

Diploma in IT, Networking and Cloud

Module 2 Computer Networking Lab Manual

Disclaimer: The content is curated for educational purposes only.

© Edunet Foundation. All rights reserved.

Table of Contents

Learning Outcomes	10
Learning Outcome 1 - Able to understand basic computer network technology	11
Activity 1	12
Aim: Crimp Straight Cable using Different Color Codes.	12
Activity 2	17
Aim: Crimp Cross Cable using Different Color Codes	17
Activity 3	22
Aim: Crimp Rj45 connector with Straight and Cross cable	22
Learning outcome: Able to understand basic computer network technology.	22
Activity 4	30
Aim: Check signal transmission using LAN TESTER	30
Learning outcome: Able to understand basic computer network technology.	30
Activity 5	31
Aim: Install and configure Peer to Peer connection	31
Learning outcome: Able to understand basic computer network technology.	31
Activity 6	37
Aim: Configure IP Address.	37
Learning Outcome 2 - Able to understand and configure server environment and backup services	42
Activity 1	43
Aim: Install and configure Server-Client Network.	43
Activity 2	48

Aim: Install and Configure Windows Server.	48
Activity 3	59
Aim: Configure a Server as Web Server.	59
Activity 4	76
Aim: Configure Mailbox Server	76
Activity 5	100
Aim: Backup and Restore ADS and DHCP	100
Activity 6	124
Aim: Backup and Restore User Data	124
Activity 7	127
Aim: Permit FAT and NTFS Sharing	127
Learning Outcome 3 - Able to configure different protocol services	130
Activity 1	131
Aim: Add user Account	131
Activity 2	139
Aim: Implement AGDLP Process	139
Activity 3	140
Aim: Implement User Authentication Strategy	140
Activity 4	148
Aim: Creating Organizational Unit (OU) in Active Directory	148
Activity 5	159
Aim: Plan and Maintain Group Policies	159
Activity 6	167

Aim: Configure User Environment	167
Activity 7	169
Aim: Install and Configure Active Directory Services	169
Activity 8	183
Aim: Installation and Configuring DNS Services	183
Activity 9	200
Aim: Installation and Configuring DHCP Services	200
Activity 10	216
Aim: Install and Configure FTP Services.	216
Activity 11	237
Aim: Install and Configure HTTP Services	237
Activity 12	244
Aim: Configure IIS Services	244
Learning Outcome 4 - Able to Install and configure Linux server environment	253
Activity 1	254
Aim: Install Linux Server.	254
Activity 2	269
Aim: Create new user and group	269
Activity 3	273
Aim: Create public and data directory.	273
Activity 4	277
Aim: Create an lmhosts file.	277
Activity 5	280

Aim: Check host file	280
Activity 6	283
Aim: Filter ports	283
Activity 7	287
Aim: Secure and install SWAT server.	287
Activity 8	291
Aim: Install and configure Telnet	291
Learning Outcome 5 - Able to install & configure the different types of network devices in a network	296
Activity 1	297
Aim: Configure & Implement Unmanageable Network Switch.	297
Activity 2	300
Aim: Configure & Implement Manageable Network Switch.	300
Code/Program/Procedure (with comments):	300
Activity 3	306
Aim: Install and configure router, bridges and HUB.	306
Activity 4	309
Aim: Configure Wireless Access Point.	309
Activity 5	312
Aim: Install and Configure Wire Network.	312
Activity 6	316
Aim: Install and Configure Wireless Network.	316
Activity 7	322

Aim: Installation of AD-hoc Wireless Network.	322
Activity 8	324
Aim: Configure Gateway Service for Internet Connectivity.	324
Activity 9	327
Aim: Configure ADSL+2 Router for ISP Internet Connectivity.	327
Activity 10	330
Aim: Troubleshoot Internet Connectivity	330
Learning Outcome 6 - Able to configure and manage network security	337
Activity 1	338
Aim: Managing Server Network Security	338
Activity 2	342
Aim: Set up security baseline	342
Activity 3	350
Aim: Configure Audit Policy	350
Activity 4	359
Aim: Monitor and Troubleshoot Network protocol	359
Activity 5	363
Aim: Configure Protocol Security	363
Configure the Auto Settings	364
Activity 6	370
Aim: Plan security for Wireless Network	370
Activity 7	375
Aim: Install and Configure Different Antivirus Software	375

Activity 8	378
Aim: Install and Configure Admin Console	378
Activity 9	382
Aim: Configure a Local Security Policies	382
Activity 10	386
Aim: Configure Domain Security Policies	386
Activity 11	392
Aim: Configure RRAS Policies	392
Learning Outcome 7 - Able to configure and perform remote accessing & routing	397
Activity 1	398
Aim: Manage TCP/IP Routing	398
Activity 2	405
Aim: Configure Remote Access Authentication Protocol	405
Activity 3	407
Aim: Connect remote Desktop using RemoteAssistance.	407
Activity 4	411
Aim: Connect Remote Desktop using Telnet	411
Activity 5	413
Aim: Connect Remote Desktop using HyperTerminal	413
Activity 6	414
Aim: Connect Remote Desktop using Teamviewer	414
Learning Outcome 8 - Able to get familiarized with internet and E- Commerce sites	419
Activity 1	420

Aim: Configure web browser.	420
Activity 2	427
Aim: Search for content using popular search engines.	427
Activity 3	431
Aim: Use favourite folder for browsing quickly	431
Activity 4	434
Aim: Download & Print Webpages	434
Step 2	435
Activity 5	436
Aim: Create and send e-mail, Reply to an e-mail message and Forward email message	436
Activity 6	441
Aim: Send document/softcopy by email.	441
Activity 7	444
Aim: Activate spell check using address book and Handle SPAM	444
Activity 8	446
Aim: Sorting and searching emails.	446
Activity 9	452
Aim: Crimp Straight Cable using Different Color Codes.	452
Activity 10	460
Aim: Store download file in mail drives	460
Activity 11	467
Aim: Communicate using text, video chatting and social networking sites	467
Activity 12	470

Aim: Protect the computer against various internet threats	470
Activity 13	471
Aim: Browse ecommerce website.	471

Learning Outcomes

After completing this module a student will be able to:

1. Able to understand basic computer network technology.
2. Able to understand and configure server environment and backup services.
3. Able to configure different protocol services.
4. Able to Install and configure Linux server environment.
5. Able to Install & configure the different types of network devices in a network.
6. Able to configure and manage network security.
7. Able to configure and perform remote accessing & routing.
8. Able to get familiarize with internet and E- Commerce sites.

Learning Outcome 1 - Able to understand basic computer network technology

After achieving this learning outcome, a student will be able to understand basic computer network technology. In order to achieve this learning outcome, a student has to complete the following:

1. Crimp Straight Cable using Different Color Codes (5 Hrs)
2. Crimp Cross Cable using Different Color Codes (5 Hrs)
3. Crimp Rj45 connector with Straight and Cross cable (3 Hrs)
4. Check signal transmission using LAN TESTER (2Hrs)
5. Install and configure Peer to Peer connection. (5Hrs)
6. Configure IP Address(5Hrs)

Activity 1

Aim: Crimp Straight Cable using Different Color Codes.

Learning outcome: Able to understand basic computer network technology.

Duration: 5 hour

List of Hardware/Software requirements:

1. Crimp and connect the cable

Types of cables

There are 3 type of cables

- Straight Through Cable
- Cross Cables
- Rollover Cables

Material used

- Crimping tool
- Ethernet Cable
- RJ45 Jack

2. Ethernet Cable Type

In Computer Networks, Cat 5, Cat 5e, and Cat 6 Cables are used. Cat 6 Cables are used. Cat 6 cables have up to 400MHz for the super-fast broadband application.

Colour Code

T568A and T568B are the two different colour codes used for pairing devices. T568B is mostly used one.

Setting up before crimping

- Take the LAN cable and strip the outer cover carefully or else the internal wire will be damaged.
- There will be 4 pairs of twisted wires.

- Unwind the twisted cable and make it straight and cut the edge of the wire.

3. Ethernet Cabling tools



Ethernet Cabling Tools

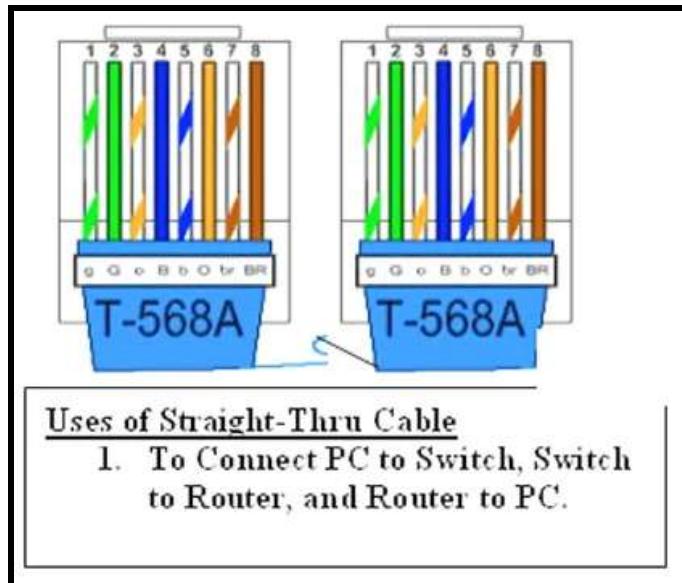
Code/Program/Procedure (with comments):

Straight Cable is used to connect different types of devices. This cable can be used to

- Connect a router to a hub.
- Connect a computer to a switch/router.
- Connect a modem to a router

a. Arrange

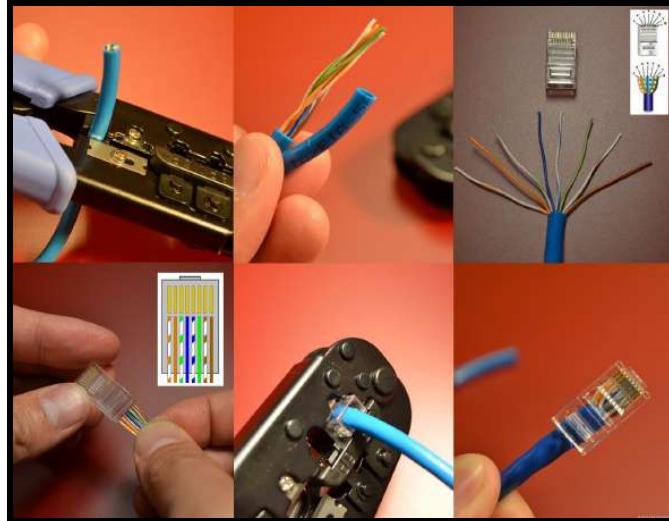
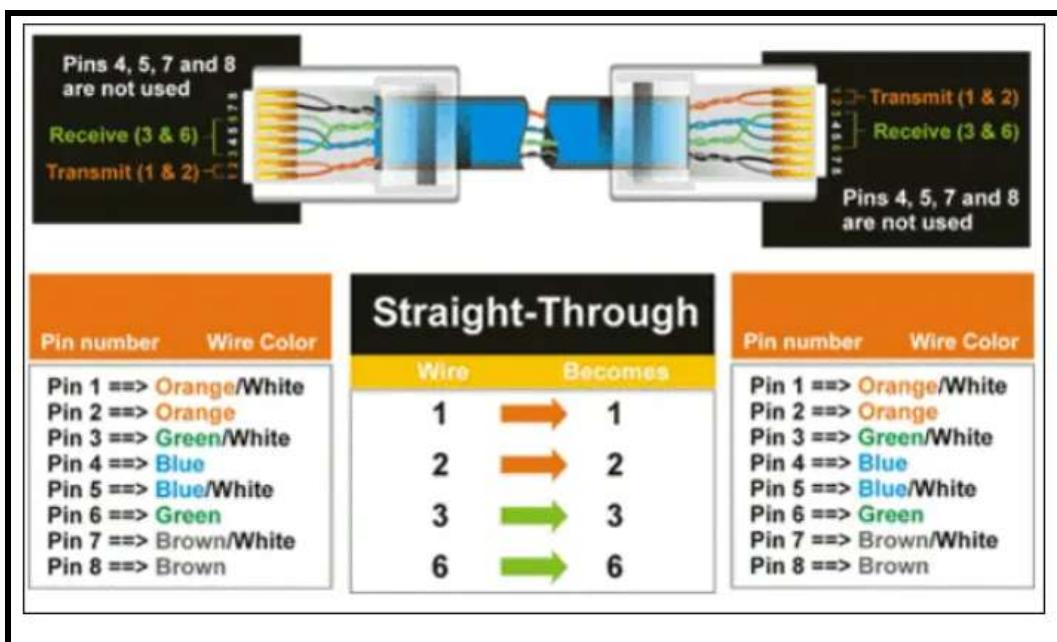
Arrange all wire in the below sequence and cut the edge. Both the end of the cables must have the same sequence of coloured wire. Both ends of the cables will have the same colour codes.



Straight Thru Cable

b. Insert

Now insert the cable into port and then crimp the cable using crimping tool like shown in the image given below:

**Crimping Steps****Output/Results snippet:**

Color Codes



Activity 2

Aim: Crimp Cross Cable using Different Color Codes

Learning outcome: Able to understand basic computer network technology.

Duration: 5 hour

List of Hardware/Software requirements:

1. Crimp and connect the cable

Types of cables

There are 3 type of cables

- Straight Through Cable
- Cross Cables
- Rollover Cables

Material used

- Crimping tool
- Ethernet Cable
- RJ45 Jack

2. Ethernet Cable Type

In Computer Networks, Cat 5, Cat 5e, and Cat 6 Cables are used. Cat 6 Cables are used. Cat 6 cables have up to 400MHz for the super-fast broadband application.

Colour Code

T568A and T568B are the two different colour codes used for pairing devices. T568B is mostly used one.

Setting up before crimping

- Take the LAN cable and strip the outer cover carefully or else the internal wire will be damaged.
- There will be 4 pairs of twisted wires.

- Unwind the twisted cable and make it straight and cut the edge of the wire.

3. Ethernet Cabling tools



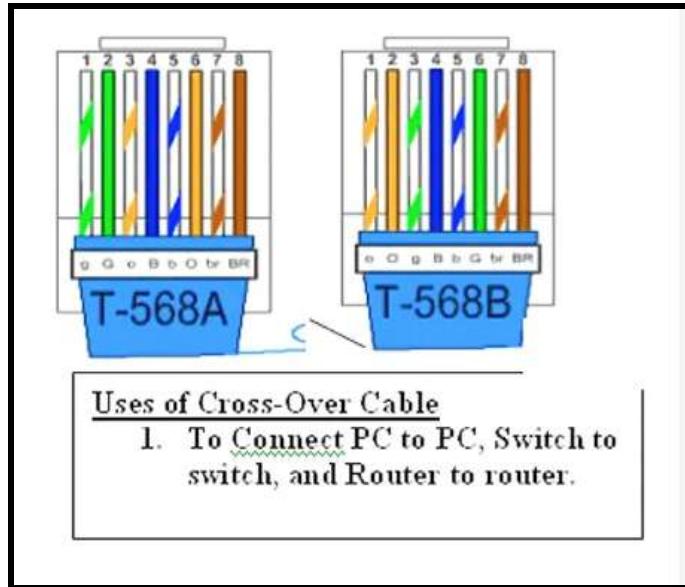
Code/Program/Procedure (with comments):

Cross cable is used to connect for the same types of devices. This can be used to:

- Connecting a computer to a computer.
- Connecting to the hub to a hub.
- Connecting to the router to a router.
- Connecting to switch to a switch.

a. Arrange

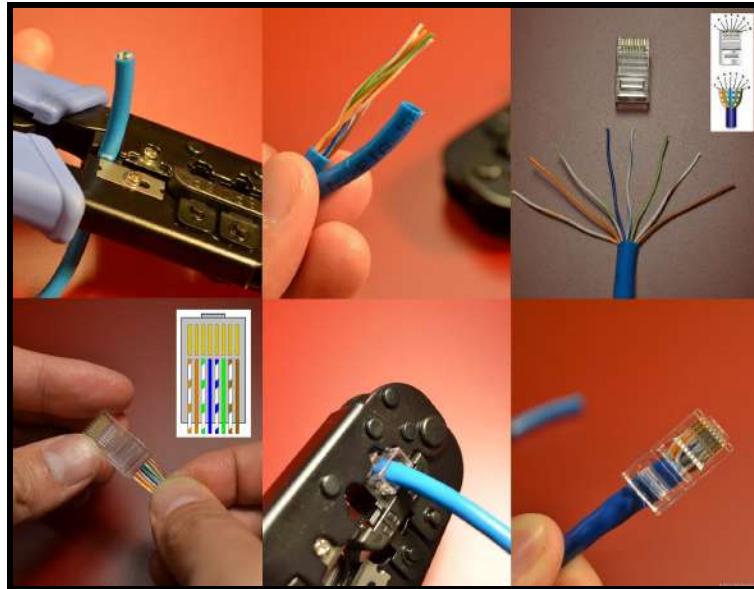
Both ends of the wire arrangement are different colour codes. In this cable T568A and T568B colour codes must be used.



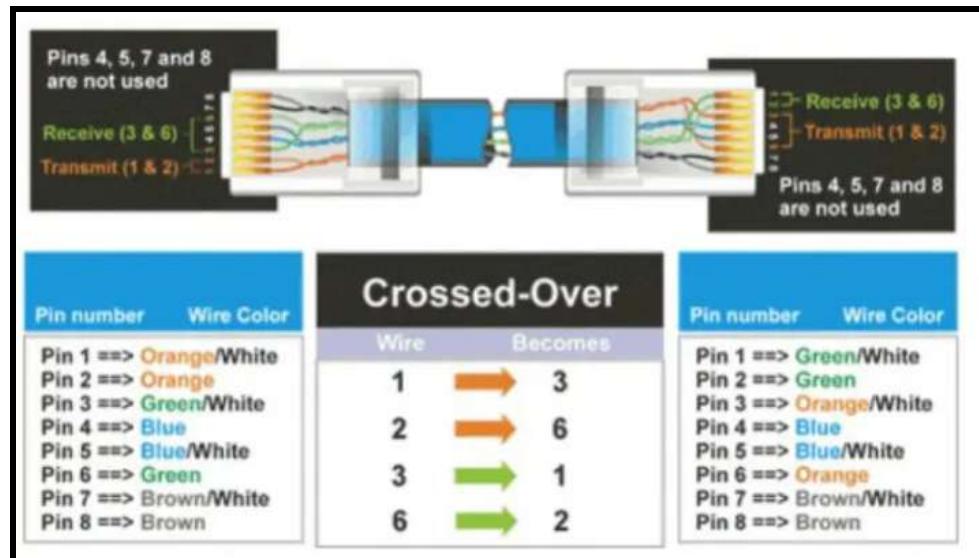
Crossover Cable

b. Insert

Now insert the cable into port and then crimp the cable using crimping tool like shown in the image given below:



Output/Results snippet:





Activity 3

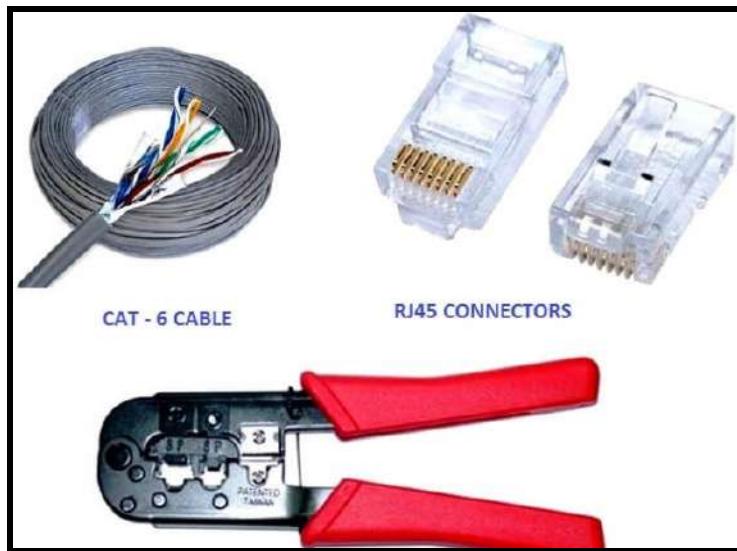
Aim: Crimp Rj45 connector with Straight and Cross cable

Learning outcome: Able to understand basic computer network technology.

Duration: 3 hour

List of Hardware/Software requirements:

1. Ethernet Cable – Category 5e or CAT5e or CAT6
2. RJ-45 Crimping tool
3. RJ45 Crimp able Connectors(Modular connector)
4. Cable tester (optional, but recommended)



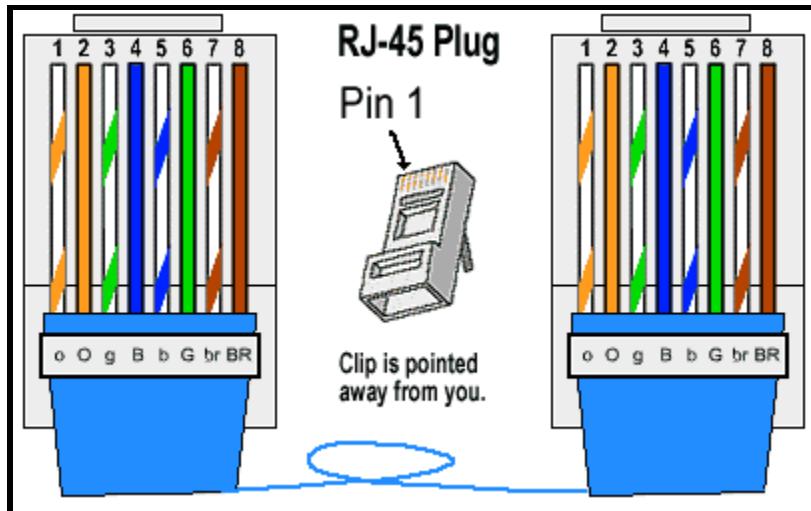
Code/Program/Procedure (with comments):

There are two kinds of Ethernet cable used for communication.

