Design and implementation of an Enterprise-Grade Wireless Network with Strong Authentication

A Project Report
Presented to
The Faculty of the College of
Engineering

San Jose State University
In Partial Fulfillment
Of the Requirements for the Degree
Master of Science in Computer Engineering

By
[Abishek Mugunthan Ajay Kumar Ravipati Roopesha Sheshappa Rai Vijaya Laxmi Durga Alekhya Nynala]
[Fall 2021]

APPROVED

DocuSigned by:
Gokay Saldamli
6D998C993017749A...

[Advisor's Name], Project Advisor

ABSTRACT

Design and implementation of an Enterprise-Grade Wireless Network with Strong Authentication

By [Abishek Mugunthan Ajay Kumar Ravipati Roopesha Sheshappa Rai Vijaya Laxmi Durga Alekhya Nynala]

Security is one of the important aspect of today's digital world. There have been numerous breaches by people with malicious intent to either steal confidential data or disrupt daily activities of a corporation. Security implemented at enterprise level still lack in certain design aspects leading to said attacks. Existing security methods are often not implemented to account for various threats and breaches. The most favored target is the end user as the highly vulnerable part of a network is the human factor.

In the present day, poor implementation and design of enterprise networks leads to data breaches and poor user security. Assumption that the network is secure after adding security at layer 2 is an overlooked mistake. Due to having the option to randomize layer data on the user- end for privacy, the layer 2 authentication methods such as MAC based authentication fail to serve their purpose on their own. layer 3 authentication methods while still securing the user at layer 3 quite often ignore the layer 2 verification of the same user.

This project aims at a design, implementation and analysis of various enterprise security and authentication methods to secure and maintain wireless users. We shall implement the security methods to point out how they are flawed when used individually and provide a solution to those issues by combining various authentication and encryption methods to make up for the said flaws.

Acknowledgments

The authors are deeply indebted to Professor Gokay Saldamli for her invaluable comments and assistance in the preparation of this study.

Design and implementation of an Enterprise-Grade Wireless Network with Strong Authentication

Abishek Mugunthan , Ajay Kumar Ravipati , Roopesha Sheshappa Rai
Vijaya Laxmi Durga Alekhya Nynala
Computer Engineering Department
San Jose State University
Email: abishek.mugunthan@sjsu.edu, ajaykumar.ravipati@sjsu.edu, roopeshasheshappa.rai@sjsu.edu
vijayalaxmidurgaalekhya.nynala@sjsu.edu

***Abstract*—Security is one of the important aspect of today's digital world. There have been numerous breaches by people with malicious intent to either steal confidential data or disrupt daily activities of a corporation. Security implemented at enterprise level still lack in certain design aspects leading to said attacks. Existing security methods are often not implemented to account for various threats and breaches. The most favored target is the end user as the highly vulnerable part of a network is the human factor.**

In the present day, poor implementation and design of enterprise networks leads to data breaches and poor user security. Assumption that the network is secure after adding security at layer 2 is an overlooked mistake. Due to having the option to randomize layer data on the user-end for privacy, the layer 2 authentication methods such as MAC based authentication fail to serve their purpose on their own. layer 3 authentication methods while still securing the user at layer 3 quite often ignore the layer 2 verification of the same user.

This project aims at a design, implementation and analysis of various enterprise security and authentication methods to secure and maintain wireless users. We shall implement the security methods to point out how they are flawed when used individually and provide a solution to those issues by combining various authentication and encryption methods to make up for the said flaws.

Keywords: Security, WPA, WPA-2, PSK, MAC, Authentication, VLAN, .

I. Project Overview

A. Introduction

1) Wireless Networks:: Wireless Networks are computer networks that use wireless connections such as radio communication between nodes on the network. Such a network implementation occurs in the physical layer of the OSI model. It requires two major components:[11]

- Clients: Clients typically include end users and can include devices like PC, laptop, mobile phones, tablets etc. and also other equipment like printers, and barcode readers to name a few.[11]
- Access Point(AP): An access point is a network hardware device that allows other Wi-Fi devices to connect to a wired network. includes a Wi-fi that is advertising a network name (Such as a service-set identifier (SSID)). [11]

2) Classification of Wireless Networks:: Wireless networks can be classified as follows:

- Wireless Personal Area Network (WPAN): These are short range networks that connect devices within a range of 30ft. It uses bluetooth to interconnect devices at a central location. Examples include interconnecting a headset to the laptop.
- Wireless Local Area Network (WLAN): Wireless LAN network makes use of radio waves for communication rather than Bluetooth technology. The range can be confined to a single room or home or can be extended across an entire building or campus using spread spectrum or OFDM technologies. It usually contains one cable that acts as an access point to the internet, such as the wired connection going into the router which then broadcasts the wireless signal to other resources.
- Wireless Wide Area Network (WWAN): WWAN are maintained over large areas by means of satellite systems, antenna sites or mobile phone signals.

- Wireless Metropolitan Area Network (WMAN): It is used to connect several different WLAN's in a metropolitan area.[12]

3) Wireless Authentication Methods:: Wireless authentication helps secure wireless networks by ensuring that only users with the proper credentials can access the network. It can be classified as :

- Open Authentication: It is the simplest authentication method and only requires the user to be aware of the Service-set identifier(SSID) to gain access to the network. The disadvantage of this method is that SSID is typically a broadcast and even if it is not a broadcast, it is easy to find the SSID using passive capturing methods.
- Shared Authentication: The shared authentication mechanism makes use of a shared key (Pre-shared key(PSK)) which is distributed on both sides of the connection and access is provided only if the keys match. It is commonly used in individual and small business WLAN implementations.
- Extensible Authentication Protocol: The EAP protocol is the most common authentication method used in enterprise networks and makes use of an authentication server that is queried using various credential options.[13]
- WLAN Encryption Methods: Use of proper encryption standards is as important as choosing a proper authentication mechanism. Earlier encryption standards were found to be insecure and easily vulnerable to attacks. Some of the common encryption standards include:
  - Wired Equivalent Privacy (WEP): WEP security mechanism was used in the 802.11(prime) Wireless standards. WEP utilizes the RC4 algorithm but has been deprecated now owing to the vulnerabilities that makes it easier to find the security key.
  - Wi-Fi Protected Access (WPA): The attacks on WEP lead to the development of WPA. WPA used a Temporal key integrity protocol (TKIP) which used dynamic keys that were not supported by WEP and RC4. Eventually vulnerabilities were found on TKIP since it used methods that were similar to WEP and hence similar kinds of attacks were used to obtain the key.
  - Wi-Fi Protected Access 2 (WPA2): WPA2 standard was developed in response to vulnerabilities in WPA standard and replaced TKIP with Counter mode with cipher block chaining message authentication code protocol (CCMP) which is based on advanced encryption standard (AES).[13]

B. Related Works

A. Skendžić et.al. analyzed the performance of an Aruba Wireless Local Area Network in a Croatian Pension insurance Institute. The analysis was performed on a wireless network that was implemented using a HP Aruba Enterprise wireless network that included a 802.11 ac (Wi-Fi 5) standard. It includes 51 access points across 6 physical locations along with associated network system infrastructure. The network performance analysis measure includes clients by location of access points, access point loads, network usage, applications used, network bandwidth and total usage.[3]

Yunus Durmus et.al. proposed a method of wifi authentication using social network. This paper abandons the centralized solution to embed social networks in Wi-Fi authentication and rather introduces a new method called EAP-SocTLS. EAP-SocTLS is a decentralized approach for authentication and authorization of Wi-Fi access points, by exploiting the embedded trust relations. It uses a simple heuristic solution of limiting the search to friends and devices in physical proximity thus offering a scalable solution. The implementation uses WebID and EAP-TLS and uses Wi-Fi probe requests to determine the device pool, thereby reducing search time of 1 minute for naïve policy down to 11 sec.[4]

Ying Wang et.al. analyze the shortcomings of WEP and WPA-PSK and possible attacks on WLAN and propose two mechanism to overcome the shortcomings. One of those methods is dWEP which adopts the ARP requests to access point as a standard to judge whether an access point is attacked and prevents those clients from accessing the network which claims access by dropping the ARP request from it. The same feature is tested experi-

mentally using loadable module, netfilter and hostap function of Linux. The d-WPA-PSK functionality uses a key generator that distributes different seeds according to AP and clients based on different PSK's. AP broadcasts a random seed to a client and the client will later send a feedback indicating it has the seed. When all client associated with an AP contain the seed, the client will generate a new PSK. This regular update of PSK's helps improve security.[9]

Mohamed A. Abo-Soliman et.al. proposed an analysis of WPA2 encryption methods and the recent attacks on WPA2 that has exposed a few vulnerabilities. The paper discusses two such attacks namely the dictionary attack and the key re-installation attack. In a dictionary attack, the intruders test accessing the network several times with different values until one hit. This is a form of brute force attack. Dictionary attack wherein the intruders collect authentication information such as EAPOL messages by exploiting the broadcast nature of wireless communication and later running an offline dictionary attack on the capture packets is called a passive dictionary attack while targeting the access point directly requesting to join a network and waiting for a response from access point for successful authentication is called an active dictionary attack. Key reinstallation attack target data confidentiality by intercepting the data flow between client and access point.[2]

Omar Nakhila et.al. analyses and propose a parallel active dictionary attack to exploit the vulnerabilities in WPA2 mechanism and provide an alternate to the active dictionary attack. An attacker applies an active dictionary attack by communicating directly with the authentication server and guess the credentials to access the wireless network. However such an attack is weak owing to the low intensity of the password guessing trials that the attacker can achieve. The proposed scheme of attack uses one wireless interface card to create multiple virtual wireless clients, wherein each communicate with the authentication server as standalone clients. This increases the speed of guessing the password by 1700 percent compared to the traditional active dictionary attack.[10]

