Brit Stevens 4/17/24

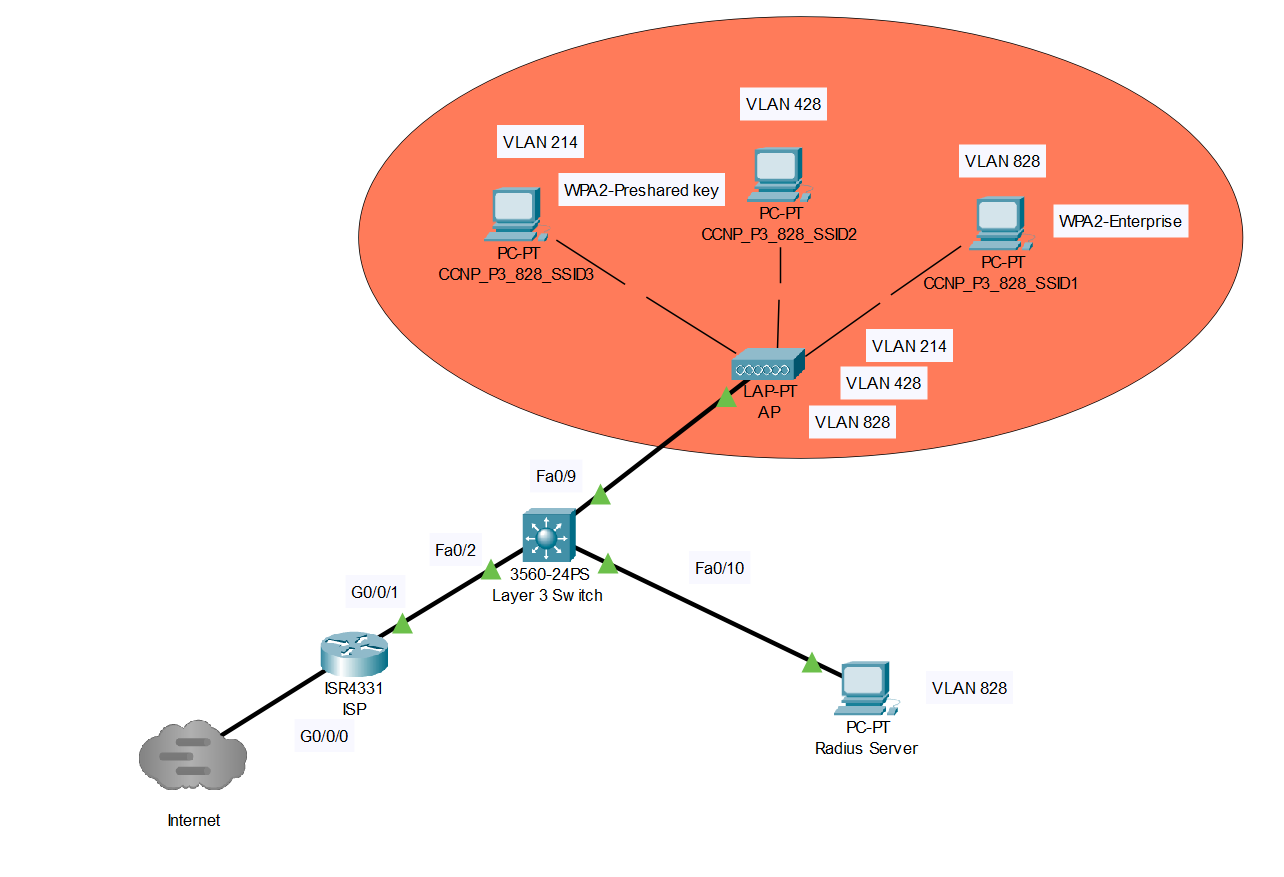
Cisco Wireless Access Point Configuration

**Purpose:**

The purpose of this lab was to expand our knowledge of Wireless Access Points which we never had extensive hands-on experience with in CCNA. We needed to learn the difference between WPA2 Enterprise and WPA2 Pre-shared key with how their authentications and configurations were different. We also needed to learn the specifics of a Cisco Access Point.

**Background Information on lab concepts:**

* **TFTP Server**
  + **TFTP** stands for **Trivial File Transfer Protocol**. This protocol lets a user on a network put or retrieve a file onto a server. It is designed to be simple and easy to use to get a network up and running while transferring small files throughout it. A more complex protocol is **FTP** which has guaranteed delivery of files due to using **TCP** instead of **UCP** as TFTP does. FTP is recommended for networks and is more commonly used as the standard, but TFTP is useful due to its use of less bandwidth.
* **UDP**
  + **User datagram Protocol** is less reliable than TCP but is faster. It is used for things like streaming or online games because it is not necessary to receive every piece of data but needs to be transmitted quickly. It establishes no connection from user to server or user to user and sends the data directly to the target all at once. It also sends an order for which data goes first in case arrive out of order.
* **TCP**
  + **Transmission Control Protocol** is a more reliable data transmission protocol as it guarantees data arrives in full packets. This is necessary for things like text, email, or websites where you would need the full webpage or message. This protocol works by establishing a link between server and client before sending any data then splitting that data into small pieces to send. If some data is seen missing, the server sends just that small piece of data again.
* **Access point** 
  + **Modes**
    - **Fat vs Lightweight**
      * When an AP is fat, sometimes referred to as **Standalone**, that means it is configurable and has every feature. It can act independently 1as its own AP and can function without any other device. When an AP is lightweight that means it needs a **WLC (Wireless LAN controller)** to configure it with other lightweight Access in the LAN.
      * **WLC** is a device used to configure many Wireless APs at once when a topology grows and spans many different APs. It makes all these APs connect and expands the wireless network while easing the management process of these numerous APs. It also increases the security and integrity of a network because it does not allow configuration errors on the APs due to the streamlined configurations given by the WLC.
    - **Local Mode**
      * The default mode of the AP that links all user traffic to the WLC and the APs radios are only function when connected to a controller.
    - **FlexConnect Mode**
      * This mode sends traffic from clients either to the controller or towards the AP’s LAN port if configured in the Wireless LAN.
    - **Bridge Mode**
      * This mode is used for mesh deployment for a wireless backhaul where data is transmitted between the Internet and the LAN wirelessly. This mesh is a combination between the wired and wireless infrastructures and guides all the data through the bridge.
    - **Monitor Mode**
      * In this mode the radios on the AP are used to monitor traffic on the Wi-Fi-channels it is configured for.
  + **WPA 2-3**
    - **Wi-Fi Protected Access** protocols provide security for wireless networks and are the standard used on most networks. It utilizes integrity checks on messages to make sure they were not altered maliciously and uses encryption like security keys created by the User when joining a network to ensure it cannot be copied to bypass the pre-shared key security. WPA3 is a newer version of WPA2 and has improved security features.
    - **WPA2 PSK** is where you log in to a network using a defined pre-shared key for that SSID.
    - **WPA2 Enterprise** is where you use a defined Username and Password to login into a network through an SSID. This can be done with a radius server.
  + **frequency bands**
    - Access point utilize three different bands of frequency – 2.4Ghz, 5GHz, and 6GHz.
    - **2.4Ghz** has the biggest range out of the three bands but cannot transmit data as fast and has less available channels.
      * When you set your AP’s radios in a certain frequency you can either set a channel or choose automatically to select open channels. For 2.4Ghz the channel width is 20MHz or 40MHz making there very few options for channel selection. Because of this, the channels can become crowded if many others use 2.4GHz when users simultaneously transmit data, slowing down everyone’s bandwidth.
    - **5Ghz** band is much faster than 2.4Ghz but has less range and does not go through things like walls as easily. It has a good range of frequency channels of 20MHz, 40MHz, 80MHz, and 160MHz, ensuring it does not congest as easily.
    - **6GHz** band is relatively new and is not as widely used but has the fastest sleep and lowest range. Because of this, it has 59 frequency channel widths of 20Mhz overlapping with all other frequency channels. You should be directly next to this kind of frequency so there will be less interference.
  + **Vlans**
    - **Virtual Local Area Networks** allow networks to be segmented, for example, between branches of a company that are unconnected. If you have a Food safety department and a finance department in your company, there would be no need for communication between them. Splitting them up with different VLANs improves security and network management as unless configured otherwise, only devices with the same VLAN tags, the same number, can communicate and send data to each other.
* **Layer 3 switch**
  + This kind of switch has the same layer 2 capabilities of a standard switch but also has the capabilities of routing if enable on interfaces. It is also used to manage VLAN traffic without the need for an external router.
* **AAA**
  + **Authentication, Authorization,** and **Accounting** is the framework that many companies follow as it greatly increases data integrity and a company’s security. It is the idea of needing each user to prove that they are who they say they are through different means like thumbprint, driver’s license, or Two Factor Authentication. After they are confirmed to be who they say they are they are then they are only given access to materials or data in our case that their role allows (Authorization). Once they are given access to their respective materials they are watched and any changes they make are accounted for. This way security is greatly increased. Radius is one example of AAA security.
* **Radius**
  + **Remote Authentication Dial-In User Service** is a protocol that provides the AAA services previously mentioned for users who connect using this service. With a radius server you must have a username configured and assign a password to that username. You can have many different usernames and passwords for individual users called the **Local user database.** You establish the link
  + Port 1812 and 1813 are the ports radius servers commonly use for Authentication and Accounting.
  + The **pre-shared key** for radius is different than that of a SSID pre-shared key. Instead being used to allow a user to access the internet, this pre-shared key connects the AP to the radius server itself when you want to use the radius server for your enterprise network. You configure it both on the AP and the radius server.
* **Cipher**
  + **AES CCMP** is a encryption protocol used in Wi-Fi enabled networks to ensure data security with the use of encryption. It used AES block ciphers to encrypt which encrypts the data into a ciphertext then scrambles chunks of that ciphertext between each other many times. To decrypt it uses a key and reverses every scramble that occurred.
  + **EAP** Authentication framework
* **Virtual Machines**
  + A virtual machine is a operating system like Windows 10 or Linux that can be downloaded and run a physical device in order to have multiple operating systems on the same device. This allows the virtualization of your topology as you can have multiple users all run off the same device or server.
  + **Linux operating system** is one of the operating systems we used in this lab to run our Radius server. This operating system is open source meaning that it is very customizable and free to use or edit how you please.



**Required Resources:**

* *Cisco AIR-LAP1042N-A-K9.*
* *PoE switch (Catalyst 3560 series PoE-24).*
* *Access to the Internet through a switch.*
* *Desktop with an Ethernet NIC.*
* *Virtual Machine or Physical Machine for dedicated Radius Server.*
* *Router NAT to the Internet (Cisco 4321).*

**Lab Summary:**

We started by configuring what we were used to with routers and the switch. We changed our topology many times but finalized the one above for this lab. We wanted our Router’s use to be minimal and learn how to use a layer 3 switch for routing capabilities. We decided on using the router for connection to the internet and giving NAT translations to the inside network. We also set up a OSPF connection between it and the layer 3 port on the Layer 3 Switch. On that switch we configured VLANs ,VLAN interfaces, and DHCP pools for the respective VLANs and SSIDs they are associated with. The new commands we used are the following:

**Router Commands:**

* Access Lists (Global Configuration Mode)
  + Access-list ‘x’ ‘permit’/’deny’ ‘x.x.x.x’/’any’/host’ (These commands let you configure an access list which denies or permits traffic from certain parameters. X.x.x.x is a subnet of addresses, any is all addresses, and host lets you configure a single host to deny or permit from.
* NAT (Global Configuration Mode)
  + Interface ‘x’
    - IP nat ‘inside’/’outside’ (These commands tell the router if the NAT traffic is coming from the inside network or the outside network. You use Ip nat outside on the port facing the Internet and inside on the network facing the inside network)
  + IP nat pool ‘x’ ‘x.x.x.x x.x.x.x’ netmask ‘x.x.x.x’ (The first x is for what you name your nat pool, the second Xs describe your range of Ips, from lowest Ip to highest to translate, and the final Xs describe the netmask of the range of Ips given)

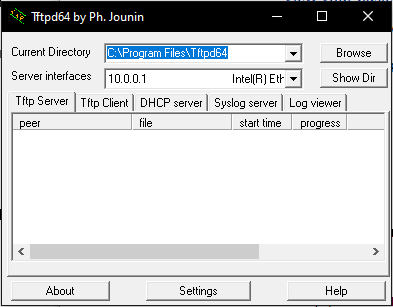
**Layer 3 Switch Commands:**

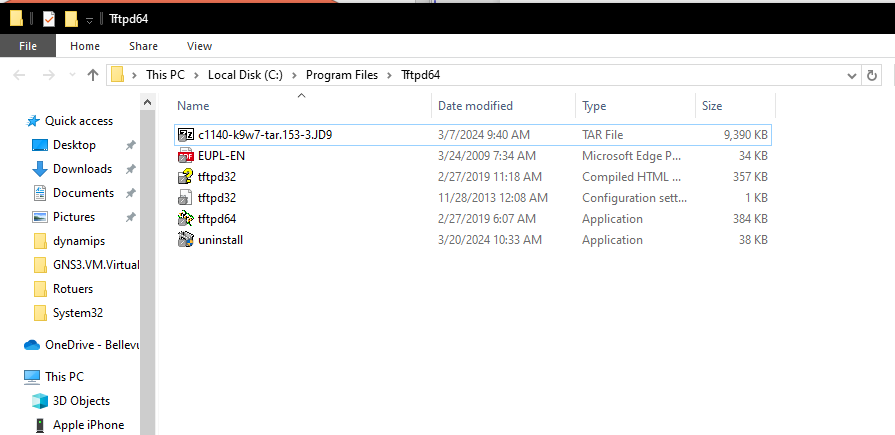
* Layer 3 routing (Global Configuration Mode)
  + Ip routing (Enables routing capabilities on the switch)
  + Interface ‘x’
    - No switchport (Enables layer 3 routing on a port)
* DHCP Server (Global Configuration Mode)
  + ip dhcp excluded-address ‘x.x.x.x’ (Tells the switch to exclude certain addresses that may be in the range of the DHCP pool)
  + ip dhcp pool ‘x’ (Allows configuration of a DHCP pool and gives the pool a name)
    - network ‘x.x.x.x’ ‘x.x.x.x’ (Lists the addresses the DHCP server can give out using a network address and its subnet mask)
    - default router ‘x.x.x.x’ (Tells any end devices that receive a DHCP address what their default router is using its Ip)
    - dns-server ‘x.x.x.x’ (Tells any connected end devices what their DNS server address is)
* VLANs (Global Configuration Mode)
  + Vlan ‘x’ (Creates a Vlan with a certain number)
    - Name ‘x’ (Gives that Vlan a name)
  + Interface Vlan ‘x’ (Configure like a normal interface).
  + Trunk configuration
    - Interface ‘x’ (The interface connected to Access point or any port that will handle traffic from multiple Vlans)
      * Switchport trunk encapsulation dot1q (tells the switch to use this encapsulation on the packets from that port to have their Vlan tagged onto it)
      * Switchport mode trunk (Puts the port into trunking mode allowing all Vlans by default, can be restricted with commands)

**Access Point Setup:**

First, you must change the IP on your pc to 10.0.0.1 and set it up as an TFTP server. To do so you can download TFTPD64 and enable your PC as a TFTP server.