- Straight Through
- Crossover cable

Straight Through cable

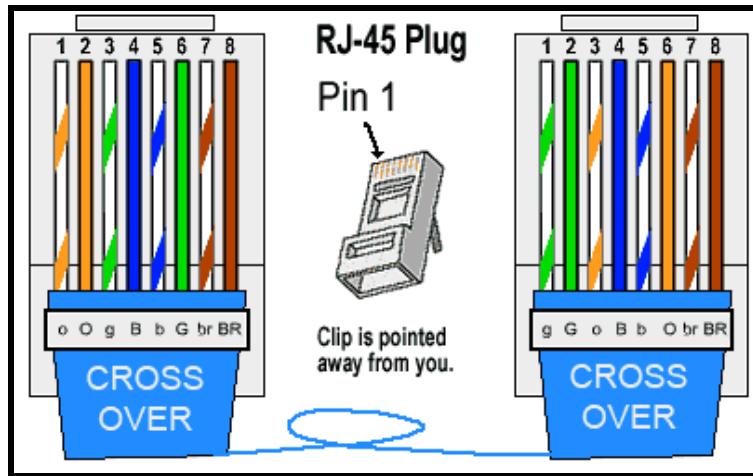
Straight Through Ethernet cables are the standard cable used for almost all purposes, and are often called “patch cables”. It is highly recommended you duplicate the color order as shown on the left. Note how the green pair is not side-by-side as are all the other pairs. This configuration allows for longer wire runs.



Straight Through Cable

Crossover Cables

The purpose of a Crossover Ethernet cable is to directly connect one computer to another computer (or device) without going through a router, switch or hub.



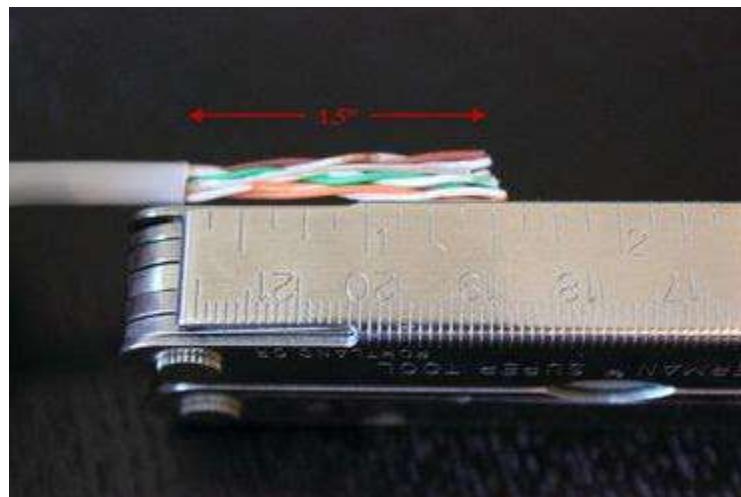
Crossover Cable

The two standards for wiring Ethernet cables are T568A and T568B. T568B is the most common and is what we'll be using for our straight Ethernet cable. The tables below show the proper orientation of the colored wires to the pins.

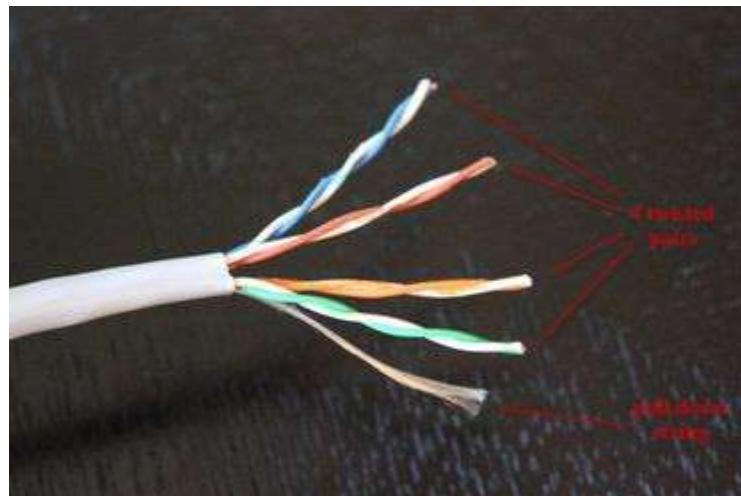
T568A Standard	
Pin 1	White/Green
Pin 2	Green
Pin 3	White/Orange
Pin 4	Blue
Pin 5	White/Blue
Pin 6	Orange
Pin 7	White/Brown
Pin 8	Brown

T568B Standard	
Pin 1	White/Orange
Pin 2	Orange
Pin 3	White/Green
Pin 4	Blue
Pin 5	White/Blue
Pin 6	Green
Pin 7	White/Brown
Pin 8	Brown

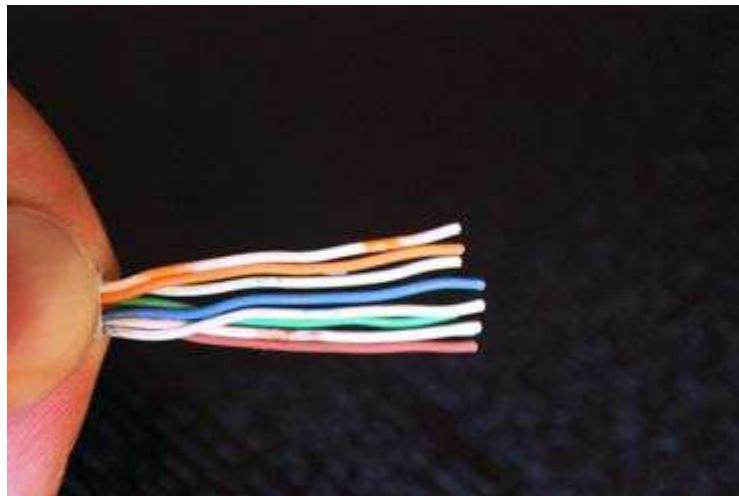
Step 1: Strip the cable jacket about 1.5 inch down from the end.



Step 2: Spread the four pairs of twisted wire apart. For Cat 5e, you can use the pull string to strip the jacket farther down if you need to, then cut the pull string. Cat 6 cables have a spine that will also need to be cut.

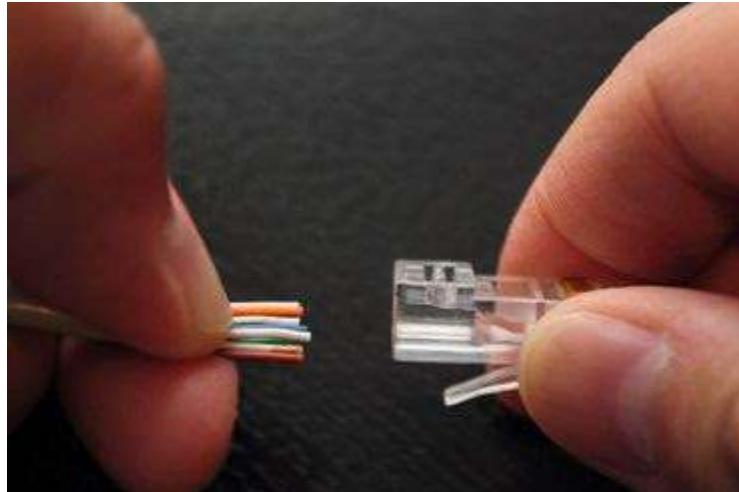


Step 3: Untwist the wire pairs and neatly align them in the T568B orientation. Be sure not to untwist them any farther down the cable than where the jacket begins; we want to leave as much of the cable twisted as possible.

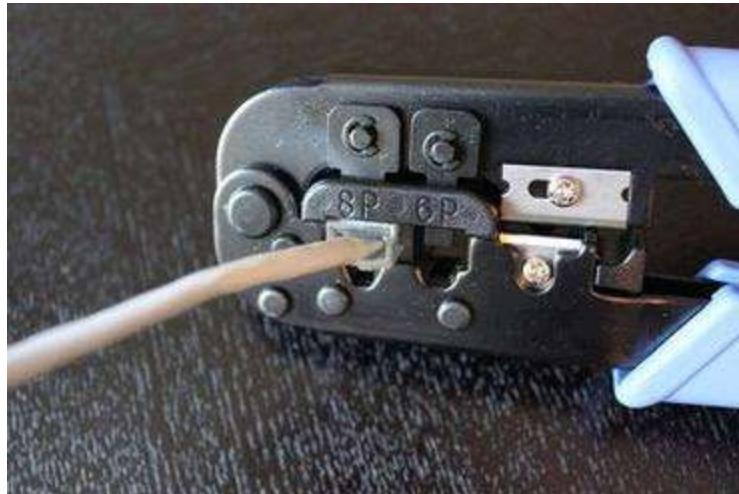


Step 4: Cut the wires as straight as possible, about 0.5 inch above the end of the jacket.

Step 5: Carefully insert the wires all the way into the modular connector, making sure that each wire passes through the appropriate guides inside the connector.



Step 6: Push the connector inside the crimping tool and squeeze the crimper all the way down.



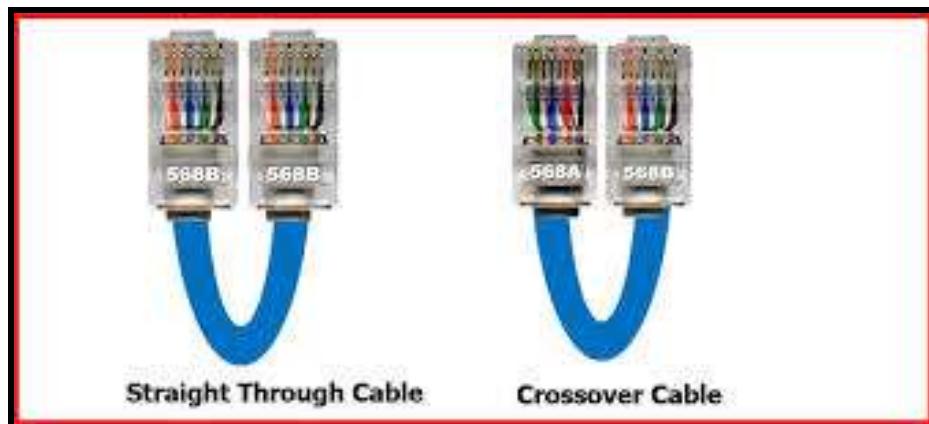
Step 7: Repeat steps 1-6 for the other end of the cable.

Step 8: To make sure you've successfully terminated each end of the cable, use a cable tester to test each pin.



For crossover cables, simply make one end of the cable a T568A and the other end a T568B.

Output/Results snippet:



Activity 4

Aim: Check signal transmission using LAN TESTER

Learning outcome: Able to understand basic computer network technology.

Duration: 2 hour

List of Hardware/Software requirements:

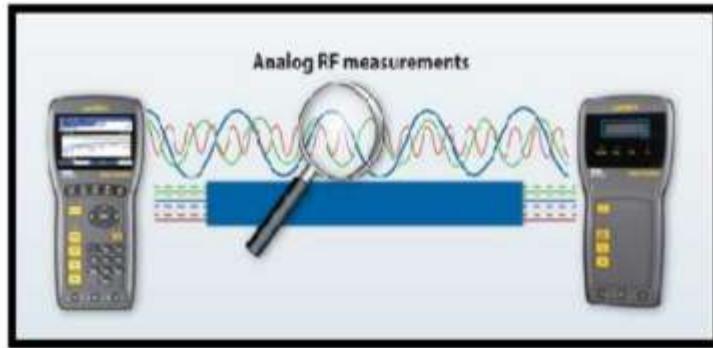
1. Cables
2. LAN TESTER



Code/Program/Procedure (with comments):

- LAN testers can determine IP Addresses, identify polarity, connected port, and link connectivity.
- LAN testers can also test which state of LAN network connection to Hub and switches. IT can analyse the traffic of a network and which IP is generated.
- RJ45 LAN tester is used to design a quick determination of the data server connected to the jack.

-
- The network topology is Ethernet and network protocol (VoIP, PoE) can be detected easily within a second.
 - It is easy, reliable and quick to determine which type of connection is connected to a port.

Output/Results snippet:

Activity 5

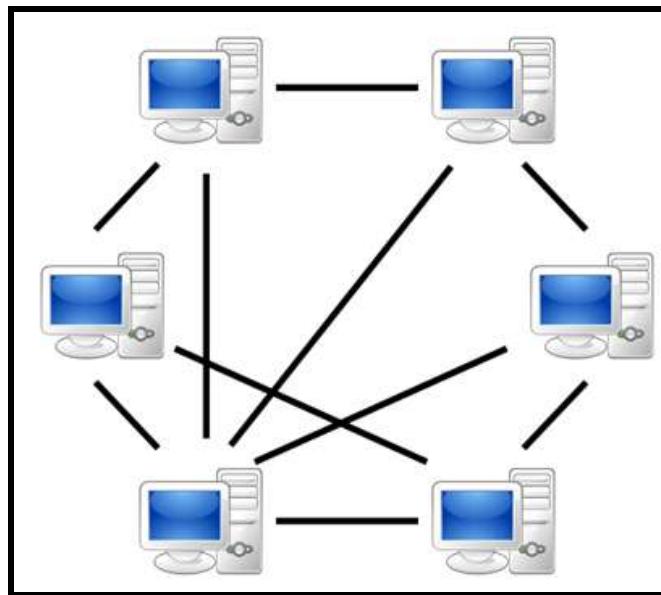
Aim: Install and configure Peer to Peer connection

Learning outcome: Able to understand basic computer network technology.

Duration: 5 hour

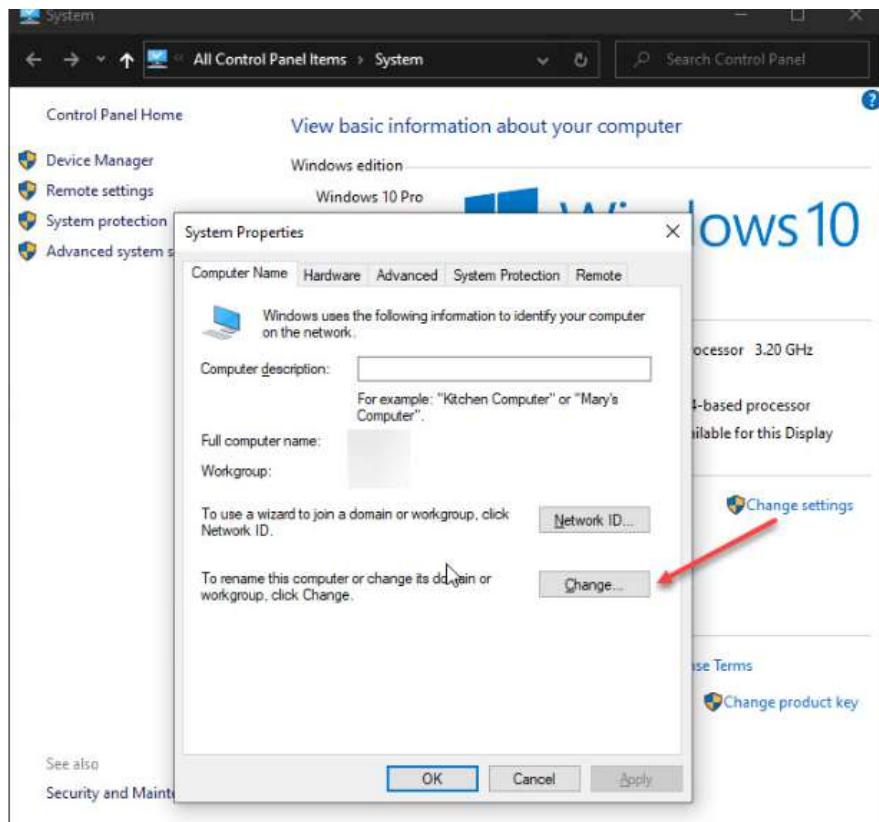
List of Hardware/Software requirements:

-
1. Multiple Client System
 2. LAN Connection without Internet
 3. Switch and Routers

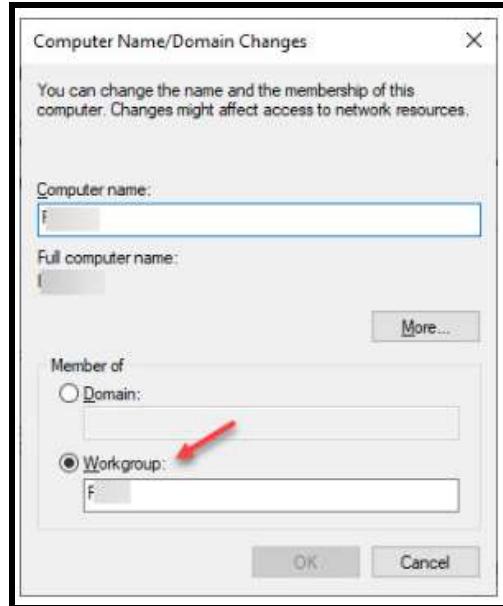
**Code/Program/Procedure (with comments):**

To share files across P2P networks, you first need to set up a network for the same. This can be done for both cable and router connections, so follow these steps for peer-to-peer network setup for your workgroup on Windows 10:

1. On your desktop, right-click on the This PC to reveal the context menu and select Properties. This should open a control panel window.
2. Locate and click on Change Settings in the window that opens. This will open a System Properties
3. Under the Computer Name tab, click on the Change button.



4. Click on the radio button next to how you wish to connect to the P2P network. If the network you wish to connect to has a domain, enter the name next to the Domain radio button. If you wish to connect through a local Workgroup, enter the name of the Workgroup after selecting the radio button for the same.



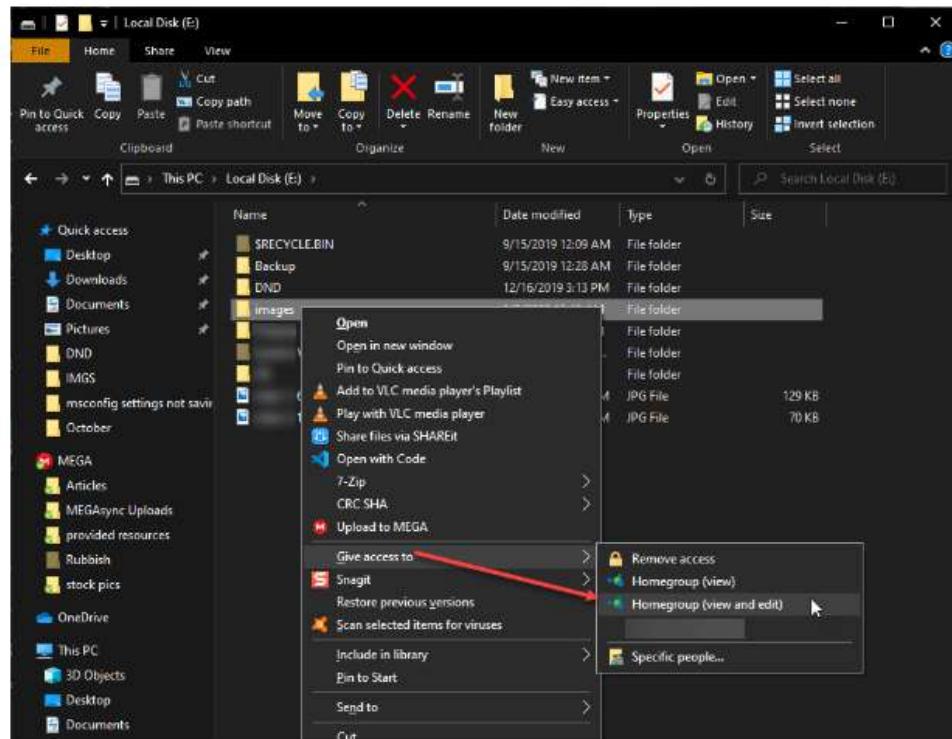
5. Click on OK. You will see a prompt for restarting your PC.
6. Restart your PC.
7. After your PC has rebooted, open File Explorer. You can use the keyboard shortcut Win + E.
8. From the left quick access menu, click on Network.
9. You should see the other computers on your Network in the top row. If you do not see your computers, you will instead be presented with a yellow bar saying Network computers are not visible. Click on this bar to change the settings.
10. Select Turn on network discovery and file sharing.
11. Refresh the explorer by pressing F5, or from the right-click context menu.

Access Files On Another PC Using Peer To Peer Connection

You can also access the files present on another PC on your network. To do this, you need to allow access to the file that you wish to share.

1. To share a file, open the folder of the file in File Explorer.
2. Right-click on the file that you wish to share to reveal the context menu.

3. Hover over ‘Give access to’ to reveal additional settings. Select Homegroup (view&Edit.)



4. On another PC, create a peer-to-peer network using the steps given above.
5. Double click on any PC to access the files on your PC.
6. Enter the credentials of the PC that you wish to gain access to and click on OK.
7. You will be able to see the folders that you shared in step 3.

Output/Results snippet:



Activity 6

Aim: Configure IP Address.

Learning outcome: Able to understand basic computer network technology.

Duration: 5 hour

List of Hardware/Software requirements:

1. PC
2. Window 10 Operating System

Code/Program/Procedure :

To set a static IP Addresses on your Windows are

- Click Start Menu → Control Panel → Network and Sharing Center.
- Click Change adapter settings.