C. State of the Art

Mathy Vanhoef et.al. analyses the WPA3 and EAP-pwd security encryption standards that works using the dragonfly handshake mechanism. While WPA3 aims at securing home networks, EAP-pwd targets the enterprise networks. Both use dragonfly handshake mechanism to provide forward secrecy and resist dictionary attacks. Dragonfly Handshake is a password authentication key exchange (PAKE) mechanism wherein it converts the password into a high entropy key. Dragonfly supports elliptical curve cryptography. The paper deals with the security provided by the dragonfly handshake, possible side channel attacks against dragonfly's password encoding method (hash to curve) and possible backward compatible defenses and protocol fixes to prevent these attacks.[6]

Evgeny Khorov et.al. provide a detailed analysis of the state of the art Wi-Fi 6 known in IEEE standard as 802.11ax. The paper discusses the different draft versions of 802.11ax and provides an in-depth analysis of orthogonal frequency division multiple access based random access approach and novel spatial frequency re-use techniques. The paper also highlights the significant improvements such as physical layer enhancements that offer advanced modulation and coding schemes, multi-user multiple input multiple output (MIMO) extensions, power saving advances etc, that provides an edge to the 802.11ax in wireless communication.[7]

Kai X. Miao proposes the development of an enterprise wireless network using WiMax technology. This paper focusses on integrating WiMax, an all-IP broadband wireless technology with an existing enterprise network thereby allowing the network to either directly host a Wimax network or use a public WiMAX network hosted by a service provider. It talks about the WiMAX architecture required, the need to strengthen the existing security of WiMAX to incorporate the needs of enterprise networks and explore how WiMAX and Wi-fi can work together to provide a unified experience.[8]

II. Problem Statement and Project Justification

As technologies move towards collecting user's data to understand their needs for providing better solutions, there is a growing concern towards

security of data usage in both consumer and service provider end. These data might be sensitive personal information. If intruders can get access to these communications, they can bring down entire communication, or they can bring down service or they can collect user's sensitive data, or they can make other genuine users get bad services. Majority of data usages are done using mobile phones, Smart Internet of Things (IoT) devices. Usually, these devices use wireless networks to communicate.

Wireless networks can be cellular networks, Home Wi-Fi networks, Enterprise Wi-Fi networks, or small-scale wireless networks like Bluetooth, Zigbee, Threads mainly used by IoT devices. Cellular networks have their own security concerns and solutions. But we focus on another consumer oriented wireless network that is Wi-Fi network.

Based on volume of users and sensitive data, Enterprise grade Wi-Fi networks are more vulnerable to attack. Generally Enterprise grade Wi-Fi networks provide communication services in companies, Stadiums, Banks, Airports, Shopping malls etc. Unlike home Wi-Fi networks, Enterprise Wi-Fi networks can not share passwords to all its users, it needs much more security. Enterprise WiFi uses an external RADIUS server to authenticate users by combining WPA2-Enterprise with 802.1X authentication. Misconfiguration of these authentication protocols may encourage intruders to access the private network.

According to a report, A security startup Verkada suffered breach over its 150,000 cameras due to lack of multi-factor authentication in March 9, 2021. Intruders gained 'super admin' level access from online and able to access many cameras in Tesla factories, Jails, Schools etc. It is just an example out of many cyber attack incidents and proves we are nowhere near to achieve a complete secure communication network. In our project we will try to implement multi-factor authentication using Aruba infrastructure and exercise its strength over attack.

III. Project Architecture

A. Introduction

We plan to implement an Enterprise Grade Wireless Network using Aruba Gear. The diagram below represents a High-level design of our network. We have two sites in San Jose and they are separated by a physical distance of 5 miles and represent a main office and a branch office. There is redundancy setup between these two controllers to ensure that there is wireless connectivity in case of a hardware failure. We shall use VRRP to provide redundancy and IPSEC to encrypt our traffic. We will display this during our final demonstration.

B. High Level System Architecture

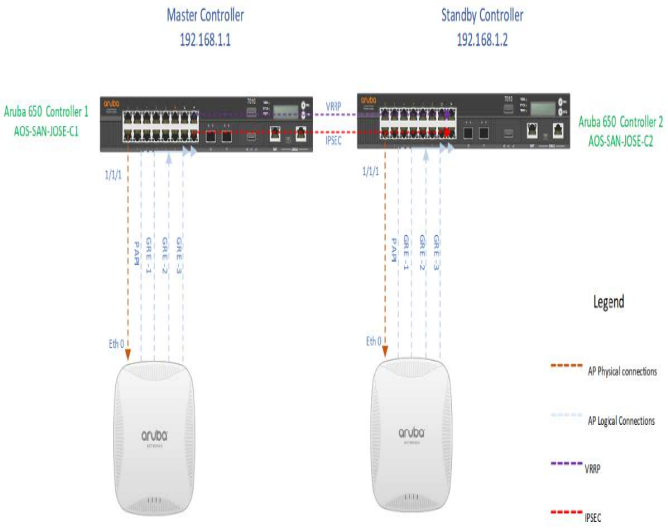


Fig. 1. High Level Architecture Diagram

The diagram also shows the physical and the logical connections between a wireless controller and an Access Point. The Aruba Access Points use 4 Tunnels to communicate with the wireless controller.

- PAPI - This tunnel is used for initial communication with the controller. IT used ports 8211 and 8209 (If control plane security is enabled).
- GRE-1 - This is a GRE (Generic Routing Encapsulation) tunnel for the 2.4 GHz Radio.
- GRE-2 - This is a GRE tunnel for the 5 GHz Radio.
- GRE-3 - This is a GRE tunnel for keepalive mechanisms between the controller and the AP.

We will have multiple WLANs (Wireless Local Area Networks) that would be user specific. We would also have multiple authentication frameworks added to the wireless SSID (Service Set IDentifier)

and also broadcast multiple ESSIDs (Extended Service Set IDentifier). An authentication flow would be captured and analysed for possible Attack surfaces and we shall also explain how the said attack surfaces could be nullified. We shall analyse the pros and cons of all the authentication methods used and propose a solution based on our testing.

The enterprise grade wireless network topology consists of two wireless controllers which has an access point connected to them. The controller acts as the default gateway to the access point. • Redundancy is provided between the two controllers using VRRP (Virtual Router Redundancy Protocol). This ensures that Controller 1 which acts as master will have controller 2 to back up in case of failure or unavailability. • The controllers are secured using IPSEC (IP Security) protocol to ensure authentication and secure encryption of packets. • The access points are configured with multiple VLAN's and there are many users within each VLAN. Each access point has the virtual router as its master controller. • Each VLAN is configured with different authentication mechanisms like Open System , Pre-Shared key, MAC authentication and different encryption methods like WPA2-PSK, WPA2-PSK-AES etc to compare the different authentication and encryption methods and identify the most efficient ones.

1) Aruba 650 Mobility Controller: The Aruba 650 Branch Mobility Controller is a compact, low cost effective all-in-one network solution. The 650 Mobility Controller includes a firewall, a WLAN (WLAN) controller, an 8-port Ethernet switch with PoE +, an IP router, a Site to site VPN edge device, a file server, and a print server in an attractive desktop-mount enclosure.

The 650 Mobility Controller can be deployed, monitored, and operated without the help of local IT thanks to Aruba's centralized zero-touch configuration and administration paradigm. Remote management and local configuration via a web interface are two other deployment alternatives.

To manage complicated and processor-intensive administration and security activities, the 650 relies on centralized Mobility Controllers in the data center. Edge services are virtualized and installed in branch offices using low-cost 650 Mobility Controllers that send user traffic to data center controllers over secure IP tunnels over a public or private transport network.

When used in conjunction with any Aruba access point (AP), the 650 Mobility Controller delivers local wireless services, or it can be utilized as a wired-only device.

Fig. 2. Aruba 650 mobility controller

2) Aruba AP-105 Access Point: The AP-105 is a multifunction indoor 802.11n access point (AP) that is ideal for high-density deployments in workplaces, hospitals, schools, and retail establishments. Warehouses and other high-ceiling facilities benefit from the integrated omni-directional downtilt antennas. The AP-105 is a small, high-speed router that provides wire-like performance at data speeds of up to 300 Mbps per radio.

The AP-105 has two internal omni-directional antennas and two 2x2 MIMO dual-band 2.4GHz/5GHz radios.

802.11n allows you to use wireless as a primary connection with the same speed and dependability as a wired LAN. It also improves performance by including channel bonding, block acknowledgement, and MIMO radios. Range and reliability are also improved with advanced antenna technology.

Aruba's innovative Adaptive Radio Management and spectrum analysis capabilities, which control the 2.4-GHz and 5-GHz radio bands to ensure optimal client performance while reducing any RF

interference, are the key to ensuring wire-like performance and dependability.

Fig. 3. Aruba AP-105 Access Point

IV. Technological Description

A. IP Address and Subnetting

1) IP Addressing: A 32-bit number is an IP address. On a TCP/IP network, it uniquely identifies a host (computer or other device, such as a printer or router).

192.168.123.132 is an example of a dotted-decimal IP address, which has four integers separated by periods. Examine an IP address in binary notation to see how subnet masks are used to distinguish between hosts, networks, and subnetworks.

The dotted-decimal IP address 192.168.123.132, for example, is the 32-bit number 11000000010100011110111000100 in binary notation. Divide this number into four parts of eight binary digits to make it easier to understand.

The routers that transfer packets of data between networks don't know the actual location of a host for which a packet of information is destined, therefore a TCP/IP wide area network (WAN) can function efficiently as a collection of networks. Routers only know which network the host belongs to, and they utilize data from their route table to figure out how to get the packet to the destination host's network. The packet is delivered to the proper host after it has been delivered to the destination's network.

