Cisco AP Lab

Name: Jacob Chen

Date: 6/7/2024

Lab Partner: Aaron Yu, Aiden Yin

Class: CCNP 2023-2024



**Purpose**

Ethernet connections while fast and stable are often inconvenient. Especially in networks where the number of users at any given time can change, Ethernet connections are outdated. This lab pushes us to start exploring the functionality of wireless access points, the various ways they can be configured and ultimately how to use them to connect users to the internet.

**Background**

This lab involved setting up all components of a wireless network. The main components that we had to set up were the Access Point, Vlans, Nat Translations and the Radius Server. Each component accomplishes a specific purpose on its own, but as a group, they help to create a wifi network that is properly managed.

The first key concept was the access point themselves. Wireless access points are the cornerstone of any wireless network. They are the devices that make devices wireless. In other words, they are the actual devices that transmit the signals that your phone or computer can talk to. They broadcast a unique “name” (also known as an SSID) that can be discovered by nearby devices. These devices then have the option to connect to the network via a variety of authentication options. It’s useful to think of them as street signs. When someone passes by the road, if they don’t see a street sign, they may not know that there is a house here. Similarly, SSIDs allow people to realize your network exists and connect to it.

The next concept covered is Vlans. Vlans stand for virtual local access network. While that’s probably a mouthful, it’s a key concept in network security. Vlans allow for sections of network traffic to be virtually separated from each other. This is especially useful when you don’t want certain types of traffic to talk. For example, lets pretend like you have an admin channel which is used to remotely manage devices and another channel for general traffic. If malicious actors could see traffic from the admin channel, that could open up new potential attack vectors. Vlans provide a solution to this problem by allowing us to create logical separations that segment traffic into different virtual channels. In our road analogy, Vlans can be thought of us private roads. A Vlan will divide a roadway into various private roads such that traffic along the roads is separated.

The third concept covered are nat translations. Originally used to help conserve IP addresses, Nat translations are used in our network to separate our device from the greater internet. It provides greater flexibility when we’re designing and configuring our own network. Nat translations are a bit more confusing to get, but they provide the important benefit of being able to “translate” your addresses. Imagine if in your neighborhood, you had your own numbering system. The houses were numbered 1-5. If someone has a letter for a house in the neighborhood, the mail carrier would have no clue where the house “1” is. Instead, it has a public address, one that can be reached by everyone else. That pubic address is then mapped and translated over to the numberings 1-5 right before the mail enters the neighborhood.

The last concept is our radius server. Radius is a technology that allows us to determine who we let into out network. For example, we can store a username and password. When someone tries to join our network, they must know the exact username and password or else they won’t be able to join. This helps provide better network security and ensure that only authorized users are on the network.

**Lab Summary**

First, we created a general topology for the entire setup including the router itself, a layer3 switch which handled inter vlan routing and a router that is in charge of NAT and a Linux machine that was running our radius server.

After wiring up the diagram, we preformed the following rough steps.

1. Set up basic device configurations on the router switch and access point.
2. Configured 3 Mbssids on the access point with 2 set to guest mode and open authentication.
3. Activated sub interfaces on the 2.4 and 5 Ghz interfaces of the access points.
4. Added Vlans on the sub interfaces.
5. Configured the router with Nat so that the inner IP addresses are translated over to the outside network.
6. Configured inter Vlan routing in the router
7. Configured a Linux machine with free radius and attached it to the network so the access point can authenticate using the radius server.

**Lab Commands**

**Hostname RX**: Sets a unique hostname to identify the various routers

**Interface g0/0/X**: Access the interfaces

**No shut**: Turns on the interfaces

**Ip add 192.168.x.x 255.255.255.0**: sets an ipv4 address on an interface

**Dot11 ssid XXX:** Turns on and allows configuration of a specific SSID.

**Authentication open:** Allows anyone to request to join the network without authentication credentials.

**Mbssid guest-mode:** Allows the SSID to be in guest mode along with other SSIDs.

**Vlan X:** Either creates a Vlan or assigns an interface to a certain Vlan.

**Interface Dot11Radio0:** Accesses the 2.4 GHZ radio interface for further configuration.

**Interface Dot11Radio1:** Accesses the 5.0 GHZ radio interface for further configuration.

**Ssid XXX:** Has a certain radio interface broadcast a previously defined SSID.

**Mbssid:** Enables multiple basic SSIDs on an interface.

**Interface Dot11Radio1.X:** Accesses a sub interface of the SSID for further configuration

**Encapsulation dot1Q X:** Assigns a sub interface to a Vlan.

**Encapsulation dot1Q X native:** Assigns a sub interface to the native Vlan X.

**Interface BVI1:** Configures the virtual interface of the access point which if used to test connectivity.

**Ip default-gateway x.x.x.x:** Sets a default gateway on the device. (Aka a default route)

**Radius server X:** Enables and allows for configuration of a radius server.

**Address ipv4 x.x.x.x auth-port X acct-port x:** Tells the access point to talk to the radius server on certain port with a certain IP address.

