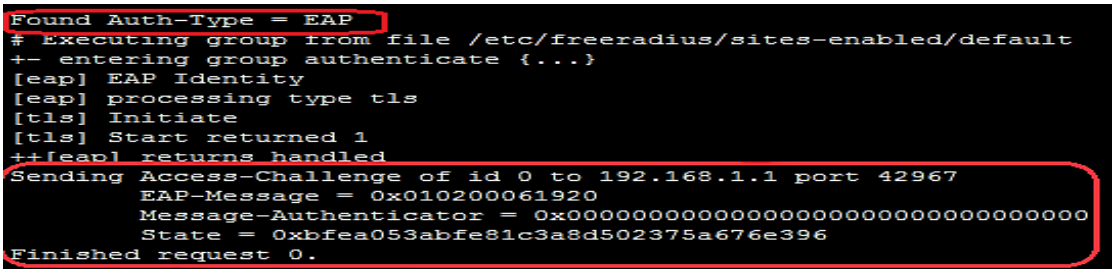
4.1 Successfully access process

As mentioned in the figure 2, The Authentication between the portable laptop and any mobility needs eight basic stages (request 0–request 7) to be a successful process.

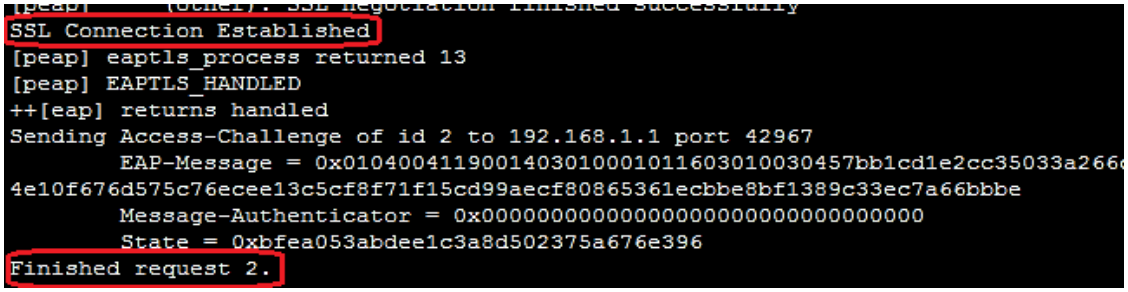
Figure 3 displays some of the successful process results between the portable laptop and M3.



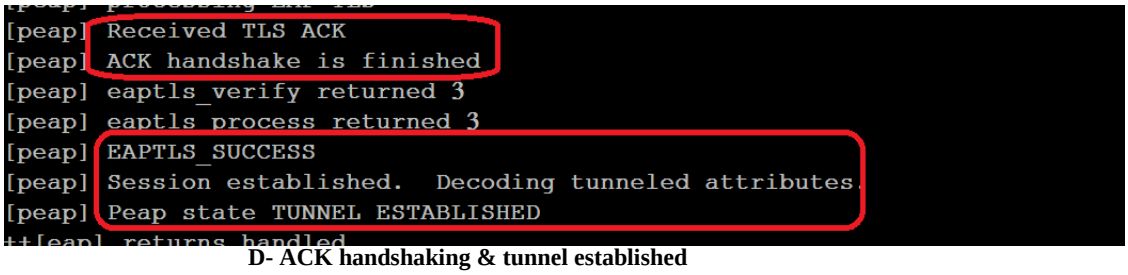
A- Starting of authentication process & checking the username



B- Selecting authentication type & sending Access-Challenge

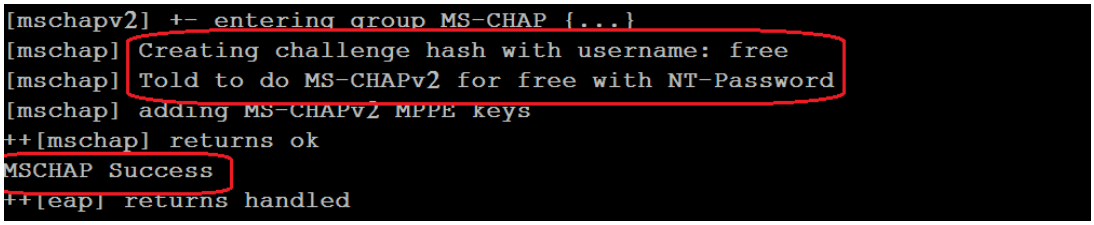


C- SSL connection established & finishing request 2

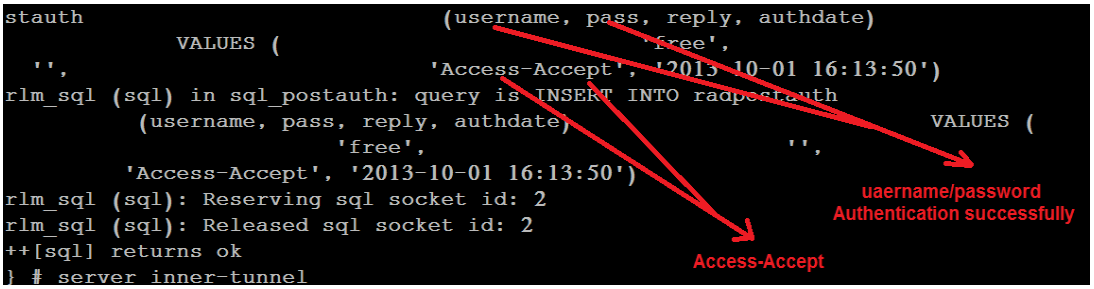


D- ACK handshaking & tunnel established

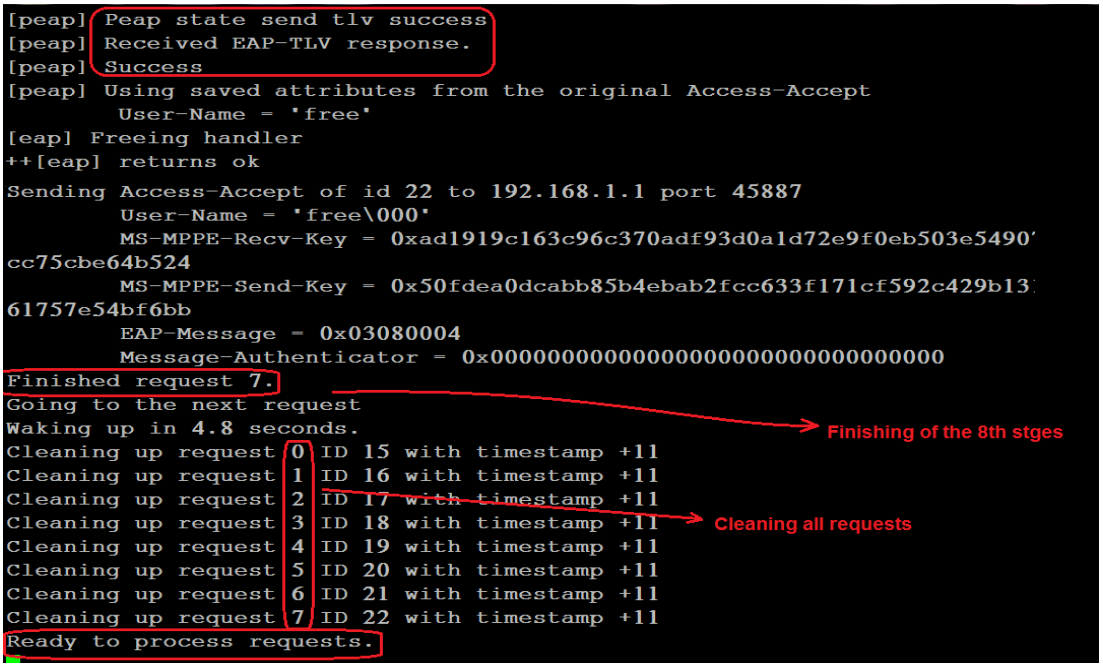
E- MS-CHAPv2 is the method using in authentication process