For this process to work, an IP address has two parts. The first part of an IP address is used as a network address, the last part as a host address. If you take the example 192.168.123.132 and divide it into these two parts, you get 192.168.123. Network .132 Host or 192.168.123.0 - network address. 0.0.0.132 - host address.

2) Subnetting: Internet addresses are allocated by the InterNIC, the organization that administers the Internet. These IP addresses are divided into classes. The most common of them are classes A, B, and C. Classes D and E exist, but aren't used by end users. Each of the address classes has a different default subnet mask. You can identify the class of an IP address by looking at its first octet. Following are the ranges of Class A, B, and C Internet addresses, each with an example address:

- Class A networks use a default subnet mask of 255.0.0.0 and have 0-127 as their first octet. The address 10.52.36.11 is a class A address. Its first octet is 10, which is between 1 and 126, inclusive.
- Class B networks use a default subnet mask of 255.255.0.0 and have 128-191 as their first octet. The address 172.16.52.63 is a class B address. Its first octet is 172, which is between 128 and 191, inclusive.
- Class C networks use a default subnet mask of 255.255.255.0 and have 192-223 as their first octet. The address 192.168.123.132 is a class C address. Its first octet is 192, which is between 192 and 223, inclusive.

A Class A, B, or C TCP/IP network can be further divided, or subnetted, by a system administrator. It becomes necessary as you reconcile the logical address scheme of the Internet (the abstract world of IP addresses and subnets) with the physical networks in use by the real world.

A system administrator who is allocated a block of IP addresses may be administering networks that aren't organized in a way that easily fits these addresses. For example, you have a wide area network with 150 hosts on three networks (in different cities) that are connected by a TCP/IP router. Each of these three networks has 50 hosts. You are allocated the class C network 192.168.123.0. (For illustration,

this address is actually from a range that isn't allocated on the Internet.) It means that you can use the addresses 192.168.123.1 to 192.168.123.254 for your 150 hosts.

Using a subnet mask of 255.255.255.192, your 192.168.123.0 network then becomes the four networks 192.168.123.0, 192.168.123.64, 192.168.123.128 and 192.168.123.192. These four networks would have as valid host addresses:

192.168.123.1-62 192.168.123.65-126 192.168.123.129-190 192.168.123.193-254

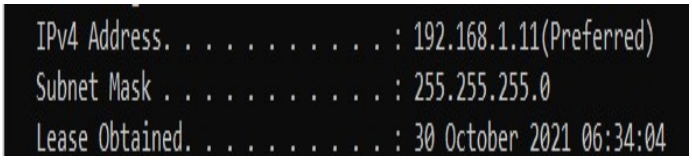


Fig. 4. Example of IP Addressing and Subnetting

B. Backup and Redundancy

The process of adding more instances of network devices and lines of communication to assist assure network availability and reduce the chance of failure along the crucial data channel is known as network redundancy.

There are two forms of network redundancy:

Fault Tolerance: A fault-tolerant redundant system mirrors applications across two or more identical systems that run in parallel, providing full hardware redundancy. If something goes wrong with the primary system, the mirrored backup system will take over and provide service without interruption. Fault-tolerance redundant systems are hard and frequently expensive to develop, but they are ideal for any business where any amount of downtime is undesirable (such as industrial or healthcare applications).

High Availability (HA) is a software-based redundancy system that uses clusters of servers to monitor each other and implement failover protocols. If one of the servers fails, the backup servers take over and restart any programs that were previously executing on the failed server. This solution to network redundancy requires less infrastructure, but it does tolerate some downtime in the form of a momentary interruption of service as backup servers start up applications.

1) Virtual Router Redundancy Protocol: The Virtual Router Redundancy Protocol (VRRP) eliminates the single point of failure that comes with a static default routed network. VRRP is an election protocol that distributes responsibility for a virtual router (a VPN 3000 Series Concentrator cluster) to one of the VPN Concentrators on a LAN on a LAN-wide basis. The Primary is the VRRP VPN Concentrator that manages the IP address(es) connected with a virtual router and directs traffic to those IP addresses. When the primary VPN Concentrator is offline, a backup VPN Concentrator takes over.

The benefits of VRRP include:

VRRP provides redundancy by allowing you to designate numerous routers as the default gateway router, reducing the risk of a single point of failure in a network.

Load Sharing—You can set up VRRP so that traffic to and from LAN clients is shared among many routers, distributing traffic load more evenly among available routers.

Multiple Virtual Routers—If the platform supports multiple MAC addresses, VRRP can support up to 255 virtual routers (VRRP groups) on a router physical interface. With the capability for multiple virtual routers, you may integrate redundancy and load sharing in your LAN architecture.

Multiple IP Addresses—The virtual router may handle a variety of IP addresses, including secondary addresses. As a result, you can configure VRRP on each subnet if you have multiple subnets defined on an Ethernet interface.

VRRP's redundancy strategy allows you to preempt a backup virtual router that has taken over for a failed master virtual router with a higher-priority backup virtual router that has become available, thanks to the redundancy scheme.

Text Authentication—By creating a basic text password, you may verify that VRRP communications received from VRRP routers that make up a virtual router are authorized.

VRRP advertising use a specific Internet Assigned Numbers Authority (IANA) standard multicast address (224.0.0.18) assigned by the Internet Assigned Numbers Authority (IANA). This addressing system reduces the number of routers required to handle multicasts while also allowing test equipment to identify VRRP packets on a segment

reliably. VRRP has the IP protocol number 112 assigned by the IANA.

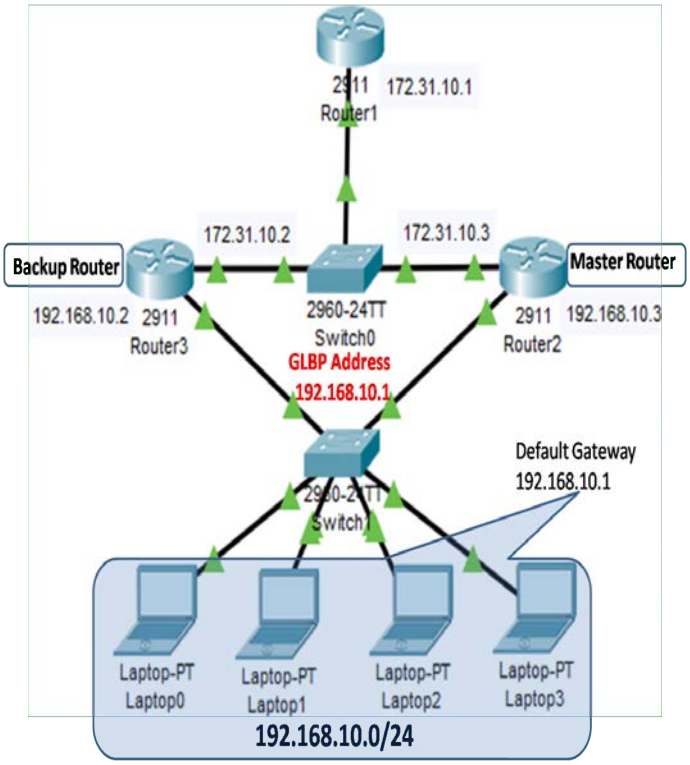


Fig. 5. Redundancy using virtual router redundancy protocol

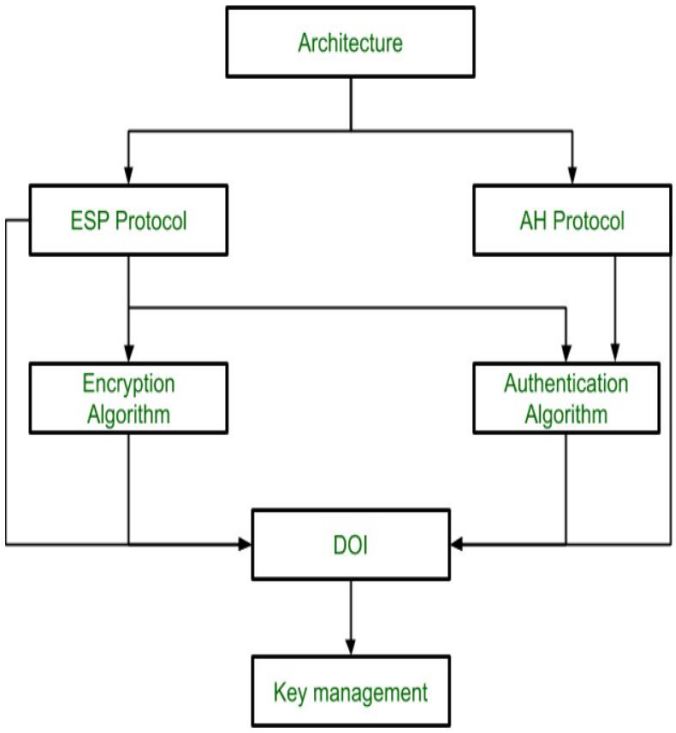


Fig. 6. IP Sec Architecture

C. IP Security

IP security (IPSec) is an Internet Engineering Task Force (IETF) standard suite of protocols that offer data authentication, integrity, and confidentiality between two communication points over an IP network.

Aruba offers the following security features:

1) AAA - Authentication, Authorization and Accounting: AAA is a framework for limiting access to computer resources intelligently, enforcing policies, auditing consumption, and delivering the data needed to bill for services. For successful network administration and security, these processes must function together.

