A white rectangular sign with black text

Description automatically generated

**Purpose**

This lab is designed to provide real-world experience in setting up Cisco wireless access points and configuring wireless local area networks (WLANs) with a wired setup and multiple Service Set Identifiers (SSIDs).

**Background Information**

Think of a wireless access point (WAP) as a bridge between fully wired and wireless networks. It is a networking device designed to connect wireless devices to an existing wired network. Utilizing WAPs to connect all wireless-capable devices in a network is far more efficient than connecting each through wires and cabling.

To install an access point, it is first connected to a wired network made of routers or switches, typically through an Ethernet cable. Once connected, the AP broadcasts a wireless signal using a specific frequency (e.g., 2.4 GHz or 5 GHz) and Wi-Fi standard (e.g., 802.11ac). Then, the AP can be configured with its own Service Set Identifier, or SSID, which is the name of the wireless network that users see when connecting to Wi-Fi on their devices. Now, data can be transmitted from the wired network to wireless devices connected to the AP. APs can also be configured with many security settings, such as passwords and encryption to prevent unwanted access. Clients within the AP’s range can easily detect its SSID and use its credentials to connect to it.

Cisco allows additional configurations to be through a wireless LAN controller (WLC); it can be accessed either through the web-based GUI, through inputting the WLC’s IP address into a web browser, or the command-line interface (CLI). Using a centralized management tool like a WLC is extremely helpful as it can simplify the AP configuration process and provide better control over networks.

This lab required the use of previous knowledge of IP Routing learned through the CCNA course, such as NAT and router-on-a-stick configurations. Configuring NAT (Network Address Translation) allows private IP addresses to be translated to a public IP address to access the Internet. “Router on a stick” configuration is used to route traffic between multiple VLANs on a network by creating multiple sub interfaces on one physical router port, which allows for traffic from different VLANs to be routed through a single port as though there are multiple ports in its place. These concepts were implemented in this lab to route traffic through each device.

A portion of this lab required installing a RADIUS (Remote Authentication Dial-In User Service) server. RADIUS servers provide users with a centralized way to manage authentication, authorization, and accounting and is commonly used in wireless networks. RADIUS servers receive authentication requests from clients, such as access points, VPNs, etc., and either grants or denies access. Such technology is often deployed in enterprise network infrastructure in the real world.

**Lab Summary**

To complete this lab, we followed these procedures:

1. Designed a topology with a TFTP server, a PoE (Power over Ethernet) Switch, wireless devices, and an access point.
2. Connected the access point to the computer with a console cable and an Ethernet cable.
3. Consoled into the switch and set up a TFTP server.
4. Set the IP addresses for the access point and the computer.
5. Entered the AP’s IP address in a web browser (Microsoft Edge preferred) to access the GUI.
6. Using the GUI, set up three SSIDs for VLANs 2, 3, and 4.
7. Set up WPA pre-shared key authentication on the access point.
8. Set VLAN configurations on the switch.
9. Configured NAT on router interfaces.
10. Configured a router-on-a-stick set-up.
11. Troubleshooted network until functioning.

**Lab Commands**

**ip routing**Enables IP routing in switch configuration mode.

**lwapp ap ip address** [ipv4 address] [subnet mask]  
Sets the IPv4 address for the access point.  
  
**lwapp ap ip default-gateway** [ipv4 address]  
Sets the default gateway address for the access point.  
  
**archive download-sw /overwrite /reload** [file]  
Overwrites and reloads a new file, in this case, TFTP file for the server.  
  
**ip nat pool** [pool name] [starting IP] [ending IP] **netmask** [subnet mask]  
Defines a range of IP addresses to be used with NAT configurations.  
  
**ip dhcp pool** [vlan name]  
Creates a new DHCP pool allowing to make parameters for a specific VLAN.   
  
**network** [ipv4 address] [subnet mask]  
Sets the range of addresses to be assigned during use of DHCP.  
  
**ip dhcp excluded-address** [ipv4 address]  
Specifies addresses to not be assigned by the DHCP server.  
  
**switchport mode trunk**  
Configures a switch interface as a trunk port, allowing traffic from multiple VLANs over a single physical port.  
  
