Cover Image Attribution: Ram Venu

Advanced Cisco Networking Academy – Configuring a Cisco Wireless Access Point and WLC with WPA2-PSK and WPA2-Enterprise with a RADIUS Server

Colin J. Faletto, CCNA

Networking Academy

Purpose

This lab is intended to reintroduce the concept of managing wireless connectivity with a WLAN Controller, a concept we visited briefly in CCNA but haven't learned about since. This lab is also meant to introduce RADIUS and the process of setting it up as an external server, which indirectly teaches basic Linux skills such as navigating the terminal. This lab also revisits aspects from the CCNA course such as subinterfaces/VLANs and virtualization.

Background

Aironet is a division of Cisco that develops wireless access points. It was founded in 1986 as an independent company and acquired by Cisco 13 years later. The Cisco Aironet 1040 series was a series of access points developed by Cisco in the early 2010s, which was discontinued in 2013 and dropped from supoport in 2018. As of 2025, the Aironet line appears to be inactive or discontinued, replaced fully by the Catalyst and Meraki lines of wireless products.

Wi-Fi Protected Access, or WPA, is a security standard developed and maintained by the Wi-Fi alliance. There are three versions of WPA, being named WPA, WPA2, and WPA3 respectively. The first generation of WPA was released in 2003, with the second version releasing just a year later in 2004. In 2018, the third generation was released. WPA uses TKIP (Temporal Key Integrity Protocol) as its encryption method, while WPA2 uses CCMP (Counter-Mode/CBC-Mac Protocol) for encryption. WPA3 keeps support for CCMP but introduces GCMP (Galois/Counter Mode Protocol) as a stronger encryption method as well.

WPA can use two different methods of authentication: Personal and Enterprise. Personal authentication uses a pre-shared 256 bit key, meaning that all devices authenticate using the same password. Enterprise authentication uses a RADIUS (Remote Authentication Dial-In User Service) server, meaning that each user authenticates using their own username and password.

Ubuntu is a distribution of Linux developed by Canonical. It is built on the older Debian distribution, including well-known features from that distrubution such as the package manager Advanced Package Tool (APT). It is the most popular Linux distribution by far, with a multitude of spin-off distributions. By default, Ubuntu uses the GNOME desktop environment, which is designed with accessibility and readability in mind.

Lubuntu is a Linux distribution built on Ubuntu known for being lightweight, both in terms of CPU/Memory utilization and storage usage. Lubuntu uses the LXQt desktop environment, which is a lightweight desktop environment that still provides all the tools necessary for basic productivity and development.

Lab Summary

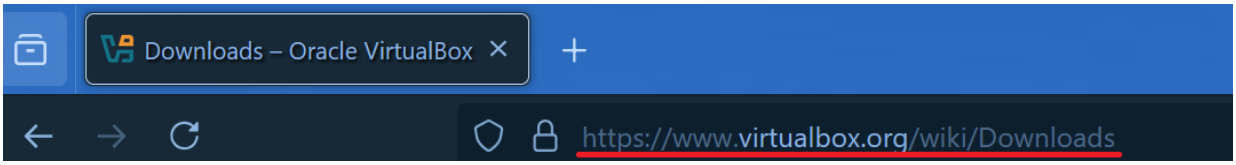
In this lab, we configured a Cisco 2504 WLAN Controller and Cisco Aironet AIR-LAP1042N Access Point with three WLANs – one configured with no security (CrunchwrapSupreme), one with WPA2-PSK (NachosBellGrande), and one with WPA2-Enterprise (CheesyGorditaCrunch). Each of these WLANs is connected to its own

VLAN, with a central router giving out addresses for each VLAN via DHCP. The central router is also connected to a management VLAN where the AP, WLAN Controller, and management PC reside.

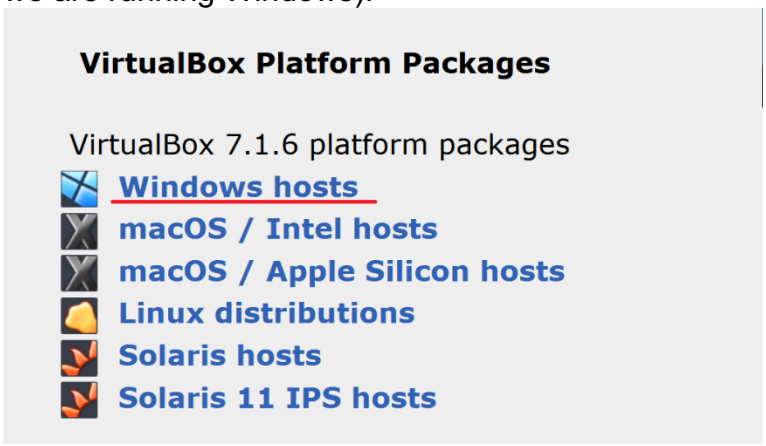
The management PC is also running a virtualized instance of Lubuntu through Virtualbox. Lubuntu is a Linux distribution we chose for its lightweight nature and similarity to the widely supported Ubuntu distribution. The Lubuntu instance runs an instance of FreeRADIUS that is used for authentication for the CheesyGorditaCrunch WLAN.

Lab Commands (Configure RADIUS Server)

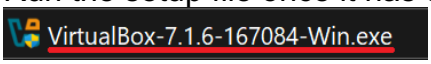
On your host PC, navigate to https://www.virtualbox.org/wiki/Downloads in a web browser.



Download the appropriate version of Virtualbox for your operating system (in this case, we are running Windows).

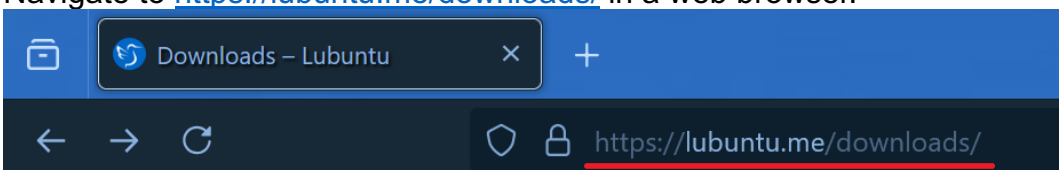


Run the setup file once it has downloaded.

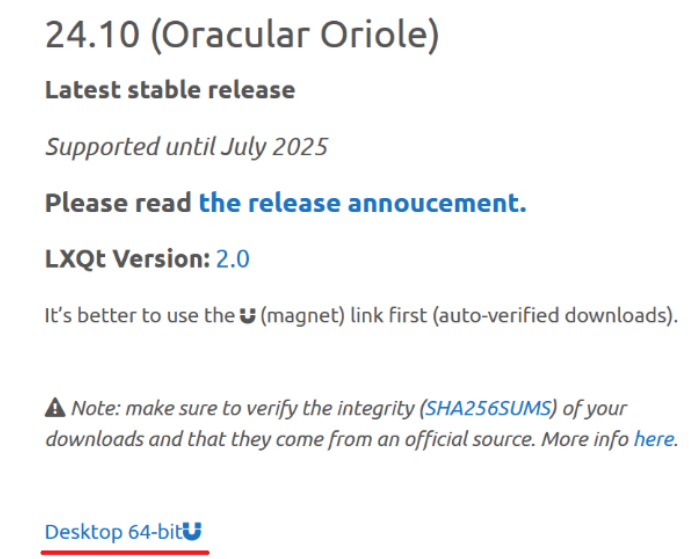


Be agreeable through the setup process, clicking Next and Install when prompted.

Navigate to https://lubuntu.me/downloads/ in a web browser.

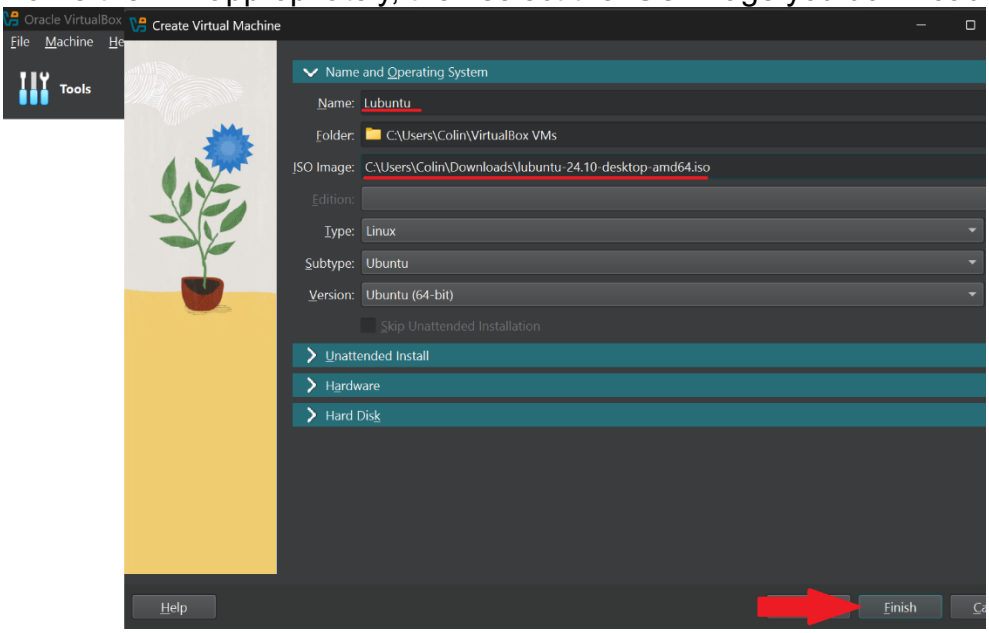


Download the ISO image for the latest stable release of the operating system.

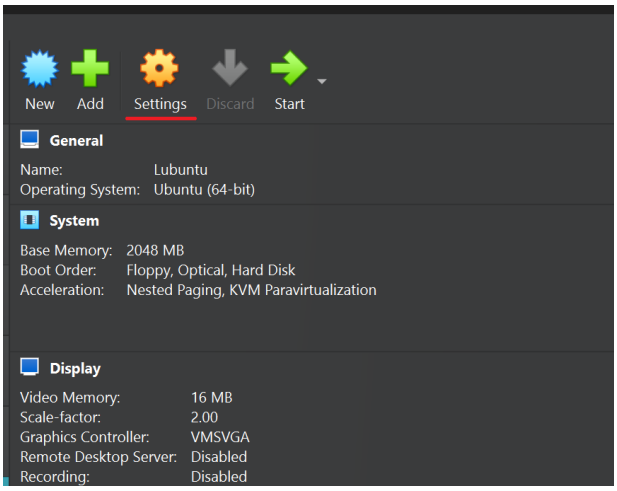


Open Virtualbox and click New.