- Authentication Before access to the network is given, authentication provides a mechanism of identifying a user, often by requiring the user to submit a valid username and password. For network access, authentication is predicated on each user having a unique set of login credentials. The AAA server validates a user's authentication credentials against those stored in a database, in this instance Active Directory. The user is permitted network access if his or her login credentials match. If the credentials don't match, authentication fails and network access is denied.
- Authorization After authentication, a user needs obtain authorisation in order to perform particular operations. A user may attempt to issue commands after logging into a system, for example. The authorization procedure decides whether or not the user is authorized to issue such commands. Simply described, authorization is the process of implementing regulations by establishing what kinds or characteristics of activities, resources, or services a user is allowed to engage in. Authentication is usually the setting in which authorization takes place. After a user has been authenticated, they may be granted several types of access or activities. When it comes to RADIUS and 802.1x network authentication, authorization can be used to determine which VLAN, Access Control List (ACL), or user role a user belongs to.

- Accounting Accounting is the final component of the AAA architecture, and it keeps track of how much bandwidth a user uses while on the network. The amount of system time or the amount of data delivered and received during a session are examples of this. Accounting is done by keeping track of session statistics and consumption data. It's utilized for permission management, billing, trend analysis, resource allocation, and data capacity planning for commercial operations. The ClearPass Policy Manager serves as an accounting server, receiving user accounting data from the Network Access Server (NAS). ClearPass Policy Manager must be configured to use the NAS as an accounting server, and the NAS must deliver appropriate accounting information to ClearPass Policy Manager.

  In ArubaOS-Switch Version 16.05.4, four AAA security enhancements have been included.

  Open Authentication (OpenAuth) Role: The Open Authentication (OpenAuth) Role allows a device to gain network access before going through the authentication process.

  Critical Authentication: This feature enhancement supports the concept of a "Critical VLAN," in which a client is placed in a "Critical VLAN" if a remote authentication scenario, such as MAC-Auth or 802.1X, begins but the authentication server is unavailable.

  Per-Port Initial Role: ArubaOS-Switches provides an initial role that is applied to clients who are refused by the radius server or clients that fail authentication owing to radius unreachability. The initial role can be adjusted to allow limited download supplicant access or to be utilized for a Wired Guest access solution.

  LMA/MAC-based authenticated clients will remain authenticated in the switch even if they are inactive throughout the log-off time if the MAC Pinning feature is activated.

V. Project Design

The project design can be split into 5 sections:

- IP Design
- Redundancy Design
- Wired Design
- Wireless Design
- Security Design

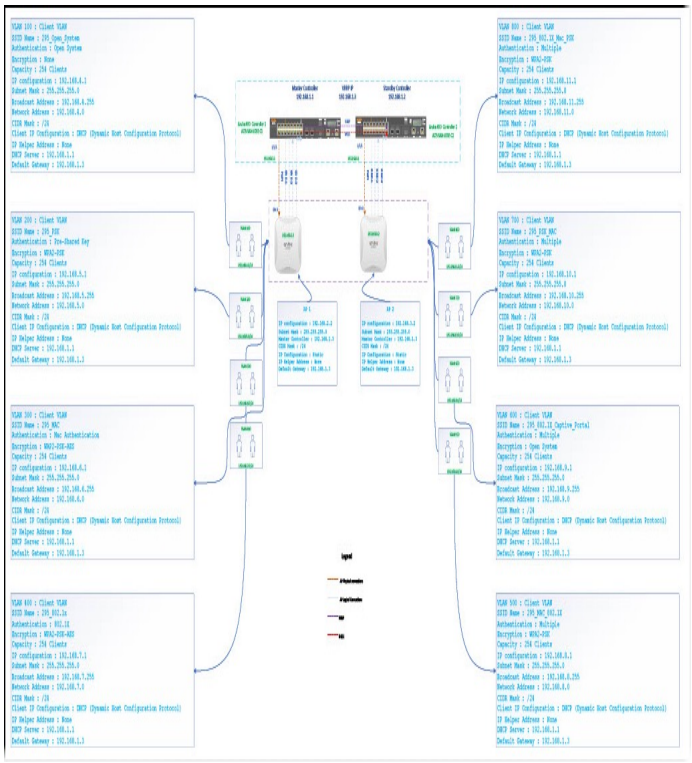


Fig. 7. Low level design architecture of enterprise grade wireless network

The enterprise grade wireless network topology consists of two wireless controllers which has an access point connected to them. The controller acts as the default gateway to the access point.

Redundancy is provided between the two controllers using VRRP (Virtual Router Redundancy Protocol). This ensures that Controller 1 which acts as master will have controller 2 to back up in case of failure or unavailability.

The controllers are secured using IPSEC (IP Security) protocol to ensure authentication and secure encryption of packets.

The access points are configured with multiple VLAN's and there are many users within each VLAN. Each access point has the virtual router as its master controller.

Each VLAN is configured with different authentication mechanisms like Open System , Pre-Shared key, MAC authentication and different encryption methods like WPA2-PSK, WPA2-PSK-AES etc to compare the different authentication and encryption methods and identify the most efficient ones.

1) IP Design: Every device connected over the IP network has to be assigned a unique IP address. The IP address contains two components: the higher-order bits representing the network prefix and lower-order bits representing the host identifier. Depending on the number of octets that constitute the network prefix, they can be classified into five classes A, B, C, and E. The above sample network is for the purpose of understanding the assignment of IP addresses. IPv4 addressing is used in the sample network. The Class C private address range 192.168.0.0 - 192.168.255.255 could be used to allocate the IP addresses on the network. The default gateways are configured to be 192.168.2.1 and 192.168.1.1. Laptops, mobile phones, personal computers, and wearable smart gadgets act as clients on the network.

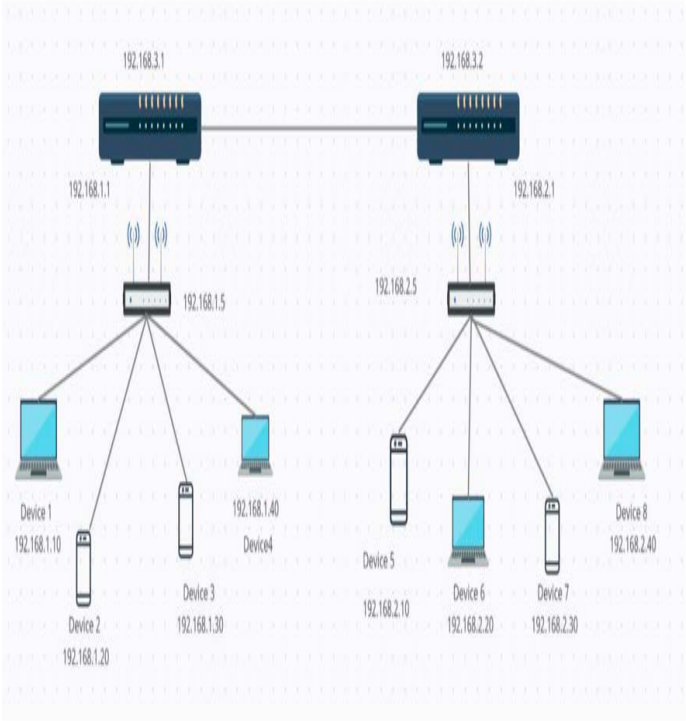


Fig. 8. IP design architecture

The devices are assigned IP address using the following command, ip address IP ADDRESS SUBNET MASK The default gateway can be configured using the following command, ip default-gateway IP ADDRESS

The table shows routers and their corresponding IP addresses with the subnet mask.

Table 3: IP Address Assignment for Router 1 and 2

Device	IP Address	Subnet Mask
Router 1	192.168.1.1 192.168.3.1	255.255.255.0
Router 2	192.168.2.1 192.168.3.2	255.255.255.0

Fig. 9. IP address for router 1 and 2

The table shows all the hosts and their corresponding IP addresses with a default gateway.

2) Security Design: Security Design includes the provision of IPSec between the controllers and the implementation of CPSec between the controller and access point for the controller to take control of the access point. IPSec between the two controllers ensures authentication and secure encryption of packets and also provides secure communication. It can be implemented as follows: crypto isakmp ipsec-over-tcp [port port 1...port0]

Ex: Crypto isakmpo ctcp port 45 ensures ipsec over tcp on port 45. CPSec which stands for control plane security is a method of sending certificates to those access point's which have been identified as valid AP's to control the access points. In order to obtain closer control, it is required to manually include each campus and remote AP's to the whitelists.

CPSec can be configured on the device manually as follows: The following procedure describes how to create the initial CPsec configuration. • In the Managed Network node hierarchy, navigate to the Configuration ¿ System ¿ CPSec tab. • Select the Control Plane Security accordion. • Click the Enable CPSEC toggle switch to enable this setting. • Click Submit. • Click Pending Changes. • In the Pending Changes window, select the check box and click Deploy changes

3) Redundancy Design: The measure of a good network design is the provision of a backup in order to avoid fatal network crash and ensure its

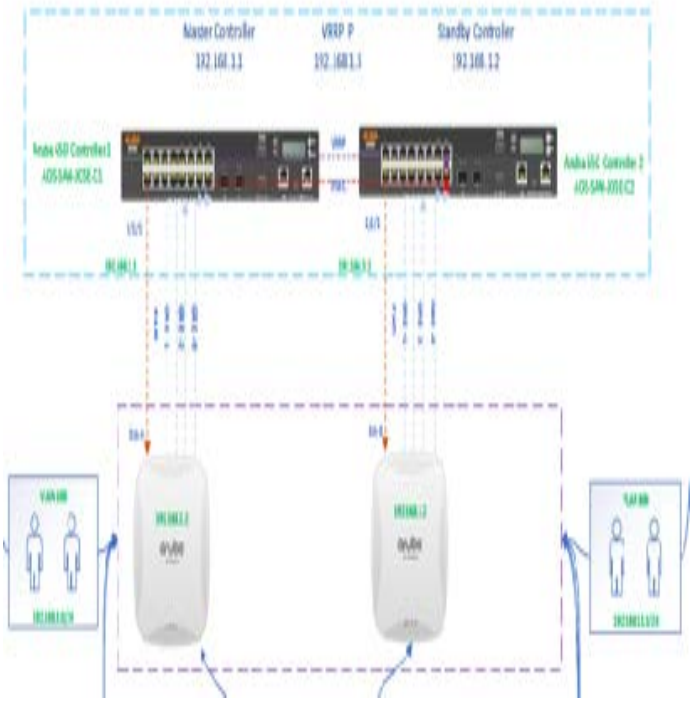


Fig. 10. Security Design Architecture

availability. In our project, we plan to implement redundancy using VRRP (Virtual Router Redundancy Protocol). VRRP protocol specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on the LAN. The VRRP Router is called the master router and the protocol provides dynamic failover in the forwarding responsibility when the master is unavailable.

