# RADIUS Authentication on Unifi Enterprise System Controller using Zero-Handoff Roaming in Wireless Communication

***Abstract***

**The demand for setting up a wireless LAN internet connectivity is almost mandatory for every commercial building, home, company, and educational institutions. With the growing number and height of buildings as well as the number of users, it has become essential to apply new techniques to provide better wireless network services, especially for security issue with many applications used by an attacker that can decrypt the traditional password to use network resources, that's lead to poor network performance for providing network services for people authorized to use it. All of that is almost a very challenge issue when applying outdated techniques. In this research a wireless network has been created considering a large number of users in a multi-floor building using a new control system which can solve the problems by setting up RADIUS authentication via that wireless network with a webpage that automatically appears to the user immediately after connecting to the wireless radio signal and automatically gaining an IP address, lead user directly to the temporary page asking him for authentication, if the user has the right username and password or even sometimes a code called Voucher, he will get a package assigned to his priority. This technology will eliminate the vulnerability on the wireless connection and the unauthorized user will be discarded from the router, in addition of that authorized users will get authenticated to make better use of network resources.**

***Keywords:*** *RADIUS, Hotspot, Unified Controller System, Zero-Handover, SSID*

## I. Introduction

For many years since the development of Local Area Network (LAN) in a wired network. LAN was very secure and reliable especially when it was not connected to the internet, but the demand for mobility of having the connecting lead to discovering the wireless radio signal that can carry the information in the air and give the user free of a move, but almost everyone in the range of radio signal can connect to the open wireless network, an old solution for that problem is to have a single password over the radio signal that has been given to an authorized user only, this technique was good at that time, but with the understanding of encryption and decryption technique nowadays and having much application that can decrypt the password, it became very easy by cybercriminal to gain access to the secured network and use its resources which became a vulnerable point for the system that been used by the company, home, business or even a school, to overcome this problem, many solutions to be considered [1], [2].

For example, the administrator of the network can make a database contain all MAC addresses for the authorized mobiles and laptop devices, these MAC addresses stored in the router and give them the access to the network and block everyone else, but this technique has the downside that a guest user will have straggled to enter the network by a process of many steps contacting the administrator and diving him the MAC address of his own device [2].

Another user management way is to make two or more wireless name called SSID (Service Set Identifier) each with a different password and each given to special users like in school environment, the (SSID) for teachers has more bandwidth with a different password that the (SSID) which given to the student which have a limitation for accessing some special websites [3], [4].

The nowadays solution in almost every enterprise and professional network environment is to set up a RADIUS wireless connection which directs the users after getting an IP address from DHCP (Dynamic Host Configuration Protocol) to a static webpage that welcomes the user and asks him either to enter the authorized username and password or even just a single code called the Voucher which is a random code generated by a specific router and printed by the network admin and given to the authored user. The decision to set up and install the Unifi Enterprise Controlling system with all of its components is dependent on many powerful features that this system offers for small and medium-size organizations and companies. Those features and aspects of a wireless network will be explained in detail as literature reviews in the following points [5]

### A. *Unifi Enterprise Controller System*

Unifi Controller Software is software from Unifi which has to manage wireless networks, view network statistics with Unifi Controller Management Interface. Unifi Controller can also be used to manage wireless networks [6], [7].

### B. *Captive Portal*

The captive portal is a feature included in Unifi Router and as its implementations have seen in coffee shops, hotels and schools usually either ask users to simply agree to terms and conditions before granting Wi-Fi access, use some sort of automatic backend to authenticate users using usernames a password or room numbers or ask for payment before access is granted. This solution effectively simplifies both the user's experience logging in, the host's experience administrating access, and still provides better access control than a simple agreement to terms and conditions. Asking for only a name rather than asking users to register with a username and password [8].

### C. *Zero-handoff Roaming*

In the large-scale industrial network, which consists of multiple access points (APs) and mobile users, there is one process that causes a delay problem, which is called as handoff or roaming, the roaming is a process when a user needs to move away from current AP to new AP promptly. In this process, the roaming delay causes the discontinuation of control. In general, the roaming delay is induced by two processes. First, the user has to disconnect from the current AP and join a new AP by channel scanning and probing. Second, the user must be authenticated at the new access point [7], [9].

### D. *Local Area Network*

Local Area Network (LAN) is a computer network that is designed for a limited geographic area such as a building or a campus. Although a LAN can be used as an isolated network to connect computers in an organization for the sole purpose of sharing resources, most LANs today are also linked to a wide area network (WAN) or the Internet [10].

