Cisco AP WLAN Setup

Emma Matsuda

Advanced CCNP

**Purpose**

The main purpose of this lab is to discover about Wireless Local Area Networks and the application of the use of Cisco access points. In this lab, we used pre-shared keys and RADIUS servers to secure the connections. We set up WLANs with 3 SSIDs, two that were with WPA2-PSK and the other with WPA2-Enterprise (used with the RAIUDS server).

**Background Info**

Wireless Local Area Networks (WLANs) enable devices to connect wirelessly within a local area, eliminating the need for physical wired connections. These networks utilize radio waves at various frequencies, adhering to the IEEE 802.11 standard, where clients communicate with access points (APs) for network access. APs form the backbone of WLANs, providing not only wireless connectivity but also advanced security features and seamless roaming in larger networks. In our lab, we employed standalone APs, which function independently and are managed individually, making them ideal for the small network we created.

WLANs offer several advantages over wired networks, including mobility, scalability, flexibility, ease of installation, and security. Mobility allows users to move freely within coverage areas without losing connection. Scalability is achieved easily by adding more access points as needed. Flexibility enables WLANs to function in a variety of physical environments and organizational structures. The ease of installation is notable, as setting up a wireless network typically requires fewer components and less effort compared to wired networks. Lastly, WLANs can implement various security features such as WPA2, WPA3, or RADIUS servers to protect data effectively.

Focusing on security, this lab utilized Wi-Fi Protected Access 2 (WPA2) with Pre-Shared Keys (PSKs) and WPA2 with a RADIUS server. WPA2 secures wireless networks using AES (Advanced Encryption Standard) for encrypting data transmitted over radio waves. CCMP (Cipher Block Chaining Message Authentication Code Protocol) ensures data integrity by preventing tampering and ensuring packets remain unaltered during transit. WPA2 operates in two main modes: personal mode using PSK and enterprise mode using a RADIUS server.

Pre-Shared Keys (PSKs) are commonly used for wireless security, involving a password or key exchange between the client and AP for authentication and connection establishment. The password or phrase is processed through an algorithm to generate a 256-bit key, which is manually distributed to both the client and AP, then encrypted to secure the communication pathway. However, PSKs are less practical for larger networks due to the need for manual key updates on each client machine, and the security heavily depends on the password strength. Despite these limitations, PSKs are popular in smaller home and office networks due to their simplicity.

In contrast, WPA2-Enterprise networks utilize a RADIUS (Remote Authentication Dial-In User Service) server for centralized Authentication, Authorization, and Accounting (AAA) services. In enterprise networks, clients first interact with the RADIUS server rather than the AP directly. The client sends a network access request, initiating an EAP (Extensible Authentication Protocol) connection among the client, AP, and RADIUS server. The client provides credentials, which the RADIUS server verifies against its database or an external one. Upon successful verification, the server grants access, determines the user's authorization level, and monitors network usage for accounting purposes.

**Lab Summary**

The following are steps we took to complete this lab:

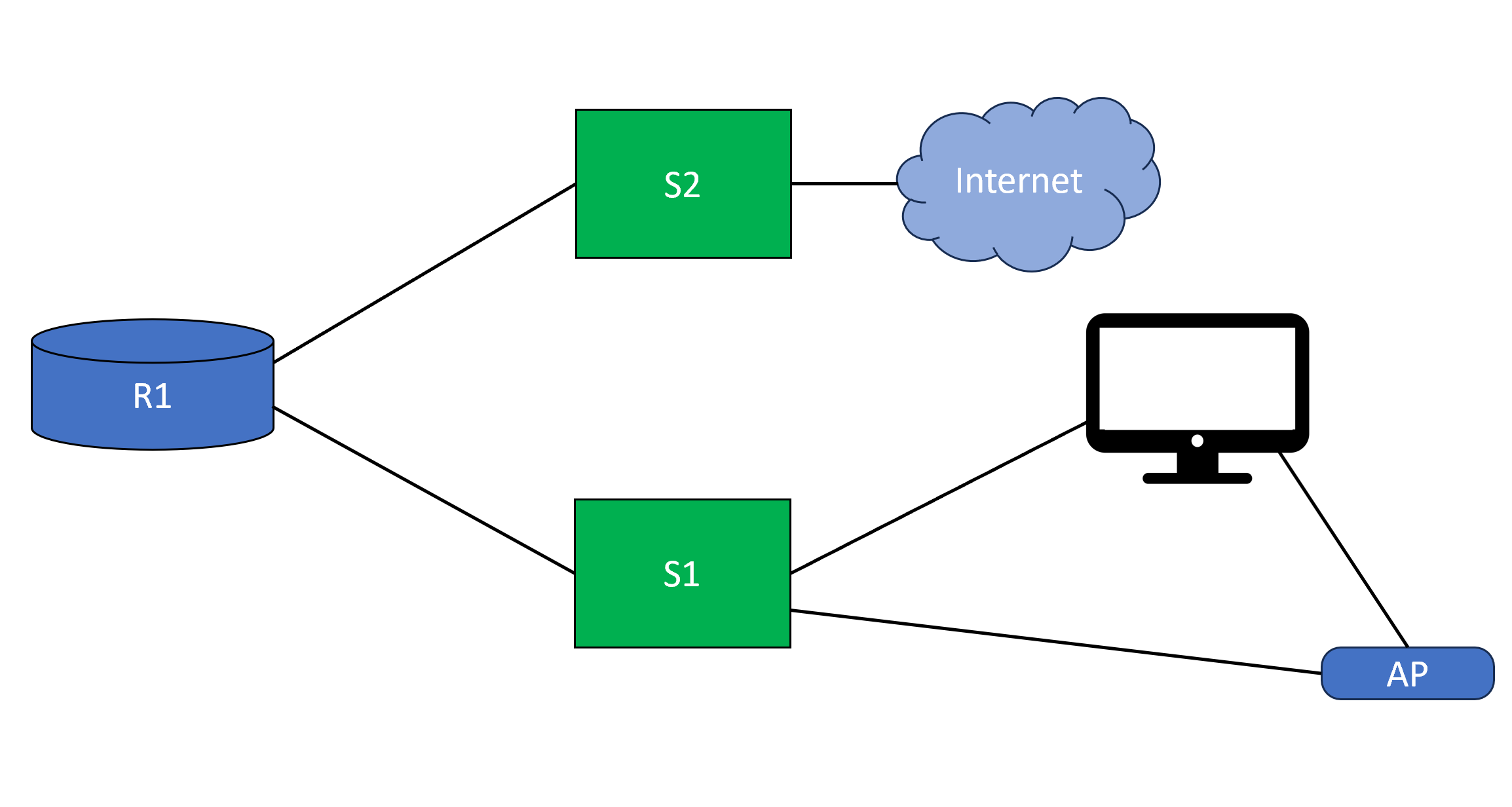
1. Using the basic instructions given out by teacher, convert the AP into a standalone AP, along with setting the update version and such to the newest so it is usable for our lab.
2. Access the Web Gui and configure the VLANs and SSIDs to use.
3. Configure the router and switch with Network Address Translation to establish a network connection with the 3 SSDs, enabling them to have an internet connection.
4. Set up an external RADIUS server to connect to the access point for the WALN-Enterprise SSID part of the lab.

**Lab Commands**

A great portion of this lab was configuring the router or switch to establish our internet connection, so no new commands were used. We did the simple configurations that we’ve known from before like setting the IP addresses to ports, configuring NAT, and configuring VLANs and trunking. This lab *did* in fact use the web GUI a lot, although there are other options, like completing the same things on the console, we decided that the web GUI was the best choice for us. To access the web GUI:

1. Wire the AP and PC to a switch and turn all of the interfaces up and running.
2. Make sure that the AP can run HTTP. Use the command **ip http server** to enable the HTTP setting.
3. Then, use a web interface like FireFox to type in [**https://[your**](https://[your) **ip-address]** to connect to the AP’s web GUI.
4. After the authentication with the default username and password, you should be granted access to the Web GUI, given the ability to configure and change the Aps settings.

**Network Diagram/Topology**



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | g0/0/0 | BGP AS | lo0 | Area | Router ID (both BGP and other respective routing protocols) |
| R1 | 10.0.0.1/24  10::1/64 | 65001 | 192.168.1.1/32  1::1/64 | N/A | 1.1.1.1 |
| R2 | 10.0.0.2/24  10::2/64 | 65002 | 192.168.2.1/32  2::2/64 | 0 | 2.2.2.2 |
| R3 | 10.0.0.3/24  10::3/64 | 65003 | 192.168.3.1/32  3::3/64 | N/A | 3.3.3.3 |

**Configurations** – show run/show ip route/show ipv6 route

**AP**

show run

Building configuration...