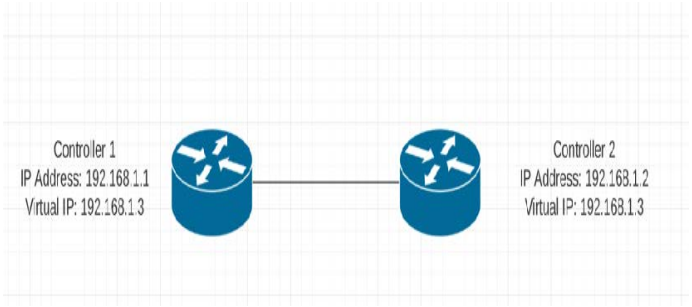


Fig. 11. Redundancy Design

Controller 1 is configured with an IP Address of 192.168.1.1 and controller 2 has an IP Address of 192.168.1.2. The redundancy is provided as follows : Controller 1 is assigned a virtual IP as 192.168.1.3 using the following command: vrrp 1 ip address 192.168.1.3 where 10 represents the vrrp group id

Controller 2 is configured with the same virtual group id and ip address.

Initially controller 1 is assigned a priority of 100 and will become the Master controller .

When controller 1 goes down or is unavailable, the controller 2 becomes the backup as both belong to the same virtual group and takes over the packet forwarding

If controller 2 should be made the master, then its priority has to be changed using the command Vrrp 1 priority 200. High priority device takes on the role of the master.

Device	IP Address	Subnet Mask	Default Gateway
Device 1	192.168.1.10	255.255.255.0	192.168.1.1
Device 2	192.168.1.20	255.255.255.0	192.168.1.1
Device 3	192.168.1.30	255.255.255.0	192.168.1.1
Device 4	192.168.1.40	255.255.255.0	192.168.1.1
Device 5	192.168.2.10	255.255.255.0	192.168.2.1
Device 6	192.168.2.20	255.255.255.0	192.168.2.1
Device 7	192.168.2.30	255.255.255.0	192.168.2.1
Device 8	192.168.2.40	255.255.255.0	198.168.2.1

Fig. 12. IP address for end devices

VI. Implementation and Results

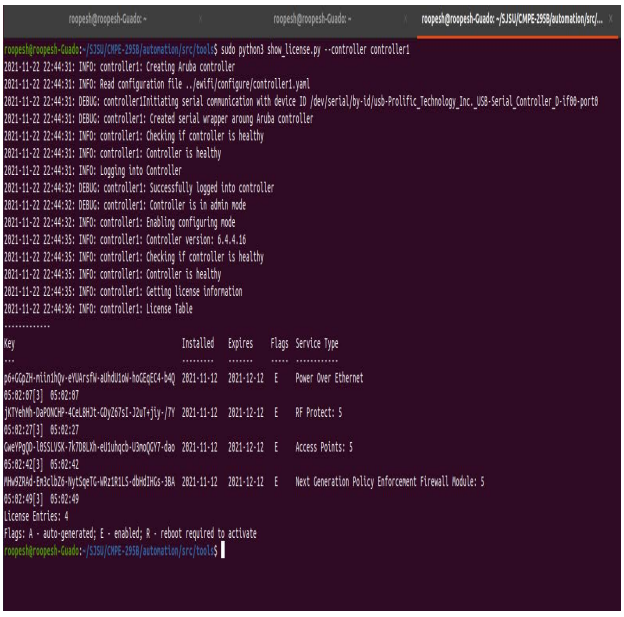
The implementation of the protocols and its output are as follows:

The lab setup includes an Aruba 650 controller to which two or more Aruba AP-105 access points are connected to the PAPI port via ethernet. The AP1 is connected to the master controller while AP2 is connected to the standby controller. The master and the standby are linked using the virtual routing redundancy protocol for backup. The rest of the ports on AP are connected to controller using

the GRE tunnel. The controller is connected to the laptop for control using the serial interface.

Fig. 13. Lab Setup of an enterprise grade wireless network

The fig(14) shows the license information for the aruba controllers and acccess points used and it is used to activate the different features provided. It is implemented using a python file and imported later.



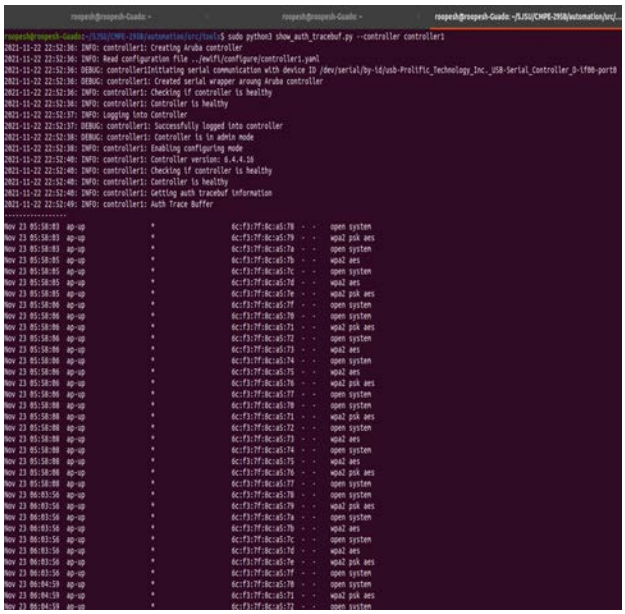
```
roopesh@roopesh-Guadc: ~                roopesh@roopesh-Guadc: ~                roopesh@roopesh-Guadc: ~/SJSU/CMPE-295B/automation/src/...
roopesh@roopesh-Guadc:~/SJSU/CMPE-295B/automation/src/tools$ sudo python3 show_license.py --controller controller1
2021-11-22 22:44:31: INFO: controller1: Creating Aruba controller
2021-11-22 22:44:31: INFO: Read configuration file ../ewifi/configure/controller1.yaml
2021-11-22 22:44:31: DEBUG: controller1Initiating serial communication with device ID /dev/serial/by-id/usb-Prolific_Technology_Inc._USB-Serial_Controller_D-if00-port0
2021-11-22 22:44:31: DEBUG: controller1: Created serial wrapper around Aruba controller
2021-11-22 22:44:31: INFO: controller1: Checking if controller is healthy
2021-11-22 22:44:31: INFO: controller1: Controller is healthy
2021-11-22 22:44:31: INFO: Logging into Controller
2021-11-22 22:44:32: DEBUG: controller1: Successfully logged into controller
2021-11-22 22:44:32: DEBUG: controller1: Controller is in admin mode
2021-11-22 22:44:32: INFO: controller1: Enabling configuring mode
2021-11-22 22:44:33: INFO: controller1: Controller version: 6.4.4.16
2021-11-22 22:44:33: INFO: controller1: Checking if controller is healthy
2021-11-22 22:44:33: INFO: controller1: Controller is healthy
2021-11-22 22:44:35: INFO: controller1: Getting license information
2021-11-22 22:44:36: INFO: controller1: License Table
.............
Key                                    Installed   Expires     Flags  Service Type
---                                    .........   .......     -----  ............
p6+GQpZH-mtn1hQv-eVUArsfU-aUhdUtoH-hoGEgEC4-b4Q  2021-11-12  2021-12-12  E    Power Over Ethernet
05:02:07[3]  05:02:07
jK7YeVHh-DaPONCHP-4CeL8H2t-GDy267sI-J2uT+jIy-/7Y  2021-11-12  2021-12-12  E    RF Protect: 5
05:02:27[3]  05:02:27
GweVPgQD-lOSSlVSK-7kTD8LXh-eUIuhqcb-U3moQCY7-dao  2021-11-12  2021-12-12  E    Access Points: 5
05:02:42[3]  05:02:42
MHwQZR6d-Ex3clbZ6-HytSQeTG-WRzIRILS-dbHdIHGs-3BA  2021-11-12  2021-12-12  E    Next Generation Policy Enforcement Firewall Module: 5
05:02:49[3]  05:02:49
License Entries: 4
Flags: A - auto-generated; E - enabled; R - reboot required to activate
roopesh@roopesh-Guadc:~/SJSU/CMPE-295B/automation/src/tools$
```

Fig. 14. License information of different devices used

We then move on to implementing the different authentication for vlans on the AP's. The following commands are used to create a WPA2-PSK and AES encryption on one of the AP's.