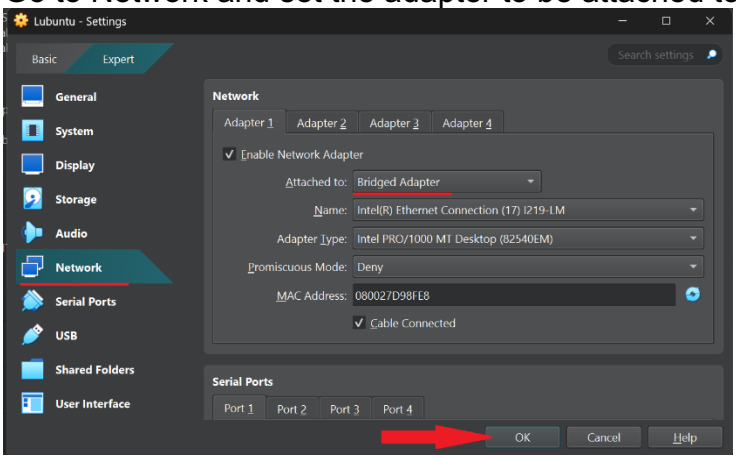
Name the VM appropriately, then select the ISO image you downloaded earlier.



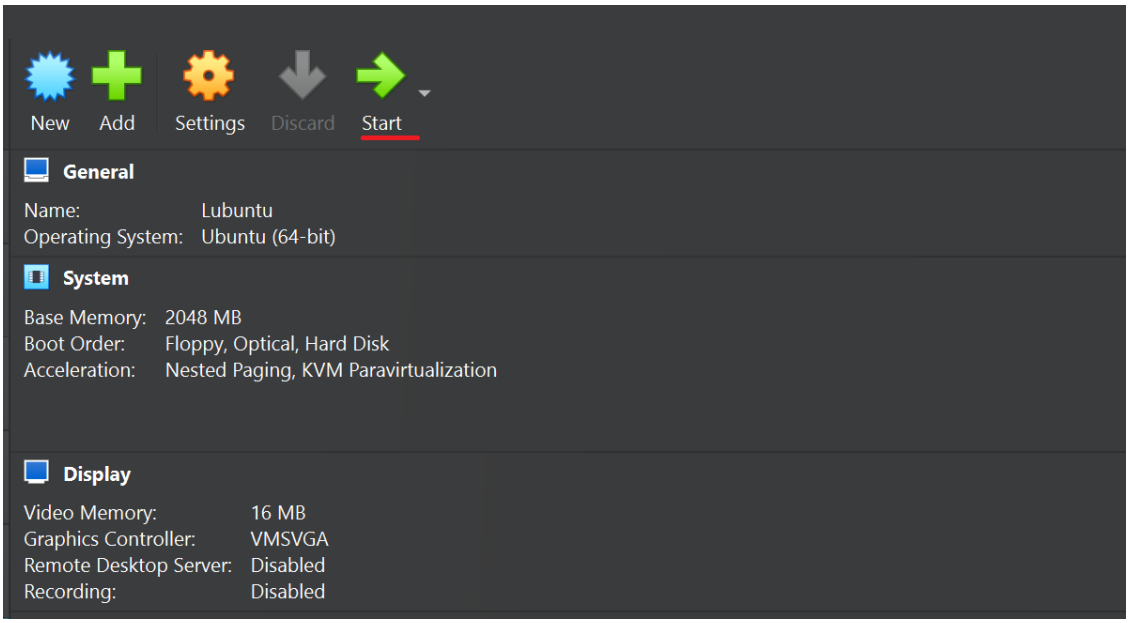
Click Settings.



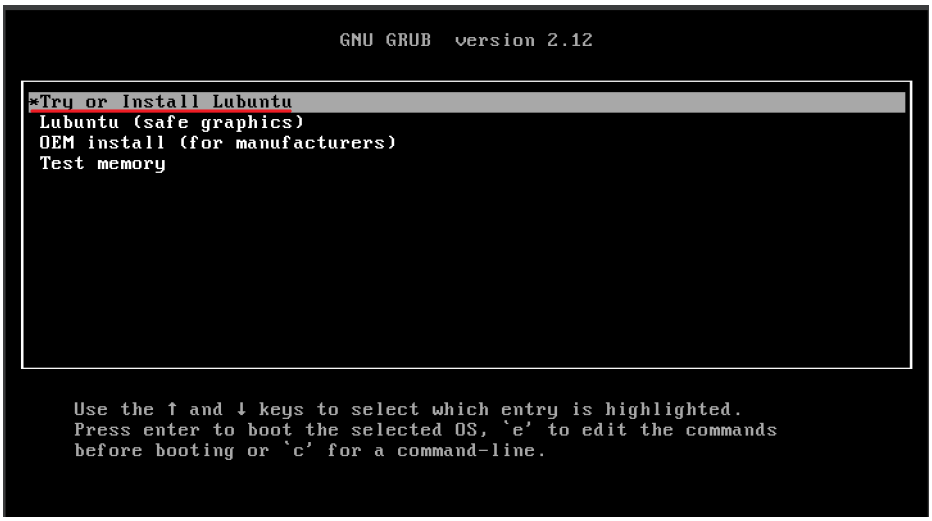
Go to Network and set the adapter to be attached to a Bridged Adapter. Click OK.



Click Start.



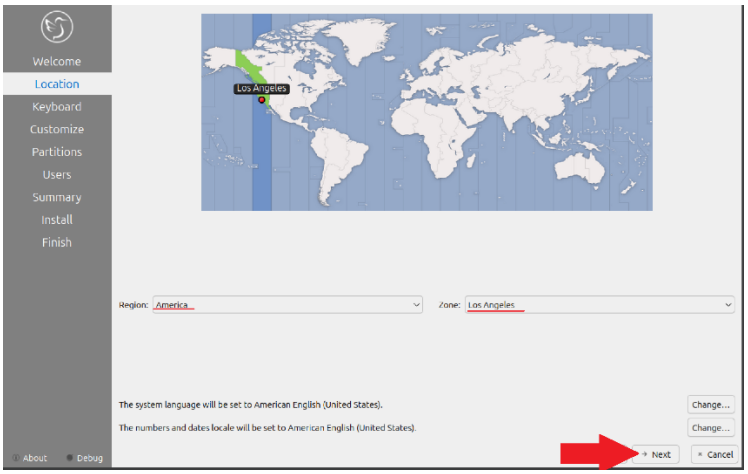
Select Try or Install Lubuntu.



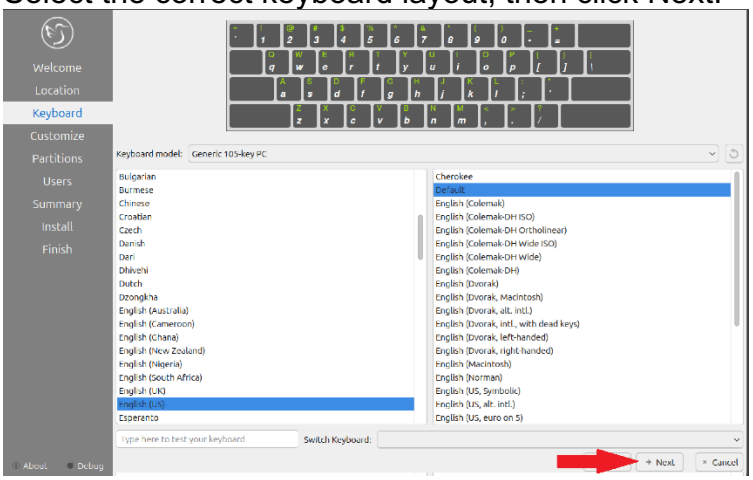
Select Install Lubuntu.

Click Next.

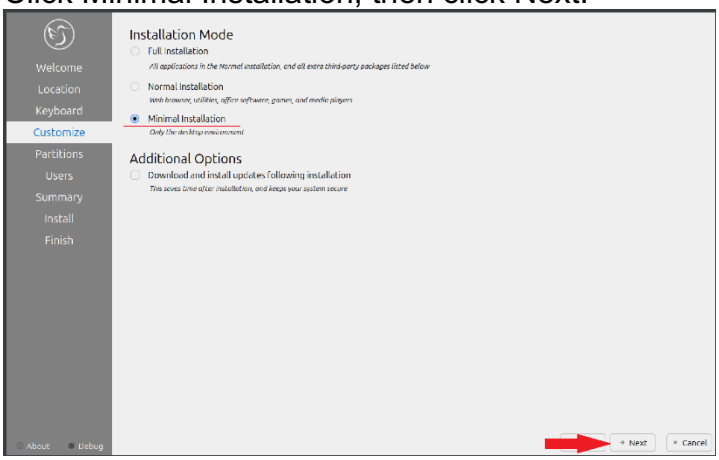
Set the correct time zone, then click Next.



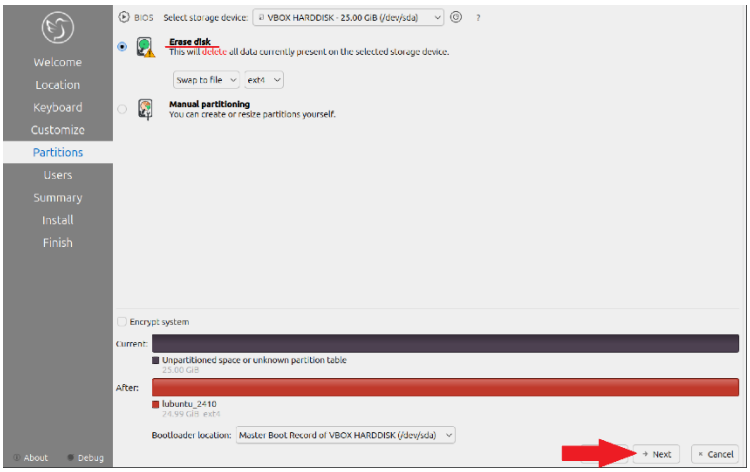
Select the correct keyboard layout, then click Next.