**Switchport trunk encapsulation dot1q:** makes a certain switch interface a trunk interface.

**Switchport trunk native vlan X:** configures a native vlan on an interface.

**Switchport trunk allowed vlan X:** Allows certain vlans on the interface.

**Ip dhcp excluded-address x.x.x.x:** Excludes a specified IP address from being handed out during DHCP assignment.

**Ip dhcp pool X:** Creates a DHCP pool with a particular name.

**Network x.x.x.x 255.255.255.0:** Specifies a certain network to be used in the DHCP pool. The router will give IP addresses out of this network.

**Dns-server:** Along with an IP address, this gives each DHCP client a default DNS-server.

**Default-router:** Configures a default router that each DHCP configuration will have the client point to.

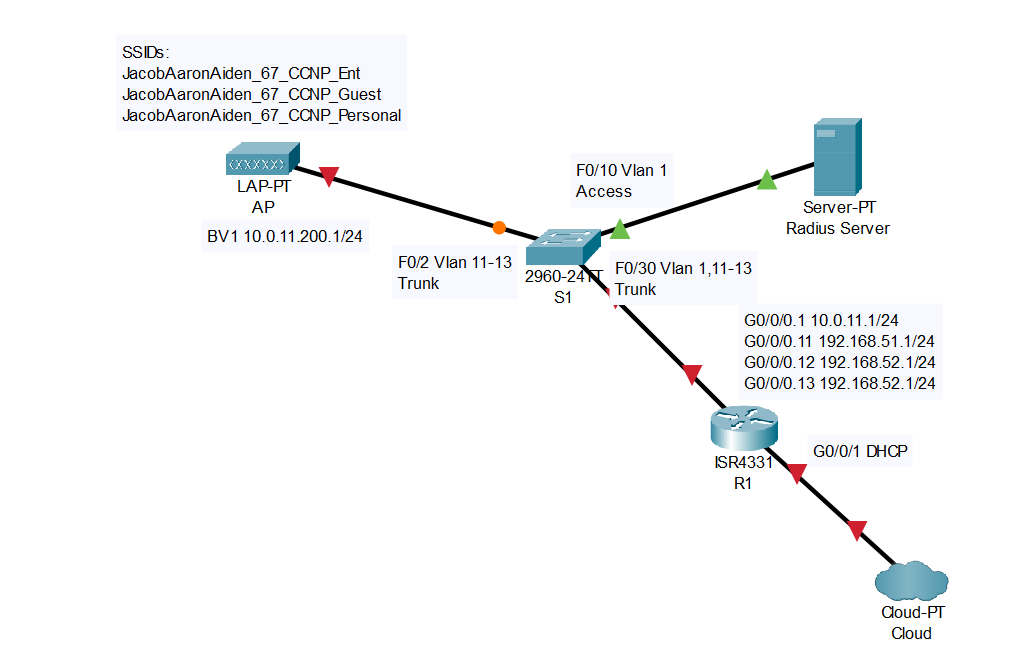
**Ip nat inside:** Configures a certain interface of the router as the inside interface such that incoming IP addresses will be translated.

**Ip nat outside:** configures an outside interface such that incoming traffic can be Nat-ed back into it’s original IP address.

**Access-list 1 permit x.x.x.x 0.0.0.255:** Creates an access list that permits certain addresses

**Ip nat inside source list X interface GX/X/X:** Assigns an access list to an interface such that only IPs permitted by the access list can be translated.

**Network Diagram**



**Configuration:**

**AP:**

hostname AP

aaa group server radius AP\_RAD\_GROUP

server name Jacob\_PC

dot11 ssid JacobAaronAiden\_67\_CCNP\_Ent

vlan 13

authentication open eap eap\_methods

authentication network-eap eap\_methods

authentication key-management wpa version 2

mbssid guest-mode

dot11 ssid JacobAaronAiden\_67\_CCNP\_Guest

vlan 11

authentication open

mbssid guest-mode

dot11 ssid JacobAaronAiden\_67\_CCNP\_Personal

vlan 12

authentication open

authentication key-management wpa version 2

mbssid guest-mode

wpa-psk ascii 7 106D000A061843595F

interface Dot11Radio0

no ip address

shutdown

!