- **encryption mode ciphers aes-ccm**
- **authentication key-management wpa version 2**
- **wpa-psk ascii 0 aruba aruba**

In the same way we will be adding authentication methods to rest of vlans and AP's. The traceauth command is used to display the AP's along with the authentication configured on it.



```
roopesh@roopesh-Guadc: ~                roopesh@roopesh-Guadc: ~                roopesh@roopesh-Guadc: ~/SJSU/CMPE-295B/automation/src/...
roopesh@roopesh-Guadc:~/SJSU/CMPE-295B/automation/src/tools$ sudo python3 show_auth_tracebuf.py --controller controller1
2021-11-22 22:52:36: INFO: controller1: Creating Aruba controller
2021-11-22 22:52:36: INFO: Read configuration file ../ewifi/configure/controller1.yaml
2021-11-22 22:52:36: DEBUG: controller1Initiating serial communication with device ID /dev/serial/by-id/usb-Prolific_Technology_Inc._USB-Serial_Controller_D-if00-port0
2021-11-22 22:52:36: DEBUG: controller1: Created serial wrapper around Aruba controller
2021-11-22 22:52:36: INFO: controller1: Checking if controller is healthy
2021-11-22 22:52:36: INFO: controller1: Controller is healthy
2021-11-22 22:52:37: INFO: Logging into Controller
2021-11-22 22:52:37: DEBUG: controller1: Successfully logged into controller
2021-11-22 22:52:38: DEBUG: controller1: Controller is in admin mode
2021-11-22 22:52:38: INFO: controller1: Enabling configuring mode
2021-11-22 22:52:40: INFO: controller1: Controller version: 6.4.4.16
2021-11-22 22:52:40: INFO: controller1: Checking if controller is healthy
2021-11-22 22:52:40: INFO: controller1: Controller is healthy
2021-11-22 22:52:48: INFO: controller1: Getting auth tracebuf information
2021-11-22 22:52:49: INFO: controller1: Auth Trace Buffer
...............
Nov 23 05:58:03  ap-up          *               0c:f1:7f:8c:a5:78  -  -   open system
Nov 23 05:58:03  ap-up          *               0c:f1:7f:8c:a5:79  -  -   wpa2 psk aes
Nov 23 05:58:03  ap-up          *               0c:f1:7f:8c:a5:7a  -  -   open system
Nov 23 05:58:05  ap-up          *               0c:f1:7f:8c:a5:7b  -  -   wpa2 aes
Nov 23 05:58:05  ap-up          *               0c:f1:7f:8c:a5:7c  -  -   open system
Nov 23 05:58:05  ap-up          *               0c:f1:7f:8c:a5:7d  -  -   wpa2 aes
Nov 23 05:58:05  ap-up          *               0c:f1:7f:8c:a5:7e  -  -   wpa2 psk aes
Nov 23 05:58:06  ap-up          *               0c:f1:7f:8c:a5:7f  -  -   open system
Nov 23 05:58:06  ap-up          *               0c:f1:7f:8c:a5:70  -  -   open system
Nov 23 05:58:06  ap-up          *               0c:f1:7f:8c:a5:71  -  -   wpa2 psk aes
Nov 23 05:58:06  ap-up          *               0c:f1:7f:8c:a5:72  -  -   open system
Nov 23 05:58:06  ap-up          *               0c:f1:7f:8c:a5:73  -  -   wpa2 aes
Nov 23 05:58:06  ap-up          *               0c:f1:7f:8c:a5:74  -  -   open system
Nov 23 05:58:06  ap-up          *               0c:f1:7f:8c:a5:75  -  -   wpa2 aes
Nov 23 05:58:06  ap-up          *               0c:f1:7f:8c:a5:76  -  -   wpa2 psk aes
Nov 23 05:58:06  ap-up          *               0c:f1:7f:8c:a5:77  -  -   open system
Nov 23 05:58:08  ap-up          *               0c:f1:7f:8c:a5:78  -  -   open system
Nov 23 05:58:08  ap-up          *               0c:f1:7f:8c:a5:79  -  -   wpa2 psk aes
Nov 23 05:58:08  ap-up          *               0c:f1:7f:8c:a5:72  -  -   open system
Nov 23 05:58:08  ap-up          *               0c:f1:7f:8c:a5:73  -  -   wpa2 aes
Nov 23 05:58:08  ap-up          *               0c:f1:7f:8c:a5:74  -  -   open system
Nov 23 05:58:08  ap-up          *               0c:f1:7f:8c:a5:75  -  -   wpa2 aes
Nov 23 05:58:08  ap-up          *               0c:f1:7f:8c:a5:76  -  -   wpa2 psk aes
Nov 23 05:58:08  ap-up          *               0c:f1:7f:8c:a5:77  -  -   open system
Nov 23 06:03:56  ap-up          *               0c:f1:7f:8c:a5:78  -  -   open system
Nov 23 06:03:56  ap-up          *               0c:f1:7f:8c:a5:79  -  -   wpa2 psk aes
Nov 23 06:03:56  ap-up          *               0c:f1:7f:8c:a5:7a  -  -   open system
Nov 23 06:03:56  ap-up          *               0c:f1:7f:8c:a5:7b  -  -   wpa2 aes
Nov 23 06:03:56  ap-up          *               0c:f1:7f:8c:a5:7c  -  -   open system
Nov 23 06:03:56  ap-up          *               0c:f1:7f:8c:a5:7d  -  -   wpa2 aes
Nov 23 06:03:56  ap-up          *               0c:f1:7f:8c:a5:7e  -  -   wpa2 psk aes
Nov 23 06:03:56  ap-up          *               0c:f1:7f:8c:a5:7f  -  -   open system
Nov 23 06:04:59  ap-up          *               0c:f1:7f:8c:a5:70  -  -   open system
Nov 23 06:04:59  ap-up          *               0c:f1:7f:8c:a5:71  -  -   wpa2 psk aes
Nov 23 06:04:59  ap-up          *               0c:f1:7f:8c:a5:72  -  -   open system
```

Fig. 15. Tracing authentication implemented on the AP's

The image below displays the list of virtual AP's or the virtual LAN's that have been implemented. We can create virtual LAN using the command

- **vlan vlan number**

Show the list of access points in the controller's database.The show ap database command is used to display the information of the entire AP that has been implemented including its IP address and current status. The output of the command show ap database shows the controller's database of information for APs in the group default. The output also includes a description of the flag types that may appear in the Flags column.

This command shows a configured VLAN interface number, description and associated ports. Issue this command to show the selected VLAN configuration. The VLAN column lists the VLAN

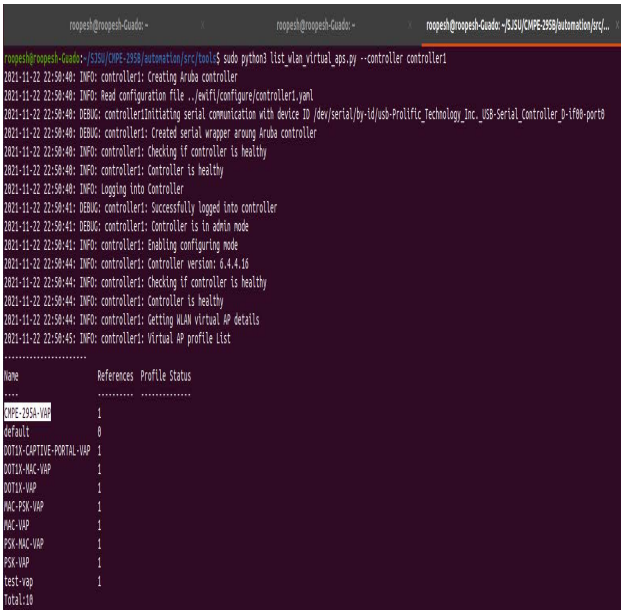


Fig. 16. Display the virtual AP's

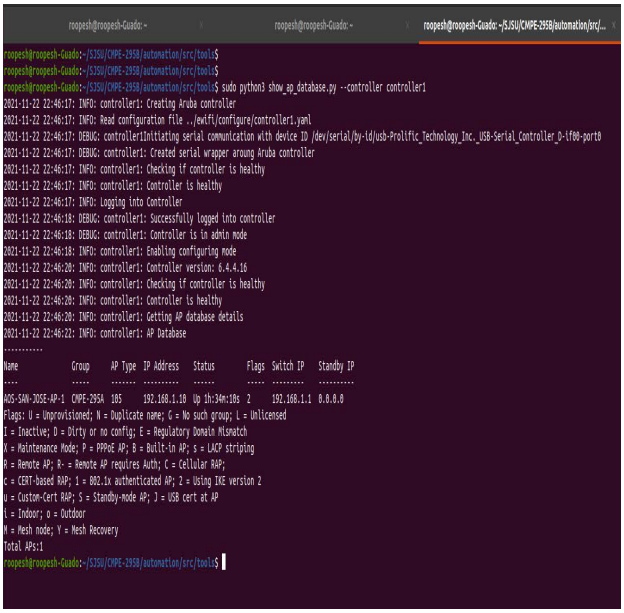


Fig. 17. Display the AP database

ID. The Description column provides the VLAN name or number and the Ports column shows the VLAN's associated ports. The AAA Profile column shows if a wired AAA profile has been assigned to a VLAN, enabling role-based access for wired clients connected to an untrusted VLAN or port on the controller.