Current configuration : 4848 bytes

version 15.3

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

hostname ap

logging rate-limit console 9

enable secret 5 $1$fENt$/2GTfkRUVWzSNNT5SU4YM/

aaa new-model

aaa group server radius my-radius-image

server name my-radius-image

aaa group server radius rad\_eap

server name Docker

aaa group server radius rad\_mac

aaa group server radius rad\_acct

aaa group server radius rad\_admin

aaa group server tacacs+ tac\_admin

aaa group server radius rad\_pmip

aaa group server radius dummy

aaa group server radius rad\_eap3

server name Docker

aaa authentication login eap\_methods group rad\_eap

aaa authentication login mac\_methods local

aaa authentication login eap\_methods3 group rad\_eap3

aaa authorization exec default local

aaa accounting network acct\_methods start-stop group rad\_acct

aaa session-id common

no ip source-route

no ip cef

dot11 pause-time 100

dot11 syslog

dot11 vlan-name CCNP-5457-2 vlan 2

dot11 vlan-name CCNP-5457-3 vlan 3

dot11 vlan-name CCNP-5457-4 vlan 4

dot11 vlan-name VLAN1 vlan 1

dot11 ssid CCNP-12-5457-SSID-2

vlan 2

authentication open

authentication key-management wpa version 2

mbssid guest-mode

wpa-psk ascii 7 03145A1815182E5E4A

dot11 ssid CCNP-12-5457-SSID-3

vlan 3

authentication open

authentication key-management wpa version 2

guest-mode

mbssid guest-mode

wpa-psk ascii 7 051B071C325B411B1D

dot11 ssid CCNP-12-5457-SSID-4

vlan 4

authentication open eap eap\_methods3

authentication network-eap eap\_methods3

authentication key-management wpa

mbssid guest-mode

eap profile trest

method md5

no ipv6 cef

username Cisco password 7 01300F175804

bridge irb

interface Dot11Radio0

no ip address

shutdown

antenna gain 0

station-role root

bridge-group 1

bridge-group 1 subscriber-loop-control

bridge-group 1 spanning-disabled

bridge-group 1 block-unknown-source

no bridge-group 1 source-learning

no bridge-group 1 unicast-flooding

interface Dot11Radio1

no ip address

encryption vlan 2 mode ciphers aes-ccm

encryption vlan 3 mode ciphers aes-ccm

encryption vlan 4 mode ciphers aes-ccm

encryption vlan 1 mode ciphers wep128

ssid CCNP-12-5457-SSID-2

ssid CCNP-12-5457-SSID-3

ssid CCNP-12-5457-SSID-4

antenna gain 0

peakdetect

dfs band 3 block

mbssid

channel dfs

station-role root

interface Dot11Radio1.1

encapsulation dot1Q 1 native

bridge-group 1

bridge-group 1 subscriber-loop-control

bridge-group 1 spanning-disabled

bridge-group 1 block-unknown-source

no bridge-group 1 source-learning

no bridge-group 1 unicast-flooding

!

interface Dot11Radio1.2

encapsulation dot1Q 2

bridge-group 2

bridge-group 2 subscriber-loop-control

bridge-group 2 spanning-disabled

bridge-group 2 block-unknown-source

no bridge-group 2 source-learning

no bridge-group 2 unicast-flooding

interface Dot11Radio1.3

encapsulation dot1Q 3

bridge-group 3

bridge-group 3 subscriber-loop-control

bridge-group 3 spanning-disabled

bridge-group 3 block-unknown-source

no bridge-group 3 source-learning

no bridge-group 3 unicast-flooding

interface Dot11Radio1.4

encapsulation dot1Q 4

bridge-group 4

bridge-group 4 subscriber-loop-control

bridge-group 4 spanning-disabled

bridge-group 4 block-unknown-source

no bridge-group 4 source-learning

no bridge-group 4 unicast-flooding

interface GigabitEthernet0

no ip address

duplex auto

speed auto

interface GigabitEthernet0.1

encapsulation dot1Q 1 native

bridge-group 1

bridge-group 1 spanning-disabled

no bridge-group 1 source-learning

interface GigabitEthernet0.2

encapsulation dot1Q 2

bridge-group 2

bridge-group 2 spanning-disabled

no bridge-group 2 source-learning

interface GigabitEthernet0.3

encapsulation dot1Q 3

bridge-group 3

bridge-group 3 spanning-disabled

no bridge-group 3 source-learning

interface GigabitEthernet0.4

encapsulation dot1Q 4

bridge-group 4

bridge-group 4 spanning-disabled

no bridge-group 4 source-learning

interface BVI1

mac-address 44d3.ca5a.86bb

ip address 10.0.0.2 255.255.255.0

ipv6 address dhcp

ipv6 address autoconfig

ipv6 enable

ip forward-protocol nd

ip http server

no ip http secure-server

ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag

ip radius source-interface BVI1

radius-server local

no authentication eapfast

no authentication mac

nas 10.0.0.67 key 7 03105E1812062F4B1F5B4A

user CCNP nthash 7 12415D43442D5B210B0E01701517734250372751007B7C770C5D533A410C000170

