



Wireless Access Point Setup Lab

Joshua Widjaja

Period 0-2 CCNP

Mr. Mason

**Purpose:**

The purpose of this lab was to learn about how to configure a CISCO Access Point (AP) using 3 Service Set Identifiers (SSIDs). We also had to familiarize ourselves in configuring SSIDs with encryptions such as WPA2-Personal and WPA2-Enterprise security protocols and creating a Router using Network Address Translation (NAT) to allow for wireless internet access while being protected. We then learned to assign VLANs to specific SSIDs to divide the network into smaller parts.

**Background Information:**

|  |  |
| --- | --- |
| **Concepts** | **Information** |
| Access Point (AP) | An access point is a networking hardware device that allows wireless devices to connect to a wired network and in this lab specifically, this connection is done through Wi-Fi. Wi-Fi is a networking technology that uses radio waves to provide wireless internet access. An access point is essentially a bridge between the wireless devices and the wired networks, allowing for communication between the two to happen. A Cisco access point generally has a coverage range of around 100 to 300 feet indoors and whichever devices are within this range will be connected to the wired network. Access points are crucial for extending network coverage and providing flexibility and scalability in a large array of commonly used environments such as homes, schools, and businesses. |
| SSIDs (Service Set Identifiers) | An SSID is a distinct name that identifies a wireless network. When a wireless device such as a phone scans for Wi-Fi networks to connect to, the phone settings will display names of the networks they detect which are SSIDs. The phone user can then click onto the wireless network they want to connect to. Access points and routers broadcast their SSIDs to reach out to wireless devices within the AP and routers network range. Each SSID can be configured with different security protocols and assigned to different VLANs for network segmentation. |
| WPA2-Personal | WPA2-Personal (Wi-Fi Protected Access 2 – Personal) is a security protocol created to provide security to wireless networks. WPA2-Personal uses a pre-shared key (PSK) to authenticate its users. A pre-shared key is a unique password that is shared to all users who want to access the wireless network. WPA2-Personal also uses Advanced Encryption Standard (AES) encryption to secure the data that is being sent to the wireless network. |
| WPA2-Enterprise | WPA2-Enterprise (Wi-Fi Protected Access 2 – Enterprise) is a security protocol created to provide reliable and scalable authentication and encryption for larger wireless networks such as businesses. While WPA2-Personal uses a pre-shared key to authenticate its users, WPA2-Enterprise uses an authentication server such as a RADIUS server. WPA2-Enterprise uses the IEEE 802.1x standard to authenticate network devices and uses AES encryption similar to WPA2-Personal. With more control over network access through a centralized management of an authentication server, WPA2-Enterprise provides stronger security than WPA2-Personal by granting administrators control over individual user credentials. This allows for WPA2-Enterprise to have incredible scalability suitable for larger organizations with many users as there is no need for each individual to share their own pre-shared key. |

**Lab Summary with Lab commands:**

**Access Point Configuration:**

**Cabling:** First off, plug the black console cable into the console port of the AP to configure it. We connected a crossover cable connecting from the AP’s ethernet port to a port on the POE (power over ethernet switch). This allows your computer to be able to configure the access point.

**AP Setup:** We first rebooted our AP by holding the factory reset button down for 8 seconds. A factory reset being issued before we configure the AP is best practice because it removes previous configurations, clears SSIDs and passwords (we made our own later), and eliminates potential security risks. To reboot the access point, hold the factory reset button for 8 seconds.



Factory reset button

**A white square object with a green light

Description automatically generated**

The light will start to flash blue and once the light turns off or changes color, you can let go of the button. As soon as the image starts to load and you see ######### starting to appear, hit escape to interrupt the boot process. We deleted all previous config.txt, private-multiple-fs, and capwap-saved-configs with “**delete flash:config.txt**”.

**Update Cisco IOS:**

* Doing this required us to get a new image. I then downloaded the latest IOS image.
* To transfer the IOS image to the device, we used a TFTP server. A TFTP server must be used on the local network with the image on it so that the software can get to our AP without internet.
* After downloading the TFTP server, we verified the image transfer with the command “**dir flash:”**
* Our source IP on our computer was set to 10.0.0.1 and the access point as 10.0.0.2
* We then had to convert our access point from lightweight mode (K9W8 firmware) to autonomous mode (K9W7 firmware) using the TFTP server.
  + The command to download K9W7 firmware was “**archive download-sw / overwrite /reload tftp://10.0.0.1/c1140-k9w7-tar.153-3.JD9.tar**”
  + To delete K9W8 firmware, we entered in the following 3 commands into our AP:
    - “**delete /force /recursive flash:c1140-k9w8-mx.153-3.JA4**”
    - “**delete /force /recursive flash:c1140-k9w8-mx.v153\_80mr\_esde**”
    - “**delete /force /recursive flash:c1140-rcvk9w8-mx**”
* Next, we rebooted our AP to load the new IOS image by entering in the “**reload**”
* We learned to use the command “**show version**” to confirm whether our access point had converted to autonomous mode K9W7 firmware.