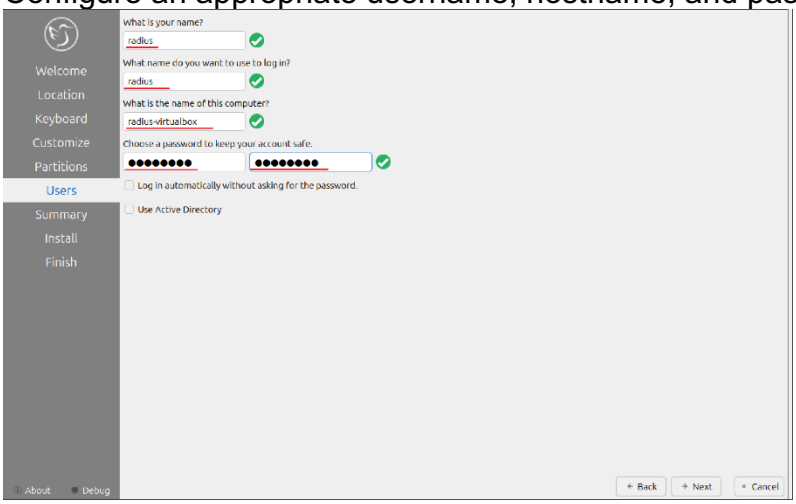
Click Minimal Installation, then click Next.



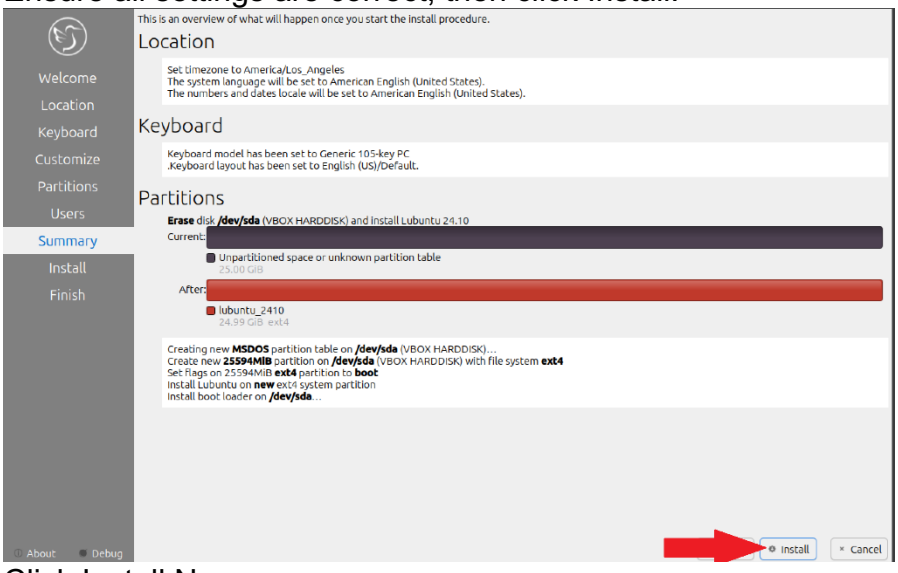
Select Erase disk, then click Next.



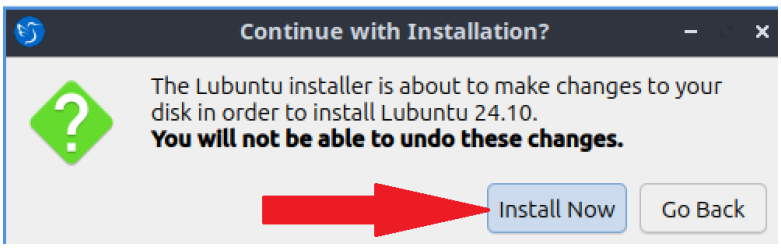
Configure an appropriate username, hostname, and password, then click Next.



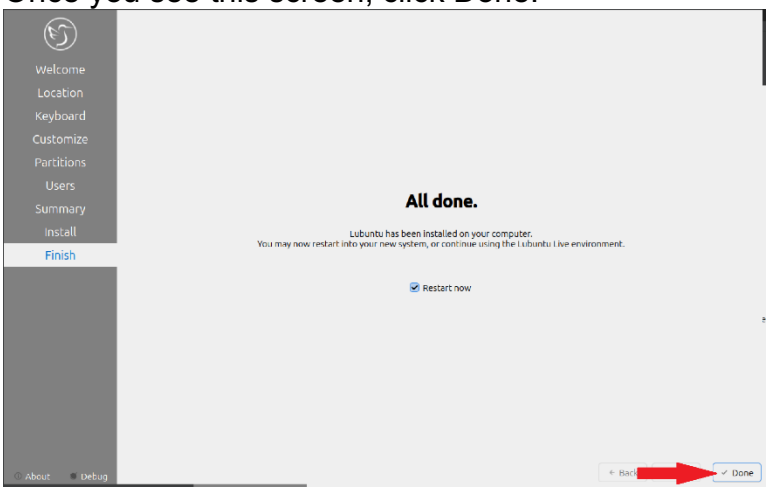
Ensure all settings are correct, then click Install.



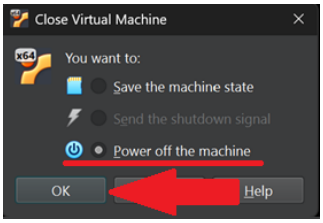
Click Install Now.



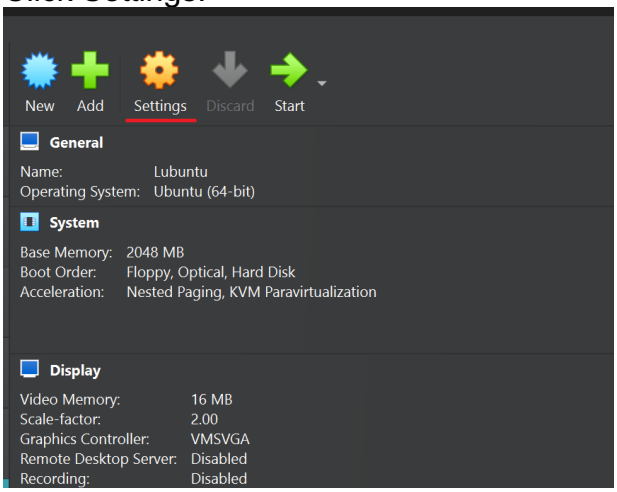
Once you see this screen, click Done.



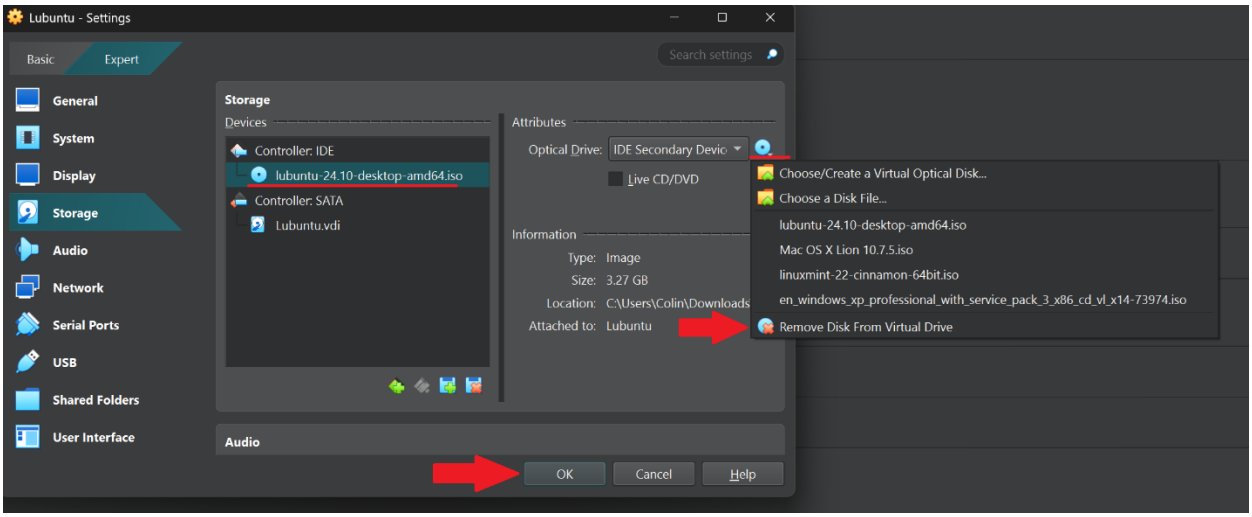
Press Right CTRL, then ALT+F4 to exit out of the VM. Select Power off the Machine, then click OK.



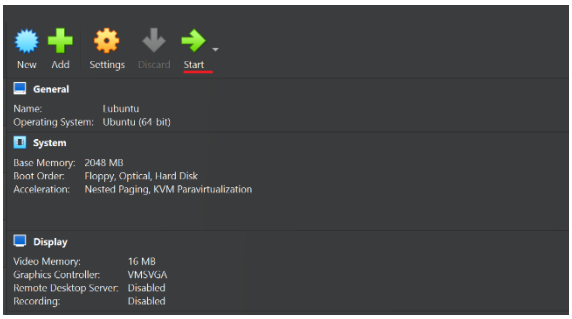
Click Settings.



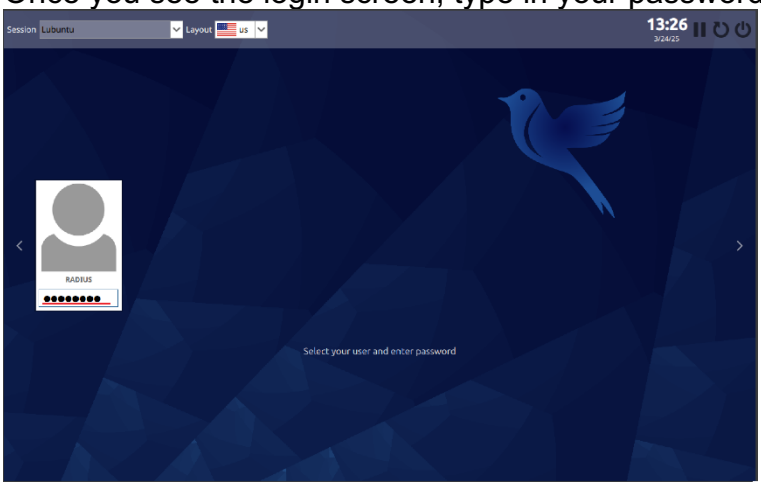
Go to Storage and click on the ISO file, click on the disk icon, then click Remove Disk from Virtual Drive. Click OK.