Next, put OS file you want for your AP in TFTP server directory.





Once copying the file into the directory hold down the reset button on the back of your AP for 8 seconds. Ensure you are consoled into the AP because as soon as you start seeing ###### hit ‘escape’.

After when you are able to type, enter the command ‘**dir flash:**’ to view any config.txt files on the AP from previous configurations. Delete any ‘config.txt’ ‘private-multiple-fs’ and ‘capwap-saved-configs’ using the command ‘**delete flash:X’** replace X with your file. Our AP had no configurations so we went to the next step.

Type ‘**reset**’ to reload your AP with no configurations. Log in with the default password ‘Cisco’ and paste the list of commands

“debug capwap console cli

debug capwap client no-reload

lwapp ap ip address 10.0.0.2 255.255.255.0

lwapp ap ip default-gateway 10.0.0.1

config t

no ip domain-lookup

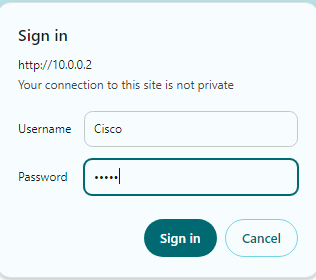
exit

archive download-sw /overwrite /reload tftp://10.0.0.1/c1140-k9w7-tar.153-3.JD9.tar

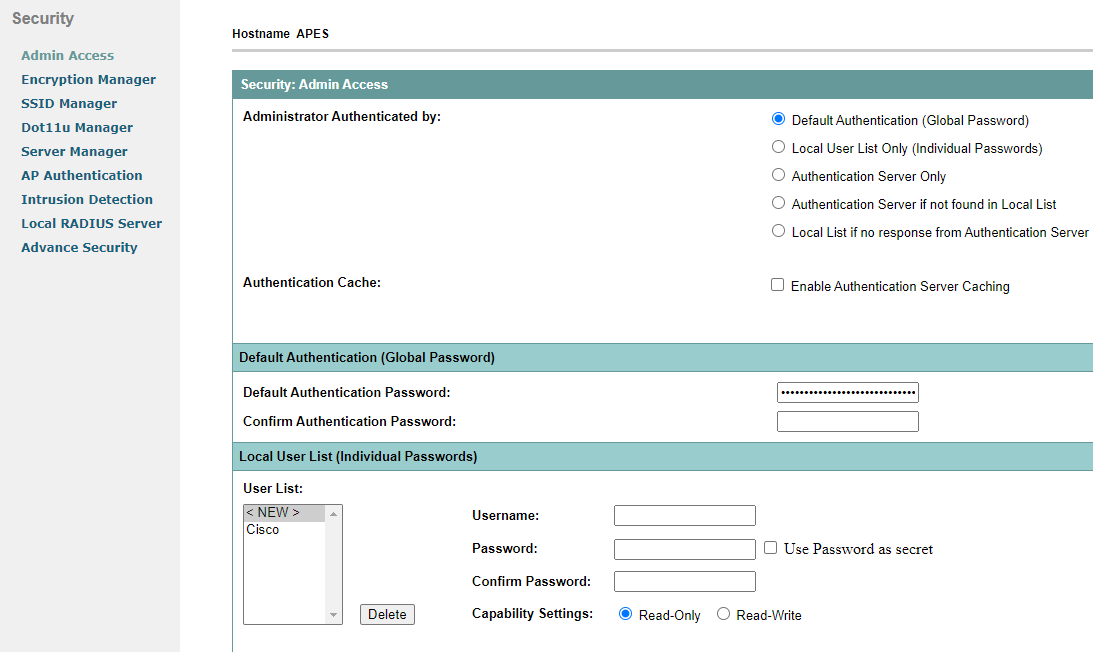
delete /force /recursive flash:c1140-k9w8-mx.153-3.JA4

delete /force /recursive flash:c1140-k9w8-mx.v153\_80mr\_esde“

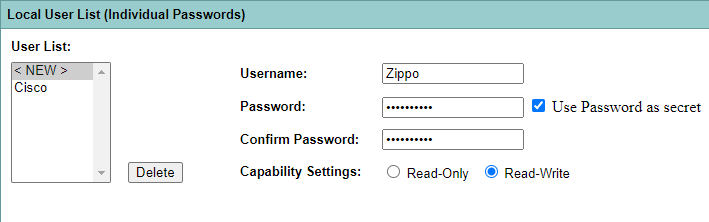
Wait until files were transferred from the TFTP server and reboot your AP to confirm the changes were made.



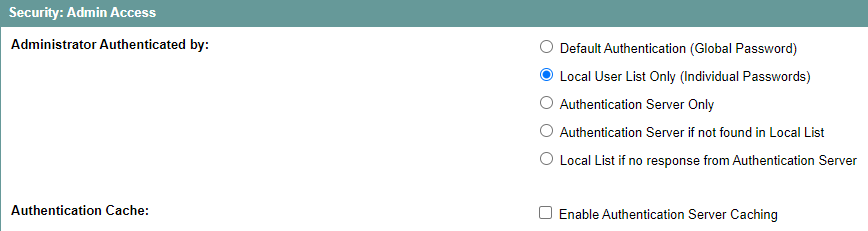
Once the AP shows a green light attempt to sign in with the default login of Cisco, Cisco.



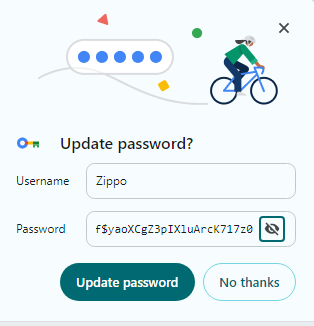
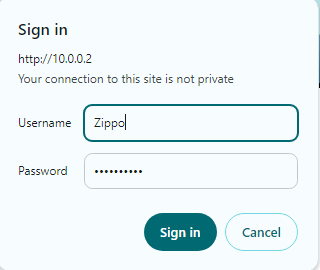
Once in AP change the Username and Password for security integrity as the default login is readily available. To do this navigate to **Security** on the top navigation bar then to **Admin Access**.



Enter your preferred Username and Password then set to **Read-Write** so you still have admin privileges. Select **use password as secret** for greater security. Click **apply** to create user which will reload the webpage. Restart PC and AP to be successful.



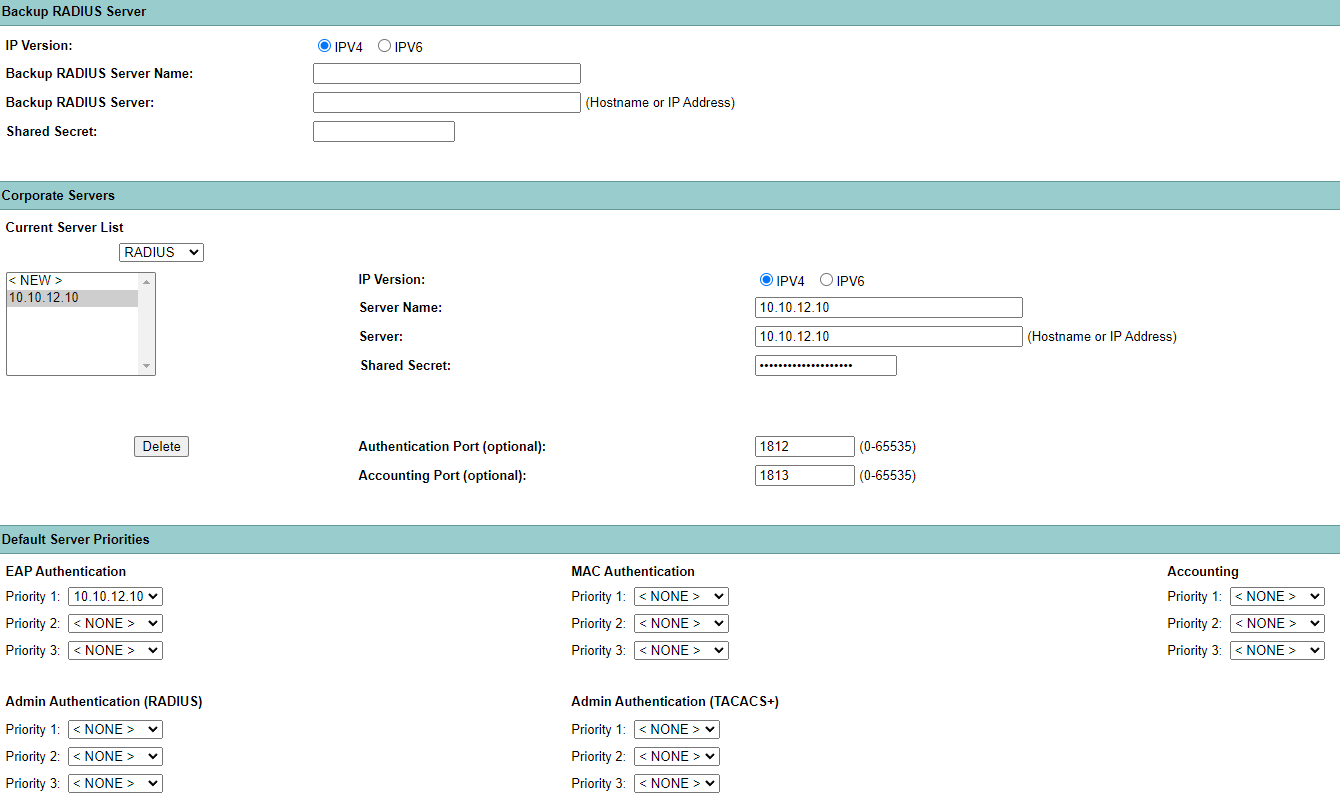
Once reloaded go back to the same settings page and set **Administrator Authenticated by** to **Local User List Only**. This will give you a prompt to delete the default username and password to which you say OK.

****

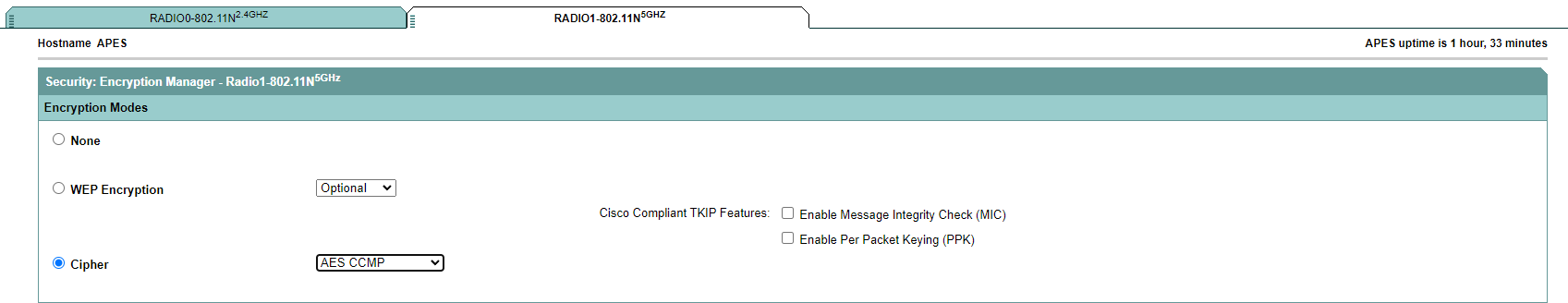
You should now be able to sign in with your new login and it is automatically encrypted because of the settings we used.