### E. *Wireless LAN*

Wireless LANs are now one of the most important access network technologies in the Internet today. Although many technologies and standards for wireless LANs were developed in the 1990s, one particular class of standards has clearly emerged as the winner: the IEEE 802.11 wireless LAN, also known as Wi-Fi [7]. An 802.11 LAN is based on a "cellular" architecture: the system is subdivided into cells. Each cell, referred to as a basic service set in the 802.11 nomenclature, is controlled by a base station, known as an access point (AP). Although a wireless LAN may be formed by a single cell, with a single AP, most installations are formed by several cells, with the APs connected through some backbone, denoted as the distribution system (DS). This backbone is typically an Ethernet [11] [12].

### F. *Power over Ethernet*

Power over Ethernet (PoE) is a networking feature defined by the IEEE 802.3af and 802.3at standards. PoE lets Ethernet cables supply power to network devices over the existing data connection. PoE-capable devices can be power sourcing equipment (PSE), powered devices (PDs), or sometimes both. The device that transmits power is a PSE, while the device that is powered is a PD. Most PSEs are either network switches or PoE injectors intended for use with non-PoE switches. Common examples of PDs include VoIP phones, wireless access points, and IP cameras [13], [14].

### G. *Wireless Access Point*

A wireless access point (WAP) is a node configured to allow wireless devices to access the local area network (LAN). WAPs are just plugged into a switch or into an Ethernet hub. An access point has its own range. When two or more access points are in an environment, the range overlaps to provide roaming [15], and also has the responsibility of transferring signal from Ethernet cable mean of connection to a wireless signal of frequency either 2.4 GHz or 5 GHz [10].

### H. *Authentication Methods*

Different encryption systems have been implemented for the safety of wireless networks from the early years to the present. The encryption standards used for wireless networks are shown with technical specifications in Table I [16]–[18].

TABLE I. AUTHENTICATION METHOD USED IN WLAN

| **Method** | **Authentication** | **Encryption Algorithm** |
|---|---|---|
| WEP | Open/Shared Key | RC4 (24 bit) |
| WPA Personal | Pre-Shared Key(PSK) | RC4 (48 bit) |
| WPA2 Personal | Pre-shared Key(PSK) | AES |
| WPA Enterprise | 802.1x | RC4 (48 bit) |
| WPA2 Enterprise | 802.1x | AES |
| WPA3 Personal | Simultaneous Authentication of Equal (SAE) | 128 bit |
| WPA3 Enterprise | Simultaneous Authentication of Equal (SAE) | 192 bit |

Authentication sequence between a device that is trying to authenticate and an access point that is using shared key authentication. In Figure 1, the device uses WEP key matches the access point's key, so the device can authenticate and communicate.

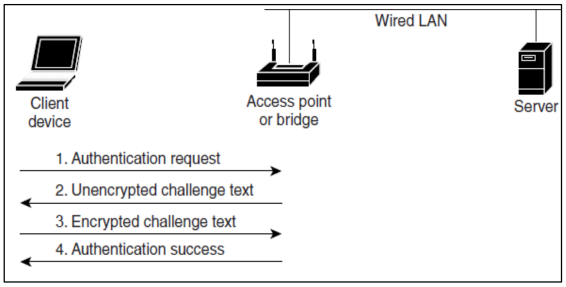

Wired LAN
Client device
Access point or bridge
Server
1. Authentication request
2. Unencrypted challenge text
3. Encrypted challenge text
4. Authentication success

Fig. 1. Sequence of Shared Key Authentication

### I. *RADIUS Server*

RADIUS which stands for "Remote Authentication Dial-In User Service" is a network protocol - a system that defines rules and conventions for communication between network devices - for remote user authentication and accounting. Commonly used by Internet Service Providers (ISPs), cellular network providers, and corporate and educational networks [19]. RADIUS is [17], [18], [20] an AAA protocol (authentication, authorization, and accounting) for applications such as network access or IP mobility. RADIUS is usually used for network devices such as routers, modem servers, switches [2][17][18][5].