Displays the list of all Virtual AP profiles, or detailed configuration information for a specific

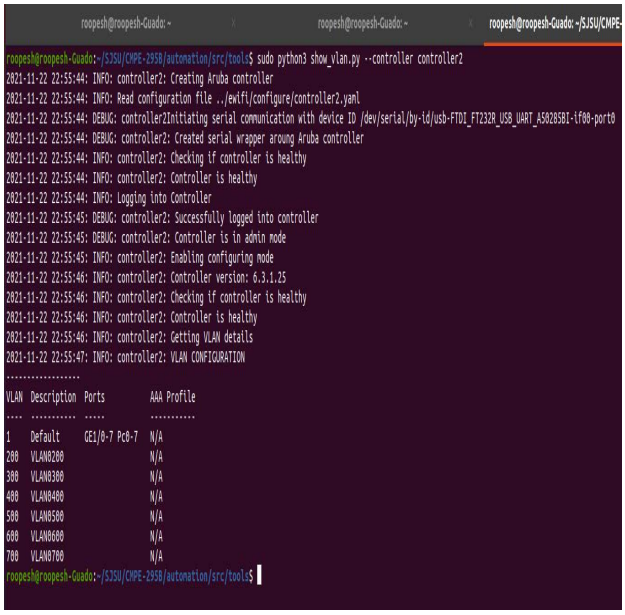


Fig. 18. Display the VLAN's configured

Virtual AP profile. Issue this command without the ¡profile-name¿ parameter to display the entire Virtual AP profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile. The output of this command includes the following parameters:

- Name : Displays the name of the Virtual AP profile.
- References : Displays the number of other profiles with references to the Virtual AP profile.
- Profile Status : Displays whether the Virtual AP profile is predefined.

Displays detailed information about the controller's connection to a user device, in regards to mobility state and statistics, authentication statistics, VLAN assignment method, AP datapath tunnel info, radius accounting statistics, user name, user-role derivation method, datapath session flow entries, and 802.11 association state and statistics. The show user command allows you to filter specific information by parameter. Use the show user-table command to show detailed user statistics which includes the entire output of the user-table, mobility state and statics, authentication statistics, VLAN assignment method, AP datapath tunnel information, radius accounting statistics, user-role derivation method, datapath session flow entries, and 802.11 association

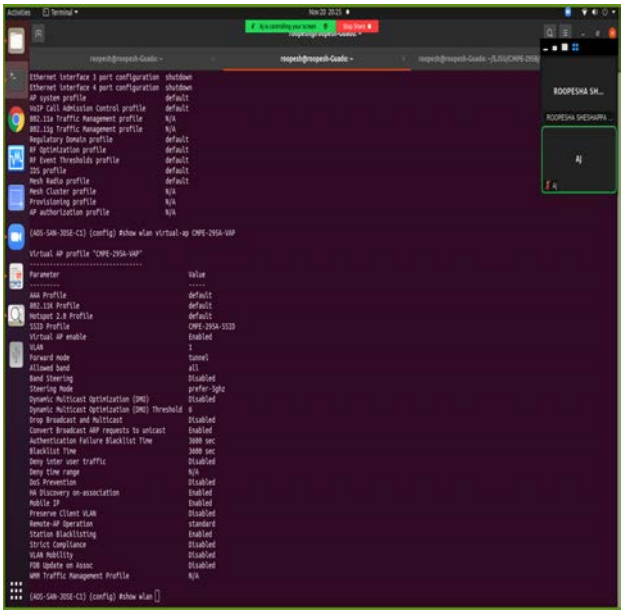


Fig. 19. WLAN interface of virtual AP

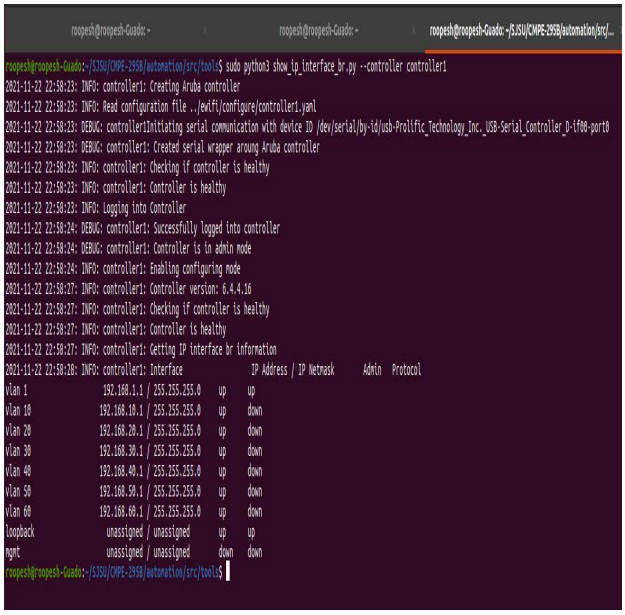


Fig. 21. IP Interface Table

state and statistics.

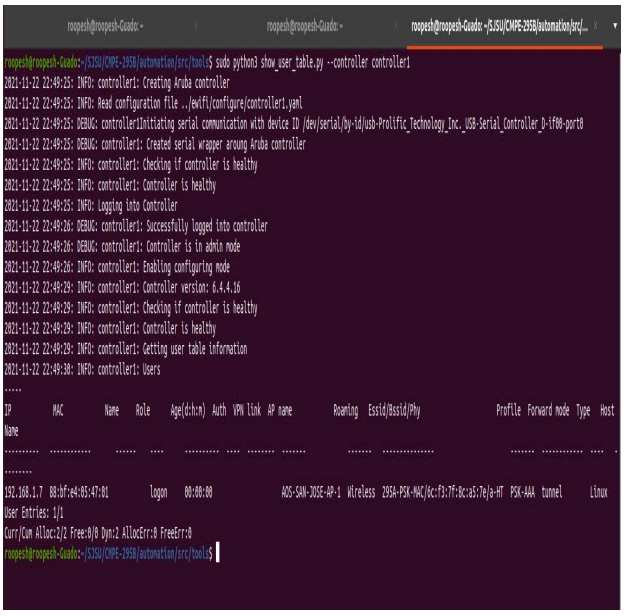


Fig. 20. User Table

This command displays a summary of IP related information for all interfaces configured on an IAP. Use this command to view a brief summary of IP related information for the IAP interfaces.

This command displays Internet Key Exchange (IKE) parameters for the Internet Security Association and Key Management Protocol (ISAKMP). Use the show crypto isakmp command to view ISAKMP settings, statistics and policies. The show crypto isakmp stats command shows the IKE statistics.

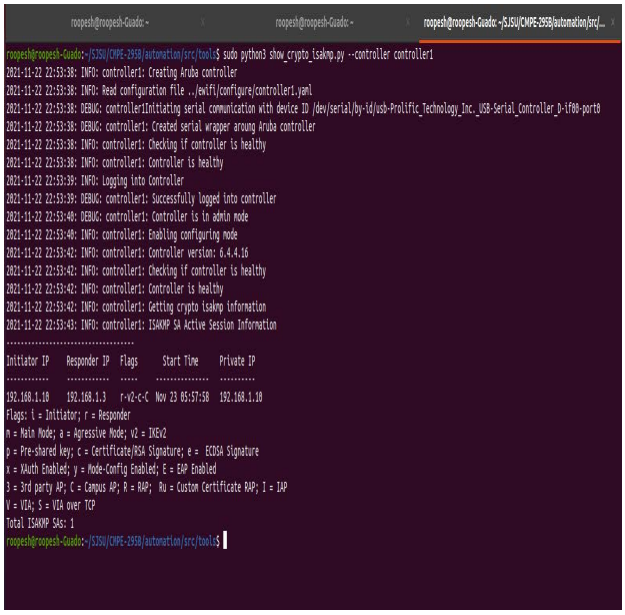


Fig. 22. Configuring internet key exchange for ISAKMP

The show ipsec data file is used to display the information of the different IP security policies implemented on the AP's.

This command shows the system statistics for your IAP. Use the show datapath command to

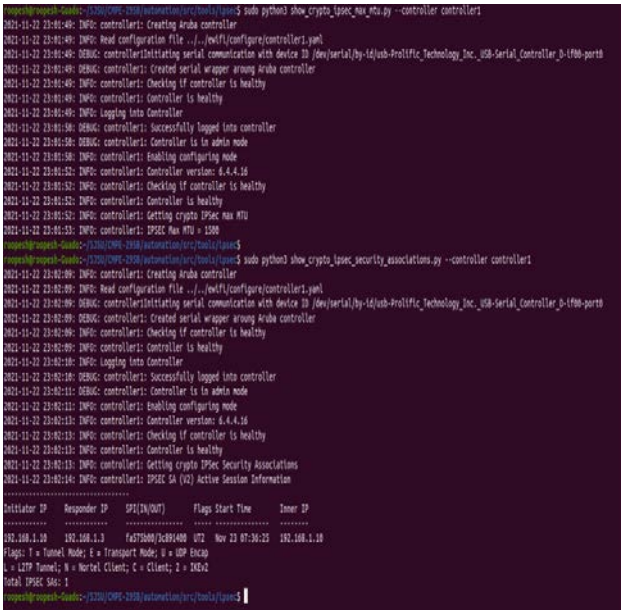


Fig. 23. IPSec Table

display various datapath statistics for debugging purposes.