Go to **Security** and navigate to **Server Manager.**

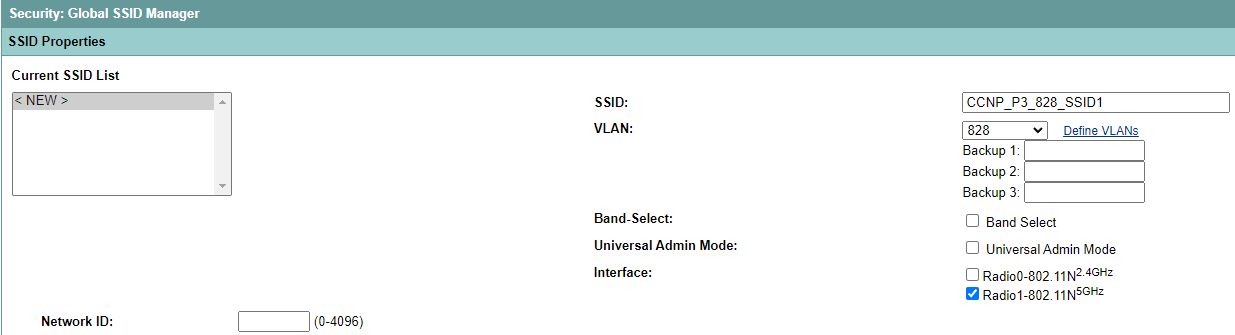


Once in **Server Manager** select IPV4 and enter the name you want for your Radius Sever, The IP you will set on the Radius, and the pre-shared key you will configure between the AP and the Radius server. Use port 1812 and 1813 in the corresponding sections for Authentication and Accounting. Click apply and you will see the new radius server pop up in the server list when the page refreshes.

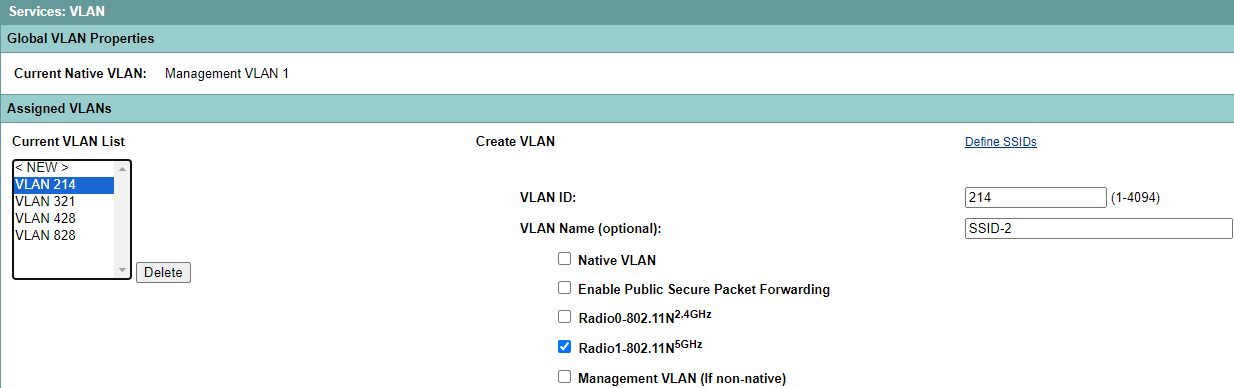


Navigate to **Security -> Encryption Manager** and select **Radio1-802.11N5GHz** as it is the broadcast frequency we are using. Select **Cipher** and choose **AES CCMP** for encryption. Click apply.

To create an SSID for your AP, navigate to **Security -> SSID Manager**.

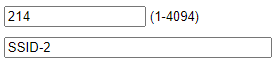
****

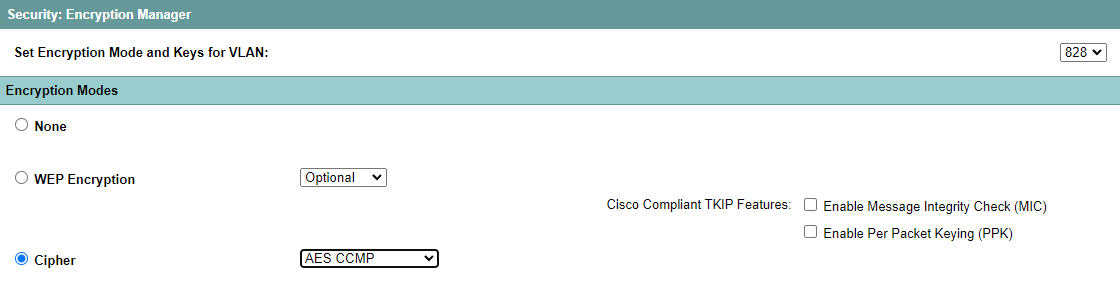
Before setting up our SSIDs we should configure the three VLANs that will be associated with the SSIDs. Click **Define VLANs** on the right-hand side to do so.



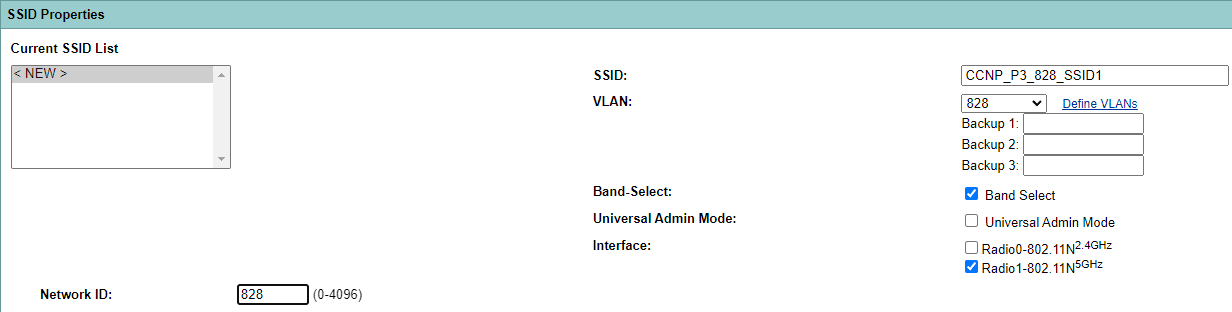


Choose any number besides 1 for the VLAN ID and give it a VLAN Name that is rememberable by you and will correspond with the SSID it is assigned to. Enable Radio1-802.11N5GHz since that is the frequency of the SSID they will be applied to. Repeat for the other 2 VLANs you make for WPA2 PSK.

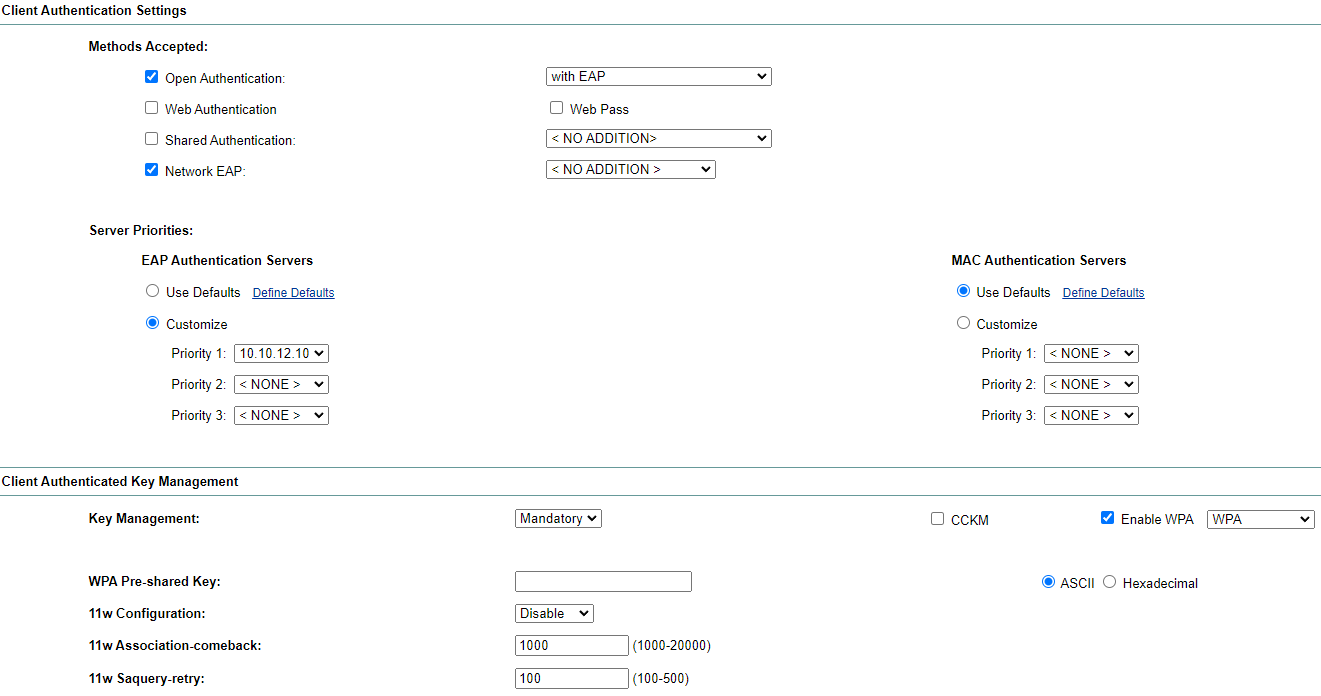
 

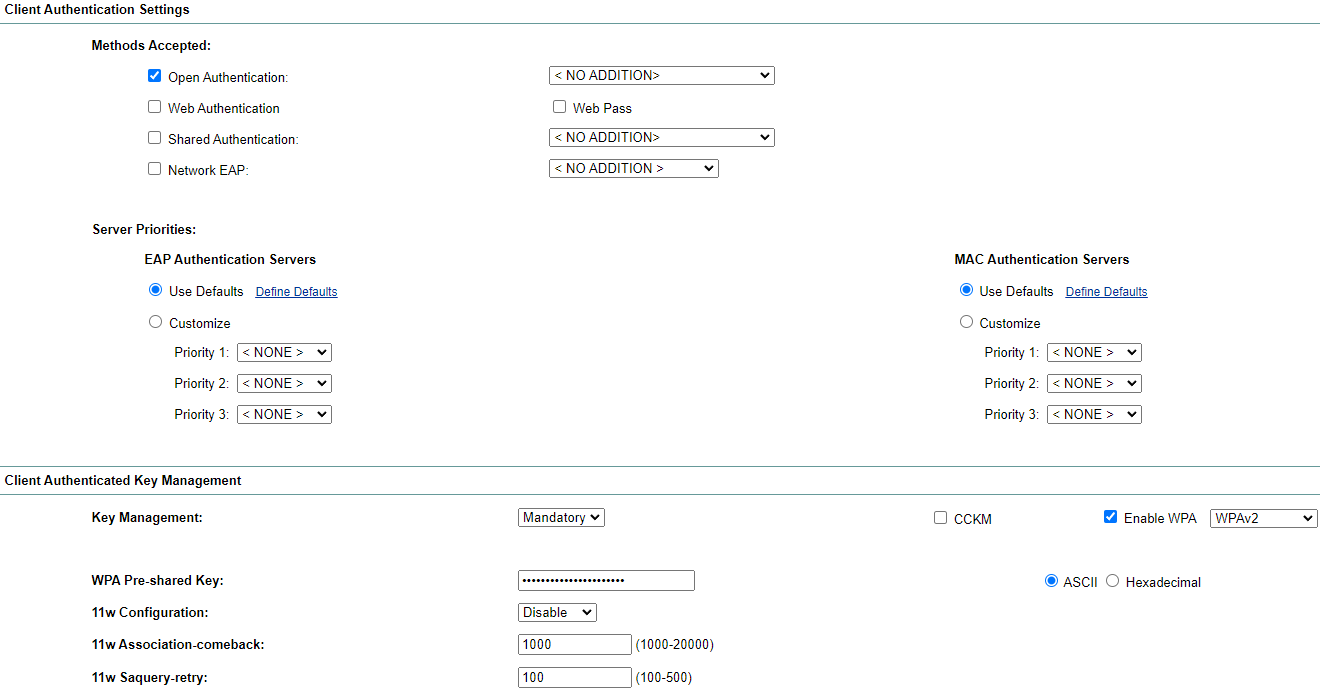
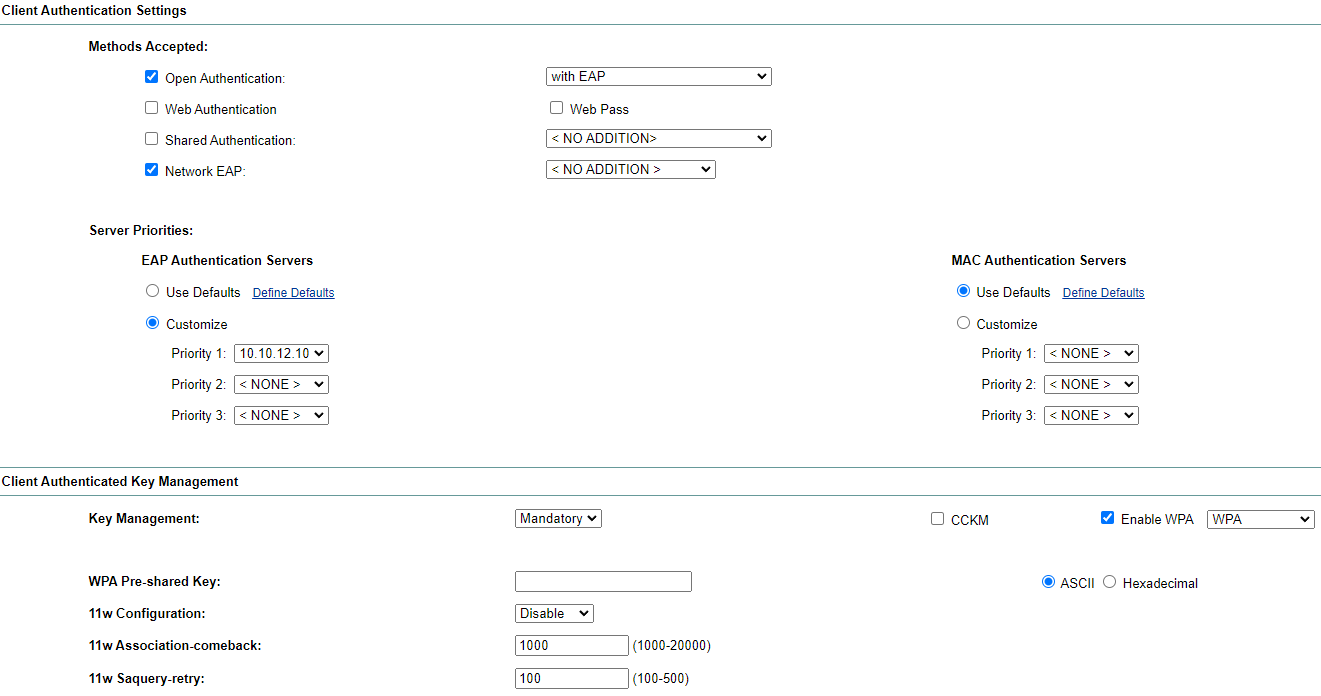
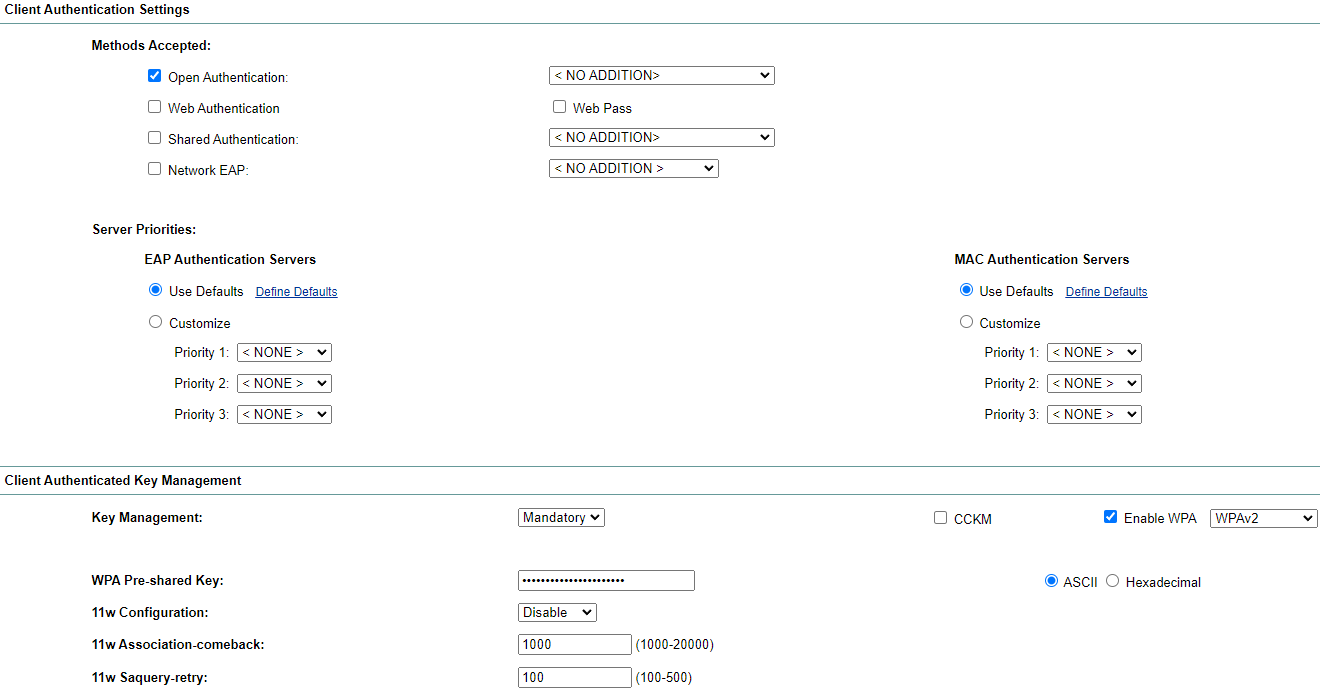


