



Alysia Chen

CCNP 3-4

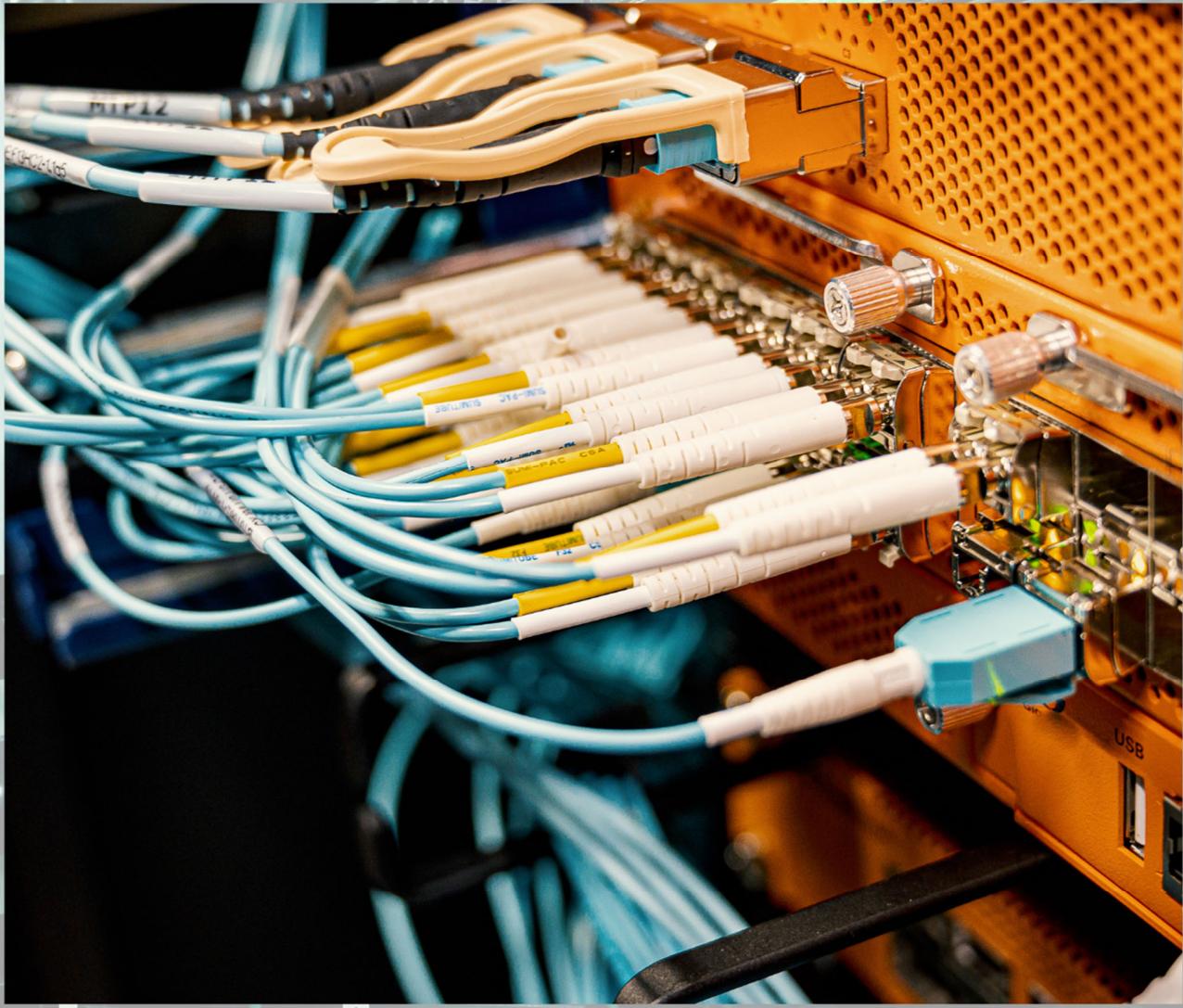
Networking
Academy



Table of Contents

Lab 1	1
Lab 2	16
Lab 3	25
Lab 4	43
Lab 5	59
Lab 6	129
Lab 7	190
Lab 8	201
Lab 9	217

Lab 1: Windows Format and Installation



PURPOSE:

To learn how to set up operating systems.

BACKGROUND INFORMATION ON LAB CONCEPTS:

An operating system is a program that, after being booted, is used to manage other computer programs. In our case, we install Windows.

Windows is a Microsoft-proprietary operating system. First released in 1985, the latest version of Windows is now Windows 11. Additionally, Windows is the most popular operating system in the world (with 70% of the market share). Windows 11 was released in 2021.

Putty is used to access networking devices via SSH or Telnet. SSH is used to securely send commands over an insecure network, while Telnet does not provide this secure feature. This will facilitate configuring networking devices and the network in general, among other tasks important in Cisco Networking Academy.

Office 365 is used for many Microsoft Office programs in the classroom setting. For example, it contains Word (which is used to write documents), Excel (which is used to make spreadsheets), Outlook (which is used to communicate via electronic mail), among others. In this class, it is important to write lab writeups, which will rely heavily on applications like Microsoft Word.

Lenovo Commercial Vantage is used for configuring Windows 10 and 11. It is where updates are checked and run.

LAB SUMMARY:

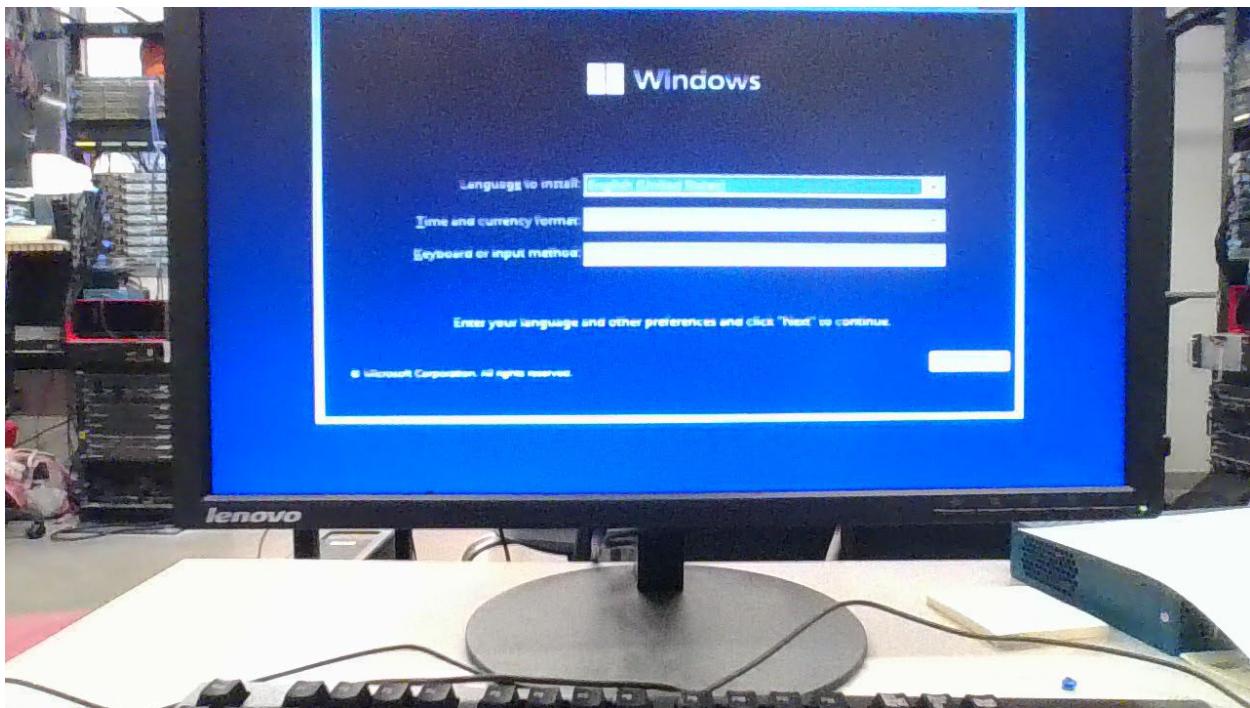
Install operating system (Windows), install Putty, install Office 365, and install Lenovo Commercial Vantage.

LAB COMMANDS:

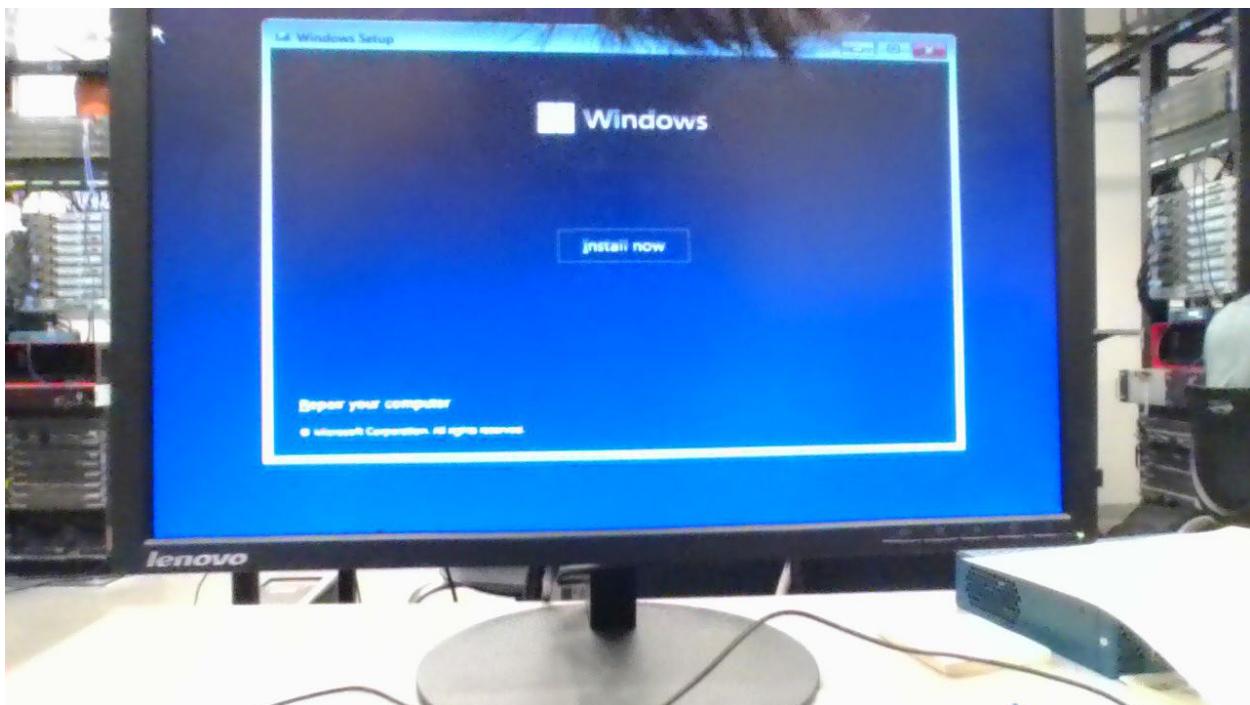
First, plug the USB as well as the drive into the computer. Start the computer, spamming the F12 key.

After a while, you will be taken to this page:

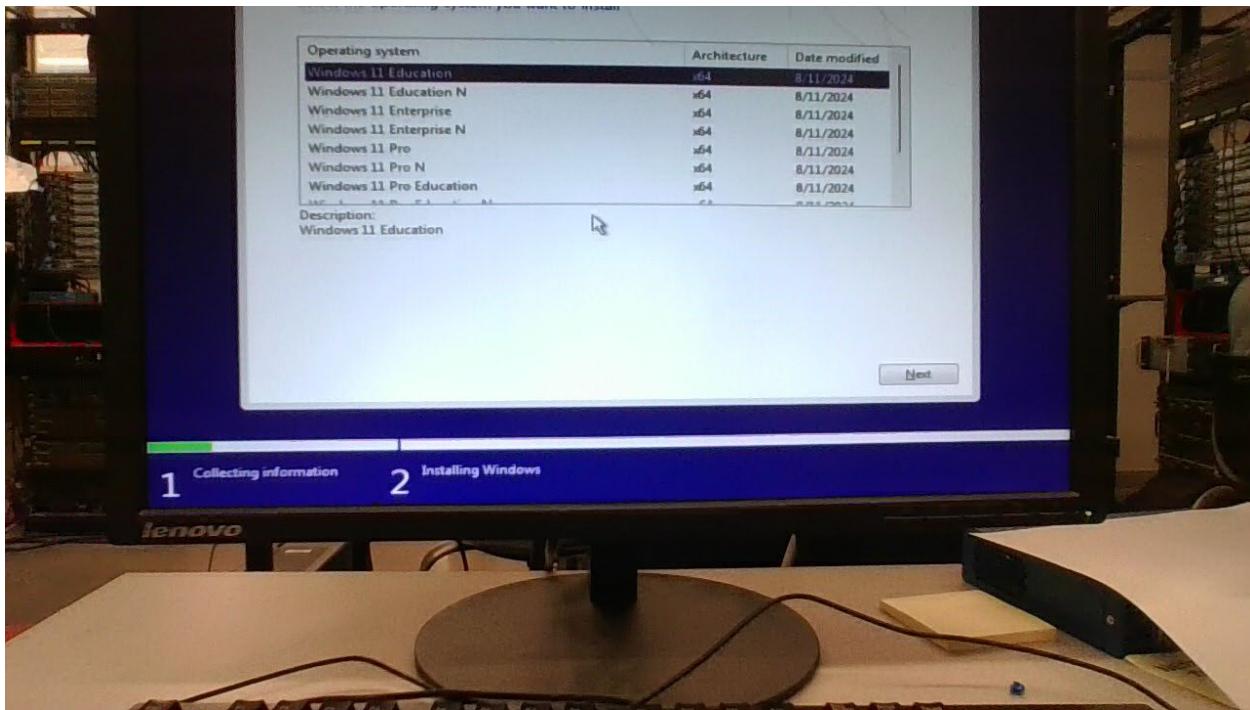




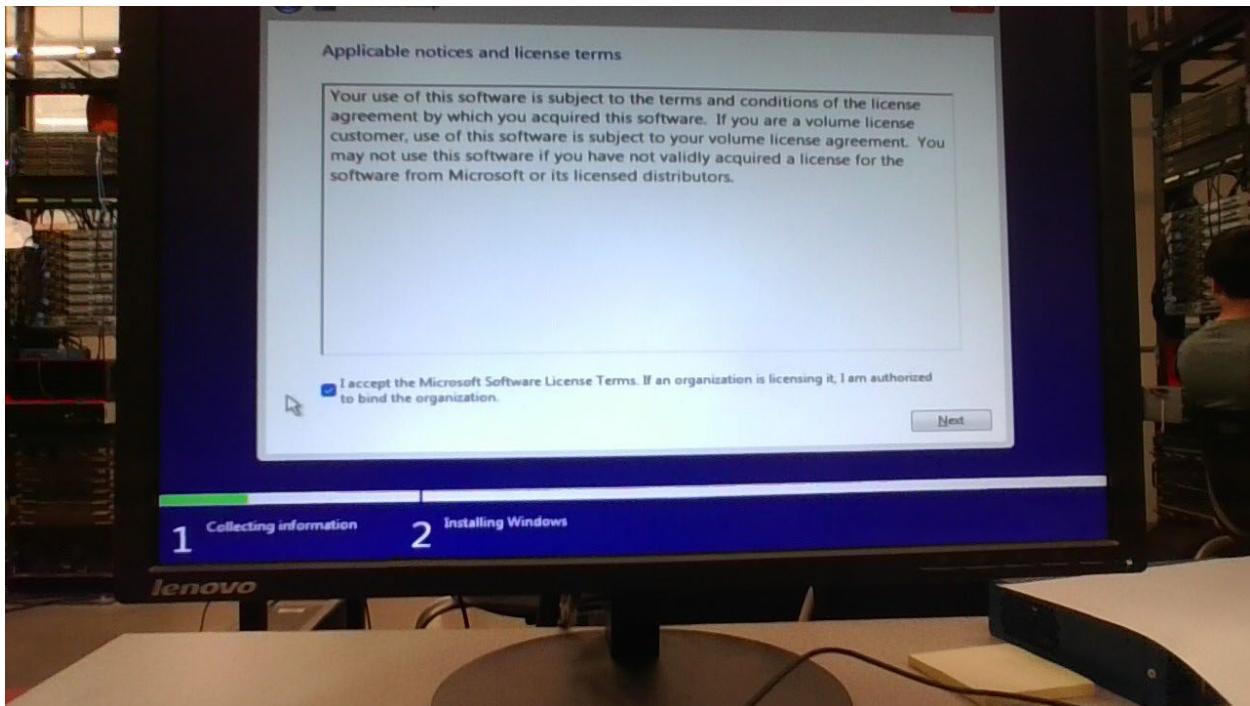
Select your language preference and click next.



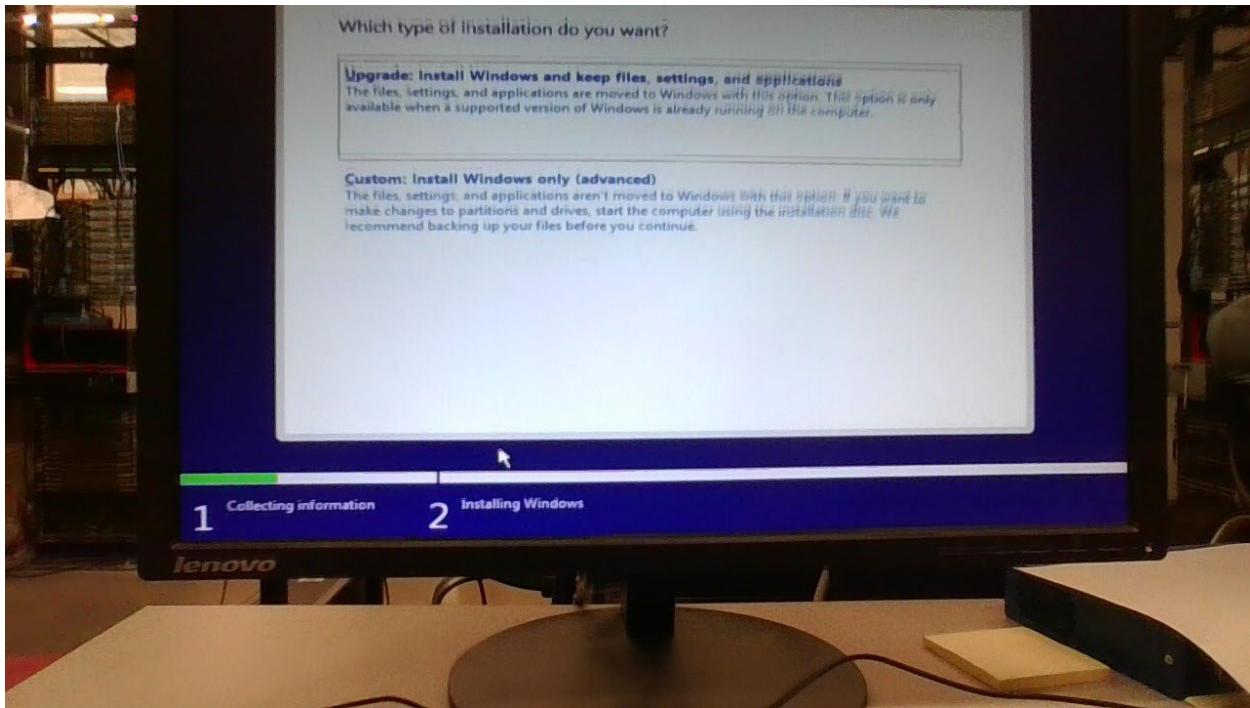
Click "Install Now". After a while, a new page will load.



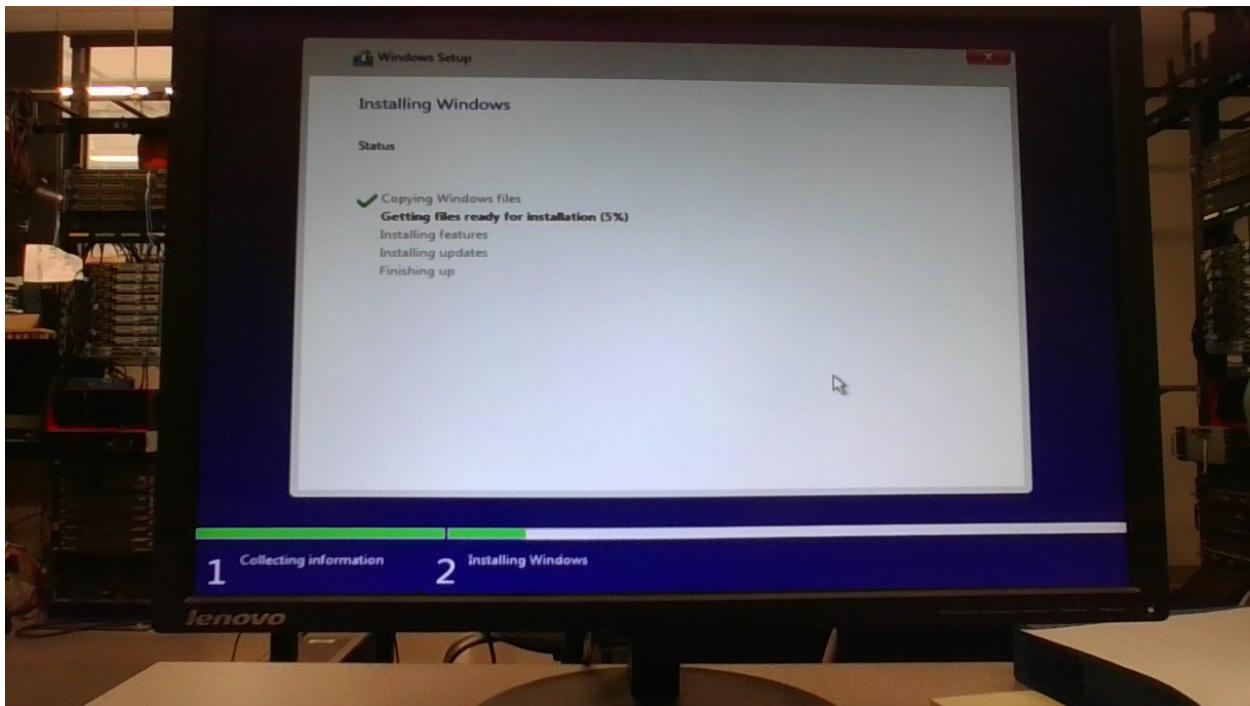
From the options above, select the Windows 11 Education option.



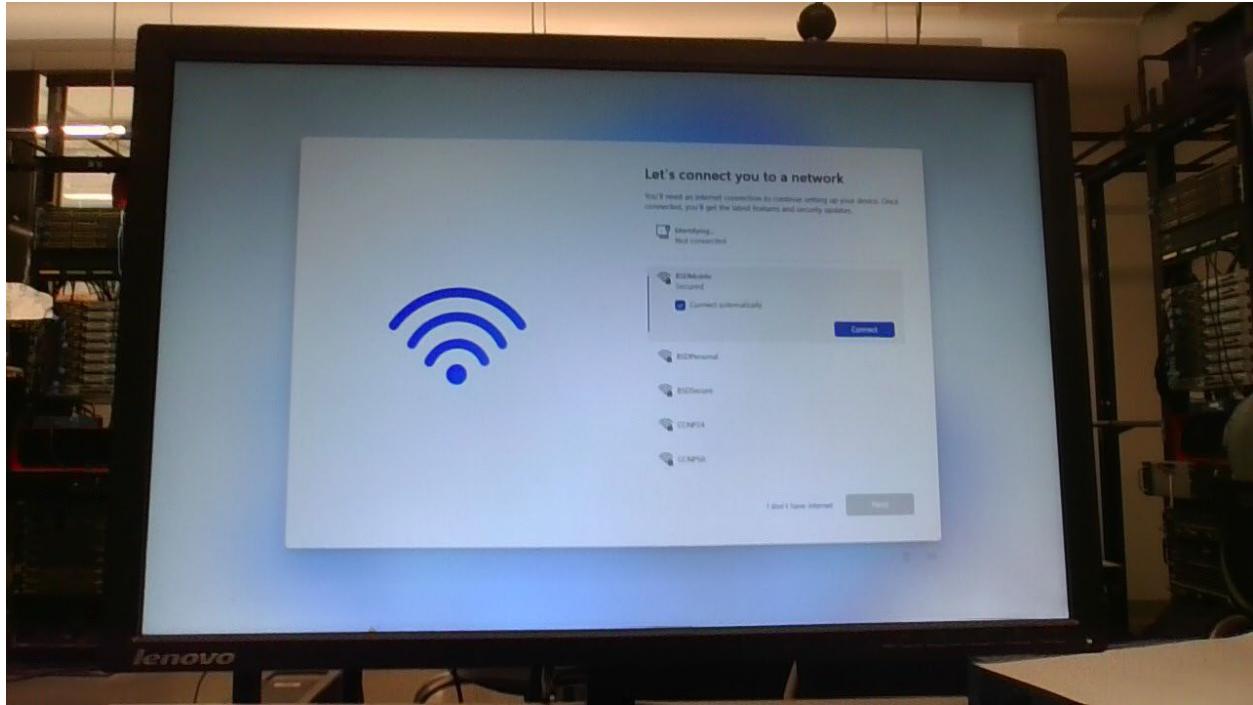
Click next.



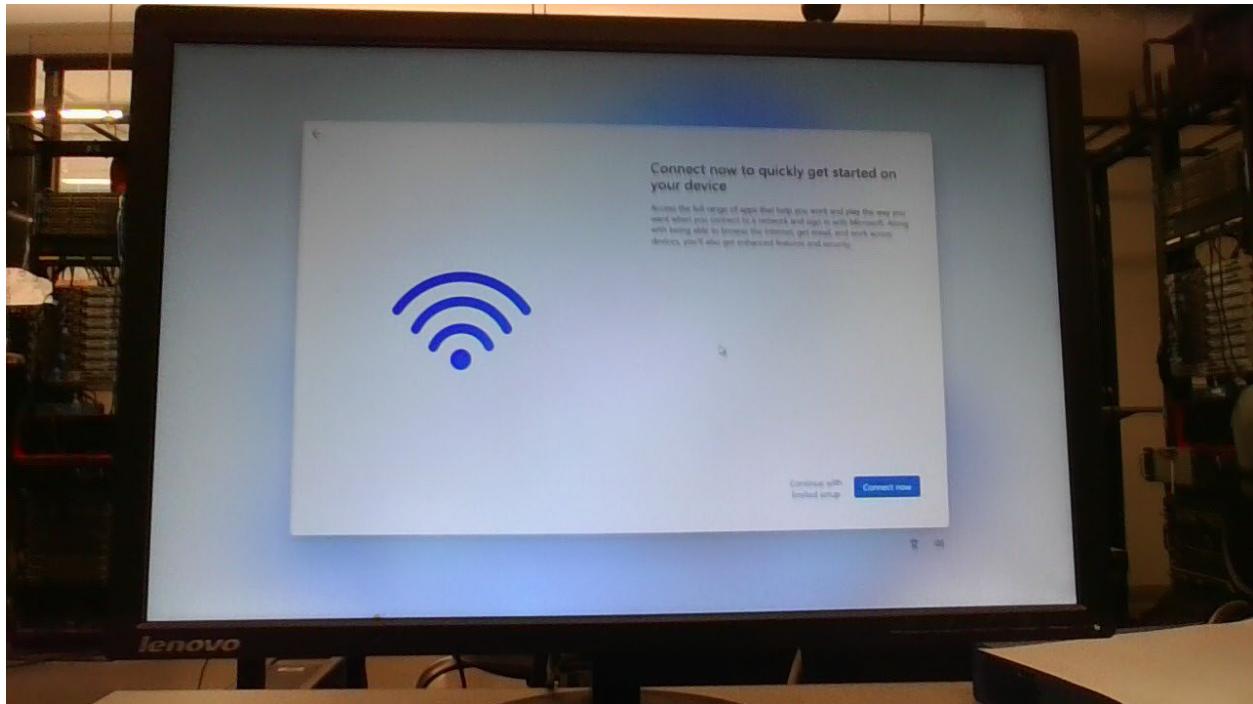
Click on “custom”.



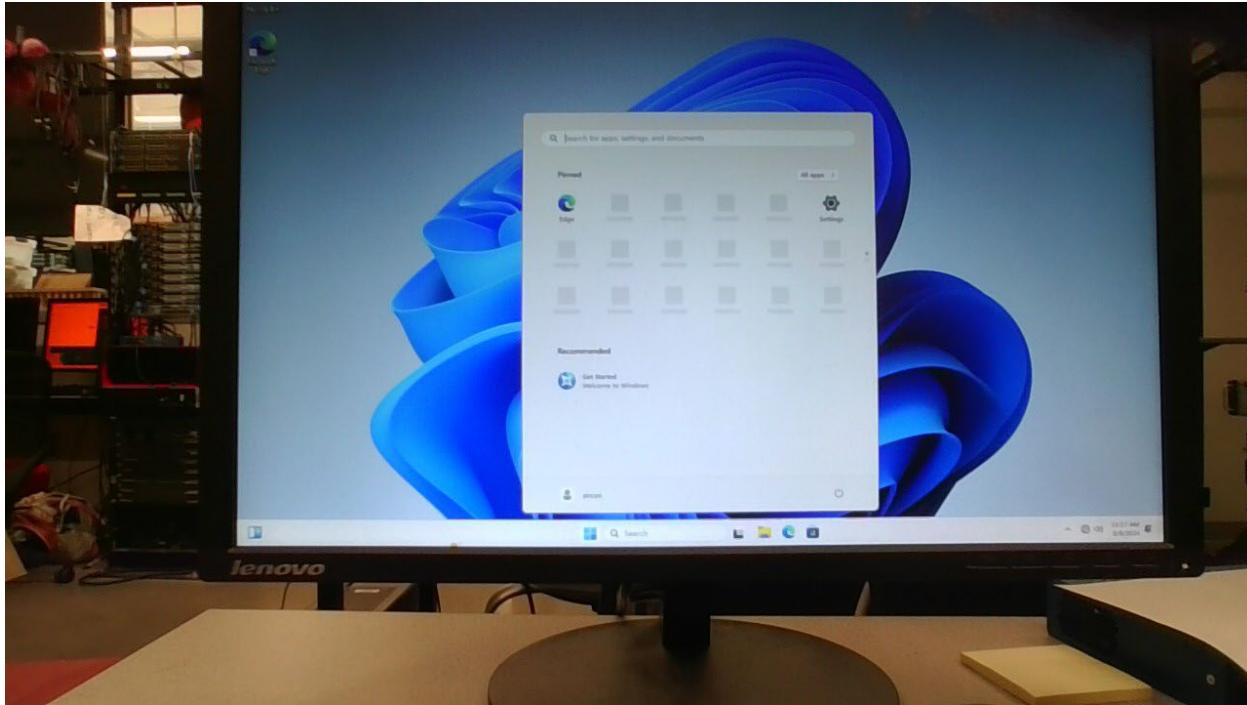
Windows is installing!



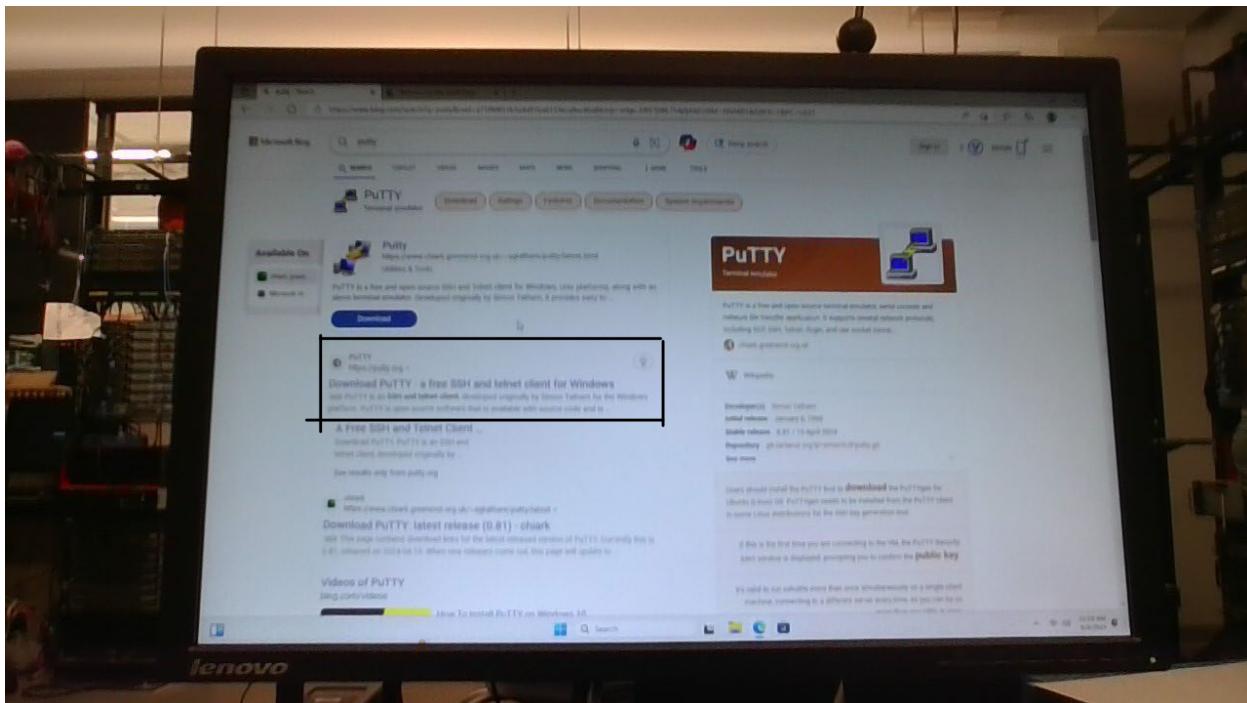
Do not connect to network. Click on “I don’t have internet” at the bottom right.



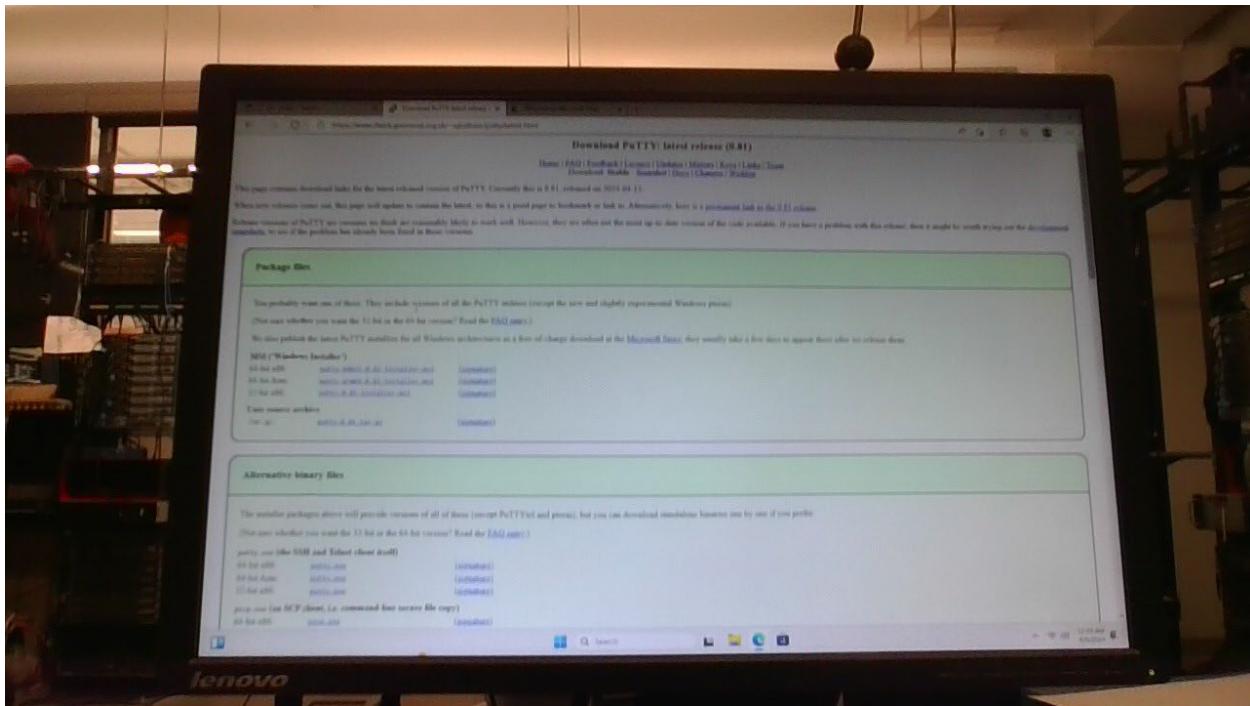
Click “continue with limited settings”.



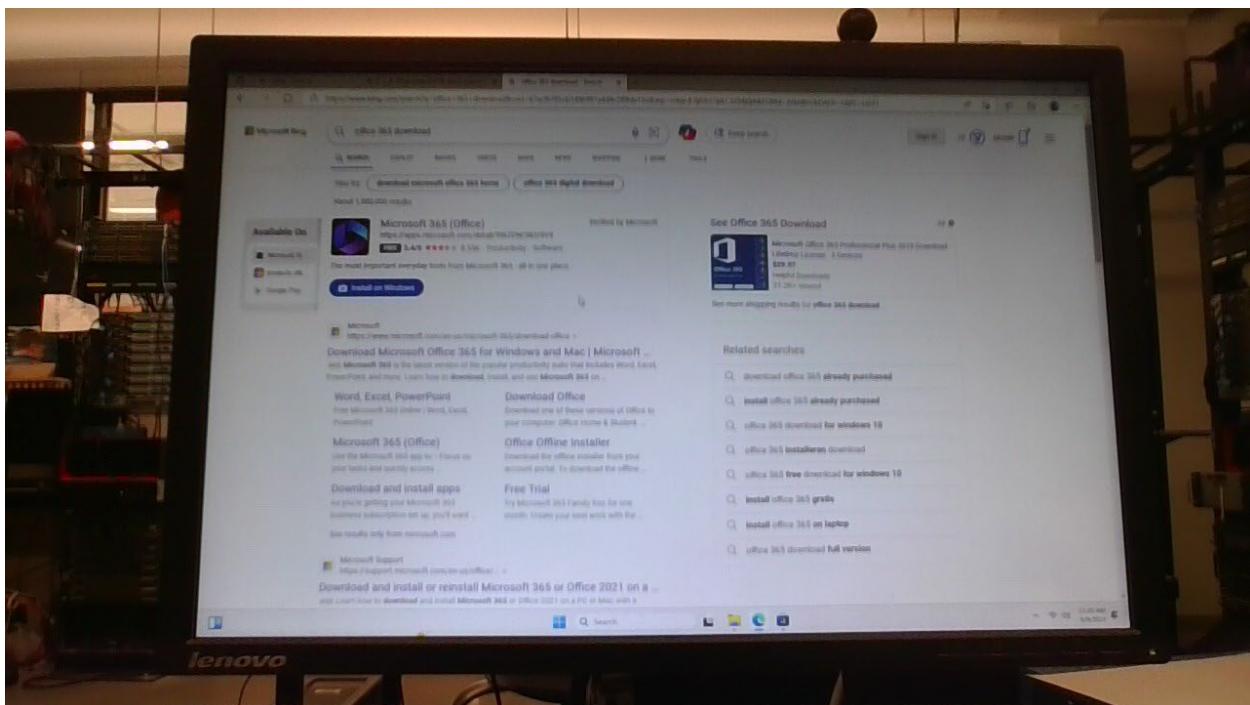
Your computer should start up now!



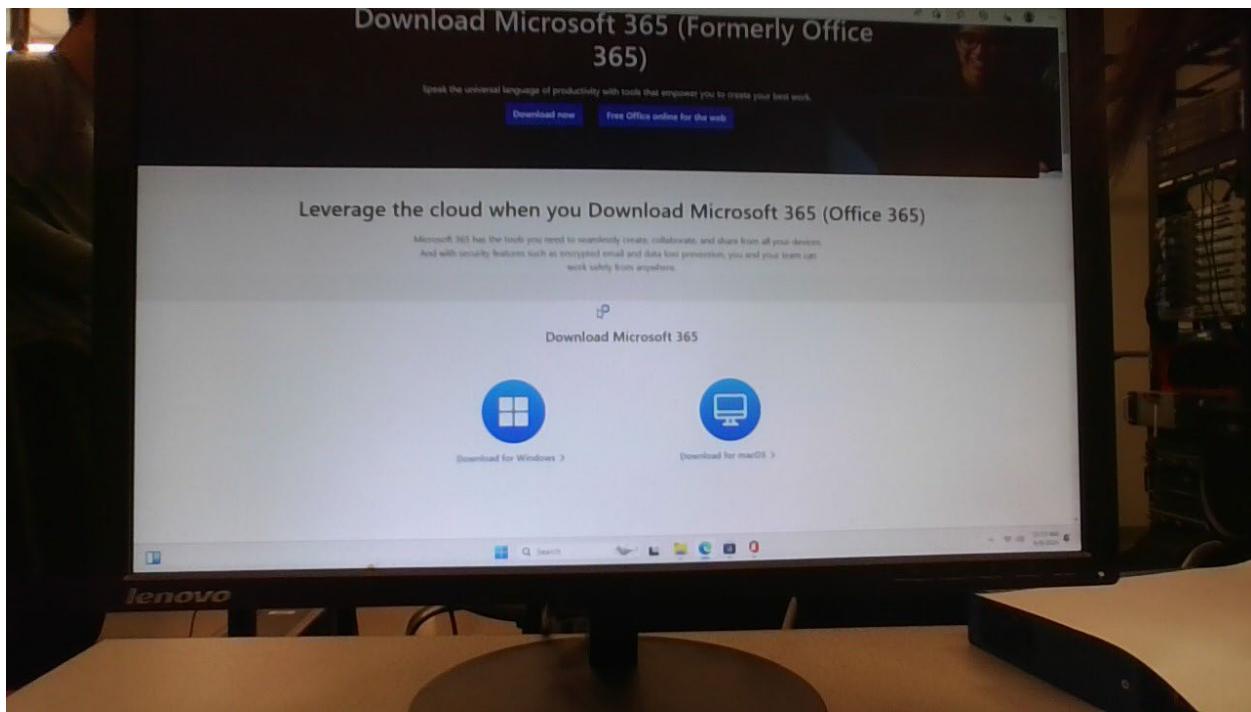
Open Microsoft Edge and search for “PuTTY”. Click on the boxed hyperlink.



Download the very first option on the webpage.

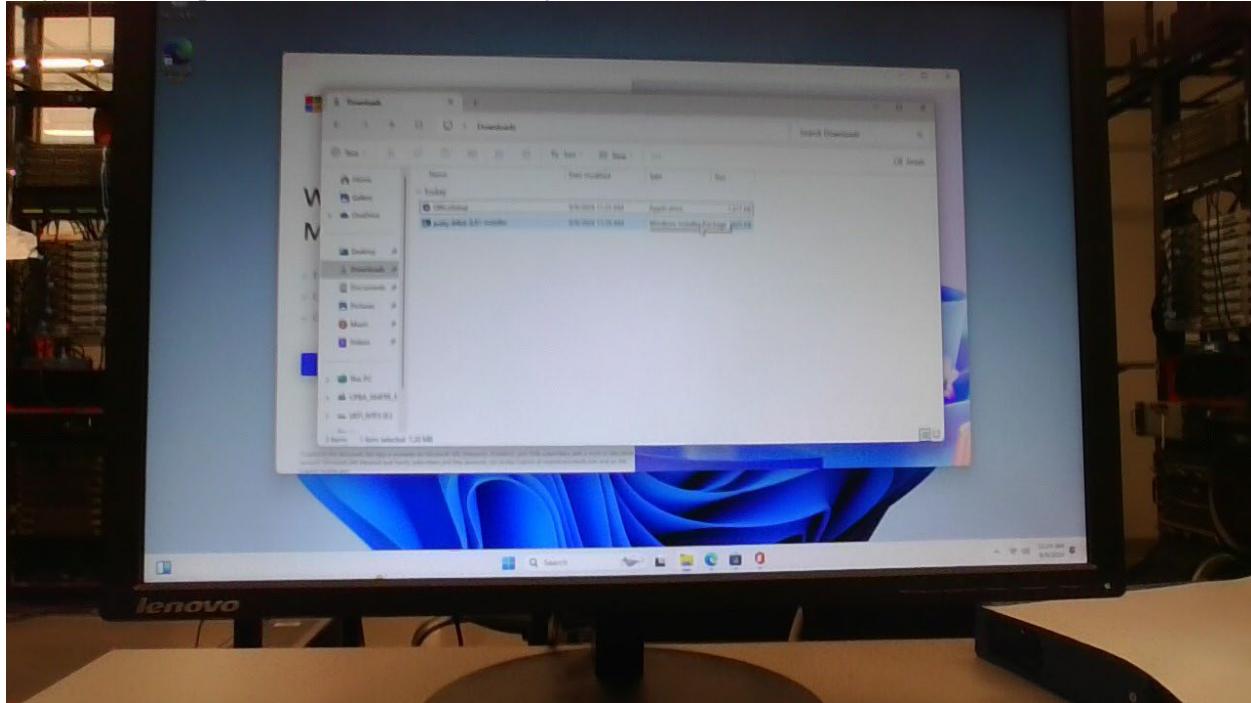


Search for Office 365 and download Microsoft Office 365 for Windows.

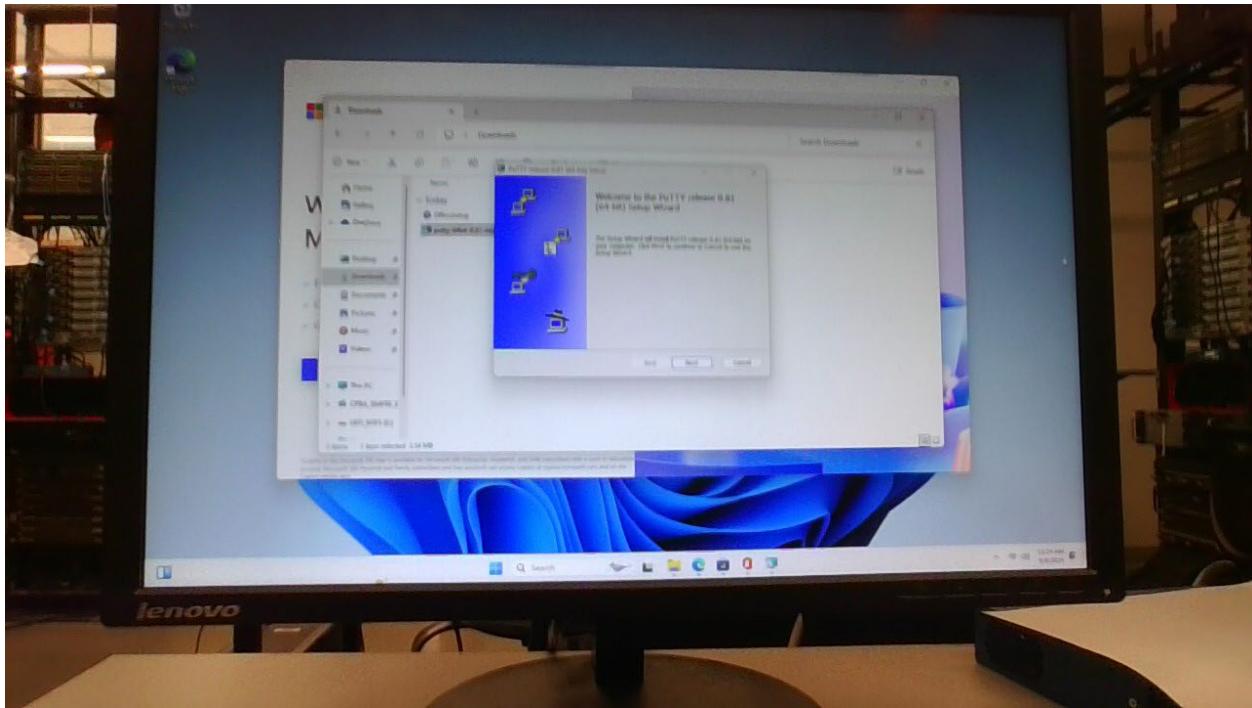


You should reach the page shown above.