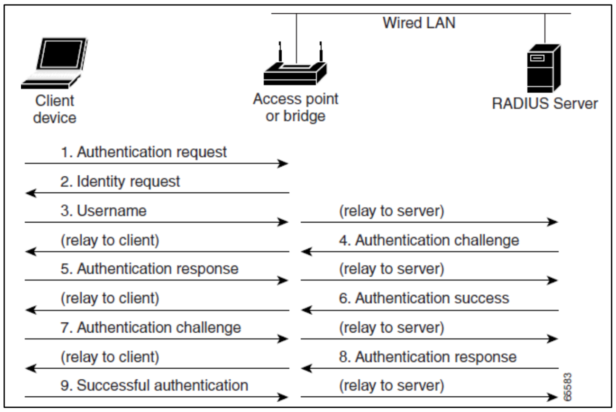


Fig. 2. Sequence of RADIUS Authentication

### J. *Ubiquity System Compare to Other Vendors*

A High-density test conducted by Aletha with Both Bands (2.4GHz and 5GHz) Enabled on a pre-Release version of Ubiquity AP, model Unifi AP-AC-HD, firmware version 3.7.37.6065, on 18th, 19th and 20th January of 2017 in Bangalore. Performance of this particular Access Point was compared with Access Points from Ruckus [R710:R710_104.0.0.0.1347], Aruba [IAP-325-US:6.4.4.0-4.2.3] and Meraki [MR52:up-to-date]. Clients used in the tests were configured with 2x2 MIMO Wi-Fi cards. 70% of the clients were 802.11a/b/g/n/ac capable and 30% were 802.11a/b/g/n capable. Tests were run on all APs with both 2.4GHz and 5GHz bands enabled. Measurements were taken with 40 clients, 70 clients and 100 clients and shows test result as in Figure 3 [24].

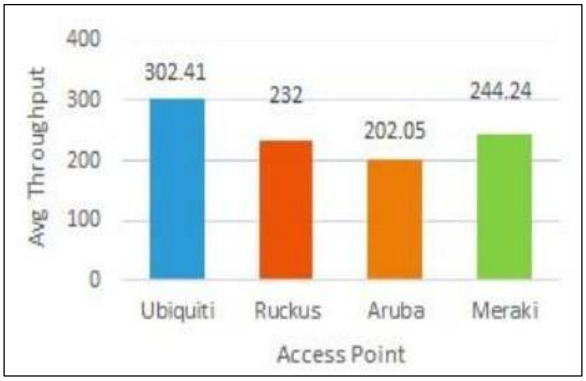


Fig. 3. Average Throughput (Mbps) in Both Bands

## II. Related Works

Many researchers have been done over RADIUS Server in wireless network to explore the vulnerability and strengths points of the system using RADIUS authentication method over traditional password based wireless method. A study of Shared Secret Key Update Scheme between RADIUS Server and Access Point using PUFs explored the existing AP and Radius Server used the SSK (Shared Secret Key) to authenticate the accounting messages between devices [21]. Another study of AWLAN Security Threats and Countermeasures Given the security flaws of the 802.11 standard, all businesses need to define their security requirements based on applications using WLAN. It is covered all the security issues and solutions to issues so that WLAN is protected like Wired LAN and make a comparisons between password based wireless network and RADIUS Server [22]. In [20] he explored that using RADIUS server leads use employees to use their credentials that are integrated with the RADIUS server, or they should use a voucher which is given to them. Apart from the authentication methods described, the network will not be accessible except the authorized users, so it is safe from unwanted attacks and network abuse. Another similar research [7] used the UNIFI devices, the system enables end-to-end roaming for complete roaming, making it seamless and virtually uninterruptable. Another study defined that roaming becomes an important aspect because many applications rely on real-time communication and therefore need seamless handover between access points [23]. In [1] they proposed a method for securing WLAN, their approach focused on creating a network for a medium size office which has 3 subnets and several servers. They used WPA2 Enterprise, firewall captive portal, and certification techniques. They have two types of network users which are employer and visitor. Then they tested their proposed method by exposing their network to attacks, these attacks were created by many attacker tools like air dump, aireply, and air crack. Their work gives better results than using only WPA2 PSK. Another researcher designed a network for universities in the developing countries. He took in the consideration the budget challenges. All used switches, access points, routers and firewall are from Cisco Company. This network designed to be used by 5075 users. [25]. And also in [26] To consider materials used in buildings mostly absorb Wi-Fi signal that make the access point placement inefficient as the transmitted signal blocked, absorbed, dispersed or reflected back by the wall and building structures. Isolative materials, such as concrete absorb and disperse the Wi-Fi signal, while conductive materials such as metal reflect Wi-Fi signal.

