A logo with red letters

Description automatically generated

***Wireless Access Point Setup Lab***



Charlie Qu

Period 0-2

Mason/Hansen

6/1/2024

Wireless Access Point Setup Lab

Purpose:

Utilize a Layer 3 switch to configure a Wireless Access Point (WAP) for Internet connectivity through three separate SSIDs. Two of these SSIDs should utilize Wi-Fi Protected Access Version 2 (WPA2) with a Pre-shared Key (PSK), while the third should use WPA2 Enterprise Mode, authenticated via a RADIUS server.

Background Information:

What is a Wireless Access Point (WAP)?

A Wireless Access Point (WAP) is a device that enables wireless-compatible devices to connect to a wired network. It simplifies network setup by eliminating the need for physical cables, thus enhancing connectivity efficiency. This makes WAPs particularly useful in large buildings spanning multiple levels.

Further Advantages of a WAP

* Additional User Access: Unlike typical wireless routers that support 10-20 users, a WAP can accommodate 50-100 or more users due to its higher signal capacity.
* Broader Transmission Range and Mobility: WAP signals can cover 100-300 meters, making them ideal for larger businesses and allowing users to move freely within the network.
* Flexible Networking: WAPs are well-suited for various environments, especially those outside the home with numerous wireless devices and complex networking topologies.

Configuring a WAP: CLI vs. GUI

* CLI (Command Line Interface): Users interact with the system by typing commands into a terminal and receiving text-based responses.
* GUI (Graphical User Interface): Users interact with the system through graphical elements like windows, scrollbars, buttons, and icons, making it more intuitive. In this lab, the GUI was primarily used for configuring the WAP, while the CLI was employed to verify configurations in a concise form.

Using a RADIUS Server

We used a RADIUS (Remote Authentication Dial-In User Service) server to connect our third SSID to the internet. RADIUS is a security protocol that provides centralized authentication for network access, storing user credentials in a central database to ease administration and enhance security. In practice, a client sends a request to the Access Control Server (ACS), which responds with an access-accept message if credentials match or an access-reject message if they do not. In this lab, our instructor provided a pre-configured username and password, allowing devices to access the internet using sudo commands on Linux.

Advantages of RADIUS

* Open Standard Protocol: RADIUS can be used across various devices wanting to access the network.
* Greater Accounting Support: Provides more extensive accounting features than TACACS+.
* Flexible User Management: Allows administrators to manage users and permissions with greater granularity.
* Integration with Other Protocols: Can work with protocols like LDAP or Kerberos for added flexibility.
* Scalability: Supports large networks with many users and devices, making it ideal for this lab.

DHCP (Dynamic Host Configuration Protocol)

* DHCP is a protocol that automatically allocates IP addresses to devices, simplifying IP address management, especially in large work environments. The DHCP process includes:
* DHCP Discover Message: The client broadcasts a message to find DHCP servers.
* DHCP Offer Message: Servers respond with available IP addresses and TCP configuration information.
* DHCP Request Message: The client requests the offered IP address.
* DHCP Acknowledgement Message: The server binds the IP address to the client and acknowledges the request.

NAT (Network Address Translation)

NAT translates private IP addresses into public IP addresses for internet access, allowing multiple devices to use a single public IP address. NAT terms include:

* Inside Local Address: Private IP address assigned to a host within the local network.
* Inside Global Address: IP address representing inside local addresses to the outside world.
* Outside Local Address: Actual IP address of the destination host within the local network post-translation.
* Outside Global Address: IP address of the outside destination host before translation.

Trunk Ports for InterVLAN Routing

Trunk ports carry traffic from multiple VLANs, essential for interVLAN routing. In this lab, trunking was configured to allow traffic exchange between switches on different racks, providing greater network flexibility and scalability.

Lab Summary:

To set up this lab, we started by connecting an ethernet cable from the BVI1 port of the WAP to our PoE (Power over Ethernet) Layer 3 switch, providing both power and network connectivity. Following our teacher's instructions, we then imaged the WAP. Full access to the WAP required a TFTP server, which we configured using the desktop app TFTPD64. We also connected ethernet cables from our Layer 3 switch to PCs to access the WAP’s GUI.

We assigned IP addresses to the interfaces used in this lab either manually or through DHCP pools we created, enabling automatic IP assignment to users. Because the internet router was on a different rack, we configured trunking on the Layer 3 switch to enable internet access. On R1, we set up NAT to allow devices with private IP addresses to access the internet.