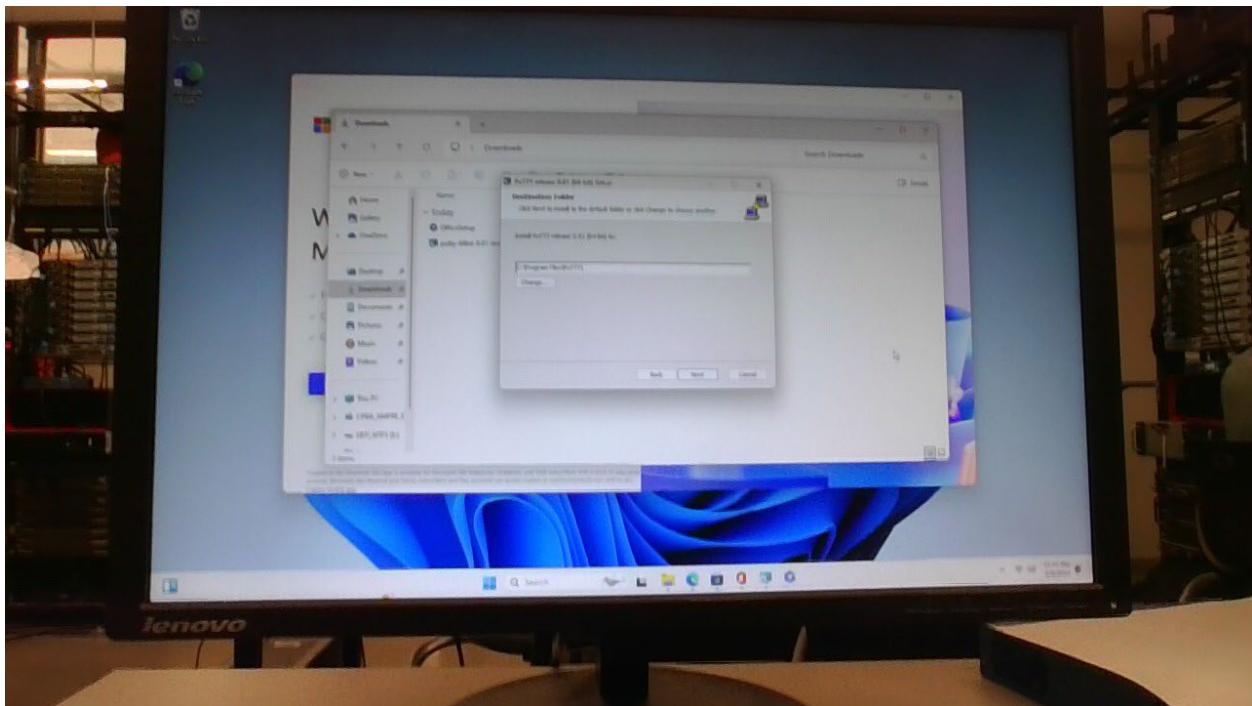
In your File Explorer downloads section, you should see this:



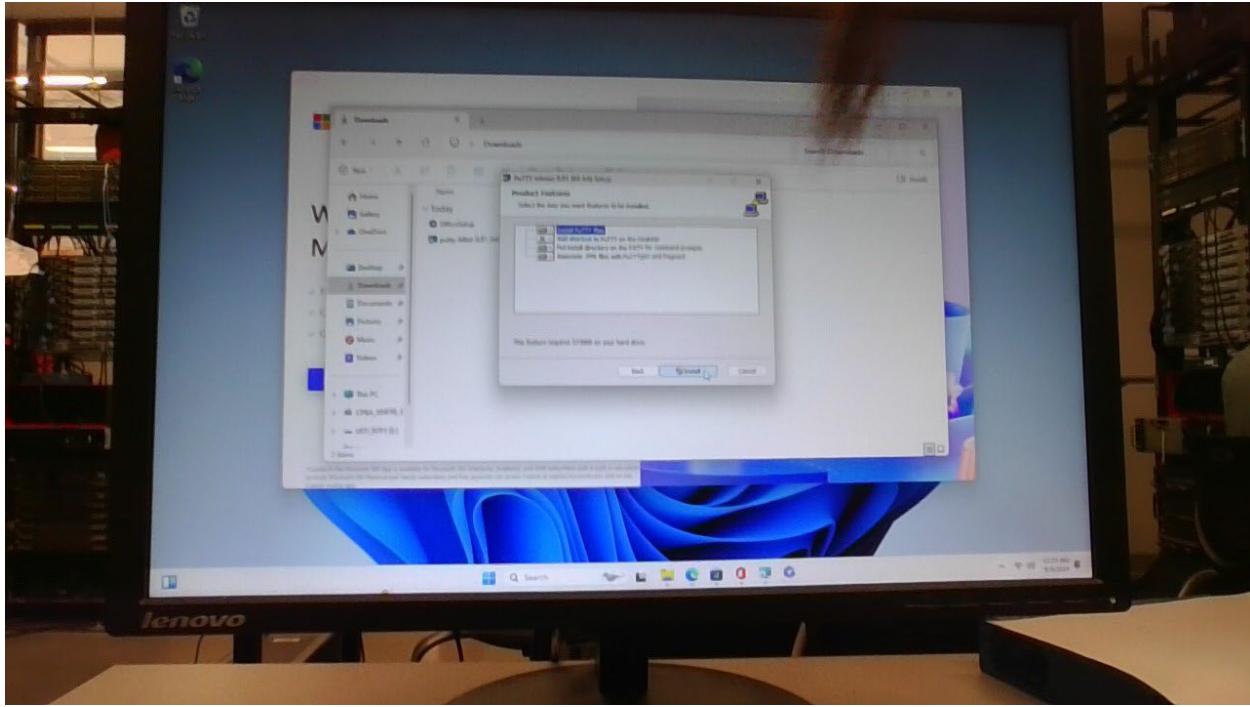
Open both files to start the setup process for PuTTY and Office 365.



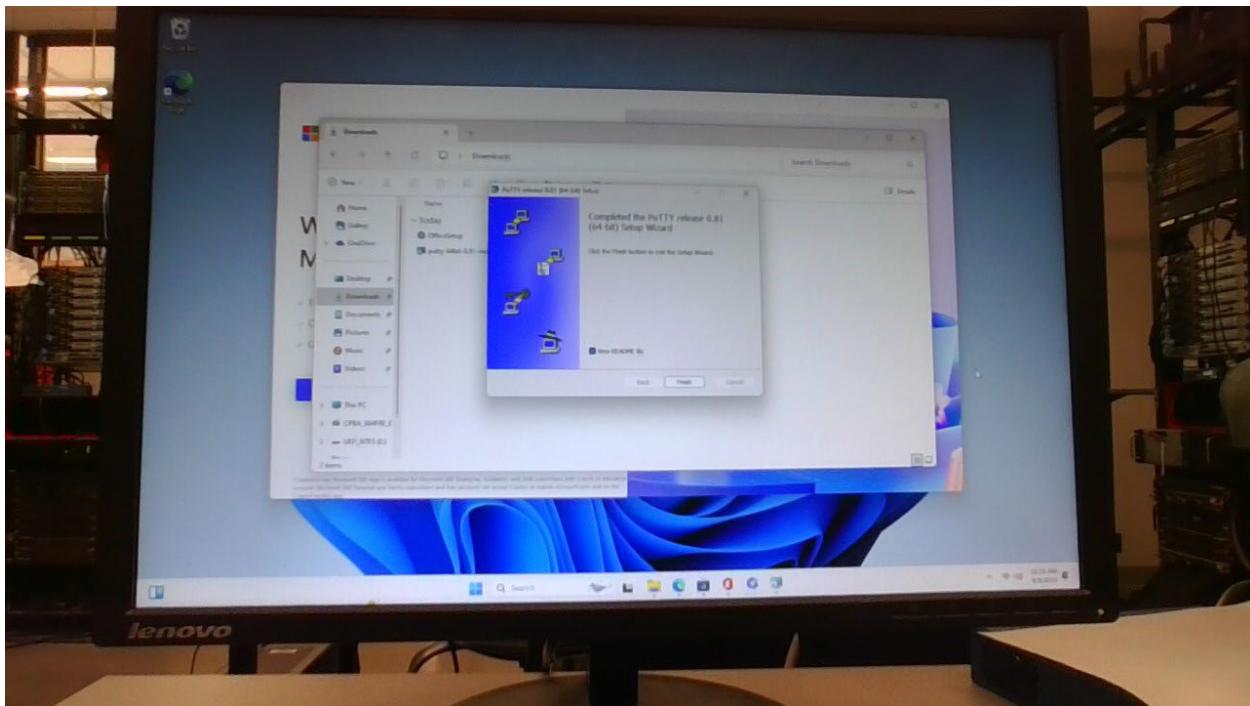
Click next.



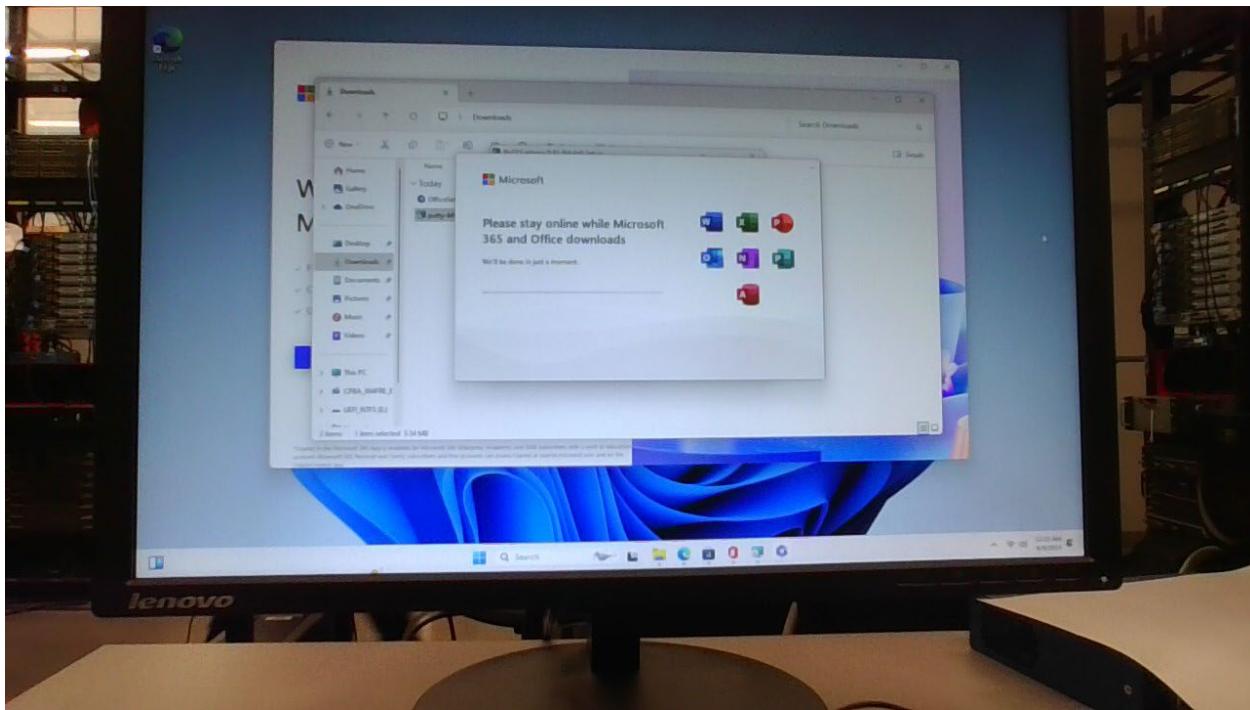
Click next.



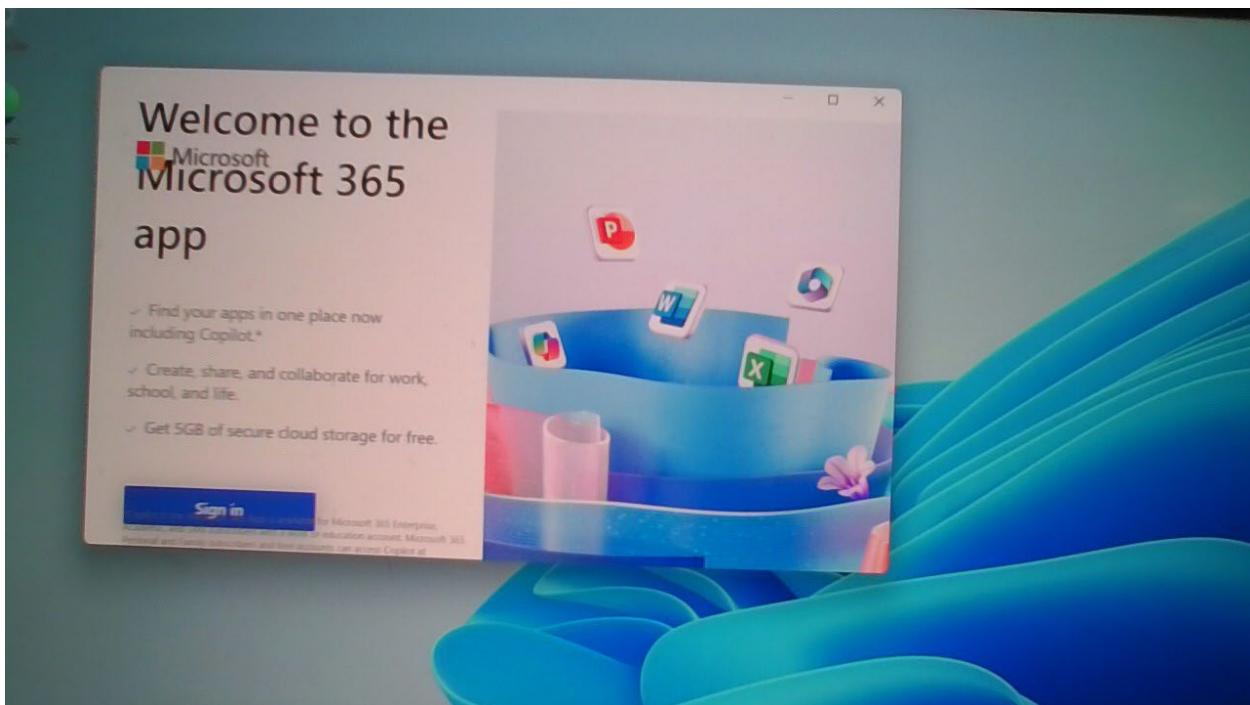
Click install.

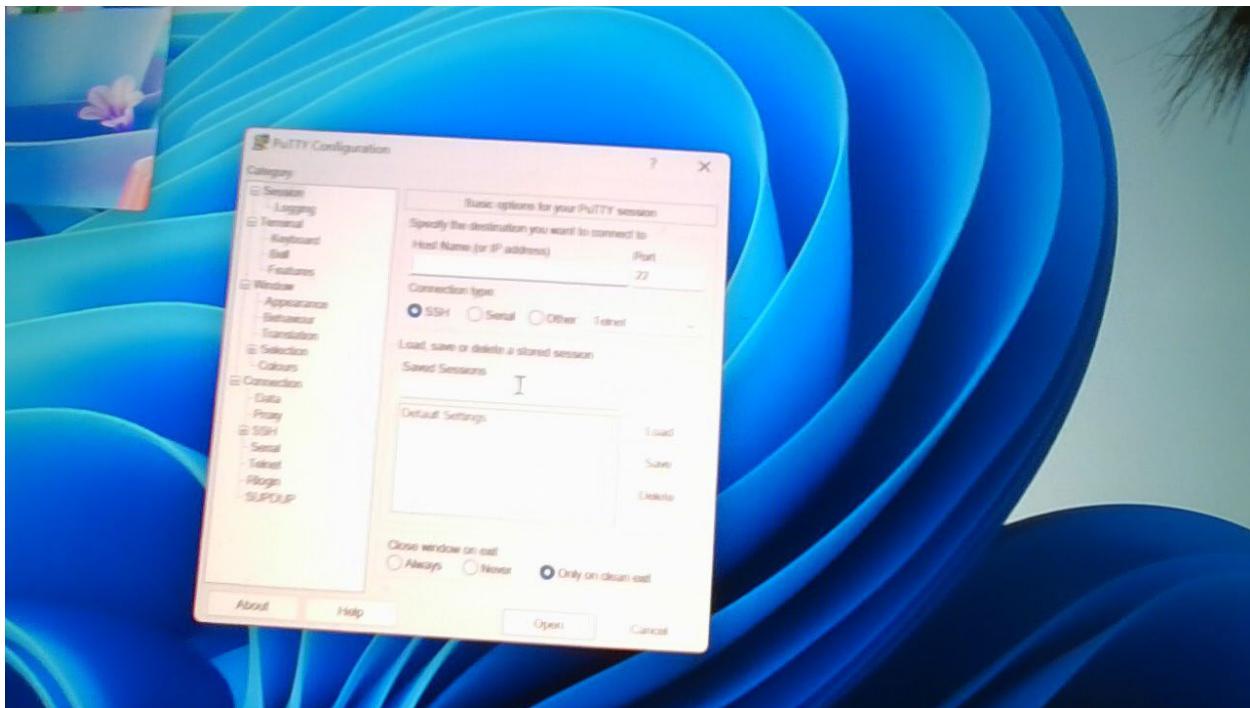


Click finish.

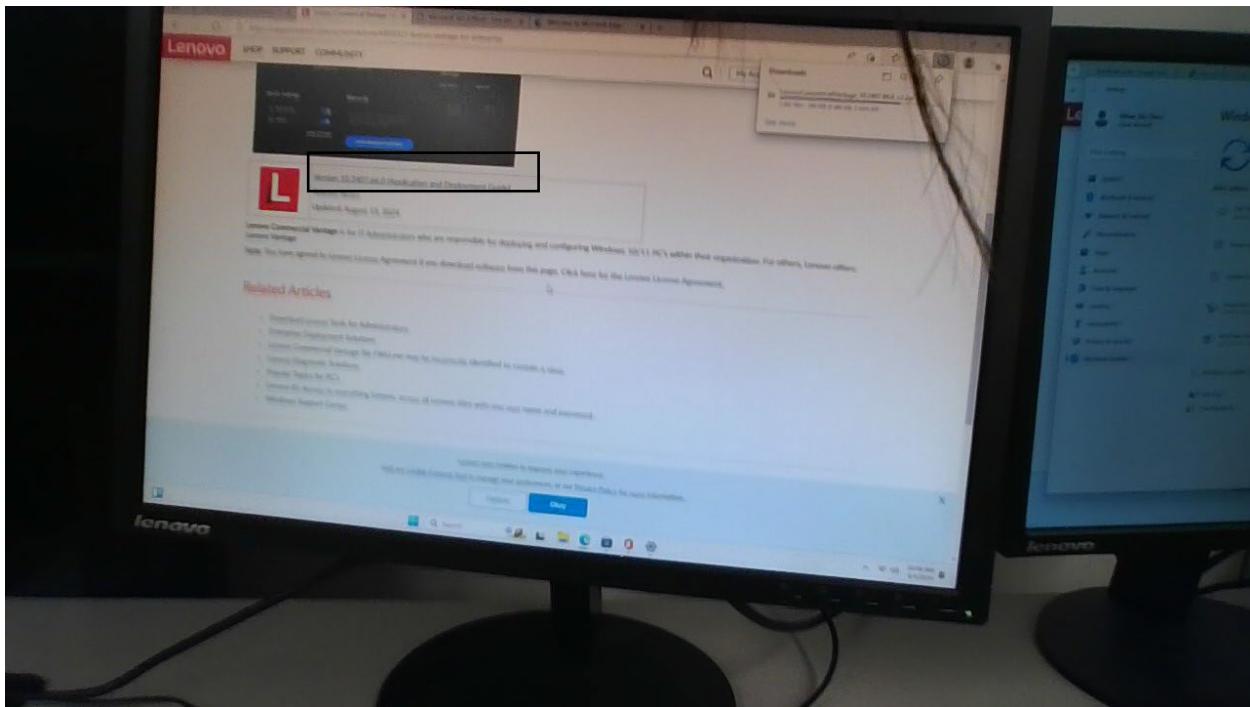


Wait for Office 265 to fully download. Once PuTTY and Office 365 are installed, click allow changes to the computer when prompted. Check to make sure you can make open the two applications, as shown below:





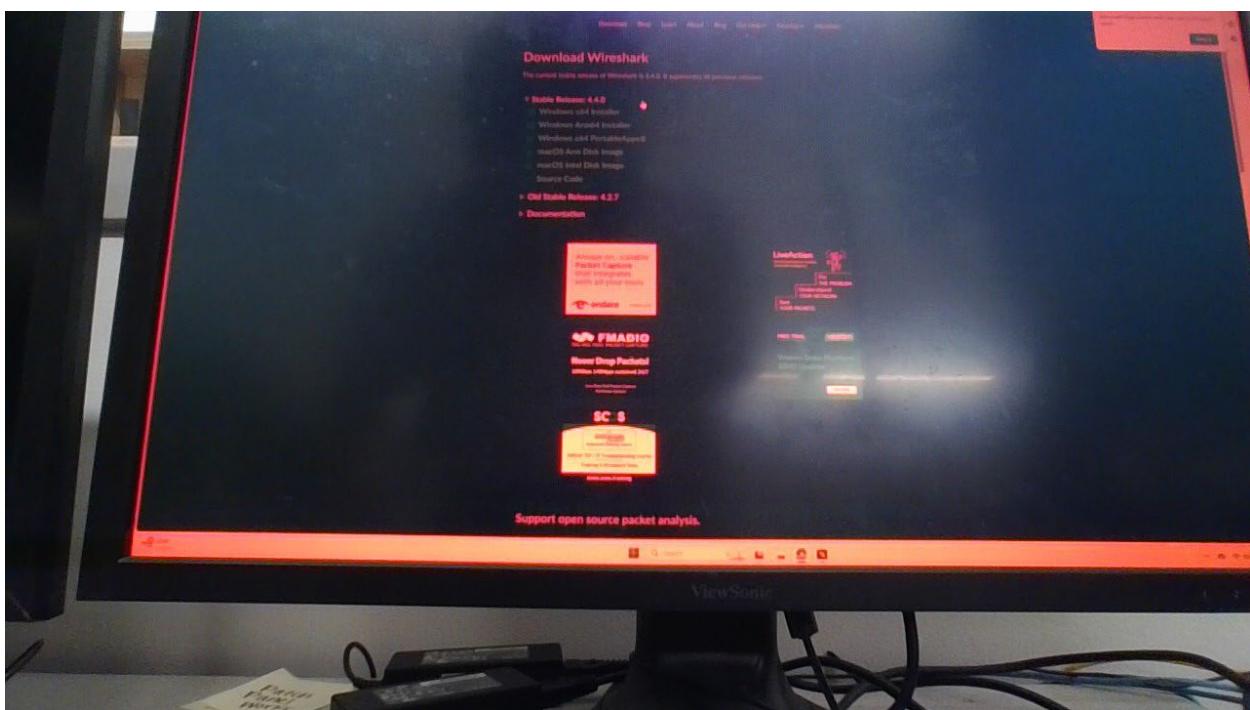
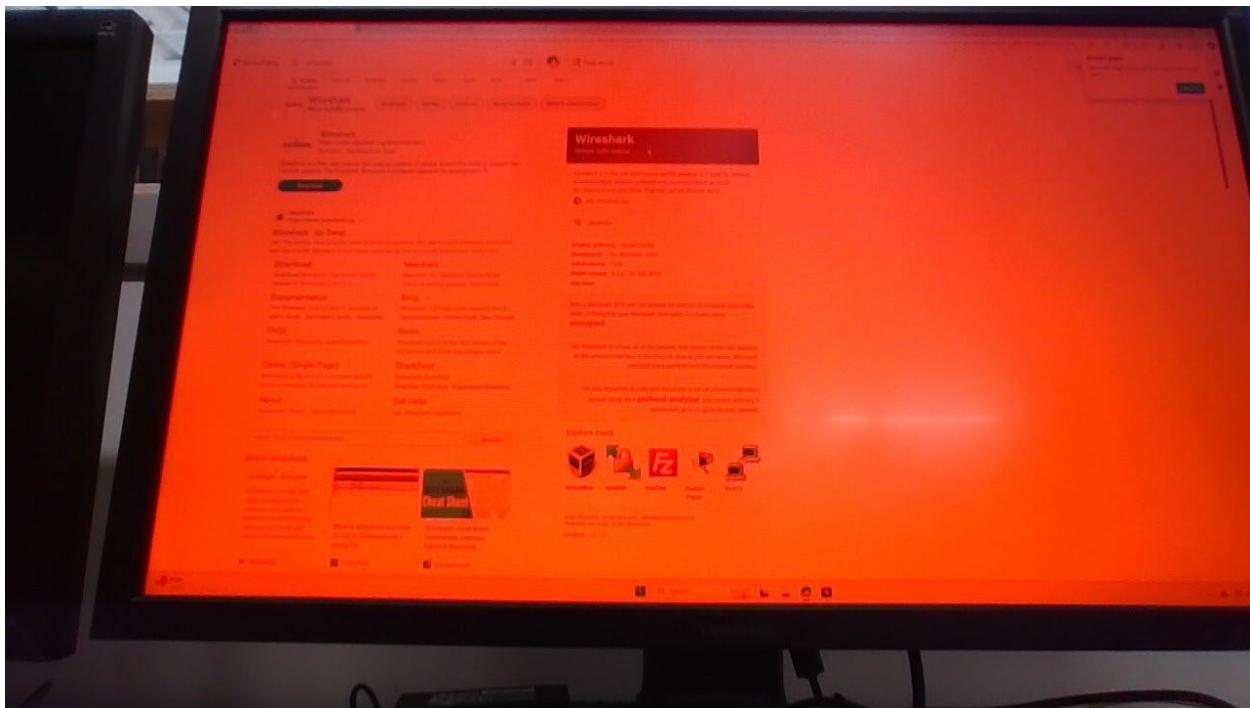
Next, search on Microsoft Edge for Lenovo Commercial Vantage. Install the application the same way PuTTY and Office 365 were installed.



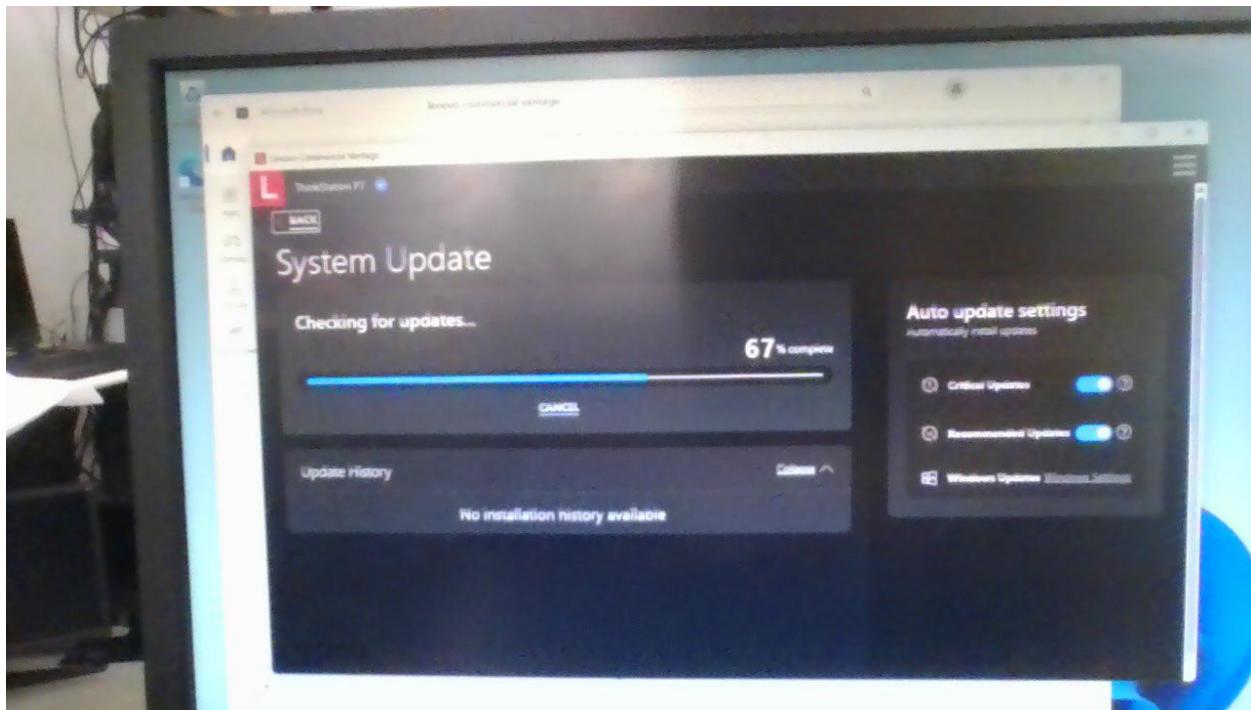
Afterwards, install Wireshark by searching for it on Microsoft Edge, clicking on the Windows x64 Installer option, opening the file, and clicking next for all options presented.



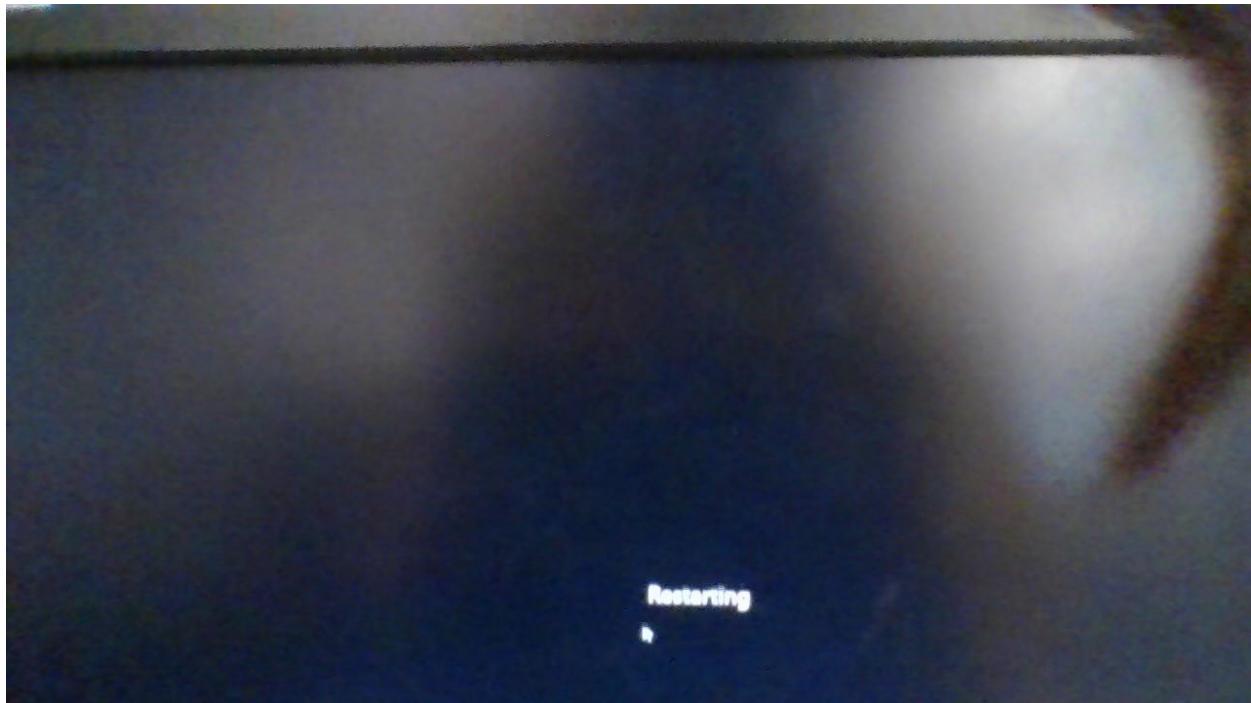
Alysia Chen



Click on the boxed hyperlink to start the download. However, I found downloading through Microsoft Store (which is already installed) to be much easier, so consider downloading through there instead.



Check for updates using Lenovo Commercial Vantage and install as necessary. You may need to restart.



PROBLEMS

To use a local Microsoft account, we had to select “I don’t have internet” option during the initial setup, which was confusing, and then later manually connect.

I found installing the Lenovo Commercial Vantage using Microsoft Edge to be confusing; however, using the Microsoft Store facilitated the process.

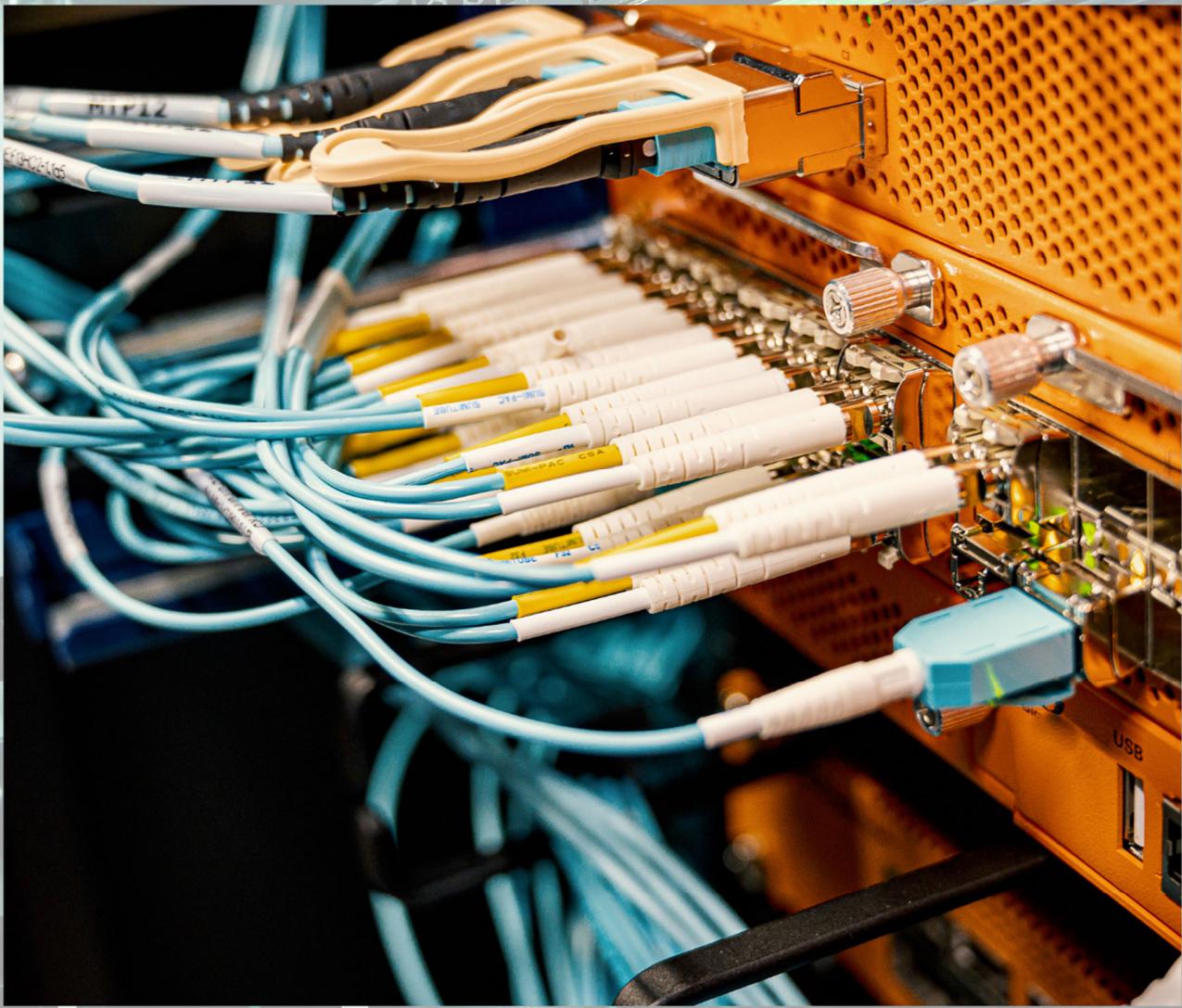
While updating, one of the desktops would not turn on after restarting, so I had to use another computer.

CONCLUSION

I learned how to setup a computer in its most basic form. However, there were some challenges, and I’m glad I was able to troubleshoot all of them.



Lab 2: Multi-Area OSPF



PURPOSE:

Review how to configure OSPFv2 and OSPFv3 (multiarea) and understand how to use a multi-layer switch as part of the configuration.

BACKGROUND INFORMATION ON LAB CONCEPTS:

OSPF is a routing protocol that uses the concept of areas. A network administrator can divide the routing domain into distinct areas that help control routing and update traffic, increasing efficiency.

OSPF, which stands for Open Shortest Path First, was developed as an alternative for the Routing Information Protocol (RIP). OSPF offers faster network convergence and can scale to much larger network implementations.

OSPF is able to detect changes in network topology within seconds. Using Dijkstra's algorithm, OSPF can compute the shortest path for each route. It calculates link metrics—helping judge the quality of potential links—based on distance of a router, amount of data, and link availability and reliability.

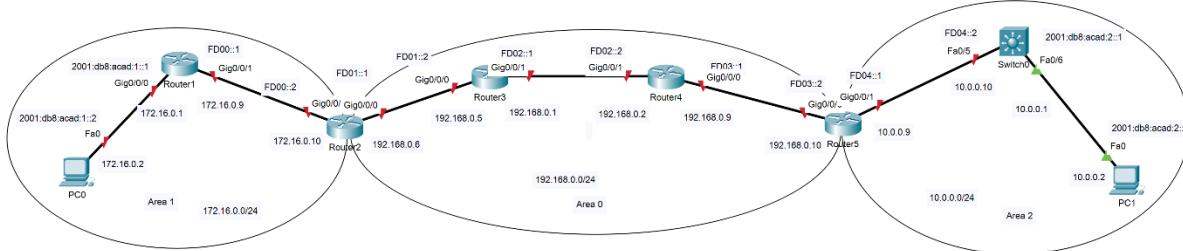
By convention, area 0 represents the backbone area of an OSPF network. Each additional area must have a connection to the OSPF backbone area.

OSPF does not use a transport protocol, unlike routing protocols like RIP and the Border Gateway Protocol. Instead, it encapsulates its data directly.

LAB SUMMARY:

In this lab, we configured multiarea OSPF, both for IPv4 and IPv6. We also were able to find out how to set up a multi-layer switch using OSPF.

NETWORK DIAGRAM:



LAB COMMANDS:

Follow the following steps for each routing device (router or multilayer switch) to configure the OSPF process ID, router ID, and interfaces.

MultilayerSwitch>en



MultilayerSwitch#config

MultilayerSwitch(config)#ip routing

MultilayerSwitch(config)#router ospf 1

This command enables OSPF with a process ID of 1.

MultilayerSwitch(config-router)#router-id 6.6.6.6

This command sets the router ID to 6.6.6.6.

MultilayerSwitch(config)#int fa0/5

For the multilayer switch, there is an additional step since we want the switch to be in routing, not switching, mode. As such, we have to use the following command:

MultilayerSwitch(config-if)#no switchport

Next, we continue by configuring the IP addresses and OSPF on each interface.

MultilayerSwitch(config-if)#ip add 10.0.0.10 255.255.255.252

MultilayerSwitch(config-if)#ip ospf 1 area 2

This command above configures the area in which the multilayer switch will belong to.

MultilayerSwitch(config-if)#exit

Repeat this process by configuring additional interfaces (using the no switchport command for interfaces on the multilayer switch).

We proceed by configuring the IPv6 addresses.

MultilayerSwitch(config)#ipv6 unicast-routing

MultilayerSwitch(config)#int f0/5

MultilayerSwitch(config-if)#ipv6 add fd04::2/64

MultilayerSwitch(config-if)#exit

Afterwards, we configure OSPFv3.

MultilayerSwitch(config)#ipv6 router ospf 1

MultilayerSwitch(config-rtr)#router-id 6.6.6.6

MultilayerSwitch(config-rtr)#exit

MultilayerSwitch(config)#int r fa0/5-6

MultilayerSwitch(config-if-range)#ipv6 ospf 1 area 2



We configure similarly for OSPFv2 and OSPFv3, on the routers:

Router 1 2001:db8:acad:1::1; 172.16.0.9

Router1>en

Router1#config

Router1(config)#ip routing

Router1(config)#router ospf 1

Router1(config-router)#router-id 1.1.1.1

Router1(config)#int g0/0/0

Router1(config-if)#ip add 172.16.0.1 255.255.255.252

Router1(config-if)#ip ospf 1 area 1

Router1(config)#int g0/0/1

Router1(config-if)#ip add 172.16.0.9 255.255.255.252

Router1(config-if)#ip ospf 1 area 1

Router1(config-if)#exit

Router1(config)#ipv6 router ospf 1

Router1(config-rtr)#router-id 1.1.1.1

Router1(config-rtr)#exit

Router1(config)#ipv6 unicast-routing

Router1(config)#int g0/0/0

Router1(config-if)#ipv6 add 2001:db8:acad:1::1/64

Router1(config-if)#ipv6 ospf 1 area 1

Router1(config)#int g0/0/1

Router1(config-if)#ipv6 add fd00::1/64

Router1(config-if)#ipv6 ospf 1 area 1

Repeat the above for routers R2, R3, R4, and R5.

Finally, configure PC0 and PC1's IP and IPv6 addresses. Test for connectivity and troubleshoot as needed.



CONFIGURATION:

Note that certain output has been removed for clarity and relevance.

Router 1:

```
ipv6 unicast-routing

interface GigabitEthernet0/0/0
ip address 192.168.1.1 255.255.255.0
negotiation auto
ipv6 address 2001:DB8:ACAD:F::2/64
ipv6 ospf 1 area 0

interface GigabitEthernet0/0/1
ip address 192.168.0.1 255.255.255.0
negotiation auto
ipv6 address 2001:DB8:ACAD:A::2/64
ipv6 ospf 1 area 1

router ospfv3 1
router-id 0.0.0.1
address-family ipv6 unicast
exit-address-family

router ospf 1
router-id 0.0.0.1
network 192.168.0.0 0.0.0.255 area 1
network 192.168.1.0 0.0.0.255 area 0
```

Router 2:

```
ipv6 unicast-routing

interface GigabitEthernet0/0/0
ip address 192.168.1.2 255.255.255.0
negotiation auto
ipv6 address 2001:DB8:ACAD:B::1/64
ipv6 ospf 1 area 0
```

```
interface GigabitEthernet0/0/1
```



```
ip address 192.168.0.2 255.255.255.0
negotiation auto
ipv6 address 2001:DB8:ACAD:A::2/64
ipv6 ospf 1 area 1

router ospfv3 1
router-id 0.0.0.2
address-family ipv6 unicast
exit-address-family

router ospf 1
router-id 0.0.0.2
network 192.168.0.0 0.0.0.255 area 1
```

Router 3:

```
ipv6 unicast-routing

interface GigabitEthernet0/0/0
ip address 192.168.0.5 255.255.255.252
negotiation auto
ipv6 address FD01::2/64
ipv6 enable
ipv6 ospf 1 area 0

interface GigabitEthernet0/0/1
ip address 192.168.0.1 255.255.255.252
negotiation auto
ipv6 address FD02::1/64
ipv6 enable
ipv6 ospf 1 area 0

router ospf 1
router-id 0.0.0.3
network 192.168.0.0 0.0.0.255 area 0
```

Router 4:

```
ipv6 unicast-routing
```



```
interface Loopback0
ip address 4.4.4.4 255.255.255.255

interface GigabitEthernet0/0/0
ip address 192.168.0.9 255.255.255.252
negotiation auto
ipv6 address FD03::1/64

interface GigabitEthernet0/0/1
ip address 192.168.0.2 255.255.255.252
negotiation auto
ipv6 address FD02::2/64

router ospf 1
router-id 4.4.4.4
network 192.168.0.0 0.0.0.255 area 0
```

Router 5:

```
ipv6 unicast-routing

interface Loopback0
ip address 5.5.5.5 255.255.255.255

interface GigabitEthernet0/0/0
ip address 192.168.0.10 255.255.255.252
negotiation auto
ipv6 address FD03::2/64

interface GigabitEthernet0/0/1
ip address 10.0.0.9 255.255.255.0
negotiation auto
ipv6 address FD04::1/64

router ospf 1
router-id 5.5.5.5
network 10.0.0.0 0.0.0.255 area 2
network 192.168.0.0 0.0.0.255 area 0
```

Multi-Layer Switch:

```
ipv6 unicast-routing

interface FastEthernet0/5
no switchport
ip address 10.0.0.10 255.255.255.252
ipv6 address FD04::2/64
ipv6 ospf 1 area 2

interface FastEthernet0/6
no switchport
ip address 10.0.0.1 255.255.255.252
ipv6 address 2001:DB8:ACAD:2::1/64
ipv6 ospf 1 area 2

interface Vlan1
ip address 192.168.10.1 255.255.255.0
router ospf 1
router-id 6.6.6.6
log adjacency-changes
network 10.0.0.0 0.0.0.255 area 2

ipv6 router ospf 1
router-id 6.6.6.6
```

PROBLEMS:

We encountered many problems during the configuration.

Firstly, there was a hardware issue on our original multilayer switch that prevented it from connecting to the network. When we tried using another multilayer switch, the incorrect Cisco IOS version was installed. For our lab configuration to work, we needed the IP Services version, but we originally started with the IP Base version. Therefore, to install IP Services, we had to borrow another multilayer switch to transfer and download the correct Cisco IOS version.

However, there were a few problems during the process. Firstly, transferring the IOS file directly via a USB drive didn't work. Secondly, transferring directly from one TFTP server to our TFTP server didn't work either. Lastly, we tried transferring from the multilayer switch with the correct version installed to the PC we borrowed to our PC. This was done through TFTPD64, which sets up the server. The last solution worked, and we were able to configure our multilayer switch smoothly and finish our lab.



CONCLUSION:

I learned how to set up OSPF, both version 2 and version 3, as well as on a multilayer switch. However, there were lots of challenges along the way, and I'm glad I was able to troubleshoot and be able to finish the lab successfully.



TEACHER SIGN-OFF:

Multi-Area OSPF

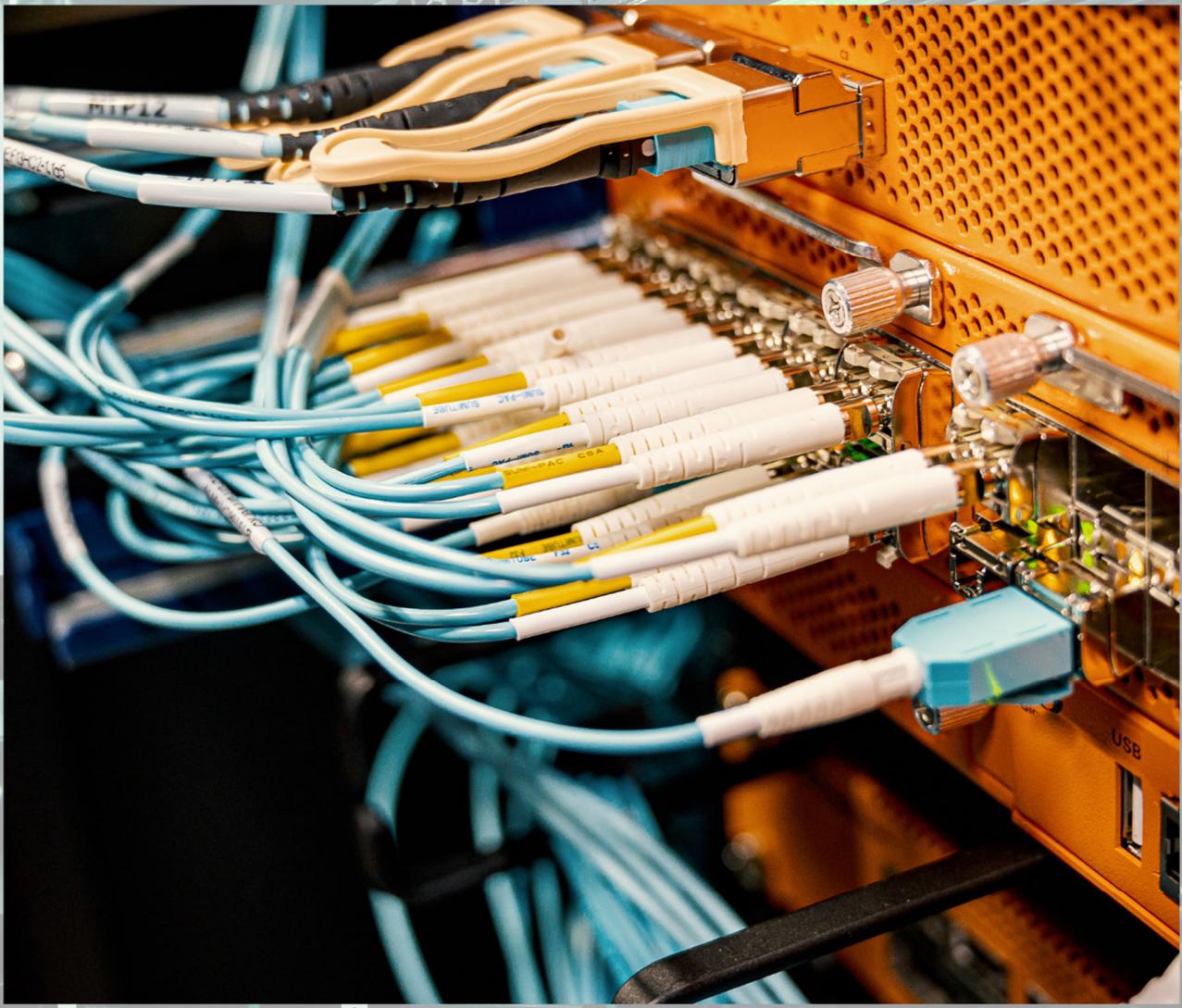
Alysia Chen

P3-4 CCNP

Mr. Mason



Lab 3: eBGP



PURPOSE:

Learn to configure the external Border Gateway Protocol, while using OSPF, EIGRP, and IS-IS as the routing protocols within each autonomous system.