## III. Problem Statement

In educational organizations there are many types of network services with different privileges and large number of users, there are many adjacent buildings, each building with many floors. In addition, the total number of users is large. Network user's management is a challenge process especially when the network should be available and dependable. A very important point in this situation is that the devices which are using the network may be mobile devices (not place static), so the mobility of devices should not give the user any feeling of network service delay that is induced of network roaming.

## IV. Experimental Details

### A. *Materials*

With the high scalability of the Unifi system, it's possible to build wireless networks for a school. The Unifi wireless network can start with one access point and expand to hundreds between the buildings even in case of future expansion in the school campus. The system uses extremely compact access points in the form of a disk-like ceiling, resembling a beautiful indoor lamp with disk sizes twenty centimeters in diameter. White glossy plastic is fitted to make it. The front panel enclosure has a built-in LED indicator that lights up in blue or white depending on the operation mode of the device.

The map feature on the UNIFI controller gives the ability to the system administrator to plan for every access point place before physical installation on the building walls, simply by uploading the building floor plan image to the map section and adding the actual measurements with wall thickness and installing the access point to estimate the number of access point needed to each floor of the building, as shown in Figure 4.

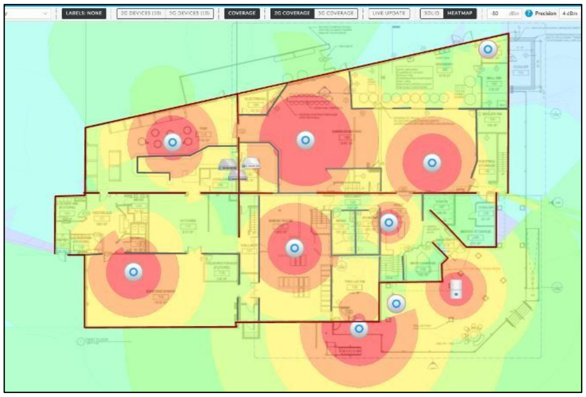
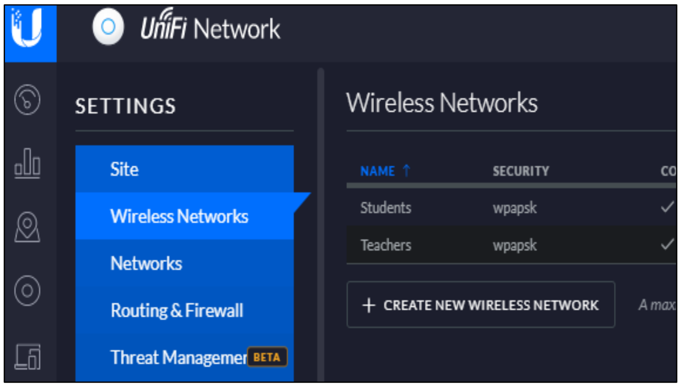


Fig. 4. Map plan of school first-floor building

After that a point to install the wall mount access point is determined as shown in the map, Ethernet cable of CAT6 type is installed to those points and all access point is installed, after that, it is necessary to connect all those access points to Unifi Security Gateway router which considered the heart of the system and through programming controller. It provides control over the entire network, security, and roaming of the end-users. The controller automatically recognizes the access point connected to the router. During the installation, information is displayed with the presence of the detected device. The router provides IP address with all information programmed through the controller like (SSID) with a password to the access point depended on the device's MAC Address.

The Unifi system is capable of providing multiple wireless networks with different access privileges. It allows splitting traffic of network users over VLANs. This is practically an opportunity to create independent wireless networks and translate them into virtual local area networks (VLANs), which is an extremely convenient and reliable way to isolate traffic to different categories of users which in the school case to have two different Wi-Fi SSID broadcasted to the users, one for teachers and staff with higher bandwidth rate of 10 Mbps and no limitation over accessing to all internet websites. Another WI-FI SSID for only student in order to give lower bandwidth rate with only 2 Mbps. It is important to note that students cannot access a predefined list of websites that are not suitable to students age, as shown in Figure 5.