interface Dot11Radio1

no ip address

encryption vlan 12 mode ciphers aes-ccm

encryption vlan 13 mode ciphers aes-ccm

ssid JacobAaronAiden\_67\_CCNP\_Ent

ssid JacobAaronAiden\_67\_CCNP\_Guest

ssid JacobAaronAiden\_67\_CCNP\_Personal

no shut

!

interface Dot11Radio1.1

encapsulation dot1Q 1 native

bridge-group 1

!

interface Dot11Radio1.11

encapsulation dot1Q 11

bridge-group 11

!

interface Dot11Radio1.12

encapsulation dot1Q 12

bridge-group 12

!

interface Dot11Radio1.13

encapsulation dot1Q 13

bridge-group 13

!

interface GigabitEthernet0

no ip address

!

interface GigabitEthernet0.1

encapsulation dot1Q 1 native

bridge-group 1

!

interface GigabitEthernet0.11

encapsulation dot1Q 11

bridge-group 11

!

interface GigabitEthernet0.12

encapsulation dot1Q 12

bridge-group 12

!

interface GigabitEthernet0.13

encapsulation dot1Q 13

bridge-group 13

!

interface BVI1

mac-address 44d3.ca03.7d2c

ip address 10.0.11.200 255.255.255.0

ipv6 address dhcp

ipv6 address autoconfig

ipv6 enable

!

ip default-gateway 10.0.11.1

radius server Jacob\_PC

address ipv4 10.0.11.100 auth-port 1812 acct-port 1813

timeout 10

retransmit 3

key 7 111D1C16031B050B557878

bridge 1 route ip

wlccp ap eap profile AUTH\_METHODS

**Switch:**

hostname S1

Vlan 11

Vlan 12

Vlan 13

interface FastEthernet0/2

switchport trunk encapsulation dot1q

switchport trunk native vlan 1

switchport trunk allowed vlan 1,11-13

switchport mode trunk

!

interface FastEthernet0/10

switchport access vlan 1

switchport mode access

!

interface FastEthernet 0/30

switchport trunk encapsulation dot1q

switchport trunk allowed vlan 1,11-13

switchport mode trunk

**Router:**

ip dhcp excluded-address 192.168.51.1

ip dhcp excluded-address 192.168.52.1

ip dhcp excluded-address 192.168.53.1

ip dhcp pool Guest

network 192.168.51.0 255.255.255.0

dns-server 1.1.1.1

default-router 192.168.51.1

ip dhcp pool Psk

network 192.168.52.0 255.255.255.0

dns-server 1.1.1.1

default-router 192.168.52.1

ip dhcp pool Enterprise

network 192.168.53.0 255.255.255.0

dns-server 1.1.1.1

default-router 192.168.53.1

interface GigabitEthernet0/0/0

no ip address

ip nat inside

interface GigabitEthernet0/0/0.1

encapsulation dot1Q 1

ip address 10.0.11.1 255.255.255.0

interface GigabitEthernet0/0/0.11

encapsulation dot1Q 11

ip address 192.168.51.1 255.255.255.0

ip nat inside

!

interface GigabitEthernet0/0/0.12

encapsulation dot1Q 12

ip address 192.168.52.1 255.255.255.0

ip nat inside

!

interface GigabitEthernet0/0/0.13

encapsulation dot1Q 13

ip address 192.168.53.1 255.255.255.0

ip nat inside

!