BACKGROUND INFORMATION ON LAB CONCEPTS:

eBGP:

eBGP is also known as external Border Gateway Protocol (BGP). It uses autonomous systems (ASes), which are the networks within the network using eBGP.

BGP finds the most efficient path through attributes like weight (which local paths are preferred), local preference (which outbound path), and AS path length (router should prefer shorter paths).

BGP is used to connect networks worldwide to the Internet. In this lab, however, we only use it to connect IS-IS to OSPF to EIGRP. Some potential flaws of BGP are due to how wide-scale it is, routes being accidentally advertised or accidentally becoming the preferred paths may cause a widespread Internet outage, but these disruptions may take a while to fix due to a slow convergence.

OSPF:

OSPF stands for Open Shortest Path First. It is a link-state routing protocol, meaning that it only sends updates when a change occurs in the routing table and that all routers in the protocol know the full topology.

OSPF is able to detect changes in network topology within seconds, calculating link metrics—which help judge the quality of potential links—based on amount of data, distance of a router, and link availability and reliability.

EIGRP:

EIGRP, or Enhanced Interior Gateway Routing Protocol, allows for faster convergence than networks like BGP. It calculates routes through evaluating the distance and whether a destination path has loops or not.

This routing protocol has both link-state and distance vector characteristics—an EIGRP router only sends updates when a change occurs in the routing table but it also only advertises its best route to a neighbor (which is more like distance vector) and does not know the entire topology.

IS-IS:

IS-IS (Intermediate System to Intermediate System) is designed to be an interior gateway protocol. It is also a link-state routing protocol and uses the same algorithm as OSPF to find the best path.

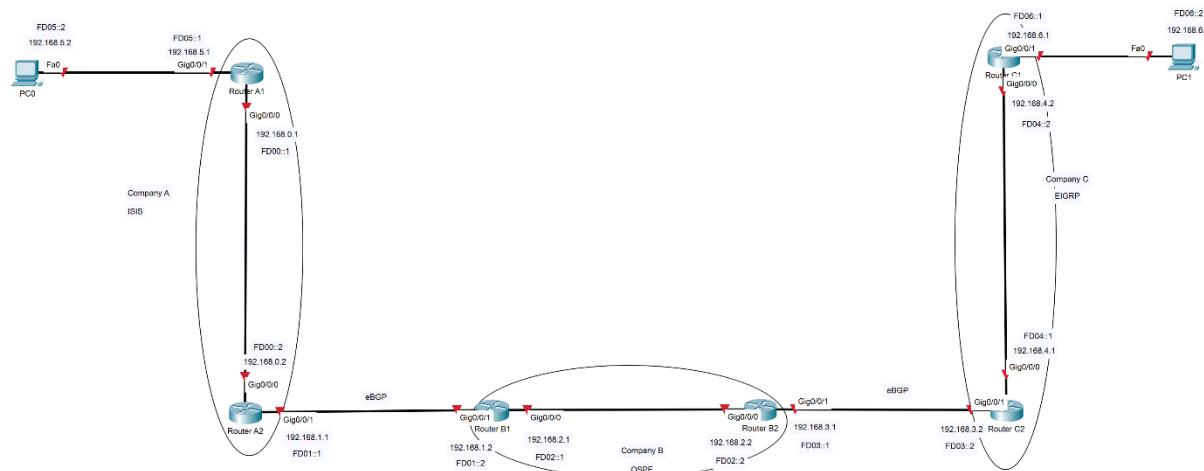


However, IS-IS is different from OSPF in that there are three types of routers used to connect different areas together: Level 1, Level 1-2, and Level 2. Level 1 can only establish neighbor adjacencies for routers in the same area; Level 2 can only establish neighbor adjacencies for routers in different areas; and Level 1-2 and perform both functions.

LAB SUMMARY:

In this lab, we configured external BGP, both for IPv4 and IPv6, to run through networks with IS-IS, OSPF, and EIGRP. We ended up connecting the two end devices—one on the network with IS-IS and one on the network with EIGRP—after successful configuration.

NETWORK DIAGRAM:



LAB COMMANDS:

First, after configuring network addresses for interfaces on each router, set up IS-IS, OSPF, and EIGRP, respectively:

IS-IS:

ip router isis enables an interface to participate in IS-IS for IPv4; *ipv6 router isis* enables an interface to participate in IS-IS for IPv6.

Since the routers will not use different areas, both of the routers (A1 and A2) will be Level 1. Enter the command *router isis* and use the global command *is-type level-1* to configure this. Specify a Network Entity Title (NET), which is the “ID” of the router in IS-IS. For example: *net 49.0001.1920.1680.0001.00*.

Then, use *redistribute connected* and *redistribute bgp [chosen Autonomous System number] [router level]*, noting to only use these commands for routers that are directly connected to a router with a different router protocol. Go into *address-family ipv6* and configure the same. These commands are used to advertised routes learned through BGP and directly connected routes into the IS-IS domain, but configuring them in this step will save some time.



OSPF:

ip ospf 1 area 0 configures the OSPF process ID (1) and the area (0, also known as the backbone area) for an interface. Process IDs are only for local identification (within the router); since only one area is needed for this lab, Area 0 is used. Repeat for IPv6, replacing *ip ospf 1 area 0* with *ipv6 ospf 1 area 0*.

In *router ospf 1*, where “1” represents the process ID, configure network statements to represent the different networks covered by OSPF, like: *network 192.168.2.0 0.0.0.255 area 0*. Next, configure the router ID, which identifies the router in the OSPF network. Do the same for IPv6, replacing *router ospf 1* with *ipv6 router ospf 1*.

Finally, use *redistribute connected* and *redistribute bgp [chosen Autonomous System number]*, noting to only use these commands for routers that are directly connected to a router with a different router protocol. These commands are used to advertised routes learned through BGP and directly connected routes into the OSPF domain, but configuring them in this step will save some time.

EIGRP:

Enter the *router eigrp 3* command to configure globally, where “3” is the chosen Autonomous System number. Configure the default metric values for routes that are redistributed through EIGRP. An example is *default-metric 10000 100 255 1 1500*, where 10000 represents the bandwidth, 100 represents the delay, 255 represents the reliability (highest reliability), 1 is the load (least load), and 1500 is the MTU.

Next, configure the network statements for the networks that the EIGRP routing protocol will cover. An example is *network 192.168.4.0 0.0.0.3*. Then, use *redistribute connected* and *redistribute bgp [chosen Autonomous System number]*, noting to only use these commands for routers that are directly connected to a router with a different router protocol. These commands are used to advertised routes learned through BGP and directly connected routes into the EIGRP domain, but configuring them in this step will save some time.

Then, type in the command *ipv6 router eigrp 3* to configure the router ID as such: *eigrp router-id 6.6.6.6*; also configure the *redistribute* commands. Configure the default metric values for IPv6 as well; the same values may be used for IPv4 and IPv6.

Configure interfaces using the command *ipv6 eigrp 3* for IPv6 only on links that are part of the EIGRP Autonomous System (AS 3).

Next, follow the following steps for each routing device to configure **eBGP**.

Enter the BGP router configuration with the global command *router bgp [router Autonomous System number]*. Configure neighbors using commands like *neighbor 192.168.3.1 remote-as 3333* for IPv4 and *neighbor FD03::1 remote-as 3333* for IPv6. Next, enter the commands *address-family ipv4* and *address-family ipv6*, respectively, to configure IPv4 and IPv6 BGP. In both, enter *redistribute connected* and *redistribute [either IS-IS, OSPF, or EIGRP, depending on the router, with the associated*



*router level, process ID, or Autonomous System number, respectively]. If needed, specific networks may be advertised using the *network [IPv4 address/IPv6 address]* command. This will allow for connected routes and routes learned through EIGRP to be advertised through BGP and make them visible across the entire network.*

CONFIGURATIONS:

A1:

IPv4 Routing Table:

```

        4.0.0.0/32 is subnetted, 1 subnets
i L1      4.4.4.4 [115/10] via 192.168.0.2, 00:12:43,
GigabitEthernet0/0/0

        5.0.0.0/32 is subnetted, 1 subnets
i L1      5.5.5.5 [115/10] via 192.168.0.2, 00:12:43,
GigabitEthernet0/0/0

        6.0.0.0/32 is subnetted, 1 subnets
i L1      6.6.6.6 [115/10] via 192.168.0.2, 00:08:10,
GigabitEthernet0/0/0

        192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C          192.168.0.0/24 is directly connected,
GigabitEthernet0/0/0

L          192.168.0.1/32 is directly connected,
GigabitEthernet0/0/0

i L1      192.168.1.0/24 [115/20] via 192.168.0.2, 00:15:03,
GigabitEthernet0/0/0

i L1      192.168.2.0/24 [115/10] via 192.168.0.2, 00:13:32,
GigabitEthernet0/0/0

        192.168.3.0/30 is subnetted, 1 subnets
i L1      192.168.3.0 [115/10] via 192.168.0.2, 00:12:43,
GigabitEthernet0/0/0

        192.168.4.0/30 is subnetted, 1 subnets
i L1      192.168.4.0 [115/10] via 192.168.0.2, 00:08:40,
GigabitEthernet0/0/0

        192.168.5.0/24 is variably subnetted, 2 subnets, 2 masks
C          192.168.5.0/24 is directly connected,
GigabitEthernet0/0/1

L          192.168.5.1/32 is directly connected,
GigabitEthernet0/0/1

        192.168.6.0/30 is subnetted, 1 subnets
i L1      192.168.6.0 [115/10] via 192.168.0.2, 00:08:10,
GigabitEthernet0/0/0

```



IPv6 Routing Table:

```

C  FD00::/64 [0/0]
    via GigabitEthernet0/0/0, directly connected
L  FD00::1/128 [0/0]
    via GigabitEthernet0/0/0, receive
I1 FD01::/64 [115/20]
    via FE80::227:90FF:FED4:F30, GigabitEthernet0/0/0
I1 FD02::/64 [115/10]
    via FE80::227:90FF:FED4:F30, GigabitEthernet0/0/0
I1 FD03::/64 [115/10]
    via FE80::227:90FF:FED4:F30, GigabitEthernet0/0/0
I1 FD04::/64 [115/10]
    via FE80::227:90FF:FED4:F30, GigabitEthernet0/0/0
C  FD05::/64 [0/0]
    via GigabitEthernet0/0/1, directly connected
L  FD05::1/128 [0/0]
    via GigabitEthernet0/0/1, receive
I1 FD06::/64 [115/10]
    via FE80::227:90FF:FED4:F30, GigabitEthernet0/0/0
L  FF00::/8 [0/0]
    via Null0, receive

```

Configuration:

```

ipv6 unicast-routing

interface GigabitEthernet0/0/0
ip address 192.168.0.1 255.255.255.0
ip router isis
negotiation auto
ipv6 address FD00::1/64
ipv6 router isis
isis circuit-type level-1

interface GigabitEthernet0/0/1
ip address 192.168.5.1 255.255.255.0
ip router isis
negotiation auto
ipv6 address FD05::1/64
ipv6 router isis

```



```

isis circuit-type level-1

router isis
  net 49.0001.1920.1680.0001.00
  is-type level-1
  metric-style narrow
  redistribute connected

```

A2:

IPv4 Routing Table:

```

        4.0.0.0/32 is subnetted, 1 subnets
B          4.4.4.4 [20/20] via 192.168.1.2, 00:11:57
        5.0.0.0/32 is subnetted, 1 subnets
B          5.5.5.5 [20/1] via 192.168.1.2, 00:11:57
        6.0.0.0/32 is subnetted, 1 subnets
B          6.6.6.6 [20/1] via 192.168.1.2, 00:07:24
        192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C            192.168.0.0/24 is directly connected,
GigabitEthernet0/0/0
L            192.168.0.2/32 is directly connected,
GigabitEthernet0/0/0
        192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C            192.168.1.0/24 is directly connected,
GigabitEthernet0/0/1
L            192.168.1.1/32 is directly connected,
GigabitEthernet0/0/1
B            192.168.2.0/24 [20/0] via 192.168.1.2, 00:12:47
        192.168.3.0/30 is subnetted, 1 subnets
B            192.168.3.0 [20/20] via 192.168.1.2, 00:11:57
        192.168.4.0/30 is subnetted, 1 subnets
B            192.168.4.0 [20/1] via 192.168.1.2, 00:07:54
i L1    192.168.5.0/24 [115/20] via 192.168.0.1, 00:15:33,
GigabitEthernet0/0/0
        192.168.6.0/30 is subnetted, 1 subnets
B            192.168.6.0 [20/1] via 192.168.1.2, 00:07:24

```

IPv6 Routing Table:

```

C      FD00::/64 [0/0]
      via GigabitEthernet0/0/0, directly connected
L      FD00::2/128 [0/0]
      via GigabitEthernet0/0/0, receive

```



```

C   FD01::/64 [0/0]
    via GigabitEthernet0/0/1, directly connected
L   FD01::1/128 [0/0]
    via GigabitEthernet0/0/1, receive
B   FD02::/64 [20/0]
    via FE80::B6A8:B9FF:FE47:9471, GigabitEthernet0/0/1
B   FD03::/64 [20/20]
    via FE80::B6A8:B9FF:FE47:9471, GigabitEthernet0/0/1
B   FD04::/64 [20/1]
    via FE80::B6A8:B9FF:FE47:9471, GigabitEthernet0/0/1
I1  FD05::/64 [115/20]
    via FE80::2C1:B1FF:FE68:AB90, GigabitEthernet0/0/0
B   FD06::/64 [20/1]
    via FE80::B6A8:B9FF:FE47:9471, GigabitEthernet0/0/1
L   FF00::/8 [0/0]
    via Null0, receive

```

Configuration:

```

ipv6 unicast-routing

interface GigabitEthernet0/0/0
ip address 192.168.0.2 255.255.255.0
ip router isis
negotiation auto
ipv6 address FD00::2/64
ipv6 router isis
isis circuit-type level-1

interface GigabitEthernet0/0/1
ip address 192.168.1.1 255.255.255.0
ip router isis
negotiation auto
ipv6 address FD01::1/64
ipv6 router isis
isis circuit-type level-1

router isis
net 49.0001.1920.1680.0002.00
is-type level-1

```



```

redistribute connected
redistribute bgp 2222 level-1
address-family ipv6
  redistribute connected
  redistribute bgp 2222 level-1

router bgp 2222
  bgp router-id 2.2.2.2
  bgp log-neighbor-changes
  neighbor 192.168.1.2 remote-as 3333
  neighbor FD01::2 remote-as 3333
  neighbor FD01::2 update-source GigabitEthernet0/0/1
  address-family ipv4
    network 192.168.1.0
    redistribute connected
    redistribute isis level-1
    neighbor 192.168.1.2 activate
  address-family ipv6
    redistribute connected
    redistribute isis level-1
    neighbor FD01::2 activate

```

B1:

IPv4 Routing Table:

```

  4.0.0.0/32 is subnetted, 1 subnets
O E2      4.4.4.4 [110/20] via 192.168.2.2, 00:11:13,
GigabitEthernet0/0/0
  5.0.0.0/32 is subnetted, 1 subnets
O E2      5.5.5.5 [110/1] via 192.168.2.2, 00:11:13,
GigabitEthernet0/0/0
  6.0.0.0/32 is subnetted, 1 subnets
O E2      6.6.6.6 [110/1] via 192.168.2.2, 00:06:40,
GigabitEthernet0/0/0
B        192.168.0.0/24 [20/0] via 192.168.1.1, 00:13:27
  192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected,
GigabitEthernet0/0/1
L        192.168.1.2/32 is directly connected,
GigabitEthernet0/0/1
  192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks

```



```

C      192.168.2.0/24 is directly connected,
GigabitEthernet0/0/0
L      192.168.2.1/32 is directly connected,
GigabitEthernet0/0/0
      192.168.3.0/30 is subnetted, 1 subnets
O E2    192.168.3.0 [110/20] via 192.168.2.2, 00:11:13,
GigabitEthernet0/0/0
      192.168.4.0/30 is subnetted, 1 subnets
O E2    192.168.4.0 [110/1] via 192.168.2.2, 00:07:10,
GigabitEthernet0/0/0
B      192.168.5.0/24 [20/20] via 192.168.1.1, 00:13:27
      192.168.6.0/30 is subnetted, 1 subnets
O E2    192.168.6.0 [110/1] via 192.168.2.2, 00:06:40,
GigabitEthernet0/0/0

```

IPv6 Routing Table:

```

B    FD00::/64 [20/0]
      via FE80::227:90FF:FED4:F31, GigabitEthernet0/0/1
C    FD01::/64 [0/0]
      via GigabitEthernet0/0/1, directly connected
L    FD01::2/128 [0/0]
      via GigabitEthernet0/0/1, receive
C    FD02::/64 [0/0]
      via GigabitEthernet0/0/0, directly connected
L    FD02::1/128 [0/0]
      via GigabitEthernet0/0/0, receive
OE2 FD03::/64 [110/20]
      via FE80::267E:12FF:FE55:5720, GigabitEthernet0/0/0
OE2 FD04::/64 [110/1]
      via FE80::267E:12FF:FE55:5720, GigabitEthernet0/0/0
B    FD05::/64 [20/20]
      via FE80::227:90FF:FED4:F31, GigabitEthernet0/0/1
OE2 FD06::/64 [110/1]
      via FE80::267E:12FF:FE55:5720, GigabitEthernet0/0/0
L    FF00::/8 [0/0]
      via Null0, receive

```

Configuration:

```
ipv6 unicast-routing
```



```
interface GigabitEthernet0/0/0
 ip address 192.168.2.1 255.255.255.0
 ip ospf 1 area 0
 negotiation auto
 ipv6 address FD02::1/64
 ipv6 ospf 1 area 0

interface GigabitEthernet0/0/1
 ip address 192.168.1.2 255.255.255.0
 negotiation auto
 ipv6 address FD01::2/64

router ospf 1
 router-id 3.3.3.3
 redistribute connected subnets
 redistribute bgp 3333 subnets
 network 192.168.2.0 0.0.0.255 area 0

router bgp 3333
 bgp router-id 3.3.3.3
 bgp log-neighbor-changes
 neighbor 192.168.1.1 remote-as 2222
 neighbor FD01::1 remote-as 2222
 neighbor FD01::1 update-source GigabitEthernet0/0/1
 address-family ipv4
 network 192.168.1.0
 network 192.168.2.0
 redistribute connected
 redistribute ospf 1 match external 1 external 2
 neighbor 192.168.1.1 activate
 address-family ipv6
 redistribute connected
 redistribute ospf 1 match external 1 external 2
 neighbor FD01::1 activate

ipv6 router ospf 1
 router-id 3.3.3.3
 redistribute connected
 redistribute bgp 3333
```



B2:

IPv4 Routing Table:

```

        4.0.0.0/32 is subnetted, 1 subnets
C           4.4.4.4 is directly connected, Loopback0
        5.0.0.0/32 is subnetted, 1 subnets
B           5.5.5.5 [20/0] via 192.168.3.2, 00:08:19
        6.0.0.0/32 is subnetted, 1 subnets
B           6.6.6.6 [20/130816] via 192.168.3.2, 00:03:27
O E2  192.168.0.0/24 [110/1] via 192.168.2.1, 00:08:04,
GigabitEthernet0/0/0
O E2  192.168.1.0/24 [110/20] via 192.168.2.1, 00:08:04,
GigabitEthernet0/0/0
        192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C           192.168.2.0/24 is directly connected,
GigabitEthernet0/0/0
L           192.168.2.2/32 is directly connected,
GigabitEthernet0/0/0
        192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C           192.168.3.0/30 is directly connected,
GigabitEthernet0/0/1
L           192.168.3.1/32 is directly connected,
GigabitEthernet0/0/1
        192.168.4.0/30 is subnetted, 1 subnets
B           192.168.4.0 [20/0] via 192.168.3.2, 00:03:57
O E2  192.168.5.0/24 [110/1] via 192.168.2.1, 00:08:04,
GigabitEthernet0/0/0
        192.168.6.0/30 is subnetted, 1 subnets
B           192.168.6.0 [20/3072] via 192.168.3.2, 00:03:27

```

IPv6 Routing Table:

```

OE2 FD00::/64 [110/1]
    via FE80::B6A8:B9FF:FE47:9470, GigabitEthernet0/0/0
OE2 FD01::/64 [110/20]
    via FE80::B6A8:B9FF:FE47:9470, GigabitEthernet0/0/0
C   FD02::/64 [0/0]
    via GigabitEthernet0/0/0, directly connected
L   FD02::2/128 [0/0]
    via GigabitEthernet0/0/0, receive
C   FD03::/64 [0/0]
    via GigabitEthernet0/0/1, directly connected

```



```

L   FD03::1/128 [0/0]
    via GigabitEthernet0/0/1, receive
B   FD04::/64 [20/0]
    via FE80::CE7F:76FF:FE83:16D1, GigabitEthernet0/0/1
OE2 FD05::/64 [110/1]
    via FE80::B6A8:B9FF:FE47:9470, GigabitEthernet0/0/0
B   FD06::/64 [20/281856]
    via FE80::CE7F:76FF:FE83:16D1, GigabitEthernet0/0/1
L   FF00::/8 [0/0]
    via Null0, receive

```

Configuration:

```

ipv6 unicast-routing

interface Loopback0
  ip address 4.4.4.4 255.255.255.255

interface GigabitEthernet0/0/0
  ip address 192.168.2.2 255.255.255.0
  ip ospf 1 area 0
  negotiation auto
  ipv6 address FD02::2/64
  ipv6 ospf 1 area 0

interface GigabitEthernet0/0/1
  ip address 192.168.3.1 255.255.255.252
  negotiation auto
  ipv6 address FD03::1/64

router ospf 1
  router-id 4.4.4.4
  redistribute connected subnets
  redistribute bgp 3333 subnets
  network 192.168.2.0 0.0.0.255 area 0

router bgp 3333
  bgp router-id 4.4.4.4
  bgp log-neighbor-changes
  neighbor fd03::2/64 remote-as 3

```



```

neighbor 192.168.3.2 remote-as 3
address-family ipv4
  network 192.168.2.0
  network 192.168.3.0
  redistribute connected
  redistribute ospf 1 match external 1 external 2
  neighbor 192.168.3.2 activate
address-family ipv6
  redistribute connected
  redistribute ospf 1 match external 1 external 2
  network FD02::/64
  network FD03::/64
  neighbor fd03::2 activate

ipv6 router ospf 1
  router-id 4.4.4.4
  redistribute connected
  redistribute bgp 3333

```

C1:

IPv4 Routing Table:

	4.0.0.0/32 is subnetted, 1 subnets
B	4.4.4.4 [20/0] via 192.168.3.1, 00:06:44
	5.0.0.0/32 is subnetted, 1 subnets
C	5.5.5.5 is directly connected, Loopback0
	6.0.0.0/32 is subnetted, 1 subnets
D EX	6.6.6.6 [170/130816] via 192.168.4.2, 00:02:20, GigabitEthernet0/0/0
B	192.168.0.0/24 [20/1] via 192.168.3.1, 00:06:15
B	192.168.1.0/24 [20/20] via 192.168.3.1, 00:06:15
B	192.168.2.0/24 [20/0] via 192.168.3.1, 00:06:44
	192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C	192.168.3.0/30 is directly connected, GigabitEthernet0/0/1
L	192.168.3.2/32 is directly connected, GigabitEthernet0/0/1
	192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C	192.168.4.0/30 is directly connected, GigabitEthernet0/0/0



```

L      192.168.4.1/32 is directly connected,
GigabitEthernet0/0/0
B      192.168.5.0/24 [20/1] via 192.168.3.1, 00:06:15
      192.168.6.0/30 is subnetted, 1 subnets
D          192.168.6.0 [90/3072] via 192.168.4.2, 00:02:16,
GigabitEthernet0/0/0

```

IPv6 Routing Table:

```

B      FD00::/64 [20/1]
      via FE80::267E:12FF:FE55:5721, GigabitEthernet0/0/1
B      FD01::/64 [20/20]
      via FE80::267E:12FF:FE55:5721, GigabitEthernet0/0/1
B      FD02::/64 [20/0]
      via FE80::267E:12FF:FE55:5721, GigabitEthernet0/0/1
C      FD03::/64 [0/0]
      via GigabitEthernet0/0/1, directly connected
L      FD03::2/128 [0/0]
      via GigabitEthernet0/0/1, receive
C      FD04::/64 [0/0]
      via GigabitEthernet0/0/0, directly connected
L      FD04::1/128 [0/0]
      via GigabitEthernet0/0/0, receive
B      FD05::/64 [20/1]
      via FE80::267E:12FF:FE55:5721, GigabitEthernet0/0/1
EX     FD06::/64 [170/281856]
      via FE80::521C:B0FF:FE42:AF80, GigabitEthernet0/0/0
L      FF00::/8 [0/0]
      via Null0, receive

```

Configuration:

```

ipv6 unicast-routing

interface Loopback0
  ip address 6.6.6.6 255.255.255.255

interface GigabitEthernet0/0/0
  ip address 192.168.4.2 255.255.255.252
  negotiation auto
  ipv6 address FD04::2/64

```



```

ipv6 eigrp 3

interface GigabitEthernet0/0/1
 ip address 192.168.6.1 255.255.255.252
 negotiation auto
 ipv6 address FD06::1/64

router eigrp 3
 default-metric 10000 100 255 1 1500
 network 192.168.4.0 0.0.0.3
 network 192.168.6.0
 redistribute connected

ipv6 router eigrp 3
 eigrp router-id 6.6.6.6
 redistribute connected
 default-metric 10000 100 255 1 1500

```

C2:**IPv4 Routing Table:**

```

4.0.0.0/32 is subnetted, 1 subnets
D EX      4.4.4.4 [170/281856] via 192.168.4.1, 00:00:21,
GigabitEthernet0/0/0

5.0.0.0/32 is subnetted, 1 subnets
D EX      5.5.5.5 [170/130816] via 192.168.4.1, 00:00:21,
GigabitEthernet0/0/0

6.0.0.0/32 is subnetted, 1 subnets
C          6.6.6.6 is directly connected, Loopback0

D EX      192.168.0.0/24
          [170/281856] via 192.168.4.1, 00:00:21,
GigabitEthernet0/0/0

D EX      192.168.1.0/24
          [170/281856] via 192.168.4.1, 00:00:21,
GigabitEthernet0/0/0

D EX      192.168.2.0/24
          [170/281856] via 192.168.4.1, 00:00:21,
GigabitEthernet0/0/0

192.168.3.0/30 is subnetted, 1 subnets
D          192.168.3.0 [90/3072] via 192.168.4.1, 00:00:21,
GigabitEthernet0/0/0

```



```

        192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C             192.168.4.0/30 is directly connected,
GigabitEthernet0/0/0
L             192.168.4.2/32 is directly connected,
GigabitEthernet0/0/0
D EX  192.168.5.0/24
                [170/281856] via 192.168.4.1, 00:00:21,
GigabitEthernet0/0/0
        192.168.6.0/24 is variably subnetted, 2 subnets, 2 masks
C             192.168.6.0/30 is directly connected,
GigabitEthernet0/0/1
L             192.168.6.1/32 is directly connected,
GigabitEthernet0/0/1

```

IPv6 Routing Table:

```

EX  FD00::/64 [170/281856]
    via FE80::CE7F:76FF:FE83:16D0, GigabitEthernet0/0/0
EX  FD01::/64 [170/281856]
    via FE80::CE7F:76FF:FE83:16D0, GigabitEthernet0/0/0
EX  FD02::/64 [170/281856]
    via FE80::CE7F:76FF:FE83:16D0, GigabitEthernet0/0/0
EX  FD03::/64 [170/281856]
    via FE80::CE7F:76FF:FE83:16D0, GigabitEthernet0/0/0
C   FD04::/64 [0/0]
    via GigabitEthernet0/0/0, directly connected
L   FD04::2/128 [0/0]
    via GigabitEthernet0/0/0, receive
EX  FD05::/64 [170/281856]
    via FE80::CE7F:76FF:FE83:16D0, GigabitEthernet0/0/0
C   FD06::/64 [0/0]
    via GigabitEthernet0/0/1, directly connected
L   FD06::1/128 [0/0]
    via GigabitEthernet0/0/1, receive
L   FF00::/8 [0/0]
    via Null0, receive

```

Configuration:

```
ipv6 unicast-routing
```

```
interface Loopback0
```



```
ip address 5.5.5.5 255.255.255.255

interface GigabitEthernet0/0/0
 ip address 192.168.4.1 255.255.255.252
 negotiation auto
 ipv6 address FD04::1/64
 ipv6 eigrp 3

interface GigabitEthernet0/0/1
 ip address 192.168.3.2 255.255.255.252
 negotiation auto
 ipv6 address FD03::2/64

router eigrp 3
 default-metric 10000 100 255 1 1500
 network 192.168.3.0
 network 192.168.4.0 0.0.0.3
 redistribute connected
 redistribute bgp 3

router bgp 3
 bgp log-neighbor-changes
 neighbor 192.168.3.1 remote-as 3333
 neighbor FD03::1 remote-as 3333
 address-family ipv4
 redistribute connected
 redistribute eigrp 3
 neighbor 192.168.3.1 activate
 address-family ipv6
 redistribute connected
 redistribute eigrp 3
 network FD03::/64
 neighbor FD03::1 activate

ipv6 router eigrp 3
 eigrp router-id 5.5.5.5
 redistribute bgp 3
 redistribute connected
 default-metric 10000 100 255 1 1500
```



PROBLEMS:

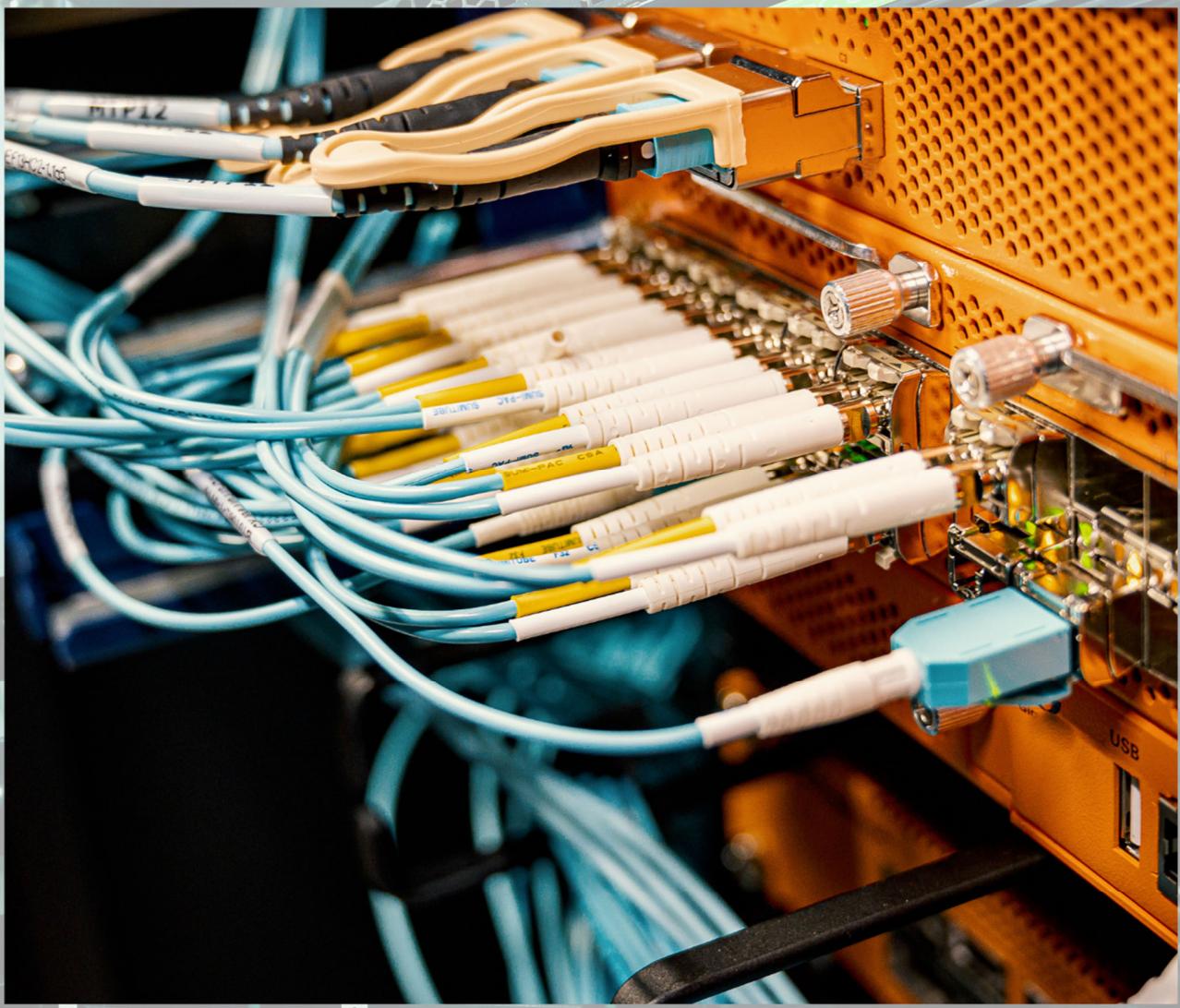
I mostly struggled with connectivity through EIGRP. However, I soon realized that for EIGRP, I needed to have a default metric for it to work. Additionally, while configuring EIGRP, the routing protocol could not be seen through the commands `show ip route` and `show ipv6 route` until I figured out that for EIGRP, we should only configure interfaces on an EIGRP router that connect to other routers with EIGRP. After configuring a metric and fixing the interface configurations, the routers with EIGRP running were able to successfully ping other networks.

CONCLUSION:

I learned how to set up eBGP—something I found very complex as it not only involved setting up routing protocols but also a routing protocol that connected each of the domains to allow for end-to-end connectivity. Although there challenging moments, I'm glad I was able to finish the lab successfully.



Lab 4: iBGP



PURPOSE:

Learn to configure the internal Border Gateway Protocol, while using OSPF, EIGRP, and IS-IS, as well as the external Border Gateway Protocol to route between Autonomous Systems.

BACKGROUND INFORMATION ON LAB CONCEPTS:

BGP (iBGP and eBGP):

BGP is a routing protocol that uses autonomous systems (AS). It makes routing decisions by considering paths, network policies, and rule-sets (which are configured by a network administrator). BGP is the only commonly used routing protocol with TCP as its transport protocol. When BGP uses the same AS number and therefore the same autonomous systems for peers, it is called iBGP.

A BGP peer uses a finite-state machine with six states for connections with peers: Idle, Connect, Active, OpenConfirm, and Established. All routers within an AS, like in iBGP, must be configured in a full mesh topology, meaning that each router must be a peer to every other router in the network. However, this may hinder scalability. However, BGP is said to be the “most scalable of all routing protocols,” due to route reflectors that reduce the number of connections required.

An analogy that could be used to explain iBGP (internal BGP) and eBGP (external BGP) usage within this lab involves a group of oranges. Imagine they reside in different farms, but they need to coordinate together to escape and return to Orange Land. To do that, they would need a communication system like eBGP that would ensure that oranges from different farms—similar to different networks—can still communicate with each other. They would need to do so as unified groups, which requires iBGP to act like a communication network with walkie-talkies that allows all oranges within a farm to receive the escape plans.

OSPF:

OSPF stands for Open Shortest Path First. It is a link-state routing protocol, meaning that it only sends updates when a change occurs in the routing table and that all routers in the protocol know the full topology.

OSPF is able to detect changes in network topology within seconds, calculating link metrics—which help judge the quality of potential links—based on amount of data, distance of a router, and link availability and reliability.

EIGRP:

EIGRP, or Enhanced Interior Gateway Routing Protocol, allows for faster convergence than networks like BGP. It calculates routes through evaluating the distance and whether a destination path has loops or not.



This routing protocol has both link-state and distance vector characteristics—an EIGRP router only sends updates when a change occurs in the routing table but it also only advertises its best route to a neighbor (which is more like distance vector) and does not know the entire topology.

IS-IS:

IS-IS (Intermediate System to Intermediate System) is designed to be an interior gateway protocol. It is also a link-state routing protocol and uses the same algorithm as OSPF to find the best path.

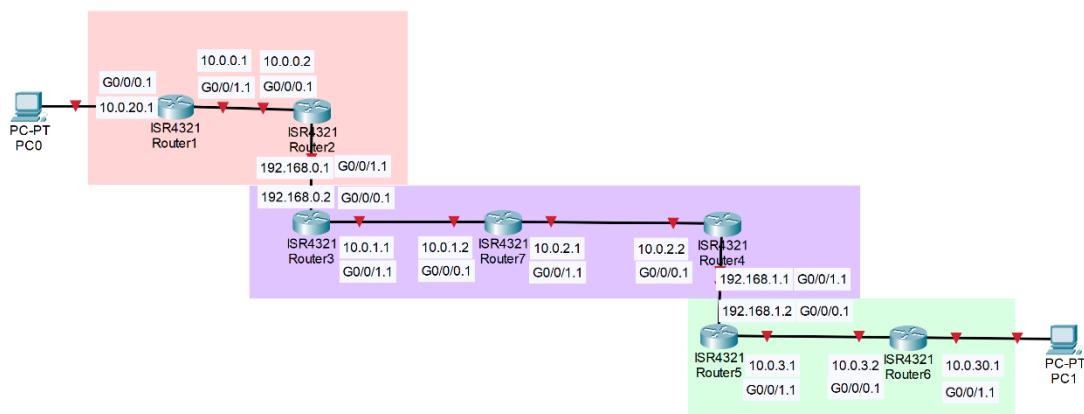
However, IS-IS is different from OSPF in that there are three types of routers used to connect different areas together: Level 1, Level 1-2, and Level 2. Level 1 can only establish neighbor adjacencies for routers in the same area; Level 2 can only establish neighbor adjacencies for routers in different areas; and Level 1-2 and perform both functions.

LAB SUMMARY:

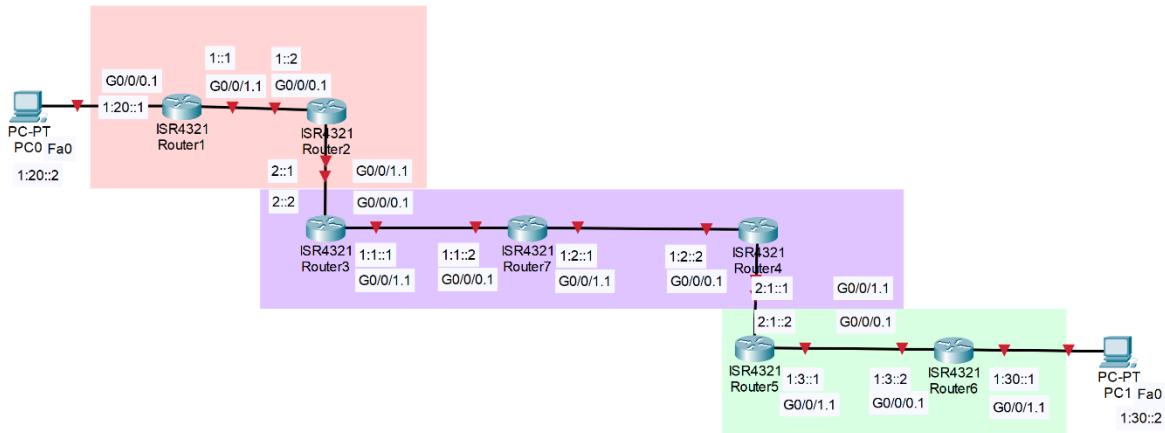
In this lab, we configured internal BGP, both for IPv4 and IPv6, within AS 2; the middle router uses EIGRP as the interior gateway protocol. eBGP sessions were established between AS 1 and AS 2, as well as between AS 2 and AS 3, with its routes carried through iBGP. We ended up connecting the two end devices after successful configuration.

NETWORK DIAGRAMS:

IPv4:



IPv6:



Router	Routing Protocols Used
R1	OSPF (IPv4 & IPv6)
R2	OSPF (IPv4 & IPv6), eBGP
R3	EIGRP (IPv4 & IPv6), eBGP, iBGP
R4	EIGRP (IPv4 & IPv6), eBGP, iBGP
R5	IS-IS (IPv4 & IPv6), eBGP
R6	IS-IS (IPv4 & IPv6)
R7	EIGRP (IPv4 & IPv6), iBGP

LAB COMMANDS:

First, after configuring network addresses for interfaces on each router, set up IS-IS, OSPF, and EIGRP, respectively:

IS-IS:

ip router isis enables an interface to participate in IS-IS for IPv4; *ipv6 router isis* enables an interface to participate in IS-IS for IPv6.

Since the routers will not use different areas, both of the routers (A1 and A2) will be Level 1. Enter the command *router isis* and use the global command *is-type level-1* to configure this. Specify a Network Entity Title (NET), which is the “ID” of the router in IS-IS. For example: *net 49.0001.1920.1680.0001.00*.

Then, use *redistribute connected* and *redistribute bgp [chosen Autonomous System number] [router level]*, noting to only use these commands for routers that are directly connected to a router with



a different router protocol. Go into *address-family ipv6* and configure the same. These commands are used to advertised routes learned through BGP and directly connected routes into the IS-IS domain, but configuring them in this step will save some time.

OSPF:

ip ospf 1 area 0 configures the OSPF process ID (1) and the area (0, also known as the backbone area) for an interface. Process IDs are only for local identification (within the router); since only one area is needed for this lab, Area 0 is used. Repeat for IPv6, replacing *ip ospf 1 area 0* with *ipv6 ospf 1 area 0*.

In *router ospf 1*, where “1” represents the process ID, configure network statements to represent the different networks covered by OSPF, like: *network 192.168.2.0 0.0.0.255 area 0*. Next, configure the router ID, which identifies the router in the OSPF network. Do the same for IPv6, replacing *router ospf 1* with *ipv6 router ospf 1*.

Finally, use *redistribute connected* and *redistribute bgp [chosen Autonomous System number]*, noting to only use these commands for routers that are directly connected to a router with a different router protocol. These commands are used to advertised routes learned through BGP and directly connected routes into the OSPF domain, but configuring them in this step will save some time.

EIGRP:

Enter the *router eigrp 3* command to configure globally, where “3” is the chosen Autonomous System number in this example. Configure the default metric values for routes that are redistributed through EIGRP. An example is *default-metric 10000 100 255 1 1500*, where 10000 represents the bandwidth, 100 represents the delay, 255 represents the reliability (highest reliability), 1 is the load (least load), and 1500 is the MTU.

Next, configure the network statements for the networks that the EIGRP routing protocol will cover. An example is *network 192.168.4.0 0.0.0.3*. Then, use *redistribute connected* and *redistribute bgp [chosen Autonomous System number]*, noting to only use these commands for routers that are directly connected to a router with a different router protocol. These commands are used to advertised routes learned through BGP and directly connected routes into the EIGRP domain, but configuring them in this step will save some time.

Then, type in the command *ipv6 router eigrp 3* to configure the router ID as such: *eigrp router-id 6.6.6.6*; also configure the *redistribute* commands. Configure the default metric values for IPv6 as well; the same values may be used for IPv4 and IPv6.

Configure interfaces using the command *ipv6 eigrp 3* for IPv6 only on links that are part of the EIGRP Autonomous System (AS 3).

Next, follow the following steps for each routing device to configure **BGP**.



Enter the BGP router configuration with the global command *router bgp [router Autonomous System number]*. Configure neighbors using commands like *neighbor 192.168.3.1 remote-as 3333* for IPv4 and *neighbor FD03::1 remote-as 3333* for IPv6. For iBGP, make sure to use the same Autonomous System number for both *router bgp* and *neighbor* commands. For eBGP, make sure to use the neighboring network's Autonomous System number. Next, enter the commands *address-family ipv4* and *address-family ipv6*, respectively, to configure IPv4 and IPv6 BGP. In both, enter *redistribute connected* and *redistribute [either IS-IS, OSPF, or EIGRP, depending on the router, with the associated router level, process ID, or Autonomous System number, respectively]*. If needed, specific networks may be advertised using the *network [IPv4 address/IPv6 address]* command. This will allow for connected routes and routes learned through other routing protocols to be advertised through BGP and make them visible across the entire network.

The following are some iBGP-specific commands. We must use the *next-hop-self [router 7 IP address]* command on routers 3 and 4 within both IPv4 and IPv6 address families. This will allow Router 7—the middle router—to reach the next-hop routes otherwise unavailable. We will also need to use the *neighbor [IP address] route-reflector-client* command that, while optional, will simplify the topology, especially if we were to upscale the network. Since Router 7 is a neighbor to the two other routers in the AS, Router 3 and Router 4, we will designate Router 7 as the Route Reflector and configure this command in its IPv4 and IPv6 address families.

CONFIGURATIONS:

Trace routes from PC1 to PC0, with IPv4 and IPv6, respectively:

Tracing route to DESKTOP-27SAP3J [10.0.20.2]
over a maximum of 30 hops:

```

1      <1 ms      <1 ms      <1 ms    10.0.30.1
2      <1 ms      <1 ms      <1 ms    10.0.3.1
3      1 ms       <1 ms      <1 ms    192.168.1.1
4      <1 ms      <1 ms      <1 ms    10.0.2.1
5      1 ms       <1 ms      <1 ms    10.0.1.1
6      1 ms       1 ms       1 ms     192.168.0.1
7      1 ms       1 ms       1 ms     10.0.0.1
8      1 ms       1 ms       1 ms     DESKTOP-27SAP3J [10.0.20.2]

```

Trace complete.

Tracing route to 1:20::2 over a maximum of 30 hops

```

1      <1 ms      <1 ms      <1 ms    1:30::1
2      <1 ms      <1 ms      <1 ms    1:3::1
3      1 ms       <1 ms      1 ms     2:1::1
4      1 ms       <1 ms      <1 ms    1:2::1
5      1 ms       1 ms       1 ms     1:1::1
6      1 ms       1 ms       1 ms     2::1

```



```
7      1 ms      1 ms      1 ms  1::1
8      1 ms      1 ms      1 ms  1:20::2
```

Trace complete.