radius-server attribute 32 include-in-access-req format %h

radius server Docker

address ipv4 10.0.0.4 auth-port 1812 acct-port 1813

key 7 131112011F050A2D7A767B

bridge 1 route ip

line con 0

line vty 0 4

transport input all

End

**Router 1**

show run

Current configuration : 1760 bytes

! Last configuration change at 15:38:22 UTC Wed May 8 2024

version 16.7

service timestamps debug datetime msec

service timestamps log datetime msec

platform qfp utilization monitor load 80

no platform punt-keepalive disable-kernel-core

hostname Router

boot-start-marker

boot-end-marker

vrf definition Mgmt-intf

address-family ipv4

exit-address-family

address-family ipv6

exit-address-family

no aaa new-model

subscriber templating

vtp domain cisco

vtp mode transparent

multilink bundle-name authenticated

license udi pid ISR4321/K9 sn FDO220523GF

license boot level appxk9

no license smart enable

diagnostic bootup level minimal

spanning-tree extend system-id

redundancy

mode none

interface GigabitEthernet0/0/0

ip address dhcp

ip nat outside

negotiation auto

interface GigabitEthernet0/0/1

ip address 10.0.0.1 255.255.255.0

ip nat inside

negotiation auto

interface Serial0/1/0

interface Serial0/1/1

interface GigabitEthernet0/2/0

negotiation auto

interface GigabitEthernet0/2/1

negotiation auto

interface GigabitEthernet0

vrf forwarding Mgmt-intf

no ip address

shutdown

negotiation auto

ip nat pool natpool 192.168.41.160 192.168.41.191 netmask 255.255.255.224

ip nat inside source list 10 pool natpool

ip forward-protocol nd

ip http server

ip http authentication local

ip http secure-server

ip tftp source-interface GigabitEthernet0/0/0

access-list 10 permit 10.0.0.0 0.0.0.255

control-plane

line con 0

transport input none

stopbits 1

line aux 0

stopbits 1

line vty 0 4

login

ntp server pool.ntp.org

wsma agent exec

wsma agent config

wsma agent filesys

wsma agent notify

End

**Switch 1**

show run

Current configuration : 4005 bytes

version 12.2

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

hostname Switch

boot-start-marker

boot-end-marker

no aaa new-model

system mtu routing 1500

authentication mac-move permit

ip subnet-zero

ip routing

no ip domain-lookup

ip dhcp excluded-address 10.0.0.33

ip dhcp excluded-address 10.0.0.3

ip dhcp excluded-address 10.0.0.55

ip dhcp excluded-address 10.0.0.66

ip dhcp excluded-address 10.0.0.99

ip dhcp pool vlan2

network 10.0.0.32 255.255.255.224

domain-name vlan2.com

dns-server 1.1.1.1

default-router 10.0.0.33

ip dhcp pool vlan3

network 10.0.0.64 255.255.255.224

domain-name vlan3.com

dns-server 1.1.1.1

default-router 10.0.0.65

ip dhcp pool vlan4

network 10.0.0.96 255.255.255.224

domain-name vlan4.com

dns-server 1.1.1.1

default-router 10.0.0.97

crypto pki trustpoint TP-self-signed-2701734016

enrollment selfsigned

subject-name cn=IOS-Self-Signed-Certificate-2701734016

revocation-check none

rsakeypair TP-self-signed-2701734016

crypto pki certificate chain TP-self-signed-2701734016

certificate self-signed 01

3082023F 308201A8 A0030201 02020101 300D0609 2A864886 F70D0101 04050030

31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274

69666963 6174652D 32373031 37333430 3136301E 170D3933 30333031 30303031

30355A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649

4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 37303137

33343031 3630819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281

8100D9E3 792B6F1C F24ACCD9 B9D7AE3C 8F1307DF C14A4E00 B6EA85A0 B5AED2C9

A27DBE76 1406AE8C DA64AA91 0A852C79 411C3B1F 190A211F 68E6A5BC 6AB13F71

6C0D711F 88A03BD8 9B2F25F4 184E39E6 8F6B562F A21DA2DE CA9271BC AFEE842C

C6B05647 FC9AD81F F52BDCE5 BA67B631 C60087CD 86083694 B0E73F65 4365995A

A33F0203 010001A3 67306530 0F060355 1D130101 FF040530 030101FF 30120603

551D1104 0B300982 07537769 7463682E 301F0603 551D2304 18301680 141013FD

DCD0C791 6BD931D2 9D8D8266 3E6EB9FB 94301D06 03551D0E 04160414 1013FDDC