F- Appling hash function using MS-CHAPv2



G- Access-Accept of the authentication process

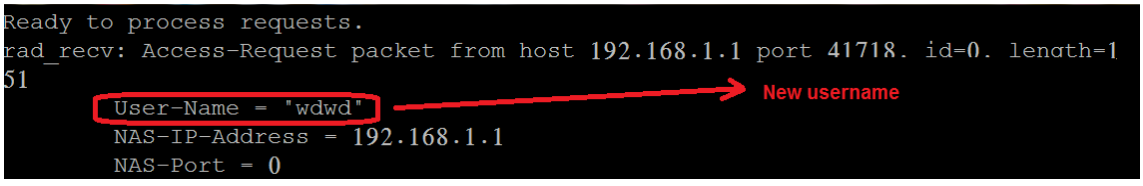


H- Finishing of all requests & ready to another process requests

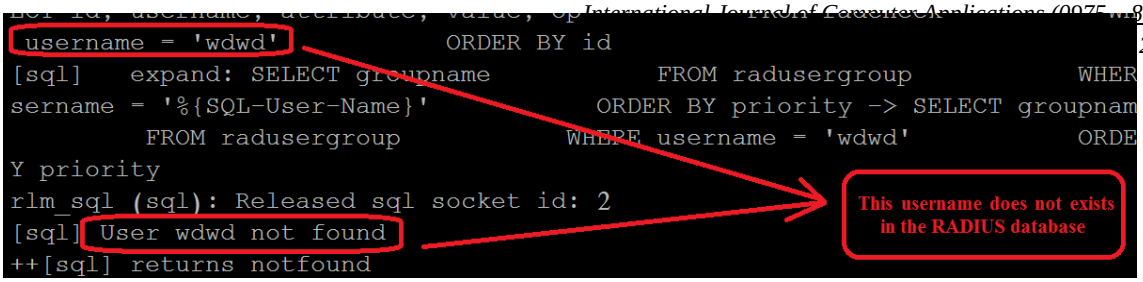
Fig 3: shows the processing steps of the authentication between the portable laptop and M3

4.2 Failure access request

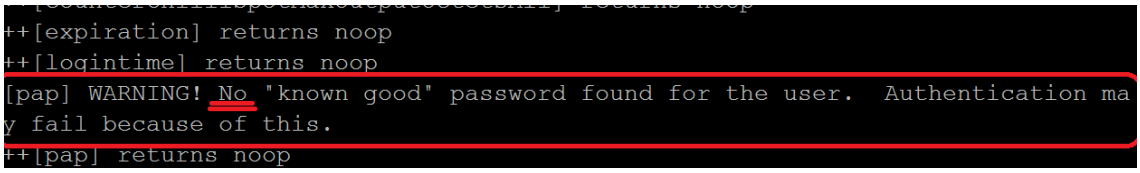
The unsuccessful authentication process passes through three stages only, It begins with request 0 and ends with request 2, the process of checking user's access (wdwd as a username) is achieved in the first stage, the authentication between the laptop and M4 will be failed because of the obstacle between them. Figure 4 shows the steps of a failed authentication process.