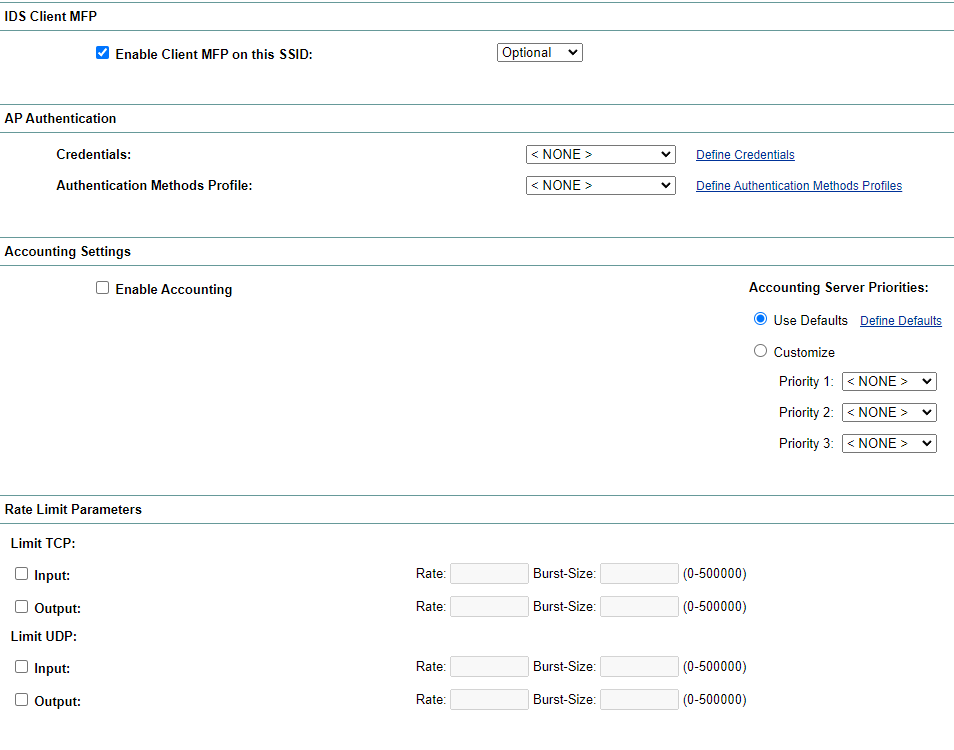
Go to **Encryption Manager** and select **Cipher ->AES CCMP**. Do this for the VLAN you select to be in WPA2 enterprise mode.

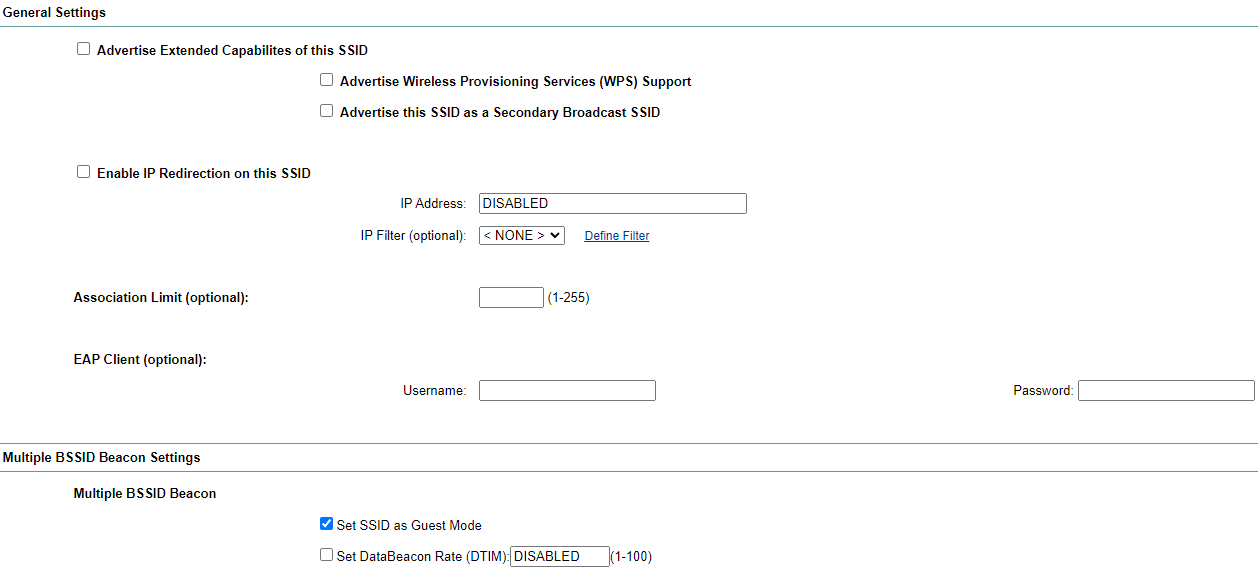


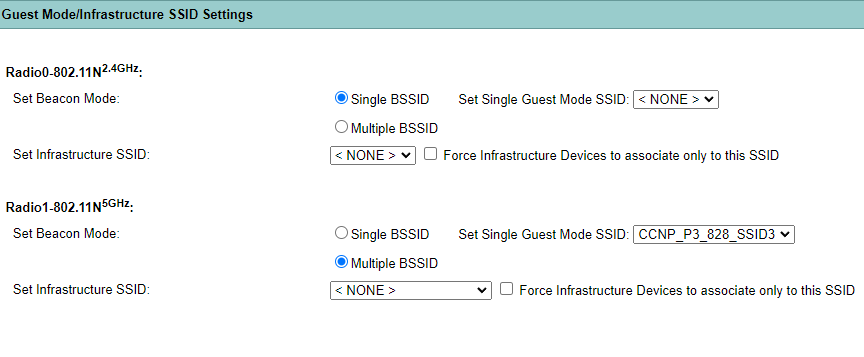
Now we can configure the SSIDs. Enter the name of your SSID and assign a VLAN to it. Enable **Band-Select** to allow the radio to automatically determine what frequency is free to broadcast the SSID to. Enable interface Radio1. Leave Network ID as blank.