interface GigabitEthernet0/0/1

ip address dhcp

ip nat outside

negotiation auto

ip nat inside source list 1 interface GigabitEthernet0/0/1 overload

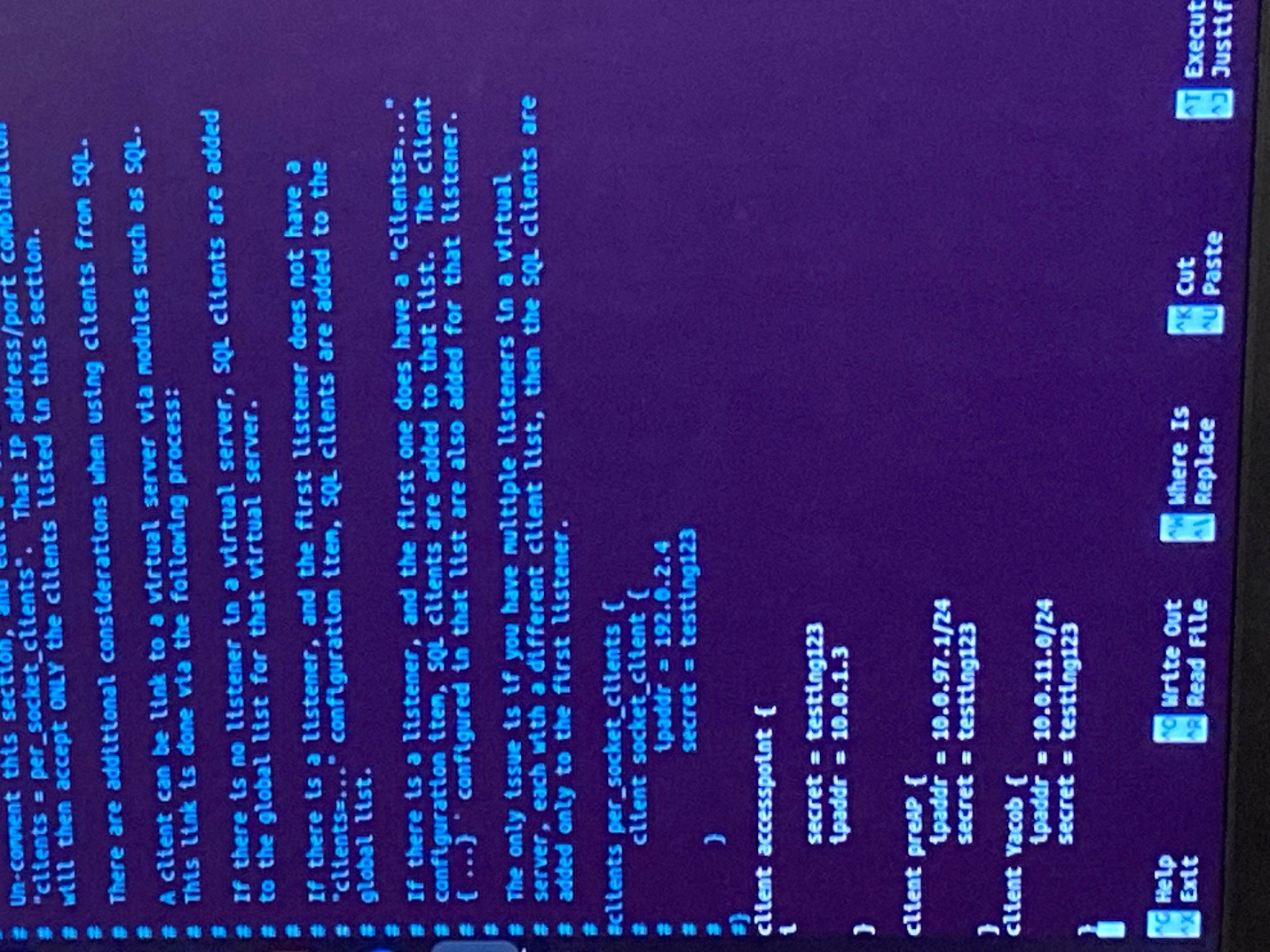
access-list 1 permit 192.168.51.0 0.0.0.255