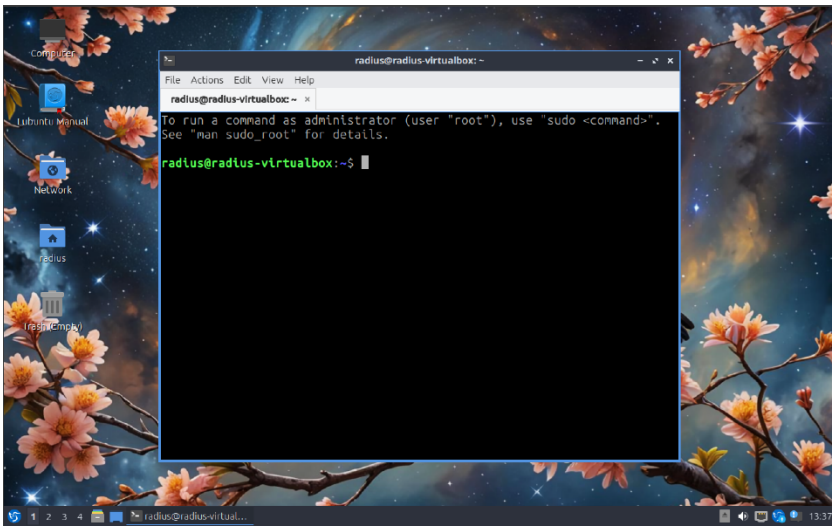
Click Start.



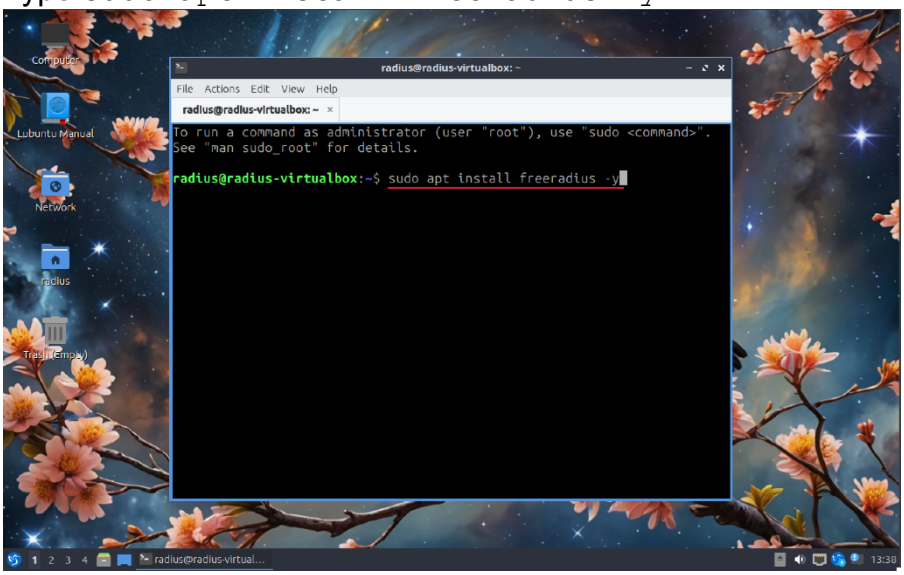
Once you see the login screen, type in your password and press Enter.



Press CTRL + ALT + T to open the terminal.



Type `sudo apt install freeradius -y`.



Type your password.

```
[sudo] password for radius:
```

Once freeradius has installed, type `sudo nano /etc/freeradius/3.0/clients.conf`.

```
radius@radius-virtualbox:~$ sudo nano /etc/freeradius/3.0/clients.conf
```

Add the following lines:

```
client wlc {
      ipaddr = 192.168.0.254
      secret = <secret>
}
```

With <secret> being replaced with a secure password to be specified later on the WLC.

```
client wlc {
        ipaddr = 192.168.0.254
        secret = Redbull6
}
```

Press CTRL + X, Y, then ENTER to save.

```
Save modified buffer?
 Y Yes
 N No           ^C Cancel
```

```
File Name to Write: /etc/freeradius/3.0/clients.conf
^G Help          M-D DOS Format    M-A Append        M-B Backup File
^C Cancel        M-M Mac Format    M-P Prepend       ^T Browse
```

Next, type `sudo nano /etc/freeradius/3.0/users`.

```
radius@radius-virtualbox:~$ sudo nano /etc/freeradius/3.0/users
```

Add the following lines:

```
<user>    Cleartext-Password := "<password>"
          Reply-Message := "Hello, <user>"
```

With <user> being replaced with a username and <password> being replaced with a secure password.

```
colin   Cleartext-Password := "squabbleup"
        Reply-Message := "Hello, Colin"
```

Press CTRL + X, Y, then ENTER to save.

```
Save modified buffer?
 Y Yes
 N No           ^C Cancel
```

```
File Name to Write: /etc/freeradius/3.0/users
^G Help          M-D DOS Format    M-A Append        M-B Backup File
^C Cancel        M-M Mac Format    M-P Prepend       ^T Browse
```

Lab Commands (Configuring WLC)

Connect your AP, WLC, Router, and PC to your switch as specified in the network diagram below.

Configure your switch according to the switch configuration below (Note: the WLC should be connected to port f0/1 as a trunk, and all other devices should be on access VLAN 99.).

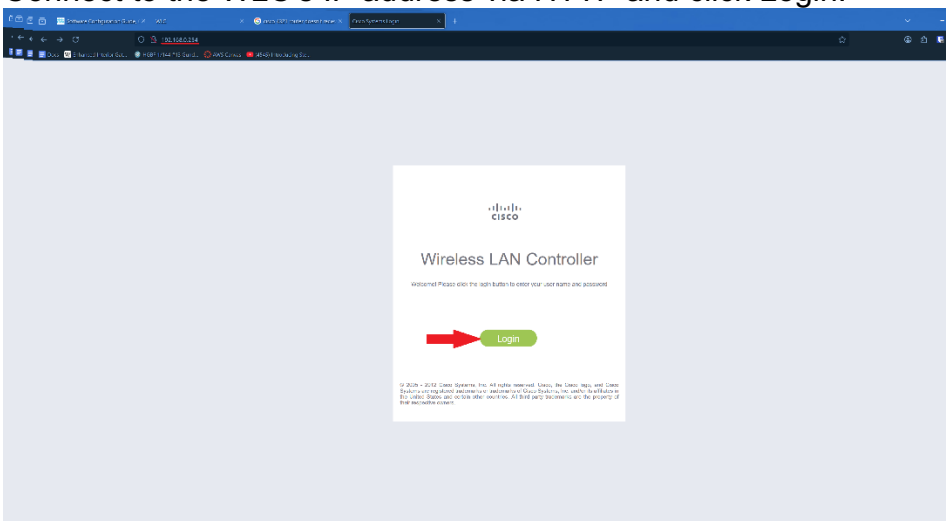
Configure your router according to the configuration below.

Ensure that PC is receiving an IP and that internet works.

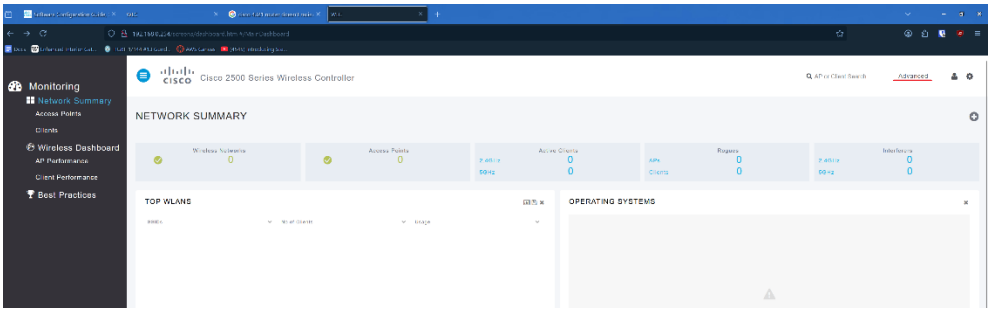
```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.0.3
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
```

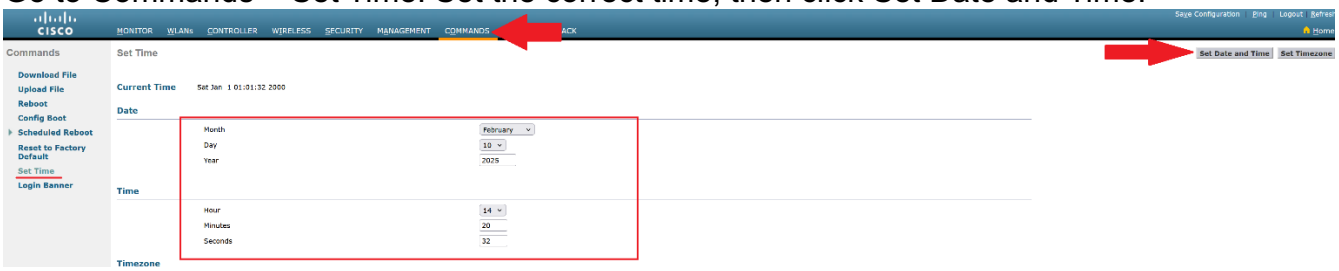
Connect to the WLC's IP address via HTTP and click Login.



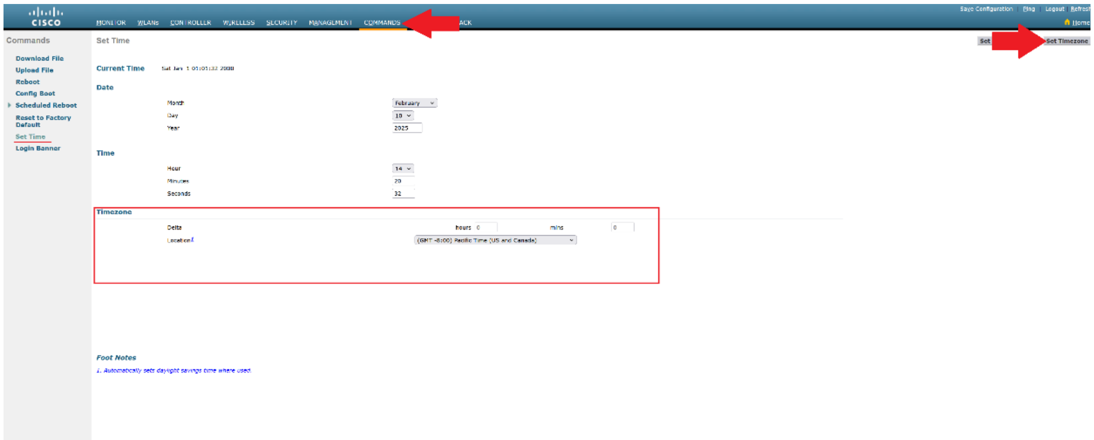
Click Advanced.



Go to Commands > Set Time. Set the correct time, then click Set Date and Time.

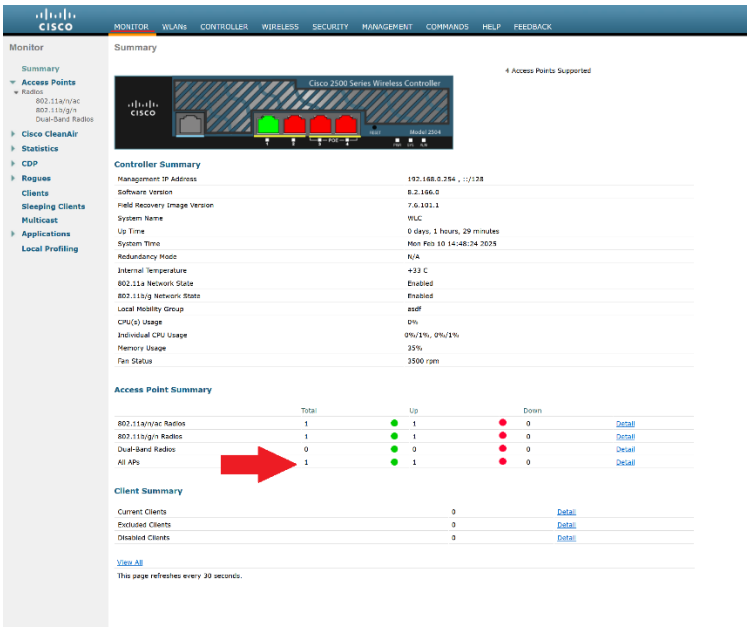


Set the timezone and click Set Timezone.

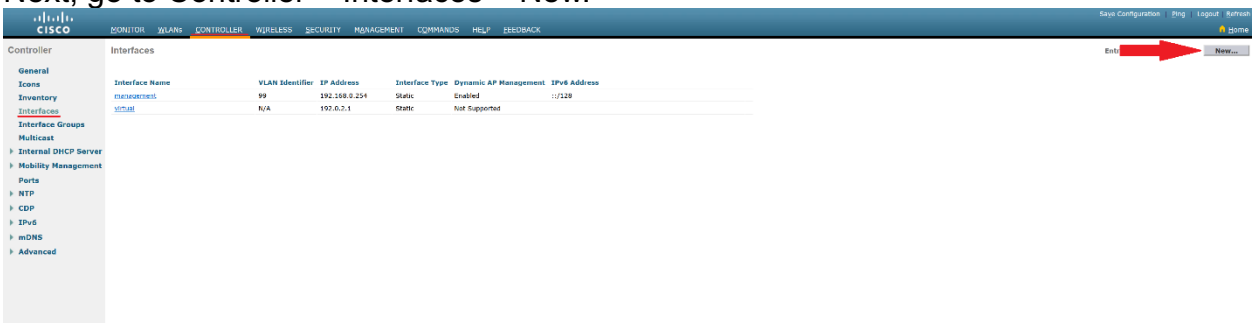


Once the correct timezone is set, the AP should automatically discover and connect to your WLC. In our case, the AP automatically downloaded and installed a software update as shown in the console log below (the image name is underlined in red):

Once the AP has finished updating, go to Monitor > Summary and ensure the WLC can see the AP (indicated by a 1 next to the All APs section)



Next, go to Controller > Interfaces > New.

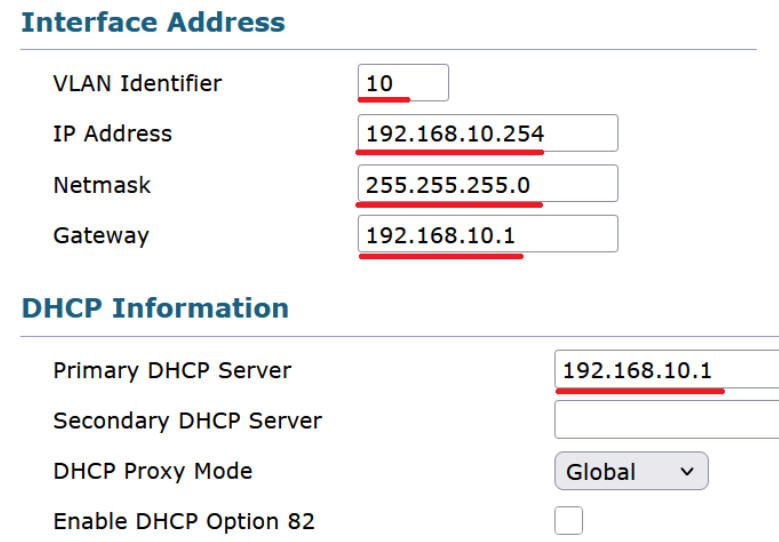


Create the Guest VLAN, setting the VLAN ID to 10.

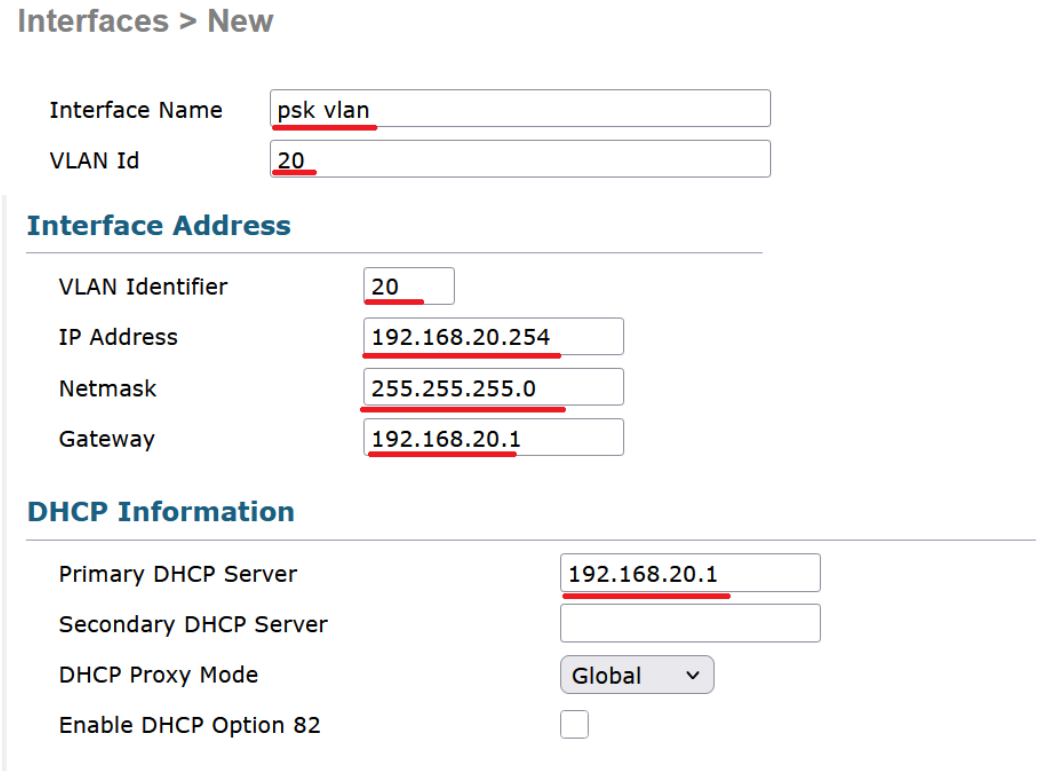
Interfaces > New

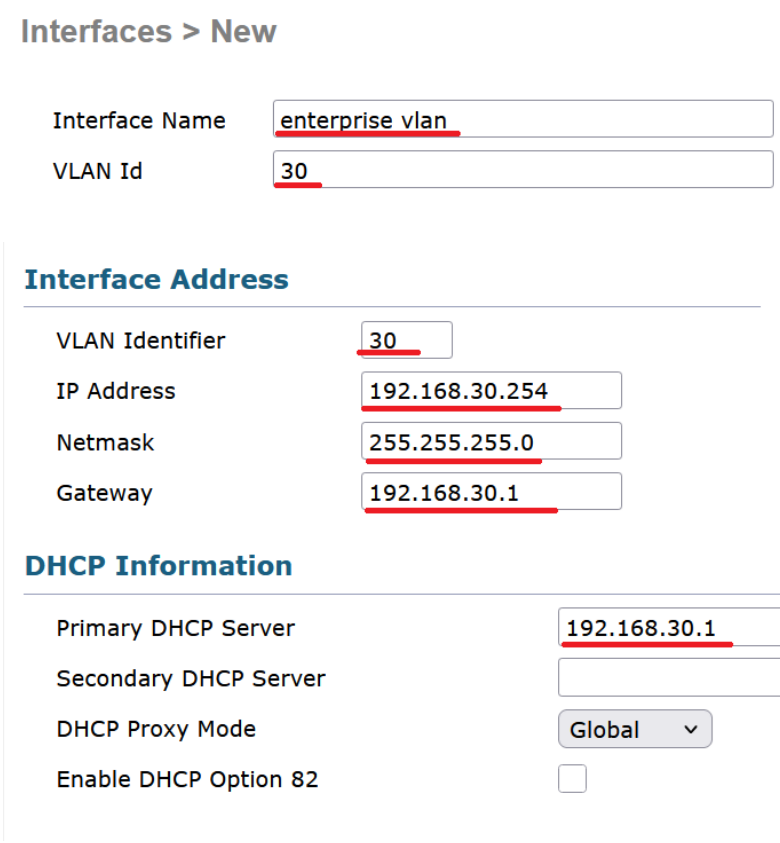
Interface Name	Guest VLAN
VLAN Id	10

Configure the VLAN ID, IP Address, Netmask, Gateway, and Primary DHCP Server for VLAN 10:

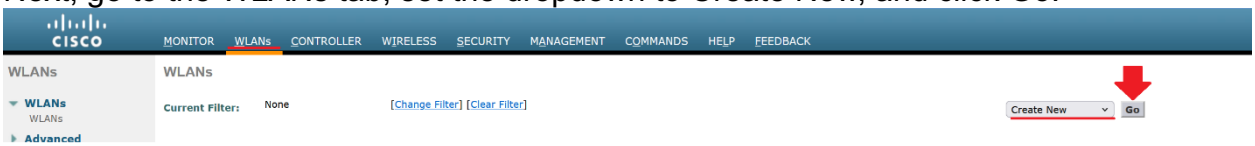


Create the PSK and Enterprise VLANs, using the VLAN information for VLANs 20 and 30 respectively:

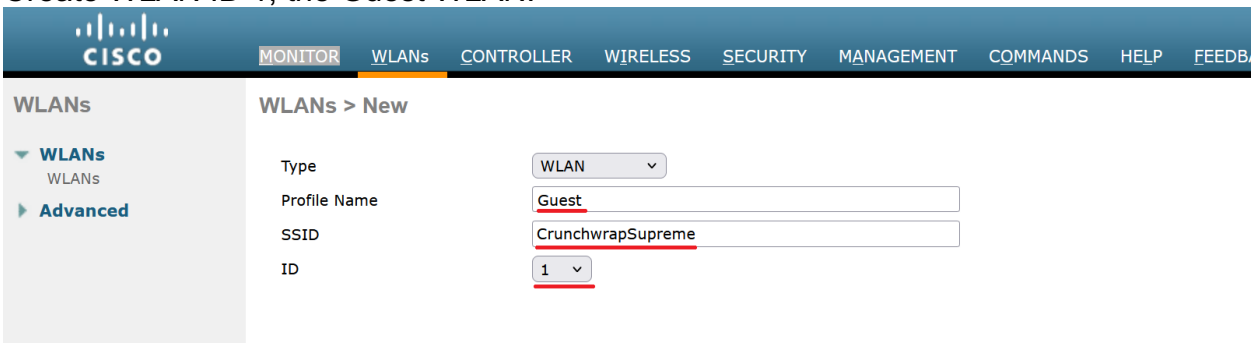




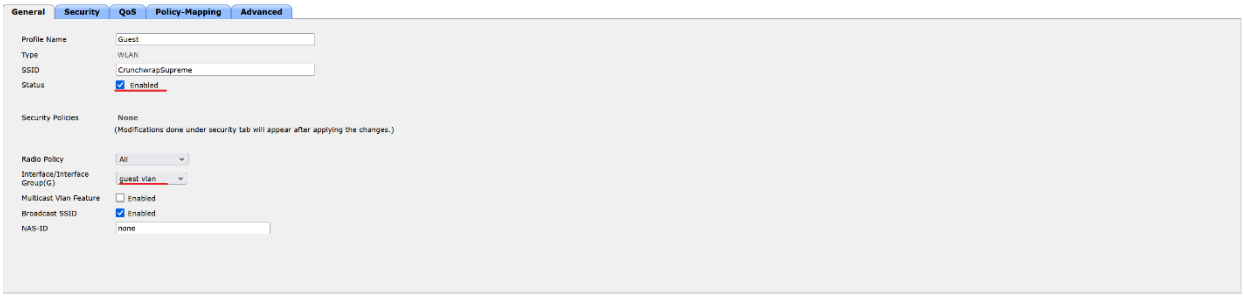
Next, go to the WLANs tab, set the dropdown to Create New, and click Go.



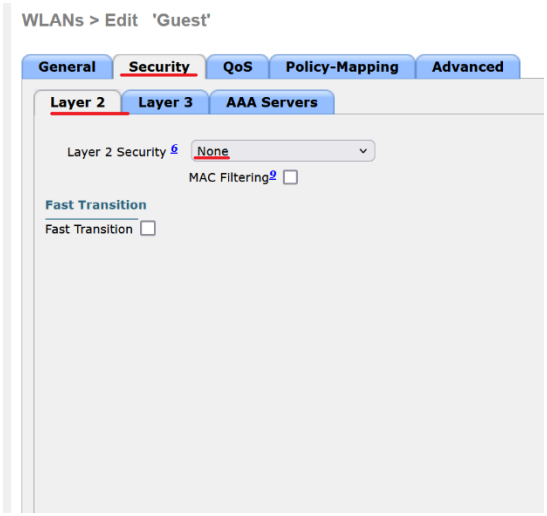
Create WLAN ID 1, the Guest WLAN:



Ensure the WLAN is enabled, and the interface is set to the guest VLAN:

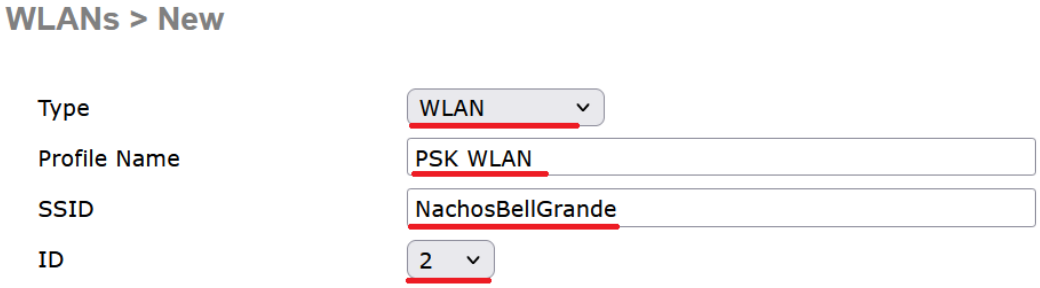


Under Security > Layer 2, set Layer 2 Security to None.

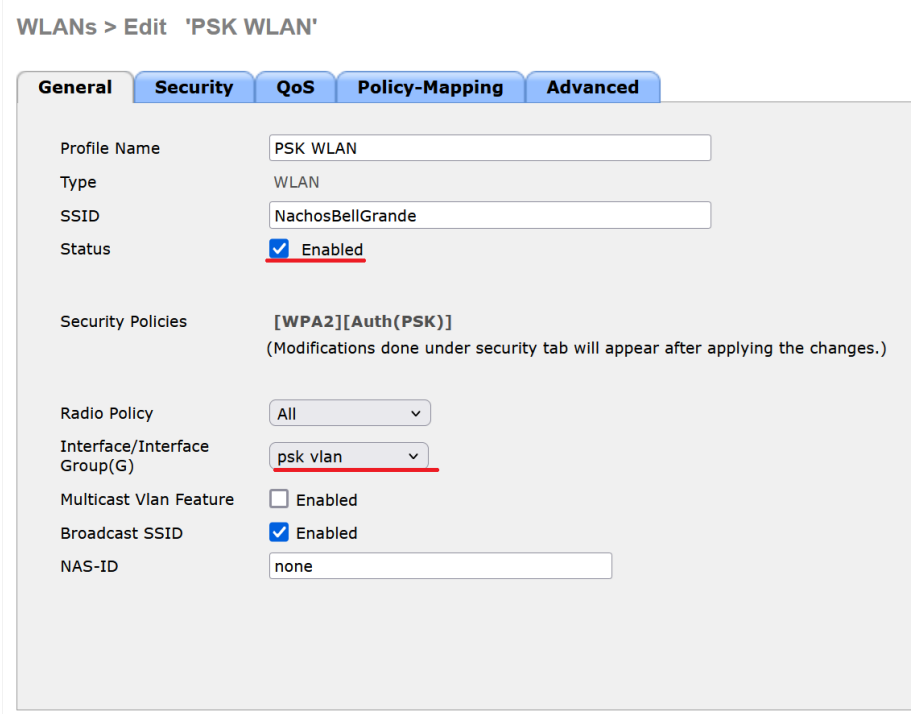


Click Apply.

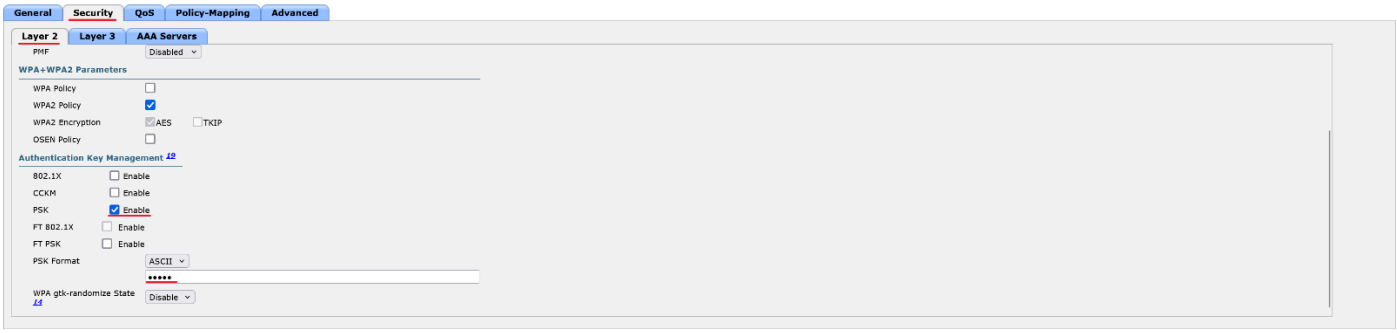
Next, configure the PSK WLAN (NachosBellGrande) with VLAN ID 2.



Ensure the WLAN is enabled and the interface is set to the PSK VLAN.

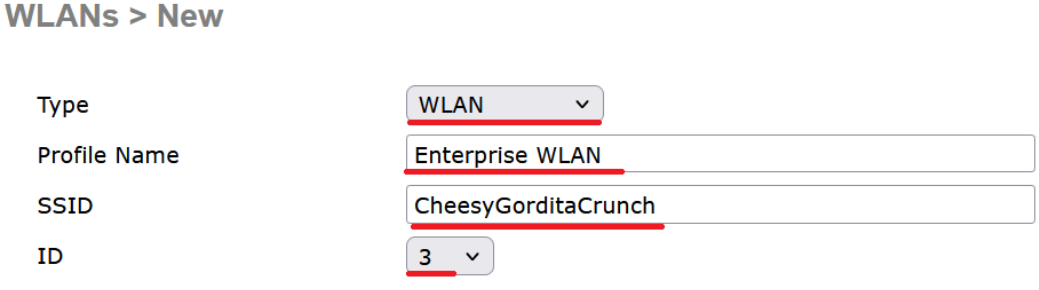


Under Security > Layer 2, Enable PSK, and under PSK Format, set a strong password.

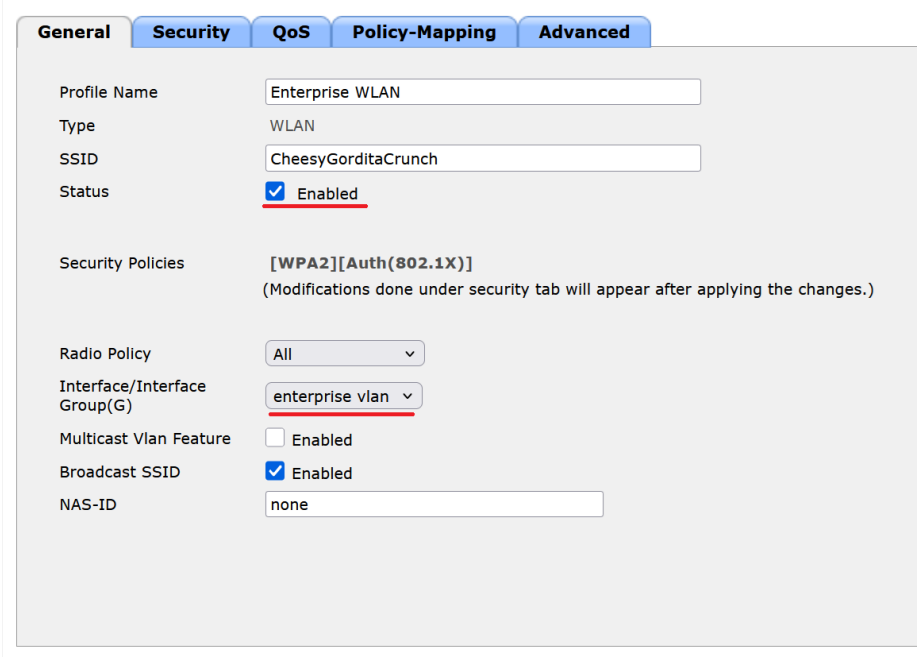


Click Apply.

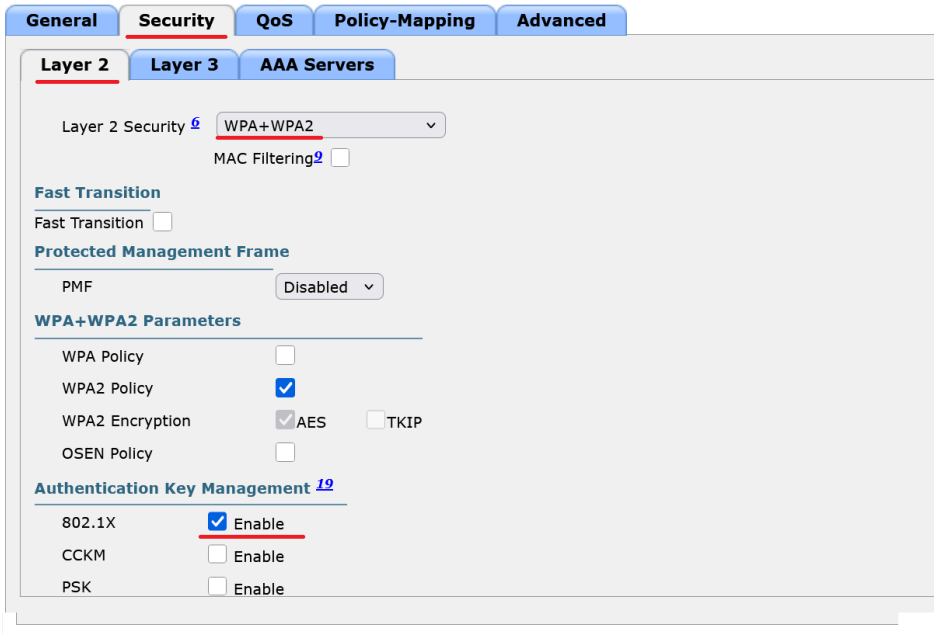
Next, Create the Enterprise WLAN.



Ensure the WLAN is enabled and set the interface to the Enterprise VLAN.

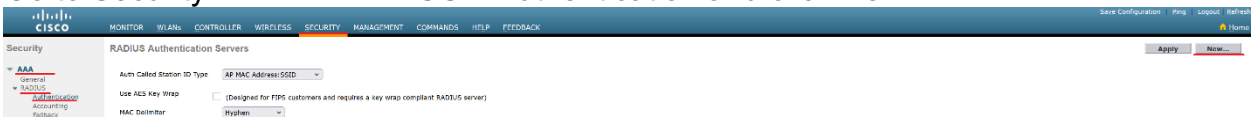


Under Security > Layer 2, set the Layer 2 securitty to WPA+WPA2, and under Authentication Key Management, ensure that 802.1X is enabled.

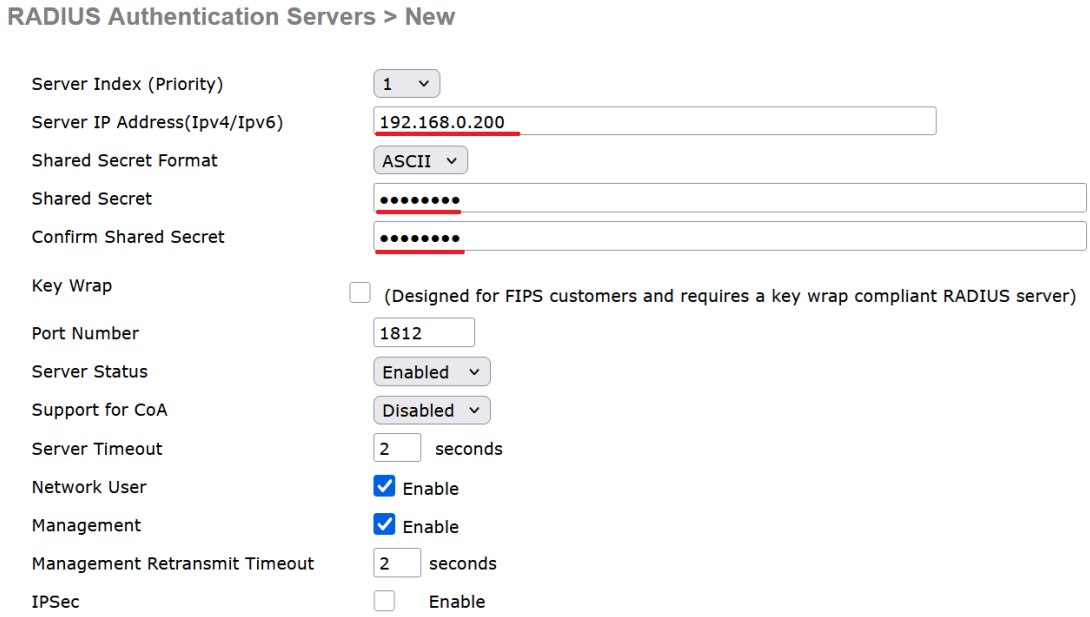


Click Apply.

Go to Security > AAA > RADIUS > Authentication and click New.



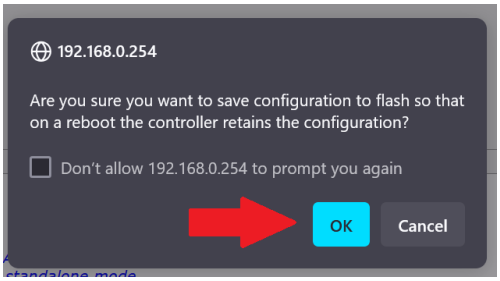
Enter the IP address of the RADIUS server, then enter the shared secret configured in the server's `clients.conf` file.



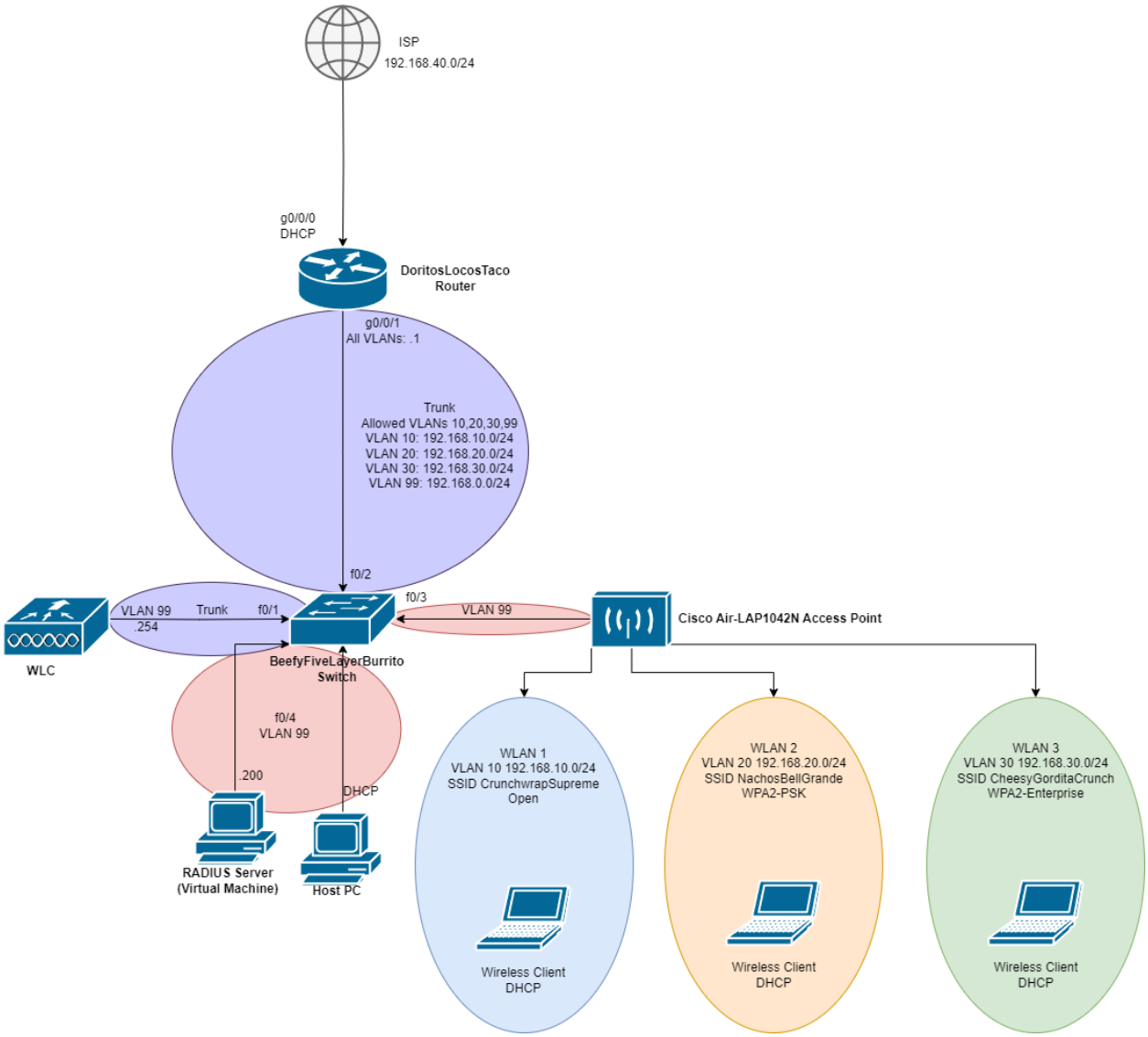
Click Apply.

Finally, click Save Configuration.

Click OK.



Network Diagram



Configuration for DoritosLocosTaco (Router)

```
Current configuration : 5312 bytes
Last configuration change at 22:07:55 UTC Tue Mar 11 2025
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
hostname DoritosLocosTaco
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 name-server 8.8.8.8 1.1.1.1
ip dhcp excluded-address 192.168.0.254
ip dhcp excluded-address 192.168.0.1
ip dhcp excluded-address 192.168.0.1 192.168.0.10
ip dhcp excluded-address 192.168.0.30 192.168.0.254
ip dhcp excluded-address 192.168.10.1
ip dhcp excluded-address 192.168.20.1
ip dhcp excluded-address 192.168.30.1
ip dhcp excluded-address 192.168.0.200
ip dhcp pool AP-POOL
 network 192.168.0.0 255.255.255.0
 default-router 192.168.0.1
 dns-server 8.8.8.8 8.8.4.4
ip dhcp pool GUEST-VLAN
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 8.8.8.8
ip dhcp pool PSK-VLAN
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.1
 dns-server 8.8.8.8
ip dhcp pool ENTERPRISE-VLAN
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
 dns-server 8.8.8.8
login on-success log
subscriber templating
vtp domain cisco
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO214421D1
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
 no ip address
 negotiation auto
interface GigabitEthernet0/0/1.10
 encapsulation dot1Q 10
```

```
 ip address 192.168.10.1 255.255.255.0
 ip nat inside
interface GigabitEthernet0/0/1.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
 ip nat inside
interface GigabitEthernet0/0/1.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
 ip nat inside
interface GigabitEthernet0/0/1.99
 encapsulation dot1Q 99
 ip address 192.168.0.1 255.255.255.0
 ip nat inside
interface Serial0/1/0
interface Serial0/1/1
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 negotiation auto
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip http client source-interface GigabitEthernet0/0/0
ip nat inside source list 1 interface GigabitEthernet0/0/0
overload
ip nat inside source list 10 interface GigabitEthernet0/0/0
overload
ip nat inside source list 20 interface GigabitEthernet0/0/0
overload
ip nat inside source list 30 interface GigabitEthernet0/0/0
overload
ip route 0.0.0.0 0.0.0.0 dhcp
access-list 1 permit 192.168.0.0 0.0.0.255
access-list 10 permit 192.168.10.0 0.0.0.255
access-list 20 permit 192.168.20.0 0.0.0.255
access-list 30 permit 192.168.30.0 0.0.0.255
ip access-list extended 101
control-plane
line con 0
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
```

```
end
```

Configuration for BeefyFiveLayerBurrito (Switch)

```
Current configuration : 5307 bytes
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname BeefyFiveLayerBurrito
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 portfast default
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
vlan internal allocation policy ascending
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
interface FastEthernet0/2
 switchport access vlan 99
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30,99
 switchport mode trunk
interface FastEthernet0/3
 switchport access vlan 99
interface FastEthernet0/4
 switchport access vlan 99
interface FastEthernet0/5
 switchport access vlan 99
interface FastEthernet0/6
 switchport access vlan 99
interface FastEthernet0/7
 switchport access vlan 99
interface FastEthernet0/8
 switchport access vlan 99
interface FastEthernet0/9
 switchport access vlan 99
interface FastEthernet0/10
 switchport access vlan 99
interface FastEthernet0/11
 switchport access vlan 99
interface FastEthernet0/12
```

```
 switchport access vlan 99
interface FastEthernet0/13
 switchport access vlan 99
interface FastEthernet0/14
 switchport access vlan 99
interface FastEthernet0/15
 switchport access vlan 99
interface FastEthernet0/16
 switchport access vlan 99
interface FastEthernet0/17
 switchport access vlan 99
interface FastEthernet0/18
 switchport access vlan 99
interface FastEthernet0/19
 switchport access vlan 99
interface FastEthernet0/20
 switchport access vlan 99
interface FastEthernet0/21
 switchport access vlan 99
interface FastEthernet0/22
 switchport access vlan 99
interface FastEthernet0/23
 switchport access vlan 99
interface FastEthernet0/24
 switchport access vlan 99
interface FastEthernet0/25
 switchport access vlan 99
interface FastEthernet0/26
 switchport access vlan 99
interface FastEthernet0/27
 switchport access vlan 99
interface FastEthernet0/28
 switchport access vlan 99
interface FastEthernet0/29
 switchport access vlan 99
interface FastEthernet0/30
 switchport access vlan 99
interface FastEthernet0/31
 switchport access vlan 99
interface FastEthernet0/32
 switchport access vlan 99
interface FastEthernet0/33
 switchport access vlan 99
interface FastEthernet0/34
 switchport access vlan 99
interface FastEthernet0/35
 switchport access vlan 99
```

```
interface FastEthernet0/36
 switchport access vlan 99
interface FastEthernet0/37
 switchport access vlan 99
interface FastEthernet0/38
 switchport access vlan 99
interface FastEthernet0/39
 switchport access vlan 99
interface FastEthernet0/40
 switchport access vlan 99
interface FastEthernet0/41
 switchport access vlan 99
interface FastEthernet0/42
 switchport access vlan 99
interface FastEthernet0/43
 switchport access vlan 99
interface FastEthernet0/44
 switchport access vlan 99
interface FastEthernet0/45
 switchport access vlan 99
interface FastEthernet0/46
 switchport access vlan 99
 switchport mode access
interface FastEthernet0/47
 switchport access vlan 99
 switchport mode access
interface FastEthernet0/48
 switchport access vlan 99
interface GigabitEthernet0/1
interface GigabitEthernet0/2
interface GigabitEthernet0/3
interface GigabitEthernet0/4
interface Vlan1
 no ip address
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
```

Routing Table for DoritosLocosTaco

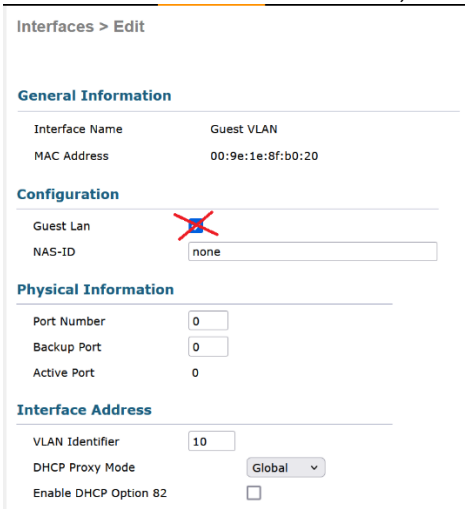
```
S*    0.0.0.0/0 [1/0] via 192.168.40.1
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
```

```
C        192.168.0.0/24 is directly connected, GigabitEthernet0/0/1.99
L        192.168.0.1/32 is directly connected, GigabitEthernet0/0/1.99
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected,
GigabitEthernet0/0/1.10
L        192.168.10.1/32 is directly connected,
GigabitEthernet0/0/1.10
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.20.0/24 is directly connected,
GigabitEthernet0/0/1.20
L        192.168.20.1/32 is directly connected,
GigabitEthernet0/0/1.20
      192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.30.0/24 is directly connected,
GigabitEthernet0/0/1.30
L        192.168.30.1/32 is directly connected,
GigabitEthernet0/0/1.30
C     192.168.40.0/23 is directly connected, GigabitEthernet0/0/0
      192.168.40.0/32 is subnetted, 1 subnets
L        192.168.40.110 is directly connected, GigabitEthernet0/0/0
```

Problems

Originally, our AP did not connect to the WLC, and we couldn't figure out why. It turns out that this was due to the time being set incorrectly on the WLC. The time is set to January 1, 2000 at 12:00AM by default, which prevents an HTTPS connection from being formed between the AP and the WLC as the AP's certificates are set to only work after a certain date. This problem is the reason that setting the time on the WLC is one of the first configuration steps we outline in this lab.

Originally, we checked the "Guest LAN" box for the Guest VLAN interface, assuming that this option was necessary. It turns out that the Guest Lan option is meant for guest authentication for wired clients, and will not work for a wireless guest network.



Conclusion

To wrap up, I am now much more confident in my skills setting up wireless networks, especially in their addressing and security settings. I also now understand RADIUS and its open-source implementations to a much greater extent, and am confident that I could replicate this setup in a real-world environment. This type of

network with three WLANs, one for guest use, personal use, and secure use, is especially useful in the real world, and is very similar to the WLAN configuration that our school district uses for tens of thousands of students and staff.