Wireless Networks

| NAME ↑ | SECURITY | CO |
|---|---|---|
| Students | wpapsk | ✓ |
| Teachers | wpapsk | ✓ |

Fig. 5. Different SSID and Profiles

Unifi Access Point Pro gets its configuration from Unifi Security Gateway pro in programming controllers by the system administrator; those functions are to provide roaming between access points without interrupting the end-user connection. This is a problem that in other types of networks cannot be solved or just costs quite expensive. The Unifi system access points are the first system that has a built-in programmable controller with low cost. The end-user is provided with the ability to navigate the network without even noticing that it connects to different a base station which lets the teachers and students move freely between the buildings while having an uninterrupted internet connection.

The Unifi system control web interface allows managing each user, analyzing traffic, and setting the necessary parameters for each client individually. This enables the network administrator to see user activity through diagrams and to notice sources of irregularities and increased network load, for the school administrator it was essential to monitor teachers and student's behavior while they using the internet resource and some-time block some of them if they used too much of internet bandwidth downloading unnecessary files, as shown in Figure 6

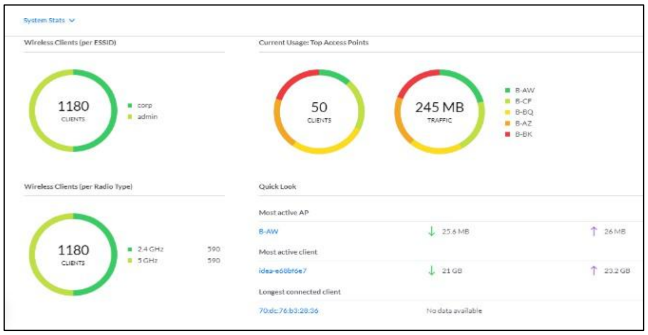


Fig. 6. Administrator web controller and monitor

It is essential to configure the RADIUS method for both SSID names by automatically redirecting those users to a website with IP address 192.168.0.24 with port 1813 to restrict the access to network resource unless the user enters the valid voucher code which is given to him by a system administrator, as shown in Figure 7.

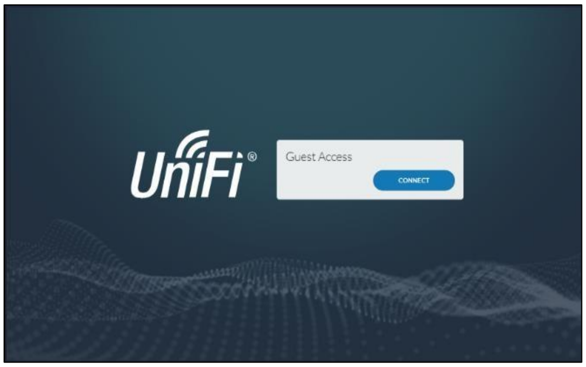
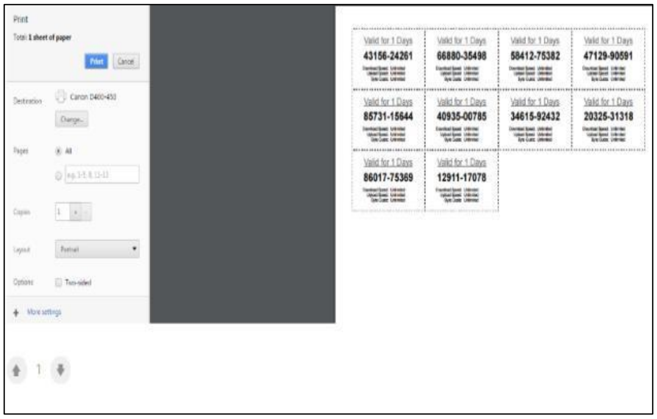


Fig. 7. RADIUS Sing-in Portal

RADIUS server needed to be configured according to some specific steps, firstly the guest controller is needed to be chosen as Hotspot then a Voucher generating web portal is given by the controller to the system administrator to create different voucher code each with specific download and upload limitations and either limited or unlimited vouchers lifetime, as shown in Figure 8.



| | | | |
|---|---|---|---|
| Valid for 1 Days<br>43156-24261 | Valid for 1 Days<br>66880-35498 | Valid for 1 Days<br>58412-75382 | Valid for 1 Days<br>47129-90591 |
| Valid for 1 Days<br>85731-15644 | Valid for 1 Days<br>40935-00785 | Valid for 1 Days<br>34615-92432 | Valid for 1 Days<br>20325-31318 |
| Valid for 1 Days<br>86017-75369 | Valid for 1 Days<br>12911-17078 | | |

Fig. 8. Voucher Generating Portal

With that Voucher entered in the controller by the portal RADIUS server, the system administrator can monitor user activity, download and upload bandwidth, and can block him anytime the user consuming too much of the system bandwidth.