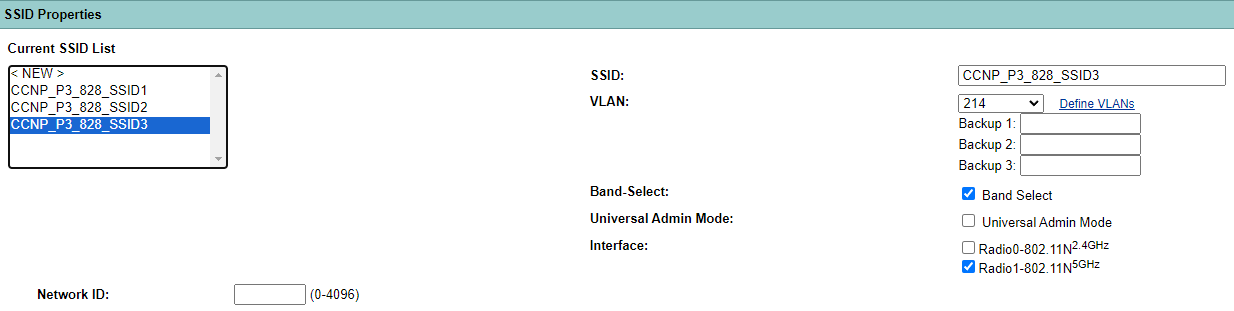


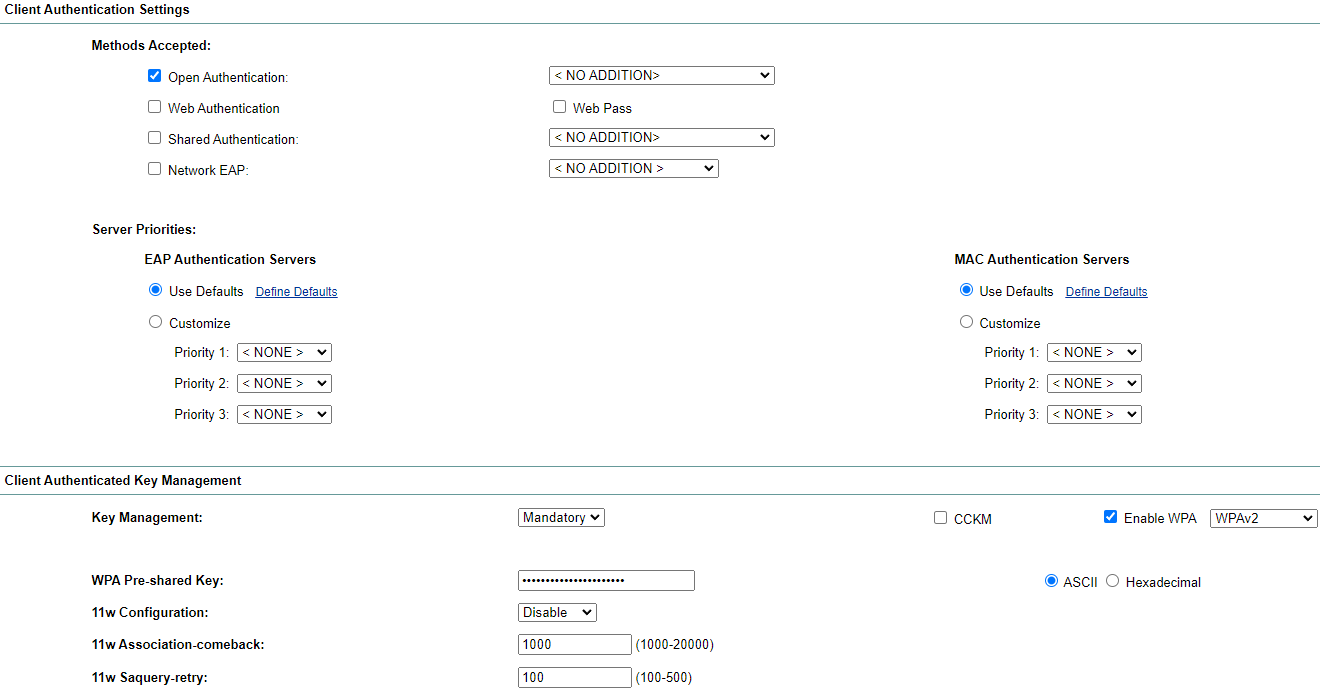


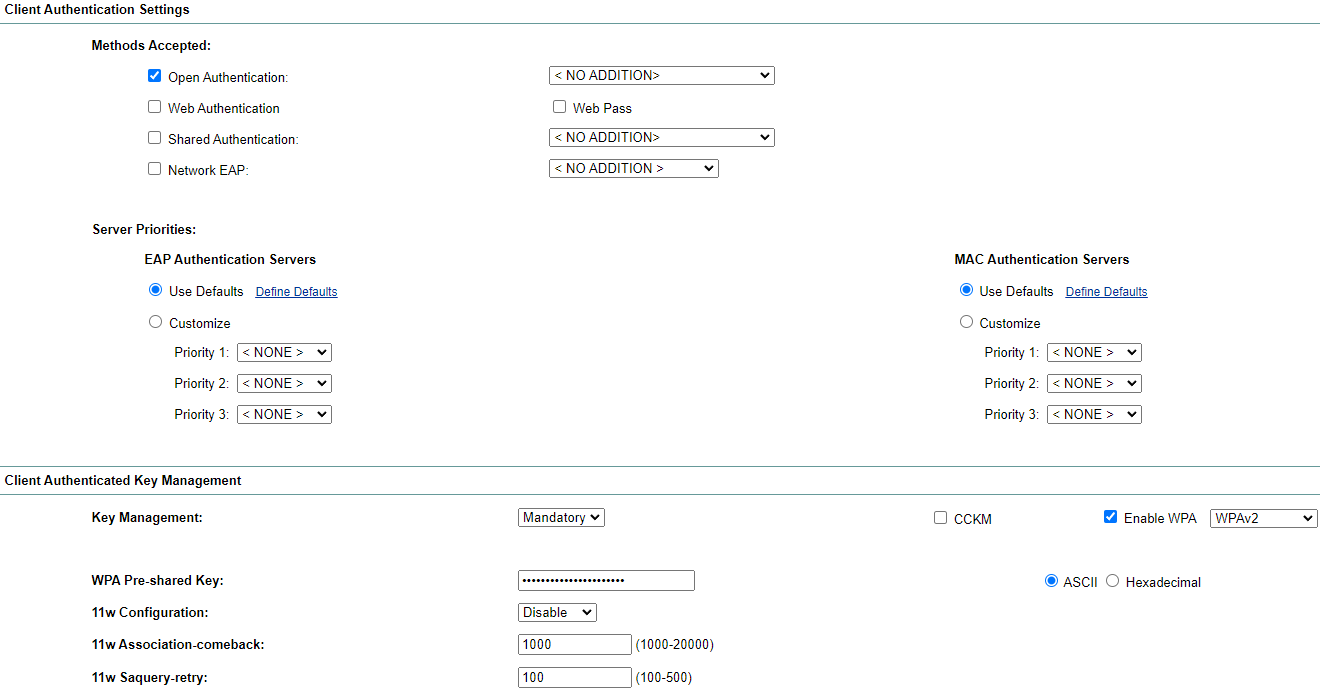
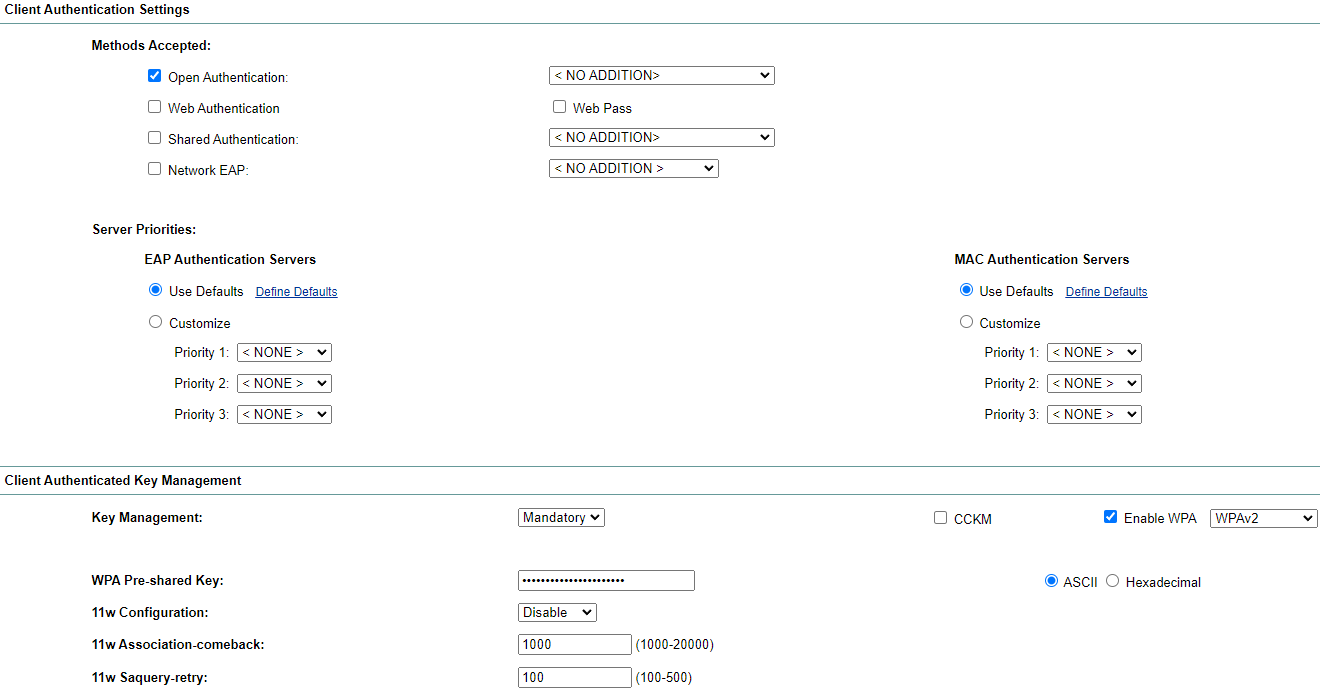
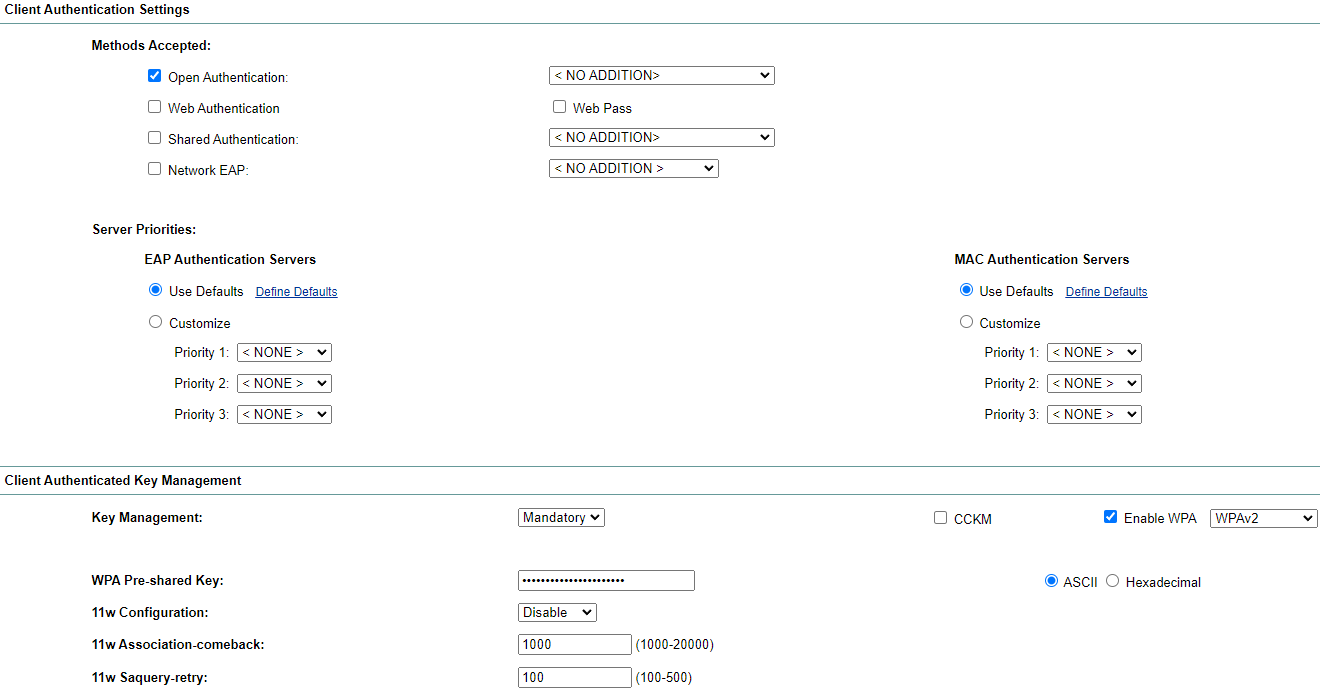


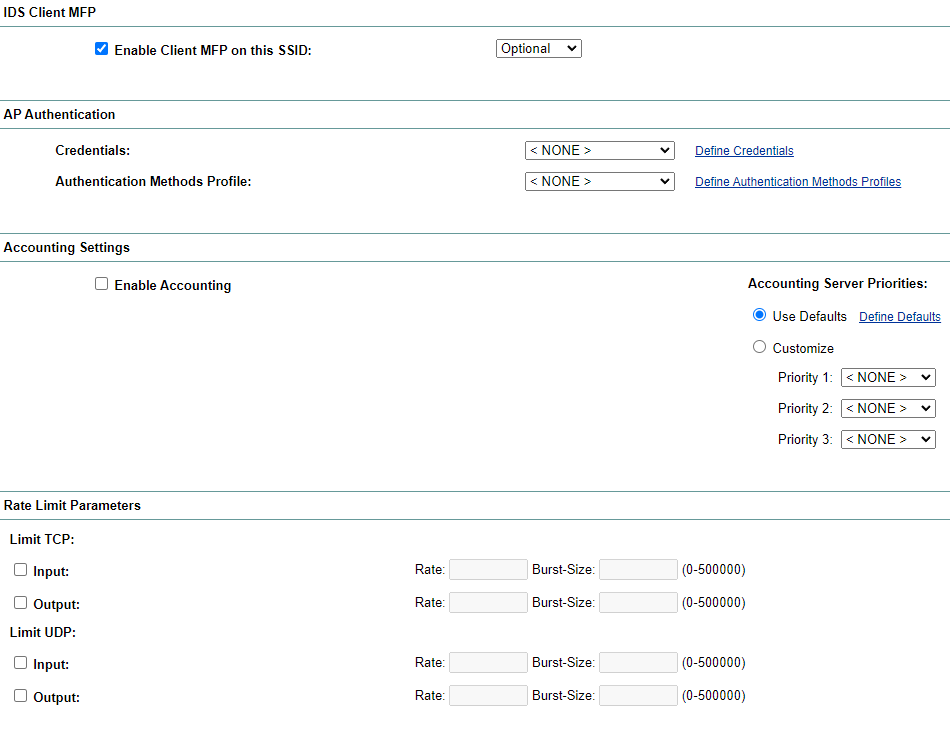


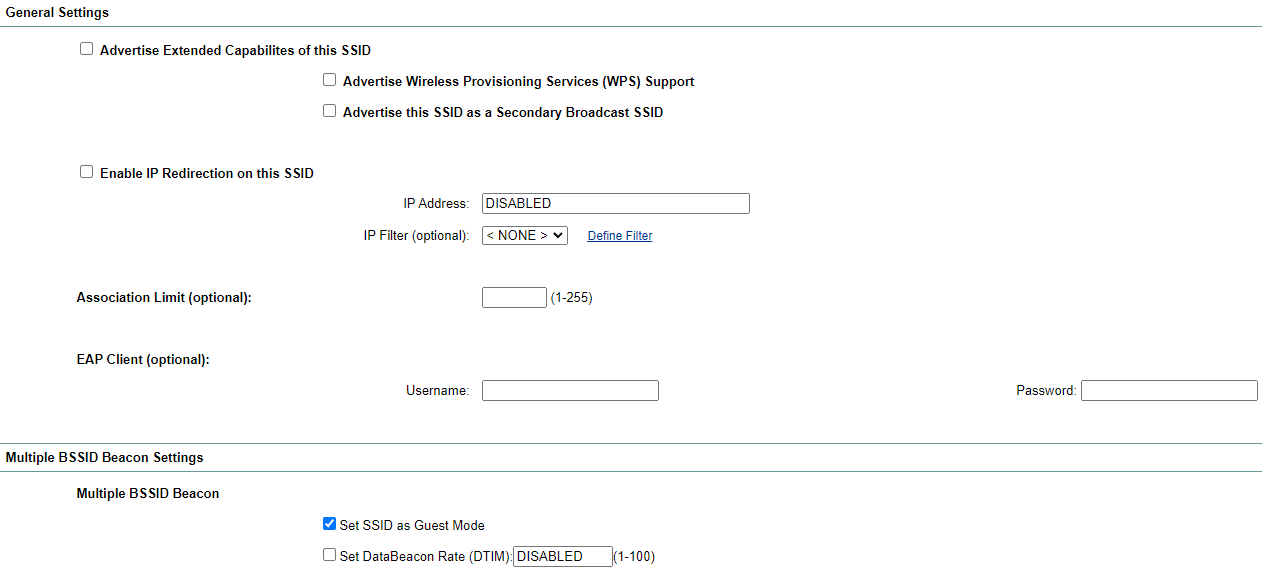
For the Enterprise SSID, scroll down to the next options box, and check the **Open Authentication** and **Network EAP** authentication method. Select **With EAP** for open authentication. Scroll down to Authentication Key Manager and set to **mandatory**, enable **WPA,** and select **WPA2**. If you select WPAv2 dot11r it will not be a true enterprise mode. Set SSID as **Guest Mode** and **Beacon Mode** to **Multiple BSSID** to allow all SSIDs to broadcast from the AP and be seen by end devices.