**Switch configuration:**

* **VLANs:** We configured VLANS on the switch for network segmentation for our traffic. After creating VLANs, we assigned an IP address to them.
  + In privileged mode, enter “s4(config)#**interface vlan [*vlan number*]**”to enter a certain VLAN for configuration
  + Once you are in the VLAN interface mode, enter “s4(config-if)#**ip address [*ip address*] [*subnet mask*]**” to assign a IP address with a subnet mask on a VLAN interface
* **Trunking:** On our Power over Ethernet Switch, we had f0/4 connected to our access point and f0/6 connected into our router via a crossover cable. On these ports we configured trunks to enable the configuration of multiple VLANs.
  + Commands to configure a trunk on a switch interface: In switch interface range mode, enter “s4(config-if-range)#**switchport trunk encapsulation dot1q**”followed by “s4(config-if-range)#**switchport mode trunk**”
* **DHCP Pool Configuration:** The creation of DHCP (Dynamic Hose Configuration Protocol) pools allow the switch to automatically assign IP addresses to devices on the network. Users connecting to our configured network will dynamically be assigned an IP address, reducing the manual workload. DHCP was set up on our layer 3 switch for each VLAN for dynamic IP address distribution. Here are the following commands to configure DHCP pools:
  + Switch# config terminal
  + Switch(config)# ip dhcp pool [*name\_of\_pool*]
  + Switch(dhcp-config)#network [network\_address] [subnet mask]
  + Switch)dhcp-config)#dns-server 1.1.1
  + Switch(dhcp-config)#default-router [default-gateway]
  + Switch(dhcp-config)#domain-name [name]
* **Excluding DHCP Addresses:** DHCP addresses are excluded to prevent IP address conflicts. If a host connects to a network with static IP addresses and they overlap with the DHCP server’s address pool, the server may assign the same addresses to other hosts, leading to IP address conflicts. This command excludes DHCP addresses:
* Switch(config)# ip dhcp excluded-address [IP\_Address]

**Router Configuration:**

* **Cabling:** We first plugged the router into our power over ethernet switch and another interface into an internet connection. This was done so that we could configure our router with internet connectivity.
* **Creating an IP scheme:** We created an IP scheme of /27 subnet masks for the VLANs 1, 2, 3, and 4.

**A screenshot of a computer code

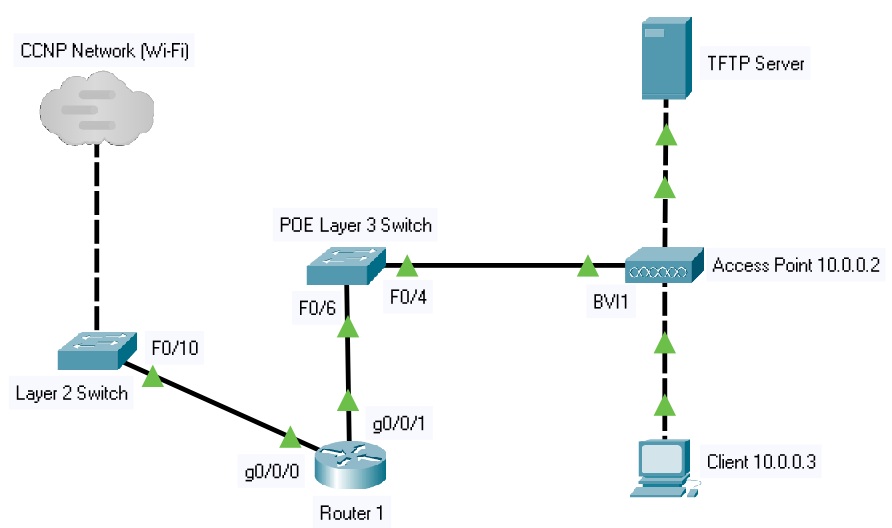
Description automatically generated**

* We then configured **access lists** to filter certain traffic. Our access list permitted all traffic in the 10.0.0.0 0.0.0.255 network which was essentially all our configured IP addresses.
* **NAT Configuration:** Nat configured on the router is important for internet connectivity because it conserves the limited number of publicly routable IPv4 addresses and hides the IP address behind a single public IP address for security reasons. Here are the following commands to configure NAT translation:
  + Router(config)# interface [inside-interface]
  + Router(config-if)# ip nat inside
  + **To define NAT pool:** Router(config)# ip nat inside source list [Pool\_name] [starting\_ip\_address\_of\_pool\_range] [ending\_ip\_add\_of\_pool\_range] netmask [NETMASK]
* To specify the source interface that the devise should use when sending TFTP packets, enter the command:
  + Switch(config)# ip tftp source-interface [*interface*]