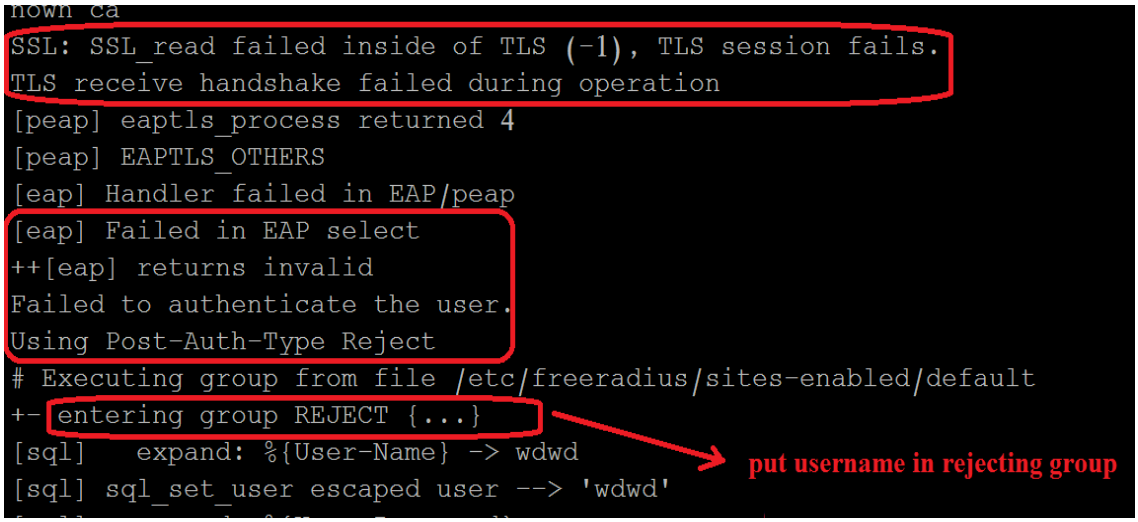
A- Trying another user name



B- This username does not exist in RADIUS



C- No password found for this username database



D- Failure of EAP selection & Putting username in rejecting group

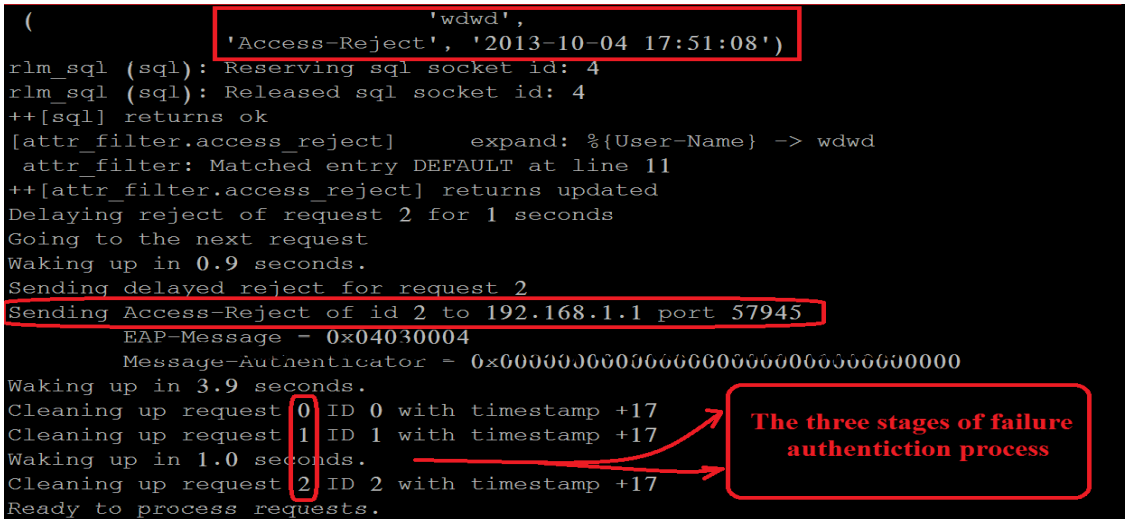


Fig 4: shows the unsuccessful authentication between the portable laptop and M4

4.3 Comparison between the authentication process of Galaxy note, iPhone and laptop

By taking samples from each of the eight stages of successful authentication of Android, IOS and windows 7 operating systems, Table (1) shows a comparison between the different devices under test.

Table 1. A comparison between the authentication process of Galaxy note, iPhone and laptop

	Galaxy note	IPhone	Laptop
Operating system	Android	IOS	Windows 7
Request (0, 1, 2, 3)	Identical	Identical	Identical
NO of EAP Messages	4	2	2
Acct-Interim-Interval (Request 4)	60	60	–
Request (5)	Replacing User-Password	Replacing User-Password	–
Request (6, 7)	Identical	Identical	Identical

Appendix [A] shows samples of the results which are obtained during the authentication processes of the different operating systems and mobiles (devices).

5. CONCLUSION

The security protocol 802.1x is Characterized by its capability of working with different types of devices (Samsung Galaxy Note, iPhone and Laptop) and under various operating systems such as Android, IOS and Windows 7.

It is found that eight stages are required for successful authentication (i.e. Authorized user). On the other hand, it is also proven that in the case of unauthorized users or the presence of obstacles between the client and the authenticator, three stages are sufficient to stop authentication process.

As a consequence, the remaining stages will be hidden and out of reach by the unauthorized users. This fact makes 802.1x so secure against different hackers attacks. Concerning the devices under test, this paper proves that Samsung Galaxy Note provides higher security than the other types.