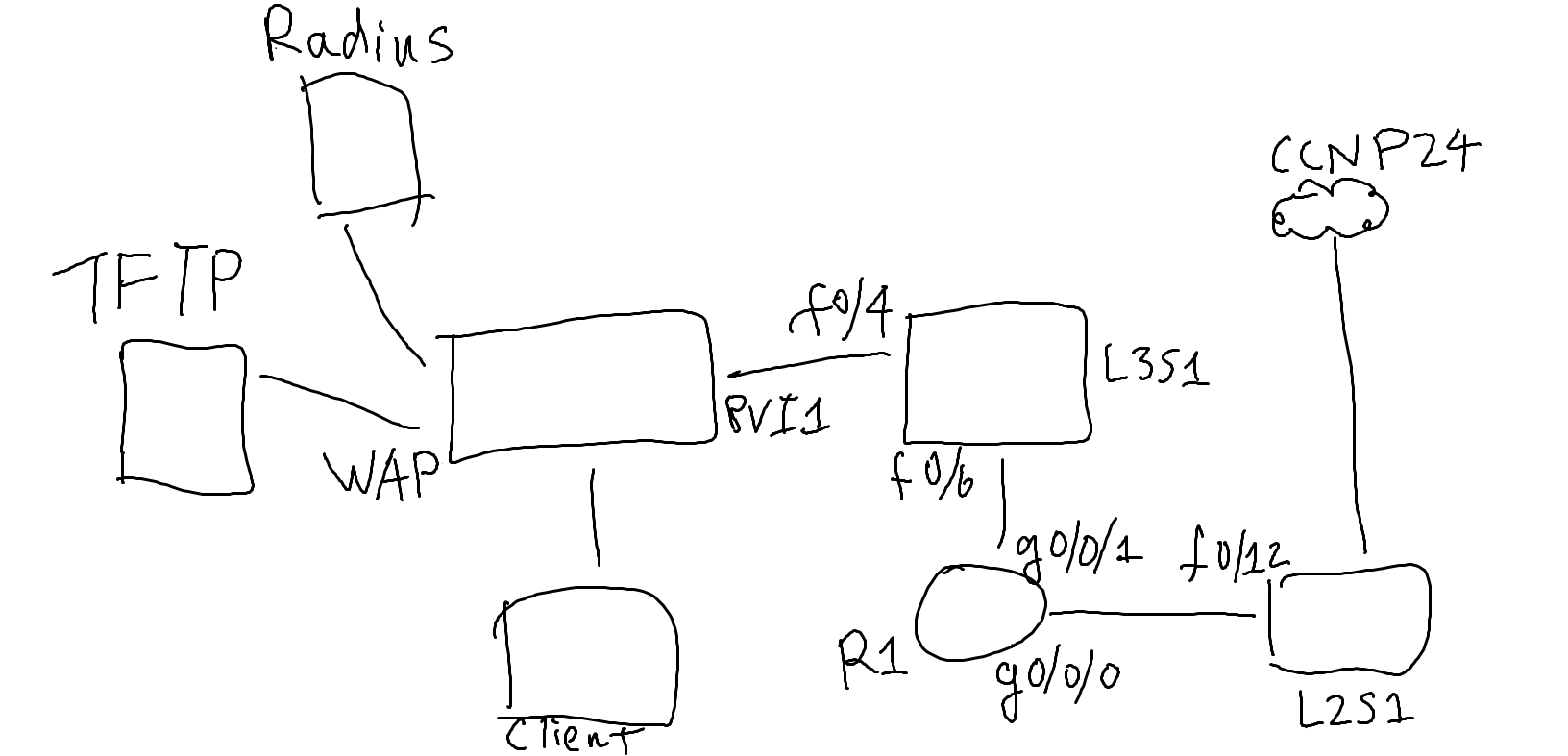
Within the WAP’s GUI, we created three SSIDs for internet connectivity. Two SSIDs used WPA2 with a Pre-Shared Key (PSK), while the third used WPA2 Enterprise mode, requiring a RADIUS server for authentication. After finalizing the SSID settings, we assigned them to separate VLANs and created a native VLAN.

For the third SSID requiring RADIUS, we used a separate drive with the Open Free RADIUS app installed. By entering commands on Linux, we configured the SSID to connect to the internet. We then tested all three SSIDs to ensure they successfully connected to the internet and could reach a selected webpage.