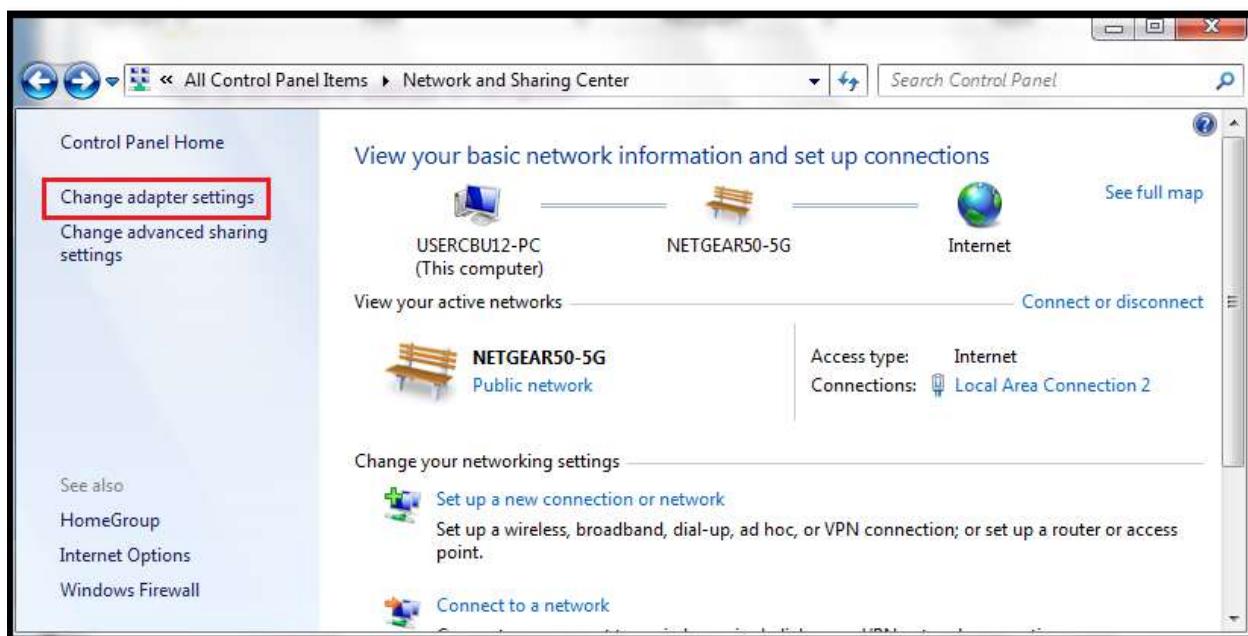
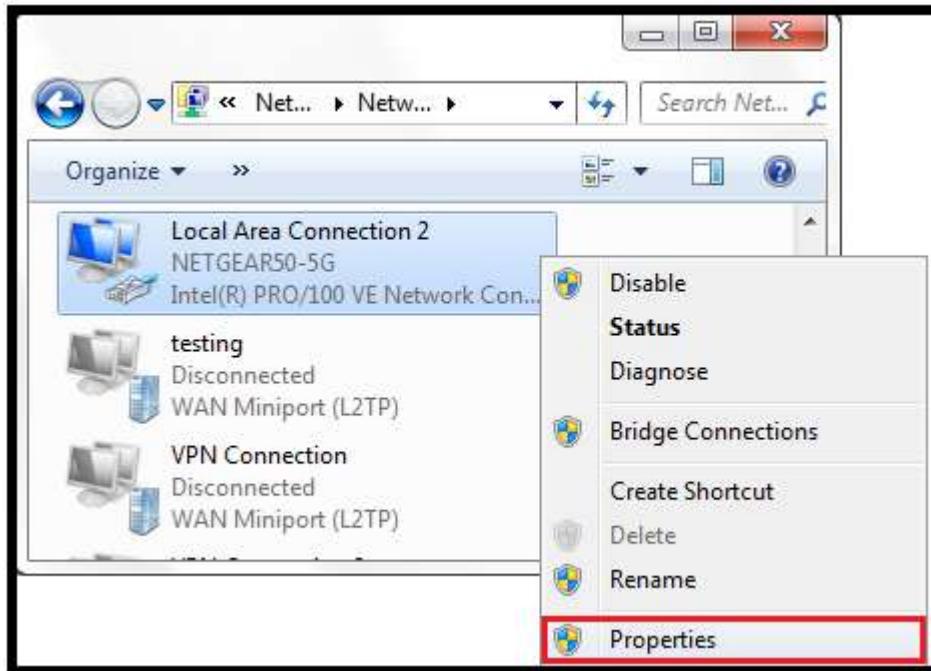


Image 1:Configure IP Address

- Right click on the Local area connection icon and click on the Properties.

**Image 2:LAN Properties**

- Select Internet Protocol Version 4(TCP/IP) and click on the Properties.

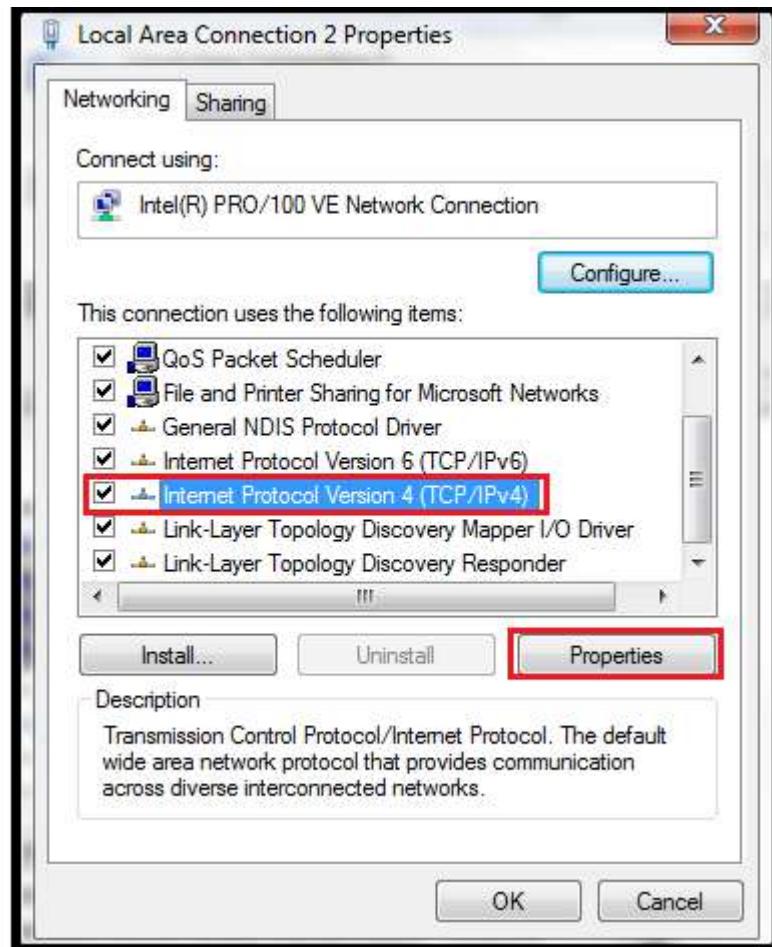


Image 3:TCP/IP Properties

- Select the following IP address and enter the IP address, Subnet Mask, Default Gateway and DNS server. Click on the **OK button** and then close the Local Area Connection properties window.

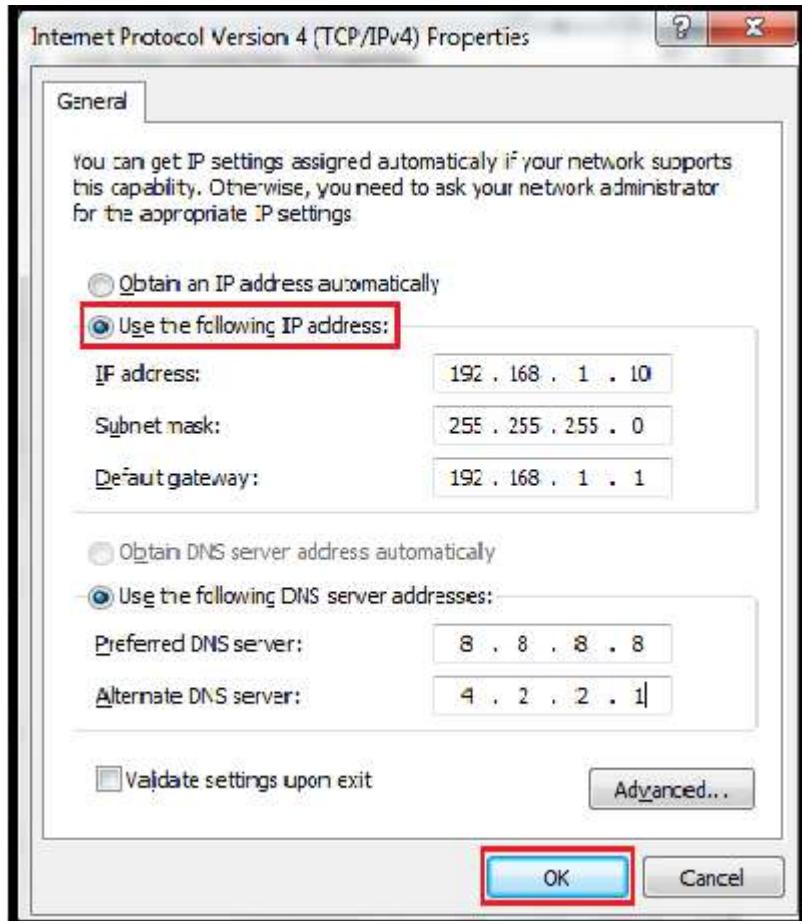


Image 4:LAN Properties

Output/Results snippet:

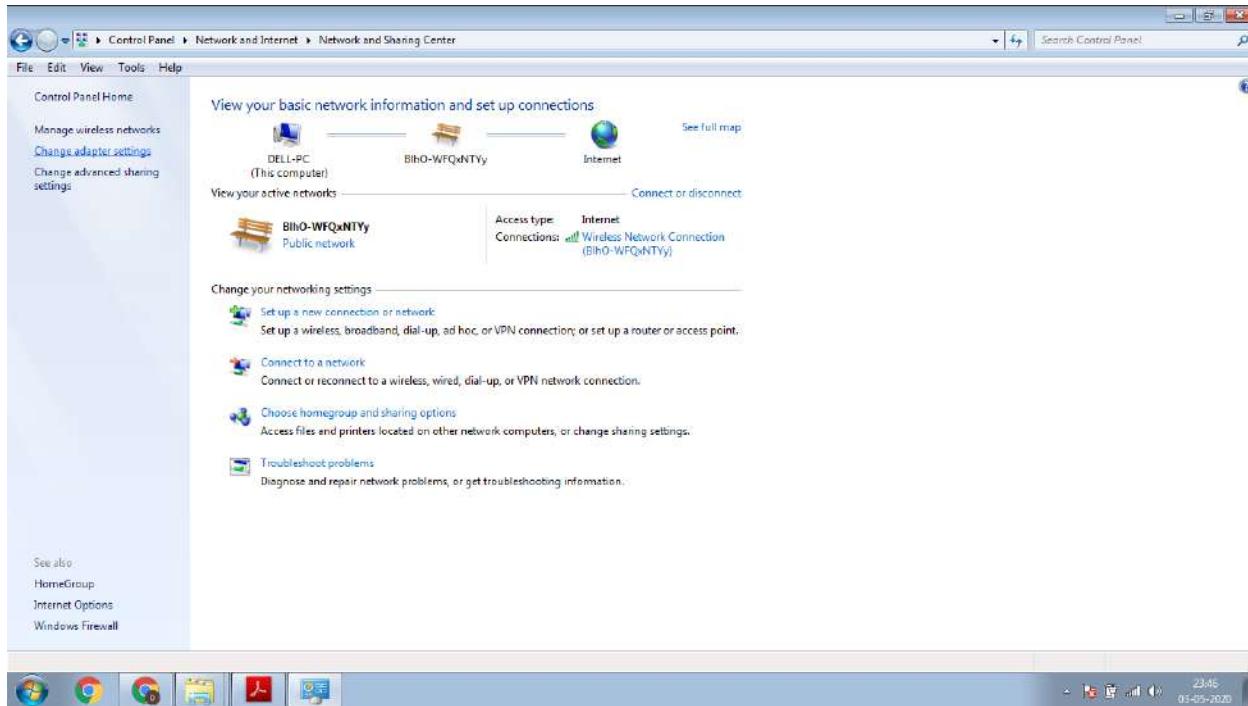


Image 5:Configure IP address

Learning Outcome 2 - Able to understand and configure server environment and backup services

After achieving this learning outcome, a student will be able to understand and configure server environment and backup services. In order to achieve this learning outcome, a student has to complete the following:

1. Install and configure Server -Client Network(5 Hrs)
2. Install and configure Windows Server(5 Hrs)
3. Configure a server as web server(5 Hrs)
4. Configure Mailbox Server (2 Hrs)
5. Backup and Restore ADS and DHCP (3Hrs)
6. Backup and Restore User Data (2Hrs)
7. Permit FAT and NTFS Sharing (3Hrs)

Activity 1

Aim: Install and configure Server-Client Network.

Learning outcome: Able to understand and configure server environment and backup services.

Duration: 5 hour

List of Hardware/Software requirements:

1. Windows 7/windows10 or Windows Server 2008 or newer
2. Microsoft .NET Framework 4 or newer

Code/Program/Procedure:

- Check the bit of Operating system and which windows version of the computer.

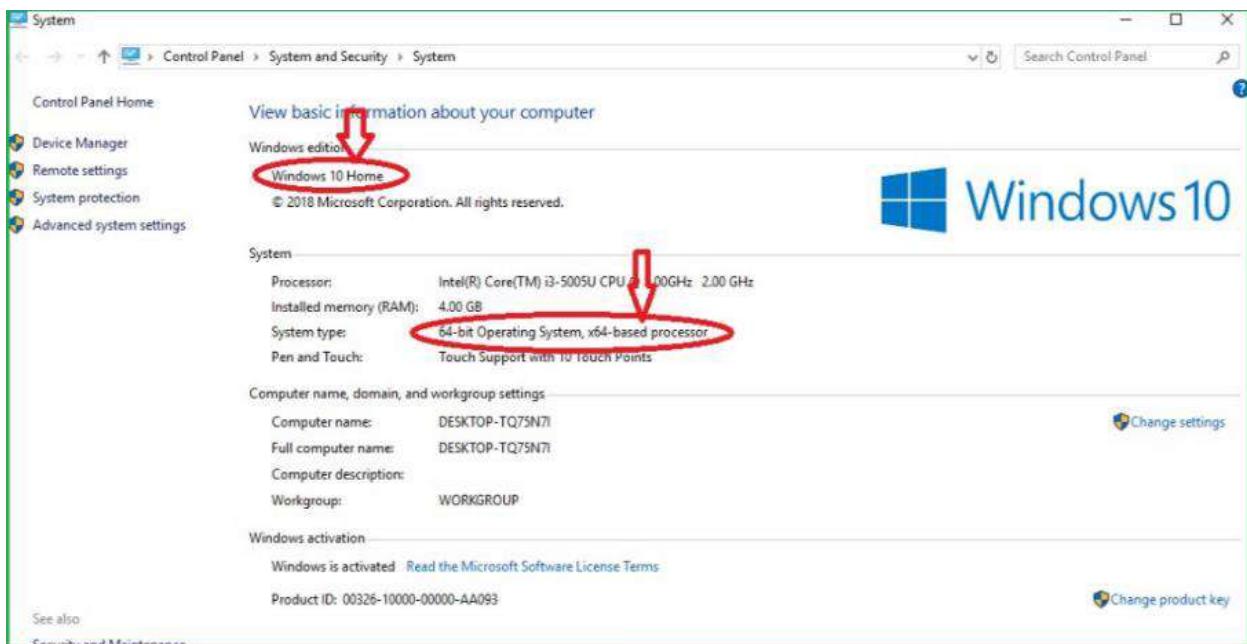


Image1: System Properties

Name the server

- ✓ Go to control panel
- ✓ Select system& security
- ✓ Select the system
- ✓ Select system properties

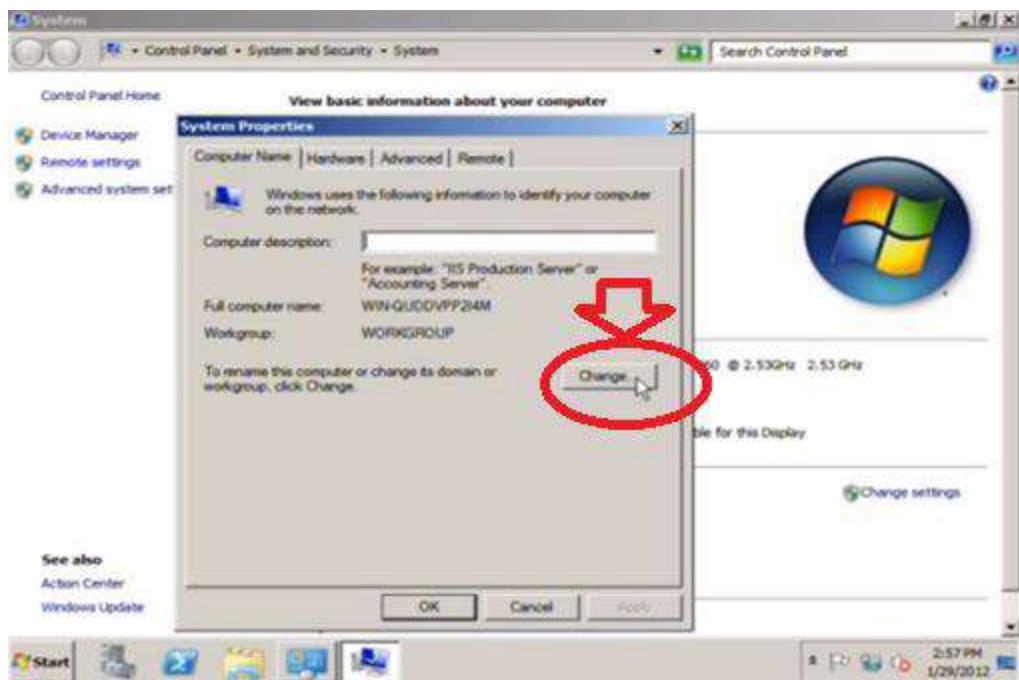


Image 2: System Properties

- Click on the change button, computer name /Domain changes page will display.
- Then change the name and click on ok button

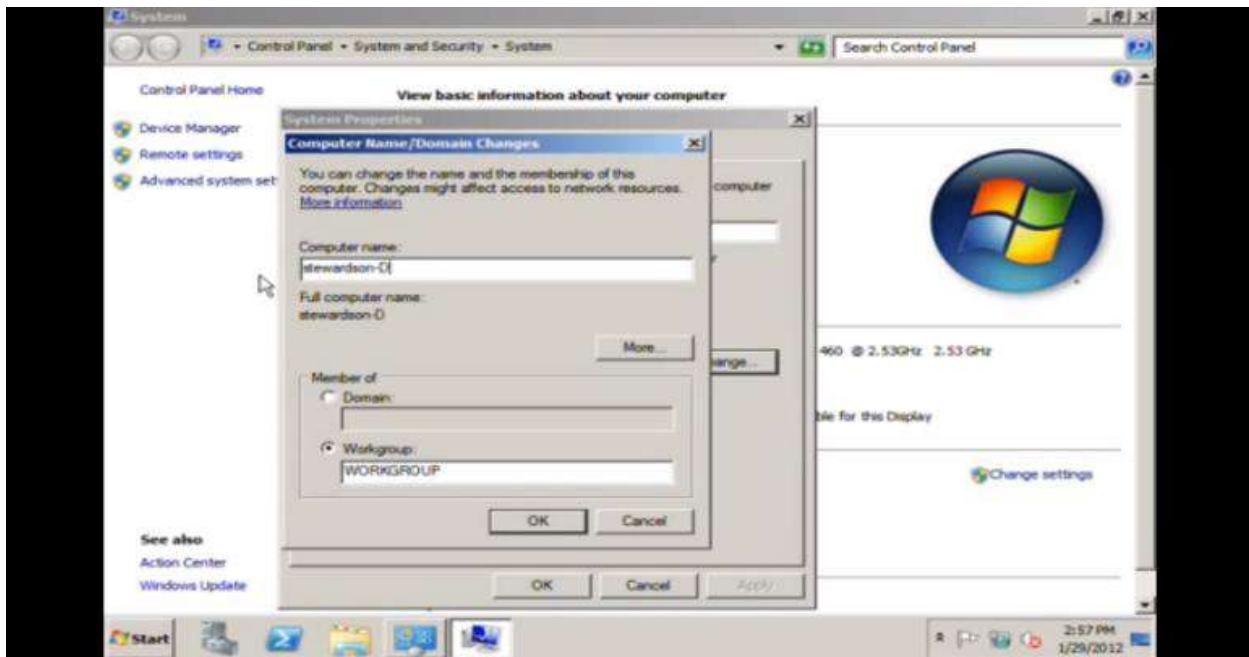


Image 3:Domain Change icon

- Restart the computer to apply the changes, the page will display then click on the ok button, Restart the computer.