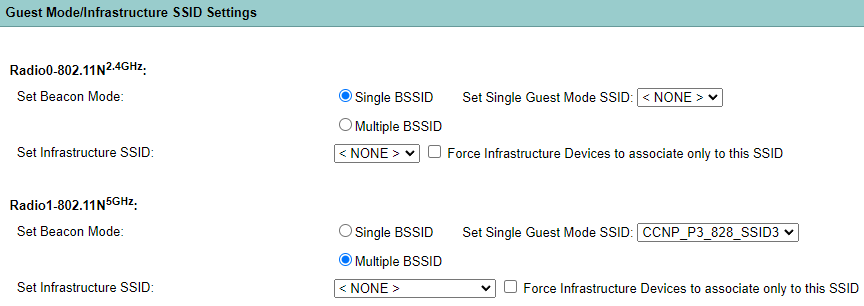












The configurations for WPA PSK SSIDs are mostly the same with a few differences. Only select **Open Authentication** with **no additions**. Set the pre-shared key to a password you want which will be used to log into the SSID.



Go to **Network -> Radio1-802.11N 5GHz** and enable Radio1, set to access point mode, disable Max clients, and disable 11r Config. Your SSIDs should now be up and have internet connection.

**Radius:**

****

To install radius you must decide which OS to use and what software for your Radius Server. After you have your preferred OS and your Radius Server file go to the CLI. For our lab we used a Linux based OS and FreeRadius.



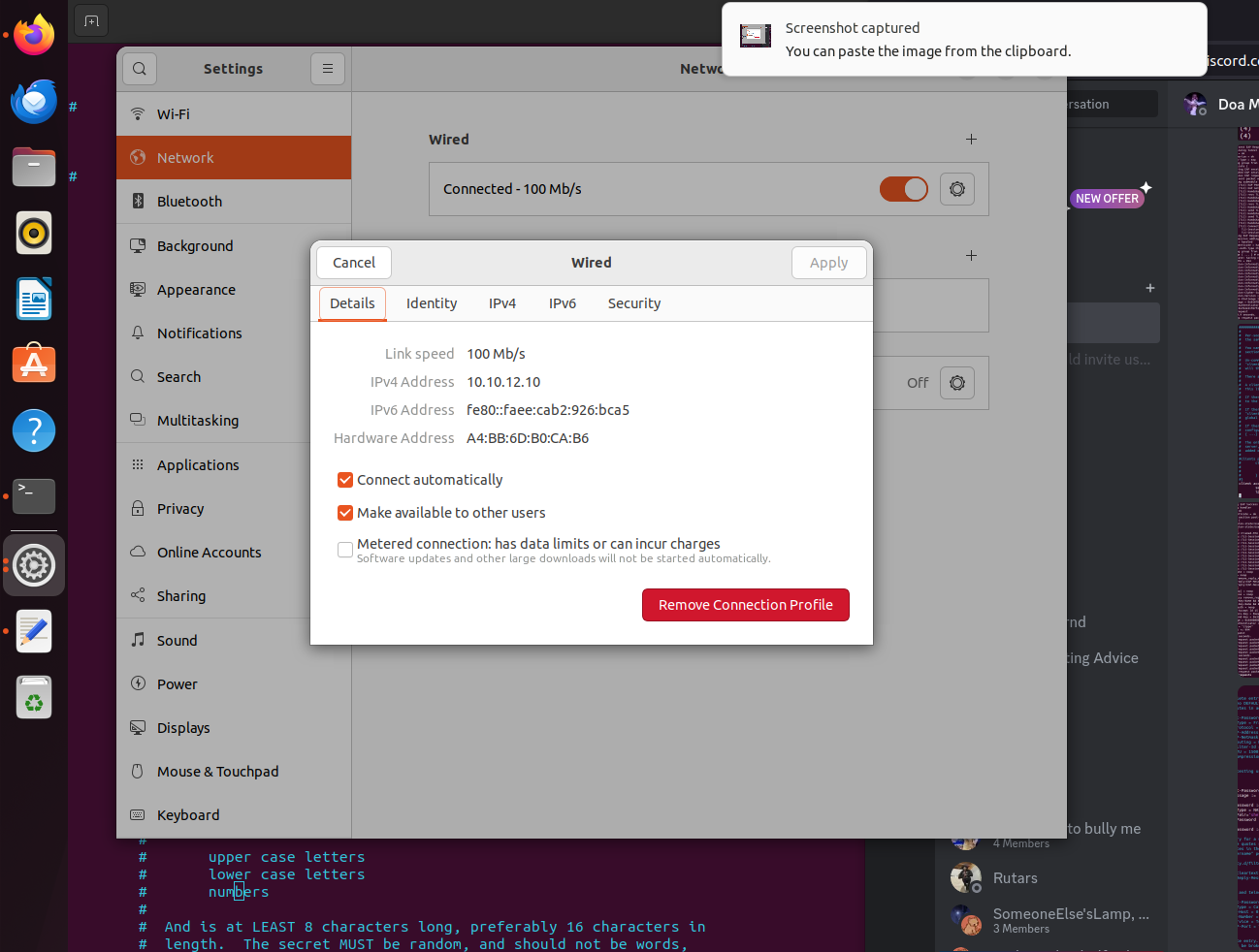
Type ‘**Sudo su’** to enter priveledged mode and install freeradius using **‘apt-get install freeradius’** or replace freeradius with the application name of your radius server.



Once it is installed type **‘sudo vim /etc/freeradius/3.0/users’** to edit the username and password for the login credentials of the Radius Server. You will see the list above which gives you the format of how you will type your new username and password into this file. Type **‘I’** to enable editing and use the arrow keys to navigate through the text file to type your credentials anywhere in the file. Press escape to stop editing and type **‘:wq’** to exit the file.

****

Type **‘sudo vim /etc/freeradius/3.0/clients.conf’** to edit connections to this radius server in the text file. Clients are devices like our AP that will use the Radius server as its way of authenticating connections to enterprise networks. add the client in the same way as editing the other file with the new format given for this text file. After ‘client’ put your device’s name to label the entry, the secret is what you entered earlier in the AP for your shared secret with the Radius server, and the IP address is the IP address of the AP that uses the enterprise network.



Set the Ip on the device running the Radius Server to the IP you used on the AP for the Radius Server. This IP must be in the same subnet as the VLAN associated with the Enterprise network. You can now bring up the Radius Server.

Type **‘sudo freeradius -X’** to bring the Radius Server up and running and you should see a prompt in the CLI stating that it is ready for new connections. If you do not see this or you have an error like ‘binding is unsuccessful’ type **‘sudo service freeradius stop’** and bring the server back up after.

When you attempt to log in on an end device you will see a lot of text like below confirming that the AP is attempting to use the Radius Server for Authentication. You know this is successful when you see the highlighted text below:

Waking up in 2.4 seconds.

(10) Received Access-Request Id 15 from 10.10.12.5:1645 to 10.10.12.10:1812 length 258

(10) User-Name = "zippo"

(10) Framed-MTU = 1400

(10) Called-Station-Id = "64d9.89e9.65c0:CCNP\_P3\_828\_SSID1"

(10) Calling-Station-Id = "14ab.c535.9170"

(10) Cisco-AVPair = "ssid=CCNP\_P3\_828\_SSID1"

(10) Service-Type = Login-User

(10) Cisco-AVPair = "service-type=Login"

(10) Message-Authenticator = 0x64c52a60f4164ef44afd7230a5e468ff

(10) EAP-Message = 0x020b002e190017030300230000000000000004ec9d0c0847304232da678367b42717808ef05e034d576196ae05d3

(10) NAS-Port-Type = Wireless-802.11

(10) NAS-Port = 265

(10) NAS-Port-Id = "265"

(10) State = 0x9ed72dba96dc3446ce6323da3b399986

(10) NAS-IP-Address = 10.10.12.5

(10) NAS-Identifier = "APBM"

(10) Restoring &session-state

(10) &session-state:Framed-MTU = 994

(10) &session-state:TLS-Session-Information = "(TLS) recv TLS 1.3 Handshake, ClientHello"

(10) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerHello"

(10) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, Certificate"

(10) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerKeyExchange"

(10) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerHelloDone"

(10) &session-state:TLS-Session-Information = "(TLS) recv TLS 1.2 Handshake, ClientKeyExchange"

(10) &session-state:TLS-Session-Information = "(TLS) recv TLS 1.2 Handshake, Finished"

(10) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 ChangeCipherSpec"

(10) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, Finished"

(10) &session-state:TLS-Session-Cipher-Suite = "ECDHE-RSA-AES256-GCM-SHA384"

(10) &session-state:TLS-Session-Version = "TLS 1.2"

(10) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default

(10) authorize {

(10) policy filter\_username {

(10) if (&User-Name) {

(10) if (&User-Name) -> TRUE

(10) if (&User-Name) {

(10) if (&User-Name =~ / /) {

(10) if (&User-Name =~ / /) -> FALSE

(10) if (&User-Name =~ /@[^@]\*@/ ) {

(10) if (&User-Name =~ /@[^@]\*@/ ) -> FALSE

(10) if (&User-Name =~ /\.\./ ) {

(10) if (&User-Name =~ /\.\./ ) -> FALSE

(10) if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/)) {

(10) if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/)) -> FALSE

(10) if (&User-Name =~ /\.$/) {

(10) if (&User-Name =~ /\.$/) -> FALSE

(10) if (&User-Name =~ /@\./) {

(10) if (&User-Name =~ /@\./) -> FALSE

(10) } # if (&User-Name) = notfound

(10) } # policy filter\_username = notfound

(10) [preprocess] = ok

(10) [chap] = noop

(10) [mschap] = noop

(10) [digest] = noop

(10) suffix: Checking for suffix after "@"

(10) suffix: No '@' in User-Name = "zippo", looking up realm NULL

(10) suffix: No such realm "NULL"

(10) [suffix] = noop

(10) eap: Peer sent EAP Response (code 2) ID 11 length 46

(10) eap: Continuing tunnel setup

(10) [eap] = ok

(10) } # authorize = ok

(10) Found Auth-Type = eap

(10) # Executing group from file /etc/freeradius/3.0/sites-enabled/default

(10) authenticate {

(10) eap: Expiring EAP session with state 0x514bac845148a802

(10) eap: Finished EAP session with state 0x9ed72dba96dc3446

(10) eap: Previous EAP request found for state 0x9ed72dba96dc3446, released from the list

(10) eap: Peer sent packet with method EAP PEAP (25)

(10) eap: Calling submodule eap\_peap to process data

(10) eap\_peap: (TLS) EAP Done initial handshake

(10) eap\_peap: Session established. Decoding tunneled attributes

(10) eap\_peap: PEAP state send tlv success

(10) eap\_peap: Received EAP-TLV response

(10) eap\_peap: Success

(10) eap: Sending EAP Success (code 3) ID 11 length 4

(10) eap: Freeing handler

(10) [eap] = ok

(10) } # authenticate = ok

(10) # Executing section post-auth from file /etc/freeradius/3.0/sites-enabled/default

(10) post-auth {

(10) if (session-state:User-Name && reply:User-Name && request:User-Name && (reply:User-Name == request:User-Name)) {

(10) if (session-state:User-Name && reply:User-Name && request:User-Name && (reply:User-Name == request:User-Name)) -> FALSE

(10) update {

(10) &reply::Framed-MTU += &session-state:Framed-MTU[\*] -> 994

(10) &reply::TLS-Session-Information += &session-state:TLS-Session-Information[\*] -> '(TLS) recv TLS 1.3 Handshake, ClientHello'

(10) &reply::TLS-Session-Information += &session-state:TLS-Session-Information[\*] -> '(TLS) send TLS 1.2 Handshake, ServerHello'

(10) &reply::TLS-Session-Information += &session-state:TLS-Session-Information[\*] -> '(TLS) send TLS 1.2 Handshake, Certificate'

