CCA 625 Project 1: Simulating a Network Using Mininet and Analyzing Packets Using Wireshark

In this lab exercise, you will perform the following steps:

1. Log in to AWS Academy and go to the AWS console.
2. Provision an AWS EC2 instance using provided Amazon Machine Image (AMI).
3. Make the instance available for remote desktop access and connect to it.
4. Run the Mininet simulator, ping one simulated Mininet host from another simulated host, and capture the packets using the Wireshark packet analyzer. Inspect the packets.

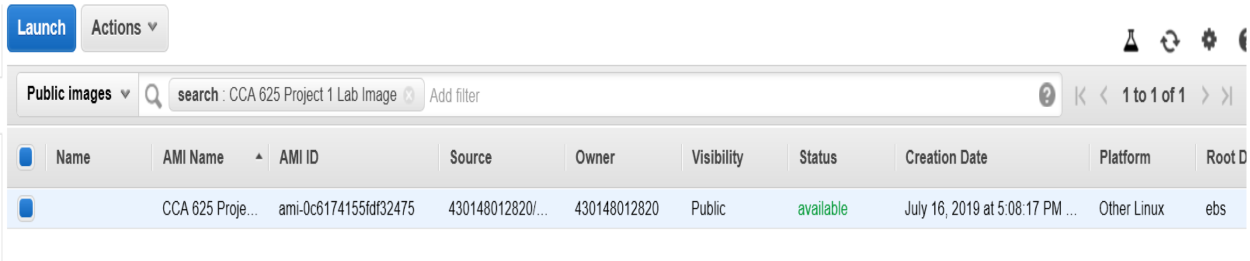
You will write a lab report describing the steps you've taken, include required screenshots, and provide answers to questions.

Step 1: Log In to Your AWS Academy Classroom

- Go to AWS Academy
- You will be rostered into the AWS Academy course before the start of the course.
- Review the AWS Academy Learner Labs Student Guide before you start

Step 2: Provision an AWS EC2 Instance Using a Preconfigured Amazon Machine Image (AMI)

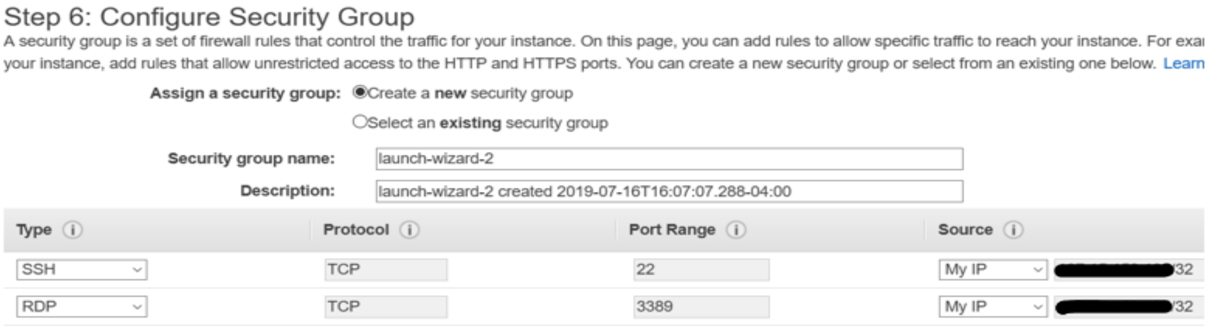
1. Make sure that you are in the "US East (N. Virginia)" region (check in the top right corner).
2. In the AWS Management Console, click on "EC2" under "Compute."
3. The EC2 dashboard will open. Click on "AMIs" under "IMAGES" on the left panel.
4. Select "Public Images" in the drop-down menu called "Owned by me." In the search box next to it, type "CCA 625 Project 1 Lab Image" and hit Enter. It should find the image with the image ID of "ami-0c6174155fdf32475" and the description of "ubuntu lxde xrdp wireshark mininet". (Those attributes can be also used as search criteria). **Take a screenshot of the whole screen and include it in your lab report.** Select it and click the "Launch" button.