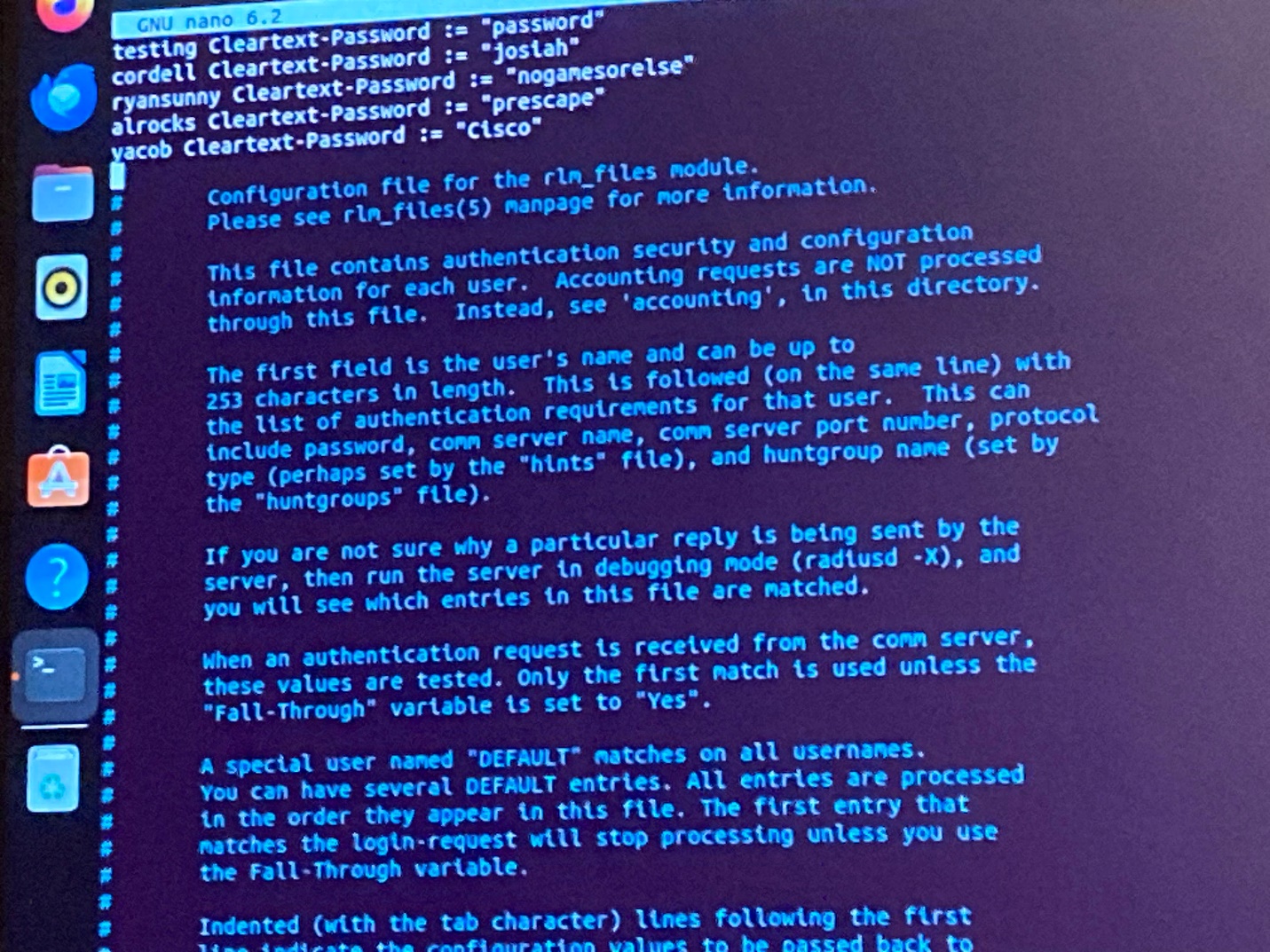
access-list 1 permit 192.168.52.0 0.0.0.255

access-list 1 permit 192.168.53.0 0.0.0.255

**Configuring Radius Server:**

**Adding the Server**



**Adding the Users**

**Show Run**

**AP**

Current configuration : 4029 bytes

!

! Last configuration change at 04:58:51 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 $1$ySJC$WKGeN6ausDAtFkMop0BIE1

!

aaa new-model

!

aaa group server radius AP\_RAD\_GROUP

server name Jacob\_PC

!

aaa authentication login eap\_methods group AP\_RAD\_GROUP

!

aaa session-id common

no ip source-route

no ip cef

no ip domain lookup

!

dot11 pause-time 100

dot11 syslog

!

dot11 ssid JacobAaronAiden\_67\_CCNP\_Ent

vlan 13

authentication open eap eap\_methods

authentication network-eap eap\_methods

authentication key-management wpa version 2

mbssid guest-mode

!

dot11 ssid JacobAaronAiden\_67\_CCNP\_Guest

vlan 11

authentication open

mbssid guest-mode

!

dot11 ssid JacobAaronAiden\_67\_CCNP\_Personal

vlan 12

authentication open

authentication key-management wpa version 2

mbssid guest-mode

wpa-psk ascii 7 106D000A061843595F

!

!

!

eap profile AUTH\_METHODS

method mschapv2

!

no ipv6 cef

!

username Cisco password 7 01300F175804

!

bridge irb

interface Dot11Radio0

no ip address

shutdown

antenna gain 0

station-role root

bridge-group 1

bridge-group 1 subscriber-loop-control

bridge-group 1 spanning-disabled

bridge-group 1 block-unknown-source

no bridge-group 1 source-learning

no bridge-group 1 unicast-flooding

!

interface Dot11Radio1

no ip address

!

encryption vlan 12 mode ciphers aes-ccm

!

encryption vlan 13 mode ciphers aes-ccm

!

ssid JacobAaronAiden\_67\_CCNP\_Ent

!

ssid JacobAaronAiden\_67\_CCNP\_Guest

!

ssid JacobAaronAiden\_67\_CCNP\_Personal

!