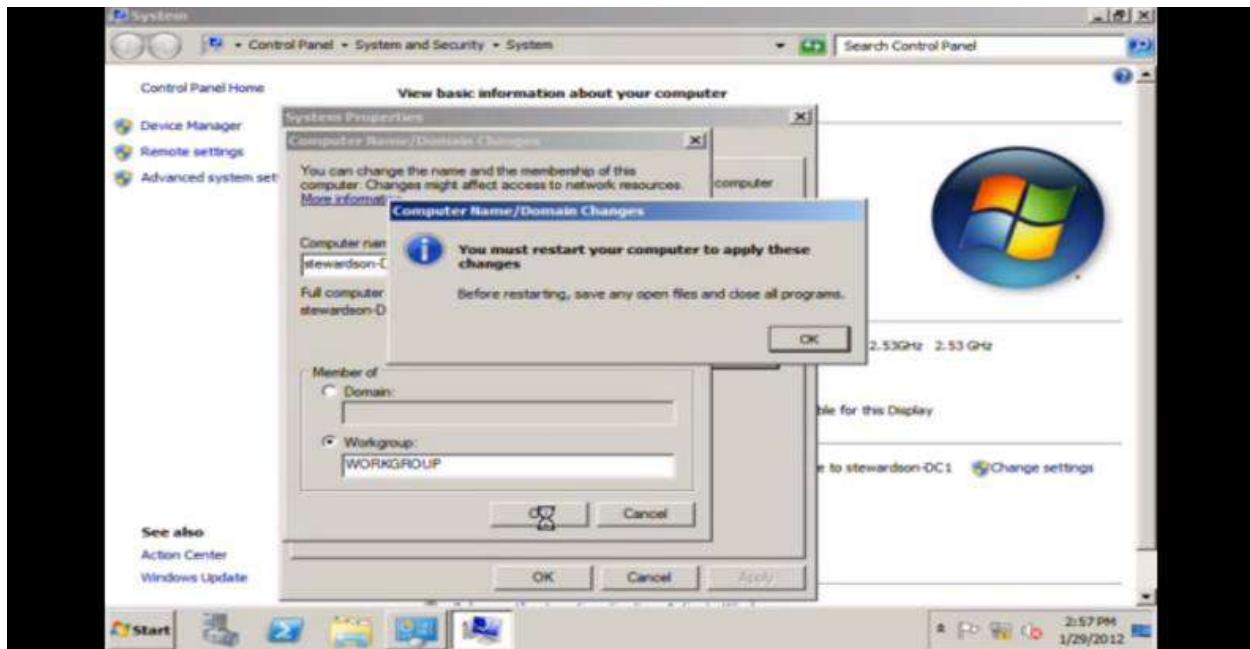


Image 4:Domain Change icon

Output/Results snippet:

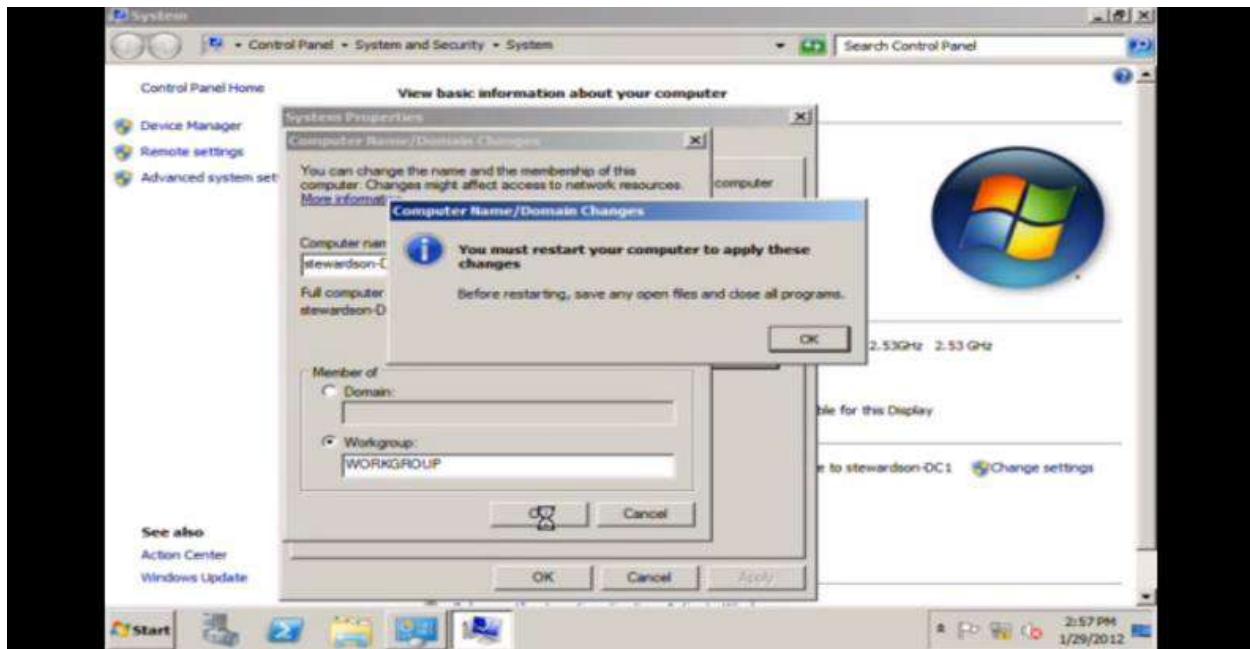


Image 5:Domain Change icon

References:

- <https://www.techwalla.com/articles/how-do-i-set-up-a-server-to-client-network>
- <https://www.quora.com/How-do-I-setup-a-local-client-server-network>

Activity 2

Aim: Install and Configure Windows Server.

Learning outcome: Able to understand and configure server environment and backup services.

Duration: 5 hour

List of Hardware/Software requirements:

1. CPU speed: 133MHz (550MHz recommended)
2. RAM: 128MB (256MB recommended; 4GB maximum on Standard Server)
3. Disk space for setup: 1.5GB
4. CD-ROM drive: 12X
5. Monitor: Super VGA capable of providing 800 x 600 resolution

Code/Program/Procedure :

Follow the procedures given below:

1. Open browser type windows server
2. Select Microsoft Windows server.
3. Select download the trail.

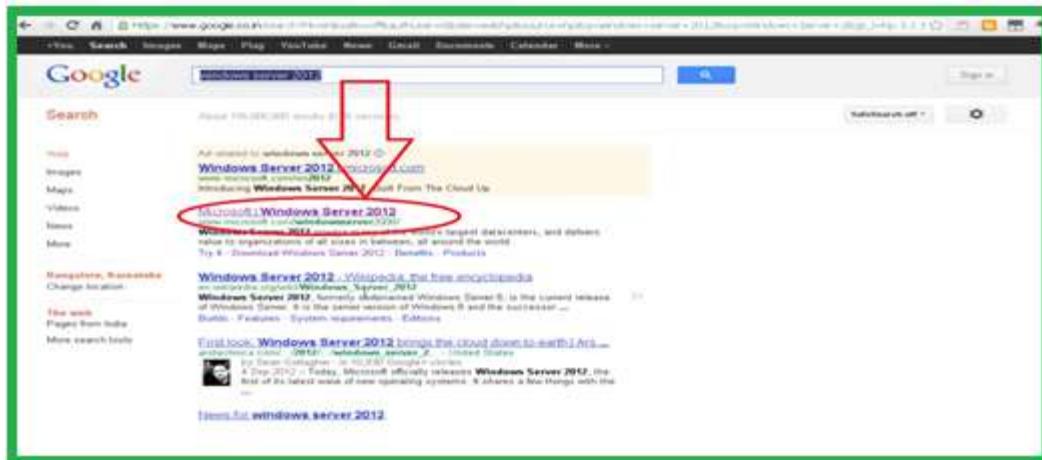


Image 6: Web browser



Image 7: Windows Server download

4. Click on GET STARTED button

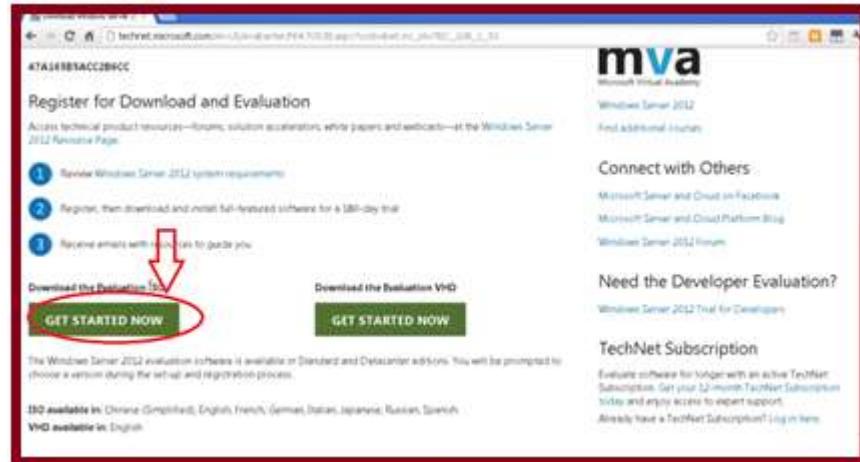


Image 8:Windows Server Start/Register

5. Enter the Microsoft username and password, if it's not created then create it and click on the continue button.

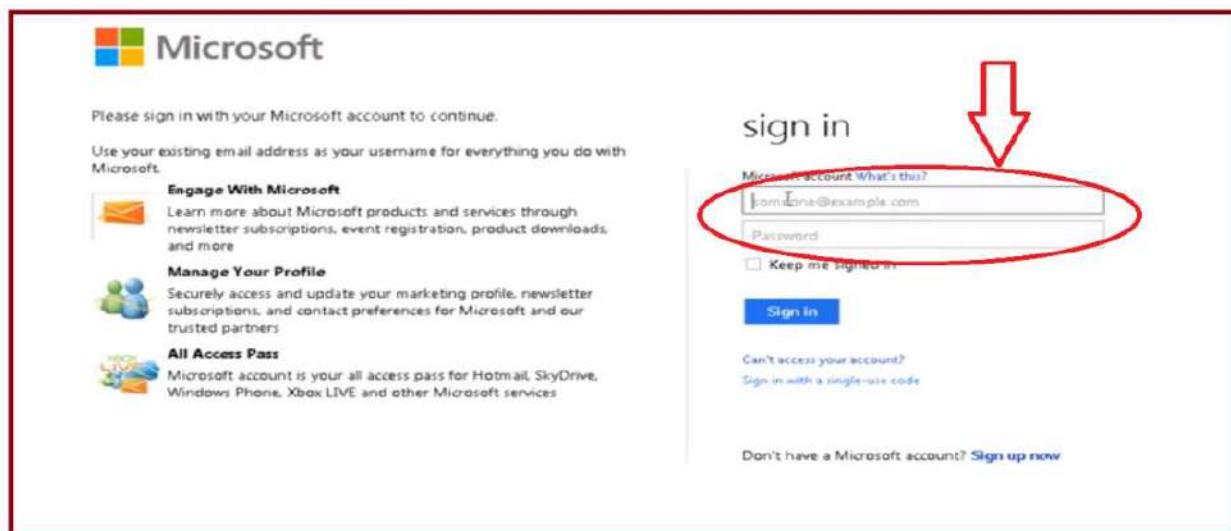


Image 9: Microsoft Login

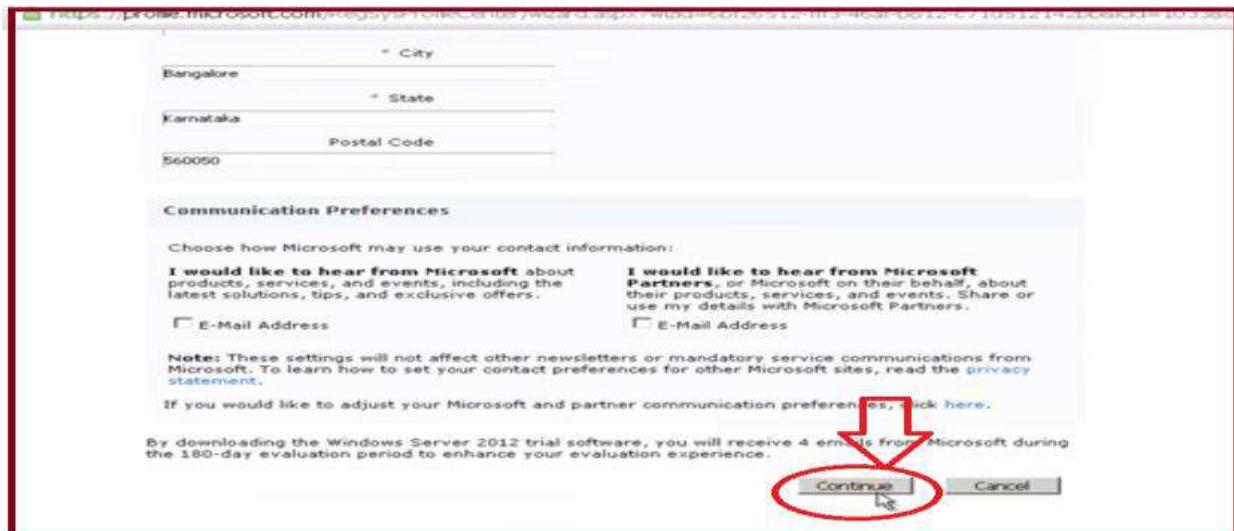


Image 10:Microsoft Register

6. Download the Iso file and save the file, double click on downloaded file.

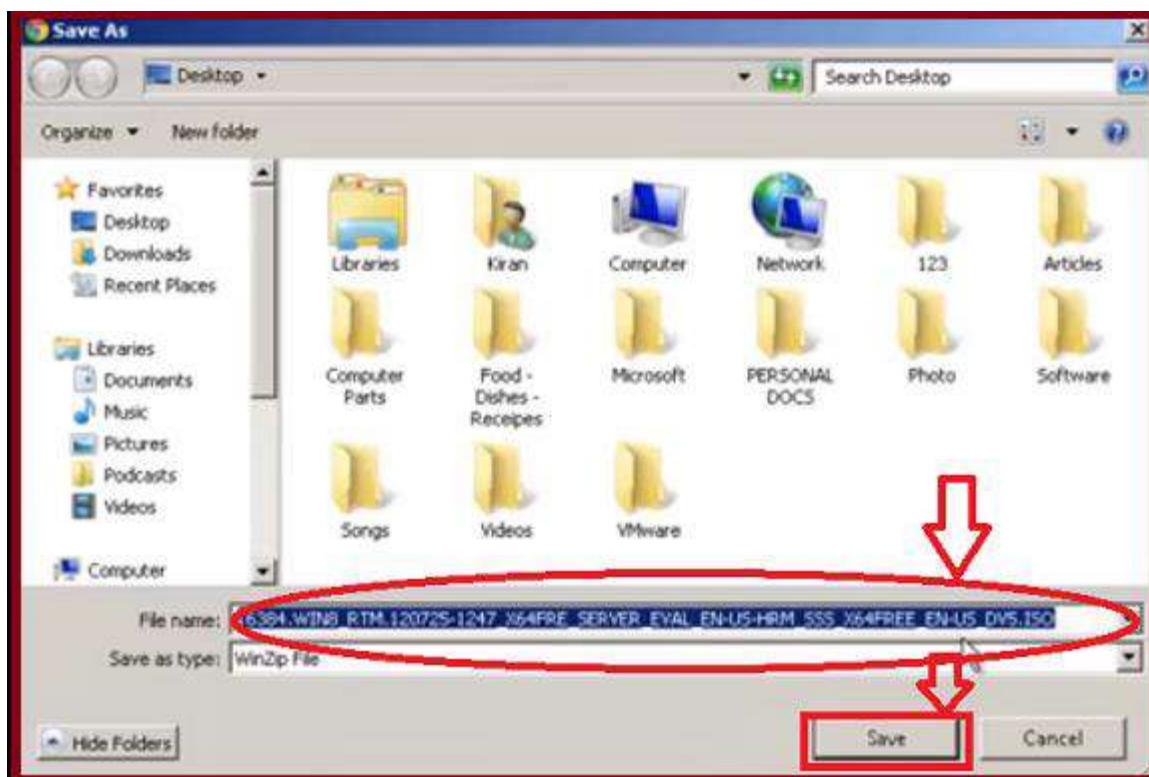


Image 11:Saving the File**Image 12:Downloading**

7. Click on power on this virtual machine, it will run VMware software.

**Image 13:VMware software Tools**



Image14:VMware software new file

8. Select the language
9. Select the terms and conditions
10. Select 'I accept' checkbox
11. Click on next button.



Image 15:Windows Server Register

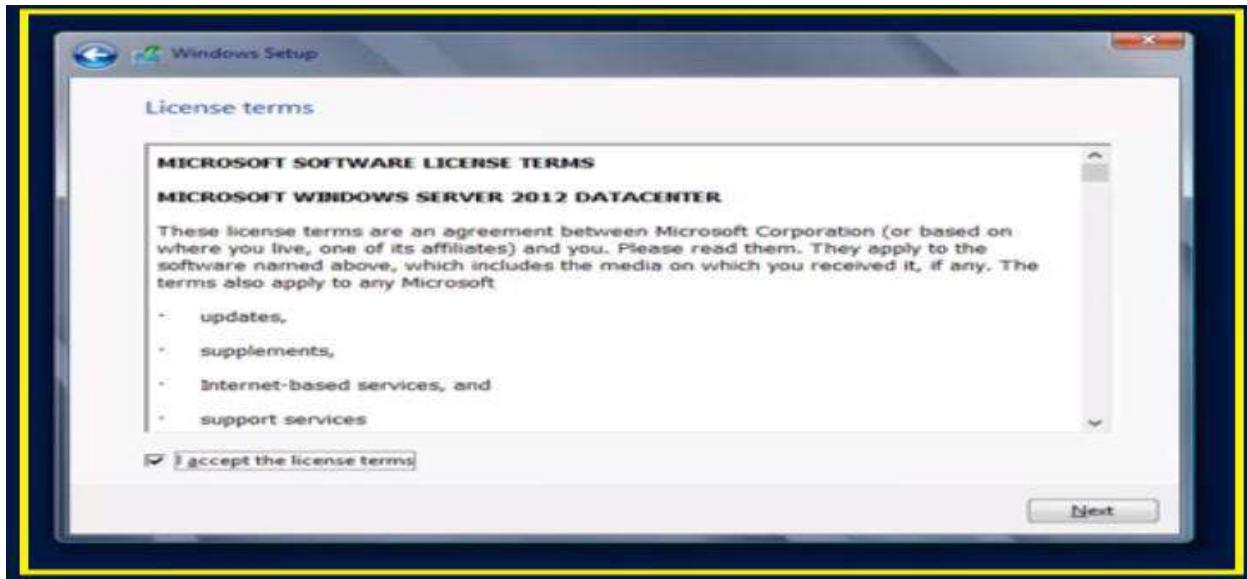


Image 16:Windows Server terms and conditions

12. Select upgrade install etc and it will go to the next page from their select the drive 0 unallocated space and click on next.

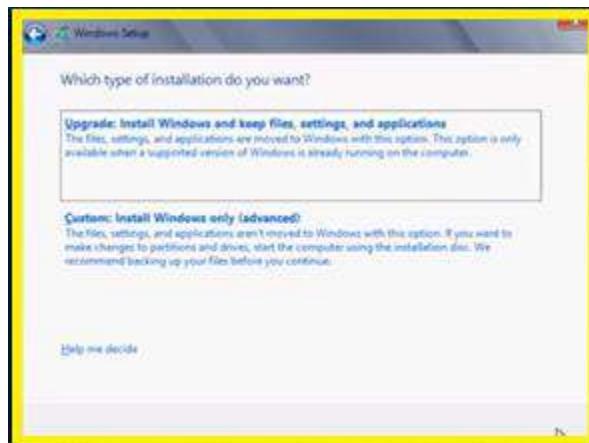


Image 17:Windows Server Update

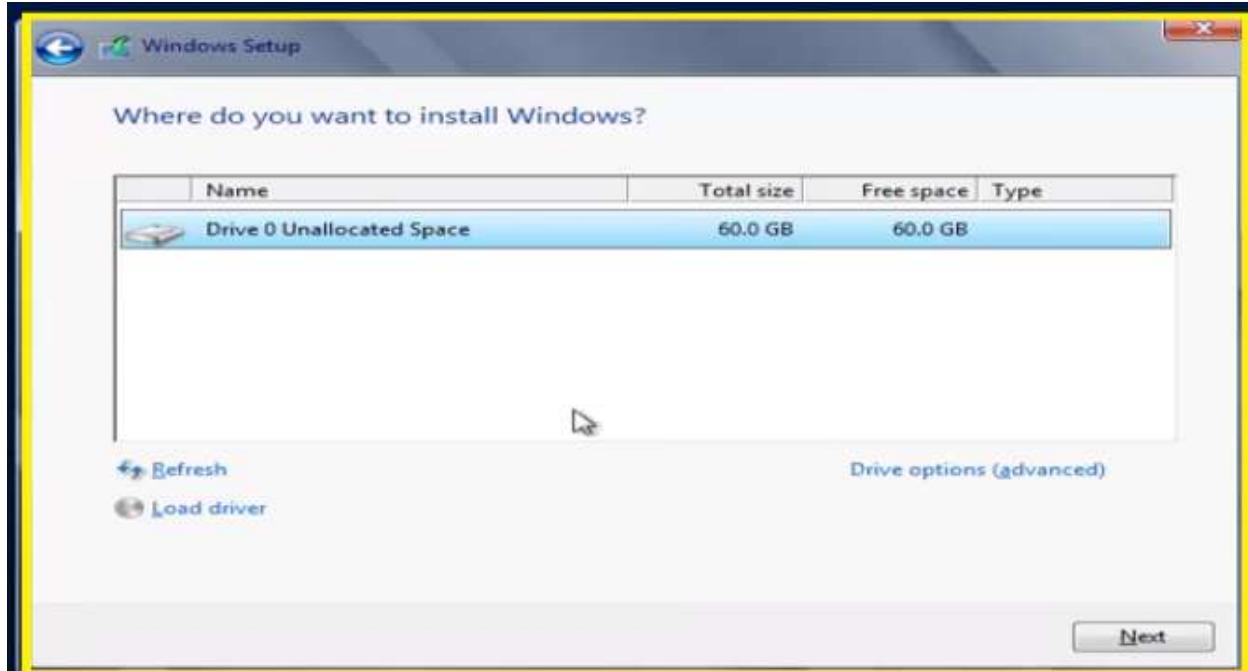


Image 18:Windows Server Installation

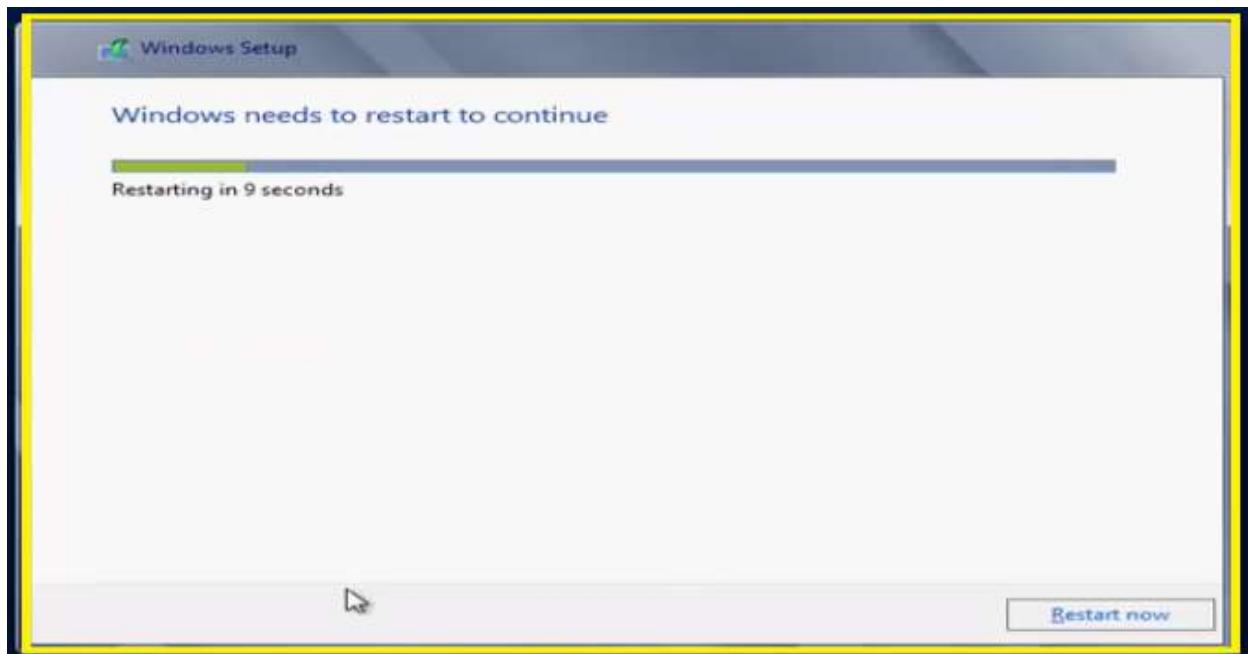


Image 19:Windows Server Setup

-
13. Click on restart now, enter (administration) username and password and click on the finish button.