	Name	AMI Name	AMI ID	Source	Owner	Visibility	Status	Creation Date	Platform	Root D
●		CCA 625 Proje...	ami-0c6174155fdf32475	430148012820/...	430148012820	Public	available	July 16, 2019 at 5:08:17 PM ...	Other Linux	ebs

Source: Amazon Web Services.

5. In "Step 2 – Select the Instance Type," accept the preselected "T2.micro" type, which is free-tier eligible.
6. On top of the screen, click on "6. Configure Security Group." Security groups act as firewalls, defining which ports are open for which protocols on AMI instances. They also define allowed IP addresses or their ranges for machines that can communicate through these ports. On the "Step 6: Configure Security Group" screen, you will see that under "Assign a Security Group" heading, the option "Create a new security group" is preselected. Keep it.
7. Look at the list of allowed protocols and ports. It will have the one rule for the SSH protocol, which allows you to connect to instance command line interfaces. Click on the "Add Rule" button. In the Type column, scroll down to RDP and select it. Add rule with port 3389 – default port for the remote desktop connections, which we will use to access the instance.
   By default, the rule for SSH specifies the source for connections as "Custom 0.0.0.0/0," which means that any IP address can try to connect to instances in this security group. It is recommended that in the Source column, select "My IP" in the drop-down list. It should enter your public IPv4 address in the address box, in the form of the/32 CIDR. Note: This will prevent a connection to this EC2 instance from any other computer than the one you are currently using. If you plan to continue this lab from another computer in another network (for example your work computer), you need to either enter the public IP address of your other computer, or you need to keep the source as "Custom 0.0.0.0/0." Click on the "Review and Launch" button.



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For exa your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn

Assign a security group: ● Create a **new** security group
○ Select an **existing** security group

Security group name: launch-wizard-2

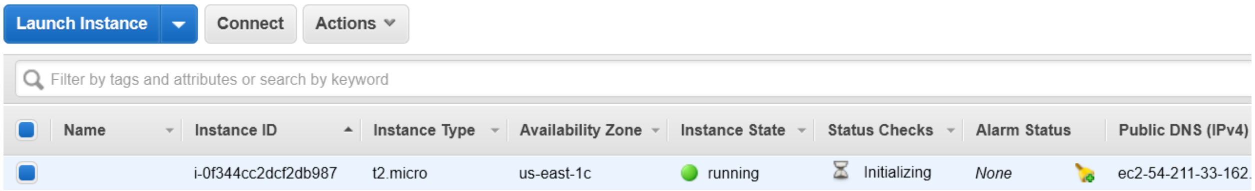
Description: launch-wizard-2 created 2019-07-16T16:07:07.288-04:00

Type	Protocol	Port Range	Source	
SSH	TCP	22	My IP	[redacted]32
RDP	TCP	3389	My IP	[redacted]32

Source: Amazon Web Services.

8. On "Step 7: Review Instance Launch" screen, review the instance's detail. **Take a screenshot of the whole instance detail screen and include it in your lab report.** Click on "Launch."

9. The "Select an existing key pair or create a new key pair" window pops up. If you have an existing key pair in your AWS account, select it in the second drop-down, but make sure you still have access to the private key pair. If this is the first time you are launching an EC2 instance, you likely don't have an existing key pair. If so, select "Create a new key pair" in the first drop-down, give it the name "CCA625P1-key," and click the "Download Key Pair" button. Save the .pem file in a convenient location—you will need it to connect to the instance. Do not lose this file.
10. Click the "Launch Instances" button. Your instance will start provisioning. Go to "Services," then "EC2," to see the EC2 dashboard and click on "Running Instances." You will see your instance being provisioned.
11. Once the instance is in the running state (green ball) and you see a green checkmark under "Status Checks," take note of its Public DNS name (in the Public DNS (IPv4) column or from the instance detail at the bottom of the screen). Then, make sure that the instance is selected and click on the Connect button on top.