Hostname R1:

```
ipv6 unicast-routing

interface GigabitEthernet0/0/0
 ip address 10.0.20.1 255.255.255.0
 negotiation auto
 ipv6 address 1:20::1/64
 ipv6 ospf 1 area 0

interface GigabitEthernet0/0/1
 ip address 10.0.0.1 255.255.255.0
 negotiation auto
 ipv6 address 1::1/64
 ipv6 ospf 1 area 0

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

router ospf 1
 router-id 1.1.1.1
 network 10.0.0.0 0.0.0.255 area 0
 network 10.0.20.0 0.0.0.255 area 0

ipv6 router ospf 1
 router-id 1.1.1.1
```

Hostname R2:

```
ipv6 unicast-routing
```



```
interface GigabitEthernet0/0/0
 ip address 10.0.0.2 255.255.255.0
 negotiation auto
 ipv6 address 1::2/64
 ipv6 ospf 1 area 0

interface GigabitEthernet0/0/1
 ip address 192.168.0.1 255.255.255.0
 negotiation auto
 ipv6 address 2::1/64
 ipv6 ospf 1 area 0

interface Serial0/1/0

interface Serial0/1/1

interface GigabitEthernet0/2/0
 no ip address
 shutdown
 negotiation auto

interface GigabitEthernet0/2/1
 no ip address
 shutdown
 negotiation auto

interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto

router ospf 1
 router-id 2.2.2.2
 redistribute bgp 1 metric 10 subnets
 network 10.0.0.0 0.0.0.255 area 0
 network 192.168.0.0 0.0.0.255 area 0

router bgp 1
 bgp router-id 2.2.2.2
 bgp log-neighbor-changes
 neighbor 2::2 remote-as 2
 neighbor 192.168.0.2 remote-as 2

address-family ipv4
 redistribute connected
 redistribute ospf 1
```



```
no neighbor 2::2 activate
neighbor 192.168.0.2 activate
exit-address-family

address-family ipv6
 redistribute connected
 redistribute ospf 1 metric 10
 neighbor 2::2 activate
exit-address-family

ipv6 router ospf 1
router-id 2.2.2.2
redistribute bgp 1 metric 10
```

Hostname R3:

```
ipv6 unicast-routing

interface Loopback0
 ip address 3.3.3.3 255.255.255.255
 ipv6 address 100:3::3/128
 ipv6 eigrp 1

interface GigabitEthernet0/0/0
 ip address 192.168.0.2 255.255.255.0
 negotiation auto
 ipv6 address 2::2/64
 ipv6 eigrp 1

interface GigabitEthernet0/0/1
 ip address 10.0.1.1 255.255.255.0
 negotiation auto
 ipv6 address 1:1::1/64
 ipv6 eigrp 1

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

router eigrp 1
  network 3.3.3.3 0.0.0.0
  network 10.0.1.0 0.0.0.255
  network 192.168.0.0
  eigrp router-id 3.3.3.3

router bgp 2
  bgp router-id 3.3.3.3
  bgp log-neighbor-changes
  neighbor 2::1 remote-as 1
  neighbor 100:4::4 remote-as 2
  neighbor 100:4::4 update-source Loopback0
  neighbor 100:7::7 remote-as 2
  neighbor 100:7::7 update-source Loopback0
  neighbor 4.4.4.4 remote-as 2
  neighbor 4.4.4.4 update-source Loopback0
  neighbor 7.7.7.7 remote-as 2
  neighbor 7.7.7.7 update-source Loopback0
  neighbor 192.168.0.1 remote-as 1

  address-family ipv4
    redistribute connected
    no neighbor 2::1 activate
    no neighbor 100:4::4 activate
    no neighbor 100:7::7 activate
    neighbor 4.4.4.4 activate
    neighbor 7.7.7.7 activate
    neighbor 7.7.7.7 next-hop-self
    neighbor 192.168.0.1 activate
  exit-address-family

  address-family ipv6
    redistribute connected
    neighbor 2::1 activate
    neighbor 100:4::4 activate
    neighbor 100:7::7 activate
    neighbor 100:7::7 next-hop-self
  exit-address-family

ipv6 router eigrp 1
  eigrp router-id 3.3.3.3

```

Hostname R4:

```
ipv6 unicast-routing
```



```
interface Loopback0
    ip address 4.4.4.4 255.255.255.255
    ipv6 address 100:4::4/128
    ipv6 eigrp 1

interface GigabitEthernet0/0/0
    ip address 10.0.2.2 255.255.255.0
    negotiation auto
    ipv6 address 1:2::2/64
    ipv6 eigrp 1

interface GigabitEthernet0/0/1
    ip address 192.168.1.1 255.255.255.0
    negotiation auto
    ipv6 address 2:1::1/64
    ipv6 eigrp 1

interface Serial0/1/0
    no ip address

interface Serial0/1/1
    no ip address

interface GigabitEthernet0/2/0
    no ip address
    negotiation auto

interface GigabitEthernet0/2/1
    no ip address
    negotiation auto

interface GigabitEthernet0
    vrf forwarding Mgmt-intf
    no ip address
    negotiation auto

router eigrp 1
    network 4.4.4.4 0.0.0.0
    network 10.0.2.0 0.0.0.255
    network 192.168.1.0
    eigrp router-id 4.4.4.4

router bgp 2
    bgp router-id 4.4.4.4
    bgp log-neighbor-changes
    neighbor 2:1::2 remote-as 3
```



```

neighbor 100:3::3 remote-as 2
neighbor 100:3::3 update-source Loopback0
neighbor 100:7::7 remote-as 2
neighbor 100:7::7 update-source Loopback0
neighbor 3.3.3.3 remote-as 2
neighbor 3.3.3.3 update-source Loopback0
neighbor 7.7.7.7 remote-as 2
neighbor 7.7.7.7 update-source Loopback0
neighbor 192.168.1.2 remote-as 3

address-family ipv4
  redistribute connected
  no neighbor 2:1::2 activate
  no neighbor 100:3::3 activate
  no neighbor 100:7::7 activate
  neighbor 3.3.3.3 activate
  neighbor 7.7.7.7 activate
  neighbor 7.7.7.7 next-hop-self
  neighbor 192.168.1.2 activate
exit-address-family

address-family ipv6
  redistribute connected
  neighbor 2:1::2 activate
  neighbor 100:3::3 activate
  neighbor 100:7::7 activate
  neighbor 100:7::7 next-hop-self
exit-address-family

ipv6 router eigrp 1
  eigrp router-id 4.4.4.4

```

Hostname R5:

```

ipv6 unicast-routing

interface GigabitEthernet0/0/0
  ip address 192.168.1.2 255.255.255.0
  ip router isis
  negotiation auto
  ipv6 address 2:1::2/64
  ipv6 router isis

interface GigabitEthernet0/0/1
  ip address 10.0.3.1 255.255.255.0
  ip router isis
  negotiation auto

```



```

ipv6 address 1:3::1/64
ipv6 router isis

interface GigabitEthernet0
vrf forwarding Mgmt-intf
no ip address
shutdown
negotiation auto

router isis
net 49.0012.0000.0000.0005.00
is-type level-1
metric-style wide
log-adjacency-changes
redistribute bgp 3 metric 30 level-1
address-family ipv6
  redistribute bgp 3 metric 30 level-1
exit-address-family

router bgp 3
bgp router-id 5.5.5.5
bgp log-neighbor-changes
no bgp default ipv4-unicast
neighbor 2:1::1 remote-as 2
neighbor 192.168.1.1 remote-as 2

address-family ipv4
  redistribute connected
  redistribute isis level-1 metric 10
  neighbor 192.168.1.1 activate
exit-address-family

address-family ipv6
  redistribute connected
  redistribute isis metric 10 level-1
  neighbor 2:1::1 activate
exit-address-family

```

Hostname R6:

```

ipv6 unicast-routing

interface GigabitEthernet0/0/0
ip address 10.0.3.2 255.255.255.0
ip router isis
negotiation auto
ipv6 address 1:3::2/64

```



```
ipv6 router isis

interface GigabitEthernet0/0/1
 ip address 10.0.30.1 255.255.255.0
 ip router isis
 negotiation auto
 ipv6 address 1:30::1/64
 ipv6 router isis

interface Serial0/1/0
 no ip address
 shutdown

interface Serial0/1/1
 no ip address
 shutdown

interface Service-Engine0/2/0
 no ip address
 shutdown

interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto

interface Vlan1
 no ip address
 shutdown

router isis
 net 49.0012.0000.0000.0006.00
 is-type level-1
 metric-style wide
 log-adjacency-changes
```

Hostname R7:

```
ipv6 unicast-routing

interface Loopback0
 ip address 7.7.7.7 255.255.255.255
 ipv6 address 100:7::7/128
 ipv6 eigrp 1

interface GigabitEthernet0/0/0
```



```
ip address 10.0.1.2 255.255.255.0
negotiation auto
ipv6 address 1:1::2/64
ipv6 eigrp 1

interface GigabitEthernet0/0/1
ip address 10.0.2.1 255.255.255.0
negotiation auto
ipv6 address 1:2::1/64
ipv6 eigrp 1

interface Serial0/1/0
no ip address

interface Serial0/1/1
no ip address

interface GigabitEthernet0/2/0
no ip address
negotiation auto

interface GigabitEthernet0/2/1
no ip address
negotiation auto

interface GigabitEthernet0
vrf forwarding Mgmt-intf
no ip address
negotiation auto

interface Vlan1
no ip address

router eigrp 1
network 7.7.7.7 0.0.0.0
network 10.0.1.0 0.0.0.255
network 10.0.2.0 0.0.0.255
eigrp router-id 7.7.7.7

router bgp 2
bgp router-id 7.7.7.7
bgp log-neighbor-changes
neighbor 100:3::3 remote-as 2
neighbor 100:3::3 update-source Loopback0
neighbor 100:4::4 remote-as 2
neighbor 100:4::4 update-source Loopback0
neighbor 3.3.3.3 remote-as 2
```



```
neighbor 3.3.3.3 update-source Loopback0
neighbor 4.4.4.4 remote-as 2
neighbor 4.4.4.4 update-source Loopback0

address-family ipv4
  no neighbor 100:3::3 activate
  no neighbor 100:4::4 activate
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 route-reflector-client
  neighbor 4.4.4.4 activate
  neighbor 4.4.4.4 route-reflector-client
exit-address-family

address-family ipv6
  neighbor 100:3::3 activate
  neighbor 100:3::3 route-reflector-client
  neighbor 100:4::4 activate
  neighbor 100:4::4 route-reflector-client
exit-address-family

ipv6 router eigrp 1
  eigrp router-id 7.7.7.7
```

PROBLEMS:

Although there weren't significant challenges, when we were testing out our pings from our PCs, we realized that we couldn't ping from the end devices at all, even though Router 1 could ping Router 6. We soon realized that the physical Ethernet connection between PC0 and Router 1 and between PC1 and Router 6 was not set up; after that, we were successfully able to ping from end-to-end!

CONCLUSION:

This lab was very complex and took some time for me to understand due to how iBGP needed to run inside the Interior Gateway Protocol (EIGRP in our case), eBGP needed to connect the different Autonomous Systems, and we still needed to set up IS-IS and OSPF. However, after extensive research, I feel that I've gained a lot of knowledge from this lab and got reminded to never forget to plug in the Ethernet cables to the PCs when setting up the topology!



TEACHER SIGN-OFF:

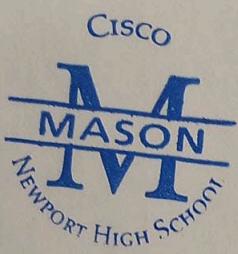
Configuring a multiprotocol Network with iBGP

Alysia Chen

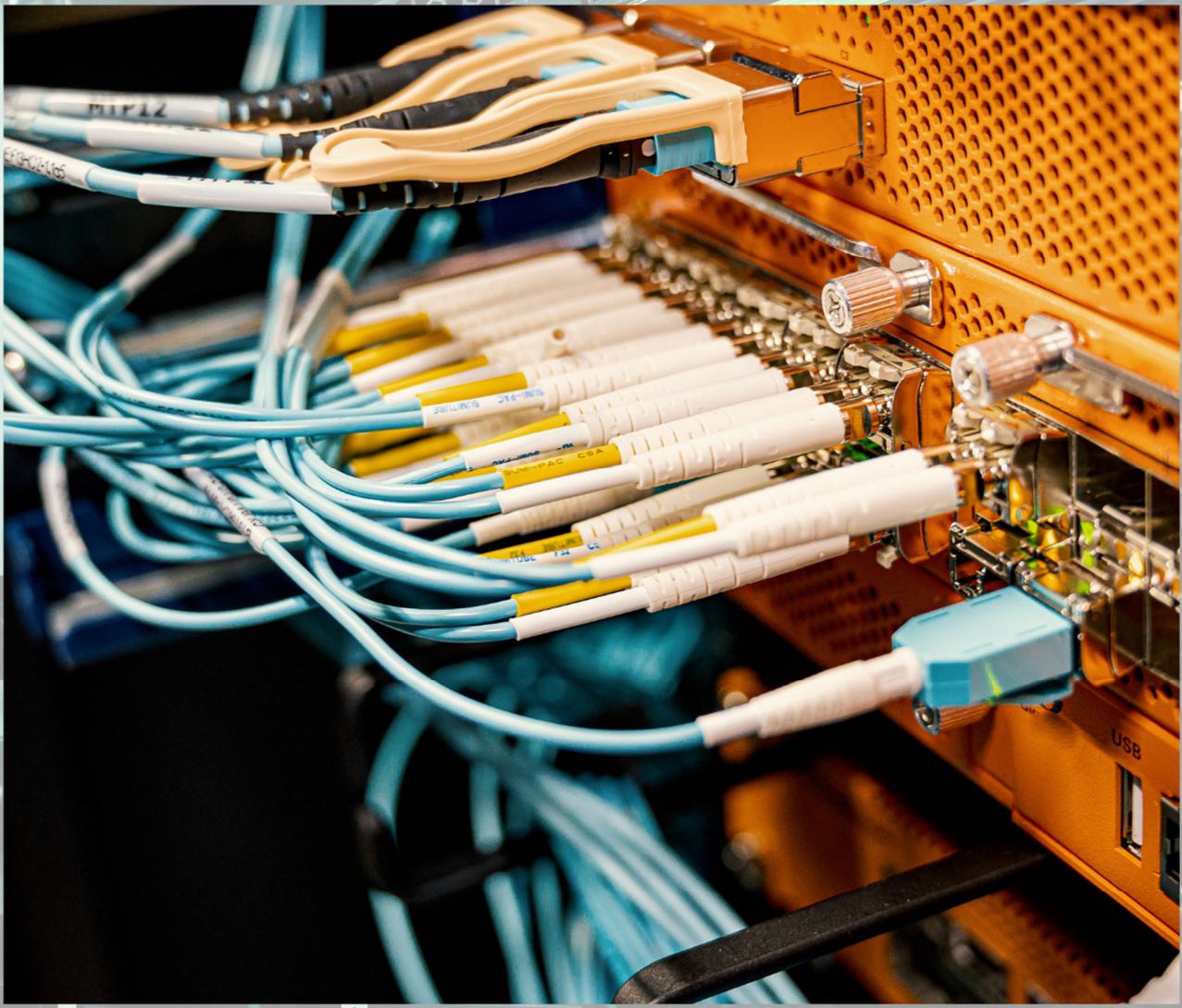
P3-4

CCNP

Mr. Mason



Lab 5: Amazon Cloud Foundations 1-3



PURPOSE:

Learn to configure AWS IAM, build a VPC and launch a web server, and learn about Amazon EC2.

BACKGROUND INFORMATION ON LAB CONCEPTS:

IAM:

AWS Identity and Access Management has many purposes. Some of these purposes include the management of IAM Users (which are individuals), including their credentials and permissions; the management of IAM Roles (which can be assigned to anyone and multiple people at once if needed), including their credentials and permissions; and the management of identity federation so that existing users can have access permissions without needing to create individual IAM User credentials. Authentication is provided by matching a new user's sign-in credentials to a principal (an IAM user, federated user, IAM role, or application) that is trusted; a request is made to grant the principal access to resources, which will be allowed only if the user has permission.

VPC:

Amazon Virtual Private Cloud, also known as Amazon VPC, enables one to launch Amazon Web Services (AWS) into a virtual network that is defined by the network administrator. This virtual network is similar to a traditional network, but with the added benefits of scalability and flexibility. A VPC may span multiple Availability Zones. VPC has subnets (a range of IP addresses) that must be in a single Availability Zone. The network administrator can assign IP addresses (both IPv4 and IPv6) to VPCs and subnets. Gateways connect a VPC to another network; endpoints connect a VPC to AWS privately (without using internet gateway or a NAT device). Transit gateways act like central hubs to route traffic between the networks of VPCs and other connections.

EC2:

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that allows for scalability in the cloud. EC2 has over 750 instances and choice of the latest processor, storage, networking, operating system, and purchase model—the broadest and deepest compute platform. Benefits include on-demand infrastructure, secure compute, optimization, and more.

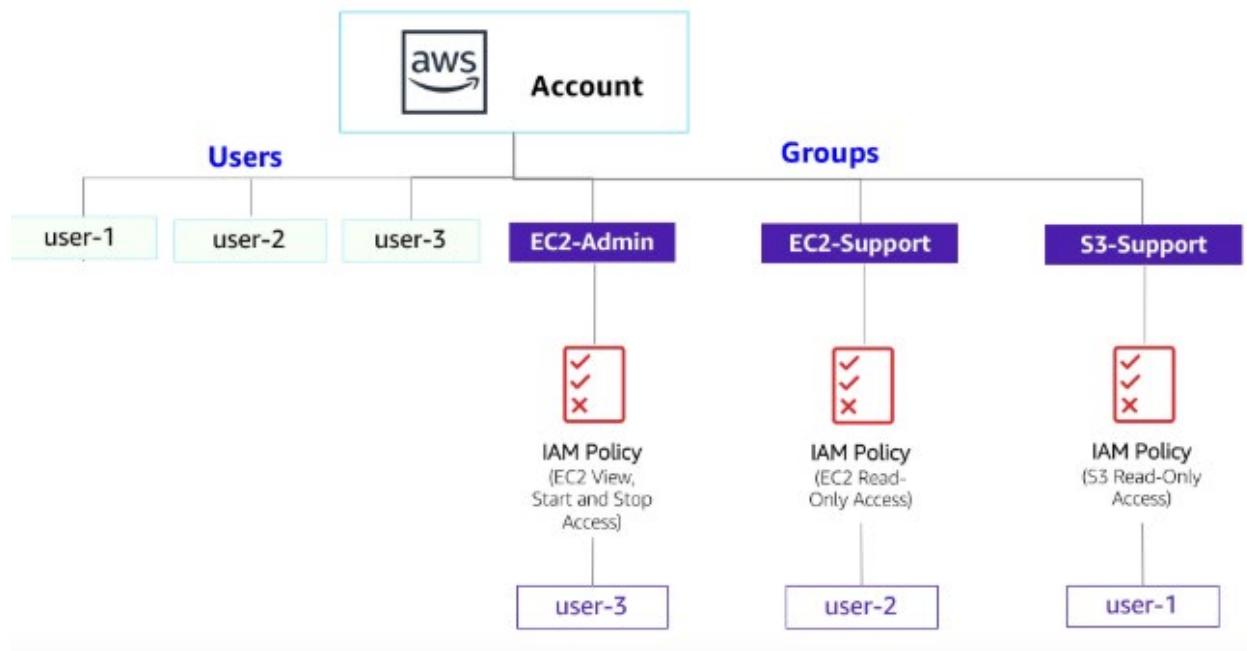
LAB SUMMARY:

In these labs, I learned about different services that Amazon AWS offers—their purposes and how they work. I used the AWS Console and terminal sessions to complete different tasks, including configurations and checks.

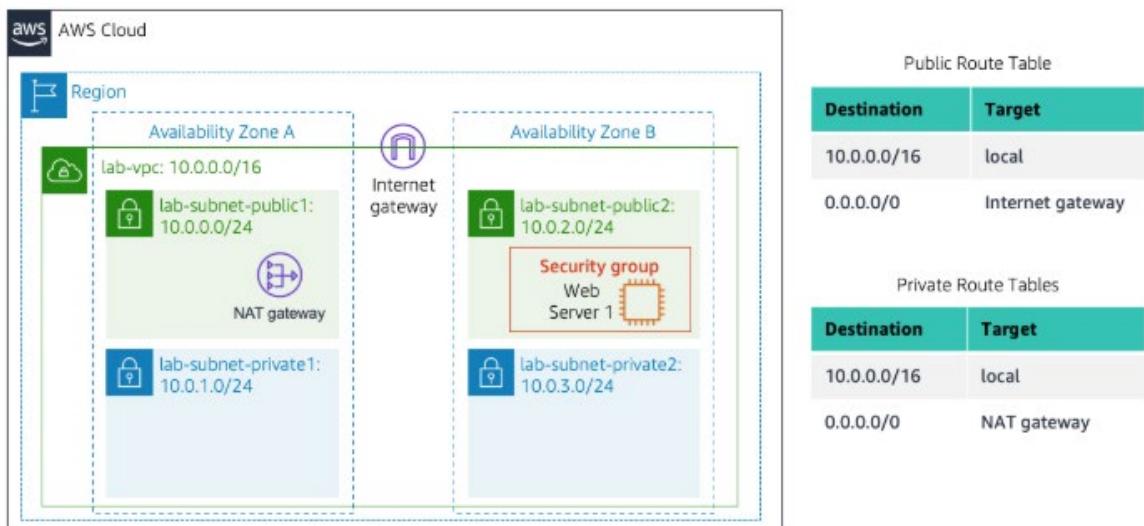


DIAGRAMS:

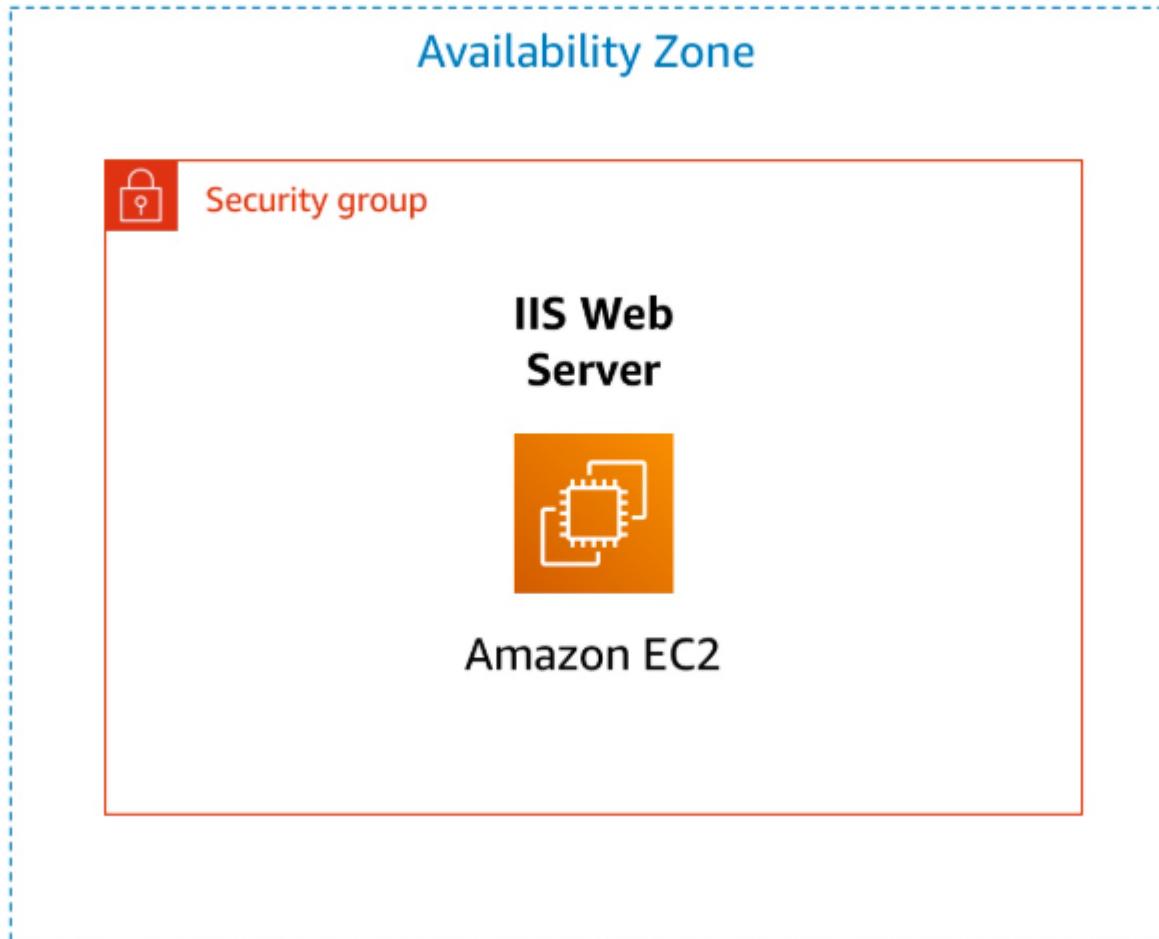
Lab 1



Lab 2



Lab 3



LAB COMMANDS:

LAB 1

Go into the search box to open the IAM console and choose Users in the navigation pane.



The screenshot shows the AWS IAM Users page. At the top, there are navigation links for AWS, Home, Search, Notifications, Help, and a dropdown for the current user. The URL in the address bar is `voclabs/user3701192=Alys`. Below the header, the navigation path is `IAM > Users`. On the right, there are three buttons: a blue 'Info' button, a grey 'Delete' button, and an orange 'Create user' button.

The main section is titled 'Users (4) Info' with a 'Create user' button. A descriptive text below says, 'An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.' There is a search bar labeled 'Search' and a pagination control showing page 1 of 1.

The table lists four users:

User name	Path	Groups	Last modified
awsstudent	/	Access denied	Edit
user-1	/spl66/	0	-
user-2	/spl66/	0	-
user-3	/spl66/	0	-

Click on the user-1 link, which will bring you to the Permissions tab as shown below:

The screenshot shows a navigation bar at the top with tabs: 'Permissions' (highlighted in blue), 'Groups', 'Tags (1)', and 'Security credentials'. Below the navigation bar is a section titled 'Permissions policies (0)' with three buttons: 'Add permissions' (highlighted in blue), 'Remove', and a circular icon with a 'C'.

Below this section, a message states: 'Permissions are defined by policies attached to the user directly or through groups.' There is a 'Filter by Type' button above a search bar and a dropdown menu set to 'All types'.

At the bottom of the page, there is a message: 'No resources to display'.

Choose the Groups tab.

The screenshot shows the AWS IAM Groups tab selected. At the top, there are tabs for Permissions, Groups (which is underlined in blue), Tags (1), and Security credentials. Below the tabs, a section titled "User groups membership" contains a "Remove" button and a "Add user to groups" button. A descriptive text explains that a user group is a collection of IAM users and can have up to 10 groups. A table header row includes "Group name" and "Attached policies". The main content area displays a message "No resources" and a note that the user does not belong to any groups.

Then, look at the Security credentials tab; user-1 has a Console password assigned.

The screenshot shows the AWS IAM Security credentials tab. It features a "Console sign-in" section with a "Manage console access" button. Under "Console sign-in link", there is a checkbox next to a URL: <https://787399707848.signin.aws.amazon.com/console>. To the right, there is a "Console password" section showing it was updated 26 minutes ago (2025-01-31 15:46 PST). Below that is a "Last console sign-in" section indicating "Never".

In the navigation pane, choose User groups.



User groups (3) Info


[Delete](#)
[Create group](#)

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

 Search

< 1 >

<input type="checkbox"/>	Group name	▲	Users	▼	Permissions	▼
<input type="checkbox"/>	EC2-Admin		⚠ 0	✓ Defined		
<input type="checkbox"/>	EC2-Support		⚠ 0	✓ Defined		
<input type="checkbox"/>	S3-Support		⚠ 0	✓ Defined		

From these groups, click on the EC2-Support group. Choose the Permissions tab.

EC2-Support Info

[Delete](#)

Summary

[Edit](#)
User group name

EC2-Support

Creation time

January 31, 2025, 15:46 (UTC-08:00)

ARN

arn:aws:iam::787399707848:grou
p/spl66/EC2-Support

The screenshot shows the 'Permissions policies' section of the AWS IAM console. It displays a single policy named 'AmazonEC2ReadOnlyAccess'. The interface includes a search bar, filter options, and navigation controls.

Policy name	Type	Attached to
AmazonEC2ReadOnlyAccess	AWS managed	1

Click on the plus (+) icon to expand the AmazonEC2ReadOnlyAccess row. This policy is called a Managed Policy, and they are pre-built policies whose changes will be applied to all Users and Groups associated.

<input type="checkbox"/>	Policy name	Type	<input type="checkbox"/> Attac...
<input type="checkbox"/>		AWS managed	<input type="checkbox"/> 1

AmazonEC2ReadOnlyAccess

Provides read only access to Amazon EC2 via the AWS Management Console.

```

1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Effect": "Allow",
6              "Action": [
7                  "ec2:Describe*",
8                  "ec2:GetSecurityGroupsForVpc"
9              ],
10             "Resource": "*"
11         },
12         {
13             "Effect": "Allow",
14             "Action": "elasticloadbalancing:Describe*",
15             "Resource": "*"
16         },
17         {
18             "Effect": "Allow",

```

Enter the S3-Support group's Permissions tab, noticing how the S3-Support group has the AmazonS3ReadOnlyAccess policy.

S3-Support <small>Info</small>	<input type="button" value="Delete"/>								
<p>Summary</p> <table border="0"> <tr> <td>User group name</td> <td>Creation time</td> </tr> <tr> <td>S3-Support</td> <td>January 31, 2025, 15:46 (UTC-08:00)</td> </tr> <tr> <td>ARN</td> <td><input type="button" value="Edit"/></td> </tr> <tr> <td colspan="2"><input type="checkbox"/> arn:aws:iam::787399707848:grou p/spl66/S3-Support</td> </tr> </table>		User group name	Creation time	S3-Support	January 31, 2025, 15:46 (UTC-08:00)	ARN	<input type="button" value="Edit"/>	<input type="checkbox"/> arn:aws:iam::787399707848:grou p/spl66/S3-Support	
User group name	Creation time								
S3-Support	January 31, 2025, 15:46 (UTC-08:00)								
ARN	<input type="button" value="Edit"/>								
<input type="checkbox"/> arn:aws:iam::787399707848:grou p/spl66/S3-Support									



The screenshot shows the AWS IAM Permissions policies page. At the top, there are three tabs: 'Users (1)', 'Permissions' (which is selected), and 'Access Advisor'. Below the tabs, it says 'Permissions policies (1) [Info](#)'. There are three buttons: 'Simulate [↗](#)' (highlighted in blue), 'Remove', and 'Add permissions [▼](#)'. A note says 'You can attach up to 10 managed policies.' Below this is a 'Filter by Type' section with a search bar and a dropdown set to 'All types'. A pagination indicator shows '1' of 1 page. The main table has columns: 'Policy name [↗](#)', 'Type', and 'Attached to'. One row is shown: 'AmazonS3ReadOn...', 'AWS managed', and '1'. The Cisco logo is at the bottom left, and the name 'Alysia Chen' is at the bottom right.

Policy name ↗	Type	Attached to
AmazonS3ReadOn...	AWS managed	1

Next, go into the EC2-Admin group link and choose the Permissions tab. This group has an Inline Policy, which is used to apply permissions to exceptions.

The screenshot shows the AWS IAM 'Permissions policies' page for the 'EC2-Admin' user group. The page title is 'Permissions policies (1) [Info](#)'. Below it are three buttons: 'Simulate' (highlighted in blue), 'Remove', and 'Add permissions'. A note says 'You can attach up to 10 managed policies.' There is a search bar and a filter dropdown set to 'All types'. The main table lists one policy:

<input type="checkbox"/>	Policy name EC2-Admin-Policy	Type	Attachments
<input type="checkbox"/>	EC2-Admin-Policy	Customer inline	0

Clicking on the policy name 'EC2-Admin-Policy' opens its details view. The title is 'EC2-Admin-Policy'. It includes 'Copy JSON' and 'Edit' buttons. The JSON code is displayed:

```

1  {
2    "Version": "2012-10-17",
3    "Statement": [
4      {
5        "Action": [
6          "ec2:Describe*",

```

Let's add users to groups. First, navigate to the S3-Support group and choose the Users tab.

☰ [IAM](#) > [User groups](#) > [S3-Support](#)

The screenshot shows the AWS IAM User Groups page. At the top, there are three tabs: **Users** (which is highlighted with a blue underline), **Permissions**, and **Access Advisor**. Below the tabs, the heading **Users in this group (0)** is displayed, along with a **Remove** button and a **Add users** button. A search bar with the placeholder **Search** is present. To the right of the search bar are navigation icons for pages 1, 2, and 3, and a gear icon for settings. Below the search bar, there is a column header with a checkbox icon and the text **User name**. To the right of the column header are icons for **Groups** and **Actions**. The main content area below the header contains the message **No resources to display**.

Add user-1 by selecting the button and checking the box next to user-1.

Add users to S3-Support Info

Other users in this account (1/4)

user X 3 matches

< 1 > |

User name	Groups
<input checked="" type="checkbox"/> user-1	0
<input type="checkbox"/> user-2	0
<input type="checkbox"/> user-3	0

[Cancel](#) [Add users](#)

As you can see, user-1 has been added:

The screenshot shows the AWS IAM Groups interface. At the top, there are three tabs: 'Users' (1), 'Permissions', and 'Access Advisor'. The 'Users' tab is selected. Below the tabs, a heading says 'Users in this group (1)'. To the right of this heading are three buttons: a blue circular button with a white 'C' (Copy), a grey 'Remove' button, and a blue 'Add users' button. A descriptive text follows: 'An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.' Below this is a search bar with the placeholder 'Search' and a magnifying glass icon. Underneath the search bar are navigation controls: a left arrow, a page number '1', a right arrow, and a gear icon for settings. There are two columns of data: 'User name' and 'Groups'. The first row shows a checkbox next to 'user-1', which is underlined, indicating it is selected. The second column shows the value '1'.

Add user-2 and user-3 to EC2-Support and EC2-Admin, respectively.

The screenshot shows the AWS IAM User Groups page for the group 'EC2-Support'. The navigation path is: IAM > User groups > EC2-Support. There are three tabs at the top: 'Users' (1), 'Permissions', and 'Access Advisor'. The 'Users' tab is selected. Below it, a section titled 'Users in this group (1)' shows one user named 'user-2'. There are buttons for 'Remove' and 'Add users'. A search bar and pagination controls are also present. The user 'user-2' is listed with a checkbox next to its name.

User Name	Groups
user-2	1

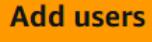
Add users to EC2-Admin Info

Other users in this account (1/4) 

us  3 matches 

< 1 > 

 User name 	 Groups
<input type="checkbox"/> user-1	1
<input type="checkbox"/> user-2	1
<input checked="" type="checkbox"/> user-3	0

The screenshot shows the AWS IAM User Groups page for the 'EC2-Admin' group. The navigation path is: IAM > User groups > EC2-Admin. The 'Users' tab is selected, showing 1 user in the group: 'user-3'. The 'Permissions' and 'Access Advisor' tabs are also visible. A modal window titled 'Users in this group (1)' displays the user 'user-3'. The modal includes a search bar, pagination (page 1 of 1), and buttons for 'Remove' and 'Add users'. The user list table has columns for 'User name' and 'Groups', with 'user-3' listed under 'Groups'.

User name	Groups
user-3	1

Next, navigate to Dashboard to access the sign-in URL for IAM users, opening it in a private window.

IAM resources



Resources in this AWS Account

User groups

3

Users

4

Roles

14

Policies

1

Identity providers

0

AWS Account

Account ID 787399707848**Account Alias**[Create](#)**Sign-in URL for IAM users in this account** <https://787399707848.signin.aws.amazon.com/console>Access the user-1 account through the IAM user name **user-1** and password **Lab-Password1**.

United States (Ohio) ▾

user-1 @ 7873-9970-7848 ▾

[Reset to default layout](#)[+ Add widgets](#)

⋮ Applications (0)

[Create application](#)

Region: US East (Ohio)

us-east-2 (Current Region) ▾

 Find applications

Search for and open the S3 console through the search box, in which the user should be able to view the list of buckets and contents as part of the S3-Support group.

The screenshot shows the Amazon S3 console interface. On the left, there is a navigation sidebar with sections like 'Amazon S3' (General purpose buckets, Directory buckets, Table buckets, Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3), 'Storage Lens' (Dashboards, Storage Lens groups, AWS Organizations settings), and 'AWS Marketplace for S3'. The main area displays an 'Account snapshot - updated every 24 hours' with a link to 'View Storage Lens dashboard'. Below this, under 'General purpose buckets', there is a table showing one bucket named 'samplebucket--7ef4b050'. The table includes columns for Name, AWS Region, IAM Access Analyzer, and Creation date. The bucket details show it was created on January 31, 2025, at 15:45:55 (UTC-08:00) in US East (N. Virginia) us-east-1. There are buttons for 'Copy ARN', 'Empty', 'Delete', and 'Create bucket'.

samplebucket--7ef4b050 [Info](#)

This screenshot shows the object list for the 'samplebucket--7ef4b050' bucket. At the top, there is a navigation bar with tabs for 'Objects', 'Metadata', 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. The 'Objects' tab is selected. Below the navigation bar, there is a section titled 'Objects (0)' with a table header for 'Name', 'Type', 'Last modified', 'Size', and 'Storage class'. A large orange button labeled 'Upload' is prominently displayed. A message below the table states: 'Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions.' There is also a link to 'Learn more'.

Next, go to the search box and choose EC2.



The screenshot shows the AWS EC2 Dashboard with the following sections:

- Resources:** A summary of Amazon EC2 resources in the US East (N. Virginia) Region. It includes:

Instances (running)	0	Auto Scaling Groups	✖ API Error
Capacity Reservations	✖ API Error	Dedicated Hosts	✖ API Error
Elastic IPs	✖ API Error	Instances	✖ API Error
Key pairs	✖ API Error	Load balancers	✖ API Error
Placement groups	✖ API Error	Security groups	✖ API Error
Snapshots	✖ API Error	Volumes	✖ API Error
- Launch instance:** Options to launch an instance or migrate a server. A note states: "To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud."
 - Launch instance**
 - Migrate a server**
- Service health:** An error occurred retrieving service health information. A link to "Diagnose with Amazon Q" is provided.
- Zones:** A table with columns for Zone name and Zone ID.
- Instance alarms:** A section for monitoring instances.

On the left sidebar, the following navigation items are visible:

- Dashboard** (selected)
- EC2 Global View
- Events
- Instances** (expanded)
 - Instances
 - Instance Types
 - Launch Templates
 - Spot Requests
 - Savings Plans
 - Reserved Instances
 - Dedicated Hosts
 - Capacity Reservations
- Images** (expanded)
 - AMIs
 - AMI Catalog
- Elastic Block Store** (expanded)
 - Volumes
 - Snapshots
 - Lifecycle Manager
- Network & Security** (expanded)
 - Security Groups
 - Elastic IPs
 - Placement Groups
 - Key Pairs

At the bottom of the dashboard, there are links for CloudShell and Feedback, and a copyright notice: © 2025, Amazon Web Services.

Choose Instances.



The screenshot shows the AWS EC2 Instances page. The left sidebar includes sections for Dashboard, EC2 Global View, Events, Instances (selected), Images, Elastic Block Store, Network & Security, and more. The main content area is titled "Instances Info". It features a search bar, filter buttons for "All states" and "Actions", and a "Launch instances" button. A prominent red-bordered error message box states: "You are not authorized to perform this operation. User: arn:aws:iam::787399707848:user/spl66/user-1 is not authorized to perform: ec2:DescribeInstances because no identity-based policy allows the ec2:DescribeInstances action". Below the error message is a "Select an instance" section.

The user does not have permission to view instances. Now, sign out, use the URL from the IAM dashboard, and sign in as user-2 (IAM user name **user-2** and password **Lab-Password2**). Navigate to EC2 Instances.

The screenshot shows the AWS EC2 Instances page after logging in as user-2. The left sidebar remains the same. The main content area is titled "Instances (2) Info". It shows two running instances: "LabHost" and "Bastion Host". The "LabHost" instance has an ID of i-0b182d7885e77d9c4 and is a t2.micro type. The "Bastion Host" instance has an ID of i-039db931ebcb05b2d and is also a t2.micro type. Both instances are marked as "Running" and have "2/2 checks passed". The "View alarms" and "us-east-1a" status are also visible. The "Select an instance" section is present below the instance list.

Select LabHost. In the Instance state menu, select Stop instance, as seen below:



The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with sections like Dashboard, EC2 Global View, Events, Instances (with sub-options like Instance Types, Launch Templates, etc.), Images, Elastic Block Store, Network & Security, and more. The main area displays two instances: 'LabHost' (i-0b182d7885e77d9c4) and 'Bastion Host' (i-039db931ebcb05b2d). The 'LabHost' instance is selected. A context menu is open over it, with 'Stop instance' highlighted. Below the instances, there are tabs for Details, Status and alarms, Monitoring, Security, Networking, Storage, and Tags.

There is an error message because you are unauthorized to stop this instance.

The screenshot shows the same AWS EC2 Instances page as the previous one, but with a large red box highlighting an error message. The message reads: 'Failed to stop the instance i-0b182d7885e77d9c4. You are not authorized to perform this operation. User: arn:aws:iam::787399707848:user/spl66/user-2 is not authorized to perform: ec2:StopInstances on resource: arn:aws:ec2:us-east-1:787399707848:instance/i-0b182d7885e77d9c4 because no identity-based policy allows the ec2:StopInstances action. Encoded authorization failure message: [long encoded string]'. Below the error message, the instance details for 'LabHost' are shown, including its ID, public and private IP addresses, and state.

To check whether user-2 can also access S3 like user-1, search for the S3 console and view the buckets. It turns out that user-2 does not have permission to view the buckets.



Account snapshot - updated every 24 hours [All AWS Regions](#)

Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. [Learn more](#)

[View Storage Lens dashboard](#)

General purpose buckets [Info](#) [All AWS Regions](#)

Buckets are containers for data stored in S3.

Find buckets by name

Name	AWS Region	IAM Access Analyzer	Creation date
You don't have permissions to list buckets After you or your AWS administrator has updated your permissions to allow the s3>ListAllMyBuckets action, refresh this page. Learn more about Identity and access management in Amazon S3			

[Create bucket](#)

Sign out and sign in again as user-3 with the password Lab-Password3. Open the EC2 console and select Instances. You should be able to stop the LabHost instance this time.

Instances (1/2) [Info](#) Last updated less than a minute ago

Find Instance by attribute or tag (case-sensitive)

Actions

- Stop instance
- Start instance
- Reboot instance
- Hibernate instance
- Terminate (delete) instance

Instance state

Launch instances

Instance state = running

Details Status and alarms Monitoring Security Networking Storage Tags

Instance summary

Instance ID i-0b182d7885e77d9c4	Public IPv4 address 18.232.180.6 open address	Private IPv4 addresses 10.1.11.218
IPv6 address -	Instance state Running	Public IPv4 DNS ec2-18-232-180-6.compute-1.amazonaws.com open address
Hostname type	Private IP DNS name (IPv4 only)	



Instances (2) [Info](#)

Last updated less than a minute ago [Connect](#) [Instance state](#) [Actions](#) [Launch instances](#)

Find Instance by attribute or tag (case-sensitive) [All states](#)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability
LabHost	i-0b182d7885e77d9c4	Stopped	t2.micro	-	User: arn:aws:	us-east-1a
Bastion Host	i-039db931ebcb05b2d	Running	t2.micro	2/2 checks passed	User: arn:aws:	us-east-1a

LAB 2

Navigate to the VPC console using the search box and click on Create VPC.

[Create VPC](#) [Launch EC2 Instances](#)

Note: Your Instances will launch in the US East region.

Resources by Region [Refresh Resources](#)

You are using the following Amazon VPC resources

VPCs ▶ See all regions	US East 2	NAT Gateways ▶ See all regions	US East 0
Subnets ▶ See all regions	US East 7	VPC Peering Connections ▶ See all regions	US East 0



Select VPC and more in the VPC settings “Resources to create”.

The screenshot shows the AWS VPC settings page for creating a new VPC. At the top, the navigation bar includes links for 'aws', 'Your VPCs', and 'Create VPC'. Below the navigation is a section titled 'Create VPC' with an 'Info' link. A descriptive text explains that a VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances. It also states that users can mouse over a resource to highlight the related resources. The main configuration area is titled 'VPC settings' and contains a section for 'Resources to create' with an 'Info' link. Below this, there are two options: 'VPC only' and 'VPC and more'. The 'VPC and more' option is selected, indicated by a blue outline around its button and a blue dot next to the text. To the right of the main content area, there is a vertical sidebar with a large letter 'P'.

Next, under Name tag auto-generation, set the value that's auto-generated to **lab**. Keep the IPv4 CIDR block setting, number of public subnets, and number of private subnets. Set the number of availability zones to **1**.

VPC settings

Resources to create [Info](#)

Create only the VPC resource or the VPC and other networking resources.

VPC only

VPC and more

Name tag auto-generation [Info](#)

Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

Auto-generate

lab

IPv4 CIDR block [Info](#)

Determine the starting IP and the size of your VPC using CIDR notation.

10.0.0.0/16

65,536 IPs

CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)

- No IPv6 CIDR block
- Amazon-provided IPv6 CIDR block



Number of Availability Zones (AZs) [Info](#)

Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

1 2 3

► Customize AZs

Number of public subnets [Info](#)

The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

0 **1**

Number of private subnets [Info](#)

The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

0 **1** 2

▼ Customize subnets CIDR blocks

Public subnet CIDR block in us-east-1a

10.0.0.0/24	256 IPs
-------------	---------

Expanding the Customize subnets CIDR blocks section, change the Public subnet CIDR block in us-east-1a to **10.0.0.0/24** and change Private subnet CIDR block in us-east-1a to **10.0.1.0/24**. Set NAT gateways to **In 1 AZ**. Set VPC endpoints to **None**. Enable both DNS hostnames and DNS resolution.



Private subnet CIDR block in us-east-1a

10.0.1.0/24

256 IPs

NAT gateways (\$) [Info](#)

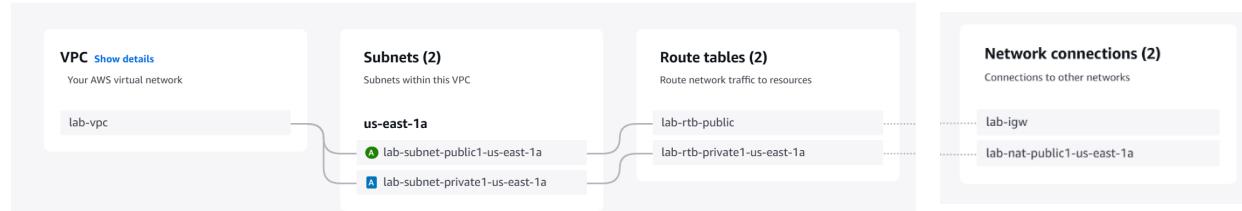
Choose the number of Availability Zones (AZs) in which to create NAT gateways.
Note that there is a charge for each NAT gateway

None**In 1 AZ****1 per AZ****VPC endpoints** [Info](#)

Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

None**S3 Gateway****DNS options** [Info](#)

- Enable DNS hostnames
- Enable DNS resolution

Preview

After clicking Create VPC, make sure it is complete before continuing:



Alysia Chen

Create VPC workflow

✓ Success

▼ Details

- ✓ Create VPC: [vpc-0d33058613d468d48](#) ↗
- ✓ Enable DNS hostnames
- ✓ Enable DNS resolution
- ✓ Verifying VPC creation: [vpc-0d33058613d468d48](#) ↗
- ✓ Create subnet: [subnet-0178ef5ee1932ca44](#) ↗
- ✓ Create subnet: [subnet-0202c40f5f1a36f18](#) ↗
- ✓ Create internet gateway: [igw-04f41534d6ddbf9f](#) ↗
- ✓ Attach internet gateway to the VPC
- ✓ Create route table: [rtb-0e8579a0804968da8](#) ↗
- ✓ Create route
- ✓ Associate route table
- ✓ Allocate elastic IP: [eipalloc-0e71e2ed8cae99508](#) ↗
- ✓ Create NAT gateway: [nat-0198db2e4fc51fdfd](#) ↗

Choose View VPC to look at the settings using the VPC console links. Some options are to select Subnets and Route tables to look through those details.



subnet-0178ef5ee1932ca44 / lab-subnet-public1-us-east-1a

Actions ▾

Details

Subnet ID

subnet-0178ef5ee1932ca44

IPv4 CIDR

10.0.0.0/24

Availability Zone

us-east-1a

Route table

[rtb-0e8579a0804968da8 | lab-rtb-public](#)

Auto-assign IPv6 address

No

Subnet ARN

arn:aws:ec2:us-east-1:877002603542:subnet/subnet-0178ef5ee1932ca44

Available IPv4 addresses

250

Availability Zone ID

use1-az2

Network ACL

[acl-04dc06315b61731cc](#)

Auto-assign customer-owned IPv4 address

rtb-057e9bf174445d743 / lab-rtb-private1-us-east-1a

Actions ▾

Details Info

Route table ID

rtb-057e9bf174445d743

Main

No

VPC

[vpc-0d33058613d468d48 | lab-vpc](#)

Owner ID

877002603542

Explicit subnet associations

[subnet-0202c40f5f1a36f18 / lab-subnet-private1-us-east-1a](#)

Edge associations

-

Now, create additional subnets by selecting Subnets from the left navigation pane. Choose Create subnet.

Subnets (7) Info

Last updated
12 minutes ago



Actions ▾

Create subnet



Find resources by attribute or tag

< 1 > |

| Name

▼ | Subnet ID

-

[subnet-009ffcd7362c3f2f](#)

-

[subnet-01dbe3c3b762d3a6f](#)

-

[subnet-0155154deb7541c84](#)



Select a subnet



Alysia Chen

Configure the following: VPC ID (use **lab-vpc**), subnet name (**lab-subnet-public2**), Availability Zone (select the second Availability Zone from the top), and IPv4 CIDR block (**10.0.2.0/24**).

Create subnet Info

VPC

VPC ID

Create subnets in this VPC.

vpc-0d33058613d468d48 (lab-vpc) ▾

Associated VPC CIDRs

IPv4 CIDRs

10.0.0.0/16

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

lab-subnet-public2

The name can be up to 256 characters long.

Availability Zone Info

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

US East (N. Virginia) / us-east-1b ▾

IPv4 VPC CIDR block Info

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

10.0.0.0/16 ▾

IPv4 subnet CIDR block

10.0.2.0/24

256 IPs



Next, create a second private subnet (since a second public subnet was created). Use the same settings, but change the subnet name to **lab-subnet-private2** and the IPv4 CIDR block to **10.0.3.0/24**.

Create subnet Info

VPC

VPC ID

Create subnets in this VPC.

vpc-0d33058613d468d48 (lab-vpc) ▾

Associated VPC CIDRs

IPv4 CIDRs

10.0.0.0/16



Subnet 1 of 1

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

lab-subnet-private2

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

US East (N. Virginia) / us-east-1b



IPv4 VPC CIDR block [Info](#)

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

10.0.0.0/16



IPv4 subnet CIDR block

10.0.3.0/24

256 IPs

Next, in the left navigation pane, select Route tables.