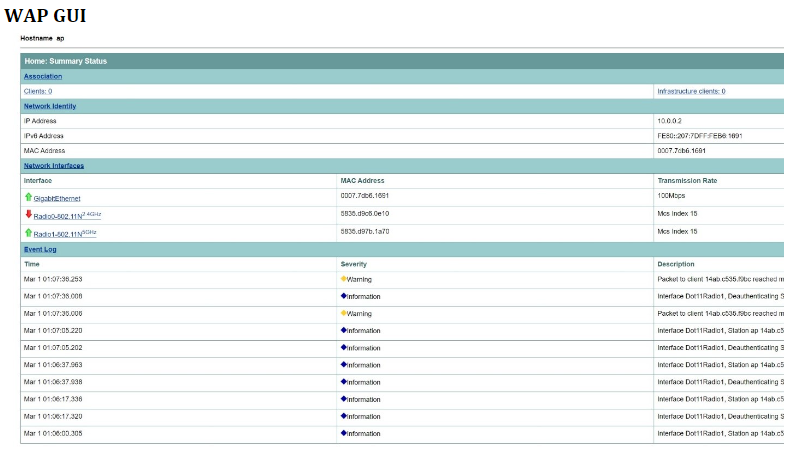
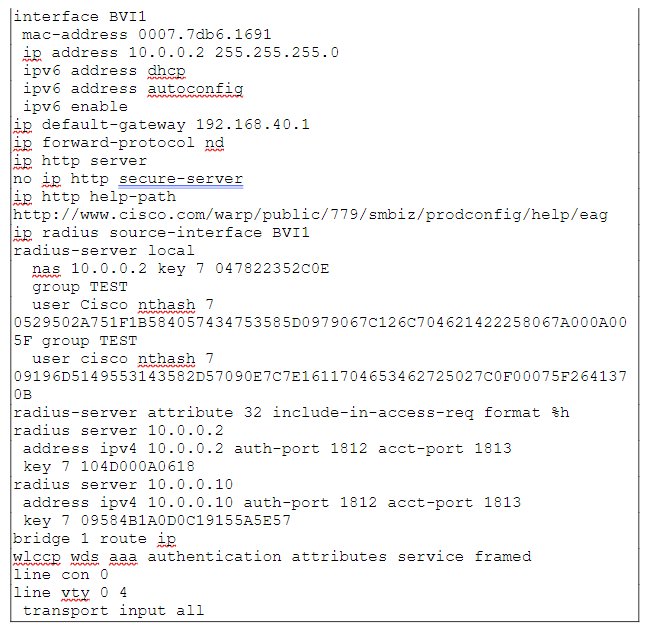
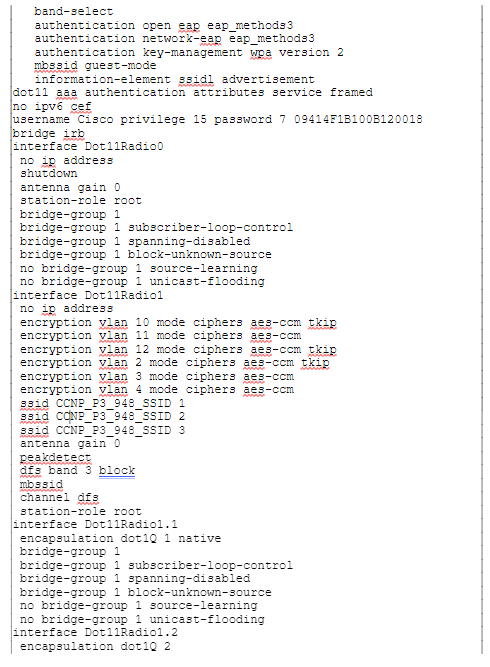
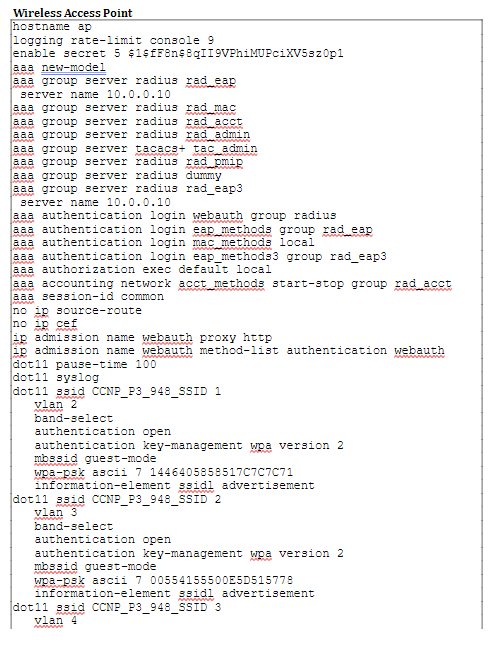
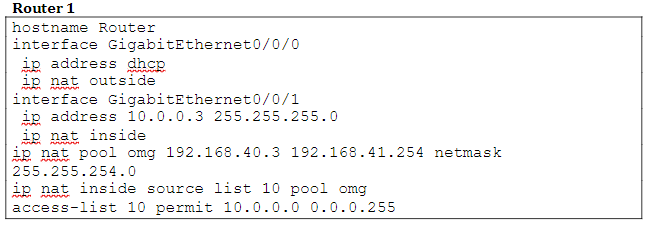
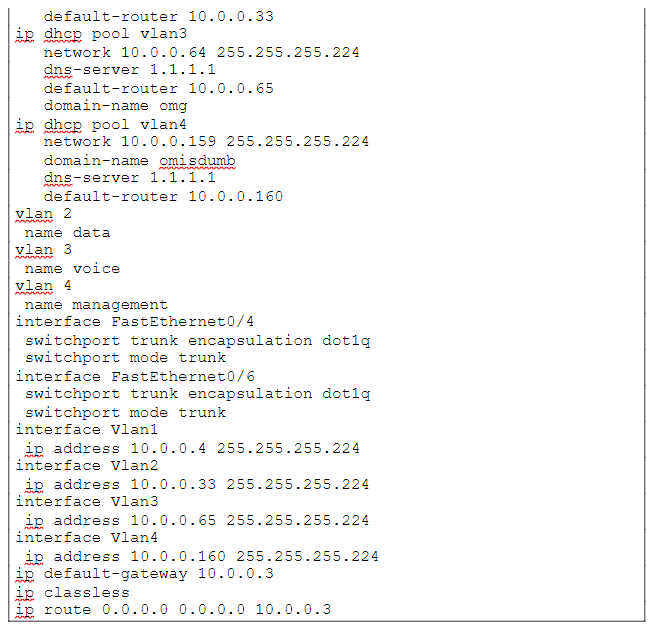
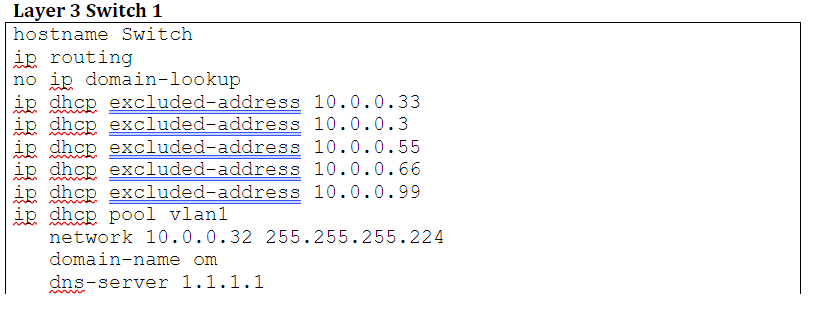
Lab Commands:

* ip address dhcp – Acquires a dynamically assigned IP address for a designated interface.
* ip nat inside/outside – Activates and associates NAT processing with either the inside or outside of an interface.
* ip nat pool pool-name start-ip end-ip netmask netmask – Specifies a range of global IP addresses that can be allocated to users connecting to the network.
* access-list access-list-number permit source wildcard mask – Creates a standard access list that permits translated IP addresses to traverse the network.
* ip dhcp excluded-address ip – Specifies IP addresses to be excluded from the DHCP pool.
* ip dhcp pool [name] – Configures a DHCP pool with a defined range of IP addresses.

Network Diagram:



Configurations:



In the WAP’s summary screen, the Radio 5 GHz has been activated to operate on a channel free from interference.

A close-up of a computer screen

Description automatically generatedA close-up of a computer screen

Description automatically generated

A close-up of a computer screen

Description automatically generated

In the same Summary tab, the WAP was configured with IP settings, enabling DHCP in the upper left corner. All three SSIDs were created under the 5 GHz radio band in the bottom right, and the labels for these SSIDs are displayed in the upper right corner.

A close-up of a computer screen

Description automatically generatedA close-up of a computer screen

Description automatically generatedA close-up of a computer screen

Description automatically generated

In the left panel under the Services tab, the VLAN page has been selected. Here, we configured our three VLANs, each assigned to an SSID and set as the Native VLAN. Additionally, information about packet traffic is displayed at the bottom of the page.