**ip route** [destination network] [subnet mask] [next-hop ipv4 address] [metric number]  
Creates a static route to define the paths a packet should follow in order to reach the destination network. Used in situations where no routing protocols are used.  
  
**dot11 ssid** [SSID name]  
Used on wireless access point to set the SSID name.  
  
**authentication open**  
Allows clients to associate with the SSID with open authentication  
  
**authentication key-management wpa version 2**  
Specifies the key management method for securing wireless communications, specifically WPA2 (Wi-Fi Protected Access version 2), which provides high security.

**Topology & IP Scheme**

A diagram of a computer network

Description automatically generated

**Configurations**

**Router1:**

Show run:

Building configuration...  
Current configuration : 1602 bytes  
version 15.5  
service timestamps debug datetime msec  
service timestamps log datetime msec  
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  
multilink bundle-name authenticated  
license udi pid ISR4321/K9 sn FDO21491LXV  
license accept end user agreement  
license boot level securityk9  
spanning-tree extend system-id  
redundancy  
mode none  
vlan internal allocation policy ascending  
interface GigabitEthernet0/0/0  
ip address 10.0.0.193 255.255.255.0  
ip nat inside  
negotiation auto  
interface GigabitEthernet0/0/1  
ip address dhcp  
ip nat outside  
negotiation auto  
interface Serial0/1/0  
interface Serial0/1/1  
interface GigabitEthernet0  
vrf forwarding Mgmt-intf  
no ip address  
shutdown  
negotiation auto  
interface Vlan1  
no ip address  
shutdown  
ip nat pool AP\_POOL 192.168.40.2 192.168.41.254 netmask 255.255.254.0  
ip nat inside source list 1 pool AP\_POOL overload  
ip forward-protocol nd  
no ip http server  
no ip http secure-server  
ip tftp source-interface GigabitEthernet0  
ip route 0.0.0.0 0.0.0.0 192.168.40.1  
access-list 1 permit 10.0.0.0 0.0.0.255  
control-plane  
line con 0  
exec-timeout 0 0  
stopbits 1  
line aux 0  
stopbits 1  
line vty 0 4  
login  
ntp server pool.ntp.org  
end

**Switch:**

Show run:

Building configuration...

Current configuration : 2322 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**

**ip dhcp excluded-address 10.0.0.65**

**ip dhcp excluded-address 10.0.0.129**

**ip dhcp excluded-address 10.0.0.1**

**ip dhcp excluded-address 10.0.0.193**

**ip dhcp pool VLAN2**

**network 10.0.0.0 255.255.255.192**

**default-router 10.0.0.1**

**domain-name cisco.com**

**dns-server 1.1.1.1**

**ip dhcp pool VLAN3**

**network 10.0.0.64 255.255.255.192**

**default-router 10.0.0.65**

**dns-server 1.1.1.1**

**domain-name cisco2.com**

**ip dhcp pool VLAN4**

**network 10.0.0.128 255.255.255.192**

**default-router 10.0.0.129**

**dns-server 1.1.1.1**

**domain-name cisco3.com**

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**

**switchport trunk encapsulation dot1q**

**switchport mode trunk**

**interface FastEthernet0/3**

**switchport access vlan 2**

**switchport trunk encapsulation dot1q**

**switchport mode trunk**

interface FastEthernet0/4

interface FastEthernet0/5

interface FastEthernet0/6

interface FastEthernet0/7

interface FastEthernet0/8

interface FastEthernet0/9

interface FastEthernet0/10

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**

**ip address 10.0.0.252 255.255.255.192**

**interface Vlan2**

**ip address 10.0.0.1 255.255.255.192**

**interface Vlan3**

**ip address 10.0.0.65 255.255.255.192**

**interface Vlan4**

**ip address 10.0.0.129 255.255.255.192**

**ip default-gateway 10.0.0.193**

ip classless

**ip route 0.0.0.0 0.0.0.0 10.0.0.193**

ip http server

ip sla enable reaction-alerts

line con 0

line vty 0 4

login

line vty 5 15

login

end

**Access Point:**

Show run:

Building configuration...  
Current configuration : 4735 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 $1$iqK4$gs1Txjbm6FNlnfh/zkixY0  
aaa new-model  
aaa group server radius rad\_eap  
server name freeradius  
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 freeradius  
aaa authentication login eap\_methods group rad\_eap  
aaa authentication login mac\_methods local  
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 ssid CCNP\_P1\_0507\_VLAN2  
   vlan 2  
   authentication open  
   authentication key-management wpa version 2  
   mbssid guest-mode  
   wpa-psk ascii 7 112A1016141D5A5E57  
dot11 ssid CCNP\_P1\_0507\_VLAN3  
   vlan 3  
   authentication open  
   authentication key-management wpa version 2  
   mbssid guest-mode  
   wpa-psk ascii 7 112A1016141D5A5E57  
dot11 ssid CCNP\_P1\_0507\_VLAN4  
   vlan 4  
   authentication open eap eap\_methods3  
   authentication network-eap eap\_methods3  
   authentication key-management wpa  
   mbssid guest-mode  
dot11 wpa handshake timeout 500  
no ipv6 cef  
username Cisco privilege 15 password 7 02250D480809  
bridge irb  
interface Dot11Radio0  
no ip address  
shutdown  
encryption vlan 3 mode ciphers aes-ccm  
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 3 mode ciphers aes-ccm  
encryption vlan 4 mode ciphers aes-ccm  
encryption vlan 1 key 2 size 128bit 7 F820D71D63394A6BD63DE57FD26B transmit-key  
encryption vlan 1 mode wep mandatory  
encryption vlan 2 mode ciphers aes-ccm  
ssid CCNP\_P1\_0507\_VLAN2  
ssid CCNP\_P1\_0507\_VLAN3  
ssid CCNP\_P1\_0507\_VLAN4  
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 Dot11Radio1.21  
interface Dot11Radio1.31  
interface Dot11Radio1.41  
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 GigabitEthernet0.21  
interface GigabitEthernet0.31  
interface GigabitEthernet0.41  
interface BVI1  
description freaky  
mac-address 44d3.ca19.96af  
ip address 10.0.0.253 255.255.255.0  
ipv6 address dhcp  
ipv6 address autoconfig  
ipv6 enable  
ip default-gateway 192.168.40.1  
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 attribute 32 include-in-access-req format %h  
radius server freeradius  
address ipv4 10.0.0.254 auth-port 1645 acct-port 1646  
key 7 123A0C041104  
bridge 1 route ip  
line con 0  
line vty 0 4  
transport input all  
end

**Problems**

At times, when we resumed the lab the next day, we weren’t able to connect to the GUI during class. The cause of this wasn’t obvious and was primarily solved by simply reopening the lab the following day.

After troubleshooting and verifying our configurations were functioning, we discovered that the problem related to Layer 1, since the Ethernet cable connecting the switch to the router was physically connected to the wrong ports. To fix this, the cable was switched from port g0/0/0 to g0/0/1.

When initially configuring the switch, we didn’t know it was required for each VLAN to have a name. We quickly resolved this by using the **vlan name** [name] command.

After being unable to connect to our network, we troubleshooted with a set of pings on each device and discovered that the switch could not ping the access point. Entering the **show ip interface brief** command showed IP address configurations and allowed us to figure out that VLAN 1 was missing an IP address. Once the VLAN interface was up, by using the **no shutdown** command, and had an IP, pings were able to travel through the switch.  
  
**Conclusion**  
Completing this lab helped us experience working with wireless devices along with networking practices usually used with wired topologies. We learned how to set up a Cisco LWAP and use multiple SSIDs to communicate between devices.

**Lab Signoff**

A close-up of a paper

Description automatically generateds