Last updated less than a minute ago

Actions

Create route table

Find resources by attribute or tag

<input type="checkbox"/>	Name	Route table ID
<input type="checkbox"/>	lab-rtb-private1-us-east-1a	rtb-057e9bf174445d743
<input type="checkbox"/>	lab-rtb-public	rtb-0e8579a0804968da8

Check the box for the lab-rtb-private1-us-east-1a route table.

<input type="checkbox"/>	Name	Route table ID
<input checked="" type="checkbox"/>	lab-rtb-private1-us-east-1a	rtb-057e9bf174445d743
<input type="checkbox"/>	lab-rtb-public	rtb-0e8579a0804968da8

rtb-057e9bf174445d743 / lab-rtb-private1-us-east-1a

Routes (2)

Both **Edit routes**

Filter routes

Notice that in the Routes tab pictured above, Destination 0.0.0.0/0 is set to Target nat-xxxxxxxxx, showing that traffic going towards the Internet, which has an IP address of 0.0.0.0/0, will be sent to the NAT Gateway before being forwarded to the Internet.



A screenshot of the AWS Route Tables interface. At the top, there is a search bar labeled "Filter routes" and navigation controls (back, forward, and settings). Below is a table with the following columns: Destination, Target, Status, and Propagated. There are two entries:

Destination	Target	Status	Propagated
0.0.0.0/0	nat-0198db...	Active	No
10.0.0.0/16	local	Active	No

Next, click on the Subnet associations tab and click on Edit subnet associations.

A screenshot of the AWS Route Table details page for route table ID "rtb-057e9bf174445d743". The top section shows the name "lab-rtb-private1-us-east-1a" and the route table ID. Below is a table with columns: Name and Route table ID. Two subnets are listed: "lab-rtb-private1-us-east-1a" (selected) and "lab-rtb-public".

Name	Route table ID
<input checked="" type="checkbox"/> lab-rtb-private1-us-east-1a	rtb-057e9bf174445d743
<input type="checkbox"/> lab-rtb-public	rtb-0e8579a0804968da8

The route table ID "rtb-057e9bf174445d743 / lab-rtb-private1-us-east-1a" is displayed prominently. Below, there are tabs for Details, Routes, Subnet associations (which is selected), and Edge associations. The Subnet associations tab shows "Explicit subnet associations (1)" and an "Edit subnet associations" button. A search bar at the bottom allows finding a subnet association.

Select both lab-subnet-private1-us-east-1a and lab-subnet-private2, before selecting Save associations.

Available subnets (2/4)

<input type="text"/> Filter subnet associations			
	Name	Subnet ID	IPv4 CIDR
<input type="checkbox"/>	lab-subnet-public1-us-e...	subnet-0178ef5ee1932...	10.0.0.0/24
<input checked="" type="checkbox"/>	lab-subnet-private1-us-east-1a	subnet-0202c40f5f1a36f18...	10.0.1.0/24
<input type="checkbox"/>	lab-subnet-public2	subnet-01f99b36a0745...	10.0.2.0/24
<input checked="" type="checkbox"/>	lab-subnet-private2	subnet-01ffcf6a42b204323...	10.0.3.0/24

Selected subnets

[subnet-0202c40f5f1a36f18 / lab-subnet-private1-us-east-1a](#) 

[subnet-01ffcf6a42b204323 / lab-subnet-private2](#) 

[Cancel](#)

[Save associations](#)

There should be a pop-up as such:

 You have successfully updated subnet associations for rtb-057e9bf174445d743 / lab-rtb-private1-us-east-1a.



Next, deselect lab-rtb-private1-us-east-1a and select lab-rtb-public.

<input type="checkbox"/>	lab-rtb-private1-us-east-1a	rtb-043083483bde52654
<input type="checkbox"/>	-	rtb-0d25b324bf54a1c28
<input type="checkbox"/>	-	rtb-0caf6367454159d61
<input checked="" type="checkbox"/>	lab-rtb-public	rtb-0b4b657e2eec6509d
<input type="checkbox"/>	Work Public Route Table	rtb-030c55421b73eec52
<input type="checkbox"/>	-	rtb-0ed12730ec43162c0

In the Subnet associations tab, choose Edit subnet associations and select both lab-subnet-public1-us-east-1a and lab-subnet-public2.

Available subnets (2/4)

Filter subnet associations

<input type="checkbox"/>	Name	Subnet ID	IPv4 CIDR
<input checked="" type="checkbox"/>	lab-subnet-public2	subnet-05c70d7f35179...	10.0.2.0/24
<input type="checkbox"/>	lab-subnet-private1-us-east-1a	subnet-0669be98d561...	10.0.1.0/24
<input checked="" type="checkbox"/>	lab-subnet-public1-us-east-1a	subnet-00ca8f447358cf...	10.0.0.0/24
<input type="checkbox"/>	lab-subnet-private2	subnet-041db064ddc41...	10.0.3.0/24

Click on Save associations. In the left navigation pane, select Security groups. Click on Create security group (as shown below).

Security Groups (4) Info

Find resources by attribute or tag

Configure the following, as shown below:

Basic details

Security group name [Info](#)

Web Security Group

Name cannot be edited after creation.

Description [Info](#)

Enable HTTP access

VPC [Info](#)

vpc-0d33058613d468d48 (lab-vpc)



Inbound rules [Info](#)

This security group has no inbound rules.

[Add rule](#)

Click on Add rule under Inbound rules and configure the following:



Inbound rules [Info](#)

Inbound rule 1

[Delete](#)

Type [Info](#)

HTTP

Protocol [Info](#)

TCP

Port range [Info](#)

80

Source type [Info](#)

Anywhere-IPv4

Source [Info](#)

0.0.0.0/0 [X](#)

Description - optional [Info](#)

Permit web requests

[Add rule](#)

Scroll to the bottom and click on Create security group. There should be a pop-up signifying the successful creation of Web Security Group.

Security group ([sg-0418161432183a8a8 | Web Security Group](#)) [X](#)

was created successfully

[► Details](#)

sg-0418161432183a8a8 - Web Security Group

[Actions ▾](#)


Alysia Chen

Search for EC2 to open the EC2 console.

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

[Launch instance](#)

[Migrate a server](#)

Note: Your instances will launch in the US East (N. Virginia) Region

Service health

[AWS Health Dashboard](#)



Region
US East (N. Virginia)

Status
🕒 This service is operating normally.

Zones

Zone name	Zone ID
us-east-1a	use1-az2
us-east-1b	use1-az4

Click on Launch instance. Name the instance Web Server 1, as shown below:

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name

Web Server 1

Add additional tags



Do not change any of the settings under Application and OS Images. Keep the Instance type as the default t2.micro; select **vockey** from the Key pair name menu.

▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below



Search our full catalog including 1000s of application and OS images

Recents

Quick Start

Amazon Linux



macOS



Ubuntu



Windows



Red Hat



SUSE Linu



Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI

ami-0c614dee691cbbf37 (64-bit (x86), uefi-preferred) / ami-0b29c89c15cfb8a6d (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible



Alysia Chen

▼ Instance type [Info](#) | [Get advice](#)

Instance type

t2.micro

Free tier eligible

Family: t2 1 vCPU 1 GiB Memory

Current generation: true

On-Demand Windows base pricing: 0.0162 USD per Hour

On-Demand Ubuntu Pro base pricing: 0.0134 USD per Hour

On-Demand SUSE base pricing: 0.0116 USD per Hour

On-Demand RHEL base pricing: 0.026 USD per Hour

On-Demand Linux base pricing: 0.0116 USD per Hour

All generations

[Compare instance types](#)

[Additional costs apply for AMIs with pre-installed software](#)

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

vockey



[Create new key pair](#)

Click on Edit next to network settings, configuring the VPC, subnet, and auto-assign public IP settings as shown below, as well as the security group. Do not change any settings under Configure storage.



▼ Network settings [Info](#)

VPC - required [Info](#)

vpc-0d33058613d468d48 (lab-vpc)
10.0.0.0/16



Subnet [Info](#)

subnet-01f99b36a07454455
lab-subnet-public2
VPC: vpc-0d33058613d468d48
Owner: 877002603542
Availability Zone: us-east-1b
Zone type: Availability Zone
IP addresses available: 251 CIDR: 10.0.2.0/24)



[Create new subnet](#)

Auto-assign public IP [Info](#)

Enable



Additional charges apply when outside of [free tier allowance](#)

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group

Select existing security group

Common security groups [Info](#)

Select security groups



[Compare security group rules](#)

Web Security Group sg-0418161432183a8a8

VPC: vpc-0d33058613d468d48

Security groups that you add or remove here will be added to or removed from all your network interfaces.

► Advanced network configuration

▼ Configure storage [Info](#)

[Advanced](#)

1x

8

GiB

gp3



Root volume 3000 IOPS (Not encrypted)

Expand the Advanced details section, scrolling down and copying the following code into the User data box.

User data - optional | [Info](#)

Upload a file with your user data or enter it in the field.

 [Choose file](#)

```
#!/bin/bash
# Install Apache Web Server and PHP
dnf install -y httpd wget php mariadb105-server
# Download Lab files
wget https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-
100-ACCLFO-2/2-lab2-vpc/s3/lab-app.zip
unzip lab-app.zip -d /var/www/html/
# Turn on web server
chkconfig httpd on
service httpd start
```

- User data has already been base64 encoded

There should be a pop-up signaling the successful launch of an instance.



Successfully initiated launch of instance ([i-0e5d85fb55e319cc9](#))



Scroll to the very bottom to click on View Instances, which will bring you to this page:

Instances (2) Info		Last updated less than a minute ago	Connect	Instance state ▾	Actions ▾	Launch instances	▼
				All states ▾			
<input type="checkbox"/>	Name 🔗	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input type="checkbox"/>	Bastion Host	i-01ce344c979fb6472	Running 🔗 🔍	t2.micro	2/2 checks passed View alarms +	us-east-1a	ec2-52
<input type="checkbox"/>	Web Server 1	i-0e5d85fb55e319cc9	Running 🔗 🔍	t2.micro	Initializing View alarms +	us-east-1b	ec2-18

Wait until the Status for Web Server 1 reads 2/2 checks passed; you may need to select the Refresh icon a few times until then.

Instances (2) Info		Last updated less than a minute ago	Connect	Instance state ▾	Actions ▾	Launch instances	▼
				All states ▾			
<input type="checkbox"/>	Name 🔗	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input type="checkbox"/>	Bastion Host	i-01ce344c979fb6472	Running 🔗 🔍	t2.micro	2/2 checks passed View alarms +	us-east-1a	ec2-52
<input type="checkbox"/>	Web Server 1	i-0e5d85fb55e319cc9	Running 🔗 🔍	t2.micro	2/2 checks passed View alarms +	us-east-1b	ec2-18

Select Web Server 1.

The screenshot shows the AWS EC2 Instance Details page for the instance **i-03e70c32a6e15ff7b (Web Server 1)**. The instance state is **Running**. The Public IPv4 DNS address is listed as **ec2-98-84-100-26.compute-1.amazonaws.com**, with a link to open the address in a browser. The Private IP DNS name (IPv4 only) is also listed.

Instance state Running	Public IPv4 DNS ec2-98-84-100-26.compute-1.amazonaws.com open address
Hostname type	Private IP DNS name (IPv4 only)

Copy and paste the Public IPv4 DNS address into a new browser tab. A web page similar to the following should load.





Meta-Data	Value
InstanceId	<i>i-03e70c32a6e15ff7b</i>
Availability Zone	<i>us-east-1b</i>

Current CPU Load: **12%**

LAB 3

In the AWS Management Console, choose Services before clicking on Compute.



The screenshot shows the AWS Management Console with the URL `voclabs/user370119` in the top right corner. The left sidebar has a red navigation bar at the top with icons for Recently visited, Favorites, All applications, and All services. Below this, under the Compute category, are links for Analytics, Application Integration, Blockchain, Business Applications, Cloud Financial Management, Compute, Containers, Customer Enablement, Database, and Developer Tools. The main content area is titled "Compute" and lists several services: "AWS App Runner" (Build and run production web applications at scale), "Batch" (Fully managed batch processing at any scale), "EC2" (Virtual Servers in the Cloud), "EC2 Global View" (described as providing a global dashboard and search functionality for EC2 and VPC resources), "EC2 Image Builder" (A managed service to automate build, customize and deploy OS images), "Elastic Beanstalk" (Run and Manage Web Apps), and "Lambda".

Click on EC2 under Compute.

Key pairs	1	Load balancers	0
Placement groups	0	Security groups	4
<u>Snapshots</u>	0	Volumes	1

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance



Migrate a server 

Note: Your instances will launch in the US East (N. Virginia) Region

Service health

[AWS Health Dashboard !\[\]\(19139bd4163c66165e8330347d352a72_img.jpg\)](#)



Region

US East (N. Virginia)

Status

 This service is operating normally.

Select the Launch instance button from the Launch instance menu. Configure the name as show below:



Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name

Web Server

[Add additional tags](#)

Do not change any of the settings under Application and OS Images. Keep the Instance type as the default t2.micro; select **vockey** from the Key pair name menu.



▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

 *Search our full catalog including 1000s of application and OS images*

Recents

Quick Start



[Browse more AMIs](#)

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI

ami-0c614dee691cbbf37 (64-bit (x86), uefi-preferred) / ami-0b29c89c15cfb8a6d (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible



▼ Instance type [Info](#) | [Get advice](#)

Instance type

t2.micro Free tier eligible

Family: t2 1 vCPU 1 GiB Memory

Current generation: true

On-Demand Windows base pricing: 0.0162 USD per Hour

On-Demand Ubuntu Pro base pricing: 0.0134 USD per Hour

On-Demand SUSE base pricing: 0.0116 USD per Hour

On-Demand RHEL base pricing: 0.026 USD per Hour

On-Demand Linux base pricing: 0.0116 USD per Hour

All generations

[Compare instance types](#)

Additional costs apply for AMIs with pre-installed software

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

vockey



[Create new key pair](#)

Click on Edit next to network settings, configuring the VPC, subnet, and auto-assign public IP settings as shown below, as well as the security group. Make sure to remove the Inbound Security Group rule. Do not change any settings under Configure storage.



▼ Network settings [Info](#)

VPC - required | [Info](#)

vpc-0a22c25179aafaf59 (Lab VPC)
10.0.0.0/16



Subnet | [Info](#)

subnet-0a247df5f8a1a02de
VPC: vpc-0a22c25179aafaf59 Owner: 684713641101
Availability Zone: us-east-1a Zone type: Availability Zone
IP addresses available: 1 CIDR: 10.0.1.0/28)

PublicSubnet1



[Create new subnet](#)

Auto-assign public IP | [Info](#)

Enable



Additional charges apply when outside of [free tier allowance](#)

Firewall (security groups) | [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group

Select existing security group

Security group name - required

Web Server security group

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#@[]+=&;{}!\$*

Description - required | [Info](#)

Security group for my web server

Inbound Security Group Rules

No security group rules are currently included in this template. Add a new rule to include it in the launch template.

[Add security group rule](#)

Then, expand Advanced details and enable Termination protection. Copy the following code into the User Data box:

```
#!/bin/bash
```

```
dnf install -y httpd
```

```
systemctl enable httpd
```

```
systemctl start httpd
```



```
echo '<html><h1>Hello From Your Web Server!</h1></html>' >
/var/www/html/index.html
```

Select Launch instance and choose View all instances after a Success message pops up. Wait until the Instance State is Running and the two Status Checks are both passed, clicking on the Refresh icon:

Instances (2) Info		Last updated less than a minute ago	Connect	Instance state ▾	Actions ▾	Launch instances ▾
				All states ▾		
<input type="checkbox"/>	Name 🔗	Instance ID	Instance state	Instance type	Status check	Alarm status
<input type="checkbox"/>	Bastion Host	i-0c224858e4637d2ee	Running 🔗 🔗	t2.micro	2/2 checks passed View alarms +	us-east-1a
<input type="checkbox"/>	Web Server	i-040e5abaa2c5a3ba6	Running 🔗 🔗	t2.micro	2/2 checks passed View alarms +	us-east-1a

Select the Web Server using the checkbox, navigating to the Status checks tab. Ensure that both the system reachability and Instance reachability checks have passed.

-	Name 🔗	Instance ID	Instance state
<input type="checkbox"/>	Bastion Host 🔗	i-0c224858e4637d2ee	Running 🔗 🔗
<input checked="" type="checkbox"/>	Web Server	i-040e5abaa2c5a3ba6	Running 🔗 🔗

i-040e5abaa2c5a3ba6 (Web Server)

[Actions](#) ▾

Status checks [Info](#)

Status checks detect problems that may impair i-040e5abaa2c5a3ba6 (Web Server) from running your applications.

System status checks <ul style="list-style-type: none"> ✓ System reachability check passed 	Instance status checks <ul style="list-style-type: none"> ✓ Instance reachability check passed
---	---

You may also use the Monitoring tab to view the Amazon CloudWatch metrics. Next, select the Actions drop-down menu, click on Monitor and troubleshoot, and select Get system log.

Instances (1/2) [Info](#)

Last updated 3 minutes ago [C](#) [Connect](#) [Instance state ▾](#) [Actions ▲](#)

[Launch instances](#) [▼](#)

Find Instance by attribute or tag (case-insensitive)

[-](#) | Name [🔗](#) | Instance ID [...](#)

i-040e5abaa2c5a3ba6 (Web Server)

< | [Details](#) | [Status and alarms](#) | >

CloudWatch agent metrics
The monitoring tab will now include metrics related to a single instance.

Connect
View details
Manage instance state
Instance settings
Networking
Security
Image and templates
Monitor and troubleshoot
Get system log
Get instance screenshot
Manage detailed monitoring

Note that the HTTP package was installed, as the system log shows.

System log



[Copy log](#)

[Download](#)

Review system log for instance i-040e5abaa2c5a3ba6 as of Fri Jan 31 2025
23:35:39 GMT-0800 (Pacific Standard Time)

```
[ 45.663589] cloud-init[2213]: mod_lua-2.4.62-1.amzn2023.x86_64[0.000s]
[ 45.663609] cloud-init[2213]: Complete!
[ 45.768710] cloud-init[2213]: Created symlink /etc/systemd/system/
[ 45.070945] zram_generator::config[3580]: zram0: system has
ci-info: ++++++Authorized keys from /home
ci-info: +-----+
ci-info: | Keytype | Fingerprint
ci-info: +-----+
ci-info: | ssh-rsa | 30:a4:1c:d8:b0:9a:ea:ff:d6:b1:25:a6:a9:e7
ci-info: +-----+
<14>Feb 1 07:22:15 cloud-init: #####
<14>Feb 1 07:22:15 cloud-init: ----BEGIN SSH HOST KEY FINGERPRINTS-----
<14>Feb 1 07:22:15 cloud-init: 256 SHA256:WOhCGvi7vNYYp/YB5PrV
<14>Feb 1 07:22:15 cloud-init: 256 SHA256:ygSynl6ae7b/euJ+Toy
<14>Feb 1 07:22:15 cloud-init: ----END SSH HOST KEY FINGERPRINTS-----
<14>Feb 1 07:22:15 cloud-init: #####
-----BEGIN SSH HOST KEY KEYS-----
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdH

```

Choose Cancel at the very bottom to return to the previous page. With Web Server still selected, return to the Actions drop-down menu to select Monitor and troubleshoot. Click on Get instance screenshot.



Instances (1/2) [Info](#)

Last updated less than a minute ago

[Connect](#) [Instance state ▾](#) [Actions ▲](#)

[Launch instances](#) ▾

Find Instance by attribute or tag (case-sensitive)

Name [Edit](#) ▾ | Instance ID

i-040e5abaa2c5a3ba6 (Web Server)

[Details](#) [Status and alarms](#)

Instance summary [Info](#)

Instance ID Public IPV4 address

Connect
View details
Manage instance state
Instance settings ▾
Networking ▾
Security ▾
Image and templates ▾
Monitor and troubleshoot ▲
Get system log
Get instance screenshot
Manage detailed monitoring

This is the final way that will be explored in this lab on how to monitor an instance.

Instance screenshot



[Download](#)

i-040e5abaa2c5a3ba6 (Web Server) on 2025-01-31 at T23:38:37.731 -08:00

```
Amazon Linux 2023.6.20250128
Kernel 6.1.124-134.200.amzn2023.x86_64 on an x86_64 (-)

[ 44.128818] zram_generator::config[2444]: zram0: system has too much memory (949MB), limit is 800MB, ignoring.
[ 45.070945] zram_generator::config[3580]: zram0: system has too much memory (949MB), limit is 800MB, ignoring.
```

Choose cancel; while Web Server is still selected, navigate to the Details tab. Copy the Public IPv4 address and enter the address into a new browser tab.

=

i-040e5abaa2c5a3ba6 (Web Server)

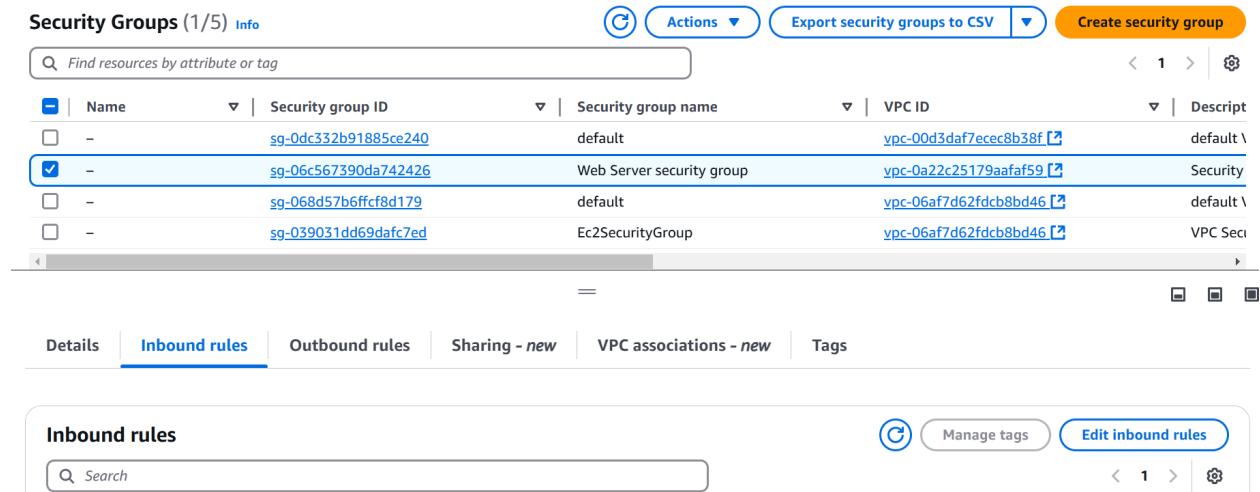
▼ Instance summary [Info](#)

Instance ID <input type="checkbox"/> i-040e5abaa2c5a3ba6	Public IPv4 address <input type="checkbox"/> 3.239.215.0 open address
Private IPv4 addresses <input type="checkbox"/> 10.0.1.5	IPv6 address -

The web browser should not be able to access the web server due to the security group blocking inbound traffic on port 80. Return to the EC2 Console tab and select Security Groups from the



navigation pane. Check the box for Web Server security group and navigate to the Inbound rules tab.



The screenshot shows the AWS Security Groups interface. At the top, there's a search bar and several navigation buttons: 'Actions', 'Export security groups to CSV', and 'Create security group'. Below the table, there are tabs for 'Details', 'Inbound rules' (which is selected), 'Outbound rules', 'Sharing - new', 'VPC associations - new', and 'Tags'. The main area displays a table of security groups:

Name	Security group ID	Security group name	VPC ID	Description
-	sg-0dc332b91885ce240	default	vpc-00d3daf7ecec8b38f	default \
<input checked="" type="checkbox"/>	sg-06c567390da742426	Web Server security group	vpc-0a22c25179aafaf59	Security
-	sg-068d57b6ffcf8d179	default	vpc-06af7d62fdcb8bd46	default \
-	sg-039031dd69dafc7ed	Ec2SecurityGroup	vpc-06af7d62fdcb8bd46	VPC Sec

Below the table, there's a section titled 'Inbound rules' with a search bar and buttons for 'Manage tags' and 'Edit inbound rules'.

Edit inbound rules and select Add rule, configuring as shown:

Inbound rules Info

Inbound rule 1

[Delete](#)**Security group rule ID**

-

Type Info

HTTP

**Protocol** Info

TCP

Port range Info

80

Source type Info

Anywhere-IPv4

Source Info0.0.0.0/0 [X](#)**Description - optional** Info

Save rules. When refreshing the web server tab, a message should appear, like the following:

← → ⌂ ⚠ Not secure 3.239.215.0

Hello From Your Web Server!

Return to the Instances page and check the box for the Web Server instance.



Alysia Chen

Instances (1/2) Info

Last updated less than a minute ago

C Connect Instance state Actions ▾

Launch instances ▾

Find Instance by attribute or tag (case-sensitive) All states ▾

< 1 > ⚙

Name	Instance ID	Instance state	Ins
Bastion Host	i-0c224858e4637d2ee	Running	t2.
Web Server	i-040e5abaa2c5a3ba6	Running	t2.

i-040e5abaa2c5a3ba6 (Web Server) ⚙ ▾

< Details Status and alarms Monitoring Security >

In the Instance state menu, select Stop instance and choose Stop. Wait until the Instance state is Stopped before continuing.

Name	Instance ID	Instance state
Bastion Host	i-0c224858e4637d2ee	Running
Web Server	i-040e5abaa2c5a3ba6	Stopped

In the Actions menu, with the Web Server instance still selected, select Instance settings and Change instance type to change the Instance Type to **t2.small**. click Apply. There should be a pop-up success message appearing.

✓ Instance type changed successfully ✕



While the Web Server Instance is selected, go into the Actions drop-down menu, selecting Instance settings, then Change stop protection. Select Enable before pressing Save. Make sure the success message for Stop protection shows up and that the Web Server instance is still selected. Choose the Storage tab.

The screenshot shows the AWS CloudWatch Instances console. At the top, a green success message box displays: "Enabled stop protection for i-040e5abaa2c5a3ba6". Below this, the main interface shows "Instances (1/2)" with an "Info" link. It includes filters for "Last updated" (2 minutes ago), "Connect", "Instance state" (dropdown), and "Actions" (dropdown). A prominent orange button labeled "Launch instances" is visible. Below these are search and filter fields: "Find Instance by attribute or tag (case-sensitive)" and "All states" (dropdown). Navigation controls include a page number "1" and a gear icon. The main content area displays an instance named "i-040e5abaa2c5a3ba6 (Web Server)". For this instance, there are tabs for "Monitoring", "Security", "Networking", and "Storage". The "Storage" tab is currently selected, indicated by a blue underline. Below the tabs, there are sections for "Volume ID" and "Volume Name".

Select the name of the Volume ID and the checkbox next to the volume.

Volumes (1/1) [Info](#)

[Actions](#) [Create volume](#)

Saved filter sets [Choose filter set](#) [Search](#)

Volume ID = vol-0b067de243192dc23 [X](#) [Clear filters](#)

<input checked="" type="checkbox"/> Name	Volume ID	Type	Size
<input checked="" type="checkbox"/> -	vol-0b067de243192dc23	gp3	8 GiB

Volume ID: vol-0b067de243192dc23

[Details](#) [Status checks](#) [Monitoring](#) [Tags](#)

Volume status <input checked="" type="checkbox"/> Okay	Availability Zone <input type="checkbox"/> us-east-1a
I/O status <input checked="" type="checkbox"/> Enabled	I/O performance <input type="checkbox"/> Not applicable

In the Actions menu, select Modify volume and change the size to 10 before clicking Modify. After the size is now 10 GiB, in the left navigation pane, choose Instances. Select the Web Server instance and in the Instance state drop-down menu, select Start instance.

✓ Successfully initiated starting of i-040e5abaa2c5a3ba6 X

Instances (1/2) Info

Last updated less than a minute ago C Connect Instance state ▾ Actions ▾

Launch instances ▼

Find Instance by attribute or tag (case-sensitive) All states ▾

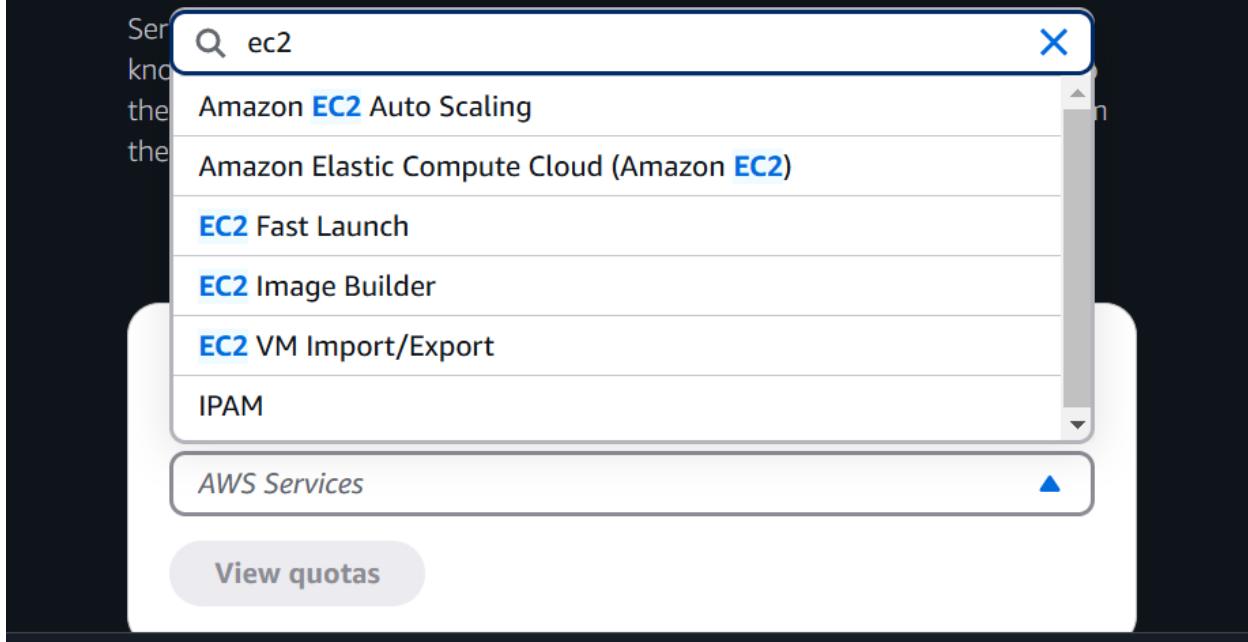
< 1 > ⚙️

=
i-040e5abaa2c5a3ba6 (Web Server) ⚙️ ▼

Next, search for and select Service Quotas, choosing AWS Services. In the Find services search bar, search for and select **Amazon Elastic Compute Cloud**.

Service Quotas

View and manage AWS quotas



After selecting View quotas, enter into the View quotas search bar **running on-demand** and observe the search results.

[Amazon Elastic Compute Cloud \(Amazon EC2\)](#)

Amazon Elastic Compute Cloud (EC2) provides resizable compute capacity through virtual machines (VM's or instances) in the cloud.

Service quotas info		Request increase at account level			
Quota name	Applied account-level quota value	AWS default quota value	Utilization	Adjustability	
Running On-Demand DL instances	96	0	0	Account level	
Running On-Demand F instances	64	0	0	Account level	
Running On-Demand G and VT instances	0	0	0	Account level	
Running On-Demand High Memory instances	0	0	0	Account level	
Running On-Demand HPC instances	192	0	0	Account level	

Next, return to the EC2 console and choose Instances. Select the Web Server instance; in the Instance state drop-down menu, select Stop instance. Choose Stop. There should be an error message. This is due to the stop protection enabled earlier.

The screenshot shows the AWS EC2 Instances page. At the top, there is a red error banner with the text: "Failed to stop the instance i-040e5abaa2c5a3ba6. The instance 'i-040e5abaa2c5a3ba6' may not be stopped. Modify its 'disableApiStop' instance attribute and try again." To the right of the banner are buttons for "Diagnose with Amazon Q" and a close "X". Below the banner, the main instance list is displayed. The first instance is a Bastion Host with the ID i-0c224858e4637d2ee, labeled as "Running". A status check indicates "2/2 checks passed". The instance name is listed as "i-040e5abaa2c5a3ba6 (Web Server)". The "Actions" dropdown menu is open, showing options like "Change stop protection", "Change instance type", "Stop", "Start", and "Reboot".

In the Actions drop-down menu, choose Instance setting and click on Change stop protection. Deselect the Enable setting and choose Save.

The screenshot shows the "Change stop protection" dialog box. It has two sections: "Instance ID" (containing the value "i-040e5abaa2c5a3ba6 (Web Server)") and "Stop protection" (containing a checkbox labeled "Enable" which is currently checked). At the bottom right of the dialog are "Cancel" and "Save" buttons.

Try again to stop the instance. It should work now, as shown by the success message below:

The screenshot shows a green notification banner at the top of the screen. The message reads: "Successfully initiated stopping of i-040e5abaa2c5a3ba6". Below the message is a "Notifications" section with icons for success (8), warning (0), error (2), info (0), and other (0).

PROBLEMS:

Although there weren't significant challenges, when I was configuring the web server in Lab 2, the time for the 2 checks to pass took an unexpectedly long time, delaying me while I was completing the tasks.



CONCLUSION:

These labs, although time-consuming, were mostly straightforward and easy-to-comprehend. At the same time, I learned a lot about AWS services offered by Amazon. I became a lot more familiar with the AWS Console used.



SIGN-OFF:

Lab 1:

Total score **40/40**

TASK 2a - Added user-1 to S3-Support group **5/5**

TASK 2b - Added user-2 to EC2-Support group **5/5**

TASK 2c - Added user-3 to EC2-Admin group **5/5**

TASK 3a - user-1 logged in **5/5**

TASK 3b - user-2 logged in **5/5**

TASK 3c - user-2 ec2 stop instance attempt **5/5**

TASK 3d - user-3 logged in **5/5**



Lab 2:

Total score 30/30

Task 1 - VPC created correctly 5/5

Task 2a - New subnets created correctly 5/5

Task 2b - Subnet route table association 5/5

Task 3 - Security group created correctly 5/5

Task 4a - EC2 instance created correctly 5/5

Task 4b - EC2 instance website accessible 5/5

Lab 3:



Total score **25/25**

Task 1 - EC2 instance created correctly **5/5**

Task 2 - get system log requested **5/5**

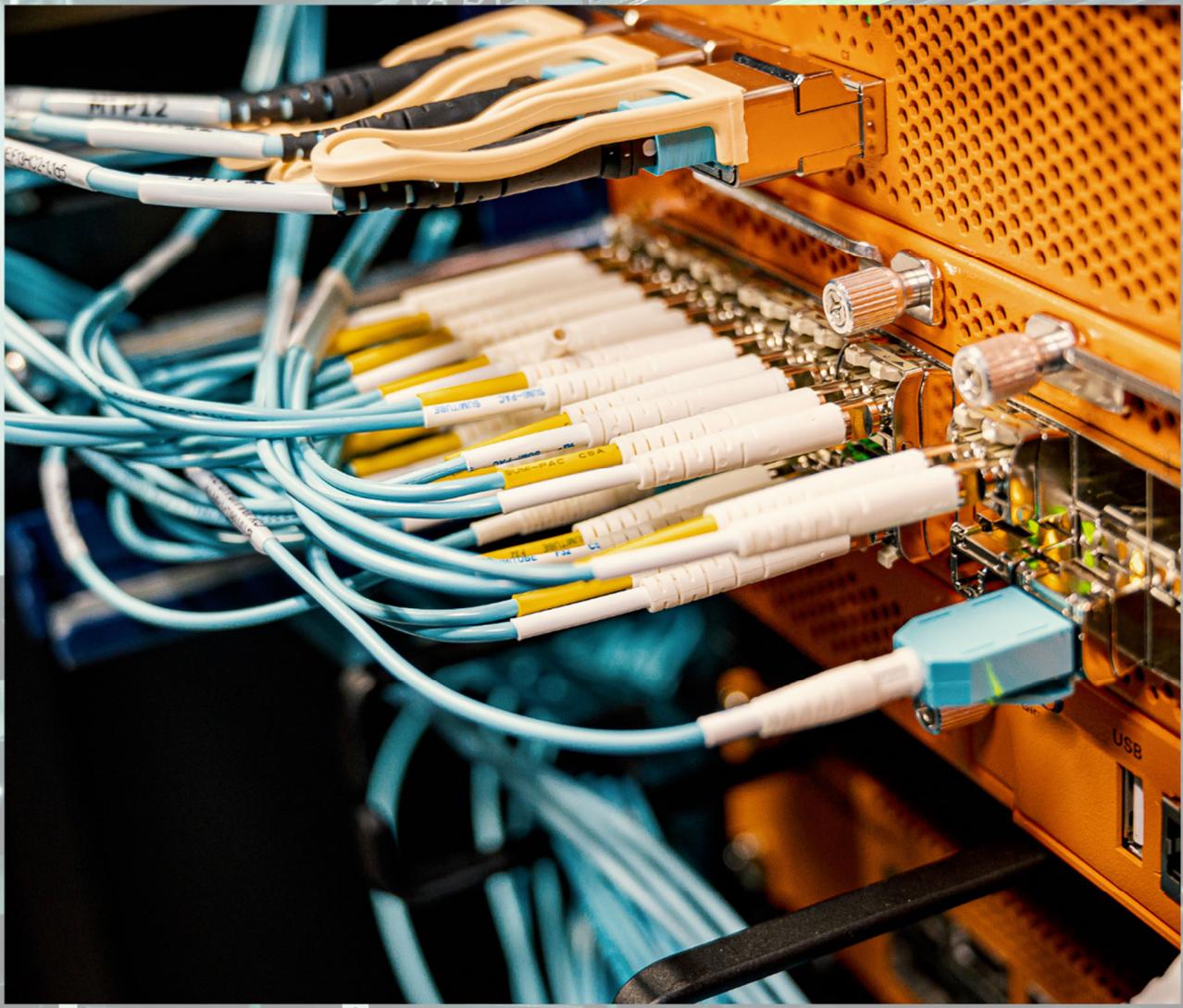
Task 3 - security group updated **5/5**

Task 4 - EC2 instance updated **5/5**

Task 6 - Instance stopped on second try **5/5**



Lab 6: Amazon Cloud Foundations 4-6



PURPOSE:

Learn to work with EBS, build a DB server, and load balance through different AWS services.

BACKGROUND INFORMATION ON LAB CONCEPTS:

EBS:

Amazon Elastic Block Store (Amazon EBS) allows for storage for EC2 instances. EBS volumes are attached to the network and are independent from instances (so if instances become unavailable, volumes may still exist). EBS volumes can be used as an EC2 instances boot partition, which can be stopped and restarted, so you only need to pay for the time you're using them. EBS volumes also offer more durability over traditional EC2 instances because they're automatically replicated on the backend.

DB Server:

Amazon Relational Database Service (Amazon RDS) facilitates the process of setting up and operating a cloud database, while allowing room for scalability. At the same time, network administrators can choose which database engines to deploy and scale. Amazon RDS will also manage backup, software patching, and recovery, while detecting failures immediately. AWS will also manage the hardware layers, unlike a traditional database server.

ELB and Auto Scaling:

Elastic Load Balancing (ELB) automatically distributes traffic across EC2 instances, allowing for an easy way to achieve fault tolerance. It also allows customers to monitor the health and performance in real time and has additional security features. Auto Scaling allows for convenient scaling, according to your pre-defined conditions and works best for applications with stable demand patterns. Auto Scaling also increases the amount of EC2 instances for change in demand to maintain the performance while minimizing the costs through decreasing capacity at less in-demand times.

LAB SUMMARY:

In these labs, I learned about different services that Amazon AWS offers—their purposes and how they work. I used the AWS Console and web browsers to complete different tasks, including configurations and checks.



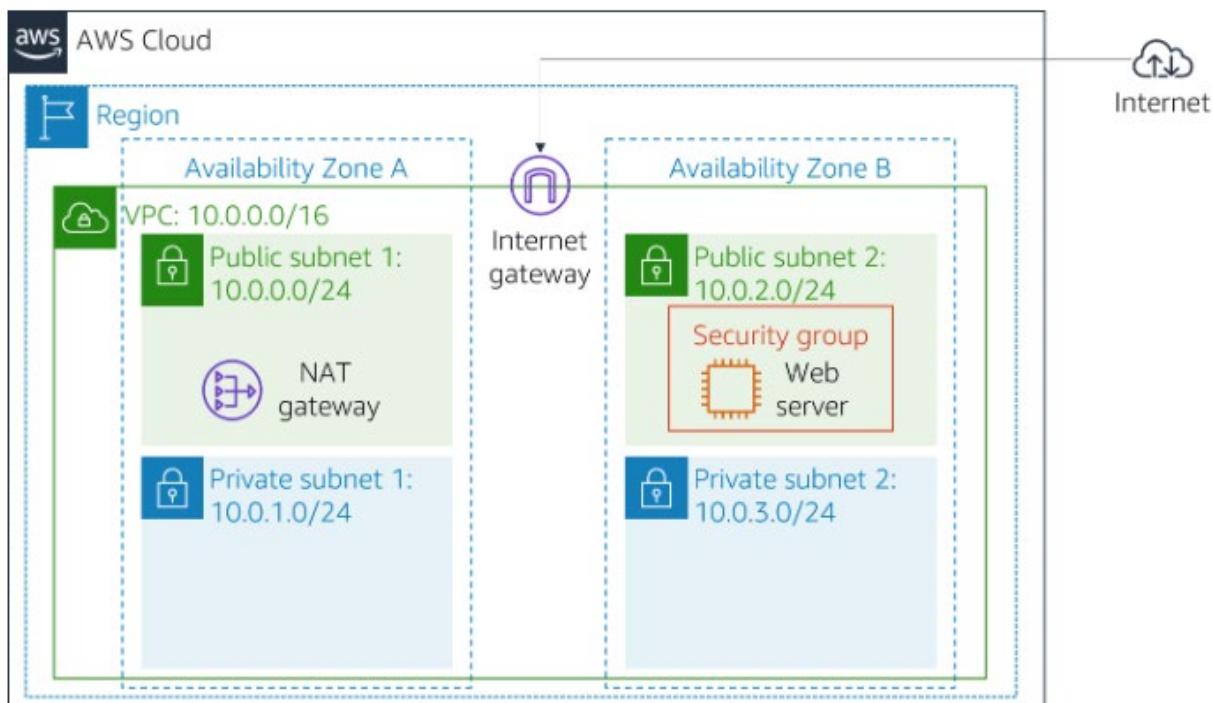
DIAGRAMS:

Lab 4

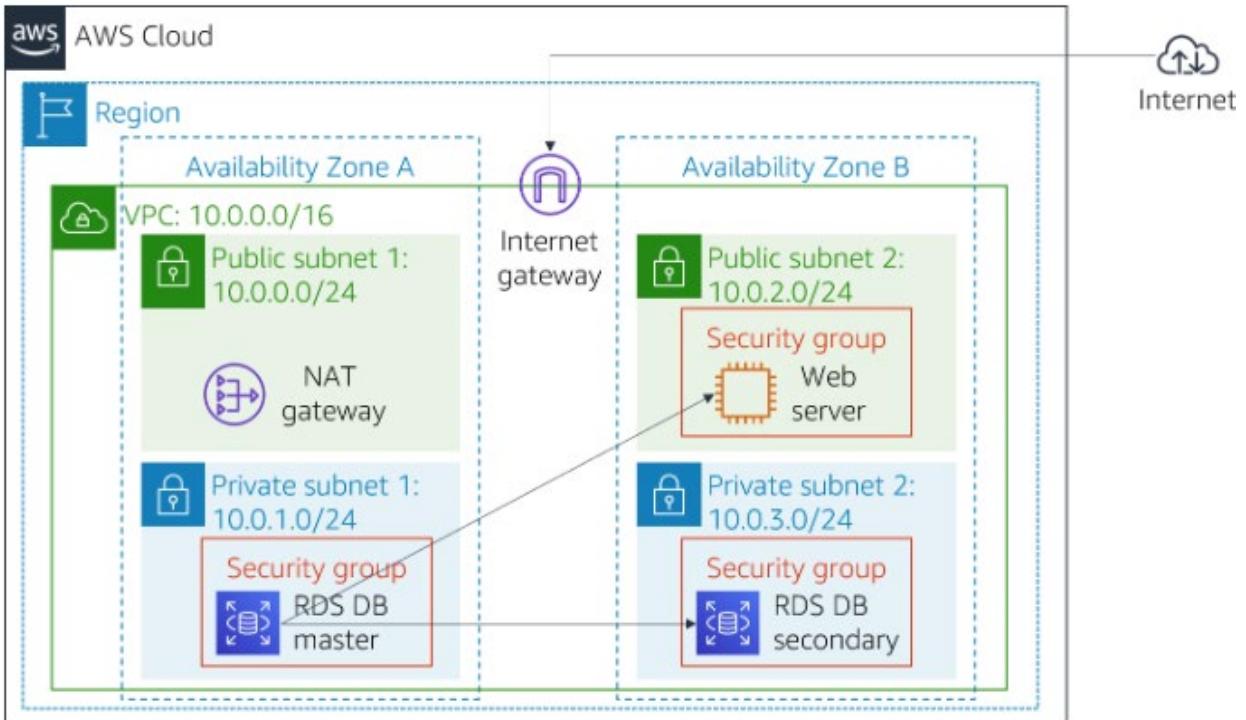


Lab 5

Beginning infrastructure:

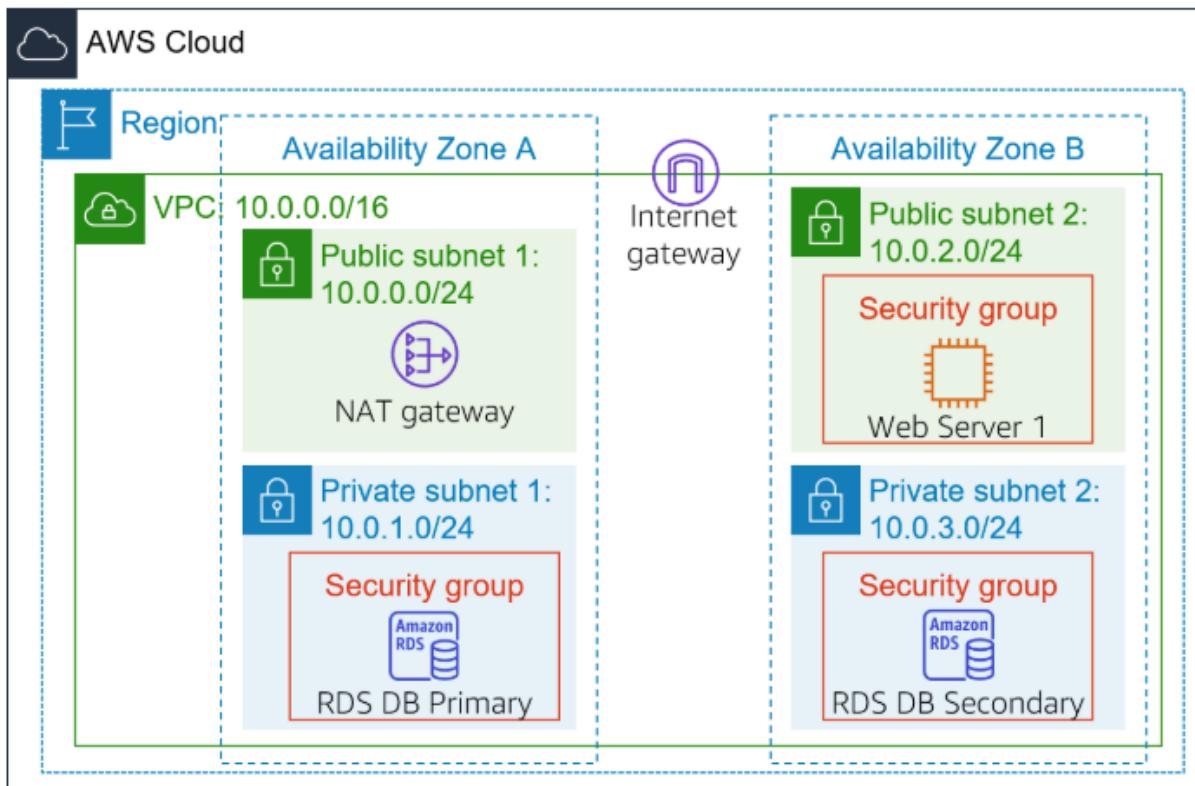


Ending infrastructure:

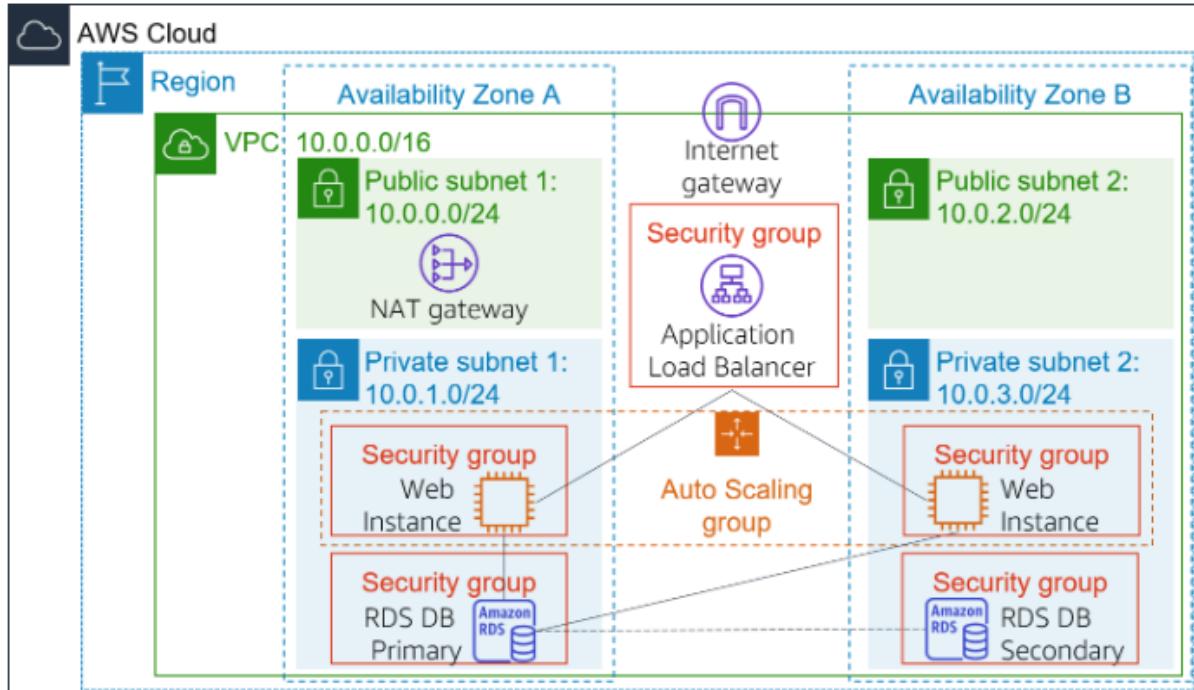


Lab 6

Beginning infrastructure:



Ending infrastructure:



LAB COMMANDS:

LAB 4

Navigate to the E2 Console page.