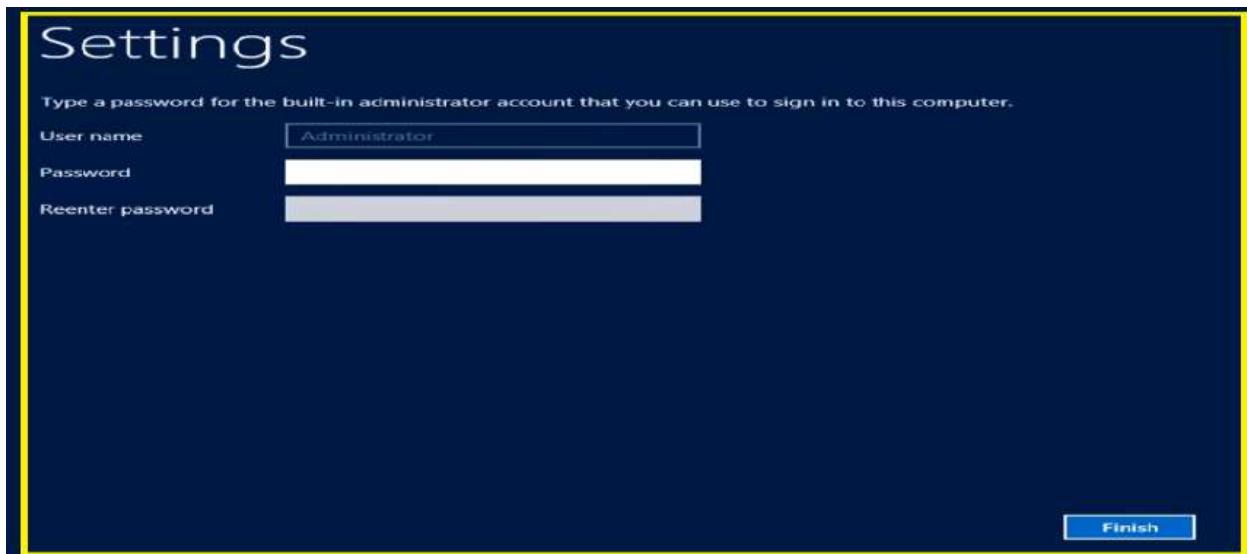


Image 20:Windows Server Login

14. Use administrator username and password to log in. Then press Ctrl+Alt+Delete to the login page.
15. Again, enter the password which you logged in before. Finally, the server web page will be displayed.

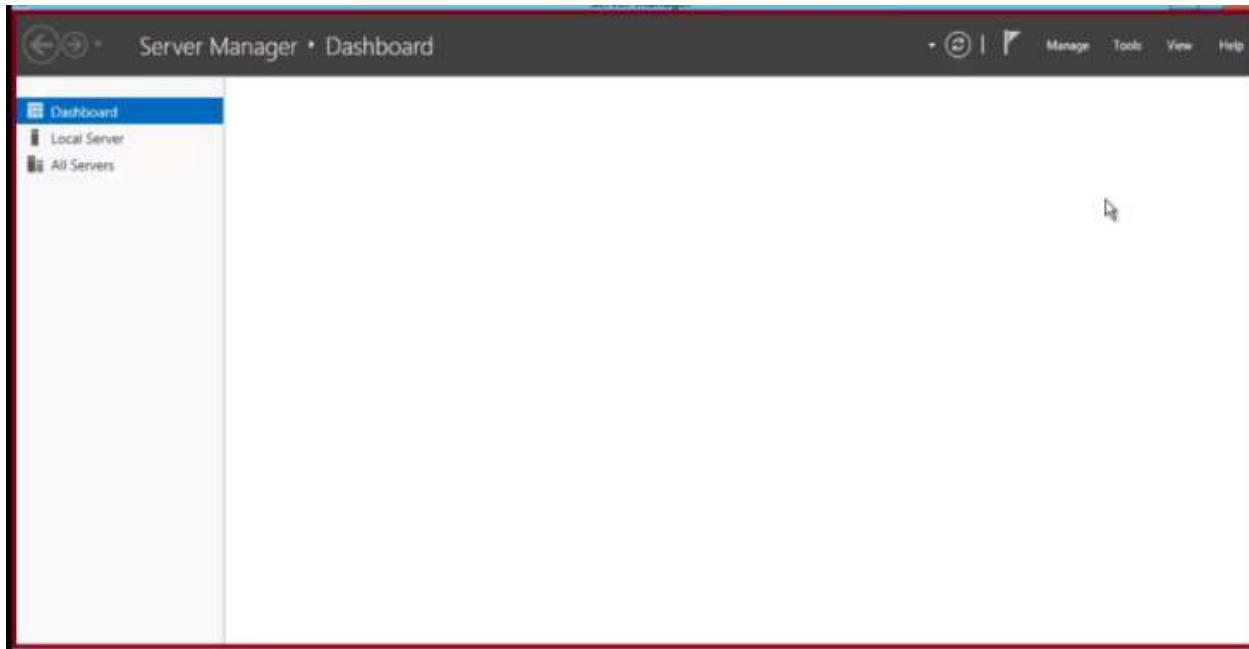


Image 21:Windows Server Home

Output/Results snippet:

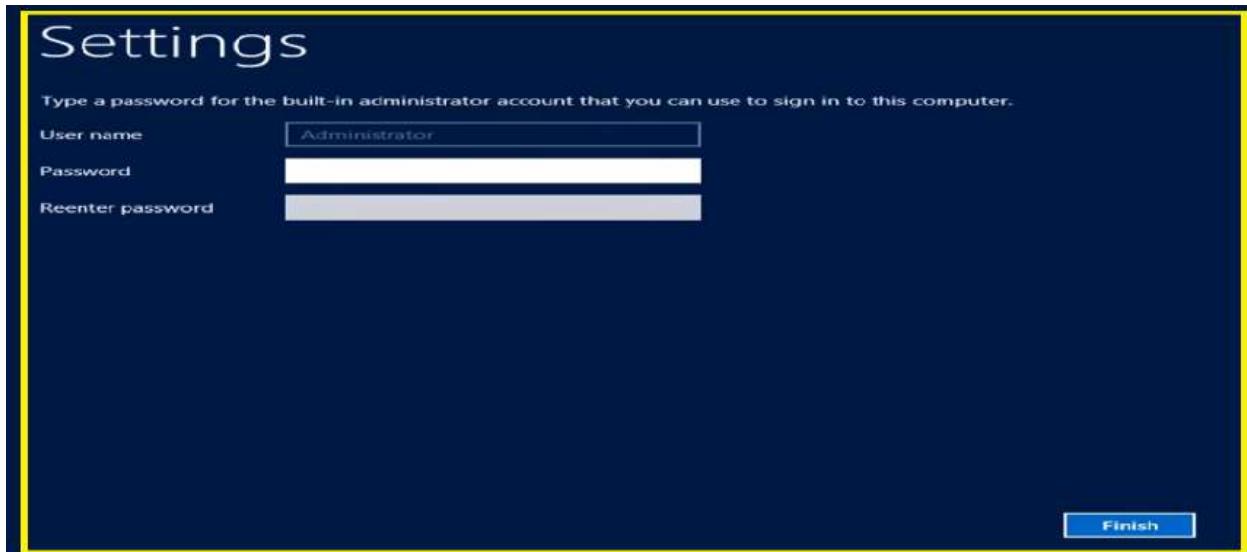


Image 22:Windows Server Login

References:

- <https://docs.microsoft.com/en-us/windows-server-essentials/install/install-and-configure-windows-server-essentials-or-windows-server-essentials-experience>
- <https://hostadvice.com/how-to/how-to-install-and-configure-windows-server-2019-and-project-honolulu/>

Activity 3

Aim: Configure a Server as Web Server.

Learning outcome: Able to understand and configure server environment and backup services.

Duration: 5 hour

List of Hardware/Software requirements:

1. **Special hardware requirements:** none.
2. **Special software requirements:** none.
3. **Internet access:** High-speed connection (greater than 28,800 BPS).

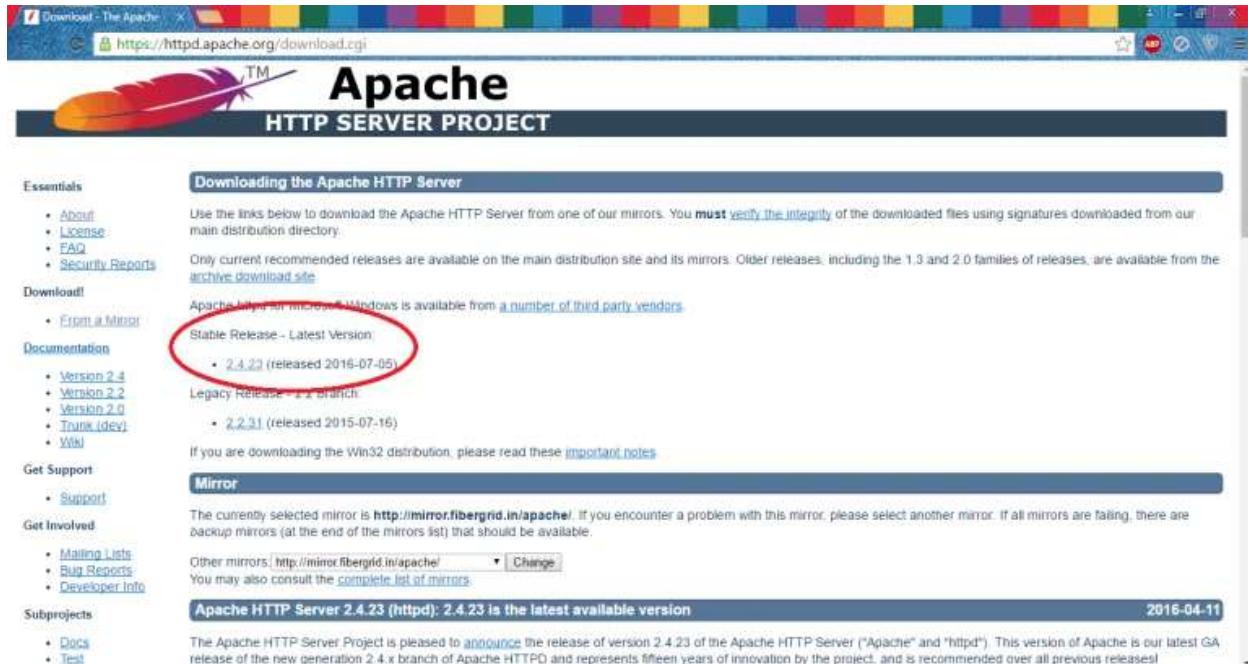
Code/Program/Procedure :

The Apache HTTP Server is an extensively used web server software. The Apache HTTP Server is an open-source software that can be run on several operating systems, including Windows. In this section, let us understand how to install the Apache web server on your Windows Computer.

Step 1.

- Apache is a software, so we have to download it, visit the site:

<https://httpd.apache.org/download.cgi>



The screenshot shows the Apache HTTP Server Project download page. The URL in the address bar is <https://httpd.apache.org/download.cgi>. The main content area features the Apache logo and the text "Apache HTTP SERVER PROJECT". On the left, there's a sidebar with links for Essentials, Download, Documentation, Get Support, and Get Involved. The "Download" section has a sub-section for "From a mirror". The "Documentation" section lists "Version 2.4", "Version 2.2", "Version 2.0", "Trunk (dev)", and "Wiki". The "Get Support" section has a "Support" link. The "Get Involved" section has links for "Mailing Lists", "Bug Reports", and "Developer Info". The "Subprojects" section has links for "Docs", "Test", and "Build". The main content area has a header "Downloading the Apache HTTP Server". It instructs users to verify the integrity of downloaded files using signatures. It notes that only current recommended releases are available on the main distribution site and its mirrors. Older releases, including the 1.3 and 2.0 families of releases, are available from the [archive download site](#). Below this, it says "Apache httpd for Windows" is available from third-party vendors. The "Stable Release - Latest Version" section is highlighted with a red circle around the link to "2.4.23 (released 2016-07-05)". It also lists "Legacy Release - 2.2 Branch" with a link to "2.2.21 (released 2015-07-16)". A note says if you're downloading the Win32 distribution, read the [important notes](#). The "Mirror" section shows the currently selected mirror as <http://mirror.fibergid.in/apache/>, with a "Change" button and a link to the "complete list of mirrors". At the bottom, a banner says "Apache HTTP Server 2.4.23 (httpd): 2.4.23 is the latest available version" and "2016-04-11". A note at the bottom states that the Apache HTTP Server Project is pleased to announce the release of version 2.4.23 of the Apache HTTP Server ("Apache" and "httpd"). This version of Apache is our latest GA release of the new generation 2.4.x branch of Apache HTTPD and represents fifteen years of innovation by the project, and is recommended over all previous releases.

- Click on the latest stable release

Step 2.

- You want the binaries, click on it.



Step 3.

- Now go to ‘win32’ and click on it.



Index of /apache//httpd/binaries

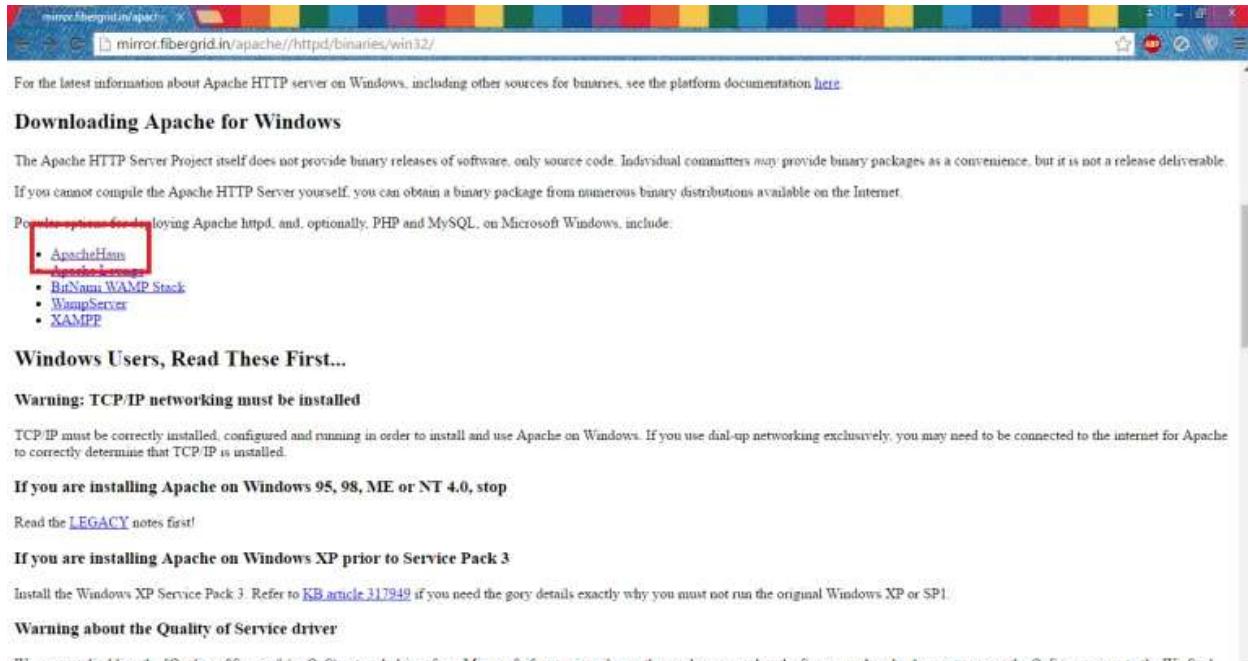
Name	Last modified	Size	Description
Parent Directory		-	HTTP Server project
Netware/	2015-10-15 06:01	-	HTTP Server project
win32/	2015-10-15 06:01	-	HTTP Server project
README.html	2013-11-17 21:53	1.1K	HTTP Server project

Download from your [nearest mirror site!](#)

Please do not download from [www.apache.org](#). This a mirror site to help us serve apache.org bandwidth.

Step 4.

- Scroll down to see ‘ApacheHaus’ , open it.



Windows Users, Read These First...

Warning: TCP/IP networking must be installed

TCP/IP must be correctly installed, configured and running in order to install and use Apache on Windows. If you use dial-up networking exclusively, you may need to be connected to the internet for Apache to correctly determine that TCP IP is installed.

If you are installing Apache on Windows 95, 98, ME or NT 4.0, stop

Read the [LEGACY](#) notes first!

If you are installing Apache on Windows XP prior to Service Pack 3

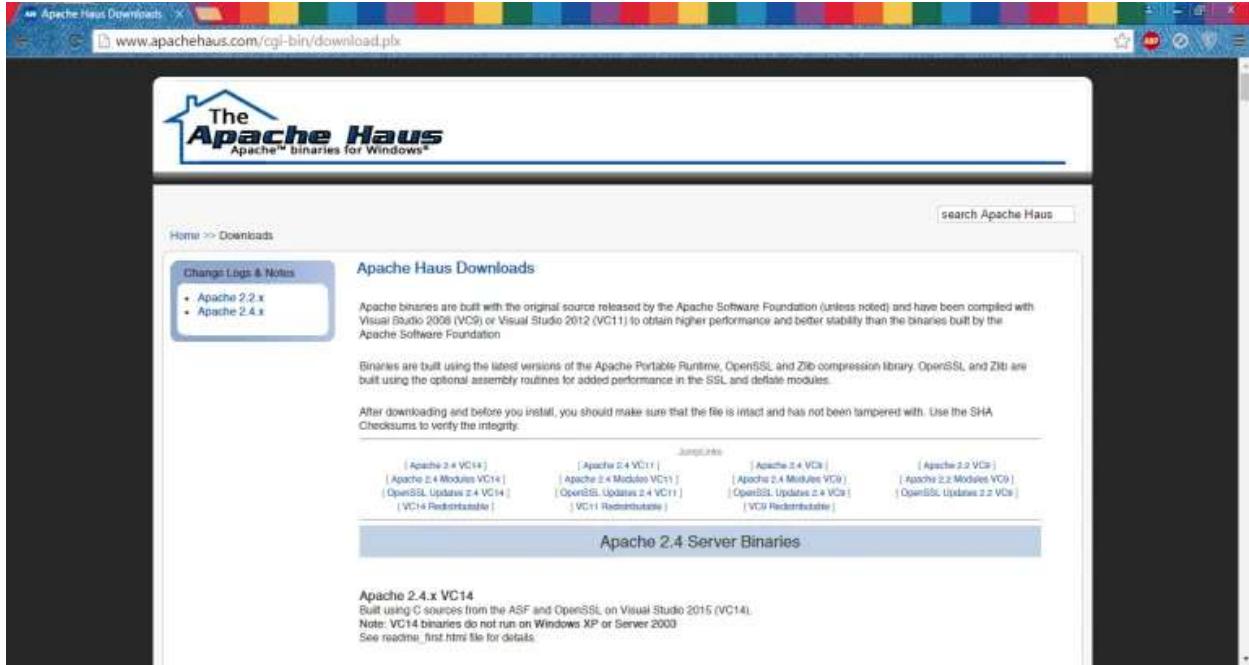
Install the Windows XP Service Pack 3. Refer to [KB article 317949](#) if you need the gory details exactly why you must not run the original Windows XP or SP1.

Warning about the Quality of Service driver

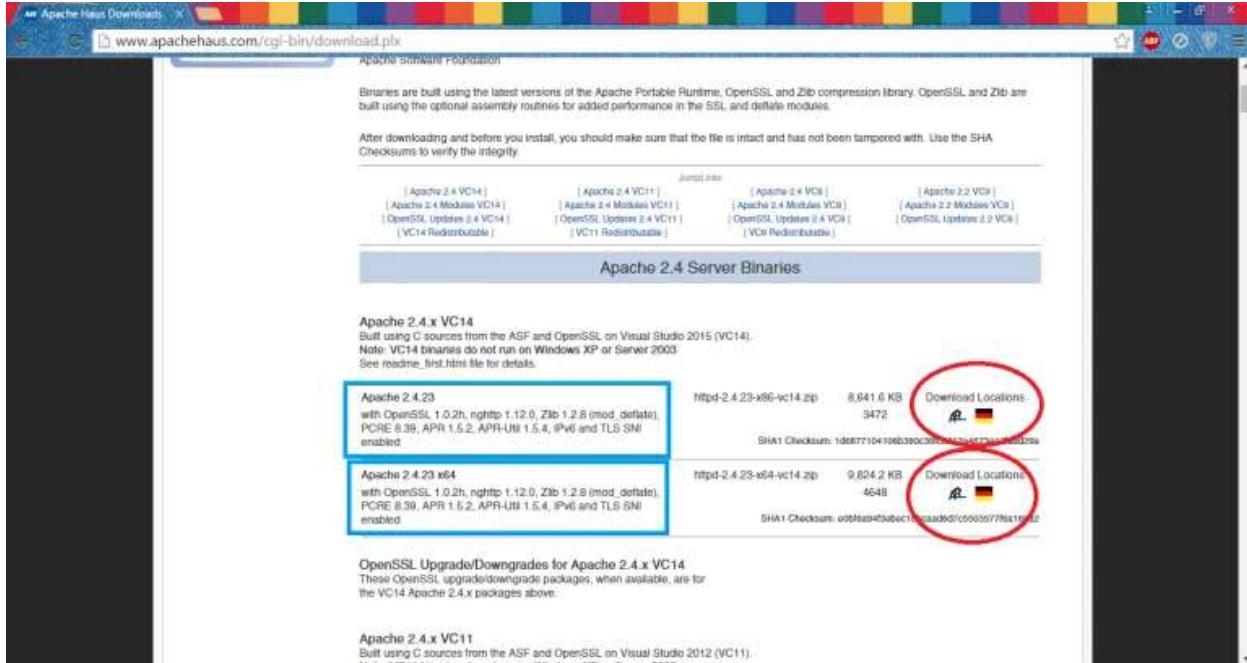
We suggest disabling the "Quality of Service" (or QoS) network driver from Microsoft if you primarily use the machine as an Apache Server, as Apache does not support the QoS extensions to the WinSock API.