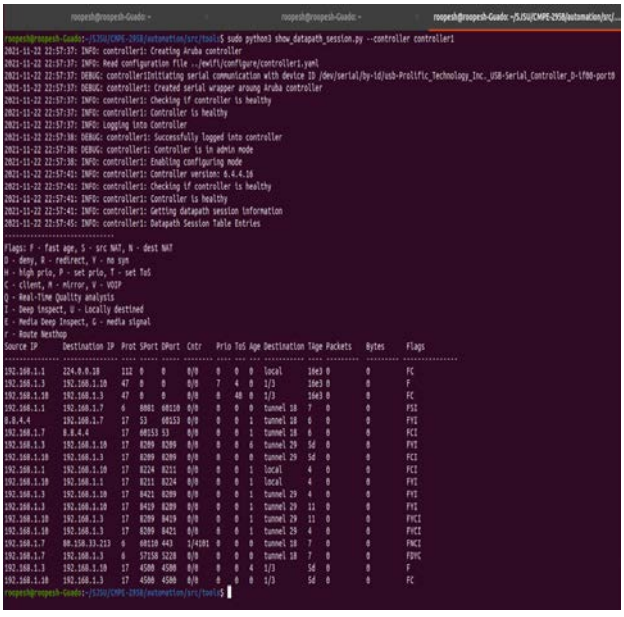


Fig. 24. Datapath session information

This command shows an ESSID summary for the controller, including the number of APs and clients associated with each ESSID. The output of this command includes the following information:

- ESSID : An Extended Service Set Identifier (ESSID) is the identifying name of an 802.11 wireless network.
- APs : Number of APs associated with the ESSID.
- MBSSID Tx BSS : (ArubaOS 8.9.0.0 or later versions). Number of APs that have the specific BSSID or virtual AP as the transmitted virtual AP.
- Clients : Number of clients associated with the ESSID.
- VLAN(s) : VLAN IDs of the VLANs for the ESSID.
- Encryption : The layer-2 authentication and encryption used on this ESSID to protect access and ensure the privacy of the data transmitted to and from the network.

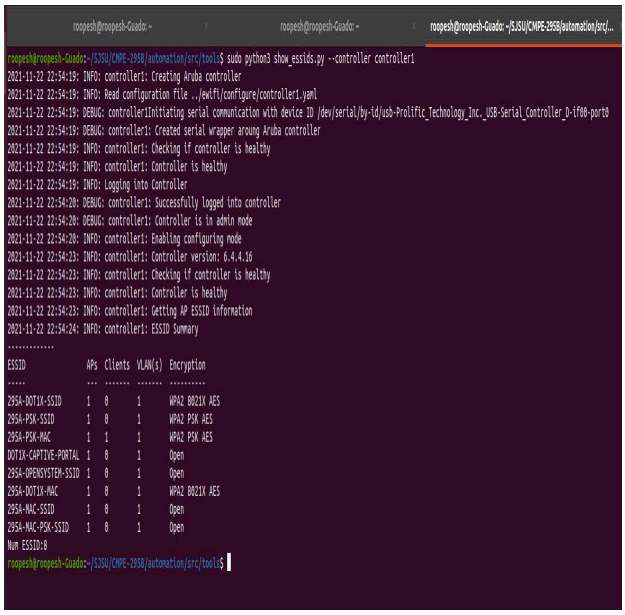


Fig. 25. SSID information

Displays the list of all VRRP configuration on the managed device. To view a specific VRRP configuration, specify the VRID number.

Displays the activity statistics on each of the port on the controller. The output of this command includes the following parameters:

- Slot-Port : Physical port in slot/module/port format.
- Port Type : Displays the type of physical port. FE: Fast Ethernet GE: Gigabit Ethernet PC: Port Channel
- Admin State : Indicates if the physical port is enabled or disabled.

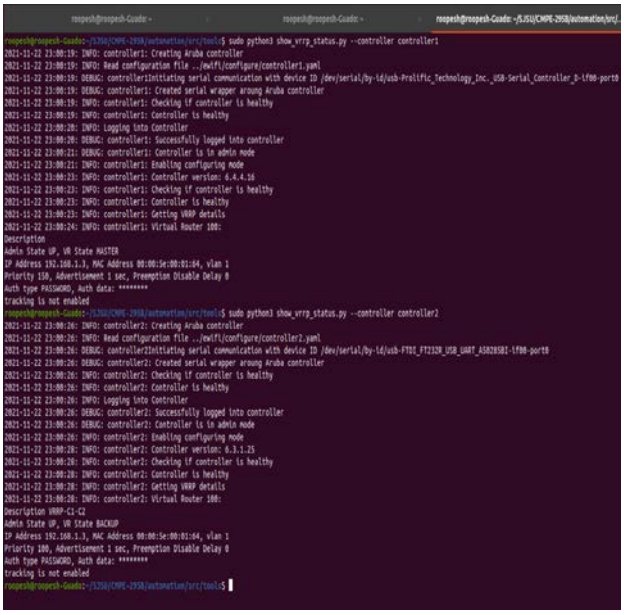


Fig. 26. Virtual Router redundancy protocol configuration

- Open State : Indicates if the current status of the physical port is up or down.
- PoE : Indicates if the physical port is Power over Ethernet (PoE) enabled
- SpanningTree : Indicates the state of spanning tree.

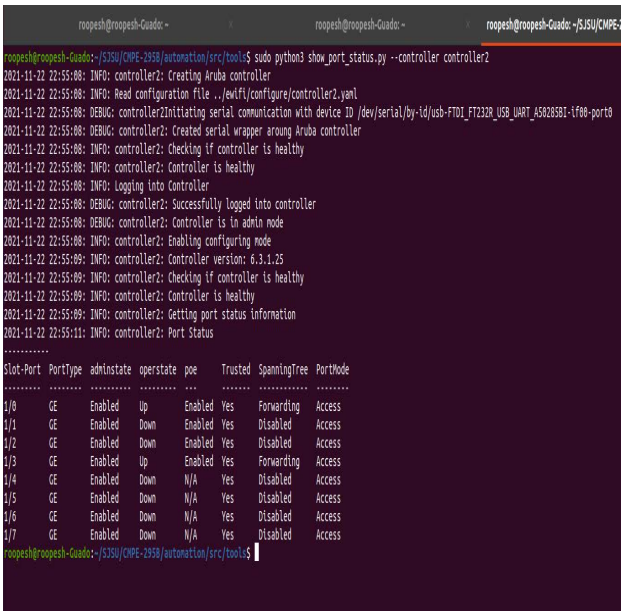


Fig. 27. Port information

VII. Conclusion and Future recommendations

Thus we have designed an enterprise grade wireless network using a combination of authentication protocols and used methods to compare the working of the different authentication protocols to find the best combination and also helped show the pro's and cons of using single and multiple authentications. This also helped gain a deeper understanding of different authentication and encryption algorithms as well as the working of Aruba devices and helped gain a real world perspective.

This can be further extended to larger networks spanning across multiple locations and thus can help take a step further in the provision of flawless network security.

References

[1] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, Ed., "Extensible Authentication Protocol (EAP)", RFC 3748, DOI 10.17487/RFC3748, June 2004,

[2] M. A. Abo-Soliman and M. A. Azer, "A study in WPA2 enterprise recent attacks," 2017 13th International Computer Engineering Conference (ICENCO), Cairo, Egypt, 2017, pp. 323-330, doi:10.1109/ICENCO.2017.8289808.

[3] A. Skendžić, B. Kovačić and L. Ljubičić, "Performance Analysis of Aruba wireless local network in Croatian Pension Insurance Institute," 2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO), Opatija, Croatia, 2020, pp. 1397-1401, doi: 10.23919/MIPRO48935.2020.9245371.

[4] Y. Durmus and K. Langendoen, "Wifi authentication through social networks — A decentralized and context-aware approach," 2014 IEEE International Conference on Pervasive Computing and Communication Workshops (PERCOM WORKSHOPS), Budapest, Hungary, 2014, pp. 532-538, doi: 10.1109/PerComW.2014.6815263.

[5] T. Radivilova and H. A. Hassan, "Test for penetration in Wi-Fi network: Attacks on WPA2-PSK and WPA2-enterprise," 2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Odessa, UKraine, 2017, pp. 1-4, doi: 10.1109/UkrMiCo.2017.8095429.

[6] M. Vanhoef and E. Ronen, "Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd," 2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2020, pp. 517-533, doi: 10.1109/SP40000.2020.00031.

[7] E. Khorov, A. Kiryanov, A. Lyakhov and G. Bianchi, "A Tutorial on IEEE 802.11ax High Efficiency WLANs," in IEEE Communications Surveys and Tutorials, vol. 21, no. 1, pp. 197-216, Firstquarter 2019, doi: 10.1109/COMST.2018.2871099.

[8] K. X. Miao, "Enterprise WiMAX building the next generation enterprise wireless infrastructure with WiMAX," 2010 International Conference on Wireless Information Networks and Systems (WINSYS), Athens, Greece, 2010, pp. 1-5.

[9] Y. Wang, Z. Jin and X. Zhao, ”Practical Defense against WEP and WPA-PSK Attack for WLAN,” 2010 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM), Chengdu, China, 2010, pp. 1-4, doi: 10.1109/WICOM.2010.5600921.

[10] O. Nakhila, A. Attiah, Y. Jin and C. Zou, ”Parallel active dictionary attack on WPA2-PSK Wi-Fi networks,” MILCOM 2015 - 2015 IEEE Military Communications Conference, Tampa, FL, USA, 2015, pp. 665-670, doi: 10.1109/MILCOM.2015.7357520.

[11] https://www.fortinet.com/resources/cyberglossary/wireless-network

[12] https://www.cdw.com/content/cdw/en/articles/datacenter/2019/03/26/what-are-the-differenttypes-of-wireless-networks.html

[13] https://www.pluralsight.com/blog/it-ops/wireless-encryption-authentication

[14] https://www.verkada.com/security-update/

[15] https://docs.microsoft.com/en-us/troubleshoot/windows-client/networking/tcpip-addressing-and-subnetting

[16] https://www.vxchnge.com/blog/network-redundancy-explained

[17] https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs-r4-0/addr-serv/configuration/guide/ic40crs1book-chapter10.html

[18] https://www.coursera.org/lecture/aruba-mobility-basics/wlan-security-and-access-control-aaa-authorization-authentication-and-accounting-T5bHW

[19] https://www.arubanetworks.com/techdocs/ArubaOS-64-Web-Help/Content/ArubaFrameStyles/Management-Utilities/Managing-Certificates.html

[20] https://www.arubanetworks.com/techdocs/ArubaOS-60/UserGuide/802.1x.php