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 Dot11Radio1.11

encapsulation dot1Q 11

bridge-group 11

bridge-group 11 subscriber-loop-control

bridge-group 11 spanning-disabled

bridge-group 11 block-unknown-source

no bridge-group 11 source-learning

no bridge-group 11 unicast-flooding

!

interface Dot11Radio1.12

encapsulation dot1Q 12

bridge-group 12

bridge-group 12 subscriber-loop-control

bridge-group 12 spanning-disabled

bridge-group 12 block-unknown-source

no bridge-group 12 source-learning

no bridge-group 12 unicast-flooding

!

interface Dot11Radio1.13

encapsulation dot1Q 13

bridge-group 13

bridge-group 13 subscriber-loop-control

bridge-group 13 spanning-disabled

bridge-group 13 block-unknown-source

no bridge-group 13 source-learning

no bridge-group 13 unicast-flooding

!

interface GigabitEthernet0

no ip address

duplex auto

speed auto

dot1x pae authenticator

!

interface GigabitEthernet0.1

encapsulation dot1Q 1 native

bridge-group 1

bridge-group 1 spanning-disabled

no bridge-group 1 source-learning

!

interface GigabitEthernet0.11

encapsulation dot1Q 11

bridge-group 11

bridge-group 11 spanning-disabled

no bridge-group 11 source-learning

!

interface GigabitEthernet0.12

encapsulation dot1Q 12

bridge-group 12

bridge-group 12 spanning-disabled

no bridge-group 12 source-learning

!

interface GigabitEthernet0.13

encapsulation dot1Q 13

bridge-group 13

bridge-group 13 spanning-disabled

no bridge-group 13 source-learning

!

interface BVI1

mac-address 44d3.ca03.7d9b

ip address 10.0.11.200 255.255.255.0

ipv6 address dhcp

ipv6 address autoconfig

ipv6 enable

!

ip forward-protocol nd

ip http server

no ip http secure-server

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

radius server Jacob\_PC

address ipv4 10.0.11.100 auth-port 1812 acct-port 1813

timeout 10

retransmit 3

key 7 111D1C16031B050B557878

!

bridge 1 route ip

!

wlccp ap eap profile AUTH\_METHODS

!

line con 0

logging synchronous

line vty 0 4

transport input all

!

end

**Router**

Current configuration : 2406 bytes

!

! Last configuration change at 21:10:12 UTC Thu Jun 6 2024

!

version 15.5

service timestamps debug datetime msec

service timestamps log datetime msec

no platform punt-keepalive disable-kernel-core

!

hostname R1

!

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

!

ip dhcp excluded-address 192.168.51.1

ip dhcp excluded-address 192.168.52.1

ip dhcp excluded-address 192.168.53.1

!

ip dhcp pool Guest

network 192.168.51.0 255.255.255.0

dns-server 1.1.1.1

default-router 192.168.51.1

!

ip dhcp pool Psk

network 192.168.52.0 255.255.255.0

dns-server 1.1.1.1

default-router 192.168.52.1

!

ip dhcp pool Enterprise

network 192.168.53.0 255.255.255.0

dns-server 1.1.1.1

default-router 192.168.53.1

!

subscriber templating

multilink bundle-name authenticated

!

license udi pid ISR4321/K9 sn FDO211216BL

license accept end user agreement

!

spanning-tree extend system-id

!

redundancy

mode none

!

vlan internal allocation policy ascending

!

interface GigabitEthernet0/0/0

no ip address

ip nat inside

negotiation auto

!

interface GigabitEthernet0/0/0.1

encapsulation dot1Q 1 native

ip address 10.0.11.1 255.255.255.0

!

interface GigabitEthernet0/0/0.11

encapsulation dot1Q 11

ip address 192.168.51.1 255.255.255.0

ip nat inside

!

interface GigabitEthernet0/0/0.12

encapsulation dot1Q 12

ip address 192.168.52.1 255.255.255.0

ip nat inside

!

interface GigabitEthernet0/0/0.13

encapsulation dot1Q 13

ip address 192.168.53.1 255.255.255.0

ip nat inside

interface GigabitEthernet0/0/1

ip address dhcp

ip nat outside

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

!

interface Vlan1

no ip address

!

ip nat inside source list 1 interface GigabitEthernet0/0/1 overload

ip forward-protocol nd

no ip http server

no ip http secure-server

ip tftp source-interface GigabitEthernet0

access-list 1 permit 192.168.51.0 0.0.0.255

access-list 1 permit 192.168.52.0 0.0.0.255

access-list 1 permit 192.168.53.0 0.0.0.255

!

control-plane

!

!

line con 0

stopbits 1

line aux 0

stopbits 1

line vty 0 4

login

!

ntp server pool.ntp.org

!

end

**Switch**

Current configuration : 2381 bytes

!

version 12.2

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname S1

!

boot-start-marker

boot-end-marker

!

no aaa new-model

system mtu routing 1500

authentication mac-move permit

ip subnet-zero

!

spanning-tree mode pvst

spanning-tree etherchannel guard misconfig

spanning-tree extend system-id

!

vlan internal allocation policy ascending

!

!

!