The screenshot shows the AWS E2 Console Resources page. At the top, there are navigation icons for Home, Services, Search, Notifications, Help, and Settings, followed by the region 'United' and a user ID 'voclabs/user3701192='.

The main section is titled 'Resources' and displays the following data:

Resource Type	Count
Instances (running)	2
Capacity Reservations	0
Elastic IPs	0
Key pairs	1
Placement groups	0
Snapshots	0
Auto Scaling Groups	0
Dedicated Hosts	0
Instances	2
Load balancers	0
Security groups	5
Volumes	2

At the bottom right of the resources section, there are three buttons: 'EC2 Global View' (highlighted), a gear icon, and a circular refresh icon.

Next, click into Instances. Notice how an EC2 instance named Lab has already been set up.



Instances (2) Info

Last updated less than a minute ago  Connect Instance state Actions

Launch instances ▾

 Find Instance by attribute or tag (case-sensitive)

All states ▾

Instance state = running  Clear filters

< 1 > 

<input type="checkbox"/>	Name 	Instance ID	Instance state	Ins
<input type="checkbox"/>	Lab	i-038d6ce58a77f3865	 Running  	t2.

Select an instance  ▾

In the left navigation pane, select Volumes.

Volumes (2) Info

Saved filter sets  Choose filter set  Search

< 1 > 

<input type="checkbox"/>	Name	Volume ID	Type	Size
<input type="checkbox"/>	-	vol-031ad13c81034f995	gp3	9 GiB
<input type="checkbox"/>	-	vol-045f21b8c9c8ddc07	gp3	8 GiB

Click on Create volume and configure as shown below:

Volume settings

Volume type | [Info](#)

General Purpose SSD (gp2) ▾

Size (GiB) | [Info](#)

1

Min: 1 GiB, Max: 16384 GiB.

IOPS | [Info](#)

100 / 3000

Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS.

Throughput (MiB/s) | [Info](#)

Not applicable

Availability Zone | [Info](#)

us-east-1a ▾

Click on Add tag, entering in a Key of **Name** and Value of **My Volume**. Choose Create Volume. You should see this screen:

The screenshot shows the AWS Lambda Volumes page. At the top, a green success message reads: "Successfully created volume [vol-0af71a9f0e1473369](#)". Below this, the page title is "Volumes (3)" with an "Info" link. There are buttons for "Actions" and "Create volume". A "Saved filter sets" dropdown is set to "Choose filter set". A search bar contains the placeholder "Search". Navigation controls include arrows and a gear icon. A table lists three volumes:

<input type="checkbox"/>	Name	Volume ID	Type	Size
<input type="checkbox"/>	My Volume	vol-0af71a9f0e1473369	gp2	1 GiB
<input type="checkbox"/>	-	vol-031ad13c81034f995	gp3	9 GiB

Select the checkbox next to My Volume and in the Actions drop-down menu, choose Attach volume. Note: you may need to wait and click on the refresh icon before you can do so.

Attach volume Info

Attach a volume to an instance to use it as you would a regular physical hard disk drive.

Basic details

Volume ID

vol-0af71a9f0e1473369 (My Volume)

Availability Zone

us-east-1a

Instance Info

Search instance ID or name tag



Only instances in the same Availability Zone as the selected volume are displayed.

Device name Info

Select a device name

Enter the Instance and Device name as shown below:



Attach volume Info

Attach a volume to an instance to use it as you would a regular physical hard disk drive.

Basic details

Volume ID

vol-0af71a9f0e1473369 (My Volume)

Availability Zone

us-east-1a

Instance | [Info](#)

i-038d6ce58a77f3865

(Lab) (running)



Only instances in the same Availability Zone as the selected volume are displayed.

Device name | [Info](#)

/dev/sdf



Recommended device names for Linux: /dev/xvda for root volume. /dev/sd[f-p] for data volumes.

Click on Attach volume. Next, go back into EC2 Instances and click on the checkbox next to Lab instance, hitting Connect.



Connect to instance Info

Connect to your instance i-038d6ce58a77f3865 (Lab) using any of these options

The screenshot shows a navigation bar with three tabs: 'EC2 Instance Connect' (selected), 'Session Manager', and 'SSH client'. Below the tabs, there's an 'Instance ID' section with a checkbox for 'i-038d6ce58a77f3865 (Lab)'. Under 'Connection Type', two options are shown: 'Connect using EC2 Instance Connect' (selected) and 'Connect using EC2 Instance Connect Endpoint'. Both options describe connecting via a browser-based client with a public IPv4 or IPv6 address. Below these, 'Public IPv4 address' is selected, showing the IP '3.89.19.65', while 'IPv6 address' is unselected.

EC2 Instance Connect Session Manager SSH client >

Instance ID
 i-038d6ce58a77f3865 (Lab)

Connection Type

Connect using EC2 Instance Connect
Connect using the EC2 Instance Connect browser-based client, with a public IPv4 or IPv6 address.

Connect using EC2 Instance Connect Endpoint
Connect using the EC2 Instance Connect browser-based client, with a private IPv4 address and a VPC endpoint.

Public IPv4 address
 3.89.19.65

IPv6 address

The above page should appear. Scroll to the very bottom and choose Connect. A terminal session should open, like the one below:





```
          #
 ~\_\#\#\#
 ~~\_\#\#\#\_
 ~~ \#\#|
 ~~ \#/   https://aws.amazon.com/linux/amazon-linux-2023
 ~~ V~'__->
 ~~~ /
 ~~~_.-./
 ~~~_/_/m/
 [ec2-user@ip-10-1-11-77 ~]$
```

i-038d6ce58a77f3865 (Lab) X

Public IPs: 3.89.19.65 Private IPs: 10.1.11.77

On the terminal session, run the following command: `df -h`. There should be an output like this:



```

          #
~\_\#\#\#_ Amazon Linux 2023
~~\_#\#\#\\
~~ \#\#\|
~~ \#/   https://aws.amazon.com/linux/amazon-linux-2023
~~ V~' '-'>
~~~ /
~~.~.~/
~/m/' [ec2-user@ip-10-1-11-77 ~]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        4.0M    0  4.0M  0% /dev
tmpfs           475M    0  475M  0% /dev/shm
tmpfs           190M  452K  190M  1% /run
/dev/xvda1       8.0G  1.6G  6.4G  20% /
tmpfs           475M    0  475M  0% /tmp
/dev/xvda128     10M   1.3M  8.7M  13% /boot/efi
tmpfs            95M    0   95M  0% /run/user/1000
[ec2-user@ip-10-1-11-77 ~]$ 

```

i-038d6ce58a77f3865 (Lab)



Public IPs: 3.89.19.65 Private IPs: 10.1.11.77

Next, enter this command: `sudo mkfs -t ext3 /dev/sdf`. This will create a new file system. `sudo mkdir /mnt/data-store` will create a directory for mounting the new storage volume; `sudo mount /dev/sdf mkdir /mnt/data-store` will mount the new volume. Run this: `echo "/dev/sdf /mnt/data-store ext3 defaults,noatime 1 2" | sudo tee -a /etc/fstab`; this will allow the volume to be mounted whenever the instance is started. View the configuration file using `cat /etc/fstab`; view the available storage again using `df -h` (see picture below for current storage).



```

Filesystem      Size  Used  Avail  Use%  Mounted on
/devtmpfs       4.0M   0     4.0M   0%    /dev
tmpfs          475M   0     475M   0%    /dev/shm
tmpfs          190M  456K  190M   1%    /run
/dev/xvda1      8.0G  1.6G  6.4G  20%   /
tmpfs          475M   0     475M   0%    /tmp
/dev/xvda128    10M   1.3M  8.7M  13%   /boot/efi
tmpfs          95M   0     95M   0%    /run/user/1000
/dev/xvdf      975M  60K   924M   1%   /mnt/data-store
[ec2-user@ip-10-1-11-77 ~]$ cat /etc/fstab
"
```

Next, create a file on the mounted volume and add some text using the first command shown below; the second command is used to verify the text has been written to the volume.

```

[ec2-user@ip-10-1-11-77 ~]$ sudo sh -c "echo some text has been written > /mnt/data-store/file.txt"
[ec2-user@ip-10-1-11-77 ~]$ cat /mnt/data-store/file.txt
some text has been written
[ec2-user@ip-10-1-11-77 ~]$ 
```

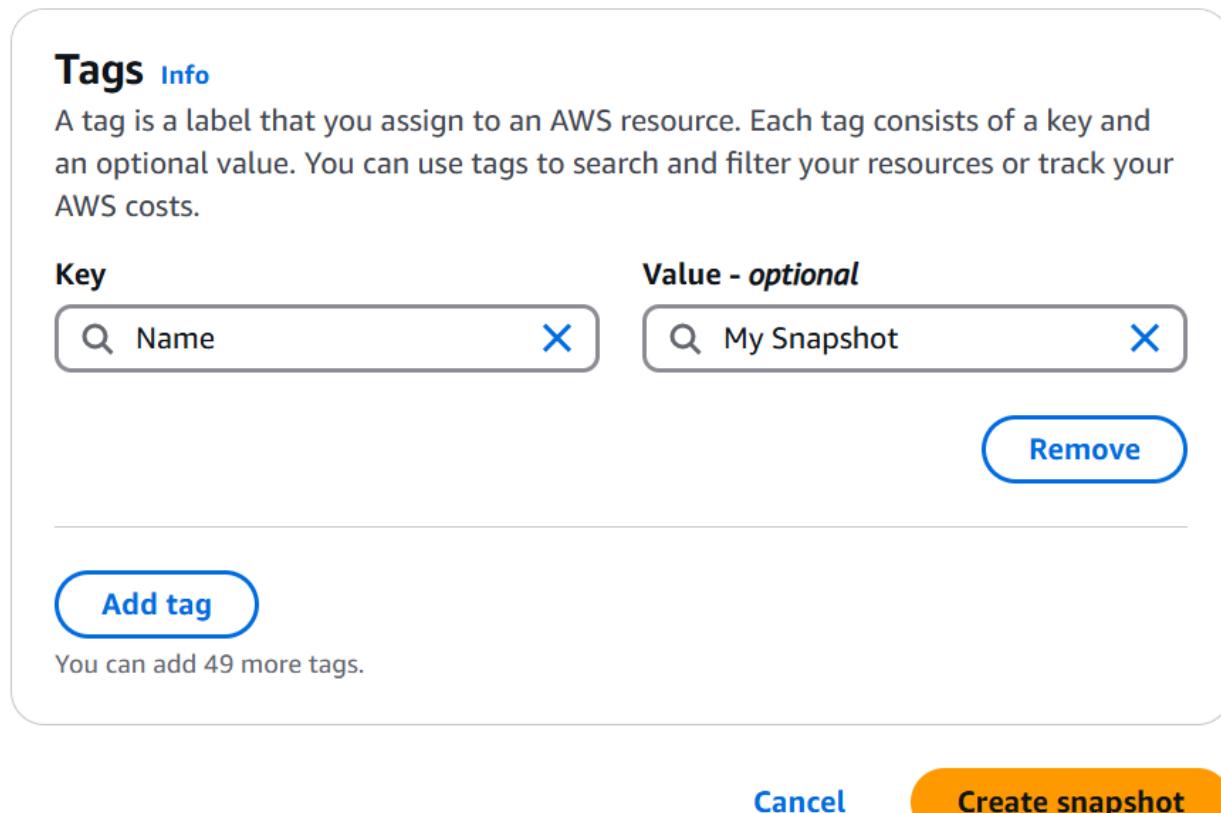
Go back into the EC2 Console, choose Volumes, and check the box next to My Volume.

The screenshot shows the AWS Lambda console interface. At the top, there's a navigation bar with 'Lambda' and other options like 'CloudWatch Metrics'. Below it, a search bar and a 'Create Function' button are visible. The main area displays a table of functions:

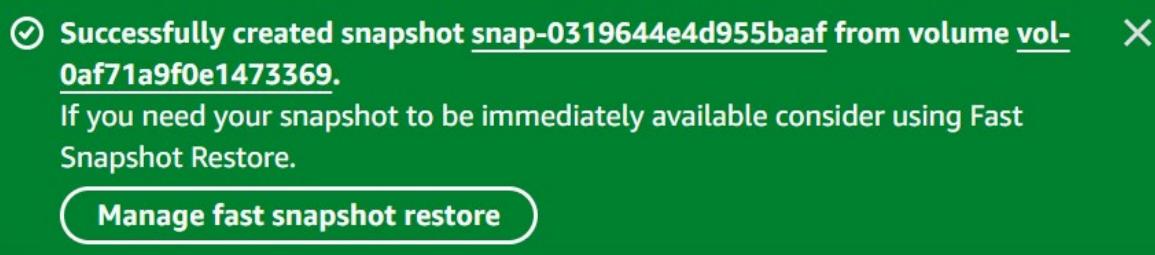
Name	Last modified	Size	Runtime	Status
HelloWorld	1 hour ago	1.46 KB	Node.js 12.x	Up to date

Below the table, there's a section for the 'HelloWorld' function with tabs for 'Details', 'Status checks', 'Monitoring', and 'Tags'. The 'Details' tab is selected, showing information like Volume ID, Size, Type, and Status check.

In the Actions drop-down menu, select Create snapshot. Choose Add tag and configure Key as **Name** and Value as **My Snapshot**. Click Create snapshot.



There should be a pop-up message like the following:



Next, in the left navigation pane, click on Snapshots, where the snapshot that was just created is displayed. In the EC2 Instance Connect terminal session, delete the file created on the volume using the command `sudo rm /mnt/data-store/file.txt`. Verify the file has been deleted using the command `ls /mnt/data-store/`.

```
[ec2-user@ip-10-1-11-77 ~]$ sudo rm /mnt/data-store/file.txt
[ec2-user@ip-10-1-11-77 ~]$ ls /mnt/data-store
lost+found
```

In the EC2 console, check the box next to My Snapshot; in the Actions menu, click on Create volume from snapshot.

The screenshot shows the AWS EC2 Snapshots page. At the top, there are navigation icons and a search bar. Below that, a toolbar with 'Recycle Bin', 'Actions' (with a dropdown arrow), and 'Create snapshot' buttons. The 'Actions' button is currently active, displaying a dropdown menu with the following options: 'Create volume from snapshot' (highlighted with a blue border), 'Create image from snapshot', 'Copy snapshot', 'Launch copy duration calculator', 'Delete snapshot', 'Manage tags', 'Snapshot settings', and 'Archiving'. To the left of the dropdown, a filter for 'Owned by me' is set to 'Name' and a specific snapshot named 'My Snapshot' is selected. On the right, there are buttons for 'Volume size' (set to 1 GiB) and 'Description'. Below the toolbar, the 'Snapshot ID: snap-0...' is displayed. At the bottom, there are tabs for 'Details' (selected), 'Snapshot settings', 'Storage tier', and 'Tags'. Under the 'Details' tab, the 'Snapshot ID' is listed as 'snap-0319644e4d955baaf (My Snapshot)' and the 'Progress' is shown as '100%' with a green checkmark.

Use the same configurations for the original volume, but for the Value attribute under Add tag instead of Volume, enter **Restored Volume**. A success message should pop up.

Successfully created volume vol-0d60e7dfbfba2f780.



Next, in the left navigation pane, navigate back to Volumes and select the check box next to Restored Volume. In the Actions drop-down menu, click on Attach volume.

The screenshot shows the AWS Lambda Volumes interface. On the left, there's a list of volumes with a filter set applied to 'Restored Volu...'. In the center, a specific volume is selected with the ID 'vol-0d60e7dfbfba2f780 (Restored Volume)'. On the right, an 'Actions' menu is open, with 'Attach volume' highlighted. A dropdown for 'Size' shows options of 1 GiB, 1 GiB, and 9 GiB.

Volumes (1/4) Info

Saved filter sets [Choose filter set](#) [Filter](#)

Name

Restored Volu...

My Volume

-

Volume ID: vol-0d60e7dfbfba2f780 (Restored Volume)

Actions

Create volume

Modify volume

Create snapshot

Create snapshot lifecycle policy

Delete volume

Attach volume

Detach volume

Force detach volume

Manage auto-enabled I/O

Manage tags

Fault injection

Size

1 GiB

1 GiB

9 GiB

Configure as following:

Volume ID

vol-0d60e7dfbfba2f780 (Restored Volume)

Availability Zone

us-east-1a

Instance | [Info](#)

i-038d6ce58a77f3865

(Lab) (running)



Only instances in the same Availability Zone as the selected volume are displayed.

Device name | [Info](#)

/dev/sdg

Recommended device names for Linux: /dev/xvda for root volume. /dev/sd[f-p] for data volumes.

i Newer Linux kernels may rename your devices to **/dev/xvdf** through **/dev/xvdp** internally, even when the device name entered here (and shown in the details) is **/dev/sdf** through **/dev/sdp**.

Choose Attach volume. Go back into the terminal session and enter the following commands:
`sudo mkdir /mnt/data-store2` to create a directory for mounting the new storage volume, mount the volume using `sudo mount /dev/sdg /mnt/data-store2`, and verify this by using `ls /mnt/data-store2/`.

```
[ec2-user@ip-10-1-11-77 ~]$ sudo mkdir /mnt/data-store2
[ec2-user@ip-10-1-11-77 ~]$ sudo mount /dev/sdg /mnt/data-store2
[ec2-user@ip-10-1-11-77 ~]$ ls /mnt/data-store2/
file.txt  lost+found
```

The file.txt is the verification that shows that mounting was successful.

LAB 5

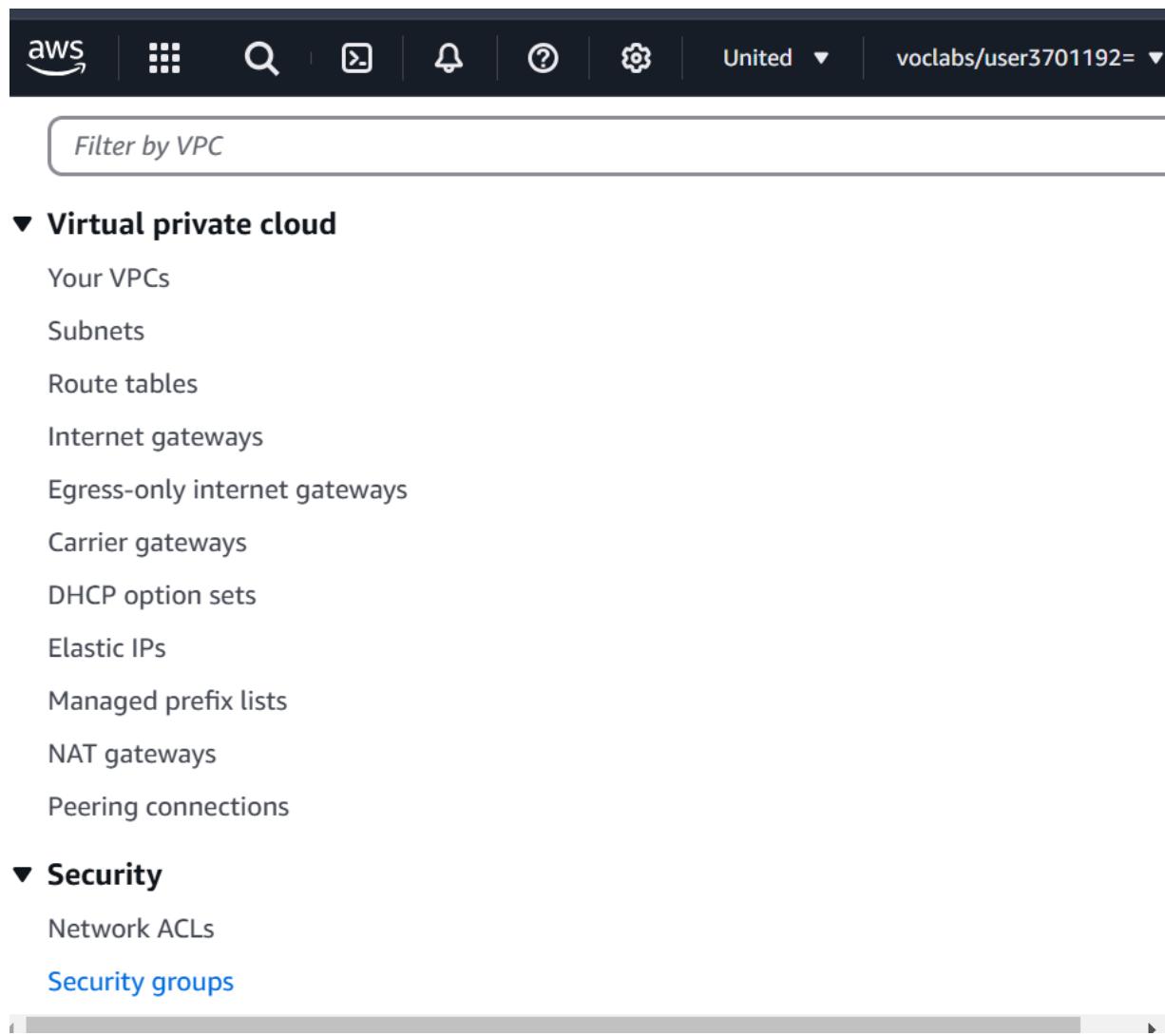
In the search box, search for and enter VPC.



The screenshot shows the AWS search interface with the query 'vpc' entered in the search bar. The 'Services' tab is selected. The results list three services:

- VPC**: Isolated Cloud Resources. Icon: Cloud with a trash can.
- AWS Firewall Manager**: Central management of firewall rules. Icon: Flame.
- Detective**: Investigate and Analyze potential security issues. Icon: Detective hat.

Select Security groups under the left navigation pane.

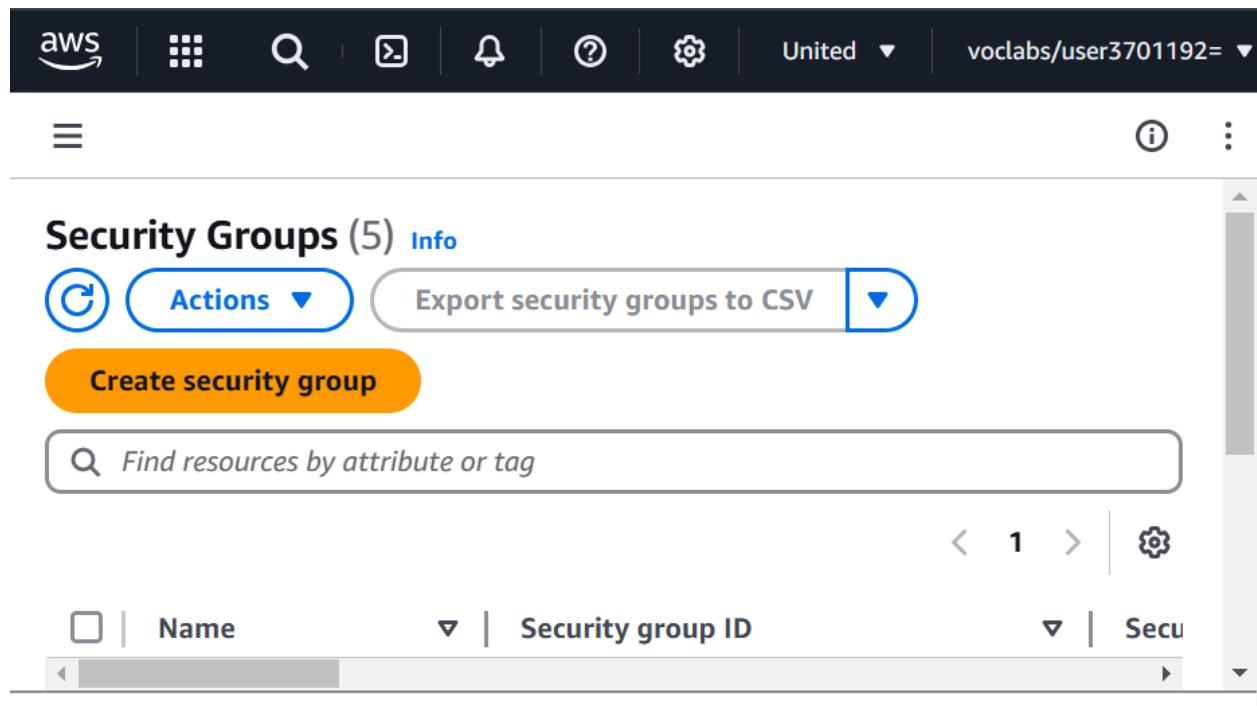


The screenshot shows the AWS VPC service page. At the top, there's a navigation bar with the AWS logo, a search icon, a refresh icon, a notifications icon, a help icon, and a settings icon. To the right of the navigation icons are the account name "United" and a user dropdown menu with the identifier "vclabs/user3701192=". Below the navigation bar is a search bar labeled "Filter by VPC". The main content area has a sidebar on the left with the following menu items:

- ▼ Virtual private cloud**
 - Your VPCs
 - Subnets
 - Route tables
 - Internet gateways
 - Egress-only internet gateways
 - Carrier gateways
 - DHCP option sets
 - Elastic IPs
 - Managed prefix lists
 - NAT gateways
 - Peering connections
- ▼ Security**
 - Network ACLs
 - Security groups**

This should take you to a screen like the one below.





The screenshot shows the AWS Management Console interface for managing Security Groups. At the top, there's a navigation bar with the AWS logo, a search icon, a refresh icon, a bell icon, a question mark icon, and a gear icon. To the right of the gear icon is the text "United" with a dropdown arrow. Further right is the user information "voclabs/user3701192=" followed by another dropdown arrow. Below the navigation bar, there's a menu icon (three horizontal lines) and an info icon.

The main content area is titled "Security Groups (5)" with an "Info" link. Below the title are three buttons: a blue "Actions" button with a dropdown arrow, a grey "Export security groups to CSV" button with a dropdown arrow, and an orange "Create security group" button. There's also a search bar with the placeholder "Find resources by attribute or tag".

Below the search bar is a pagination section with arrows for navigating through the results, a page number "1", and a gear icon for settings. The results table has columns for "Name", "Security group ID", and "Secu" (partially visible). The "Name" column includes a checkbox header. The "Security group ID" column includes a dropdown arrow header. The "Secu" column includes a dropdown arrow header.

Select Create security group and configure as shown below.

Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name [Info](#)

DB Security Group

Name cannot be edited after creation.

Description [Info](#)

Permit access from Web Security Group

VPC [Info](#)

vpc-0193fb0b3baa4abac (Lab VPC)



Add a rule under the Inbound rules section. Configure the following:



VPC > Security Groups > Create security group

Inbound rules [Info](#)

Inbound rule 1 [Delete](#)

Type Info	Protocol Info
MYSQL/Aurora	TCP
Port range Info	Source type Info
3306	Custom
Source Info	Description - optional Info
<input type="text"/> sg-01ac1a4c9759c2091 X	
<input type="text"/> sg-01ac1a4c9759c2091 X	

[Add rule](#)

In the search box, open up RDS.

The screenshot shows the AWS search interface with the query 'rds' entered in the search bar. Below the search bar, there are tabs for Services, Features, Resources, Documentation, and Knowledge. The Services tab is selected. The search results list three services: RDS, Database Migration Service, and Kinesis.

Service	Description	Action
RDS	Managed Relational Database Service	Star ^
Database Migration Service	Managed Database Migration Service	Star ^
Kinesis	Work with Real-Time Streaming Data	Star ^

It should open up a page like the one below.

i Introducing Aurora I/O-Optimized

Aurora's I/O-Optimized [\[?\]](#) is a new cluster storage configuration that offers predictable pricing for all applications and improved price-performance, with up to 40% costs savings for I/O-intensive applications.

Resources

[Refresh](#)

You are using the following Amazon RDS resources in the US East (N. Virginia) region (used/quota)

[DB Instances \(0/40\)](#)[Parameter groups \(1\)](#)[Allocated storage \(0 TB/100 TB\)](#)[Default \(1\)](#)

Instances and storage include
Neptune and DocumentDB.

[Custom \(0/100\)](#)[Increase DB instances limit \[\\[?\\]\]\(#\)](#)[Option groups \(1\)](#)[DB Clusters \(0/40\)](#)[Default \(1\)](#)[Reserved instances \(0/40\)](#)[Custom \(0/20\)](#)[Schemas \(0\)](#)[Subnet groups \(0/50\)](#)[Manual](#)[Supported platforms \[\\[?\\]\]\(#\) VPC](#)[Default network `vpc-`](#)

Next, in the left navigation pane, click on Subnet groups and click on Create DB Subnet Group, configuring as shown below:



Subnet group details

Name

You won't be able to modify the name after your subnet group has been created.

DB-Subnet-Group

Must contain from 1 to 255 characters. Alphanumeric characters, spaces, hyphens, underscores, and periods are allowed.

Description

DB Subnet Group

VPC

Choose a VPC identifier that corresponds to the subnets you want to use for your DB subnet group. You won't be able to choose a different VPC identifier after your subnet group has been created.

Lab VPC (vpc-0193fb0b3baa4abac)

4 Subnets, 2 Availability Zones



Scroll to the Add subnets part and configure the following.



Add subnets

Availability Zones

Choose the Availability Zones that include the subnets you want to add.

Choose an availability zone

us-east-1a 

us-east-1b 

Subnets

Choose the subnets that you want to add. The list includes the subnets in the selected Availability Zones.

Select subnets

Private Subnet 1

Subnet ID: subnet-03befd481dbb4f16c CIDR: 10.0.1.0/24



Private Subnet 2

Subnet ID: subnet-074ef40307ed5e8aa CIDR: 10.0.3.0/24



Click on the Create button. Next, navigate to Databases from the left navigation pane.

Databases (0)

Group resources



[Modify](#)

[Actions ▾](#)

[Restore from S3](#)

[Create database](#)



Filter by databases



1



DB identifier



Status



Role

No instances found

Choose Create database. Configure to match the following.



Alysia Chen

Choose a database creation method

Standard create

You set all of the configuration options, including ones for availability, security, backups, and maintenance.

Easy create

Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

Engine options

Engine type [Info](#)

Aurora (MySQL Compatible)



Aurora (PostgreSQL Compatible)



MySQL



PostgreSQL



Edition

MySQL Community

Engine version [Info](#)

View the engine versions that support the following database features.

▼ Hide filters

Show only versions that support the Multi-AZ DB cluster [Info](#)

Create a A Multi-AZ DB cluster with one primary DB instance and two readable standby DB instances. Multi-AZ DB clusters provide up to 2x faster transaction commit latency and automatic failover in typically under 35 seconds.

Show only versions that support the Amazon RDS Optimized Writes [Info](#)

Amazon RDS Optimized Writes improves write throughput by up to 2x at no additional cost.

Engine version

MySQL 8.0.40

Enable RDS Extended Support [Info](#)

Amazon RDS Extended Support is a [paid offering](#). By selecting this option, you consent to being charged for this offering if you are running your database major version past the RDS end of standard support date for that version. Check the end of standard support date for your major version in the [RDS for MySQL documentation](#).

Templates

Choose a sample template to meet your use case.

Production

Use defaults for high availability and fast, consistent performance.

Dev/Test

This instance is intended for development use outside of a production environment.

Free tier

Use RDS Free Tier to develop new applications, test existing applications, or gain hands-on experience with Amazon RDS. [Info](#)

Availability and durability

Deployment options [Info](#)

The deployment options below are limited to those supported by the engine you selected above.

Multi-AZ DB Cluster

Creates a DB cluster with a primary DB instance and two readable standby DB instances, with each DB instance in a different Availability Zone (AZ). Provides high availability, data redundancy and increases capacity to serve read workloads.

Multi-AZ DB instance

Creates a primary DB instance and a standby DB instance in a different AZ. Provides high availability and data redundancy, but the standby DB instance doesn't support connections for read workloads.

Single DB instance

Creates a single DB instance with no standby DB instances.



Settings

DB instance identifier [Info](#)

Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

 lab-db

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 63 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

▼ Credentials Settings

Master username [Info](#)

Type a login ID for the master user of your DB instance.

 main

1 to 16 alphanumeric characters. The first character must be a letter.

Credentials management

You can use AWS Secrets Manager or manage your master user credentials.

 Managed in AWS Secrets Manager - *most secure*

RDS generates a password for you and manages it throughout its lifecycle using AWS Secrets Manager.

 Self managed

Create your own password or have RDS create a password that you manage.

 Auto generate password

Amazon RDS can generate a password for you, or you can specify your own password.

Set the password as **lab-password**.

Master password [Info](#)

.....

Password strength [Neutral](#)

Minimum constraints: At least 8 printable ASCII characters. Can't contain any of the following symbols: / ' " @

Confirm master password [Info](#)

.....

Instance configuration

The DB instance configuration options below are limited to those supported by the engine that you selected above.

DB instance class [Info](#)

▼ Hide filters

Show instance classes that support Amazon RDS Optimized Writes [Info](#)

Amazon RDS Optimized Writes improves write throughput by up to 2x at no additional cost.

Include previous generation classes



- Standard classes (includes m classes)
- Memory optimized classes (includes r and x classes)
- Burstable classes (includes t classes)

db.t3.micro
2 vCPUs 1 GiB RAM Network: Up to 2,085 Mbps

Storage

Storage type [Info](#)

Provisioned IOPS SSD (io2) storage volumes are now available.

General Purpose SSD (gp3)
Performance scales independently from storage

Allocated storage [Info](#)

20

GiB

Minimum: 20 GiB. Maximum: 6,144 GiB



Connectivity [Info](#)

Compute resource

Choose whether to set up a connection to a compute resource for this database. Setting up a connection will automatically change connectivity settings so that the compute resource can connect to this database.

Don't connect to an EC2 compute resource

Don't set up a connection to a compute resource for this database. You can manually set up a connection to a compute resource later.

Connect to an EC2 compute resource

Set up a connection to an EC2 compute resource for this database.

Virtual private cloud (VPC) [Info](#)

Choose the VPC. The VPC defines the virtual networking environment for this DB instance.

Lab VPC (vpc-0193fb0b3baa4abac)
4 Subnets, 2 Availability Zones

Only VPCs with a corresponding DB subnet group are listed.

i After a database is created, you can't change its VPC.

DB subnet group [Info](#)

Choose the DB subnet group. The DB subnet group defines which subnets and IP ranges the DB instance can use in the VPC that you selected.

db-subnet-group

2 Subnets, 2 Availability Zones



Public access [Info](#)

Yes

RDS assigns a public IP address to the database. Amazon EC2 instances and other resources outside of the VPC can connect to your database. Resources inside the VPC can also connect to the database. Choose one or more VPC security groups that specify which resources can connect to the database.

No

RDS doesn't assign a public IP address to the database. Only Amazon EC2 instances and other resources inside the VPC can connect to your database. Choose one or more VPC security groups that specify which resources can connect to the database.

VPC security group (firewall) [Info](#)

Choose one or more VPC security groups to allow access to your database. Make sure that the security group rules allow the appropriate incoming traffic.

Choose existing

Choose existing VPC security groups

Create new

Create new VPC security group



Existing VPC security groups

Choose one or more options

DB Security Group X

RDS Proxy

RDS Proxy is a fully managed, highly available database proxy that improves application scalability, resiliency, and security.

Create an RDS Proxy [Info](#)

RDS automatically creates an IAM role and a Secrets Manager secret for the proxy. RDS Proxy has additional costs. For more information, see [Amazon RDS Proxy pricing](#).



Certificate authority - optional [Info](#)

Using a server certificate provides an extra layer of security by validating that the connection is being made to an Amazon database. It does so by checking the server certificate that is automatically installed on all databases that you provision.

rds-ca-rsa2048-g1 (default)
Expiry: May 25, 2061

If you don't select a certificate authority, RDS chooses one for you.

► Additional configuration

Tags - optional

A tag consists of a case-sensitive key-value pair.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tags.

Database authentication

Database authentication options [Info](#)

Password authentication

Authenticates using database passwords.

Password and IAM database authentication

Authenticates using the database password and user credentials through AWS IAM users and roles.

Password and Kerberos authentication

Choose a directory in which you want to allow authorized users to authenticate with this DB instance using Kerberos Authentication.

Monitoring

Enable Enhanced Monitoring

Enabling Enhanced Monitoring metrics are useful when you want to see how different processes or threads use the CPU.

▼ Additional configuration

Database options, encryption turned off, backup turned off, backtrack turned off, maintenance, CloudWatch Logs, delete protection turned off.

Database options

Initial database name [Info](#)

lab

If you do not specify a database name, Amazon RDS does not create a database.

DB parameter group [Info](#)

default.mysql8.0

Option group [Info](#)

default:mysql-8-0

Backup

Enable automated backups

Creates a point-in-time snapshot of your database



Backup

- Enable automated backups**
Creates a point-in-time snapshot of your database

Encryption

- Enable encryption**
Choose to encrypt the given instance. Master key IDs and aliases appear in the list after they have been created using the AWS Key Management Service console. [Info](#)

Log exports

Select the log types to publish to Amazon CloudWatch Logs

- Audit log
- Error log
- General log
- Slow query log

IAM role

The following service-linked role is used for publishing logs to CloudWatch Logs.

RDS service-linked role

Maintenance

Auto minor version upgrade [Info](#)

- Enable auto minor version upgrade**

Enabling auto minor version upgrade will automatically upgrade to new minor versions as they are released. The automatic upgrades occur during the maintenance window for the database.

Maintenance window [Info](#)

Select the period you want pending modifications or maintenance applied to the database by Amazon RDS.

- Choose a window
- No preference

Deletion protection

- Enable deletion protection**

Protects the database from being deleted accidentally. While this option is enabled, you can't delete the database.

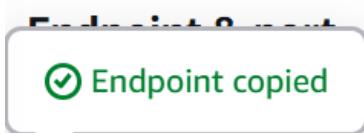
Estimated monthly costs

DB instance	24.82 USD
Storage	4.60 USD
Total	29.42 USD

After the database is available, click on lab-db and make sure the status is Modifying or Available. Navigate to the Connectivity & security section and copy the Endpoint field into a document.



Connectivity & security

**Port**

3306

Networking**Availability Zone**

us-east-1b

VPC[Lab VPC \(vpc-05164bec5cd64b23e\)](#)**Subnet group**

db-subnet-group

Subnets[subnet-01eb23f688596fb92](#)[subnet-0182d5ed057f00c49](#)**Network type**

IPv4

The following is my endpoint: lab-db.caaxcp3o3rcc.us-east-1.rds.amazonaws.com.

Next, to discover the WebServer IP address, click on the AWS Details drop-down menu above the lab instructions (not the AWS Console) and find the WebServer IP address. Copy IPv4 address into a new web browser. In this case, the IPv4 address is 23.22.44.151.



(1) ips -- public:23.22.44.151,
private:10.0.2.244 (2) ips --
public:100.27.44.122, private:10.0.0.182

SSH key

Show

Download PEM

Download PPK

AWS SSO

Download URL

SecretKey	jk6F0GcIRLWZL/0pa4sr
WebServer	23.22.44.151
BastionHost	100.27.44.122
Region	us-east-1
AccessKey	AKIARVFVZHBTT7FZA5

This should bring you to the page below.



Load Test RDS

Meta-Data	Value
InstanceId	i-0bb9b14471ffbbf3d
Availability Zone	us-east-1b

Current CPU Load: 5%



Alysia Chen

Click on the RDS link on the top of the page and configure as shown below, where the endpoint is copied from before and the password is **lab-password**:

The screenshot shows a configuration form for an AWS RDS database. The fields are as follows:

Endpoint	lab-db.caaxcp3o3rcc.us-east-1.rds.amazonaws.com
Database	lab
Username	main
Password	*****

Below the form is a "Submit" button.

However, we find that, when the above is submitted per the directions, the web page does not display anything.

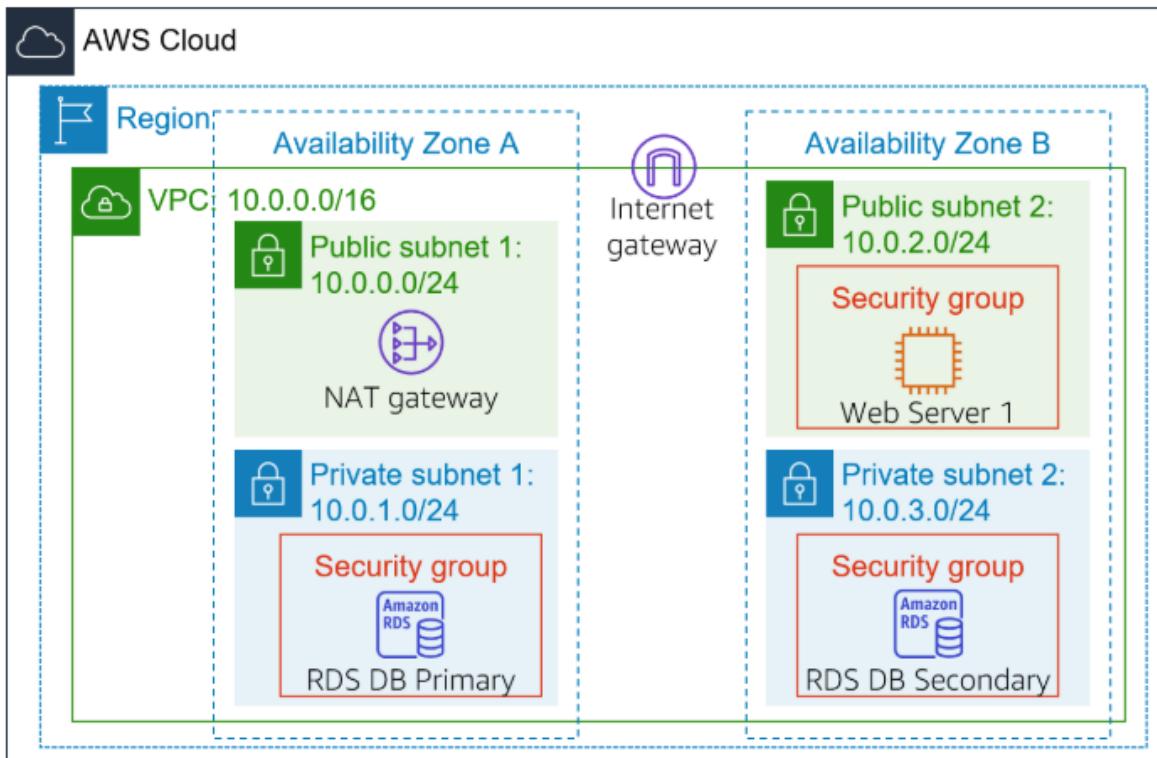


Therefore, we are unable to configure the web application to use the database.

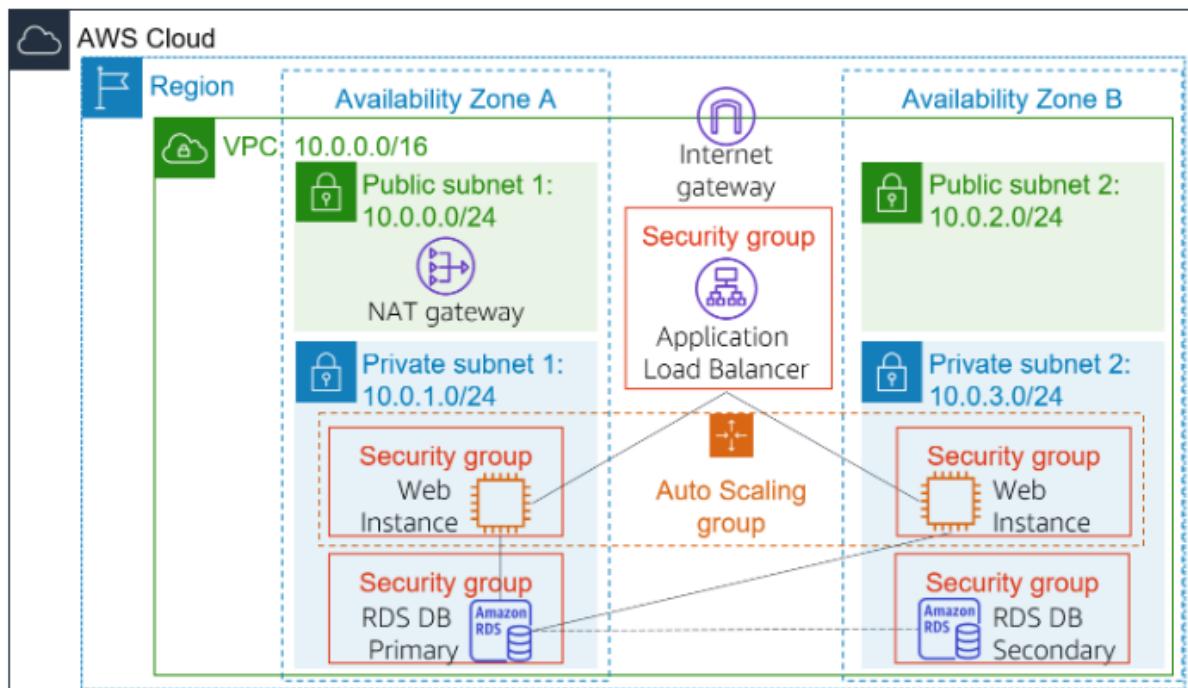
LAB 6

Start with this:





Finish with this:



Search in the search box for EC2 to open it. Choose instances in the left navigation pane. Make sure the Web Server displays 2/2 checks passed before continuing, as shown below:

Instances (2) Info		Last updated C less than a minute ago	Connect	Instance state ▾	Actions ▾	Launch instances ▾
		Find Instance by attribute or tag (case-sensitive)		All states ▾		
		Instance state = running X Clear filters				
<input type="checkbox"/>	Name F	Instance ID	Instance state	Instance type	Status check	Alarm status
<input type="checkbox"/>	Bastion Host	i-09a779f1c70ab0d26	Running Q Q	t2.micro	2/2 checks passed View alarms +	us-east-1a
<input type="checkbox"/>	Web Server 1	i-0814cecb7aee6f2ab	Running Q Q	t2.micro	2/2 checks passed View alarms +	us-east-1a
< 1 >	Filter	Edit	Delete	Details	Logs	Metrics

Check the box next to Web Server 1 and in the Actions menu, choose Image and templates and select Create image. Configure as shown in the following image.

Create image [Info](#)

An image (also referred to as an AMI) defines the programs and settings that are applied when you launch an EC2 instance. You can create an image from the configuration of an existing instance.

Instance ID
 i-0814cecb7aee6f2ab (Web Server 1)

Image name

Maximum 127 characters. Can't be modified after creation.