### B. *RADIUS Authentication Algorithm*

The following algorithms show the steps of RADIUS Authentication in Unifi Security Gateway Router.

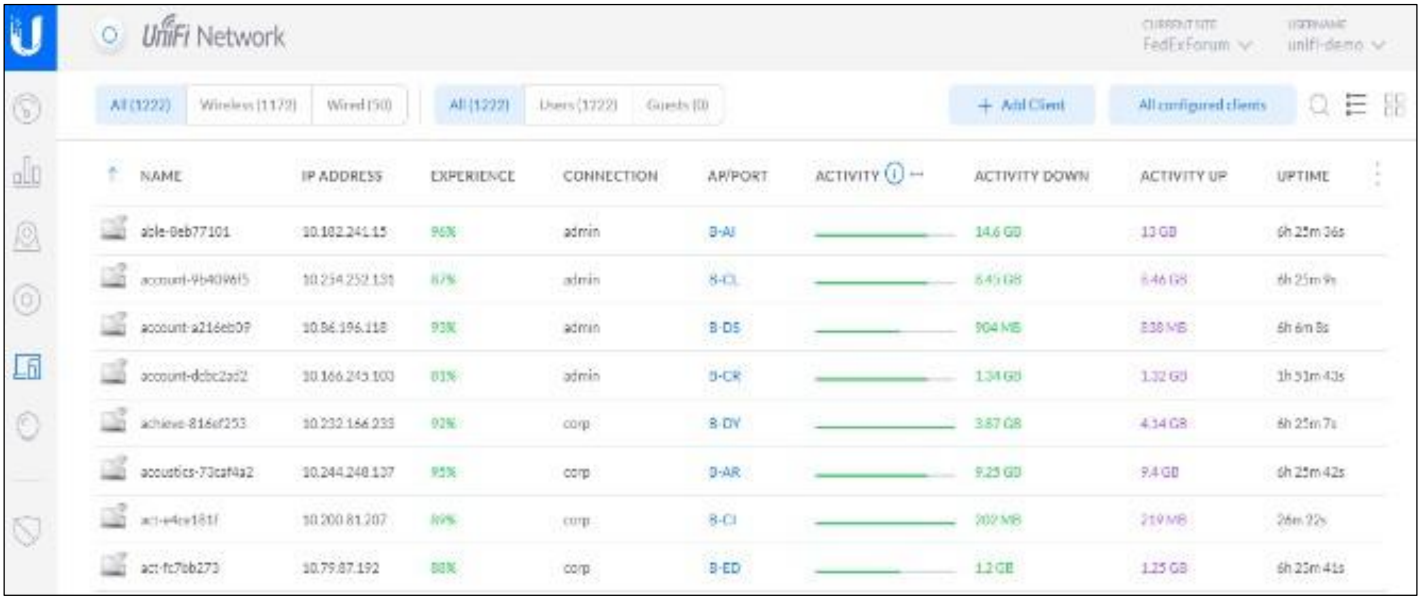
- The user device connects to an open Authentication Unifi Access Point.
- Unifi Access Point forward connects through Wired Ethernet Cable and Unifi Switch Back to Radius Server in the Unifi Security Gateway Router.
- The Radius Server Send back a Sign-in Portal HTML Page back to User Browser Contain the Filed for Entering User Voucher Authentication.
- The user entered a known key given by the administrator to that specific user.
- RADIUS server gets the user credentials and looks for a match in a user database.
- If the user voucher matches an entry in the database. The RADIUS Server Give an IP Extended time Expiration based on user policy and profile created by the administrator earlier for that user and gain internet access.
- If the user voucher didn’t match an entry in the database.

The RADIUS Server Give Access Denied to that specific User and discard that IP Address from the Unifi Security Gateway Router.

- The user device connects to an open Authentication Unifi Access Point.
- Unifi Access Point forward connects through Wired Ethernet Cable and Unifi Switch Back to Radius Server in the Unifi Security Gateway Router.
- The Radius Server Send back a Sign-in Portal HTML Page back to User Browser Contain the Filed for Entering User Voucher Authentication.
- The user entered a known key given by the administrator to that specific user.
- RADIUS server gets the user credentials and looks for a match in a user database.
- If the user voucher matches an entry in the database. The RADIUS Server Give an IP Extended Time Expiration based on user policy and profile created by the administrator earlier for that user and gain internet access.
- If the user voucher didn’t match an entry in the database. The RADIUS Server Give Access Denied to that specific User and discard that IP Address from the Unifi Security Gateway Router.