(10) &reply::TLS-Session-Information += &session-state:TLS-Session-Information[\*] -> '(TLS) send TLS 1.2 Handshake, ServerKeyExchange'

(10) &reply::TLS-Session-Information += &session-state:TLS-Session-Information[\*] -> '(TLS) send TLS 1.2 Handshake, ServerHelloDone'

(10) &reply::TLS-Session-Information += &session-state:TLS-Session-Information[\*] -> '(TLS) recv TLS 1.2 Handshake, ClientKeyExchange'

(10) &reply::TLS-Session-Information += &session-state:TLS-Session-Information[\*] -> '(TLS) recv TLS 1.2 Handshake, Finished'

(10) &reply::TLS-Session-Information += &session-state:TLS-Session-Information[\*] -> '(TLS) send TLS 1.2 ChangeCipherSpec'

(10) &reply::TLS-Session-Information += &session-state:TLS-Session-Information[\*] -> '(TLS) send TLS 1.2 Handshake, Finished'

(10) &reply::TLS-Session-Cipher-Suite += &session-state:TLS-Session-Cipher-Suite[\*] -> 'ECDHE-RSA-AES256-GCM-SHA384'

(10) &reply::TLS-Session-Version += &session-state:TLS-Session-Version[\*] -> 'TLS 1.2'

(10) } # update = noop

(10) [exec] = noop

(10) policy remove\_reply\_message\_if\_eap {

(10) if (&reply:EAP-Message && &reply:Reply-Message) {

(10) if (&reply:EAP-Message && &reply:Reply-Message) -> FALSE

(10) else {

(10) [noop] = noop

(10) } # else = noop

(10) } # policy remove\_reply\_message\_if\_eap = noop

(10) if (EAP-Key-Name && &reply:EAP-Session-Id) {

(10) if (EAP-Key-Name && &reply:EAP-Session-Id) -> FALSE

(10) } # post-auth = noop

(10) Sent Access-Accept Id 15 from 10.10.12.10:1812 to 10.10.12.5:1645 length 173

(10) MS-MPPE-Recv-Key = 0xeadf01a6441d232ae39b8c10863ad8bf37088cc5ac54132f0e2b6016c5f91977

(10) MS-MPPE-Send-Key = 0x35d1dfa6b6a416cffc59b732a2e8555175290cfda66387f1ae66bfb0ef49b239

(10) EAP-Message = 0x030b0004

(10) Message-Authenticator = 0x00000000000000000000000000000000

(10) User-Name = "zippo"

(10) Framed-MTU += 994

(10) Finished request

Waking up in 2.4 seconds.

(1) Cleaning up request packet ID 6 with timestamp +81 due to cleanup\_delay was reached

(2) Cleaning up request packet ID 7 with timestamp +81 due to cleanup\_delay was reached

(3) Cleaning up request packet ID 8 with timestamp +81 due to cleanup\_delay was reached

(4) Cleaning up request packet ID 9 with timestamp +81 due to cleanup\_delay was reached

(5) Cleaning up request packet ID 10 with timestamp +81 due to cleanup\_delay was reached

Waking up in 2.4 seconds.

(6) Cleaning up request packet ID 11 with timestamp +83 due to cleanup\_delay was reached

(7) Cleaning up request packet ID 12 with timestamp +83 due to cleanup\_delay was reached

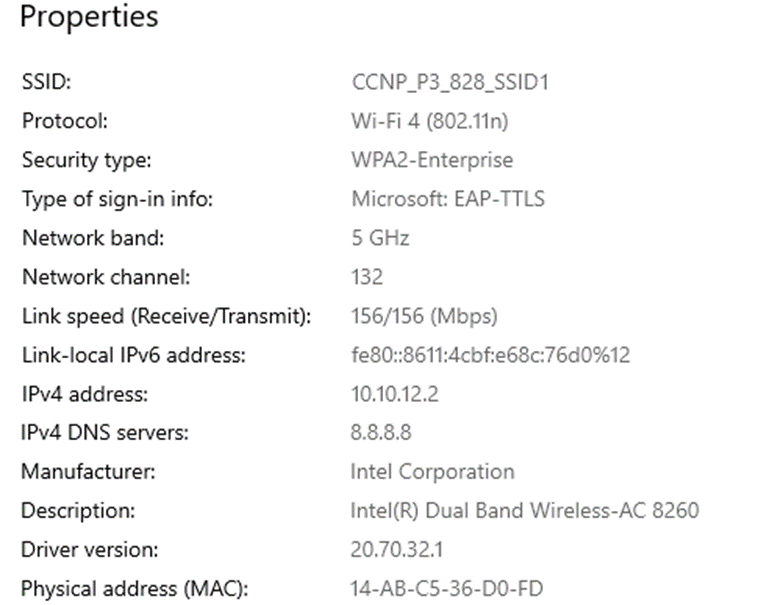
(8) Cleaning up request packet ID 13 with timestamp +83 due to cleanup\_delay was reached

(9) Cleaning up request packet ID 14 with timestamp +83 due to cleanup\_delay was reached

(10) Cleaning up request packet ID 15 with timestamp +83 due to cleanup\_delay was reached

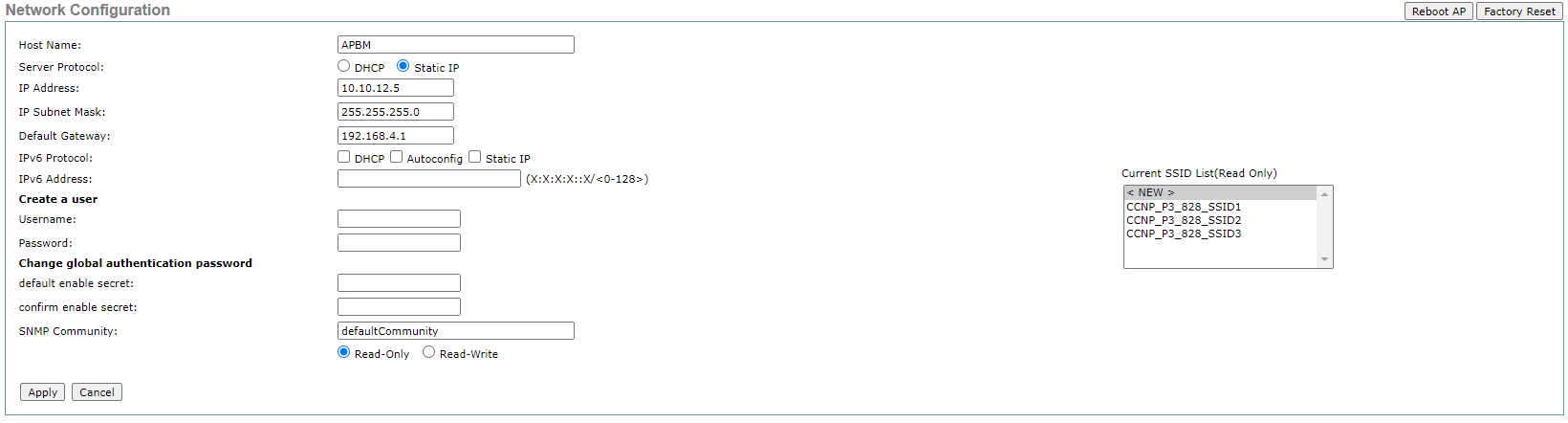
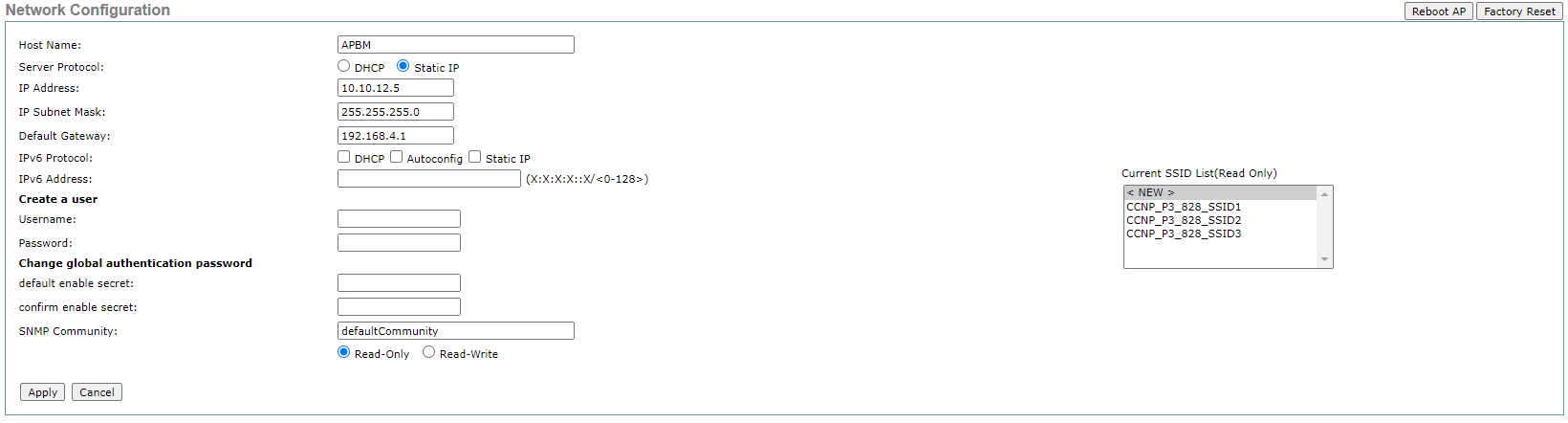
Ready to process request

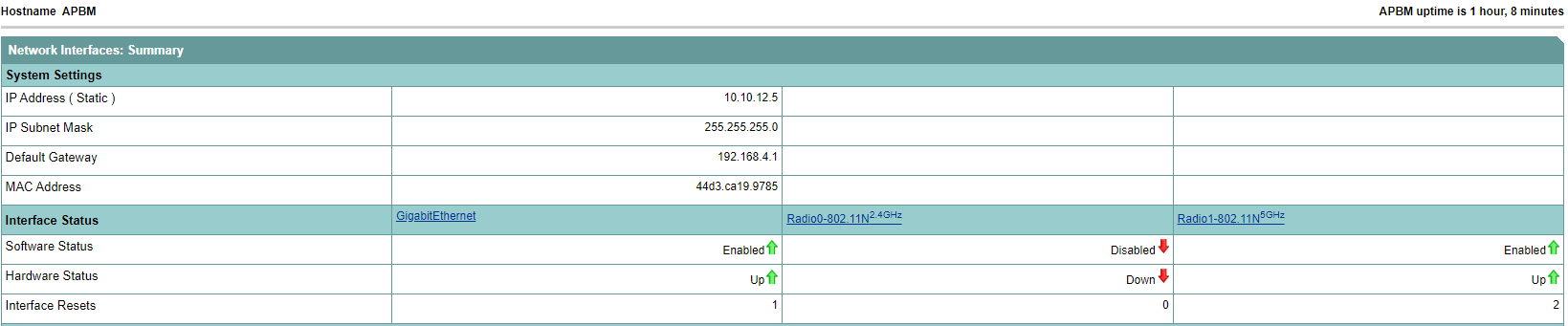
You can ensure that you successfully have WPA2-Enterprise and WPA2-Personal configured when you go to network properties on the SSIDs.





**AP Configuration:**





**Access Point Running Config:**

Building configuration...