**Graphical User Interface (GUI) Configurations:**

* To get onto the GUI, enter “**http://[BVI\_address]**” the bridge virtual interface address we previously set up into a web browser. We then entered in our assigned username and password to be granted access.
* We configured SSIDs through the access point’s GUI and assigned each with its associated VLAN for network segmentation.

**Network Diagram:**

****

**Configurations:**

**Access Point Running Configuration:**

ap#show run  
Building configuration...

Current configuration : 5480 bytes  
  
Last configuration change at 01:17:46 UTC Fri Mar 1 2002  
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 $1$fF8n$8qII9VPhiMUPciXV5sz0p1  
aaa new-model  
  
aaa group server radius rad\_eap  
server name 10.0.0.10  
  
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 10.0.0.10  
  
aaa authentication login webauth group radius  
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  
ip admission name webauth proxy http  
ip admission name webauth method-list authentication webauth  
  
dot11 pause-time 100  
dot11 syslog  
  
dot11 ssid CCNP\_P1\_7777\_SSID 1  
   vlan 2  
   band-select  
   authentication open  
   authentication key-management wpa version 2  
   mbssid guest-mode  
   wpa-psk ascii 7 1446405858517C7C7C71  
   information-element ssidl advertisement  
  
dot11 ssid CCNP\_P1\_7777\_SSID 2  
   vlan 3  
   band-select  
   authentication open  
   authentication key-management wpa version 2  
   mbssid guest-mode  
   wpa-psk ascii 7 00554155500E5D515778  
   information-element ssidl advertisement  
  
dot11 ssid CCNP\_P1\_7777\_SSID 3  
   vlan 4  
   band-select  
   authentication open eap eap\_methods3  
   authentication network-eap eap\_methods3  
   authentication key-management wpa version 2  
   mbssid guest-mode  
   information-element ssidl advertisement  
  
dot11 aaa authentication attributes service framed  
  
no ipv6 cef  
  
username Cisco privilege 15 password 7 09414F1B100B120018  
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 10 mode ciphers aes-ccm tkip  
  
encryption vlan 11 mode ciphers aes-ccm  
  
encryption vlan 12 mode ciphers aes-ccm tkip  
  
encryption vlan 2 mode ciphers aes-ccm tkip  
  
encryption vlan 3 mode ciphers aes-ccm  
  
encryption vlan 4 mode ciphers aes-ccm  
  
ssid CCNP\_P1\_7777\_SSID 1  
  
ssid CCNP\_P1\_7777\_SSID 2  
  
ssid CCNP\_P1\_7777\_SSID 3  
  
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 Dot11Radio1.121  
  
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 GigabitEthernet0.121  
  
interface BVI1  
mac-address 0007.7db6.1691  
ip address 10.0.0.2 255.255.255.0  
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 local  
  nas 10.0.0.2 key 7 047822352C0E  
  group TEST  
  
  user Cisco nthash 7 0529502A751F1B584057434753585D0979067C126C704621422258067A000A005F group TEST  
  user cisco nthash 7 09196D5149553143582D57090E7C7E1611704653462725027C0F00075F2641370B  
  
radius-server attribute 32 include-in-access-req format %h  
  
radius server 10.0.0.2  
address ipv4 10.0.0.2 auth-port 1812 acct-port 1813  
key 7 104D000A0618  
  
radius server 10.0.0.10  
address ipv4 10.0.0.10 auth-port 1812 acct-port 1813  
key 7 06120A325847071E544541  
  
bridge 1 route ip  
  
wlccp wds aaa authentication attributes service framed  
  
line con 0  
line vty 0 4  
transport input all  
  
end

**Trunk Switch Running Configuration:**

S4#show run

Building configuration...