Step 5.

- You should have something like this.

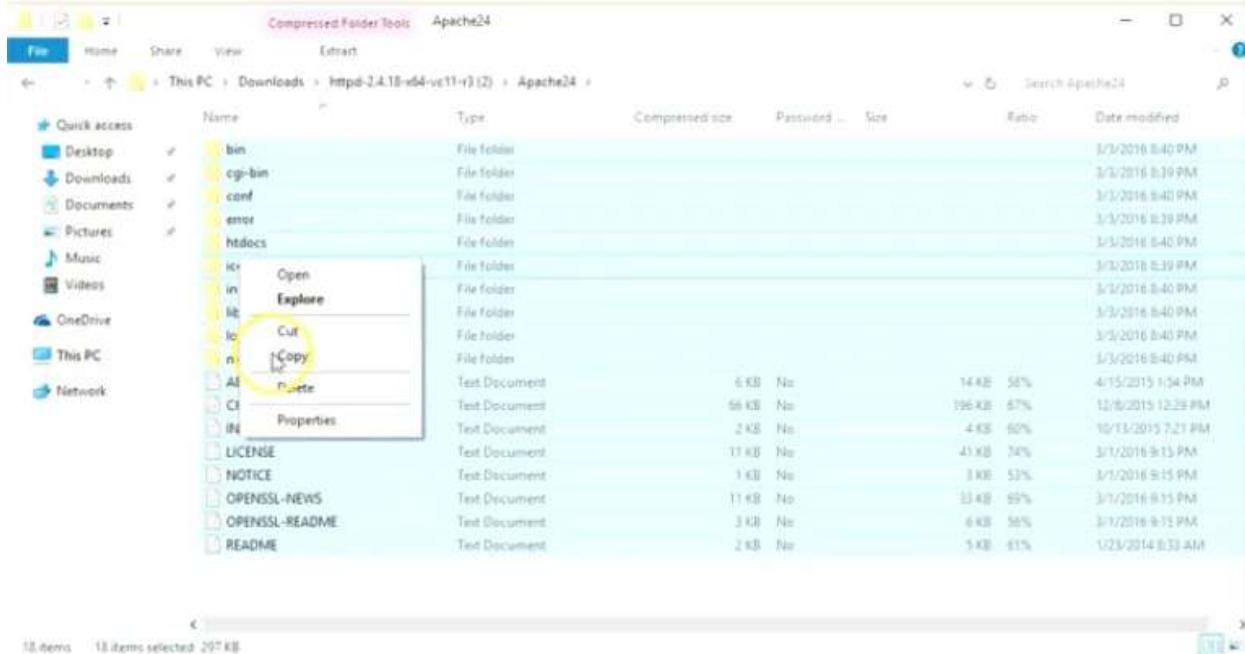


- Scroll down to see the version of Apache in two variations 32 bit and 64 bit (x64) (blue boxes).
- Click on download on whichever one you want (red circles).



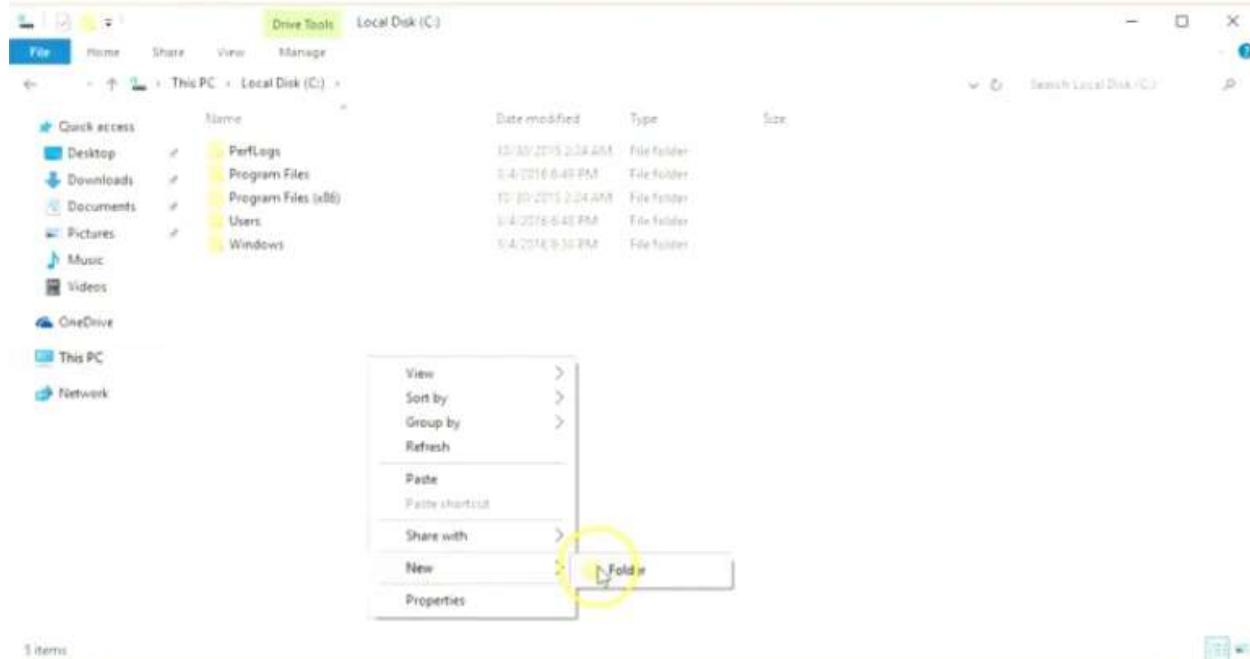
Step 6.

- Open up the downloaded file, then open up the folder with Apache24 on it.
- Copy all the files and folder in it.



Step 7.

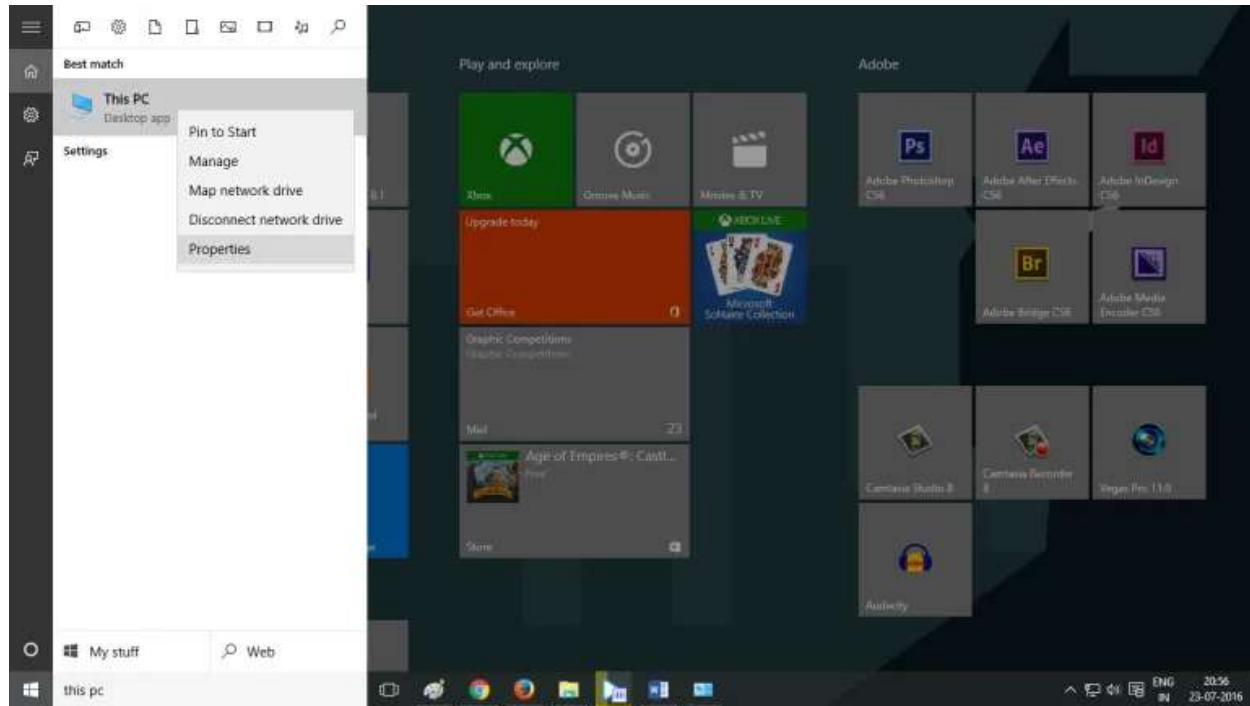
- Make a new folder in any drive and paste the files in a folder named ‘Apache24’.



- Just make sure the address is not much complicated.

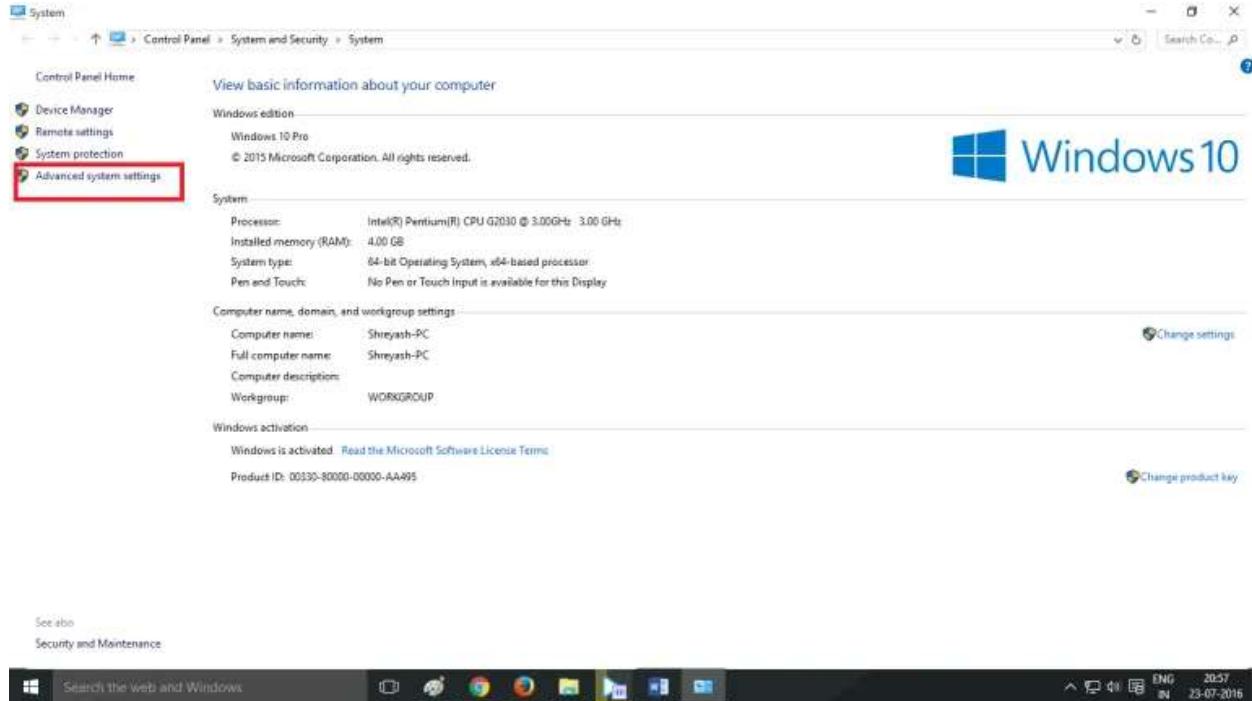
Step 8.

- Open System Properties, by right clicking on 'This PC', then properties.



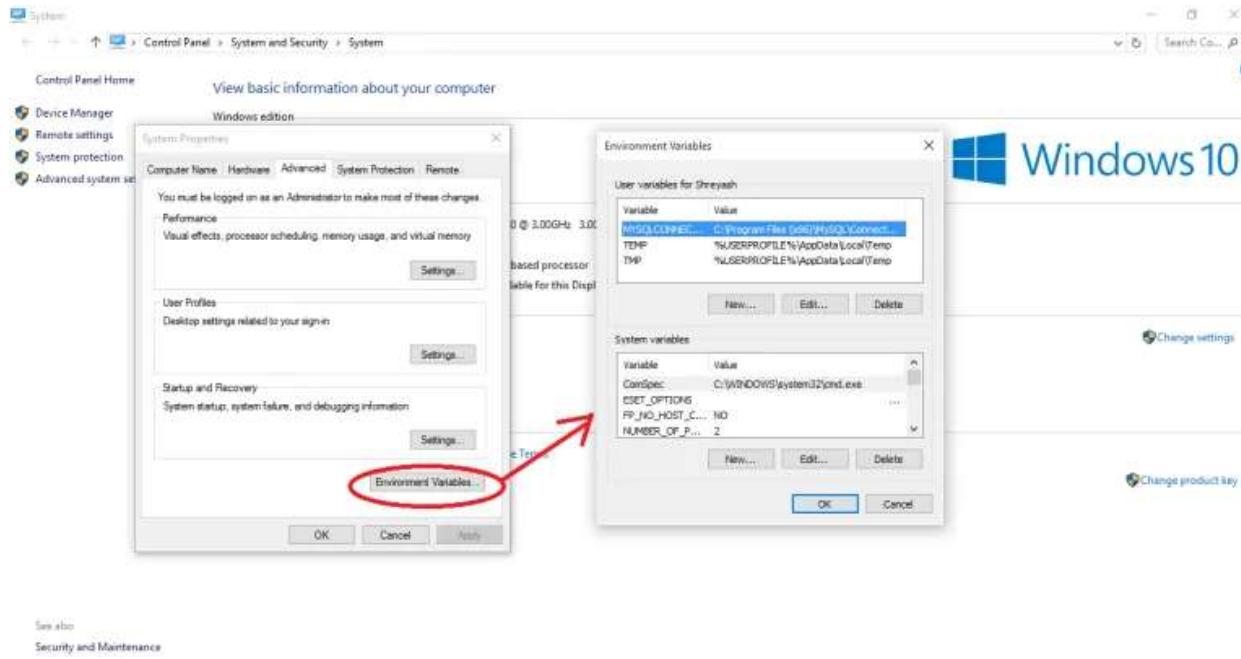
Step 9.

- Open Advanced System Settings.



Step 10.

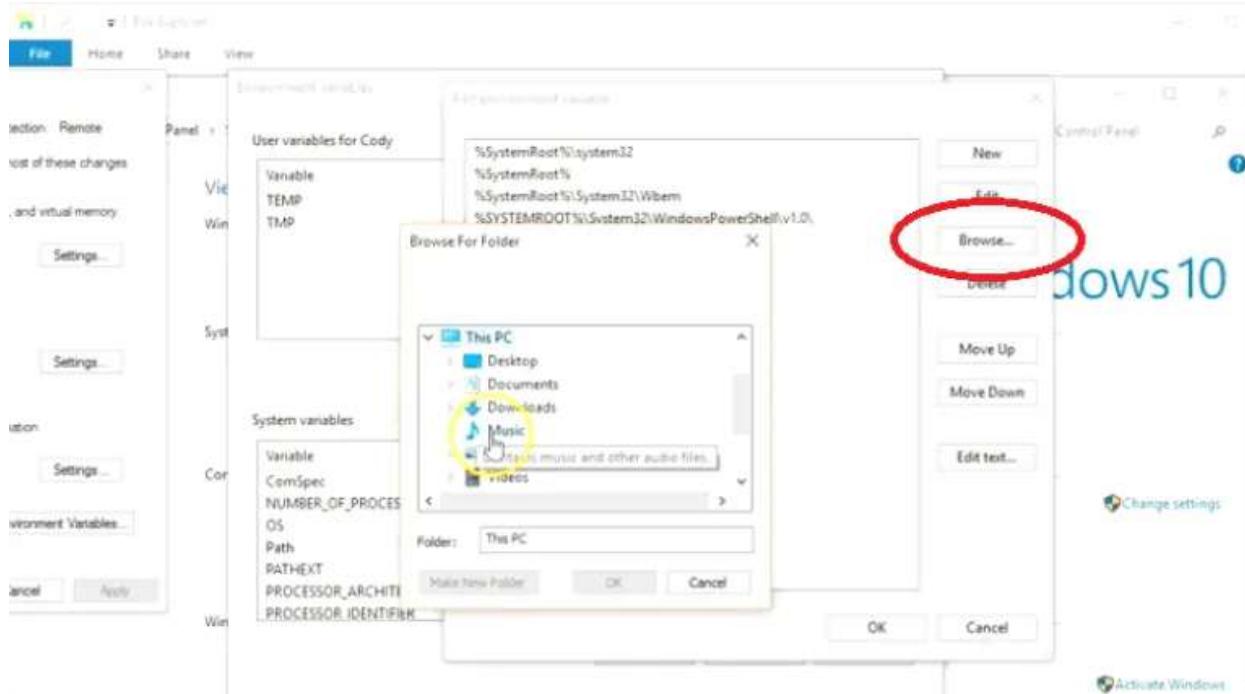
- Click on Environment Variables...



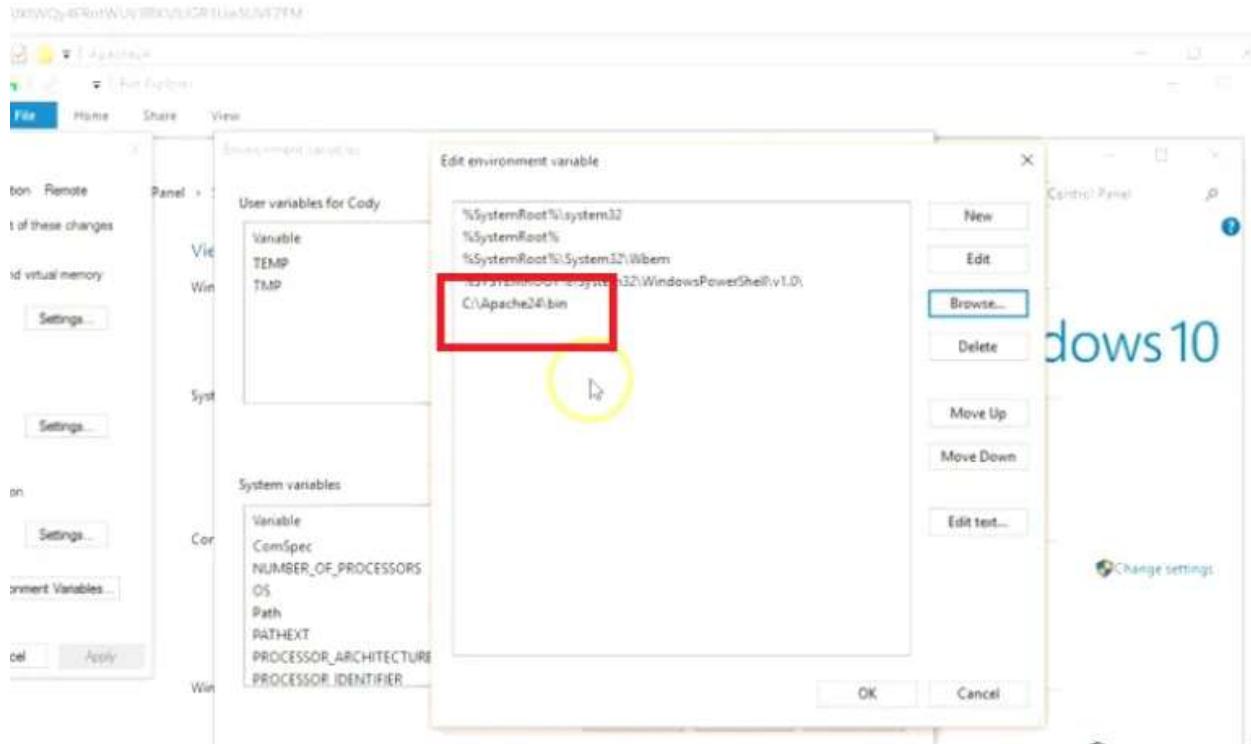
- Double Click on ‘Path’

Step 11.