!

interface FastEthernet0/1

shutdown

!

interface FastEthernet0/2

switchport trunk encapsulation dot1q

switchport trunk allowed vlan 1,11-13

switchport mode trunk

!

interface FastEthernet0/3

!

interface FastEthernet0/4

!

interface FastEthernet0/5

!

interface FastEthernet0/6

!

interface FastEthernet0/7

!

interface FastEthernet0/8

!

interface FastEthernet0/9

!

interface FastEthernet0/10

switchport mode access

!

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 FastEthernet0/25

!

interface FastEthernet0/26

!

interface FastEthernet0/27

!

interface FastEthernet0/28

!

interface FastEthernet0/29

!

interface FastEthernet0/30

switchport trunk encapsulation dot1q

switchport trunk allowed vlan 1,11-13

switchport mode trunk

!

interface FastEthernet0/31

!

interface FastEthernet0/32

!

interface FastEthernet0/33

!

interface FastEthernet0/34

!

interface FastEthernet0/35

!

interface FastEthernet0/36

!

interface FastEthernet0/37

!

interface FastEthernet0/38

!

interface FastEthernet0/39

!

interface FastEthernet0/40

!

interface FastEthernet0/41

!

interface FastEthernet0/42

!

interface FastEthernet0/43

!

interface FastEthernet0/44

!

interface FastEthernet0/45

!

interface FastEthernet0/46

!

interface FastEthernet0/47

!

interface FastEthernet0/48

!

interface GigabitEthernet0/1

!

interface GigabitEthernet0/2

!

interface GigabitEthernet0/3

!

interface GigabitEthernet0/4

!

interface Vlan1

no ip address

shutdown

!

ip classless

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

**Show Dot11 Bssid**

Interface BSSID Guest SSID

Dot11Radio1 64d9.89bd.f050 Yes JacobAaronAiden\_67\_CCNP\_Ent

Dot11Radio1 64d9.89bd.f051 Yes JacobAaronAiden\_67\_CCNP\_Guest

Dot11Radio1 64d9.89bd.f052 Yes JacobAaronAiden\_67\_CCNP\_Personal

**Show IP DHCP Bindings**

Bindings from all pools not associated with VRF:

IP address Client-ID/ Lease expiration Type State Interface

Hardware address/

User name

192.168.51.3 0114.abc5.36cc.2a Jun 07 2024 09:39 PM Automatic Active GigabitEthernet0/0/0.11

192.168.52.2 01ac.ed5c.3e56.89 Jun 07 2024 09:08 PM Automatic Active GigabitEthernet0/0/0.12

192.168.52.3 0114.abc5.36cc.2a Jun 07 2024 09:40 PM Automatic Active GigabitEthernet0/0/0.12

192.168.53.2 01ac.ed5c.3e56.89 Jun 07 2024 05:52 PM Automatic Active GigabitEthernet0/0/0.13

**Show IP Nat Translations**

Pro Inside global Inside local Outside local Outside global

tcp 192.168.40.236:4603 192.168.53.2:59045 104.16.80.230:443 104.16.80.230:443

tcp 192.168.40.236:4691 192.168.52.2:64828 44.198.23.94:443 44.198.23.94:443

tcp 192.168.40.236:4614 192.168.51.2:52875 104.16.80.230:443 104.16.80.230:443

tcp 192.168.40.236:4613 192.168.51.2:52868 104.16.80.230:443 104.16.80.230:443

tcp 192.168.40.236:4619 192.168.52.2:64709 20.25.227.174:443 20.25.227.174:443

tcp 192.168.40.236:4675 192.168.52.2:64776 52.73.235.185:443 52.73.235.185:443

tcp 192.168.40.236:4604 192.168.51.2:56532 184.28.50.162:443 184.28.50.162:443

tcp 192.168.40.236:4696 192.168.52.2:64842 34.199.53.216:443 34.199.53.216:443

tcp 192.168.40.236:4605 192.168.51.2:56534 35.186.224.39:443 35.186.224.39:443

tcp 192.168.40.236:4608 192.168.53.2:53519 104.17.143.163:443 104.17.143.163:443

tcp 192.168.40.236:4580 192.168.51.2:52838 104.16.80.230:443 104.16.80.230:443

**Show IP Route**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, \* - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP

a - application route

+ - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 192.168.40.1 to network 0.0.0.0

S\* 0.0.0.0/0 [254/0] via 192.168.40.1

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

C 10.0.11.0/24 is directly connected, GigabitEthernet0/0/0.1

L 10.0.11.1/32 is directly connected, GigabitEthernet0/0/0.1

C 192.168.40.0/23 is directly connected, GigabitEthernet0/0/1

192.168.40.0/32 is subnetted, 1 subnets

L 192.168.40.236 is directly connected, GigabitEthernet0/0/1

192.168.51.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.51.0/24 is directly connected, GigabitEthernet0/0/0.11