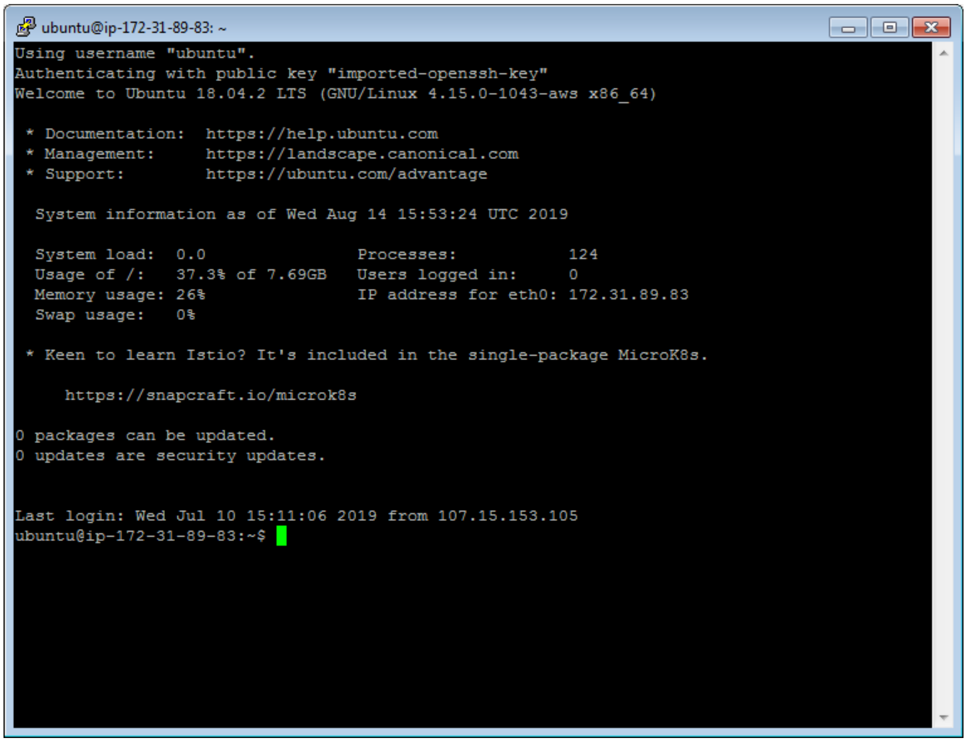
☐	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)
☐		i-0f344cc2dcf2db987	t2.micro	us-east-1c	● running	Initializing	None	ec2-54-211-33-162.

Source: Amazon Web Services.

Take a screenshot of the running instances list screen and include it in your lab report.

Step 3: Make the Instance Available for Remote Desktop Access and Connect to It

12. Following directions in the "Connect to Your Instance" pop-up window, connect to the instance using a standalone SSH client. The simplest way to do it is to invoke the ssh command as per the example in the pop-up. If you are using Windows 10, you will do this in the PowerShell command window, or if you are using a Mac, you will do this in a terminal window.
    You will need to replace the user name of root in the command (before the @ sign) with "ubuntu" – it is the default AWS user name on Ubuntu EC2 instances, which has sudo (superuser) privileges. On your computer, make sure that you are in a directory in which your private key (the .pem file) is saved. Select "Yes" to the host authenticity warning.
    If you are using any other earlier version of Windows (pre-Windows 10), you have to use PuTTY [https://www.putty.org/]. There are extra steps that you must take before you can use PuTTY. First, you must convert the .pem private key that you have downloaded into a format that PuTTY can understand. You will use the PuTTYgen program to convert this file to .ppk format. You then need to import the .ppk file into your PuTTY program before you can connect to the EC2 instance. Use the PuTTY connection instructions [https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html] for detailed steps on using PuTTY to connect to the EC2 instance. Make sure you add "ubuntu@" in front of the host name (public DNS name that you noted from step 12 above) and import the converted private key if you are using PuTTY. Once connected, you will see a black screen with the command prompt on it.