### *C. Results*

When all the configurations are done properly, the testing process is done by looking at the list of connected users, both teachers and student with different SSID seeing the results of generating vouchers, testing vouchers to access the network, and testing using radius authentication for employees to enter the network as shown in Figure 9.



| NAME | IP ADDRESS | EXPERIENCE | CONNECTION | AP/PORT | ACTIVITY | ACTIVITY DOWN | ACTIVITY UP | UPTIME |
|---|---|---|---|---|---|---|---|---|
| able-8eb77101 | 10.182.241.15 | 96% | admin | B-AI | | 14.6 GB | 13 GB | 6h 25m 36s |
| account-9b409615 | 10.254.252.131 | 87% | admin | B-CL | | 6.45 GB | 6.46 GB | 6h 25m 9s |
| account-a216eb09 | 10.86.196.118 | 93% | admin | B-DS | | 904 MB | 838 MB | 6h 6m 8s |
| account-dcbc2ad2 | 10.166.245.103 | 81% | admin | B-CR | | 1.34 GB | 1.32 GB | 1h 51m 43s |
| achieve-816ef253 | 10.232.166.233 | 92% | corp | B-DY | | 3.87 GB | 4.14 GB | 6h 25m 7s |
| acoustics-73caf4a2 | 10.244.248.137 | 95% | corp | B-AR | | 9.25 GB | 9.4 GB | 6h 25m 42s |
| act-e4ce181f | 10.200.81.207 | 89% | corp | B-CI | | 202 MB | 219 MB | 26m 22s |
| act-fc7bb273 | 10.79.87.192 | 88% | corp | B-ED | | 1.2 GB | 1.25 GB | 6h 25m 41s |

Fig. 9. List of User Connected

The user is connected using a device name able-1d6f9cc7 has got an IP address from the controller, and it can be concluded that the user has successfully connected to the access point that has been made because the voucher code used is appropriate, and the upload and download sessions have been started and use 56.2 Gbyte download and 55.3 Gbyte upload with uptime of 1 hour and 31 minutes of connection. Also user 84:41:67:60:4d connected using the RADIUS authentication method. It can be concluded that user 84: 41: 67: 60: 4d has successfully connected to the access point that was created because it was successfully authorized and the upload and download sessions have started.

## V. Conclusion

Unlike traditional router and wireless networks, which are vulnerable to various hacker attacks and show the security flow of the 80.2.11 standard wireless protocol, the Unifi system enables end-to-end using zero handoffs roaming, making it seamless and virtually uninterruptable which is useful in many cases like VOIP and Video Conference. The Unifi RADIUS comes with a software controller that can be deployed on a regular Windows computer, a part from the authenticated user described earlier, the network will not be accessible, and so it is safe from unwanted attacks and network abuse. And also installing, configuring, and managing Unifi wireless network is easy with the intuitive and easy-to-use Unifi user interface. With the high scalability of the Unifi system, it is possible to build wireless networks for a bigger school building, and in extremely large areas - hotels, universities, airports and more.

## References

[1] B. Soewito and Hirzi, “Building secure wireless access point based on certificate authentication and firewall captive portal,” EPJ Web Conf., vol. 68, Feb. 2014, doi: 10.1051/epjconf/20146800029.

[2] B. Pekevski, “Control and management of Wi-Fi networks,” MASTERS THESIS, University of Ljubljana, Ljubljana,Slovenia, 2016.

[3] I. Ong and A. . S. Phillip, “SSID BROADCAST MANAGEMENT TO SUPPORT PRIORITY OF BROADCAST,” US 2017 / 0245201 A1, Aug. 24, 2017.

[4] R. Gurudath Savoor and C. Ou, “METHODS AND APPARATUS TO MANAGE BANDWDTH IN A WIRELESS NETWORK,” US 7.924,793 B2, Apr. 12, 2011.

[5] O. Dmitry, “RADIUS server as centralized authentication,” bachelor’s thesis, Mikkeli University of Applied Sciences, Southern Savonia in Finland, 2015.