D0C7916B D931D29D 8D82663E 6EB9FB94 300D0609 2A864886 F70D0101 04050003

8181003F A15E1CF5 4A03002F 214ACD03 44A57B1C 6D553315 FB6CBD4C 6F48237E

AF43B5C9 2845BB13 113304D1 8EAA4CA5 F1DB9D09 84AF3437 7A16DB10 B7B50F51

1C7A0294 3932A56C 2D70DF0C B223C68D 71C192B9 A4A4723B 64834A0D 4B6D265A

3CC0F60E AAB0A090 1C1A2FA8 C34D65EE D78C3209 1CE61A7F 0662CCB0 AA5C67C1 9EAE3D

quit

spanning-tree mode pvst

spanning-tree etherchannel guard misconfig

spanning-tree extend system-id

vlan internal allocation policy ascending

interface FastEthernet0/1

interface FastEthernet0/2

interface FastEthernet0/3

interface FastEthernet0/4

interface FastEthernet0/5

interface FastEthernet0/6

switchport trunk encapsulation dot1q

switchport mode trunk

interface FastEthernet0/7

interface FastEthernet0/8

interface FastEthernet0/9

interface FastEthernet0/10

interface FastEthernet0/11

interface FastEthernet0/12

interface FastEthernet0/13

interface FastEthernet0/14

switchport trunk encapsulation dot1q

switchport mode trunk

interface FastEthernet0/15

interface FastEthernet0/16

interface FastEthernet0/17

interface FastEthernet0/18

interface FastEthernet0/19

interface FastEthernet0/20

interface FastEthernet0/21

interface FastEthernet0/22

interface FastEthernet0/23

interface FastEthernet0/24

interface GigabitEthernet0/1

interface GigabitEthernet0/2

interface Vlan1

ip address 10.0.0.2 255.255.255.224

interface Vlan2

ip address 10.0.0.33 255.255.255.224

interface Vlan3

ip address 10.0.0.65 255.255.255.224

interface Vlan4

ip address 10.0.0.97 255.255.255.224

ip default-gateway 10.0.0.1

ip classless

ip route 0.0.0.0 0.0.0.0 10.0.0.1

ip http server

ip http secure-server

ip sla enable reaction-alerts

line con 0

line vty 0 4

login

line vty 5 15

login

End

Config t

Vlan 2

Name ssid2

Vlan 3

Name ssid3

Vlan 4

Name ssid4

End

**FreeRADIUS configuration commands**

- sudo apt update

- sudo apt install freeradius freeradius-utils

- sudo nano /etc/freeradius/3.0/clients.conf

- clients emmAP {

ipaddr = 10.0.0.2

secret = testing123

- sudo nano /etc/freeradius/3.0/users

- bob Cleartext-Password := “testing”

- sudo freeradius -X

**Problems**

We had multiple issues throughout this lab, and here is the list:

* We had a problem with the physical layer of our configuration. The wires were not working correctly because we plugged cross over cables to our computer and not our switch. We also made a mistake in connecting it to the wrong type of switch – we were supposed to use the PoE switch but we plugged it into a normal switch. WE simply fixed this one by wiring the devices correctly.
* When we were trying to boot the AP, there were numerous configurations already on the AP that we had to delete one by one manually, this was a time consuming process but a simple fix.
* Even though our VLANs were up and showing up in the network options from our computer, our login info was not going through, we fixed this by entering the commands **debug all** & **debug aaa authentication**
* When trying to ping for clarification, we had a Native VLAN mismatch – we found out that our native VLAN has to be VLAN1, so we configured as so.
* Another problem we had while pinging was the naming on the VLANS. We forgot to name the interfaces, and the pinging did not work because of this. We simply put names on the VLANs in hopes that it will help, but this was a lesson learned because the VLAN names do not come up on the **show run** command.

**Conclusion**

In this lab, we were successfully able to configure a basic WLAN network with WPA2-PSK SSIDs and one WPA-Enterprise SSID. We were also about to convert eh access point to be standalone, use the web GUI to set up SSIDs, use a router and switched to connect the SSIDs to the internet, and create pre-shared keys and connect and external RADIUS server to all of those connections. Through this lab, I learned that many of the issues that we’re having could be the very basic things that we usually might not see as complicated.