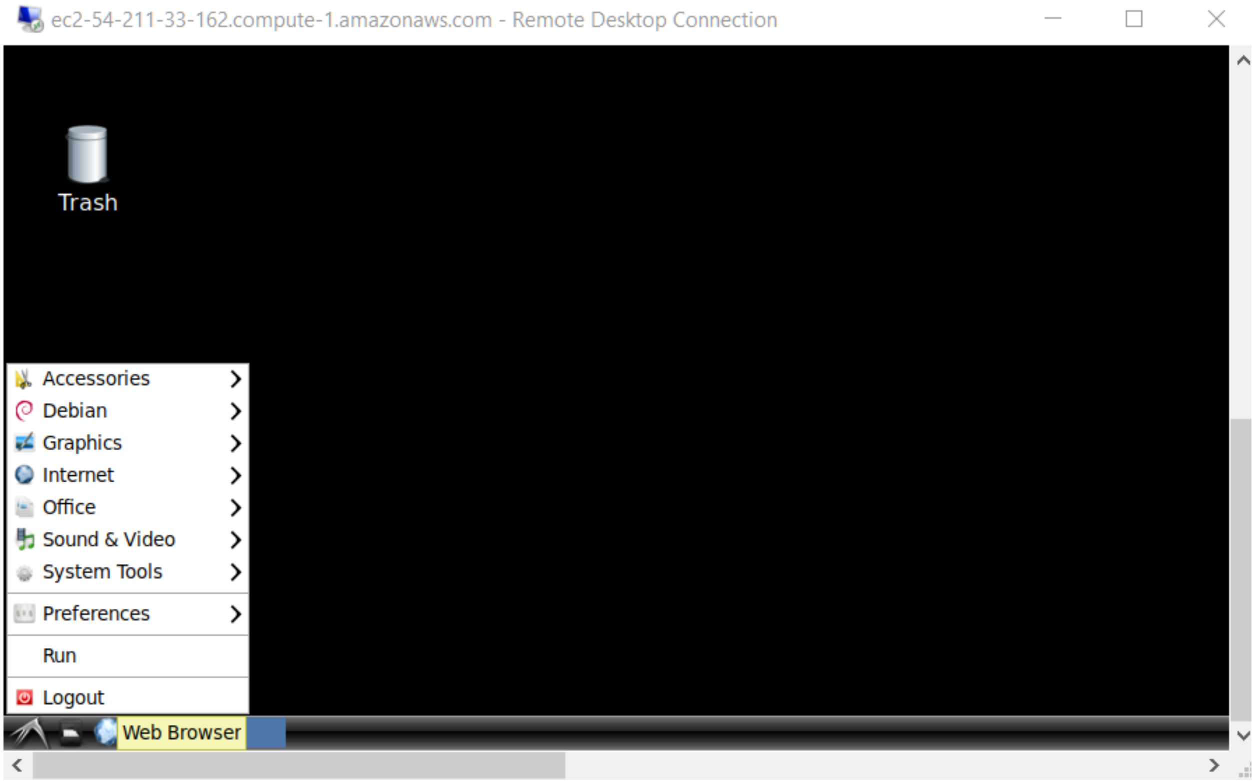


```
Using username "ubuntu".
Authenticating with public key "imported-openssh-key"
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-1043-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Aug 14 15:53:24 UTC 2019

  System load:  0.0               Processes:           124
  Usage of /:   37.3% of 7.69GB   Users logged in:     0
  Memory usage: 26%               IP address for eth0: 172.31.89.83
  Swap usage:   0%

 * Keen to learn Istio? It's included in the single-package MicroK8s.

     https://snapcraft.io/microk8s

0 packages can be updated.
0 updates are security updates.


Last login: Wed Jul 10 15:11:06 2019 from 107.15.153.105
ubuntu@ip-172-31-89-83:~$
```

Source: Ubuntu.