[6] Ubiquiti Networks, “Unifi Controller User Guide.” www.ubnt.com, 2016, [Online]. Available: https://dl.ui.com/guides/UniFi/UniFi_Controller_V5_UG.pdf.

[7] R. Pasarelski, T. Pasarelska, and S. Yotsova, “SYSTEM - UNIFI DEPLOYING WIRELESS DATA NETWORK WITH FULL ROAMING,” Nov. 2018.

[8] B. Blumenberg, “WiFi Gate Guard: A Captive Portal Implementation for Home Networks,” May 2018.

[9] K. Yamaguchi et al., A secure and fast industrial WLAN system with zero-delay roaming. 2016, p. 817.

[10] B. Forouzan, Data Communications and Networking, 4nd Edition. 2007.

[11] A. K. Ibrahim, M. H. Abdulwahab, M. B. Abdulrazzaq, and M. R. Mahmood, “A Tree Method for Managing Documents in Mongodb,” vol. 83, no. March-April2020, pp. 18351–18359, 2020.

[12] R. R. Zebari, S. R. M. Zeebaree, and K. Jacksi, “E-Business Requirements For Flexibility And Implementation Enterprise System: A Review,” Int. J. Sci. Technol. Res., vol. 8, no. 11, Nov. 2019, [Online]. Available: https://www.researchgate.net/profile/Karwan_Jacksi/publication/337404049_E-Business_Requirements_for_Flexibility_and_Implementation_Enterprise_System_A_Review/links/5dd5b4aaa6fdcc2b1fa8d875/E-Business-

Requirements-for-Flexibility-and-Implementation-Enterprise-System-A-Review.pdf.

[13] S. Maniktala, Power Over Ethernet Interoperability Guide. McGraw Hill Professional, 2013.

[14] D. Coleman and D. Westcott, “Power over Ethernet (PoE),” pp. 443–469, Sep. 2018, doi: 10.1002/9781119549406.ch12.

[15] EC-Council Press, Ed., Computer forensics: investigating wireless networks and devices. Clifton Park, NY: Course Technology Cengage Learning, 2010.

[16] A. Süzen, M. Şimşek, K. Kayaalp, and R. Gürfidan, “The Attack Methodology to Wireless Domains of Things in Industry 4.0,” Nevşehir Bilim Ve Teknol. Derg., pp. 143–151, Oct. 2019, doi: 10.17100/nevbiltek.557886.

[17] W. Odom, CCNA 200-301 Official Cert Guide, Volume 2. Cisco Press, 2019.

[18] F. N. Chughtai, R. Ulamin, A. Malik, and N. Saeed, “Performance Analysis of Microsoft Network Policy Server and FreeRADIUS Authentication Systems in 802.1x based Secured Wired Ethernet using PEAP,” Int. Arab J. Inf. Technol., vol. 16, pp. 862–870, Sep. 2019.

[19] N. R. SARL, “The FreeRADIUS Technical Guide,” 2014.

[20] H. Halimatussadiyah, “Access Point Implementation to Unifi Device with RADIUS and Captive Portal Authentication Method in PT XYZ,” Jul. 2019.

[21] J. Park and S. Jung, “Shared secret key update scheme between RADIUS server and access point using PUFs,” in 2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT), Aug. 2017, pp. 1–5, doi: 10.1109/CAIPT.2017.8320725.

[22] S. Suroto, “WLAN Security: Threats And Countermeasures,” JOIV Int. J. Inform. Vis., vol. 2, Jun. 2018, doi: 10.30630/joiv.2.4.133.

[23] S. Feirer and T. Sauter, “Seamless handover in industrial WLAN using IEEE 802.11k,” in 2017 IEEE 26th International Symposium on Industrial Electronics (ISIE), Jun. 2017, pp. 1234–1239, doi: 10.1109/ISIE.2017.8001421.

[24] R. Salih Sarhan, “Computer Network Design for Universities in Developing Countries,” Master Thises, Valparaiso University, Valparaiso, Indiana,USA, 2016.

[25] Alethea Communications Technologies, “Report on High density tests and comparative study conducted on Ubiquiti UAP-AC-HD access points.” © Alethea Communications Technologies Pvt Ltd, Jan. 18, 2017.

[26] S. Suherman, “WiFi-Friendly Building to Enable WiFi Signal Indoor,” Bulletin of Electrical Engineering and Informatics, vol. 7, Mar. 2018, doi: 10.11591/eei.v7i2.871.