- Now click on ‘Browse’
- Find the folder you created and select



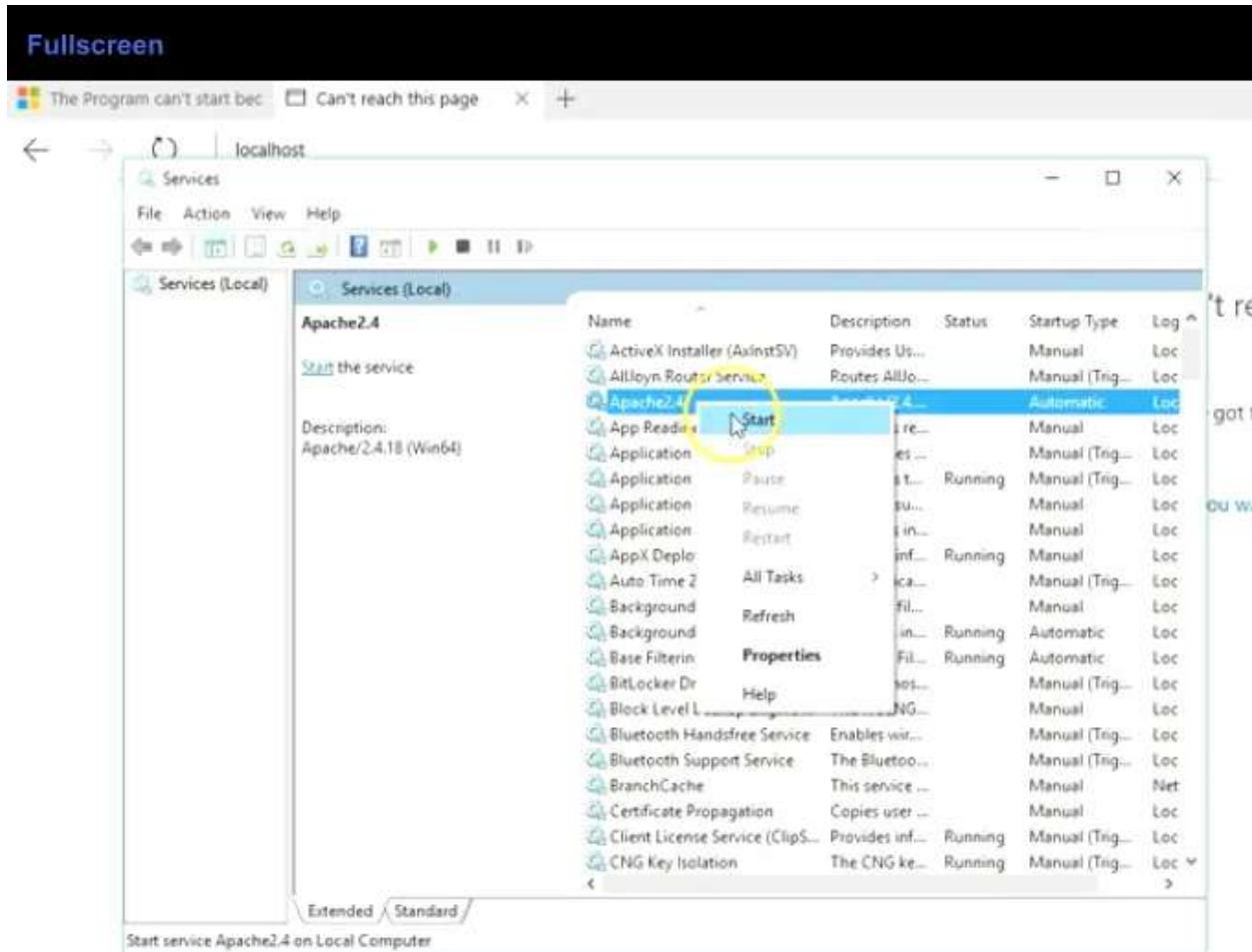
- bin from it and click ok.
- After you've done that it should look like this.



- Now click ok, and the windows will keep closing.
- This has to be done because the Web Server's daemon runs as a Service on windows.

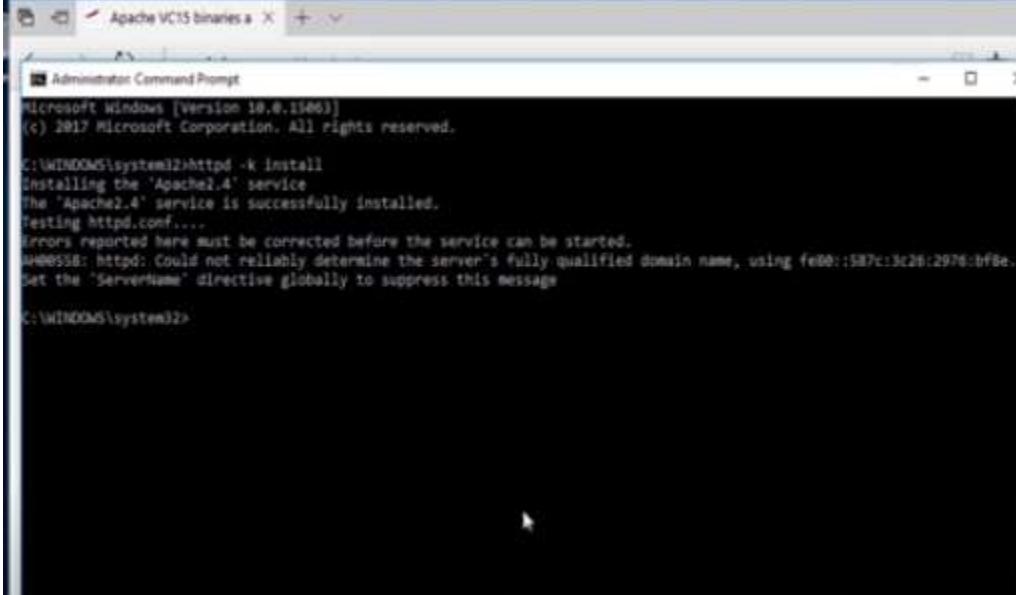
Step 12.

- Press win+R, or open Run.
- Write
- services.msc
- Find the 'Apache' service, right click on it and press start.



Step 13.

- Open Command Prompt as Admin, and write
- httpd -k install

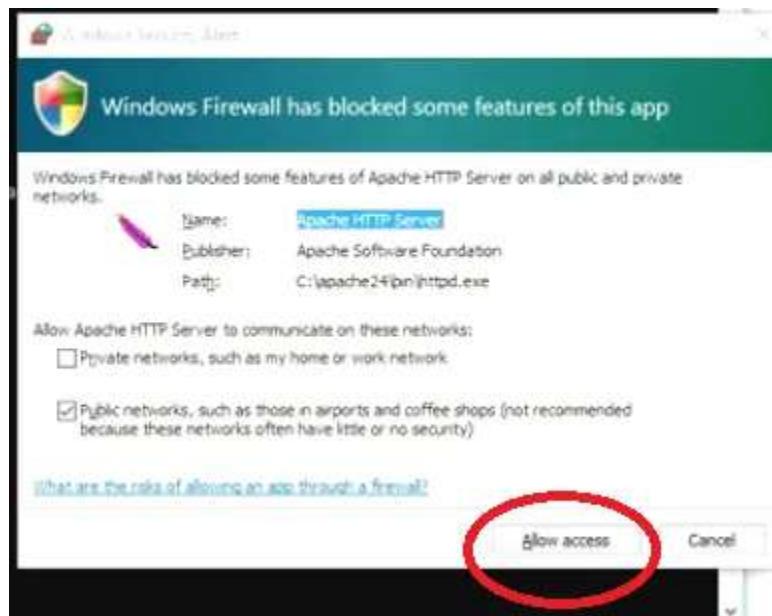


```
Administrator Command Prompt
Microsoft Windows [version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>httpd -k install
Installing the 'Apache2.4' service
The 'Apache2.4' service is successfully installed.
Testing httpd.conf....
Errors reported here must be corrected before the service can be started.
AH00551: httpd: Could not reliably determine the server's fully qualified domain name, using fe80::587c:3c26:2976:bff8e.
Set the 'ServerName' directive globally to suppress this message

C:\WINDOWS\system32>
```

- When the window pops “Allow Access”



Check

- Open up any browser and write “localhost”, the window below should appear.



You are done!!

Output/Results snippet:



Image 35:Apache Installation Finished

References:

- <https://opensource.com/article/18/2/how-configure-apache-web-server>
- <https://www.servermania.com/kb/articles/how-to-quickly-setup-your-own-web-server>

Activity 4

Aim: Configure Mailbox Server

Learning Outcome: Able to Configure Mailbox Server in windows server 2012 (or) 2016

Duration: 2 Hrs

Procedure

Installing the SMTP feature

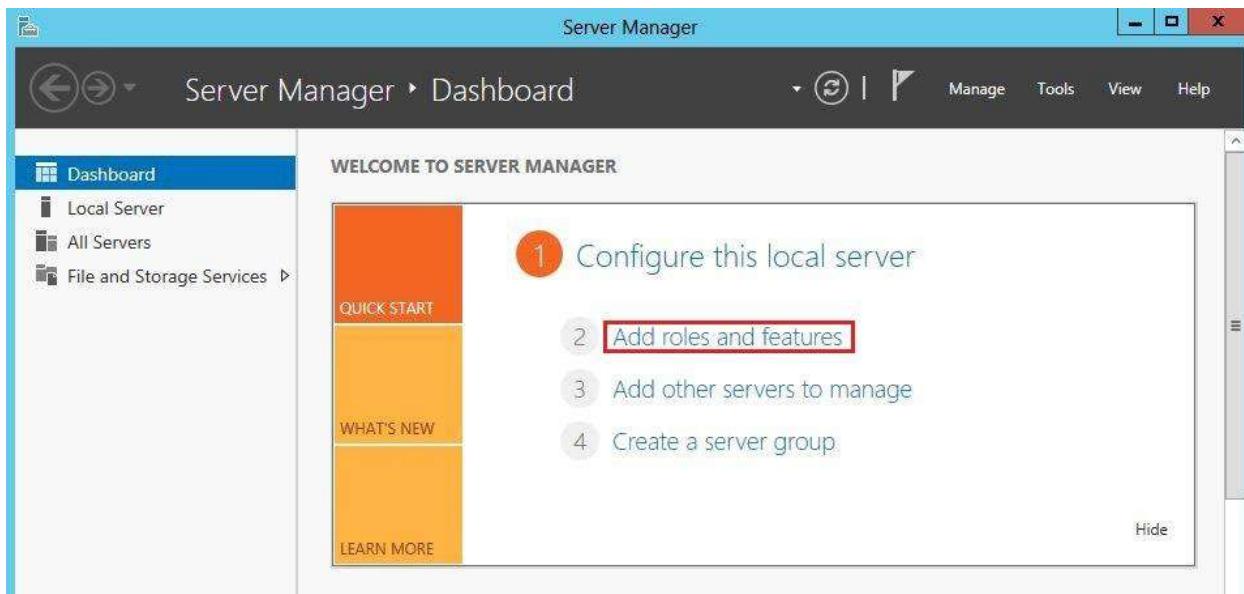
Step 1: Click on the Server Manager icon in the bottom left-hand corner to load the Server Manager Dashboard:



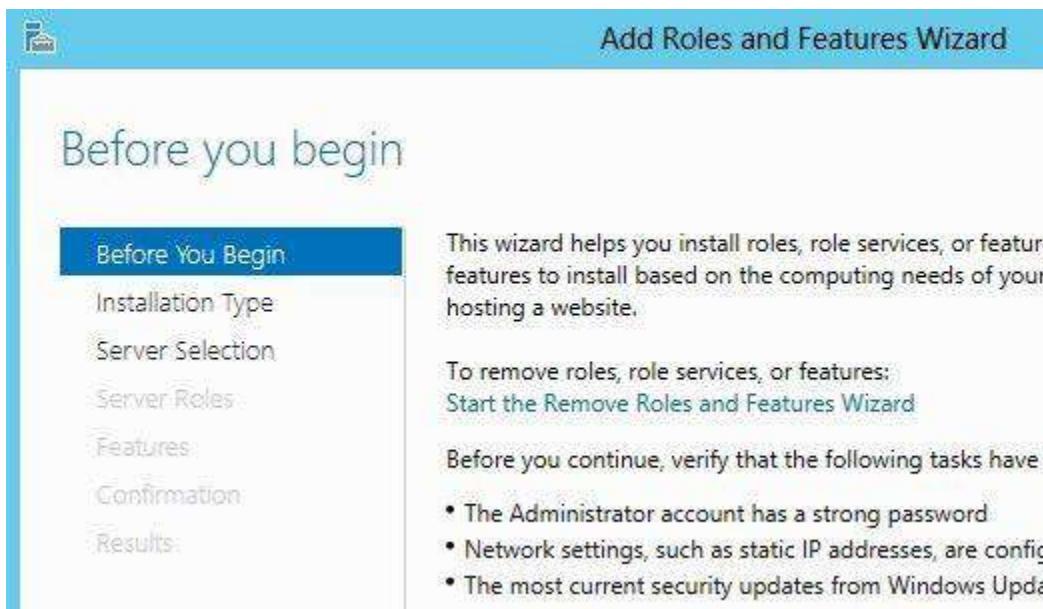
Alternatively, click on the Powershell icon to its right and enter servermanager.exe at the prompt to load the Server Manager Dashboard:

```
PS C:\Users\Admin> servermanager.exe
```

Step 2: When the Server Manager Dashboard loads, click on Add roles and features in the center pane as highlighted below:



The Add Roles and Features Wizard will load, click Next to go past the initial Before You Begin Page:



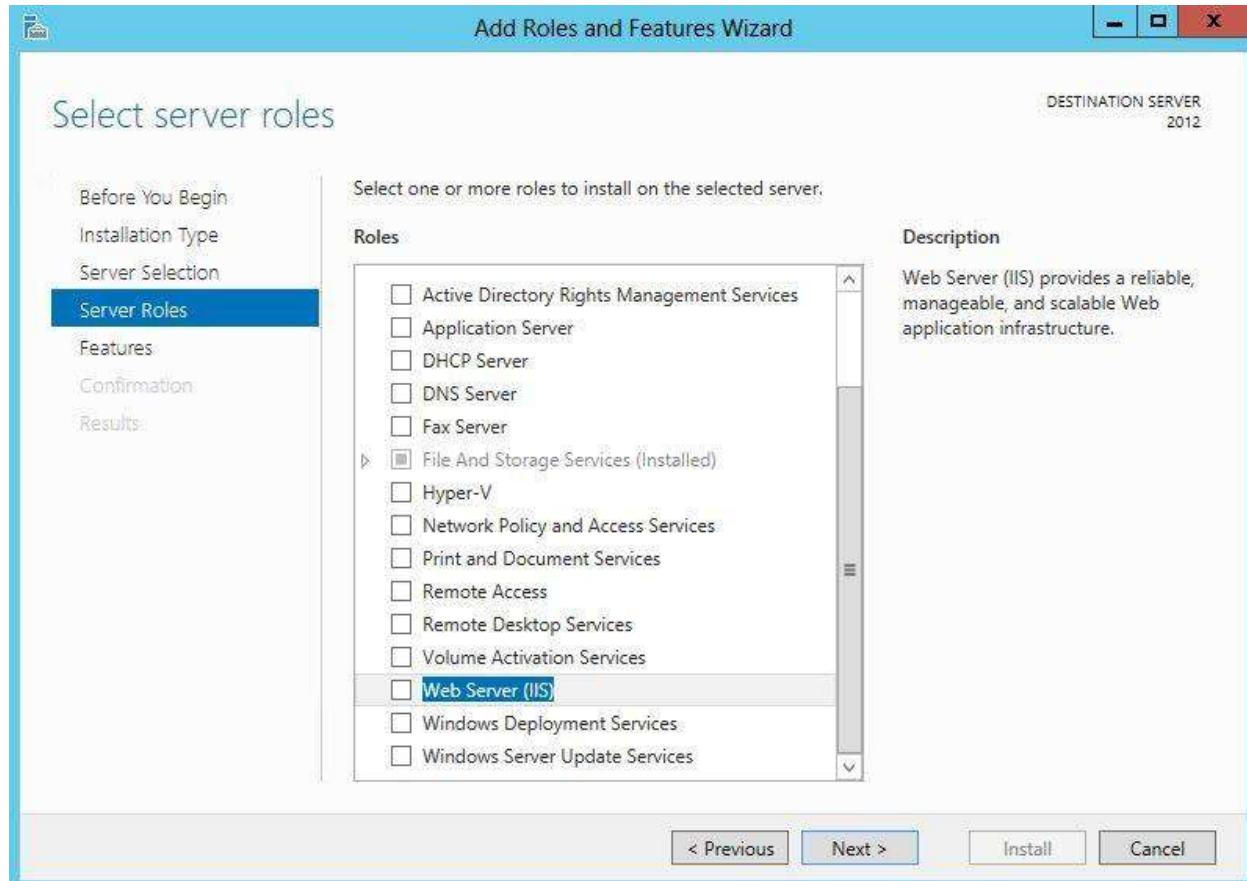
Step 3: In the Installation Type section, select Role-based or feature-based installation and click Next:



Step 4: In the Server Selection section, select your server, in my example below, my server is called 2012, then click next to proceed:



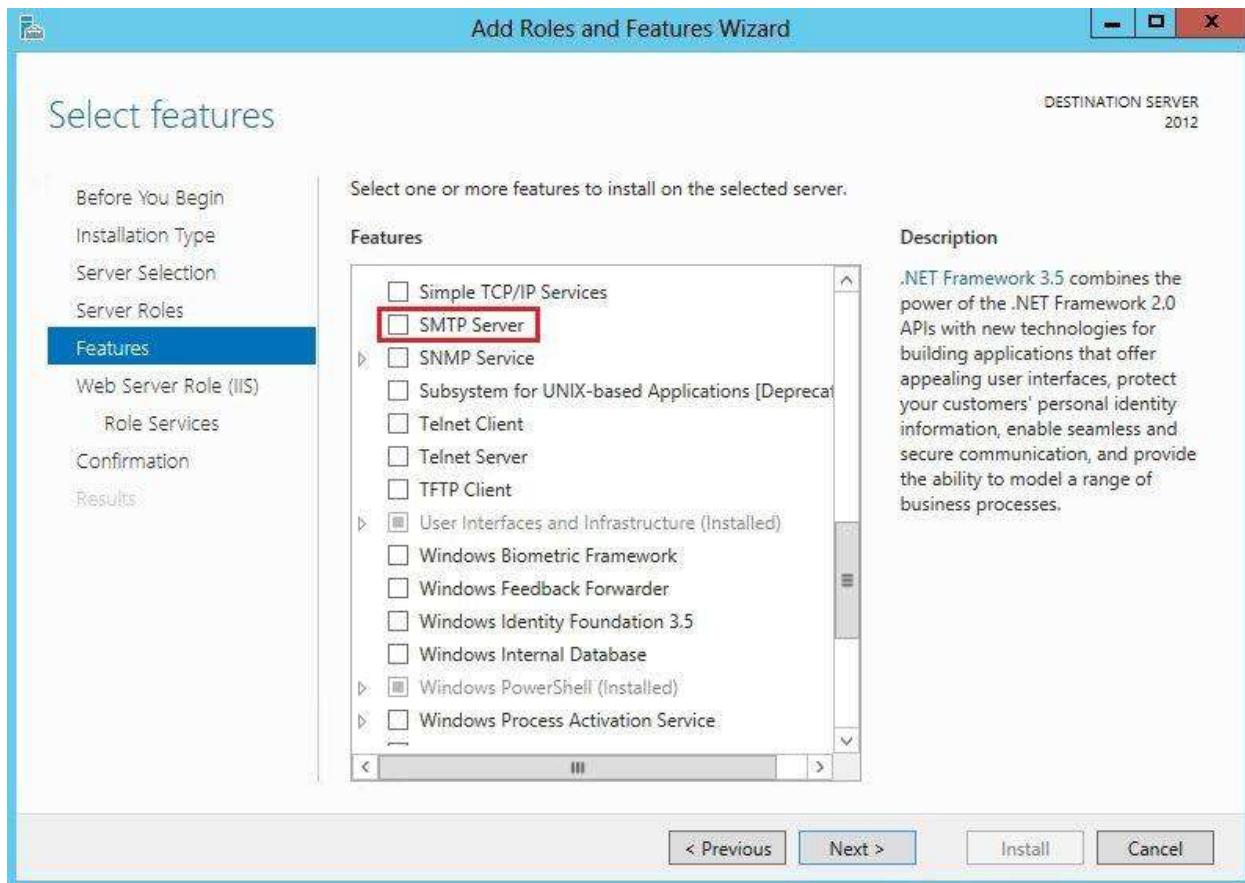
Step 5: In the Server Roles section select Web Server (IIS) as highlighted below and click Next:



Doing so will initiate a prompt to install the required IIS Management Console. Ensure you check the Include management tools (if applicable) box per the below and click Add Features to proceed:



Step 6: In the Features section, select the SMTP Server feature then click Install to proceed:



You will prompt to install services and features required by the SMTP Server. Ensure you check the Include management tools (if applicable) box per the below and click Add Features to proceed:



Include management tools (if applicable)