13. The Remote Desktop Connection app requires a username and password. The image is enabled for password authentication, but the Ubuntu user has no password defined. On the instance's command prompt, type the command "sudo passwd ubuntu" to change the password for the Ubuntu account, and enter a strong password (two times) for the Ubuntu user. **Take a screenshot of the command window and include it in your lab report.** Log out from the SSH session by typing "exit."

14. If you are on a Windows machine, open the Remote Desktop Connection application. If you are on a Mac, you can download and install the Remote Desktop 10 app [https://apps.apple.com/us/app/microsoft-remote-desktop-10/id1295203466?mt=12] from the Mac App Store.
15. In the Remote Desktop Connection window, enter the public DNS name of the instance that you noted from Step 12 above. Accept the warning pop-ups and enter ubuntu as username and the password you've created in Step 14. You should see the lxde desktop of your ubuntu instance:

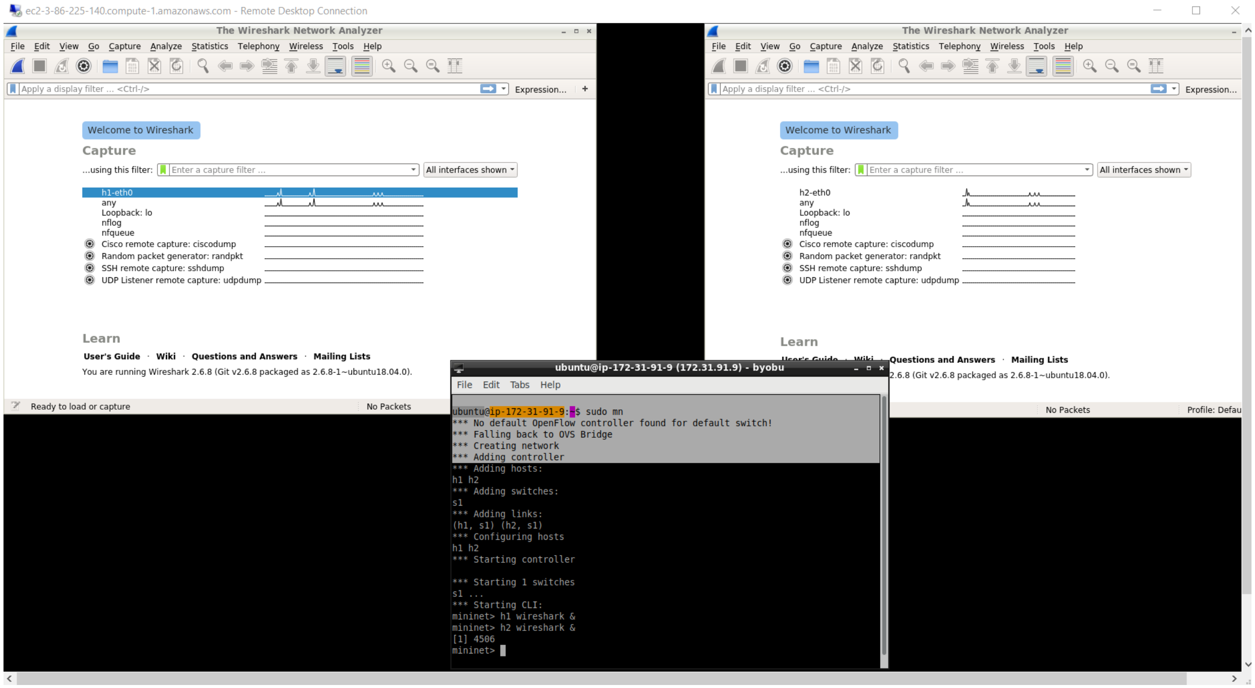


Source: Ubuntu.

16. Maximize your screen, click on the xlde icon in the lower left corner to open the list of actions as above, go to accessories, and open the Byobu terminal window.