Image description - optional

Maximum 255 characters

Reboot instance
When selected, Amazon EC2 reboots the instance so that data is at rest when snapshots of the attached volumes are taken. This ensures data consistency.

There should be a success message with the AMI ID for the new AMI: [ami-09aeb64c9c02321aa](#).

- Currently creating AMI [ami-09aeb64c9c02321aa](#) from instance i-0814cecb7aee6f2ab. Check that the AMI status is 'Available' before deleting the instance or carrying out other actions related to this AMI. X

In the left navigation pane, select Target Groups, which define where to send traffic coming into the Load Balancer. Click on Create target group and configure similar to the following.

Specify group details

Your load balancer routes requests to the targets in a target group and performs health checks on the targets.

Basic configuration

Settings in this section can't be changed after the target group is created.

Choose a target type

Instances

- Supports load balancing to instances within a specific VPC.
- Facilitates the use of [Amazon EC2 Auto Scaling](#) to manage and scale your EC2 capacity.

IP addresses

- Supports load balancing to VPC and on-premises resources.
- Facilitates routing to multiple IP addresses and network interfaces on the same instance.
- Offers flexibility with microservice based architectures, simplifying inter-application communication.
- Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.

Target group name

LabGroup

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Protocol : Port

Choose a protocol for your target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now include anomaly detection for the targets and you can set mitigation options once your target group is created. This choice cannot be changed after creation

HTTP

80

1-65535

IP address type

Only targets with the indicated IP address type can be registered to this target group.

IPv4

Each instance has a default network interface (eth0) that is assigned the primary private IPv4 address. The instance's primary private IPv4 address is the one that will be applied to the target.

IPv6

Each instance you register must have an assigned primary IPv6 address. This is configured on the instance's default network interface (eth0). [Learn more](#)

VPC

Select the VPC with the instances that you want to include in the target group. Only VPCs that support the IP address type selected above are available in this list.

Lab VPC

Click next after these configurations have been completed; do not change any other settings.



Alysia Chen

Choose Create target group at the bottom of the page; no other changes are needed. In the left navigation pane, choose Load Balancers and click on Create load balancer. Create one under Application Load Balancer and configure the following.

Basic configuration

Load balancer name

Name must be unique within your AWS account and can't be changed after the load balancer is created.

LabELB

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Scheme | Info

Scheme can't be changed after the load balancer is created.

Internet-facing

- Serves internet-facing traffic.
- Has public IP addresses.
- DNS name is publicly resolvable.
- Requires a public subnet.

Internal

- Serves internal traffic.
- Has private IP addresses.
- DNS name is publicly resolvable.
- Compatible with the **IPv4** and **Dualstack** IP address types.

Load balancer IP address type | Info

Select the front-end IP address type to assign to the load balancer. The VPC and subnets mapped to this load balancer must include the selected IP address types. Public IPv4 addresses have an additional cost.

IPv4

Includes only IPv4 addresses.

Dualstack

Includes IPv4 and IPv6 addresses.

Dualstack without public IPv4

Includes a public IPv6 address, and private IPv4 and IPv6 addresses. Compatible with **internet-facing** load balancers only.

Network mapping | Info

The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

VPC | Info

The load balancer will exist and scale within the selected VPC. The selected VPC is also where the load balancer targets must be hosted unless routing to Lambda or on-premises targets, or if using VPC peering. To confirm the VPC for your targets, view [target groups](#). For a new VPC, [create a VPC](#).

Lab VPC

vpc-0f97ce3f3fc4f6535
IPv4 VPC CIDR: 10.0.0.0/16



Availability Zones **us-east-1a (use1-az6)**

Subnet

subnet-027efbddc458e4e03
IPv4 subnet CIDR: 10.0.0.0/24

Public Subnet 1 ▾

IPv4 address

Assigned by AWS

 us-east-1b (use1-az1)

Subnet

subnet-076b0548fcc57b229
IPv4 subnet CIDR: 10.0.2.0/24

Public Subnet 2 ▾

IPv4 address

Assigned by AWS

Security groups [Info](#)A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can [create a new security group](#).**Security groups**

Web Security Group

sg-004264b6413178915 VPC: vpc-0f97ce3f3fc4f6535

**Listeners and routing** [Info](#)

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

▼ Listener **HTTP:80****Protocol****Port**

HTTP ▾ : 80
1-65535

Default action | [Info](#)

Forward to **LabGroup** HTTP ▾
Target type: Instance, IPv4

[Create target group](#)

Then, click Create load balancer. In the left navigation pane, select Launch Templates and scroll until this page is seen:



The screenshot shows the AWS Lambda console with the following interface elements:

- Top Bar:** Includes the AWS logo, navigation icons (grid, search, refresh), a notification bell, a help icon, a gear icon, a dropdown menu labeled "United", and a user account dropdown labeled "voclabs/user370119".
- Left Sidebar:** A three-line menu icon.
- Right Sidebar:** Icons for "Edit" and "Deploy".
- Callout Box:** A callout box in the top-left corner contains the text: "Ensure best practices are used across your organization. [Learn more](#)".
- Main Content Area:** A large rounded rectangle contains:
 - New launch template** (Section Header)
 - Create launch template** (Large orange button)
- Documentation Section:** A rounded rectangle below the main content area contains:
 - Documentation** (Section Header)
 - [Documentation](#)
 - [API reference](#)

Click on Create launch template and configure as shown below.



Launch template name and description

Launch template name - *required*

LabConfig

Must be unique to this account. Max 128 chars. No spaces or special characters like '&', '*', '@'.

Template version description

A prod webserver for MyApp

Max 255 chars

Auto Scaling guidance | [Info](#)

Select this if you intend to use this template with EC2 Auto Scaling

- Provide guidance to help me set up a template that I can use with EC2 Auto Scaling

► Template tags

► Source template

▼ Application and OS Images (Amazon Machine Image) - *required* [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below



Search our full catalog including 1000s of application and OS images

Recents

My AMIs

Quick Start



Owned by me



Shared with me



Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

WebServerAMI

ami-09aeb64c9c02321aa

2025-02-02T23:19:13.000Z Virtualization: hvm ENA enabled: true Root device type: ebs Boot mode: uefi-preferred



Alysia Chen

Description

Lab AMI for Web Server

Architecture

x86_64

AMI ID

ami-09aeb64c9c02321aa

▼ Instance type[Info](#) | [Get advice](#)[Advanced](#)**Instance type**

t2.micro

Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true
 On-Demand Windows base pricing: 0.0162 USD per Hour
 On-Demand Ubuntu Pro base pricing: 0.0134 USD per Hour
 On-Demand SUSE base pricing: 0.0116 USD per Hour
 On-Demand RHEL base pricing: 0.026 USD per Hour
 On-Demand Linux base pricing: 0.0116 USD per Hour

 All generations[Compare instance types](#)[Additional costs apply for AMIs with pre-installed software](#)**▼ Key pair (login)**[Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name

vockey

[Create new key pair](#)**▼ Network settings**[Info](#)**Subnet**[Info](#)

Don't include in launch template

[Create new subnet](#)

When you specify a subnet, a network interface is automatically added to your template.

Firewall (security groups)[Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

 [Select existing security group](#) [Create security group](#)

Security groups | [Info](#)

Select security groups ▾

Web Security Group sg-004264b6413178915 [X](#)
VPC: vpc-0f97ce3f3fc4f6535

 [Compare security group rules](#)

► **Advanced network configuration**

▼ **Storage (volumes)** [Info](#)

EBS Volumes

[Hide details](#)

- Volume 1 (AMI Root) (8 GiB, EBS, General purpose SSD (gp3), 3000 IOPS)
AMI Volumes are not included in the template unless modified

 Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage [X](#)

[Add new volume](#)

▼ **Resource tags** [Info](#)

No resource tags are currently included in this template. Add a resource tag to include it in the launch template.

[Add new tag](#)

You can add up to 50 more tags.

▼ **Advanced details** [Info](#)

IAM instance profile | [Info](#)

Don't include in launch template ▾

 [Create new IAM profile](#) [Edit](#)

Hostname type | [Info](#)

Don't include in launch template ▾

DNS Hostname | [Info](#)

- Enable resource-based IPv4 (A record) DNS requests
 Enable resource-based IPv6 (AAAA record) DNS requests



Instance auto-recovery | [Info](#)

Don't include in launch template ▾

Shutdown behavior | [Info](#)

Don't include in launch template ▾

Not applicable for EC2 Auto Scaling

Stop - Hibernate behavior | [Info](#)

Don't include in launch template ▾

Not applicable for Amazon EC2 Auto Scaling.

Termination protection | [Info](#)

Don't include in launch template ▾

Stop protection | [Info](#)

Don't include in launch template ▾

Detailed CloudWatch monitoring | [Info](#)

Enable ▾

There are no more configuration changes that need to be made. Click on Create launch template.



✓ Success

Successfully created [LabConfig\(lt-011a059c2662ca852\)](#).

▼ Actions log

Initializing requests **✓ Succeeded**

Create Launch Template **✓ Succeeded**

In the success message, click on the LabConfig launch template link. From the Actions drop-down menu, choose Create Auto Scaling group and configure as shown below; only change what is displayed in the images below.



Name

Auto Scaling group name

Enter a name to identify the group.

Lab Auto Scaling Group

Must be unique to this account in the current Region and no more than 255 characters.

Launch template Info

- i** For accounts created after May 31, 2023, the EC2 console only supports creating Auto Scaling groups with launch templates. Creating Auto Scaling groups with launch configurations is not recommended but still available via the CLI and API until December 31, 2023.

Launch template

Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, and security groups.

LabConfig



Click next to move onto the next step.



Network Info

For most applications, you can use multiple Availability Zones and let EC2 Auto Scaling balance your instances across the zones. The default VPC and default subnets are suitable for getting started quickly.

VPC

Choose the VPC that defines the virtual network for your Auto Scaling group.

vpc-0f97ce3f3fc4f6535 (Lab VPC)
▼
C

[Create a VPC](#)

Availability Zones and subnets

Define which Availability Zones and subnets your Auto Scaling group can use in the chosen VPC.

Select Availability Zones and subnets
▼
C

us-east-1a | subnet-0d1c477e1b50f86cf (Private Subnet 1)
X

10.0.1.0/24

us-east-1b | subnet-0305f361c529c43e5 (Private Subnet 2)
X

10.0.3.0/24

[Create a subnet](#)

Click next to move onto the next step.

Use the options below to attach your Auto Scaling group to an existing load balancer, or to a new load balancer that you define.

No load balancer
 Traffic to your Auto Scaling group will not be fronted by a load balancer.

Attach to an existing load balancer
 Choose from your existing load balancers.

Attach to a new load balancer
 Quickly create a basic load balancer to attach to your Auto Scaling group.

Attach to an existing load balancer

Select the load balancers that you want to attach to your Auto Scaling group.

Choose from your load balancer target groups
 This option allows you to attach Application, Network, or Gateway Load Balancers.

Choose from Classic Load Balancers

Existing load balancer target groups

Only instance target groups that belong to the same VPC as your Auto Scaling group are available for selection.

Select target groups
▼
C

LabGroup | HTTP
X

Application Load Balancer: LabELB

Click next to move onto the next step.



Configure group size and scaling - *optional* [Info](#)

Define your group's desired capacity and scaling limits. You can optionally add automatic scaling to adjust the size of your group.

Group size [Info](#)

Set the initial size of the Auto Scaling group. After creating the group, you can change its size to meet demand, either manually or by using automatic scaling.

Desired capacity type

Choose the unit of measurement for the desired capacity value. vCPUs and Memory(GiB) are only supported for mixed instances groups configured with a set of instance attributes.

Units (number of instances)



Desired capacity

Specify your group size.

2

Scaling [Info](#)

You can resize your Auto Scaling group manually or automatically to meet changes in demand.

Scaling limits

Set limits on how much your desired capacity can be increased or decreased.

Min desired capacity

2

Equal or less than desired capacity

Max desired capacity

6

Equal or greater than desired capacity

Automatic scaling - *optional*

Choose whether to use a target tracking policy [Info](#)

You can set up other metric-based scaling policies and scheduled scaling after creating your Auto Scaling group.

No scaling policies

Your Auto Scaling group will remain at its initial size and will not dynamically resize to meet demand.

Target tracking scaling policy

Choose a CloudWatch metric and target value and let the scaling policy adjust the desired capacity in proportion to the metric's value.

Scaling policy name

LabScalingPolicy

Metric type [Info](#)

Monitored metric that determines if resource utilization is too low or high. If using EC2 metrics, consider enabling detailed monitoring for better scaling performance.

Average CPU utilization



Target value

60

Instance warmup [Info](#)

300 seconds

Disable scale in to create only a scale-out policy



Additional settings

Instance scale-in protection

If protect from scale in is enabled, newly launched instances will be protected from scale in by default.

Enable instance scale-in protection

Monitoring | [Info](#)

Enable group metrics collection within CloudWatch

Default instance warmup

The amount of time that CloudWatch metrics for new instances do not contribute to the group's aggregated instance metrics, as their usage data is not reliable yet.

Enable default instance warmup

Click next to move onto the next step. In Step 5, no action is needed, so click next.

Add tags - optional [Info](#)

Add tags to help you search, filter, and track your Auto Scaling group across AWS. You can also choose to automatically add these tags to instances when they are launched.

- i** You can optionally choose to add tags to instances (and their attached EBS volumes) by specifying tags in your launch template. We recommend caution, however, because the tag values for instances from your launch template will be overridden if there are any duplicate keys specified for the Auto Scaling group.

X

Tags (1)

Key

Name

Value - optional

Instance

Tag new instances



Click on Create Auto Scaling group. In the left navigation pane, go back to Instances. There should be two new instances; refreshing may be necessary.



Launch instances		▼	
<input type="text"/> Find Instance by attribute or tag (case-sensitive)		All states ▼	
		< 1 >	⚙️
<input type="checkbox"/>	Name 🔎	Instance ID	Instance state ▾
<input type="checkbox"/>	Instance	i-0f901f5b6f04a4670	✓ Running <input type="button"/> <input type="button"/>
<input type="checkbox"/>	Bastion Host	i-09a779f1c70ab0d26	✓ Running <input type="button"/> <input type="button"/>
<input type="checkbox"/>	Instance	i-07f1aedd2c9599bbc	✓ Running <input type="button"/> <input type="button"/>
<input type="checkbox"/>	Web Server 1	i-0814cecb7aee6f2ab	✓ Running <input type="button"/> <input type="button"/>

In the left navigation pane, navigate to Target Groups and check the box next to LabGroup. Choose the Targets tab, as shown below.



The screenshot shows the AWS EC2 Target groups page. At the top, there's a navigation bar with 'EC2 > Target groups'. Below it is a search bar labeled 'Filter target groups'. A table lists one target group:

<input checked="" type="checkbox"/>	Name	ARN	Port
<input checked="" type="checkbox"/>	LabGroup	arn:aws:elasticloadbalancing...	80

The screenshot shows the 'Target group: LabGroup' details page. The 'Targets' tab is selected. It displays the following information:

- Registered targets (0)** Info
- Anomaly mitigation: Not applicable
- [Deregister](#)

Refresh so that there are two Registered targets that appear under this tab, both with a status of Healthy.

The screenshot shows the 'Target group: LabGroup' details page. The 'Targets' tab is selected. It displays the following registered targets:

<input type="checkbox"/>	Instance ID	Name	Port
<input type="checkbox"/>	i-0f901f5b6f04a4670	Instance	80
<input type="checkbox"/>	i-07f1aedd2c9599bbc	Instance	80

In the left navigation pane, select Load balancers and check the box next to LabELB. Under the details tab, find and copy the DNS name.

<input checked="" type="checkbox"/>	Name	DNS name	<input checked="" type="checkbox"/>	State
<input checked="" type="checkbox"/>	LabELB	<input type="checkbox"/> LabELB-340416000.us-east...	<input checked="" type="checkbox"/>	Active

Load balancer: LabELB

[subnet-076b0548fcc57b229](#) us-east-1b (use1-az1)

Load balancer ARN

arn:aws:elasticloadbalancing:us-east-1:581756684210:loadbalancer/app/LabELB/3e189924d2fac826

DNS name [Info](#)

LabELB-340416000.us-east-1.elb.amazonaws.com (A Record)

Paste the DNS name into a new web browser; the application should appear, indicating that the Load Balancer received and sent the request before passing back the result.

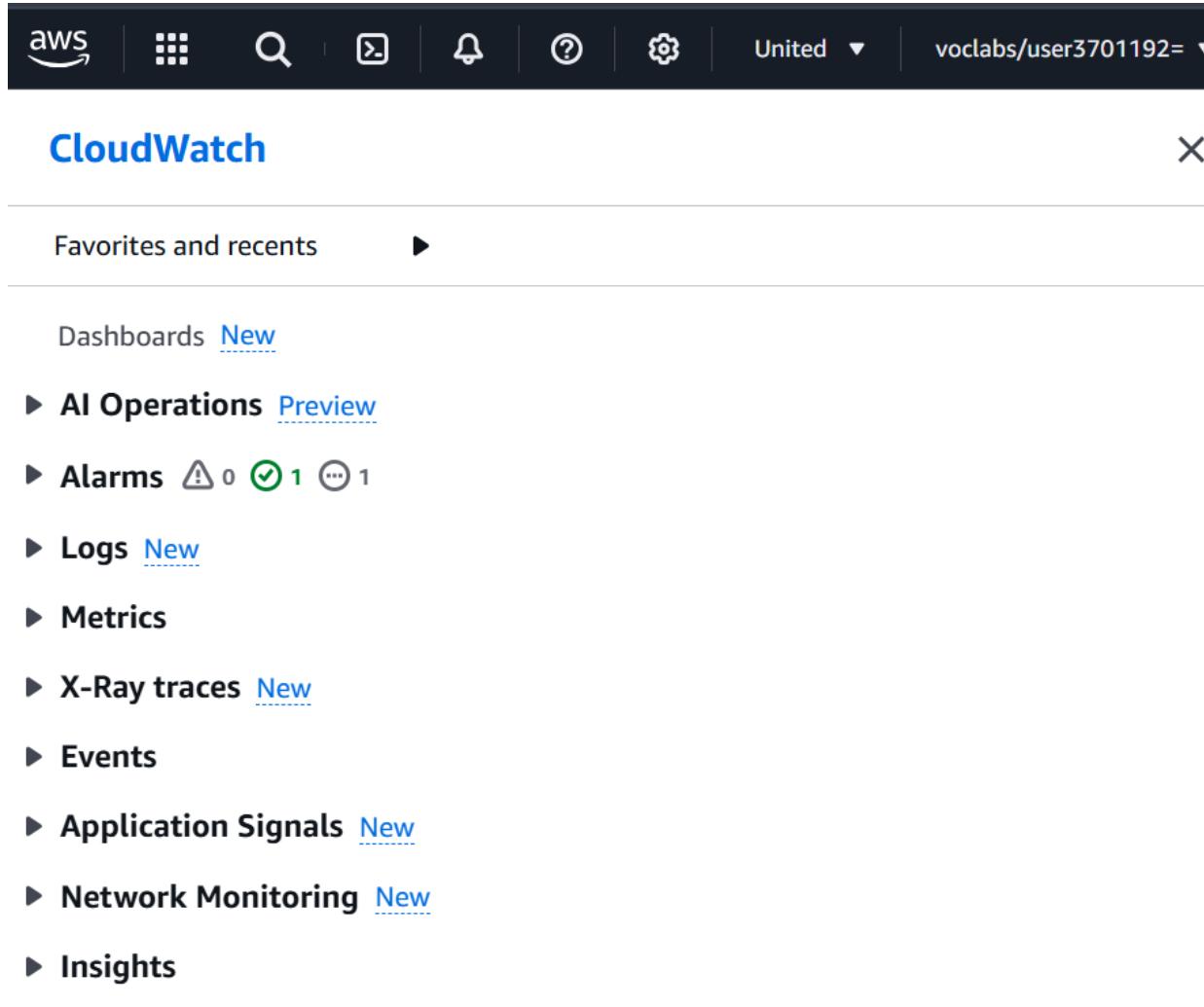


Meta-Data	Value
InstanceId	i-07f1aedd2c9599bbc
Availability Zone	us-east-1b

Current CPU Load: 5%



The browser tab may be similar to the one above when the application is running. Next, search for CloudWatch and open it without closing the application tab. The following screen should appear.



The screenshot shows the AWS CloudWatch console. At the top, there is a dark header bar with the AWS logo, a search icon, a refresh icon, a bell icon, a question mark icon, a gear icon, and the text "United" followed by a dropdown arrow. To the right of the dropdown is the URL "voclabs/user3701192=". Below the header, the title "CloudWatch" is displayed in blue, with a close button "X" to its right. A horizontal line separates the header from the main content area. In the main area, there is a section titled "Favorites and recents" with a right-pointing arrow. Below this, a list of services is shown with icons and counts: "Dashboards" (New), "AI Operations" (Preview), "Alarms" (⚠ 0, ✓ 1, ⚡ 1), "Logs" (New), "Metrics", "X-Ray traces" (New), "Events", "Application Signals" (New), "Network Monitoring" (New), and "Insights". Another horizontal line is at the bottom of this list.

Click on the Alarms drop-down menu and select All alarms.

CloudWatch

Favorites and recents ►

Dashboards [New](#)

► AI Operations [Preview](#)

▼ Alarms ⚠ 0 ✓ 1 ⋮ 1

In alarm

All alarms

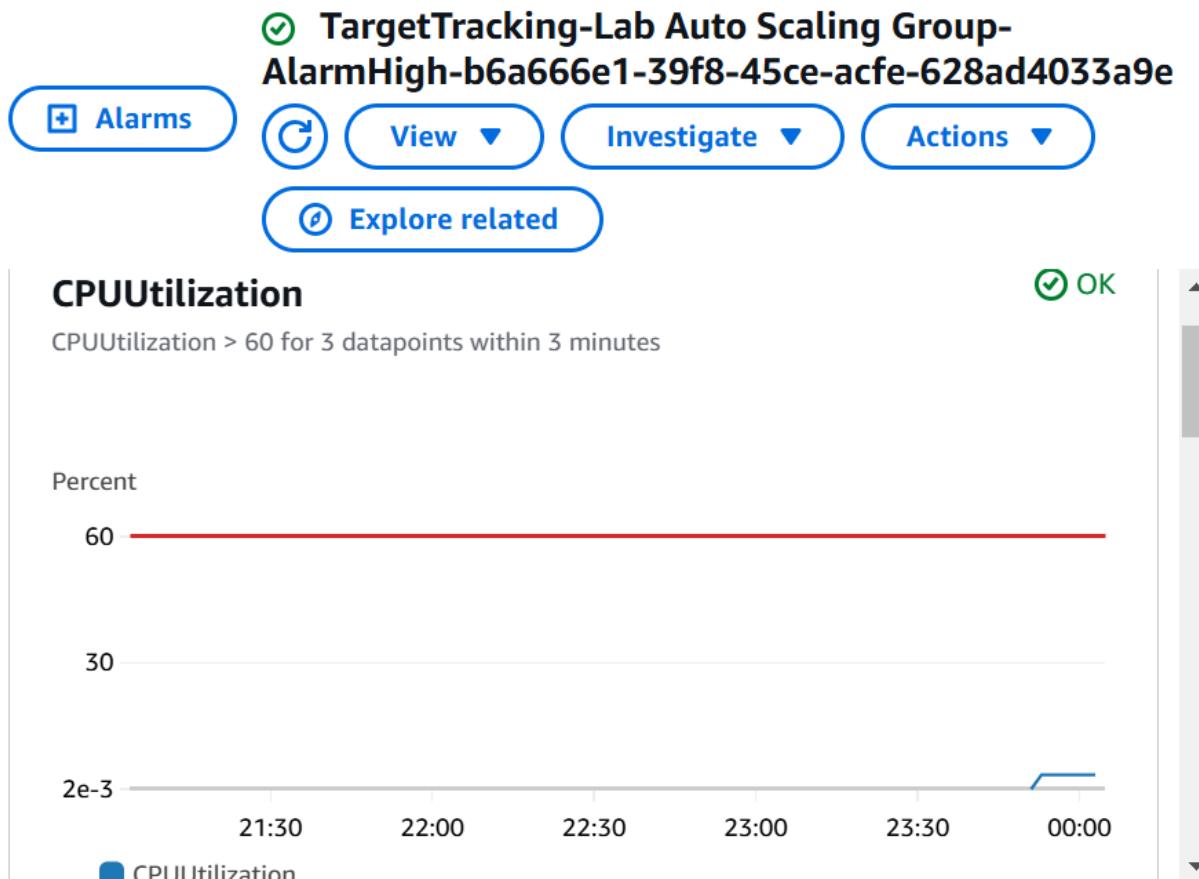
Billing

There should be two alarms displayed.

<input type="checkbox"/>	Name	State	Last state update (UTC)
<input type="checkbox"/>	TargetTracking-Lab Auto Scaling Group- AlarmHigh- b6a666e1-39f8- 45ce-acfe- 628ad4033a9e	✓ OK	2025-02-02 23:52:44
<input type="checkbox"/>	TargetTracking-Lab Auto Scaling Group- AlarmLow- 28264592-474b- 4b9f-859e- 871c121a18d8	⋮ Insufficient data	2025-02-02 23:51:10



Choose the OK alarm (the alarm containing AlarmHigh in its name). The following page should load.



Return to the web application and click on Load Test. Return to the CloudWatch console page with the two alarms and wait until the AlarmLow alarm changes to OK and AlarmHigh alarm changes to In alarm.

<input type="checkbox"/>	Name	State	Last state update (UTC)
<input type="checkbox"/>	TargetTracking-Lab Auto Scaling Group- AlarmLow- 28264592-474b- 4b9f-859e- 871c121a18d8	⚠ In alarm	2025-02-03 00:06:55
<input type="checkbox"/>	TargetTracking-Lab Auto Scaling Group- AlarmHigh- b6a666e1-39f8- 45ce-acfe- 628ad4033a9e	✓ OK	2025-02-02 23:52:44

Then, go to EC2 and into Instances through the left navigation pane. More than two instances called Instance should be running in response to the CloudWatch alarm.

<input type="checkbox"/>	Name 	Instance ID	Instance state
<input type="checkbox"/>	Instance	i-0ccc513b2159ed1e1	✓ Running  
<input type="checkbox"/>	Instance	i-0f901f5b6f04a4670	✓ Running  
<input type="checkbox"/>	Bastion Host	i-09a779f1c70ab0d26	✓ Running  
<input type="checkbox"/>	Instance	i-07f1aedd2c9599bbc	✓ Running  
<input type="checkbox"/>	Web Server 1	i-0814cecb7aee6f2ab	✓ Running  
<input type="checkbox"/>	Instance	i-0472f4baac547e5c4	✓ Running  

Select Web Server 1 and make sure it is the only instance selected.

	Name	Instance ID	Instance state			Ins
<input type="checkbox"/>	Instance	i-0ccc513b2159ed1e1	Running			t2.
<input type="checkbox"/>	Instance	i-0f901f5b6f04a4670	Running			t2.
<input type="checkbox"/>	Bastion Host	i-09a779f1c70ab0d26	Running			t2.
<input type="checkbox"/>	Instance	i-07f1aedd2c9599bbc	Running			t2.
<input checked="" type="checkbox"/>	Web Server 1	i-0814cecb7aee6f2ab	Running			t2.
<input type="checkbox"/>	Instance	i-0472f4baac547e5c4	Running			t2.

i-0814cecb7aee6f2ab (Web Server 1)



In the Instance state drop-down menu, choose Instance State and then click on Terminate Instance.

Terminate (delete) instance?



⚠️ On an EBS-backed instance, the default action is for the root EBS volume to be deleted when the instance is terminated. Storage on any local drives will be lost.

Are you sure you want to terminate these instances?

Instance ID	Termination protection
<input type="checkbox"/> i-0814cecb7aee6f2ab (Web Server 1)	Disabled

To confirm that you want to delete the instances, choose the terminate button below. Instances with termination protection enabled will not be terminated. Terminating the instance cannot be undone.

[Cancel](#)

Terminate (delete)

Confirm to Terminate.



Alysia Chen

There should be a success message:

✓ Successfully initiated termination (deletion) of i-0814cecb7aee6f2ab X

PROBLEMS:

In Lab 5, there were several problems that I encountered, one of which affected my scoring for the lab. First, I didn't uncheck Enhanced Monitoring, so I had to remake the database and delete the current one. The second time, I had the wrong DB instance identifier entered, so I had to delete the database and redo the database configuration. Afterwards, my session timed out and I was logged out of the AWS Console, so I had to restart the lab. Finally, the web page did not display anything even after the correct credentials were submitted and everything prior to this segment was displayed as correctly configured; I was unable to fix this problem due to having no incorrect configurations and just left it as is.

In Lab 6, instead of an instance named Lab Instance, the instances that were created in response were all named Instance, so the grader thought I did not finish the Auto Scaling check task. Therefore, I had to change the instance names to Lab Instance for it to register in the system, which did work. I ended up getting a full score on Lab 6.

CONCLUSION:

These labs were a lot harder than the previous labs in my opinion. Although they were equally as straightforward, some steps had lots of opportunities for mistakes, leading me to spend more time on these labs than before. However, I'm glad I was able to troubleshoot and persevere—two skills critical to becoming a network administrator.



SIGN-OFF:

Lab 4:

Total score	25/25
-------------	-------

Task 1 - Create EBS volume	5/5
----------------------------	-----

Task 2 - Attach volume	5/5
------------------------	-----

Task 4 - Volume mounted	5/5
-------------------------	-----

Task 5 - Snapshot created	5/5
---------------------------	-----

Task 6 - Snapshot restored	5/5
----------------------------	-----

Lab 5:



Total score **15/20**

Task 1 - Security Group created **5/5**

Task 2 - DB subnet group **5/5**

Task 3 - DB created **5/5**

Task 4 - App connected to DB **0/5**

Lab 6:



Alysia Chen

Total score **35/35**

Task 1 - AMI created **5/5**

Task 2 - Load Balancer created **5/5**

Task 3a - Launch Template created **5/5**

Task 3b - Auto Scaling Group created **5/5**

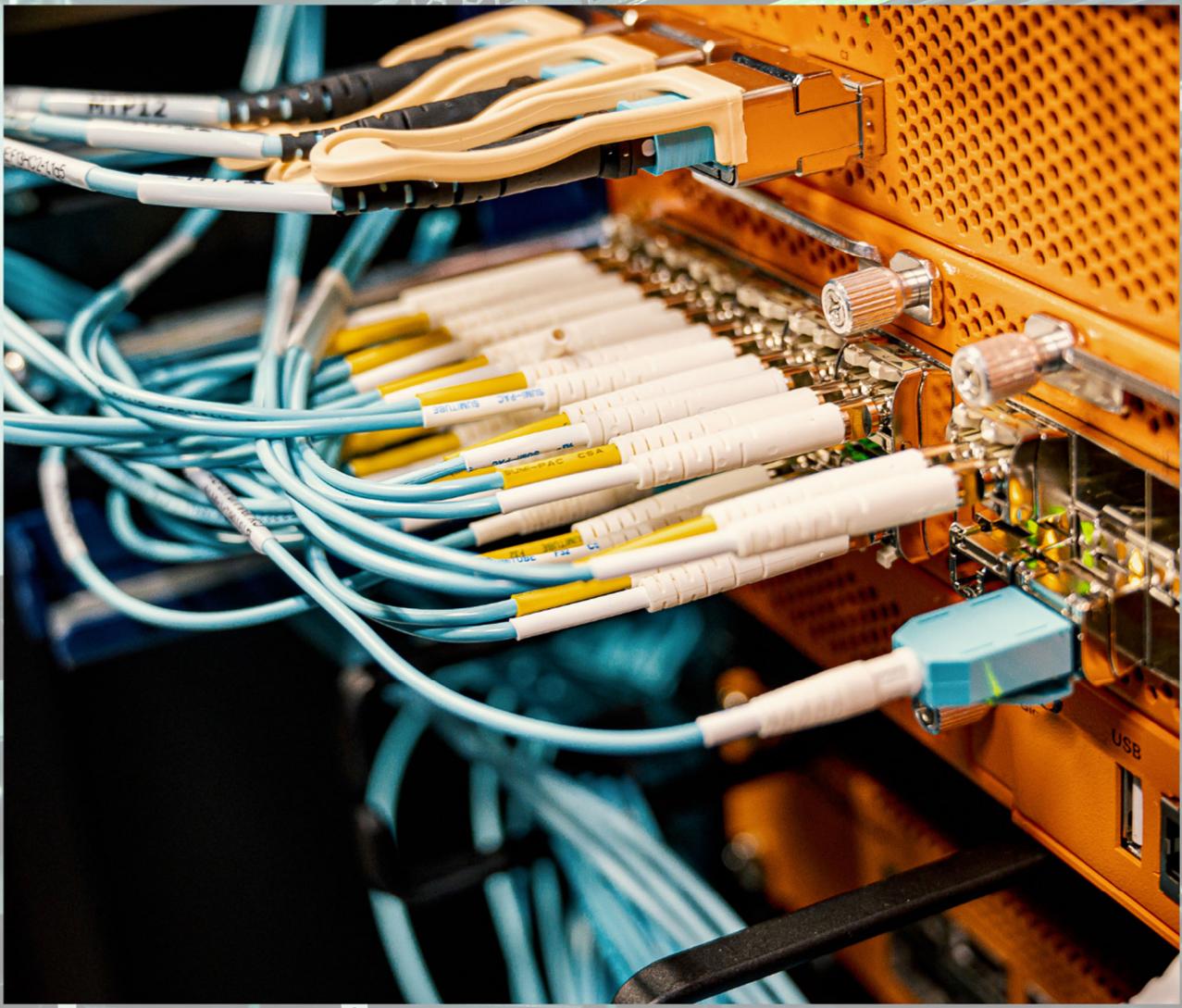
Task 4 - Load Balancer check **5/5**

Task 5 - Auto Scaling check **5/5**

Task 6 - Web Server 1 **5/5**



Lab 7: AP Configuration with RADIUS



PURPOSE:

Learn to configure IS-IS, Intermediate System to Intermediate System, in preparation for a guest speaker who made IS-IS and will be visiting in a few weeks.

BACKGROUND INFORMATION ON LAB CONCEPTS:

IS-IS (Intermediate System to Intermediate System) is designed to be an interior gateway protocol. It is also a link-state routing protocol and uses the same algorithm as OSPF to find the best path. There are also some other similarities, like how their networks both converge quickly and they both have automated neighbor discovery.

However, IS-IS is different from OSPF in that there are three types of routers used to connect different areas together: Level 1, Level 1-2, and Level 2. Level 1 can only establish neighbor adjacencies for routers in the same area; Level 2 can only establish neighbor adjacencies for routers in different areas; and Level 1-2 can perform both functions. Therefore, Level 1 is often used for routers in the local area only. Level 1-2, on the other hand, is for routers that are adjacent to both a local router and a router in a different area. They bridge the two types of routers, allowing them to exchange information. Level 2 is for routing between different areas and only establish adjacencies with other Level 2 routers. They're responsible for inter-area routing.

An analogy to illustrate the role of different routers in IS-IS is the following. Imagine in a company, there are employees, secretaries, and high-level bosses. Employees can pass messages to other employees, but they need to inform a secretary to communicate with their high-level bosses. The high-level bosses do not individually talk to their employees unless their secretary mentions it. Here, employees are like the Level 1 routers; secretaries are like the Level 1-2 routers; and high-level bosses are like the Level 2 routers.

There are a few more differences between IS-IS and OSPF. For example, IS-IS operates directly over the data link layer and uses protocol data units for communication, unlike OSPF, which uses Layer 3 IP for encapsulation. Thus, IS-IS is not dependent on IP for routing and supports multiple network layer protocols instead of just IP, which offers more options for a network administrator. IS-IS also does not have two different versions for IPv4 and IPv6, instead supporting both within IS-IS itself, unlike OSPF, which has OSPFv2 and OSPFv3. This means that it is easier to configure. Instead of assigning clear-cut areas like OSPF (which also requires there be a strong distinction between Area 0 and other areas), IS-IS opts for a less rigid structure, only designating router levels, to allow for more room for customization for network architects.

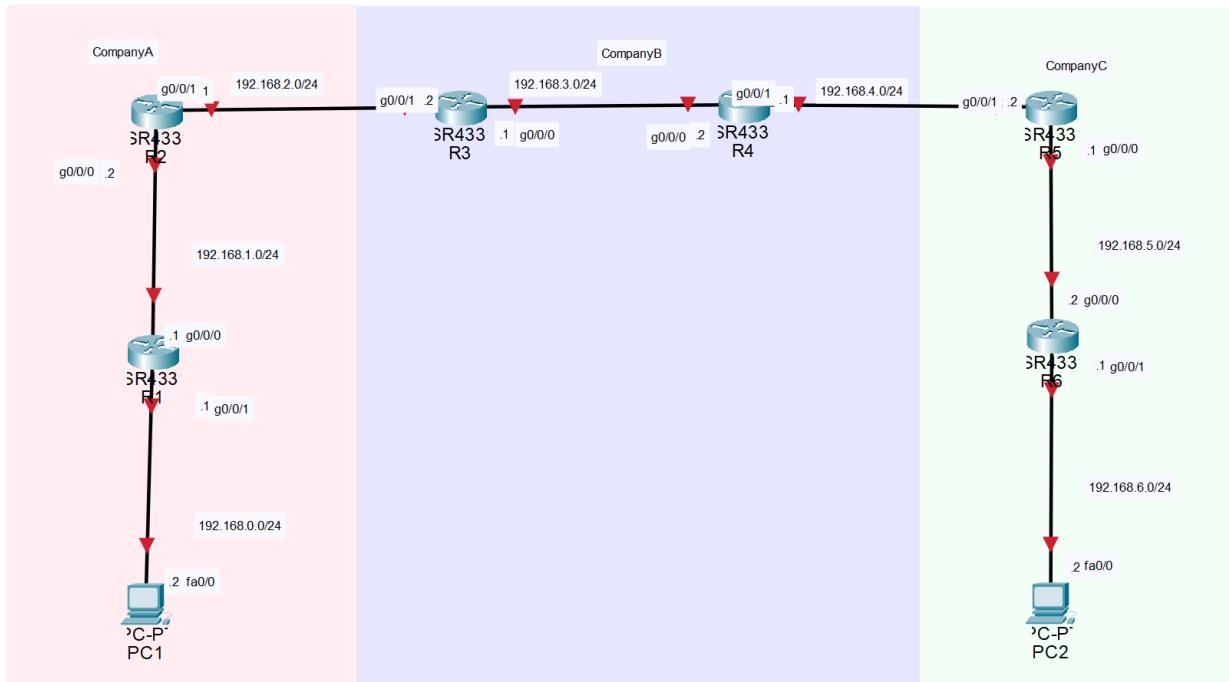
IS-IS provides a big advantage in terms of large-scale networks for its flexibility and configurability, as well as its performance in more complex topologies; however, OSPF may be better in enterprise networks because its areas allow network administrators to be able to monitor and control the network more easily and efficiently. It also has been more widely tested and used in different networks, so enterprises are likely to find OSPF more reliable and easier to find documentation about.



LAB SUMMARY:

Created an IS-IS network infrastructure for 3 companies (Company A, Company B, and Company C) using six routers and two end devices.

NETWORK DIAGRAMS:



Router	IS-IS Level
R1	Level 1
R2	Level 1-2
R3	Level 2
R4	Level 2
R5	Level 1-2
R6	Level 1

LAB COMMANDS:

After configuring network addresses for interfaces on each router, set up IS-IS:

`ip router isis` enables an interface to participate in IS-IS for IPv4.



Since the routers will use different areas, different levels of IS-IS will be configured. Enter the command `router isis` and use the global command `is-type level-1` to configure Level 1. Similarly, use the global command `is-type level-1-2` and `is-type level-2` to configure Level 1-2 and Level 2, respectively.

Specify a Network Entity Title (NET), which is the “ID” of the router in IS-IS and also determines which area the router belongs to. For example: `net 49.0001.1920.1680.0001.00`. In this case, the .0001 signifies the area, 1, that the router is in.

CONFIGURATIONS:

Note that certain output has been removed for clarity and relevance.

Traceroute from R1 to R6:

```
R1#traceroute 192.168.6.1
Type escape sequence to abort.
Tracing the route to 192.168.6.1
VRF info: (vrf in name/id, vrf out name/id)
  1 192.168.1.2 0 msec 0 msec 0 msec
  2 192.168.2.2 0 msec 1 msec 0 msec
  3 192.168.3.2 1 msec 1 msec 0 msec
  4 192.168.4.2 1 msec 1 msec 1 msec
  5 192.168.5.2 1 msec 1 msec *
```

Hostname R1—show IP route and show running configuration:

```
R1#show ip route
i*L1 0.0.0.0/0 [115/10] via 192.168.1.2, 01:14:51,
GigabitEthernet0/0/0
    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected,
GigabitEthernet0/0/0
L        192.168.1.1/32 is directly connected,
GigabitEthernet0/0/0
i L1 192.168.2.0/24 [115/20] via 192.168.1.2, 01:15:01,
GigabitEthernet0/0/0
```

```
R1#show run
interface GigabitEthernet0/0/0
    ip address 192.168.1.1 255.255.255.0
    ip router isis
    negotiation auto
!
interface GigabitEthernet0/0/1
    ip address 192.168.0.1 255.255.255.0
    ip router isis
    negotiation auto
!
```



```

interface Serial0/1/0
  no ip address
  shutdown
!
interface Serial0/1/1
  no ip address
  shutdown
!
interface GigabitEthernet0/2/0
  no ip address
  shutdown
  negotiation auto
!
interface GigabitEthernet0/2/1
  no ip address
  shutdown
  negotiation auto
!
interface GigabitEthernet0
  vrf forwarding Mgmt-intf
  no ip address
  shutdown
  negotiation auto
!
interface Vlan1
  no ip address
  shutdown
!
router isis
  net 49.0001.0000.0000.0001.00
  is-type level-1
  log-adjacency-changes

```

Hostname R2—show IP route and show running configuration:

```

R2#show ip route
  192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected,
GigabitEthernet0/0/0
L        192.168.1.2/32 is directly connected,
GigabitEthernet0/0/0
  192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected,
GigabitEthernet0/0/1
L        192.168.2.1/32 is directly connected,
GigabitEthernet0/0/1
i L2  192.168.3.0/24 [115/20] via 192.168.2.2, 01:15:46,
GigabitEthernet0/0/1

```



```

i L2 192.168.4.0/24 [115/30] via 192.168.2.2, 01:15:13,
GigabitEthernet0/0/1
i L2 192.168.5.0/24 [115/40] via 192.168.2.2, 01:14:41,
GigabitEthernet0/0/1
i L2 192.168.6.0/24 [115/50] via 192.168.2.2, 00:02:57,
GigabitEthernet0/0/1

R2#show run
interface GigabitEthernet0/0/0
  ip address 192.168.1.2 255.255.255.0
  ip router isis
  negotiation auto
!
interface GigabitEthernet0/0/1
  ip address 192.168.2.1 255.255.255.0
  ip router isis
  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
  shutdown
!
router isis
  net 49.0001.0000.0000.0002.00
  log-adjacency-changes

```

Hostname R3—show IP route and show running configuration:

```

R3#show ip route
i L2 192.168.1.0/24 [115/20] via 192.168.2.1, 01:16:58,
GigabitEthernet0/0/1
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C          192.168.2.0/24 is directly connected,
GigabitEthernet0/0/1

```



```

L      192.168.2.2/32 is directly connected,
GigabitEthernet0/0/1
      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.3.0/24 is directly connected,
GigabitEthernet0/0/0
L      192.168.3.1/32 is directly connected,
GigabitEthernet0/0/0
i L2  192.168.4.0/24 [115/20] via 192.168.3.2, 01:15:55,
GigabitEthernet0/0/0
i L2  192.168.5.0/24 [115/30] via 192.168.3.2, 01:15:23,
GigabitEthernet0/0/0
i L2  192.168.6.0/24 [115/40] via 192.168.3.2, 00:03:39,
GigabitEthernet0/0/0

R3#show run
interface GigabitEthernet0/0/0
  ip address 192.168.3.1 255.255.255.0
  ip router isis
  negotiation auto
!
interface GigabitEthernet0/0/1
  ip address 192.168.2.2 255.255.255.0
  ip router isis
  negotiation auto
!
interface Serial0/1/0
  no ip address
!
interface Serial0/1/1
  no ip address
!
interface GigabitEthernet0
  vrf forwarding Mgmt-intf
  no ip address
  negotiation auto
!
interface Vlan1
  no ip address
!
router isis
  net 49.0002.0000.0000.0003.00
  is-type level-2-only
  log adjacency-changes

```

Hostname R4—show IP route and show running configuration:

R4#show ip route



```
i L2 192.168.1.0/24 [115/30] via 192.168.3.1, 01:17:07,  
GigabitEthernet0/0/0  
i L2 192.168.2.0/24 [115/20] via 192.168.3.1, 01:17:07,  
GigabitEthernet0/0/0  
    192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks  
C      192.168.3.0/24 is directly connected,  
GigabitEthernet0/0/0  
L      192.168.3.2/32 is directly connected,  
GigabitEthernet0/0/0  
    192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks  
C      192.168.4.0/24 is directly connected,  
GigabitEthernet0/0/1  
L      192.168.4.1/32 is directly connected,  
GigabitEthernet0/0/1  
i L2 192.168.5.0/24 [115/20] via 192.168.4.2, 01:16:01,  
GigabitEthernet0/0/1
```

```
R4#show run  
interface GigabitEthernet0/0/0  
ip address 192.168.3.2 255.255.255.0  
ip router isis  
negotiation auto  
!  
interface GigabitEthernet0/0/1  
ip address 192.168.4.1 255.255.255.0  
ip router isis  
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  
shutdown  
!  
router isis
```



```
net 49.0002.0000.0000.0004.00
is-type level-2-only
log adjacency-changes
```

Hostname R5—show IP route and show running configuration:

```
R5#show ip route
i L2 192.168.1.0/24 [115/40] via 192.168.4.1, 01:17:13,
GigabitEthernet0/0/1
i L2 192.168.2.0/24 [115/30] via 192.168.4.1, 01:17:13,
GigabitEthernet0/0/1
i L2 192.168.3.0/24 [115/20] via 192.168.4.1, 01:17:13,
GigabitEthernet0/0/1
    192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.4.0/24 is directly connected,
GigabitEthernet0/0/1
L        192.168.4.2/32 is directly connected,
GigabitEthernet0/0/1
    192.168.5.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.5.0/24 is directly connected,
GigabitEthernet0/0/0
L        192.168.5.1/32 is directly connected,
GigabitEthernet0/0/0
```

```
R5#show run
interface GigabitEthernet0/0/0
ip address 192.168.5.1 255.255.255.0
ip router isis
negotiation auto
!
interface GigabitEthernet0/0/1
ip address 192.168.4.2 255.255.255.0
ip router isis
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
  shutdown
!
router isis
  net 49.0003.0000.0000.0005.00
  log-adjacency-changes
```

Hostname R6—show IP route and show running configuration:

```
R6#show ip route
i*L1  0.0.0.0/0 [115/10] via 192.168.5.1, 01:17:28,
GigabitEthernet0/0/0
i L1  192.168.4.0/24 [115/20] via 192.168.5.1, 01:17:28,
GigabitEthernet0/0/0
      192.168.5.0/24 is variably subnetted, 2 subnets, 2 masks
C          192.168.5.0/24 is directly connected,
GigabitEthernet0/0/0
L          192.168.5.2/32 is directly connected,
GigabitEthernet0/0/0
```

```
R6#show run
interface GigabitEthernet0/0/0
  ip address 192.168.5.2 255.255.255.0
  ip router isis
  negotiation auto
!
interface GigabitEthernet0/0/1
  ip address 192.168.6.1 255.255.255.0
  ip router isis
  negotiation auto
!
interface GigabitEthernet0/1/0
  no ip address
  shutdown
  negotiation auto
!
interface GigabitEthernet0/1/1
  no ip address
  shutdown
  negotiation auto
!
interface GigabitEthernet0
  vrf forwarding Mgmt-intf
  no ip address
  shutdown
  negotiation auto
```



```
!
interface Vlan1
  no ip address
  shutdown
!
router isis
  net 49.0003.0000.0000.0006.00
  is-type level-1
  log-adjacency-changes
```

PROBLEMS:

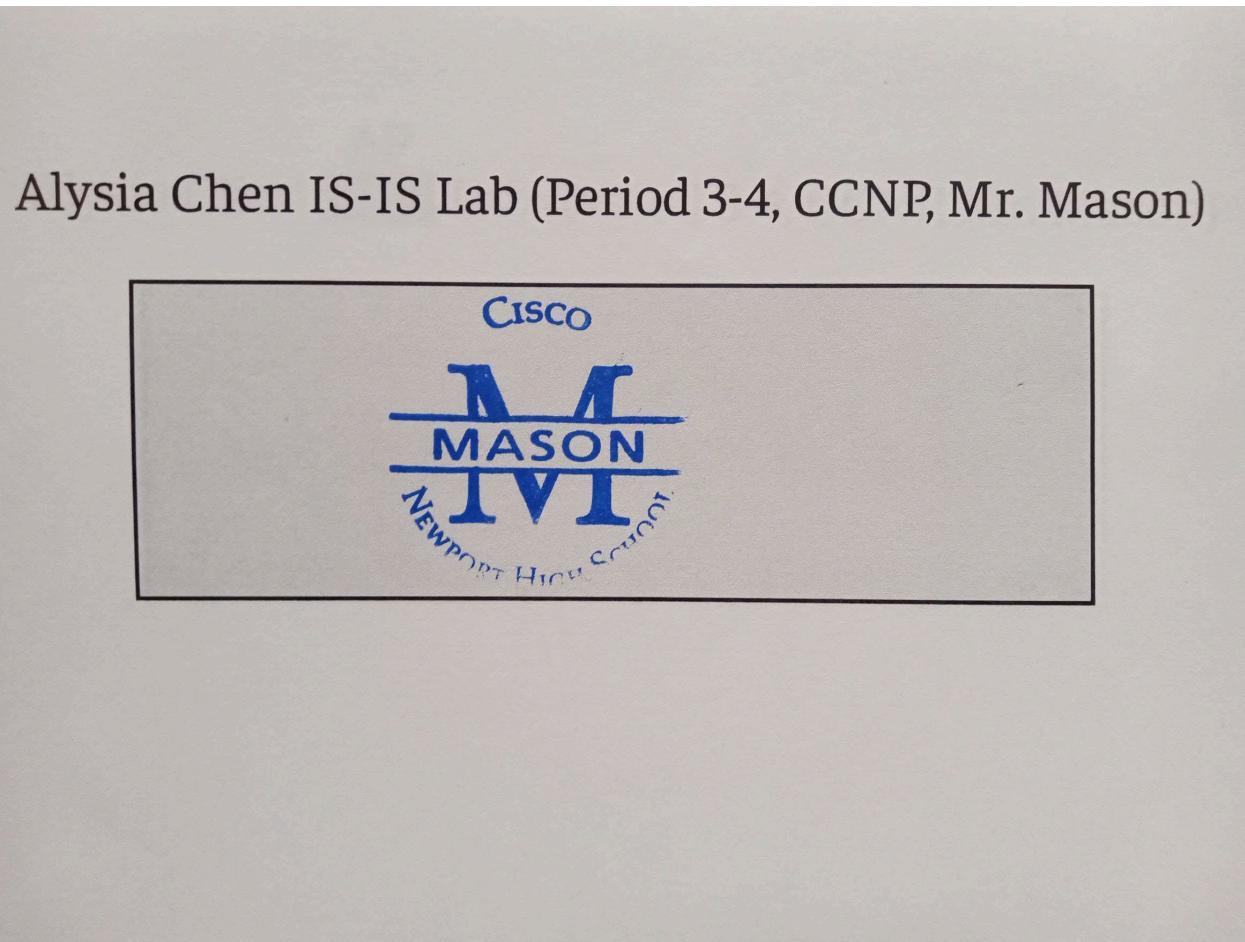
As this is my first time working alone, it was very inefficient to console into 6 routers and configure them; the same work could have been done in half the time it took for me. Additionally, I spent a significant amount of time trying to make sure the running configuration was saved properly and that I didn't accidentally save the running configuration to the startup configuration.