98ol0,k,

Last configuration change at 03:14:06 UTC Fri Mar 1 2002 by Zippo

version 15.3

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

hostname APBM

logging rate-limit console 9

aaa new-model

aaa group server radius rad\_eap

server name zippo

aaa group server radius rad\_mac

server name zippo

aaa group server radius rad\_acct

aaa group server radius rad\_admin

server name zippo

aaa group server tacacs+ tac\_admin

aaa group server radius rad\_pmip

aaa group server radius dummy

server name zippo

aaa group server radius rad\_eap1

server name 10.10.12.10

aaa authentication login default local

aaa authentication login eap\_methods group rad\_eap

aaa authentication login mac\_methods local

aaa authentication login eap\_methods1 group rad\_eap1

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

no ip domain lookup

dot11 pause-time 100

dot11 syslog

dot11 vlan-name SSID-1 vlan 828

dot11 vlan-name SSID-2 vlan 214

dot11 vlan-name SSID-3 vlan 428

dot11 ssid CCNP\_P3\_828\_SSID1

vlan 828

band-select

authentication open eap eap\_methods1

authentication network-eap eap\_methods1

authentication key-management wpa

mbssid guest-mode

dot11 ssid CCNP\_P3\_828\_SSID2

vlan 428

band-select

authentication open

authentication key-management wpa version 2

mbssid guest-mode

wpa-psk ascii 7 09764719090A47455E5F24

dot11 ssid CCNP\_P3\_828\_SSID3

vlan 214

band-select

authentication open

authentication key-management wpa version 2

guest-mode

mbssid guest-mode

wpa-psk ascii 7 023C0D4B1B095F76191D29

dot11 network-map

eap profile Leap

method leap

no ipv6 cef

dot1x credentials Zippo

username Zippo

password 7 023C0D4B1B095F76191D29

username Zippo privilege 15 secret 5 $1$u737$Z9g3S8zgkDbPq9vtfjDqx1

username 14abc5359170 password 7 040A5F070D22191D5C40544042

username 14abc5359170 autocommand exit

username 14abc536d0fd password 7 11584D0415115E5F522E7B222C

username 14abc536d0fd autocommand exit

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 mode ciphers aes-ccm

encryption vlan 828 mode ciphers aes-ccm

encryption vlan 428 mode ciphers aes-ccm

encryption vlan 214 mode ciphers aes-ccm

encryption vlan 321 mode ciphers aes-ccm

ssid CCNP\_P3\_828\_SSID1

ssid CCNP\_P3\_828\_SSID2

ssid CCNP\_P3\_828\_SSID3

antenna gain 0

peakdetect

dfs band 3 block

mbssid

channel dfs

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 Dot11Radio1.1

interface Dot11Radio1.214

encapsulation dot1Q 214

bridge-group 214

bridge-group 214 subscriber-loop-control

bridge-group 214 spanning-disabled

bridge-group 214 block-unknown-source

no bridge-group 214 source-learning

no bridge-group 214 unicast-flooding

interface Dot11Radio1.321

encapsulation dot1Q 321

bridge-group 253

bridge-group 253 subscriber-loop-control

bridge-group 253 spanning-disabled

bridge-group 253 block-unknown-source

no bridge-group 253 source-learning

no bridge-group 253 unicast-flooding

interface Dot11Radio1.428

encapsulation dot1Q 428

bridge-group 254

bridge-group 254 subscriber-loop-control

bridge-group 254 spanning-disabled

bridge-group 254 block-unknown-source

no bridge-group 254 source-learning

no bridge-group 254 unicast-flooding

interface Dot11Radio1.828

encapsulation dot1Q 828

bridge-group 255

bridge-group 255 subscriber-loop-control

bridge-group 255 spanning-disabled

bridge-group 255 block-unknown-source

no bridge-group 255 source-learning

no bridge-group 255 unicast-flooding

interface Dot11Radio1.2141

interface Dot11Radio1.8281

interface GigabitEthernet0

no ip address

duplex auto

speed auto

bridge-group 1

bridge-group 1 spanning-disabled

no bridge-group 1 source-learning

interface GigabitEthernet0.214

encapsulation dot1Q 214

bridge-group 214

bridge-group 214 spanning-disabled

no bridge-group 214 source-learning

interface GigabitEthernet0.321

encapsulation dot1Q 321

bridge-group 253

bridge-group 253 spanning-disabled

no bridge-group 253 source-learning

interface GigabitEthernet0.428

encapsulation dot1Q 428

bridge-group 254

bridge-group 254 spanning-disabled

no bridge-group 254 source-learning

interface GigabitEthernet0.828

encapsulation dot1Q 828

bridge-group 255

bridge-group 255 spanning-disabled

no bridge-group 255 source-learning

interface GigabitEthernet0.2141

interface GigabitEthernet0.8281

interface BVI1

mac-address 44d3.ca19.9785

ip address 10.10.12.5 255.255.255.0

interface BVI214

ip address 10.10.11.6 255.255.255.0

interface BVI254

mac-address 44d3.ca19.9785

ip address 10.10.12.6 255.255.255.0

ip default-gateway 192.168.4.1

ip forward-protocol nd

ip http server

ip http authentication aaa

no ip http secure-server

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

ip route 0.0.0.0 0.0.0.0 GigabitEthernet0

ip radius source-interface BVI1

radius-server local

no authentication mac

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

radius server 10.10.12.10

address ipv4 10.10.12.10 auth-port 1812 acct-port 1813

key 7 044F0E151B284249584B

bridge 1 route ip

line con 0

logging synchronous

line vty 0 4

transport input all

end

**Router Running Config:**

Building configuration...

Current configuration : 1962 bytes

! Last configuration change at 18:26:01 UTC Mon Apr 29 2024

version 16.7

service config

service timestamps debug datetime msec

service timestamps log datetime msec

platform qfp utilization monitor load 80

no platform punt-keepalive disable-kernel-core

hostname ISP

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 192.168.4.2 255.255.255.0

ip nat inside

negotiation auto

interface Serial0/1/0

interface Serial0/1/1

interface GigabitEthernet0/2/0

no ip address

negotiation auto

interface GigabitEthernet0/2/1

no ip address

negotiation auto

interface GigabitEthernet0

vrf forwarding Mgmt-intf

no ip address

negotiation auto

router ospf 1

passive-interface GigabitEthernet0/0/0

network 192.168.4.0 0.0.0.255 area 0

network 192.168.40.0 0.0.1.255 area 0

default-information originate

ip default-gateway 192.168.40.1

ip nat pool ap 192.168.40.8 192.168.41.254 netmask 255.255.254.0

ip nat inside source list 1 pool ap

ip forward-protocol nd

ip http server

ip http authentication local

ip http secure-server

ip http client source-interface GigabitEthernet0/0/0

access-list 1 permit any

control-plane

line con 0

exec-timeout 0 0

transport input none

stopbits 1

line aux 0

stopbits 1

line vty 0 4

login

wsma agent exec

wsma agent config

wsma agent filesys

wsma agent notify

End

**Switch Running Config:**

Building configuration...

Current configuration : 4318 bytes

version 12.2

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

hostname SwitchPOE

boot-start-marker

boot-end-marker

no aaa new-model

system mtu routing 1500

authentication mac-move permit

ip subnet-zero

ip routing

ip dhcp excluded-address 10.10.11.4

ip dhcp excluded-address 10.10.10.5

ip dhcp excluded-address 10.10.10.2

ip dhcp excluded-address 10.10.12.3

ip dhcp excluded-address 10.10.12.5

ip dhcp pool vlan214

network 10.10.11.0 255.255.255.0

default-router 192.168.4.1

dns-server 8.8.8.8

ip dhcp pool vlan428

network 10.10.10.0 255.255.255.0

default-router 192.168.4.1

dns-server 8.8.8.8

ip dhcp pool vlan828

network 10.10.12.0 255.255.255.0

default-router 192.168.4.1

dns-server 8.8.8.8

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

no switchport

ip address 192.168.4.1 255.255.255.0

ip ospf 1 area 0

interface FastEthernet0/3

interface FastEthernet0/4

interface FastEthernet0/5

interface FastEthernet0/6

interface FastEthernet0/7

description Access port for PC 1

switchport access vlan 428

switchport mode access

interface FastEthernet0/8

description Access port for PC 2

switchport access vlan 214

switchport mode access

interface FastEthernet0/9

switchport trunk encapsulation dot1q

switchport mode trunk

interface FastEthernet0/10

switchport trunk encapsulation dot1q

switchport mode trunk

interface FastEthernet0/11

interface FastEthernet0/12

interface FastEthernet0/13

interface FastEthernet0/14

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

no ip address

shutdown

interface Vlan214

ip address 10.10.11.4 255.255.255.0

interface Vlan428

ip address 10.10.10.5 255.255.255.0

interface Vlan828

ip address 10.10.12.3 255.255.255.0

router ospf 1

log-adjacency-changes

network 10.10.10.0 0.0.0.255 area 0

network 10.10.11.0 0.0.0.255 area 0

network 10.10.12.0 0.0.0.255 area 0

ip default-gateway 192.168.4.2

ip classless

ip route 0.0.0.0 0.0.0.0 192.168.4.2

ip http server

ip http secure-server

ip sla enable reaction-alerts

line con 0

line vty 0 4

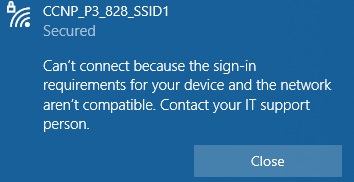
login

line vty 5 15

login

end

**Problems:**

* We were unsure if the AP had Auto-MDIX capabilities on its port.
  + Researched and couldn’t find an answer but since the switch has auto-MDIX we believe it is does not matter, went with crossover just in case as we were instructed.
* Holding down for 8 seconds did not reset the AP.
  + Figured out we had to hold mode button for 20 secs to reset while AP was powering on.
* Didn't understand TFTP servers.
  + Trial and error to get the OS file onto the TFTP server but succeeded once finding the directory.
* We changed log in credentials to the AP which caused us to be unable to load webpage.
  + Restarted PC and it gave us the prompt again but failed to fully load the webpage.
  + Reloaded AP and reenabled TFTP server on PC connected making the webpage work again.
    - Confirmed the TFTP server is required to be on the PC to access AP (didn’t need it later, found it is preferred to console into the AP instead).
* Could not login into enterprise network but visible on Wi-Fi list.
  + Attempted logging in to network manually, no prompt given to login.
  + Failed attempts
    - Turned the beacon off to see if we could manually login into the network.
    - Deleted and recreated user in the local Radius Server.
    - Changed authentication protocol to EAP fast instead of EAP.
    - Changed server priority to use our Local Radius Server as default authentication, nothing changed.
    - Tried adding a new windows user based on the login information to see if the PC user had to match the user in the Local Radius Server.
    - Tried forcing our NIC to 5ghz only in properties.
    - Made a user on the Local Radius Server with the name of the PC.
    - Reinstalled Network drivers on PC.
    - Researched multiple Videos.
      * Created new SSID with no setting to see if connection was possible.
        + Could now log into the SSID and we determined having a network ID did not allow connections without some other certificates.
        + Removed Network ID could now login on the WPA2 Pre-Shared Key users.
  + Still could not log in into Enterprise SSID.
  + 
    - Local Radius server had the wrong IP when we changed the IP of the AP previously.
      * Changed Local Radius Server IP.
        + Could not log in.
      * AAA Client Server had wrong IP.
        + Changed IP for anything that used our Local Radius Server Ip.
      * Received a NAS key mismatch warning on the AP and assumed that to be the issue causing no login.
        + The shared secret on the RADIUS server and the NAS are not the same which was not the case, the error is irrelevant.
      * Error “No Radius hosts configured or no valid server present in the server group rad\_eap”.
        + When we changed the Pre-shared Key, it got rid of our radius server in the default radius authentication prompt for the SSID.

Changed the EAP authentication to our Local Radius Server.

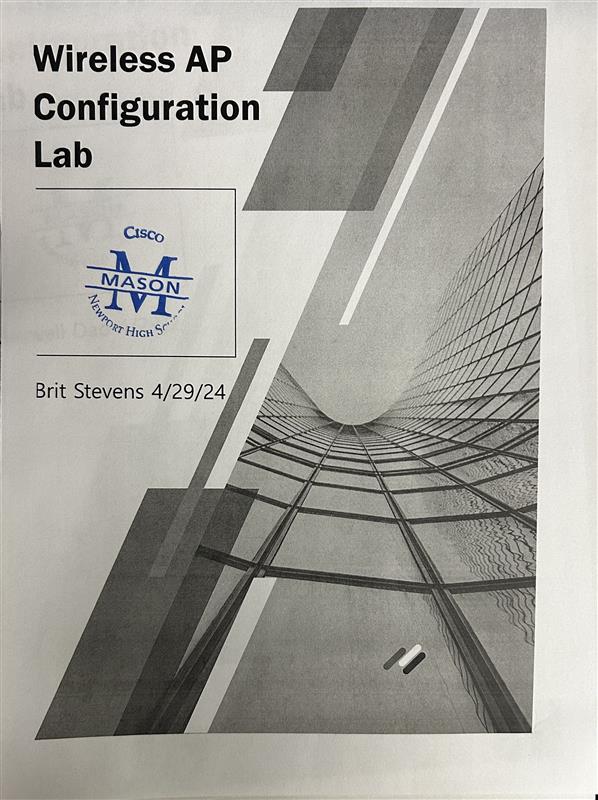
Changed the admin authentication to the Local Radius Server.

Could not log in.

* + - * We found out that Local Radius Server was not possible without a software like FreeRadius to use the server we configured.
* We had set a static route on Switch and could not access AP GUI.
  + We turned off the static route when we wanted to use the GUI.
  + Started to use the CLI instead of Gui when we knew the commands but much more complicated.
* AP could not reach the local network due to its ethernet port being in a different subnet.
  + Gave the AP’s port an IP in the range of the SSIDs’ subnets.
  + SSIDs can now ping within the local network, still no internet connection.
* AP could reach the internet and ping webpages’ IP but end devices cannot load them or use other features on the internet.
  + Used an ipconfig on the PCs and found out that the SSIDs were not giving a DNS server so we could not load webpages.
    - Changed the DHCP pools to give a DNS server as default.
* DHCP errors from layer 3 switch.
  + The DHCP server would not give out the right Ips after a reload on the switch it was resolved.
* Tried using a Hyper-V Windows server as a radius but was taking too long for the deadline.
  + Collaborated with other students to use a shared Linux Radius server on a hard drive and edited for our use.
    - VLAN’s IPs for 428 and 828 were swapped from what they were supposed to be in the configuration.
      * Changed them in the Switch’s VLAN interfaces.
    - Mismatching Pre-shared key did not allow to access the radius database from the AP
      * Had accidentally deleted a character in the key on the Radius text file.
    - IP of the Radius Server was out of the range of the enterprise network so the network could not access the Radius Server like it needed to.
      * Changed the IP of the Radius Server everywhere.

**Conclusion:**

This lab was very difficult and tedious, but we were eventually successful with some perseverance. Configuring the Access Point didn’t seem very complicated when we were in the GUI but combining it with other aspects of the lab created the challenge. This lab had the most problems out of any lab we’ve done so far making us collaborate with others more than previously. We focused on the aspects of the labs we knew how to do like the router and switch configurations first then moved onto the Access Point and Radius. My biggest takeaway from this lab is that collaborating with others when you have similar issues can greatly increase your efficiency and solve the issues fully after some time. My group was very stuck on the Radius server part while others were stuck on the IP Natting, so we exchanged ideas to solve the issues with each other’s configurations. This lab was useful for our future because we will have to collaborate with others and learn to work together towards the same goal.

****