Step 4: Run Mininet, Ping One Simulated Mininet Host From Another, and Capture and Inspect the Packets

17. In the terminal window, type "sudo mn". The mininet simulator will create an SDN network of two hosts, h1 and h2, and a switch, s1, between them. You will see the mininet command prompt.
18. Type "h1 wireshark &" on the mininet command prompt. The Wireshark window will open on the h1 host. Next, type "h2 wireshark &" on the mininet command prompt. A second Wireshark window will open on the h2 host. Arrange your xlde desktop so that all three windows are visible.



ec2-3-86-225-140.compute-1.amazonaws.com - Remote Desktop Connection
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
h1-eth0
h2-eth0
any
Loopback: lo
nflog
nfqueue
Cisco remote capture: ciscodump
Random packet generator: randpkt
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 2.6.8 (Git v2.6.8 packaged as 2.6.8-1~ubuntu18.04.0).
Ready to load or capture
No Packets
Profile: Defau
ubuntu@ip-172-31-91-9 (172.31.91.9) - byobu
File Edit Tabs Help

```
ubuntu@ip-172-31-91-9:~$ sudo mn
*** No default OpenFlow controller found for default switch!
*** Falling back to OVS Bridge
*** Creating network
*** Adding controller
*** Adding hosts:
h1 h2
*** Adding switches:
s1
*** Adding links:
(h1, s1) (h2, s1)
*** Configuring hosts
h1 h2
*** Starting controller

*** Starting 1 switches
s1 ...
*** Starting CLI:
mininet> h1 wireshark &
mininet> h2 wireshark &
[1] 4506
mininet>
```

Sources: Mininet, Wireshark.

19. Start capturing packets in both mininet windows by clicking on the shark fin icon in the toolbar (the first icon on the left).
20. In the terminal window, on the mininet prompt, type "h1 ping h2". In both Wireshark windows, you will see packets being captured on both h1 and h2 hosts. The ping command is a continuous command. You'll have to issue a break command to stop it. On the keyboard, press and hold down the Ctrl button (usually on the lower left of the keyboard) and while holding it down, press the C key, then release both keys. Click on the red square icon in both Wireshark windows toolbars to stop capturing.
21. **Take a screenshot of your remote desktop window with both command and Wireshark windows showing and include it in your lab report.**
22. Answer the following questions:
    - What are the IP addresses of both hosts?
    - What protocol packets are captured in this communication? What are these protocols? Research if needed.
    - What values are captured in the Wireshark Info column?

23. Write the lab report, showing steps you've taken, requested screenshots and answers to questions from Step 28. Submit the lab report in Project 1 Step 7 submission box.
24. Close the remote desktop window. Now, even though you have closed down the PuTTY and remote desktop connection to your EC2 instance, it is still running on AWS. You will continue to incur use charges (it will be charged against the AWS credits that you received as part of the CCA 625 AWS Educate Classroom). You will need to stop and terminate your EC2 instance to avoid further charges and to preserve your credits for future projects.

25. Go back to the AWS Console window. If you already closed it, go back to AWSEducate.com, log in, click on "My Classrooms," click on "Go to classroom" for CCA 625, and click on the "AWS Console" button. Remember, you are doing this inside a temporary AWS account created for you from within the AWS Educate environment. You are not using your personal AWS account (if you have one).
26. On the AWS Console window, click on Services, and EC2. Click on "Running Instances." Select the one EC2 instance that you have there, click on the "Action" button, then "Instance State," and "Stop." Click "Yes, Stop" on the pop-up window. Wait until the "Instance State" showed "Stopped." Now, the instance is stopped. But it will still incur a small charge for the storage space it is using. To totally stop the charges, you need to also terminate the instance. Click on the "Action" button, "Instance State," and "Terminate." Click on the "Yes, Terminate" button on the pop-up window. **Take a screenshot of the instance windows showing the instance is terminated and include it in your report.**
27. Finally, you also need to delete the nonstandard security group that you created as part of this lab. Click on "Security Groups" on the left panel. Select the one security group with the group name that start with "launch-wizard." Click on "Action" and "Delete Security Group." Click on "Yes, Delete" on the pop-up window.
28. Log out and close the AWS Console window.