CONCLUSION:

This lab was fairly simple for me, but I'm especially proud I was able to complete it working solo! I hope that in CCNP I can not only learn how to work with others like I did in the past, but be able to solve problems on my own and through online resources to get good at both asking people for help and researching online for answers.

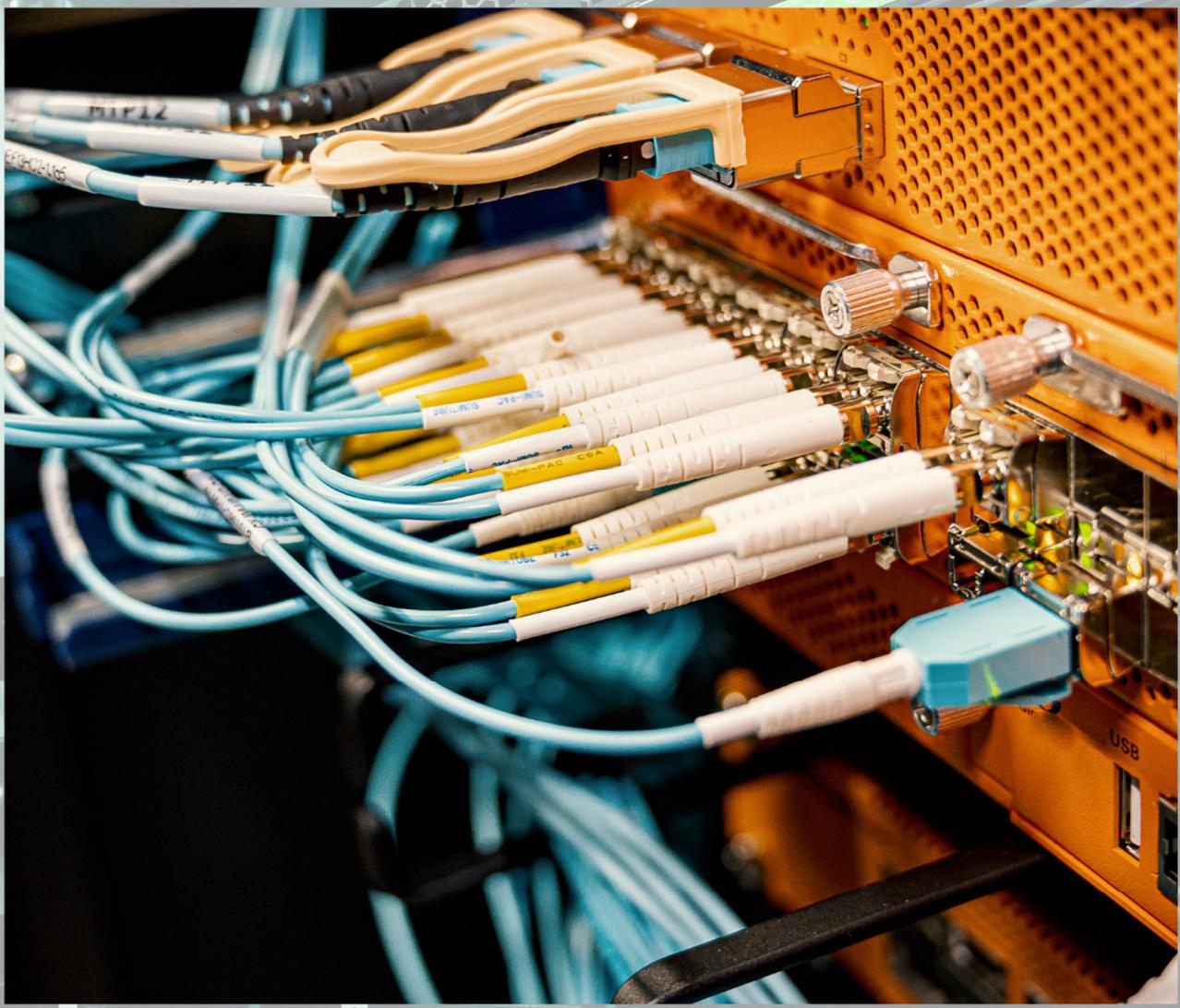


TEACHER SIGN-OFF:



Alycia Chen

Lab 8: IS-IS



PURPOSE:

Learn to configure three wireless networks using a wireless access point.

BACKGROUND INFORMATION ON LAB CONCEPTS:

An access point (AP) is a device that allows local, wireless devices to connect to the Internet by creating a wireless local area network (WLAN). It has security features and is able to support multiple devices, making it ideal for many different types of networks.

On the router, Port Address Translation (PAT), Dynamic Host Configuration Protocol, and access lists must be configured for hosts to be able to access the cloud (which is connected via a blue wire in this case).

Port Address Translation (PAT) is a specific type of Network Address Translation. Network Address Translation (NAT) is needed here because a private IP address cannot directly route to the internet unless it has a public IP address that it can “translate” to and that external networks can recognize. In other words, NAT translates a private IP address to a public IP address to route to the internet.

PAT is used in this lab because it is more scalable for our purposes than other types of NAT: it only uses one public IP address, assigning different router port numbers to each connection, and allows multiple devices through it. PAT uses both port number and IP address to translate a private IP address to the public IP address; the command *overload* for multiple devices to share the same public IP address, which distinguishes it from other subsets of Network Address Translation. This is especially important in this lab because there are three VLANs, or isolated networks, and thus three subnets of IP addresses for each, all requiring internet access through a single router.

Dynamic Host Configuration Protocol (DHCP) requires a pool of private IP addresses to be configured so that the router can automatically assign a private IP address to each device. Finally, access lists control what is permitted and what is not permitted to enter or exit a port, filtering traffic and allowing for the necessary packets of information to be transmitted.

There are many different servers being used here. The Domain Name System (DNS) server used in this particular lab can be found here: <https://developers.google.com/speed/public-dns>. DNS ensures that the domain name a user enters can be directly translated into the corresponding IP address so the user does not have to enter IP addresses to use the Internet. Another server is the DHCP server, which is just the router in this case (refer to the above explanation of DHCP). Finally, the last server is the RADIUS server, which is used for remote authentication, authorization, and accounting. In simpler terms, it is used to keep the network secure.

A trunk port carries traffic between different VLANs, while an access port carries traffic for only a single VLAN. A native trunk VLAN allows untagged traffic to be sent. Untagged traffic is traffic that does not have a VLAN tag but is assumed to be associated with the native VLAN. In this

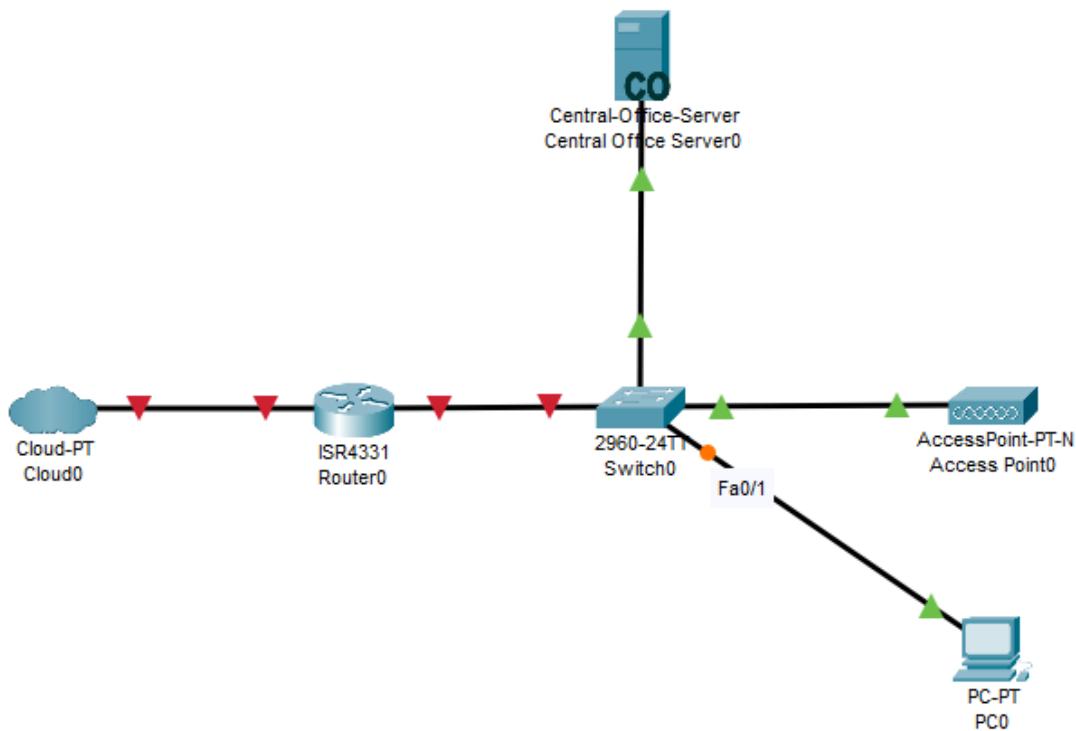


case, since there are three wireless networks, three SSIDs (which are used to identify each network) and thus three VLANs to logically separate traffic are needed.

LAB SUMMARY:

Created 3 VLANs with 3 different SSIDs: one for Guest (no password), one that is Home (pre-shared WPA2 key), and one that is WPA2 Enterprise (using Linux and RADIUS).

NETWORK DIAGRAM:



Device (Interface)	IP Address
Switch VLAN 1	192.168.0.1/24
Switch VLAN 10	192.168.10.1/24
Switch VLAN 20	192.168.20.1/24
Switch VLAN 30	192.168.30.1/24
Router G0/0/1.1	192.168.0.2/24
Router G0/0/1.10	192.168.10.2/24



Router G0/0/1.20	192.168.20.2/24
Router G0/0/1.30	192.168.30.2/24
AP BVII	192.168.0.3/24
PC0	192.168.0.4/24

LAB COMMANDS:

On the router, configure the appropriate IP addresses for each subinterface, with each subinterface corresponding to a VLAN, tagging each with the command *encapsulation dot1Q VLAN_number* and for the subinterface with the native VLAN, adding behind *VLAN_number* the keyword *native*. Make sure to create VLANs 10, 20, and 30 with the commands *vlan VLAN_number* and *name VLAN_name*.

Next, set up NAT. After determining which interface is used for connection to the internet, configure said interface to be the outside interface with the command *ip nat outside*. Configure the other interfaces with the command *ip nat inside*.

Afterwards, we will configure the access lists, permitting traffic through all of the VLANs with the commands *access-list 1 permit 192.168.0.0 0.0.0.255*, *access-list 1 permit 192.168.10.0 0.0.0.255*, *access-list 1 permit 192.168.20.0 0.0.0.255*, and *access-list 1 permit 192.168.30.0 0.0.0.255*.

The final configuration on the router involves DHCP. Enter the command *ip dhcp pool vlan[VLAN_number]* for each VLAN that is not the native VLAN. Configure the pool of DHCP addresses using the command *network [ip address] [subnet mask]*, *default-router [IP address of the router]*, and *dns-server 8.8.8.8 8.8.8.4*. Afterwards, configure the IP DHCP excluded addresses, the addresses that should not be leased out with DHCP, using the command *ip dhcp excluded-address [address 1] [address 2]*. Finally, configure the interface that is the outside interface for NAT with *ip address dhcp* to ensure it receives an address from DHCP.

There are also a few commands that the switch should be configured with. For any interfaces directly connected to a router, switch, or any other network device besides a PC, set the interface to *switchport mode trunk* and enter *switchport trunk encapsulation dot1q*. For those connected to a PC (or RADIUS server), use the command *switchport mode access* and specify which VLAN with the command *switchport access vlan VLAN_number*.



The screenshot shows the Cisco Aironet 1040 Series Access Point management interface. The top navigation bar includes links for Home, Network, Association, Wireless, Security, Services, Management, Software, and Event Log. The main content area is titled "Cisco Aironet 1040 Series Access Point". It displays the following sections:

- Hostname AP:** Shows the hostname as "ap".
- Summary Status:** Includes sections for Association (Clients: 0), Network Identity (IP Address: 192.168.0.3, MAC Address: F8E0-4C03-CAFF, FE19:90B8), and Network Interfaces (GigabitEthernet0/0: MAC Address 4463.ca19:90b, Radio 0/0.1: MAC Address 6469:89:1480, Radio 0/0.2: MAC Address 6469:89:8c10).
- Event Log:** Lists events from March 2014, such as "Full power - NEGOTIATED line power source" and "Restoring Radio Interface Dot11Radio1 due to interface reset".

Next, navigate to under Easy Setup —> Network Configuration to ensure everything is set up correctly.

Network Configuration

Host Name:	<input type="text" value="ap"/>
Server Protocol:	<input type="radio"/> DHCP <input checked="" type="radio"/> Static IP
IP Address:	<input type="text" value="192.168.0.3"/>
IP Subnet Mask:	<input type="text" value="255.255.255.0"/>
Default Gateway:	<input type="text" value="0.0.0.0"/>
IPv6 Protocol:	<input checked="" type="checkbox"/> DHCP <input checked="" type="checkbox"/> Autoconfig <input type="checkbox"/> Static IP
IPv6 Address:	<input type="text" value=""/> (X:X:X:X::X/<0-128>)
Create a user	
Username:	<input type="text"/>
Password:	<input type="text"/>
Change global authentication password	
default enable secret:	<input type="text" value="*****"/>
confirm enable secret:	<input type="text"/>
SNMP Community:	<input type="text" value="defaultCommunity"/>
<input checked="" type="radio"/> Read-Only <input type="radio"/> Read-Write	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Under Radio Configuration, configure the following and ensure that Universal Admin Mode is disabled because that is used for a lightweight access point whereas in this lab we use an autonomous access point.



Radio 5GHz

SSID :	<input type="text" value="Guest"/>
	<input checked="" type="checkbox"/> Broadcast SSID in Beacon
VLAN :	<input type="radio"/> No VLAN <input checked="" type="radio"/> Enable VLAN ID: <input type="text" value="10"/> (1-4094) <input type="checkbox"/> Native VLAN
Universal Admin Mode:	<input type="button" value="Disable"/>
Security :	<input type="button" value="No Security"/>
Role in Radio Network :	<input type="button" value="Access Point"/>
Optimize Radio Network :	<input type="button" value="Default"/>
Aironet Extensions:	<input type="button" value="Enable"/>
Channel:	<input type="button" value="Dynamic Frequency Selection"/>
Power:	<input type="button" value="Maximum"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Under Services, make sure that the Radiol-802.11N^{5GHz} box is checked.



Under the Security tab, navigate to SSID Manager and verify that the previously configured SSID is present and select that SSID.



Turn on BSSID for the 5GHz option and hit apply. Repeat using 5GHz and create the SSIDs for Home and Enterprise.



Guest Mode/Infrastructure SSID Settings

Radio0-802.11N2.4GHz:

Set Beacon Mode: Single BSSID Set Single Guest Mode SSID: <NONE>

Multiple BSSID

Set Infrastructure SSID: <NONE> Force Infrastructure Devices to associate only to this SSID

Radio1-802.11N5GHz:

Set Beacon Mode: Single BSSID Set Single Guest Mode SSID: Guest

Multiple BSSID

Set Infrastructure SSID: <NONE> Force Infrastructure Devices to associate only to this SSID

Next, we will configure the RADIUS server for authentication on the Enterprise network. First, download Oracle VirtualBox and radiusdesk-2017-0-3 ova files, completing set up. Open up the RADIUSdesk file in VirtualBox and login using the password *admin* and username *system*.

```
system@RADIUSdesk-2017-0-3:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:b3:75:b3
          inet6 addr: fe80::a00:27ff:feb3:75b3/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:20 errors:0 dropped:0 overruns:0 frame:0
              TX packets:54 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:6090 (6.0 KB) TX bytes:16380 (16.3 KB)

eth1      Link encap:Ethernet HWaddr 08:00:27:24:81:ea
          inet6 addr: fe80::a00:27ff:fe24:81ea/64 Scope:Link
              UP BROADCAST RUNNING PROMISC MULTICAST MTU:1500 Metric:1
              RX packets:32926 errors:0 dropped:0 overruns:0 frame:0
              TX packets:4908 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:31594810 (31.5 MB) TX bytes:343638 (343.6 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
              UP LOOPBACK RUNNING MTU:65536 Metric:1
              RX packets:3380 errors:0 dropped:0 overruns:0 frame:0
              TX packets:3380 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1
              RX bytes:250645 (250.6 KB) TX bytes:250645 (250.6 KB)

tun0     Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.1.0.1 P-t-P:10.1.0.1 Mask:255.255.0.0
              UP POINTOPOINT RUNNING MTU:1500 Metric:1
              RX packets:0 errors:0 dropped:0 overruns:0 frame:0
              TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:100
              RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
```



After typing `ifconfig`, find the eth0 IP address and type it into a web browser to access the graphical user interface of the RADIUS Server. The password for the graphical user interface is *admin*, and the username is *root*.

The screenshot shows the RADIUSdesk interface. On the left, there's a sidebar with icons for Data Usage, Utilities, Realm (set to MESHdesk), and time filters (Today, This Week, This Month). The main area has a large grey box labeled "MESHdesk" with "0 kb" and "In: 0 kb Out: 0 kb". Below it is a "See More..." button. To the right, there are two sections: "Top 10 Users Today" (empty) and "Active Sessions" (also empty).

Under Action, click add, selecting admin_college:

The screenshot shows the "Dynamic RADIUS Clients" section. It has tabs for Home, Document, and Nas. The table below lists two clients:

	IP Address	Name	NAS-Identifier	Available to sub-providers	Realms	Status	Notes
1	192.168.30.2	Router		No	Available to all!	Unknown	
2	127.0.0.1	localhost	localhost	No	Available to all!	Unknown	

Next, navigate to NAS Devices and click add, selecting admin_college and entering in the router IP address to add the router.



The screenshot shows the RADIUSdesk software interface. At the top, there is a navigation bar with tabs: Dynamic RADIUS Clients, NAS Devices, NAS Device Tags, and SSIDs. Below the navigation bar is a toolbar with icons for Home, Action, Document, and Nas, along with buttons for search, add, edit, and delete.

The main area is a table listing two NAS devices:

	IP Address	Name	NAS-Identifier	Available to sub-providers	Realms	Status	Notes
1	192.168.30.2	Router		No	Available to all!	Unknown	
2	127.0.0.1	localhost	localhost	No	Available to all!	Unknown	

At the bottom of the table, there is a pagination control with the text "Displaying 1 - 2 of 2".

Afterwards, set the RADIUS server in the graphical interface of the access point.



Verify that the Enterprise network is able to use the RADIUS server with the correct user credentials to function properly, and that devices are able to connect to all three networks.

CONFIGURATIONS:

Note that certain output has been removed for clarity and relevance.

Hostname AP:

```
dot11 ssid Enterprise 2.0
vlan 30
authentication open eap eap_methods
authentication network-eap eap_methods
authentication key-management wpa version 2
mbssid guest-mode
no ids mfp client
```

```
dot11 ssid Guest
```



```
vlan 10
authentication open
guest-mode
mbssid guest-mode

dot11 ssid Home
    vlan 20
    authentication open
    authentication key-management wpa version 2
    mbssid guest-mode
    wpa-psk ascii 7 0822455D0A165445415A5E57

no ipv6 cef

username Cisco password 7 032752180500701E1D
username admin password 7 01300F175804575D72

bridge irb
interface Dot11Radio0
    no ip address
    encryption vlan 20 mode ciphers aes-ccm
    ssid Guest
    antenna gain 0
    speed basic-1.0 basic-2.0 basic-5.5 basic-11.0 6.0 9.0 12.0
    18.0 24.0 36.0 48.0 54.0 m0. m1. m2. m3. m4. m5. m6. m7. m8. m9.
    m10. m11. m12. m13. m14. m15.
    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 Dot11Radio0.101
    encapsulation dot1Q 10
    bridge-group 10
    bridge-group 10 subscriber-loop-control
    bridge-group 10 spanning-disabled
    bridge-group 10 block-unknown-source
    no bridge-group 10 source-learning
    no bridge-group 10 unicast-flooding

interface Dot11Radio1
    no ip address
!
    encryption vlan 20 mode ciphers aes-ccm
```



```
!
encryption vlan 30 mode ciphers aes-ccm
!
ssid Enterprise 2.0
!
ssid Home
!
antenna gain 0
peakdetect
dfs band 3 block
mbssid
channel dfs
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 Dot11Radio1.20
encapsulation dot1Q 20
bridge-group 20
bridge-group 20 subscriber-loop-control
bridge-group 20 spanning-disabled
bridge-group 20 block-unknown-source
no bridge-group 20 source-learning
no bridge-group 20 unicast-flooding

interface Dot11Radio1.101
encapsulation dot1Q 10
bridge-group 254
bridge-group 254 subscriber-loop-control
bridge-group 254 spanning-disabled
bridge-group 254 block-unknown-source
no bridge-group 254 source-learning
no bridge-group 254 unicast-flooding

interface Dot11Radio1.301
encapsulation dot1Q 30
bridge-group 30
bridge-group 30 subscriber-loop-control
bridge-group 30 spanning-disabled
bridge-group 30 block-unknown-source
no bridge-group 30 source-learning
no bridge-group 30 unicast-flooding
```



```
interface GigabitEthernet0
  no ip address
  duplex auto
  speed auto
  bridge-group 1
  bridge-group 1 spanning-disabled
  no bridge-group 1 source-learning

interface GigabitEthernet0.10
  encapsulation dot1Q 10
  bridge-group 10
  bridge-group 10 spanning-disabled
  no bridge-group 10 source-learning

interface GigabitEthernet0.20
  encapsulation dot1Q 20
  bridge-group 20
  bridge-group 20 spanning-disabled
  no bridge-group 20 source-learning

interface GigabitEthernet0.30
  encapsulation dot1Q 30
  bridge-group 30
  bridge-group 30 spanning-disabled
  no bridge-group 30 source-learning

interface BVI1
  mac-address 44d3.ca03.7dce
  ip address 192.168.0.3 255.255.255.0
  ipv6 address dhcp
  ipv6 address autoconfig
  ipv6 enable

  ip default-gateway 192.168.0.2
  ip forward-protocol nd
  ip http server
  no ip http secure-server
  ip http help-
  path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
  ip radius source-interface BVI1

  radius-server local
    nas 192.168.0.99 key 7 13261E010803557878
    user admin ntlhash 7
0322092E515776681D5E4F2635345D28520E0F777E6365734055335A2204080D
77
```



```
radius-server attribute 32 include-in-access-req format %h  
radius server freeradius  
address ipv4 192.168.0.99 auth-port 1812 acct-port 1813  
key 7 13261E010803557878
```

Hostname AP_Router:

```
ip dhcp excluded-address 192.168.20.1 192.168.20.3  
ip dhcp excluded-address 192.168.10.1 192.168.10.3  
ip dhcp excluded-address 192.168.30.1 192.168.30.4  
  
ip dhcp pool vlan10  
network 192.168.10.0 255.255.255.0  
default-router 192.168.0.2  
dns-server 8.8.8.8 8.8.8.4  
  
ip dhcp pool vlan20  
network 192.168.20.0 255.255.255.0  
default-router 192.168.0.2  
dns-server 8.8.8.8 8.8.8.4  
  
ip dhcp pool vlan30  
network 192.168.30.0 255.255.255.0  
default-router 192.168.0.2  
dns-server 8.8.8.8 8.8.8.4  
  
vlan 10  
name Guest  
  
vlan 20  
name Home  
  
vlan 30  
name Enterprise  
  
interface GigabitEthernet0/0/0  
ip address dhcp  
ip nat outside  
negotiation auto  
  
interface GigabitEthernet0/0/1  
no ip address  
ip nat inside  
negotiation auto
```



```
interface GigabitEthernet0/0/1.1
  encapsulation dot1Q 1 native
  ip address 192.168.0.2 255.255.255.0
  ip nat inside

interface GigabitEthernet0/0/1.10
  encapsulation dot1Q 10
  ip address 192.168.10.2 255.255.255.0
  ip nat inside

interface GigabitEthernet0/0/1.20
  encapsulation dot1Q 20
  ip address 192.168.20.2 255.255.255.0
  ip nat inside

interface GigabitEthernet0/0/1.30
  encapsulation dot1Q 30
  ip address 192.168.30.2 255.255.255.0
  ip nat inside

ip nat inside source list 1 interface GigabitEthernet0/0/0
overload
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0

access-list 1 permit 192.168.0.0 0.0.0.255
access-list 1 permit 192.168.10.0 0.0.0.255
access-list 1 permit 192.168.20.0 0.0.0.255
access-list 1 permit 192.168.30.0 0.0.0.255
```

Hostname Switch:

```
interface FastEthernet0/1
  switchport trunk encapsulation dot1q
  switchport mode trunk

interface FastEthernet0/2
  switchport trunk encapsulation dot1q
  switchport mode trunk

interface FastEthernet0/3
  switchport access vlan 30
  switchport trunk encapsulation dot1q
```



```
switchport mode trunk

interface Vlan1
 ip address 192.168.0.1 255.255.255.0

interface Vlan10
 no ip address

interface Vlan20
 no ip address

interface Vlan30
 no ip address
```

PROBLEMS:

I had many problems throughout this lab. For example, although my Home Wi-Fi was able to work properly, the Guest Wi-Fi had a password, even though I did not configure a password. I ended up being able to fix this through going into the AP graphical user interface and selecting the Security section, finally navigating to Encryption Manager to turn off encryption on VLAN 10. However, once I tried connecting to the now-open network, there was no internet. After going into the command-line interface of the AP, I realized that interface dot11radio1.101, which is the subinterface used for guest, had a bridge group of 254 rather than 10. Upon changing that, I was able to get internet connection on the Guest Wi-Fi.

Unfortunately, I was unable to finish my lab. This was due to the multitude of problems I encountered while configuring my last Wi-Fi, the Enterprise one, which used a RADIUS server and required the server for authentication. Whenever I tried logging into the Wi-Fi, I received the message “Can’t connect to this network”.

Referring to the command-line interface of my AP, I see that the AP reads that the “authentication failed,” even though the username and password is the same as the one on the RADIUS server. Additionally, there are no firewalls blocking the port; the routing works because I am able to ping from my AP to the RADIUS server and the VLAN is correct because the configuration is very similar to the Guest and Home ones, which both work.

Additionally, I had tried using radtest to see if it is a problem with the RADIUS server not being able to run properly or having the wrong credentials configured, but the radtest was able to work for multiple user credentials. I also utilized the error logs. The error logs used to not show anything, but after restarting the RADIUS server, I was able to receive messages citing a connectivity issue.

After consulting with many online resources, my classmates, and my teacher, I was still unable to figure out the problem with my Enterprise network. However, I do believe the process of troubleshooting was highly valuable, and I do not regret trying my best in this lab.

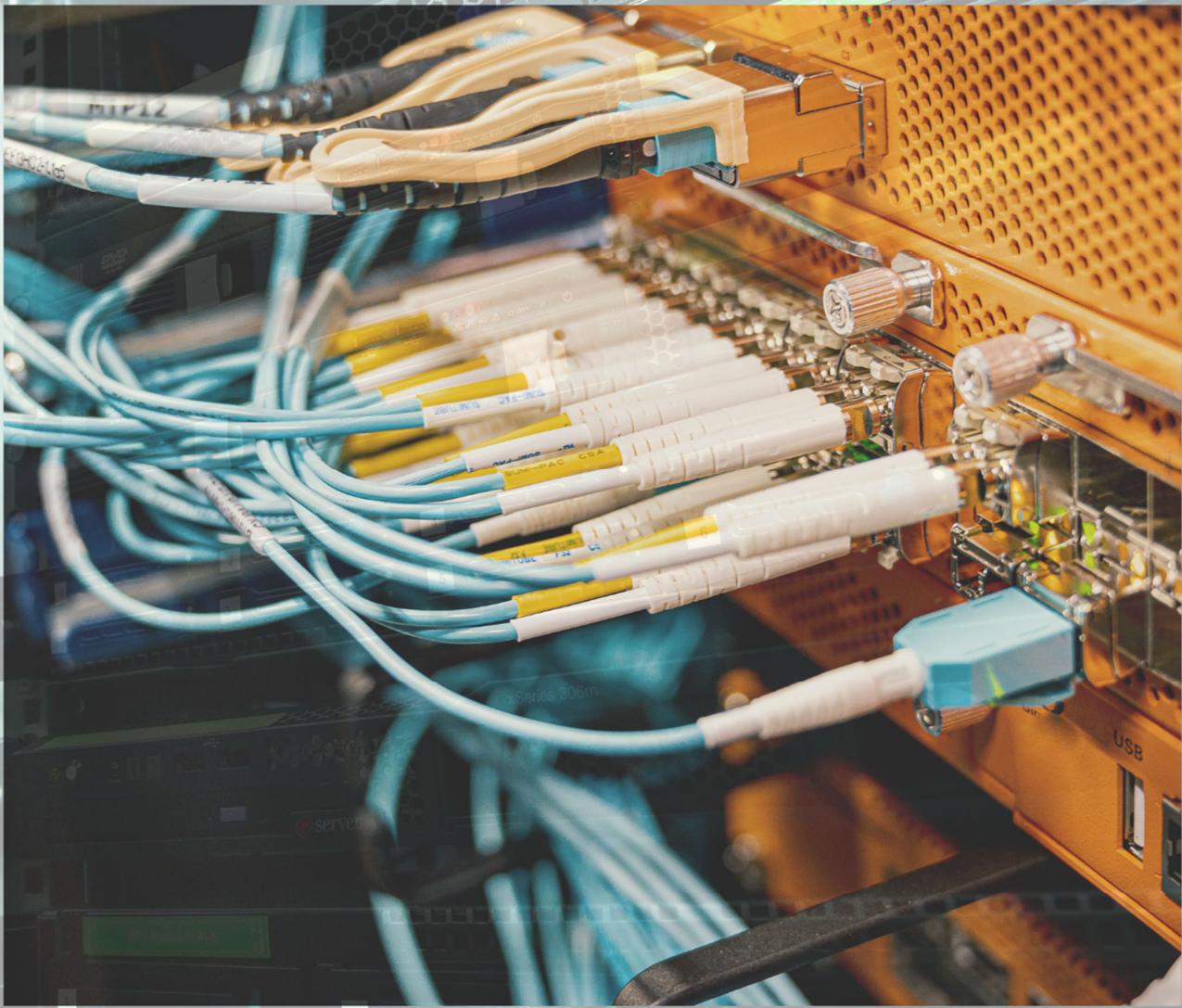


CONCLUSION:

This lab was by far the most complex. Although I worked on it by my own, I had to ask for others' help multiple times due to the variety of troubleshooting methods I had to employ in order for me to get this far. Although I was not able to finish this lab, I believe that the valuable skills I obtained in communication, resilience, and practice with troubleshooting will allow me to advance my career in this field.



Lab 9: Layer 2 Attacks and Mitigations



PURPOSE:

Learn to mitigate three different types of attacks on networks.

BACKGROUND INFORMATION ON LAB CONCEPTS:

In networking, attacks are something network administrators have to take into account for when configuring a network. However, attacks not only come from external sources, but may also be coming from inside the network. In this lab, we will be using three different types of attacks, all of them occurring inside the local network: DHCP Starvation, ARP Spoofing, and MAC Flooding.

DHCP stands for Dynamic Host Configuration Protocol. It gives IP addresses to devices on a network through a server, which in this lab is a router leasing out addresses. Each time a device connects, it will ask the DHCP server for an IP address, and the DHCP server will provide one until all available IP addresses are used up. In a DHCP starvation attack, an attacker sends many fake requests to the DHCP server to lease out all the IP addresses of the server. Once the server runs out of addresses, devices within the network that actually need IP addresses cannot connect to the network, and thus users cannot connect to the internet or internal systems. Work will be significantly delayed due to this, and additionally, attackers may introduce a new, fake DHCP server to redirect or intercept user traffic, having complete control and access over the data.

ARP stands for Address Resolution Protocol. It helps devices find each other on the network using MAC addresses. For example, if a device wants to send data to IP 192.168.1.1, it sends an ARP request asking, “Who has 192.168.1.1?” The device with that IP replies with its MAC address, and the requesting device stores this information in its ARP cache and sends data to that MAC address. In ARP spoofing, an attacker sends fake ARP replies, falsely claiming that it has the requested MAC address. The victim updates its ARP cache with the attacker’s MAC address, so when the victim then tries to send data to that IP address, the data is sent to the attacker’s MAC address instead of the intended address.

Lastly, MAC flooding involves MAC addresses, which are unique IDs assigned to network devices. Switches have a table of these addresses to be able to “switch” properly, or direct network traffic to the correct device. In a MAC flooding attack, an attacker sends lots of fake MAC addresses to the switch to overload the switch’s memory. When this happens, the switch is unable to distinguish between devices and as a result, sends traffic to all devices on the network.

Thus, it is important to defend against any internal network security threats. Attacks from inside the network can potentially see confidential data, change data, or entirely prevent data from reaching the intended address. Lastly, note that although DHCP starvation, ARP snooping, and MAC flooding are common attacks, they are not all of the possible attacks that may act on a network.

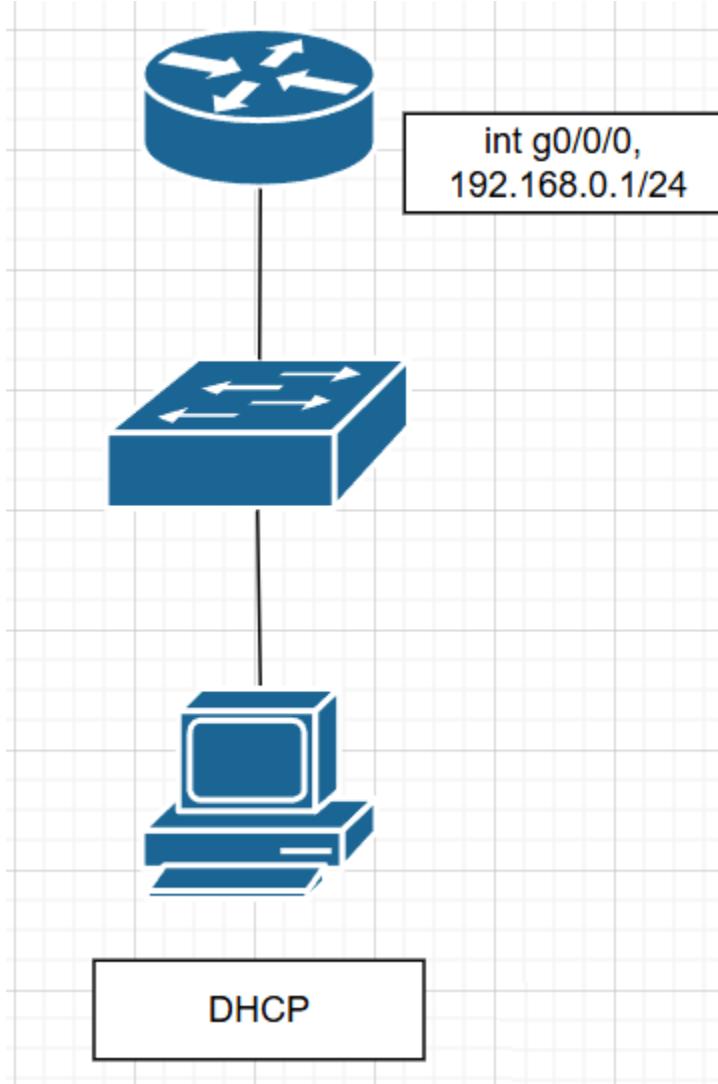


LAB SUMMARY:

Attacked a simple router-on-a-stick network through three methods: DHCP starvation, ARP snooping, and MAC flooding. Proceeded to mitigate all three attacks.

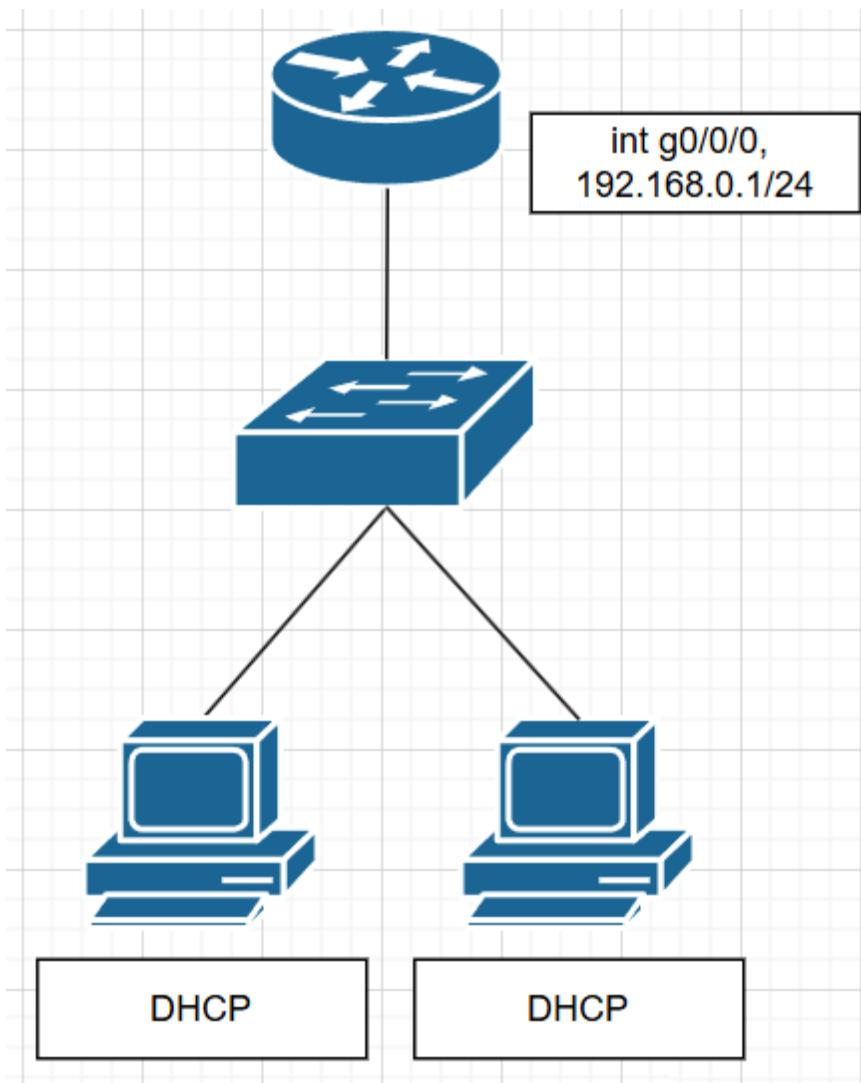
NETWORK DIAGRAMS:

For DHCP starvation and MAC flooding:



For ARP snooping:





LAB COMMANDS:

Configure DHCP with the following commands on the router in global configuration mode. Enter the command `ip dhcp pool vlan[VLAN_number]` for each VLAN that is not the native VLAN. Configure the pool of DHCP addresses using the command `network [ip address] [subnet mask]`, `default-router [IP address of the router]`, and `dns-server 8.8.8.8 8.8.8.4`. Afterwards, configure the IP DHCP excluded addresses, the addresses that should not be leased out with DHCP, using the command `ip dhcp excluded-address [address 1] [address 2]`.

Set up a virtual machine on a computer and go into its terminal. Use the `sudo yersinia -G` command to open up a software to run attacks on the network. Make sure the computer has an Ethernet connection to the switch and thus is in the same network as the router and host. Then, find the attack function and select DHCP, then check the box next to DHCP discover before running the attack.



Verify that on the PC, which should be set with an IP address obtained through DHCP, is not able to obtain an IP address anymore after the attack. See below:

IP address	Client-ID/ Hardware address/ User name	Lease expiration	Type	State	Interface
Bindings from all pools not associated with VRF:					
192.168.0.6	0104.d9c8.ba25.74	Jun 14 2025 05:12 PM	Automatic	Active	GigabitEthernet0/0/0
192.168.0.7	0148.2ae3.8eee.3f	Jun 14 2025 05:15 PM	Automatic	Active	GigabitEthernet0/0/0
192.168.0.8	76df.4a38.1e54	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.9	08e1.b642.b67d	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.10	709d.af4a.6a0d	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.11	8a80.8079.13c8	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.12	76e1.0700.3695	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.13	50db.ad29.b5d0	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.14	e216.535a.e61e	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.15	6838.421a.83cd	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.16	e66f.364e.6bfa	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.17	70a6.373c.386f	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.18	7a30.7b37.6706	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.19	c821.264b.15d0	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.20	b01f.7978.830e	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.21	ca4b.487a.b728	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.22	92c8.a90c.47b7	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.23	46ec.0c36.3921	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.24	be73.a03b.f8d1	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.25	867f.d919.fb9d	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.26	16e2.2137.077c	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.27	8459.af33.2e81	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.28	7ce0.c770.3f16	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.29	86e9.ad07.3c71	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.30	caaf.a530.dib8	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.31	b266.7132.3ae5	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.32	86e6.0558.76bb	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.33	827d.f108.ea6d	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.34	320f.460b.ceaa	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.35	da03.0531.44a5	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.36	82e4.0d0b.4760	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.37	b6fc.0c2c.e6b5	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.38	bae2.6944.3d5c	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.39	649c.595f.ec47	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.40	1ad7.2528.2d09	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.41	304e.cb61.e5dd	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.42	de78.387f.63a6	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.43	1e8a.8340.a53c	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.44	eacb.b20a.bf9f	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.45	76d5.7a0f.fd6f	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.46	7a4f.ea53.d3df	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.47	b8b2.a246.d02b	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.48	767b.f817.2922	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.49	88b3.4370.50a7	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.50	a087.3d5d.6d6e	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.51	2419.1464.88d7	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.52	3e78.ba6b.3edd	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.53	44b8.e903.b39e	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.54	9ebc.647c.bfe7	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.55	760d.384b.f39d	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.56	bab5.257d.a025	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.57	feac.7329.c8e3	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.58	d68c.e951.15af	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.59	6c4d.ef07.b454	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.60	deel.fa37.cd4f	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.61	d0e1.d564.8bb6	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0
192.168.0.62	22f6.975d.f625	Jun 13 2025 05:18 PM	Automatic	Selecting	GigabitEthernet0/0/0

Then, to mitigate, enter the following commands on the switch. *int range f0/1-24* to access all of the FastEthernet interfaces of the switch; *switchport* and *switchport mode access* in case any interface is not able to connect to end devices because it's in trunking mode; *switchport port-security* and *switchport port-security max 1* to actually secure the switchports and make sure unwanted traffic is never allowed.



Next, we run an ARP attack. First, connect a second host to the switch, as shown in the second network diagram. Configure the second host's IP address to be obtained by DHCP as well. Then, run in the terminal of the attacker's computer `sudo arpspoof -I enp3s0 -t [default gateway] [host_IP]`. Then, wait a few seconds before pinging from the host computer to the default gateway (IP address of the router). On the terminal of the attacker's computer, run the command `sudo wireshark` to open Wireshark and capture ICMP packets.

To mitigate the ARP attack, run the below commands:

```
ip dhcp snoop vlan 1-10
no ip dhcp snoop info opt
ip dhcp snoop

ip arp inspect vlan 1-10
ip arp inspec vali ip
ip arp gratui none

int range f0/1-23
ip arp inspection trust
ip dhcp snooping trust

int f0/24
ip arp inspection limit none
no ip dhcp snooping trust
```

Note that interface f0/24 is the one connected to the attacker's laptop.

After mitigation, ping from the host computer to the router again, making sure that there are no ICMP packets appearing on Wireshark, meaning that the attacker is unable to intercept packets.

Finally, we simulate a MAC flooding attack. Disconnect the second host from the switch—there is no need for it for this segment—and run the command `sudo macof -1 enp3s0` on the attacker's computer. Run the following command on the switch to show the MAC address table: `show mac address-table`. There should be thousands of MAC addresses on the table. Then, run the command `clear mac address-table dynamic` and proceed with the mitigation.

The commands are same as the ones used for DHCP starvation mitigation: `int range f0/1-24` to access all of the FastEthernet interfaces of the switch; `switchport` and `switchport mode access` in case any interface is not able to connect to end devices because it's in trunking mode; `switchport port-security` and `switchport port-security max 1` to actually secure the switchports and make sure unwanted traffic is never allowed.

When viewing the MAC address table once more, there should be less than 10 addresses leased out, significantly less than before, the rest having been blocked by port security.

CONFIGURATIONS:



Note that certain output has been removed for clarity and relevance.

Hostname R1—show running configuration:

```
ip dhcp excluded-address 192.168.0.1 192.168.0.5  
  
ip dhcp pool 1  
network 192.168.0.0 255.255.255.0  
default-router 192.168.0.1  
dns-server 8.8.8.8  
  
interface GigabitEthernet0/0/0  
ip address 192.168.0.1 255.255.255.0  
negotiation auto
```

No configuration was done on the switch, except during mitigation of each attack.

PROBLEMS:

I had a few problems getting the MAC flooding attack to work because the switch had built-in security protocols that protected it from such an attack. I included troubleshooting methods like waiting longer before stopping the attack to see if the MAC address would be more flooded and unplugging the port connected to the host to see if the host's MAC address would be unable to be seen in the address table. However, after running the command *sudo macof -l enp3s0* instead of simply *sudo macof*, the attack worked right away.

CONCLUSION:

This was a fairly simple lab. The commands were not too complicated and there was not a lot of problems I encountered. However, I'm still proud of myself for finishing the lab very efficiently while still having a complete understanding of how attacks work and more importantly, how to mitigate them.



TEACHER SIGN-OFF

Alysia Chen Attack Lab (Period 3-4, CCNP, Mr. Mason)

DHCP
starvation

ARP
spooing

MAC
flooding



Alysia Chen