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedIn the left panel, under the Security tab, the Global SSID Manager page is used to configure additional SSID settings to enable Internet access when logged in through our PCs.

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

In the left panel, under the Security tab, the Server Manager page was used to select our RADIUS server, enabling our third SSID to access the Internet after its IP was configured on Linux.

A close-up of a document

Description automatically generatedFinally, to review all configurations made in the GUI, the Security Summary tab can be checked to ensure the functionality of SSIDs and RADIUS servers after they have been applied.

After opening the Linux terminal, switch to sudo su mode to execute commands requiring administrative privileges. You can then download Freeradius by using the command apt-get install freeradius.



Use the vim command on /etc/freeradius/3.0/clients.conf to edit the configuration file.

A screenshot of a computer screen

Description automatically generated  
You should see a screen with the image above. If not, use the arrow keys to scroll up or down.



Press I to enter insert mode and edit the file. Create a client by navigating to the client access point section and setting the password and IP address.

To exit insert mode, press the Escape key, then type :wq to save the changes and exit vim.

Use the vim command on /etc/freeradius/3.0/users to edit the file.

A screenshot of a computer screen

Description automatically generated  
After pressing enter, a similar screen should appear.



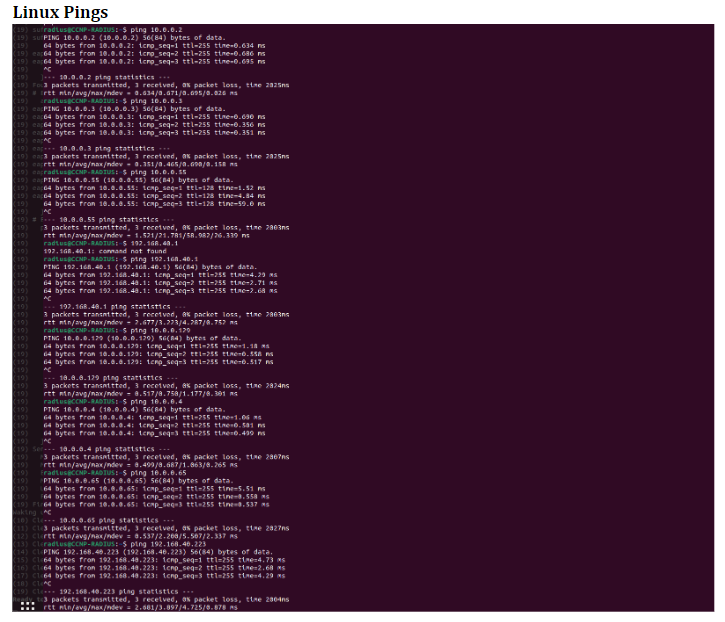
At the top of the configuration file, you should see that a user has already been created. If no user is shown, create one by typing: (User) Cleartext-Password := "password".

Exit insert mode and save your changes by typing :wq.

A screenshot of a computer

Description automatically generated

Set up your ethernet connection to use a static IP address, which will serve as the address for your RADIUS server running on your PC.

A screenshot of a computer screen

Description automatically generated

Problems:

Setting up our first two SSIDs with WPA2 and a Pre-shared Key was straightforward, and they connected to the Internet without any issues. However, we faced challenges with the third SSID, which used WPA2 Enterprise mode and required a RADIUS server. We discovered that we needed an additional VLAN to act as our Native VLAN for trunking between our Layer 3 switch and the switch providing internet access. Moreover, we used Linux for the first time in our labs to configure the RADIUS server, which was installed on a separate drive to prevent any corruption of our own systems. With the help of research and input from other groups, we used sudo commands to set a username and password for our user to access the internet, in contrast to the first two SSIDs that only required a password.

Conclusion:

Since this lab was new to our class, we spent a considerable amount of time researching how to configure wireless access points. The WAP’s GUI was particularly helpful, providing a hands-on understanding of the various components and making it easier to identify errors compared to using the CLI. Although using RADIUS through Linux was complex, it was very rewarding to see our efforts result in all three SSIDs successfully accessing the internet and reaching a webpage. This lab was a great refresher on concepts like setting up NAT, which I hadn't revisited since CCNA, while also reinforcing my existing knowledge in areas like DHCP and trunking. Collaborating with my partner and other groups was beneficial, as we assisted each other throughout different parts of the lab. Having a dedicated drive for RADIUS was also convenient, eliminating the need for individual installations.

Teacher Signoff:

