



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

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 support 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 distribution 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

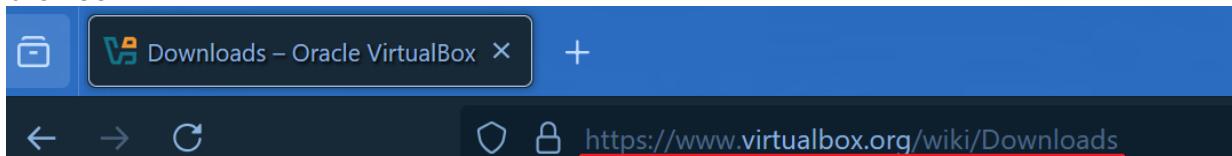
In this lab, we configured a Cisco 2504 WLAN Controller and Cisco Aironet AIR-LAP1042N Access Point with three WLANs – one configured with no security (CrunchwrapSupreme), one with WPA2-PSK (NachosBellGrande), and one with WPA2-Enterprise (CheesyGorditaCrunch). Each of these WLANs is connected to its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



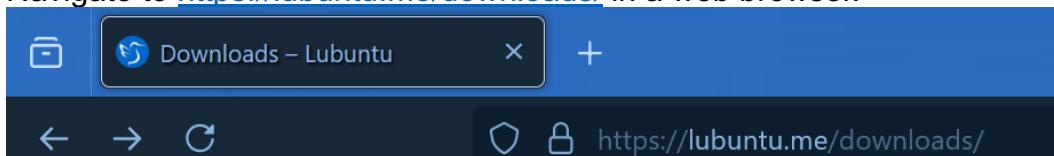
Run the setup file once it has downloaded.



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.

24.10 (Oracular Oriole)

Latest stable release

Supported until July 2025

Please read [the release announcement.](#)

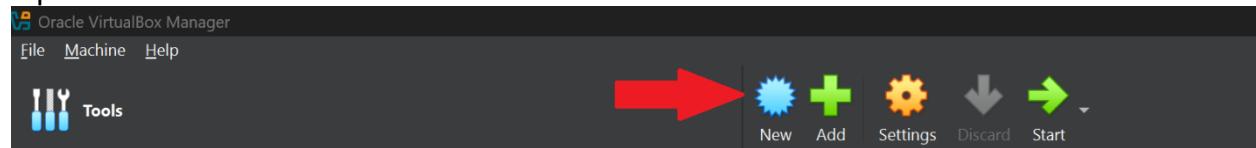
LXQt Version: 2.0

It's better to use the [\(magnet\)](#) link first (auto-verified downloads).

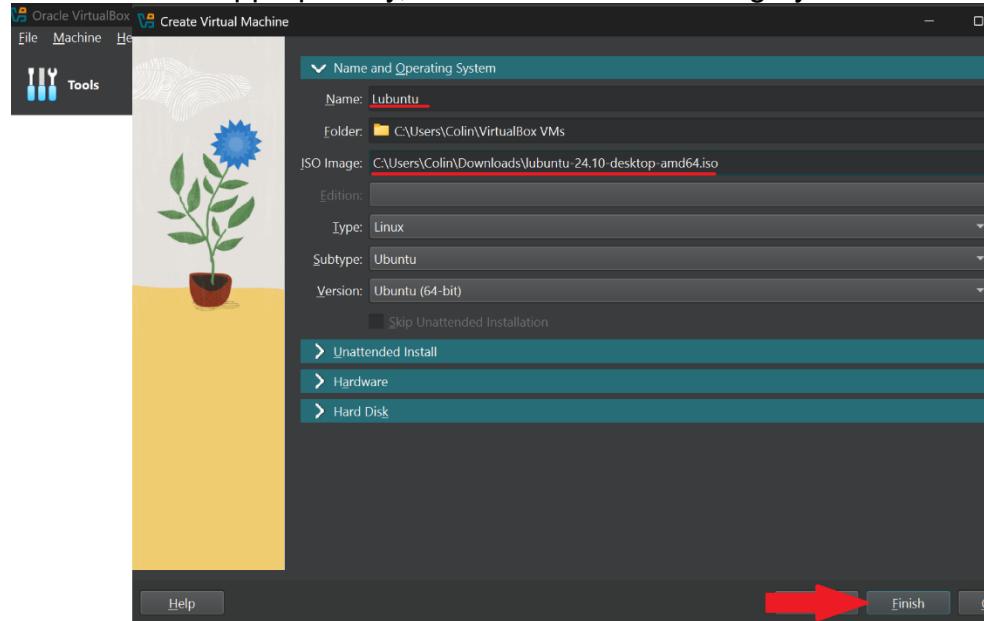
⚠ Note: make sure to verify the integrity ([SHA256SUMS](#)) of your downloads and that they come from an official source. More info [here](#).

[Desktop 64-bit](#)

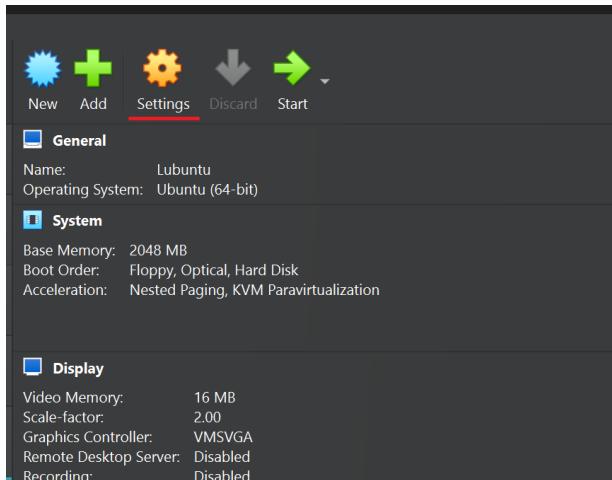
Open Virtualbox and click New.



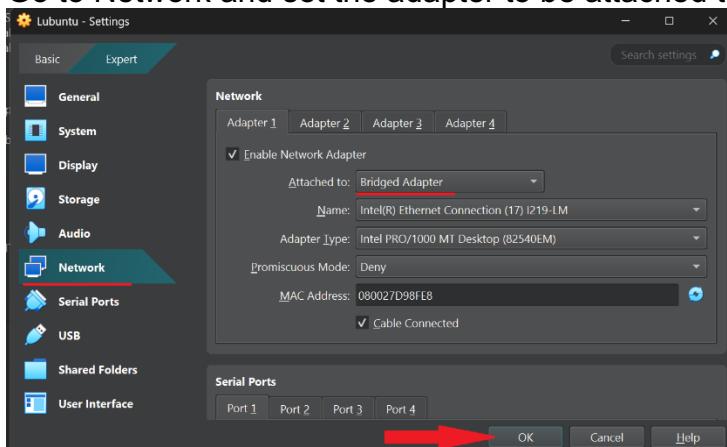
Name the VM appropriately, then select the ISO image you downloaded earlier.



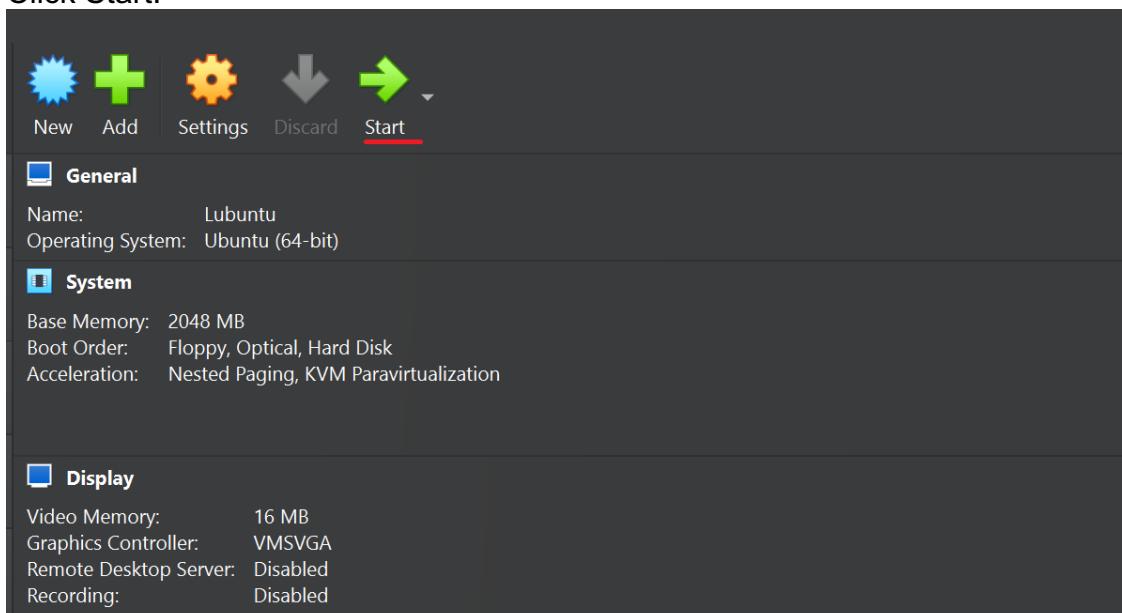
Click Settings.



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



Click Start.



Select Try or Install Lubuntu.



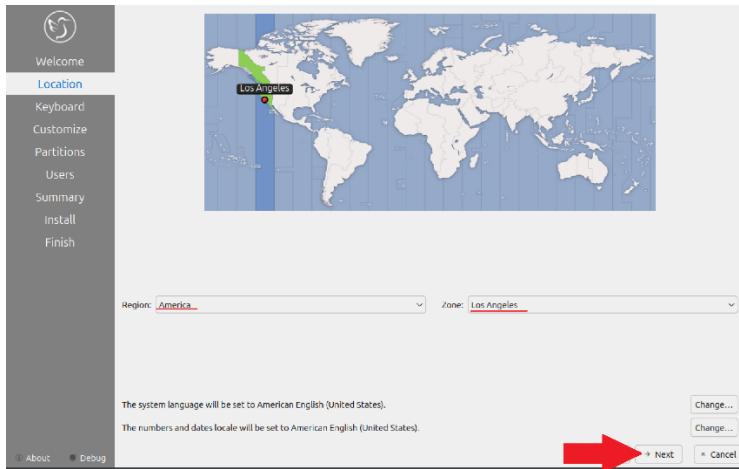
Select Install Lubuntu.



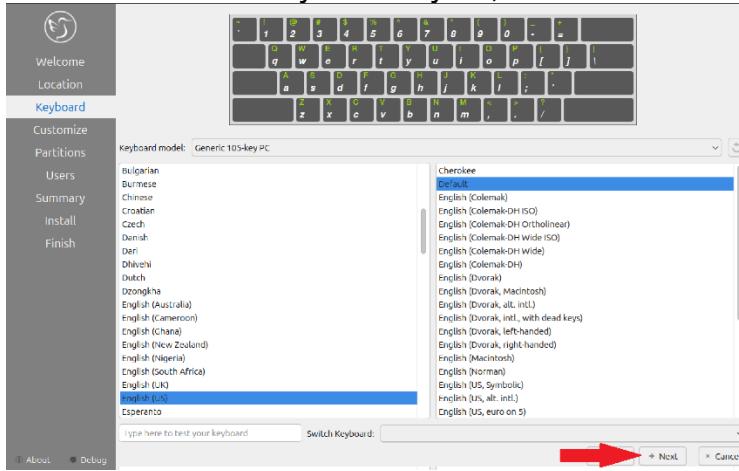
Click Next.



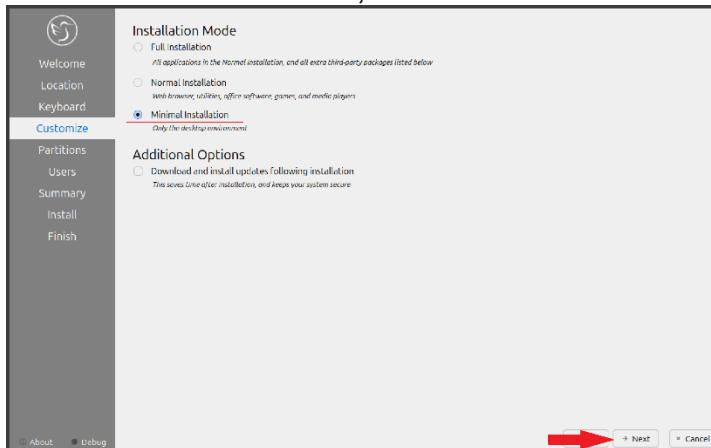
Set the correct time zone, then click Next.



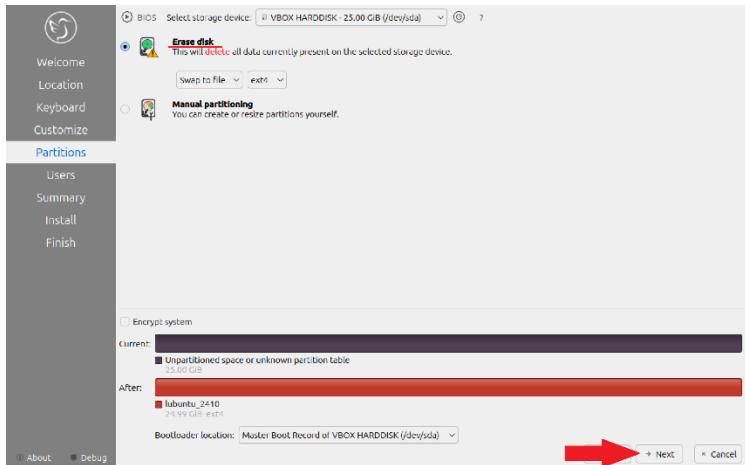
Select the correct keyboard layout, then click Next.



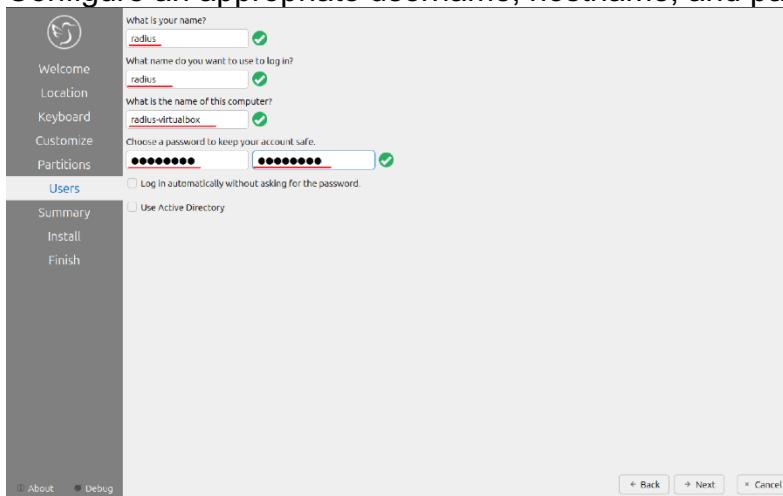
Click Minimal Installation, then click Next.



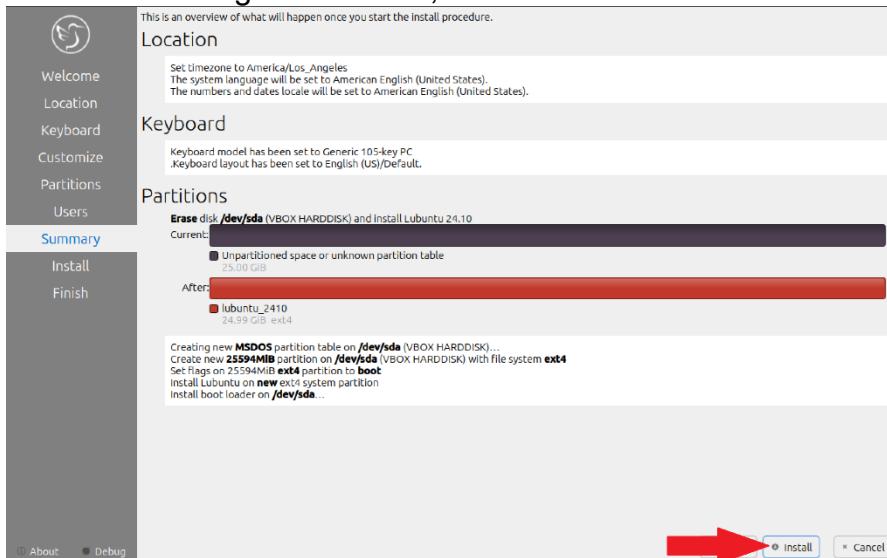
Select Erase disk, then click Next.



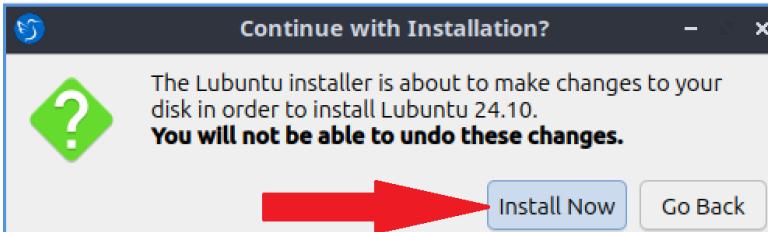
Configure an appropriate username, hostname, and password, then click Next.



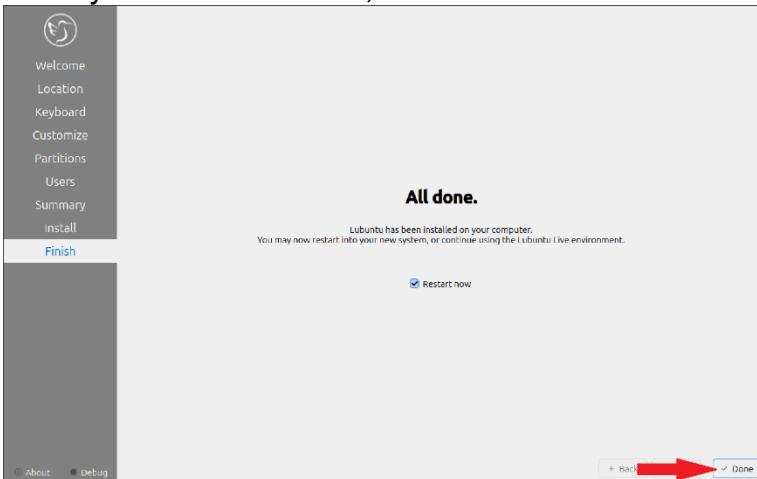
Ensure all settings are correct, then click Install.



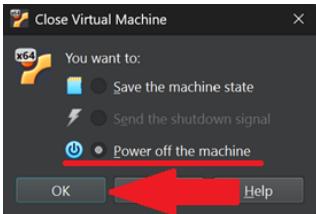
Click Install Now.



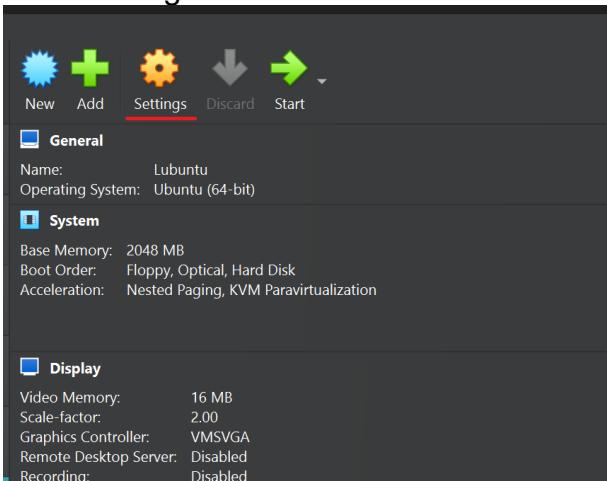
Once you see this screen, click Done.



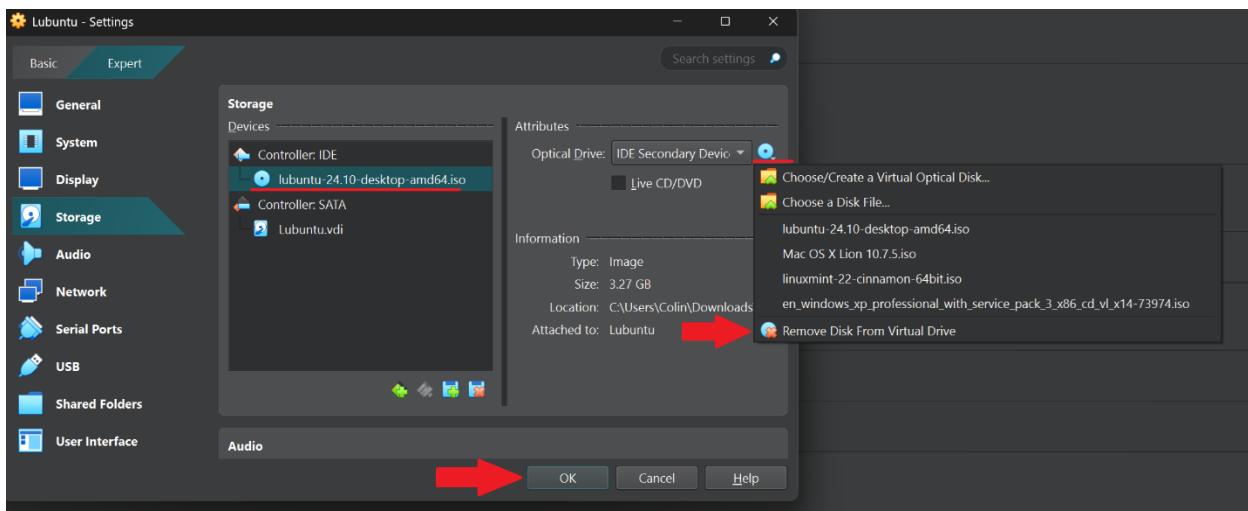
Press Right CTRL, then ALT+F4 to exit out of the VM. Select Power off the Machine, then click OK.



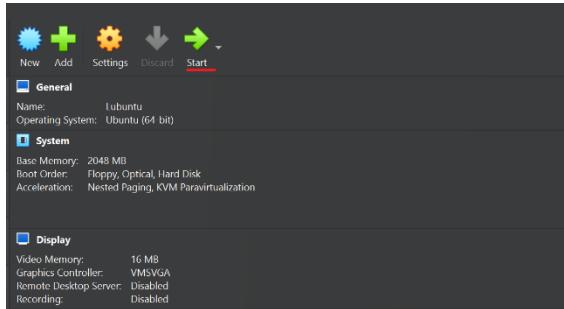
Click Settings.



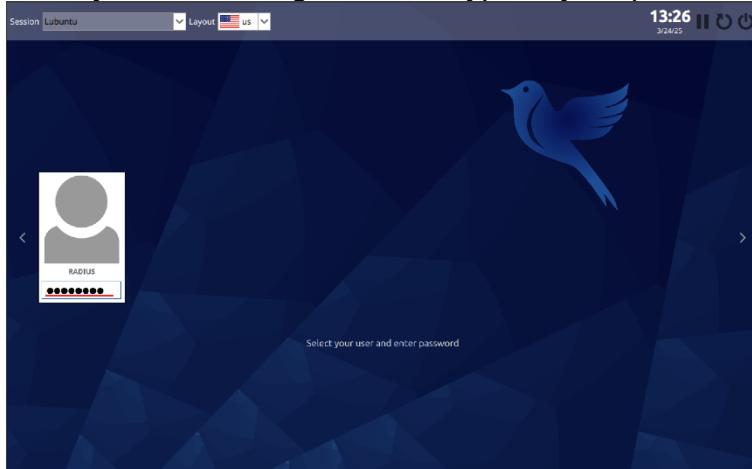
Go to Storage and click on the ISO file, click on the disk icon, then click Remove Disk from Virtual Drive. Click OK.



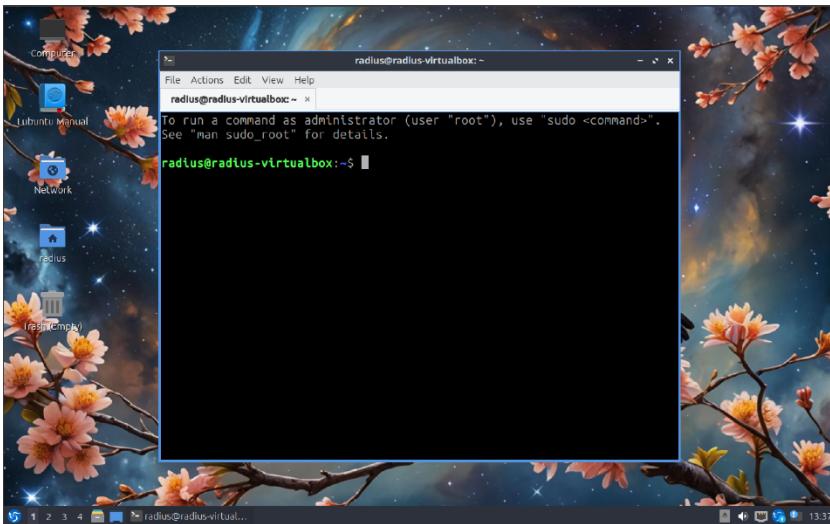
Click Start.



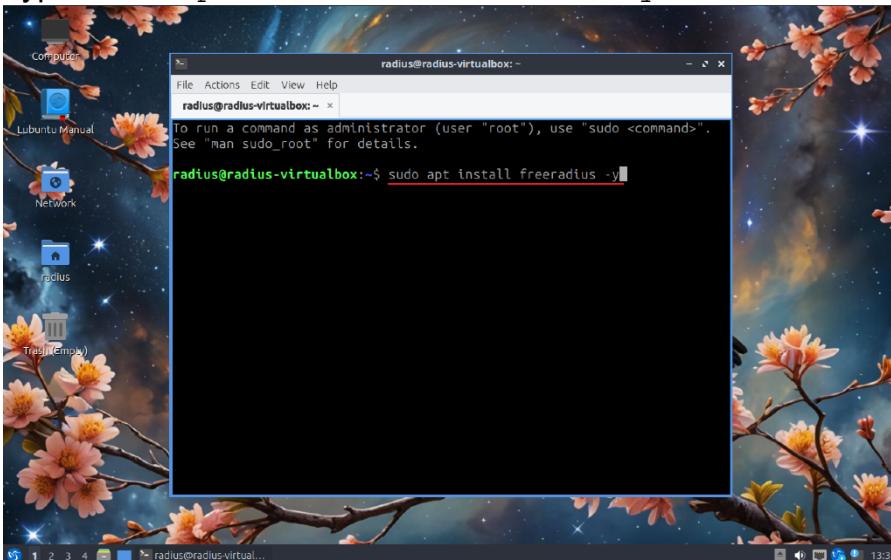
Once you see the login screen, type in your password and press Enter.



Press CTRL + ALT + T to open the terminal.



Type sudo apt install freeradius -y.



Type your password.

[sudo] password for radius: [REDACTED]

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

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

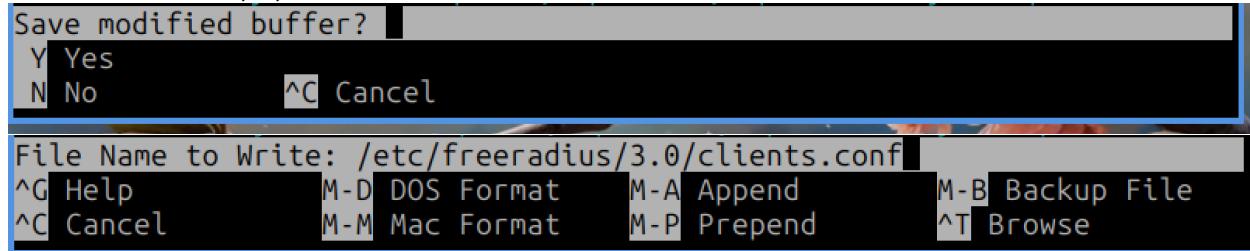
Add the following lines:

```
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.



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

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

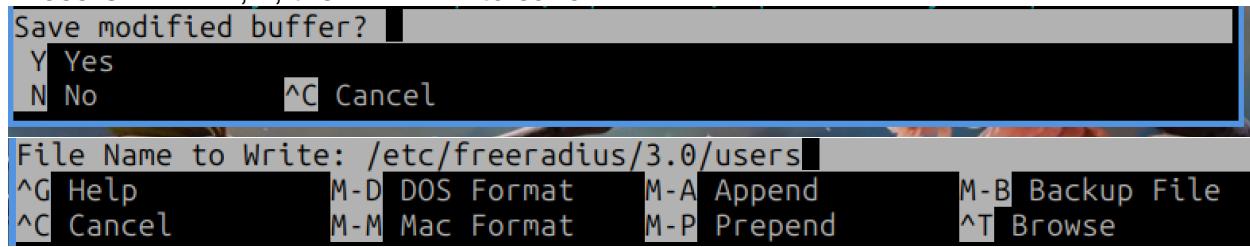
Add the following lines:

```
<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.



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.).

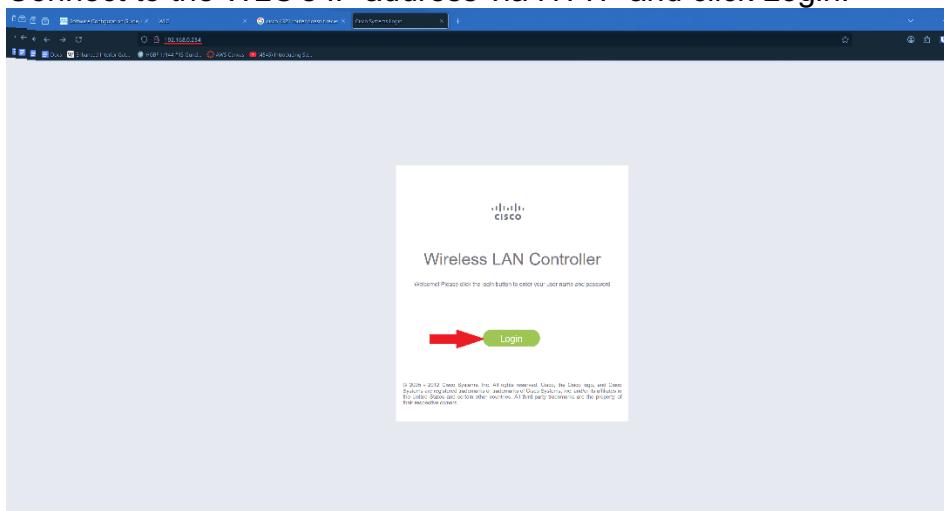
Configure your router according to the configuration below.

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

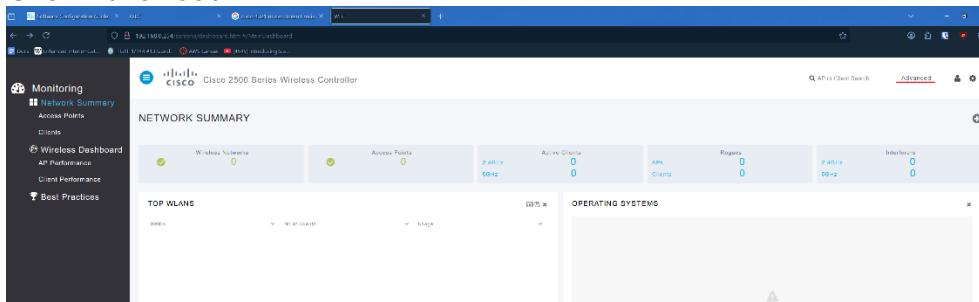
Ethernet adapter Ethernet:

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

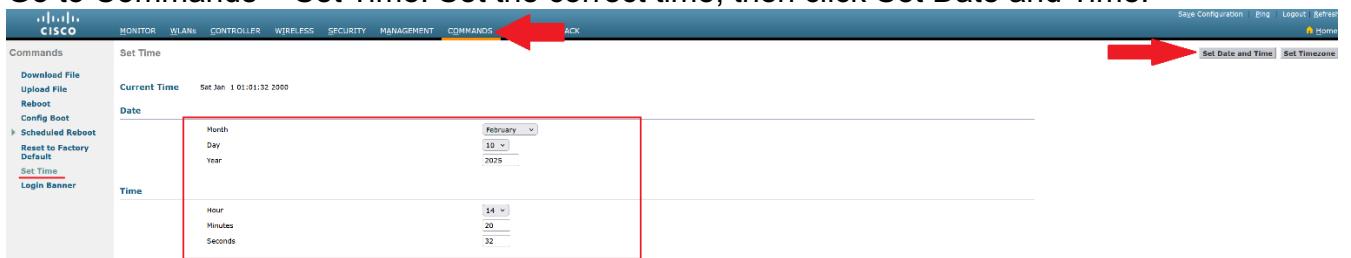
Connect to the WLC's IP address via HTTP and click Login.



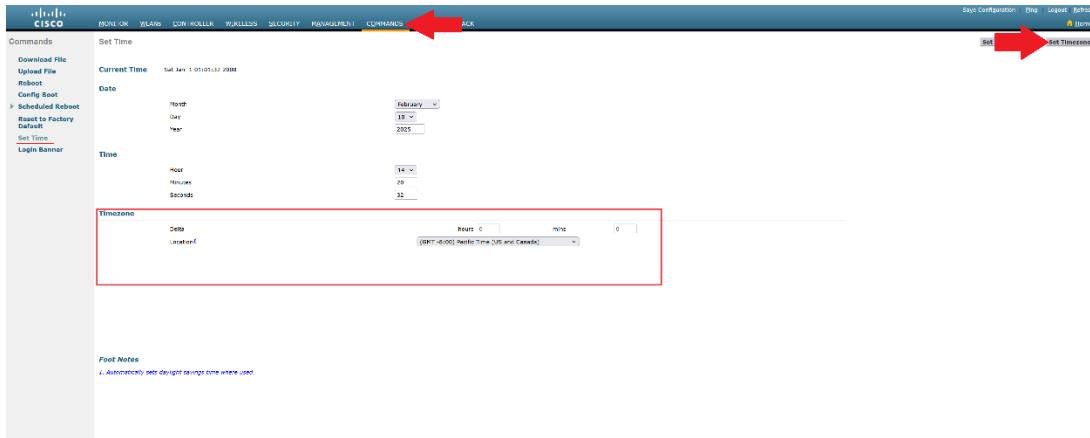
Click Advanced.



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):

```

Feb 16 14:28:48.000: %CAPWAP-5-DTLSREQUEST: DTLS connection request sent peer_ip: 192.168.0.254 peer_port: 5246
Feb 16 14:28:48.000: %CAPWAP-5-CHANGED: CAPWAP changed state to 00
Feb 16 14:28:48.000: %CAPWAP-5-CHANGED: CAPWAP changed state to 10
extracting 1020... (289 bytes)
Image info:
Version suffix: k9w8-mx.153-3.3C14
Image Name: c1140-k9w8-mx.153-3.3C14
Version Directory: c1140-k9w8-mx.153-3.3C14
Ios Image Size: 8684932
IOS Version: 11.0.2(2)AC2
Image Feature: WIRELESS LAN|LAPP
Image Family: C1140
Alarms|Switch Management Version: 8.2.166.0
Extracting files...
c1140-k9w8-mx.153-3.3C14/ (directory) 0 (bytes)
extracting c1140-k9w8-mx.153-3.3C14/8801.htm (157732 bytes)
Feb 16 14:28:49.000: %CAPWAP-5-CHANGED: CAPWAP changed state to 10|perform archive download capwap:c1140 tar file
Feb 16 14:28:49.000: %CAPWAP-5-CHANGED: CAPWAP changed state to 10|Required image not found on AP, download image from controller.
Feb 16 14:28:49.000: %CAPWAP-5-CHANGED: CAPWAP manager state to 10ed0!!!!!!
Feb 16 14:28:49.000: Loading file /c1140...
extracting c1140-k9w8-mx.153-3.3C14/file_hasher... (3030 bytes)
extracting c1140-k9w8-mx.153-3.3C14/img_sign_rel_sha2.cert (1371 bytes)
extracting c1140-k9w8-mx.153-3.3C14/final_hash.sig (51 bytes)
extracting c1140-k9w8-mx.153-3.3C14/info... (283 bytes)
extracting c1140-k9w8-mx.153-3.3C14/final_hash (141 bytes)
extracting c1140-k9w8-mx.153-3.3C14/ (directory) 0 (bytes)
extracting c1140-k9w8-mx.153-3.3C14/html/ (directory) 0 (bytes)
c1140-k9w8-mx.153-3.3C14/html/level1/ (directory) 0 (bytes)
extracting c1140-k9w8-mx.153-3.3C14/html/level1/images/ (directory) 0 (bytes)
extracting c1140-k9w8-mx.153-3.3C14/html/level1/images/liscos-logo-2007.gif (1648 bytes)
extracting c1140-k9w8-mx.153-3.3C14/html/level1/images/background_wel041.jpg (732 bytes)
extracting c1140-k9w8-mx.153-3.3C14/html/level1/images/info.gif (399 bytes)
extracting c1140-k9w8-mx.153-3.3C14/html/level1/images/icon_welcome_01.gif (10671 bytes)!!!
extracting c1140-k9w8-mx.153-3.3C14/html/level1/siteside.js (17250 bytes)
extracting c1140-k9w8-mx.153-3.3C14/html/level1/footer.js (20442 bytes)!!!
extracting c1140-k9w8-mx.153-3.3C14/html/level1/footer.html (2044 bytes)
extracting c1140-k9w8-mx.153-3.3C14/html/level1/footer.html (51 bytes)
extracting c1140-k9w8-mx.153-3.3C14/html/level1/officeExtendap.css (416 bytes)!!!
extracting c1140-k9w8-mx.153-3.3C14/html/level1/officeHome.html (1370 bytes)
extracting c1140-k9w8-mx.153-3.3C14/html/level1/officeIndex.html (653 bytes)
c1140-k9w8-mx.153-3.3C14/html/level15/ (directory) 0 (bytes)
extracting c1140-k9w8-mx.153-3.3C14/html/level15/officeExtendap.html (3150 bytes)!!!
extracting c1140-k9w8-mx.153-3.3C14/html/level15/officeExtendapConfig.html (2364 bytes)
extracting c1140-k9w8-mx.153-3.3C14/html/level15/officeExtendapBanner.htm (7514 bytes)!!!
extracting c1140-k9w8-mx.153-3.3C14/html/level15/officeExtendapSummary.htm (985 bytes)
extracting c1140-k9w8-mx.153-3.3C14/html/level15/officeExtendapXtendapip.htm (921 bytes)
extracting c1140-k9w8-mx.153-3.3C14/1140-k9w8-mx.153-3.3C14/xtendapip.htm (988 bytes)!!!
extracting c1140-k9w8-mx.153-3.3C14/1140-k9w8-mx.153-3.3C14/xtendapdown.html (852672 bytes)!!!
extracting c1140-k9w8-mx.153-3.3C14/1140-k9w8-mx.153-3.3C14/ (852672 bytes)!!!

```

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)

Controller Summary

- Management IP Address: 192.168.0.254 ::/128
- Software Version: 8.2.100.0
- Field Recovery Image Version: 7.0.101.1
- System Name: WLC
- Up Time: 0 days, 1 hours, 29 minutes
- System Time: Mon Feb 10 14:48:21 2025
- Redundancy Mode: N/A
- Internal Temperature: +23 C
- 802.11a Network State: Enabled
- 802.11bgn Network State: Enabled
- Local Mobility Group: asdf
- CPU/G3 Usage: 0%
- Individual CPU Usage: 0% (0%), 0% (1%)
- Memory Usage: 35%
- Fan Status: 3500 rpm

Access Point Summary

Total	Up	Down	
802.11a/n/ac Radios	1	1	Detail
802.11bgn Radios	1	1	Detail
Dual-Band Radios	0	0	Detail
All APs	1	1	Detail

Client Summary

Current Clients	Up	Detail
0	0	Detail
Excluded Clients	0	Detail
Detailed Clients	0	Detail

[View All](#)
This page refreshes every 30 seconds.

Next, go to Controller > Interfaces > New.

Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
esxhosttest	99	192.168.0.254	Static	Enabled	::/128
vlan10	N/A	192.0.2.1	Static	Not Supported	

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

Interfaces > New

Interface Name	<input type="text" value="Guest VLAN"/>
VLAN Id	<input type="text" value="10"/>

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

Interface Address

VLAN Identifier	10
IP Address	192.168.10.254
Netmask	255.255.255.0
Gateway	192.168.10.1

DHCP Information

Primary DHCP Server	192.168.10.1
Secondary DHCP Server	
DHCP Proxy Mode	Global
Enable DHCP Option 82	<input type="checkbox"/>

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

Interfaces > New

Interface Name	psk vlan
VLAN Id	20

Interface Address

VLAN Identifier	20
IP Address	192.168.20.254
Netmask	255.255.255.0
Gateway	192.168.20.1

DHCP Information

Primary DHCP Server	192.168.20.1
Secondary DHCP Server	
DHCP Proxy Mode	Global
Enable DHCP Option 82	<input type="checkbox"/>

Interfaces > New

Interface Name	<input type="text" value="enterprise vlan"/>
VLAN Id	<input type="text" value="30"/>

Interface Address

VLAN Identifier	<input type="text" value="30"/>
IP Address	<input type="text" value="192.168.30.254"/>
Netmask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.30.1"/>

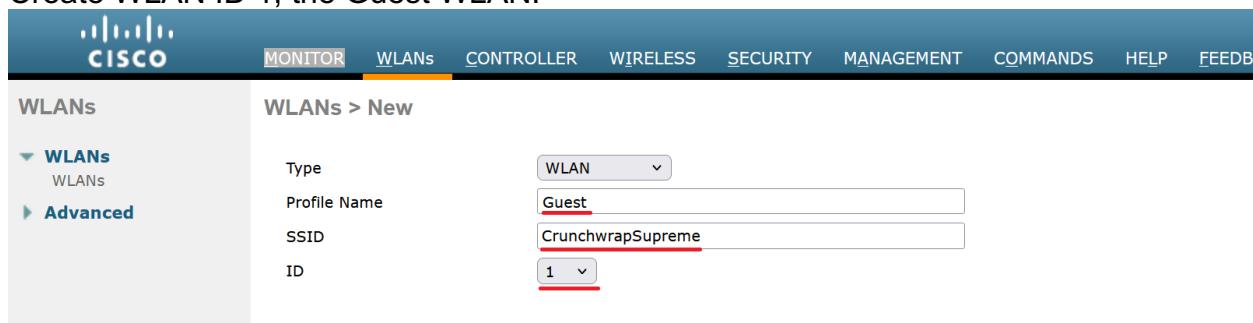
DHCP Information

Primary DHCP Server	<input type="text" value="192.168.30.1"/>
Secondary DHCP Server	<input type="text"/>
DHCP Proxy Mode	<input type="button" value="Global"/>
Enable DHCP Option 82	<input type="checkbox"/>

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.

WLANs > New

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

WLANS > Edit 'PSK WLAN'

General	Security	QoS	Policy-Mapping	Advanced
Profile Name	PSK WLAN			
Type	WLAN			
SSID	NachosBellGrande			
Status	<input checked="" type="checkbox"/> Enabled			
Security Policies	[WPA2][Auth(PSK)] (Modifications done under security tab will appear after applying the changes.)			
Radio Policy	All			
Interface/Interface Group(G)	psk vlan			
Multicast Vlan Feature	<input type="checkbox"/> Enabled			
Broadcast SSID	<input checked="" type="checkbox"/> Enabled			
NAS-ID	none			

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

General	Security	QoS	Policy-Mapping	Advanced
Layer 2	Layer 3	AAA Servers		
PMF: Disabled				
WPA+WPA2 Parameters				
<input type="checkbox"/> WPA Policy <input checked="" type="checkbox"/> WPA2 Policy <input checked="" type="checkbox"/> WPA2 Encryption: AES <input type="checkbox"/> TKIP <input type="checkbox"/> OSEN Policy				
Authentication Key Management: 12				
802.1X <input type="checkbox"/> Enable CCKM <input type="checkbox"/> Enable PSK <input checked="" type="checkbox"/> Enable FT 802.1X <input type="checkbox"/> Enable FT PSK <input type="checkbox"/> Enable PSK Format: ASCII <input type="password" value="*****"/> WPA gtk-randomize State: <input type="checkbox"/> Disable				

Click Apply.



Next, Create the Enterprise WLAN.

WLANS > New

Type	WLAN
Profile Name	Enterprise WLAN
SSID	CheesyGorditaCrunch
ID	3

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

Under Security > Layer 2, set the Layer 2 security 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.

RADIUS Authentication Servers > New

Server Index (Priority)	1
Server IP Address(Ipv4/Ipv6)	192.168.0.200
Shared Secret Format	ASCII
Shared Secret	*****
Confirm Shared Secret	*****
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for CoA	Disabled
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
Management Retransmit Timeout	2 seconds
IPSec	<input type="checkbox"/> Enable

Click Apply.

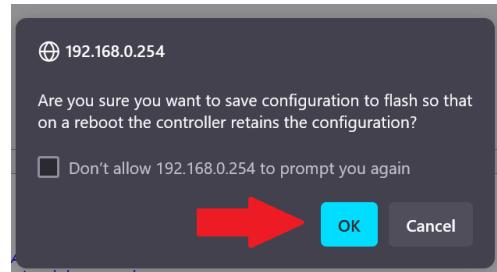


Apply

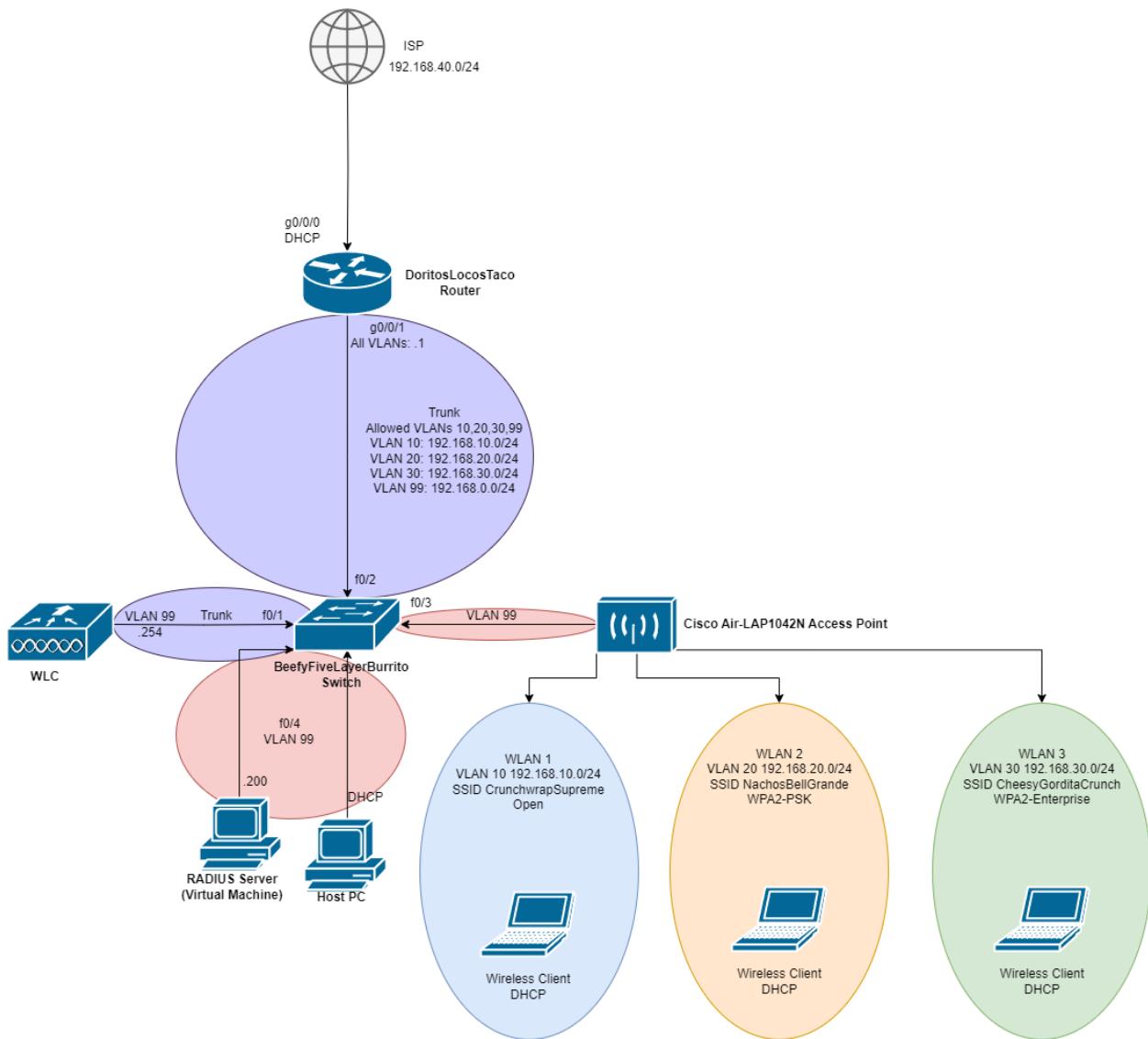
Finally, click Save Configuration.



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.

Interfaces > Edit

General Information	
Interface Name	Guest VLAN
MAC Address	00:9e:1e:8f:b0:20
Configuration	
Guest Lan	<input checked="" type="checkbox"/>
NAS-ID	none
Physical Information	
Port Number	0
Backup Port	0
Active Port	0
Interface Address	
VLAN Identifier	10
DHCP Proxy Mode	Global
Enable DHCP Option 82	<input type="checkbox"/>

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.