L 192.168.51.1/32 is directly connected, GigabitEthernet0/0/0.11

192.168.52.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.52.0/24 is directly connected, GigabitEthernet0/0/0.12

L 192.168.52.1/32 is directly connected, GigabitEthernet0/0/0.12

192.168.53.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.53.0/24 is directly connected, GigabitEthernet0/0/0.13

L 192.168.53.1/32 is directly connected, GigabitEthernet0/0/0.13

**Show Vlans**

Virtual LAN ID: 1 (IEEE 802.1Q Encapsulation)

vLAN Trunk Interfaces: Dot11Radio1.1

GigabitEthernet0.1

This is configured as native Vlan for the following interface(s) :

Dot11Radio1

GigabitEthernet0

Protocols Configured: Address: Received: Transmitted:

Dot11Radio1.1 (1)

Bridging Bridge Group 1 0 58

Other 0 12

0 packets, 0 bytes input

40 packets, 9081 bytes output

GigabitEthernet0.1 (1)

Bridging Bridge Group 1 0 58

Other 0 12

0 packets, 0 bytes input

30 packets, 6116 bytes output

Virtual LAN ID: 11 (IEEE 802.1Q Encapsulation)

vLAN Trunk Interfaces: Dot11Radio1.11

GigabitEthernet0.11

Protocols Configured: Address: Received: Transmitted:

Dot11Radio1.11 (11)

Bridging Bridge Group 11 0 0

0 packets, 0 bytes input

0 packets, 0 bytes output

GigabitEthernet0.11 (11)

Bridging Bridge Group 11 0 0

0 packets, 0 bytes input

0 packets, 0 bytes output

Virtual LAN ID: 12 (IEEE 802.1Q Encapsulation)

vLAN Trunk Interfaces: Dot11Radio1.12

GigabitEthernet0.12

Protocols Configured: Address: Received: Transmitted:

Dot11Radio1.12 (12)

Bridging Bridge Group 12 0 0

0 packets, 0 bytes input

0 packets, 0 bytes output

GigabitEthernet0.12 (12)

Bridging Bridge Group 12 0 0

0 packets, 0 bytes input

0 packets, 0 bytes output

Virtual LAN ID: 13 (IEEE 802.1Q Encapsulation)

vLAN Trunk Interfaces: Dot11Radio1.13

GigabitEthernet0.13

Protocols Configured: Address: Received: Transmitted:

Dot11Radio1.13 (13)

Bridging Bridge Group 13 0 0

0 packets, 0 bytes input

0 packets, 0 bytes output

GigabitEthernet0.13 (13)

Bridging Bridge Group 13 0 0

0 packets, 0 bytes input

0 packets, 0 bytes output

**Problems**

This lab had the most problems for any other lab that we’ve done, but through the debugging process we were able to solve and learn from them.

The first problem that we faced was with the SSIDs. Only one SSID can be broadcast with guest mode, so we had to use MBSSIDs which stands for multiple basic ssids. The configuration of MBSSIDs is a bit more confusing and takes a bit longer. We had to configure Vlans and use inter-vlan routing. Each open SSID should be on its own Vlan and talked to each other through a router on a stick topology.

We also had trouble getting the SSIDs to broadcast. The way we solved this was first turning on the SSID and configuring it, turning on the specific radio interface that we wanted to use and finally adding the SSID into that interface. Making sure to do all 3 steps helped us make sure the SSIDs were being broadcast properly.

The next issue was with the Radius server. FreeRadius is a Linux application and requires a Linux style OS to install. I originally used WSL running Ubuntu to try to get it to work. Unfortunately, WSL blocks UDP ports. As such when we would get DNS queries, they would get blocked. The next idea that we had was to use Docker. FreeRadius has a maintained docker image on dockerhub. But when we pulled the image and set it up, it wouldn’t process requests. I even tried using virtual box to install a virtual machine and running an Ubuntu image on that but for some reason virtual box kept erroring out. Finally we just decided to use a separate drive with Ubuntu on it.

Layer 3 routing on the Layer3 switch was also giving us some trouble. In the end, we decide to have the router handle the different Vlan traffic through a router on a stick, rather than try to use the switch for that.

**Conclusion**

This probably comes up a lot, but this Lab was probably the most difficult lab of the year. It required a lot of skills that’d previously become rusty (Vlans, Nat, DHCP) so in many ways it was a good review. Other than that, I think it was a really good lab. Making sure we could connect to the internet was a good example of how we could create a real network. We had to go from scratch researching how the AP actually works and build a network that would successfully connect to the internet. If I end up going into network engineering, the stuff I did in the lab was very similar to something I could imagine myself doing in my future line of work.