6. REFERENCES

[1] YongYu, Qun Wang, Van Jiang, "Research on Security of the WLAN Campus Network" International Conference on E-Health Networking, Digital Ecosystems and Technologies, 2010.

[2] M. Hasbullah Mazlan, Sharifah H.S. Ariffin, Mohammed Balfaqih, S.Norhaizum M.Hasnan, Shariq Haseeb, "Latency evaluation ofauthentication protocols incentralized 802.11 architecture", Universiti Teknologi Malaysia (UTM), 2012.

[3] Snehasish Parhi, "Attacks Due to Flaw of Protocols Used In Network Access Control (NAC) ", Their Solutions and Issues: A Survey, I. J. Computer Network and Information Security, 2012.

[4] IEEE Standards, "IEEE Standard for Local and Metropolitan Area Networks - Port-Based Network Access Control", 2010.

[5] Alexandra Chiornita, Laura Gheorghe, Daniel Rosner, "A Practical Analysis of EAP Authentication Methods, Faculty of Automatic Control and Computers", IEEE International Conference ,2010.

[6] Ling-Wei Zhou, Sheng-ju Sang, "Analysis and Improvements of PEAP Protocol in WLAN", International Symposium on Information Technology in Medicine and Education, 2012.

[7] Hadeel Tariq Al-Rayes, "Studying Main Differences between Android & Linux Operating Systems", International Journal of Electrical & Computer Sciences IJECS-IJENS Vol:12 No:05, 2012.

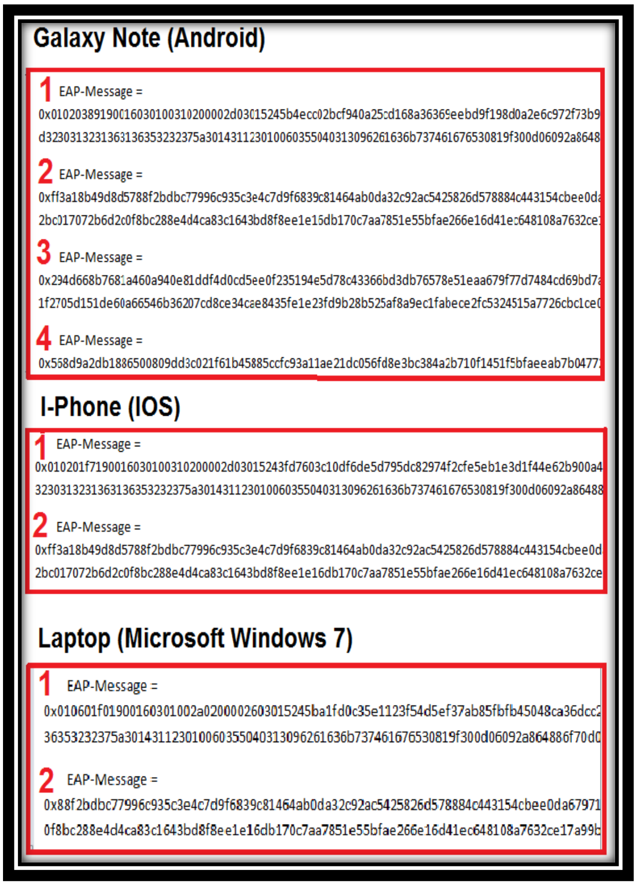
[8] Øystein Gyland, Tom Myren, Rune Sydskjør, Gunnar Bøe,"Implementation of IEEE 802.1X in Wired Networks", UNINETT led working group on security (UFS 133), 2013.

[9] Dirk van der Walt, "FreeRADIUS Beginner's Guide Manage your network resources with FreeRADIUS", PACKT publishing, BIRMINGHAM – MUMBAI, 2011.

[10] Liran Tal of Enginx, "Virtual Machine daloRADIUS Administrator Guide Version 0.9-9", 2011.

Appendix [A]
Samples of authentication process

1- The following figure shows the number of EAP messages required during the authentication process of the different devices.



2- The displayed page below shows that password warning is presented in Android and IOS, but it is absent in windows 7.