Current configuration : 2329 bytes

version 12.2

no service pad

service timestamps debug uptime

service timestamps log uptime

no service password-encryption

hostname S4

no aaa new-model

vtp domain CCNP

vtp mode transparent

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 vlan1

network 10.0.0.32 255.255.255.224

dns-server 1.1.1.1

default-router 10.0.0.33

domain-name josh

ip dhcp pool vlan3

network 10.0.0.64 255.255.2.224

dns-server 1.1.1.1

default-router 10.0.0.65

domain-name ethan

ip dhcp pool vlan4

network 10.0.0.159 255.255.255.224

dns-server 1.1.1.1

default-router 10.0.0.160

domain-name ethanos

no file verify auto

spanning-tree mode pvst

spanning-tree extend system-id

vlan internal allocation policy ascending

vlan 2

name data

vlan 3

name voice

vlan 4

name management

vlan 5

name Phoneline

vlan 10

name Business

vlan 11

name Table

vlan 20

name Data

vlan 30

name Extra

vlan 40

name Misc

vlan 50

name NATIVE

vlan 99

name MANAGEMENT

vlan 100

name Voice

vlan 400,707

vlan 996

name CUSTOMER\_NATIVE

vlan 999

interface FastEthernet0/1

interface FastEthernet0/2

interface FastEthernet0/3

interface FastEthernet0/4

switchport trunk encapsulation dot1q

switchport mode trunk

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

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 10.0.0.4 255.255.255.224

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 10.0.0.160 255.255.255.224

ip default-gateway 10.0.0.3

ip classless

ip route 0.0.0.0 0.0.0.0 10.0.0.3

ip http server

control-plane

line con 0

line vty 5 15

end

**NAT (Network Address Translation) Router Running Configuration:**

Router#show run

Building configuration...

Current configuration : 1610 bytes

Last configuration change at 18:05:53 UTC Tue Apr 23 2024

version 16.9

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

no ip domain lookup

login on-success log

subscriber templating

vtp domain cisco

vtp mode transparent

multilink bundle-name authenticated

license udi pid ISR4321/K9 sn FDO21482HZX

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 10.0.0.3 255.255.255.0

ip nat inside

negotiation auto

interface Serial0/1/0

no ip address

shutdown

interface Serial0/1/1

no ip address

shutdown

interface GigabitEthernet0

vrf forwarding Mgmt-intf

no ip address

shutdown

negotiation auto

ip forward-protocol nd

no ip http server

no ip http secure-server

ip tftp source-interface GigabitEthernet0

ip nat pool jdub 192.168.40.3 192.168.41.254 netmask 255.255.254.0

ip nat inside source list 10 pool jdub

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

end

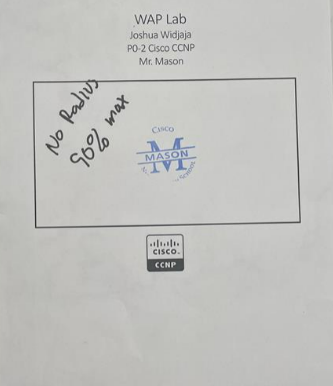
**Problems:**

One of our biggest problems that held us back was attempting to access the GUI. At first, for the computer’s source IP, I set the computer’s IP address identical to the access point’s IP address in the control panel. I was unable to access the GUI from my computer with these configurations because the access point and the computer were connected to each other and putting down the BVI1 address on the web browser would not take us to the GUI due to an overlap of IP addresses. Also, we initially chose google chrome as the search engine to access the GUI, but this would come to bite us later. After we had everything set up correctly, accessing the GUI would work some days and wasn’t able work other days. We thought that possibly our configurations were wrong and ended up changing a few unnecessary things which cost us time. We switched to using internet explorer instead of google chrome after asking a group for advice on how to deal with our problem and we ended up getting into the GUI consistently. Our next problem was that the SSIDs that we had configured weren’t showing up on the listed networks. After troubleshooting for errors on our device configurations we decided to troubleshoot on the layer 1 level. We found that our router didn’t even have an ethernet cable plugged into a layer 2 switch connected to the CCNP network. After cabling from an outside interface of the router to the layer 2 switch connected to the internet, we were able to find our SSIDs up on the listed Wi-Fi networks and was able to have internet access to them. We also made simple mathematical mistakes when finding our IP address ranges but ended up fixing those mistakes swiftly. Lastly, it was very difficult for us to find information and understand the configuration of the radius server and unfortunately ran out of time in configuring it.

**Conclusion:**

In conclusion, this lab was without a doubt in our opinion the hardest lab given to us, but that came with the most lessons and learning from it. We were given many new concepts to learn such as the configuration of SSIDs on the GUI, Radius Server, Access Point, and the implementation of a TFTP server. The familiar concepts such as VLAN setup, NAT configuration, IP scheme setup, and access lists were fairly easy to configure and served as a testament to how much we have learned. The main lesson we can take away from this lab in particular is to never underestimate a lab and to always try to get it done early because you can be hit with many different problems which can cause delays.

**Teacher Signoff Page of Lab Completed:**

****