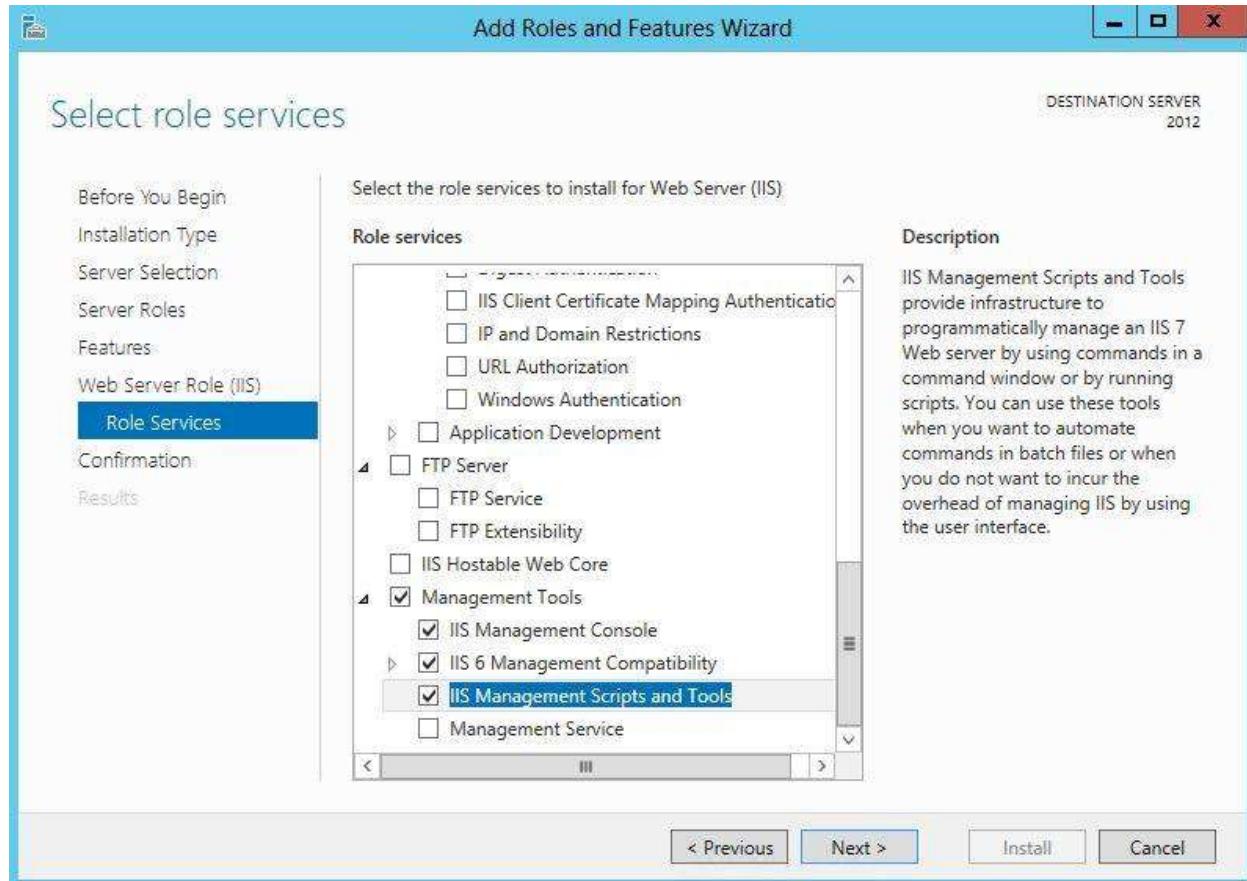
Add Features

Cancel

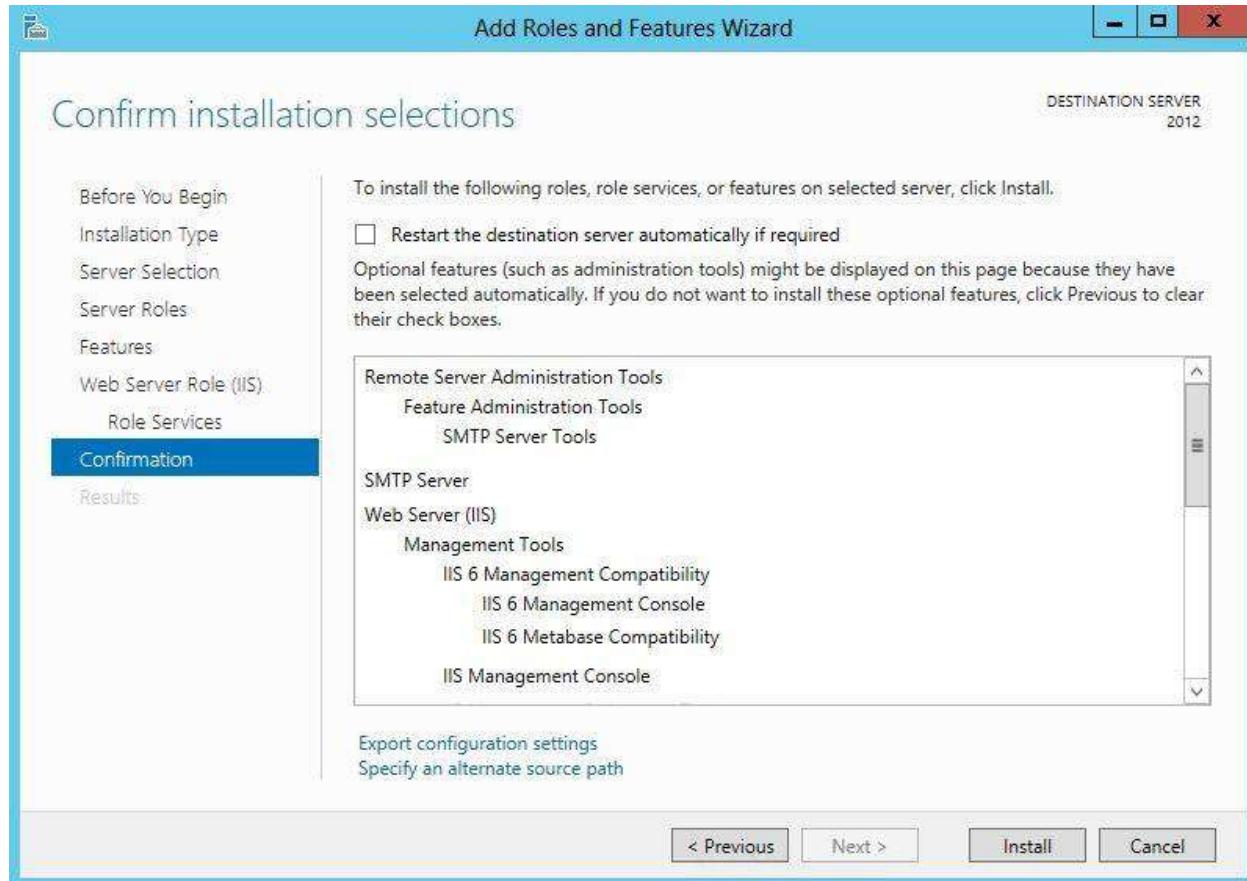
Step 7: You will now be presented with the Web Server Role (IIS) section. Click Next to proceed:



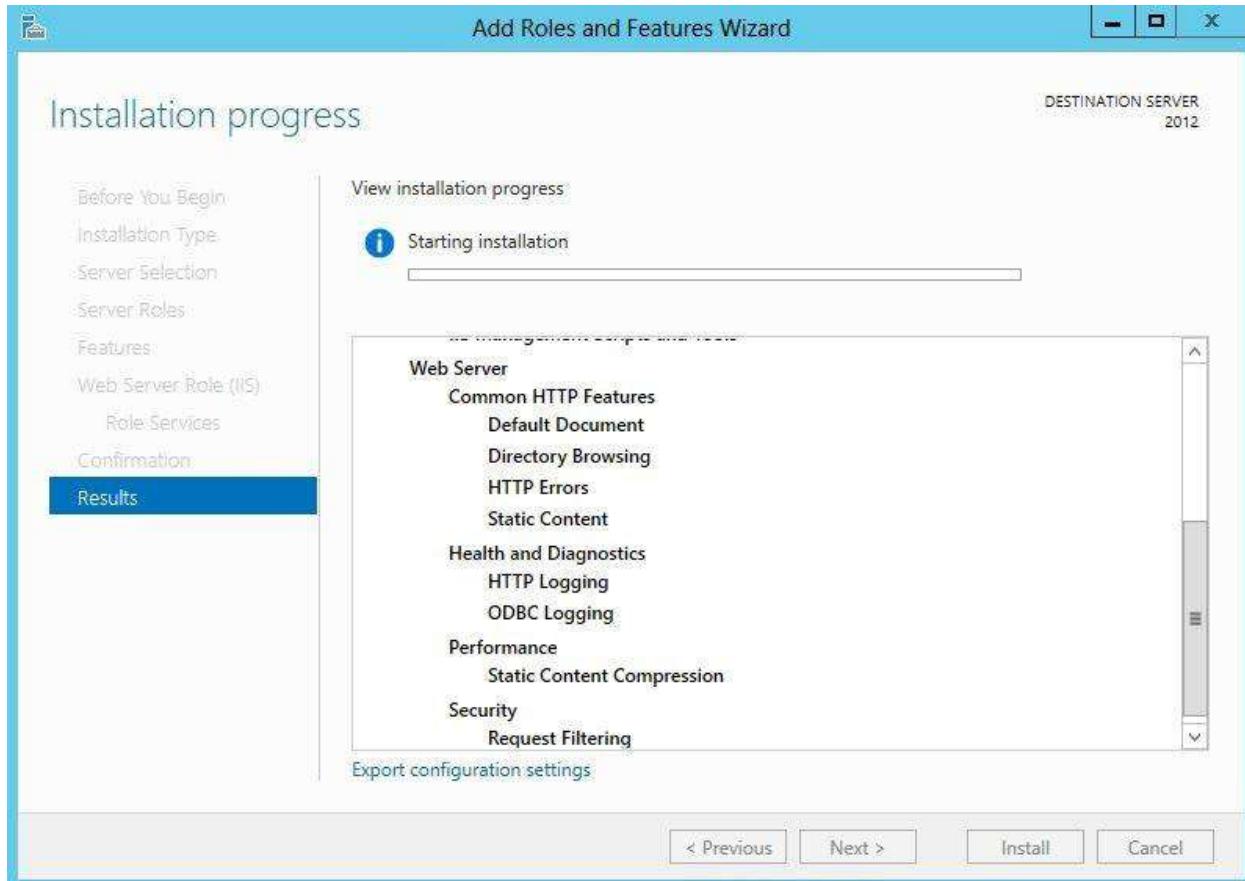
In the Role Services section, scroll down and under Management Tools select the services to match those checked in screenshot below then click Next to proceed:



Step 8: The Confirmation section will show all the role and feature configuration options you previously selected:



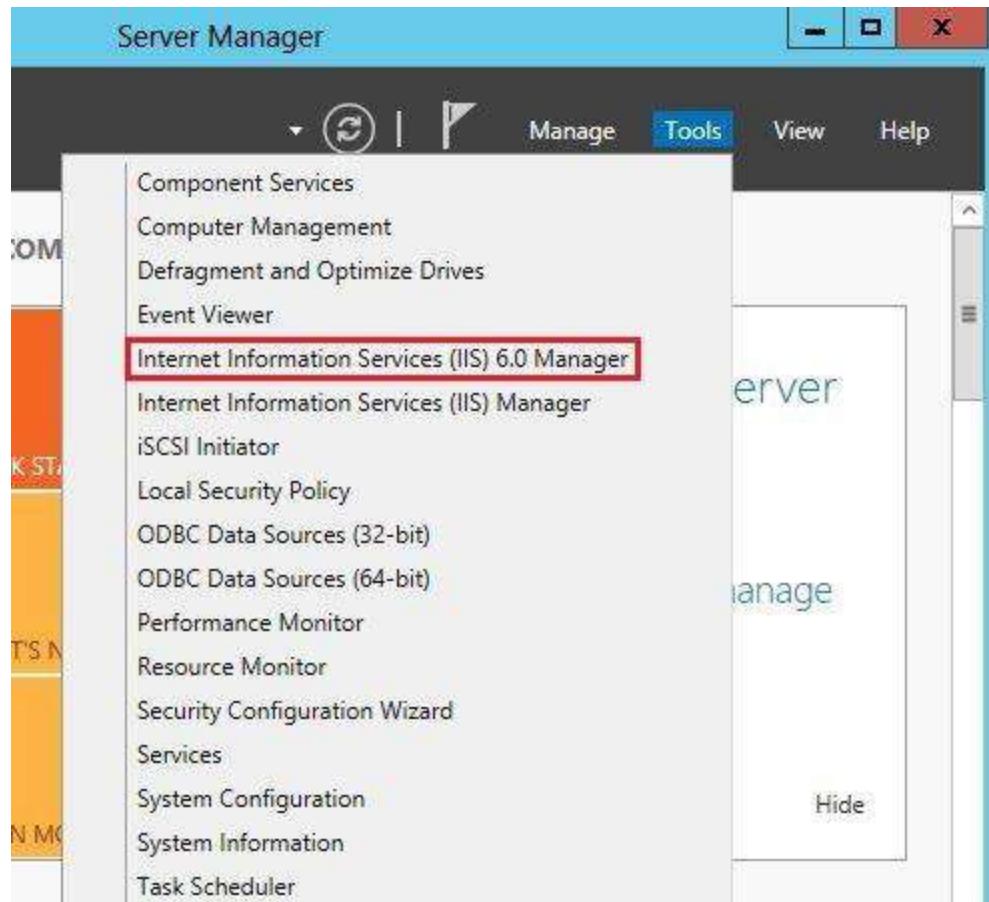
Click Install to start the installation:



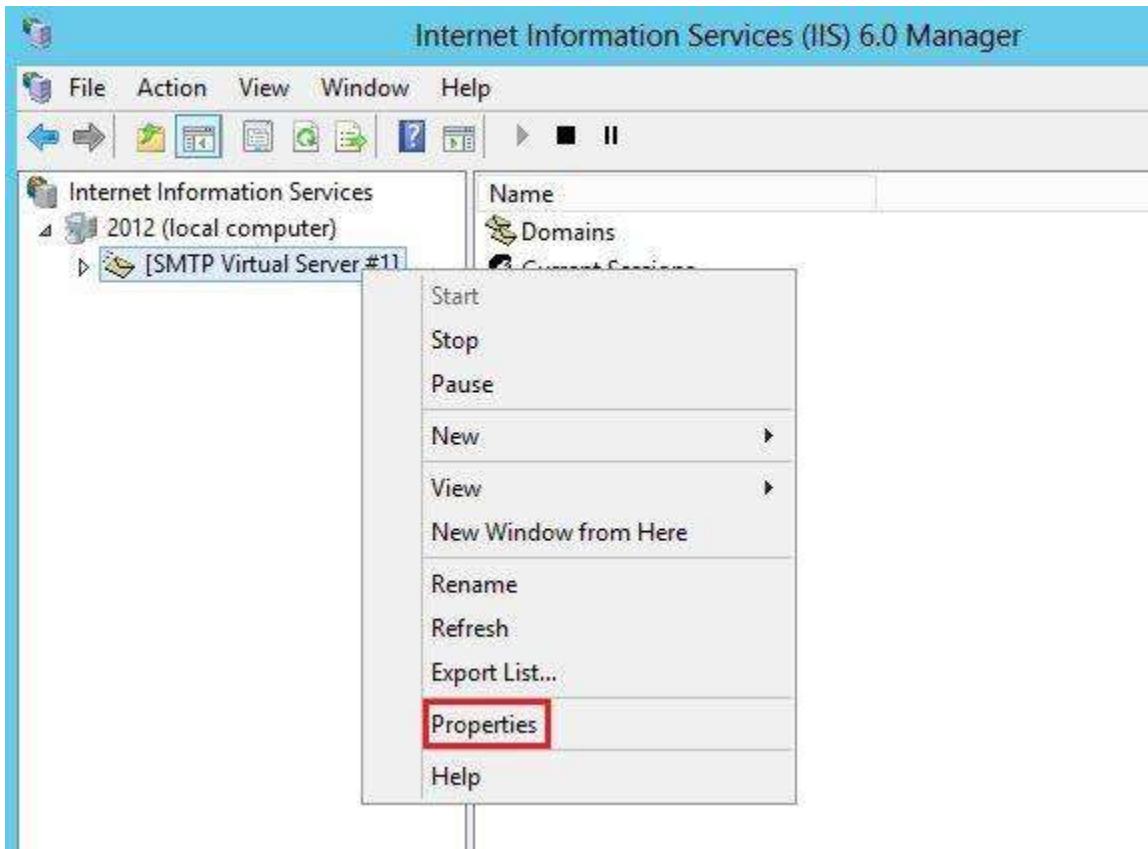
The installation should complete shortly. You may need to reboot your server to fully complete the installation.

Configuring the SMTP Server

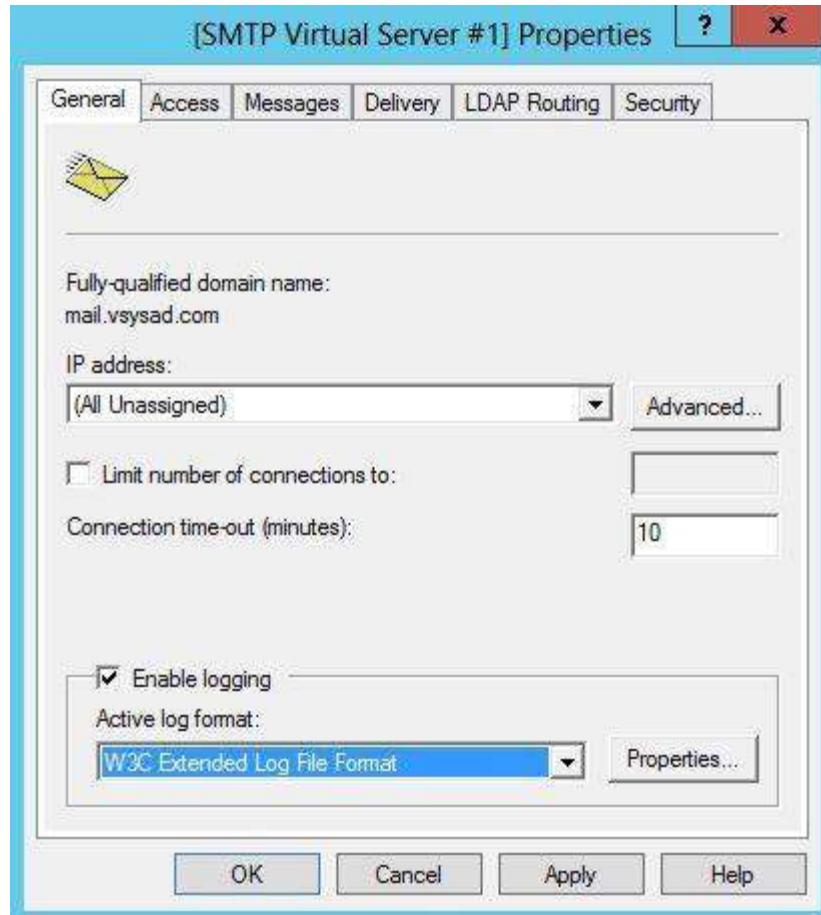
The next step is to configure SMTP. To do so we will need to open Internet Information Services (IIS) Manager 6. 10. Click on the Server Manager icon per step 1 to load the Server Manager Dashboard. Then click Tools and then click on Internet Information Services (IIS) 6.0 Manager to load IIS Manager 6:



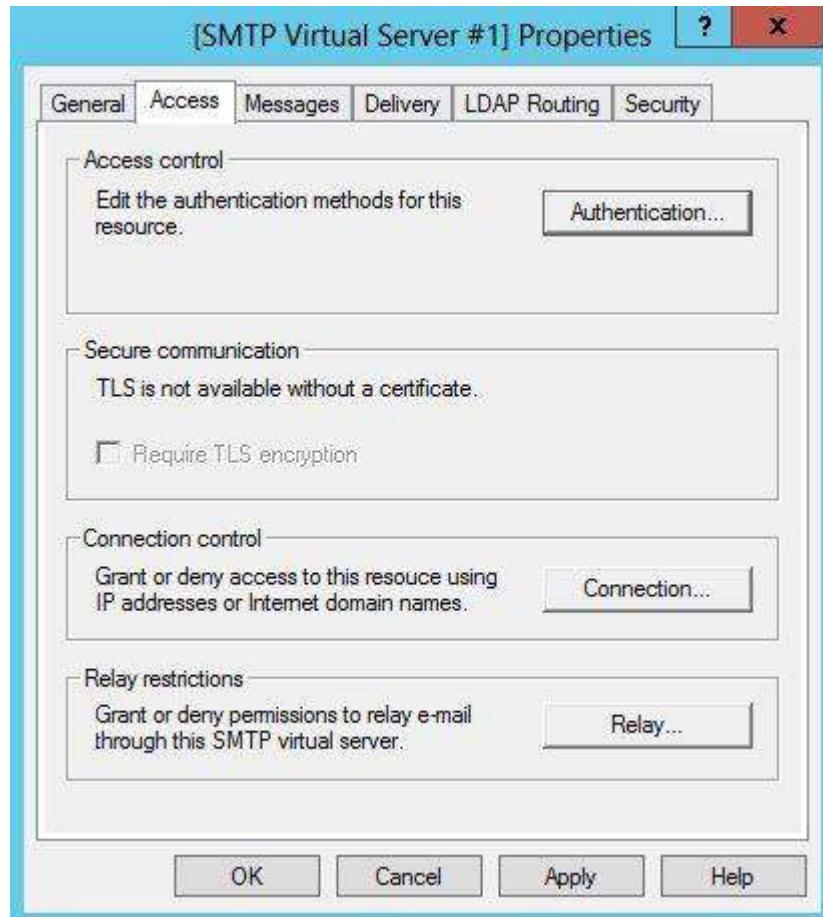
Step 9: In IIS 6 Manager, expand the server name, in my example below it is 2012, then right-click on SMTP Server and select Properties:



Step 10: In the General tab, unless you want the SMTP Server to use a specific IP address, leave the settings as they are so that the IP address is set to (All Unassigned):



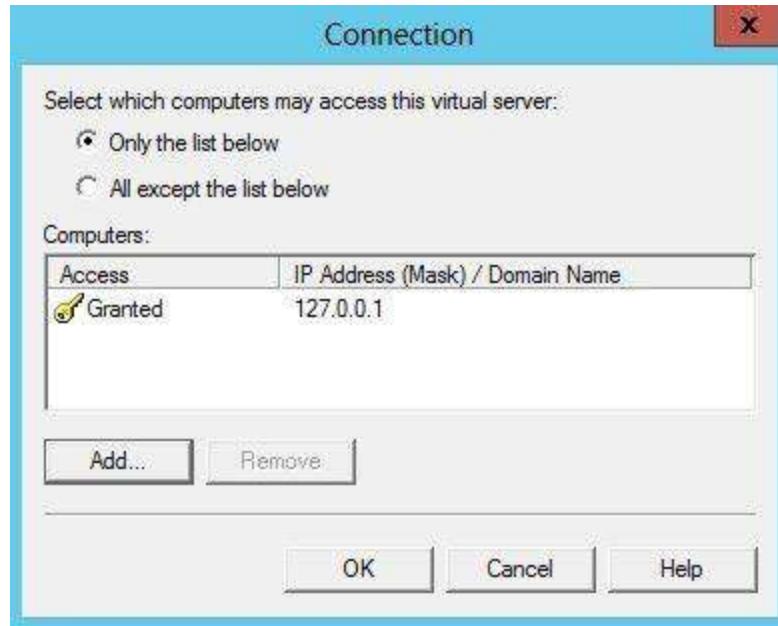
Step 11: To proceed, click on the Access tab:



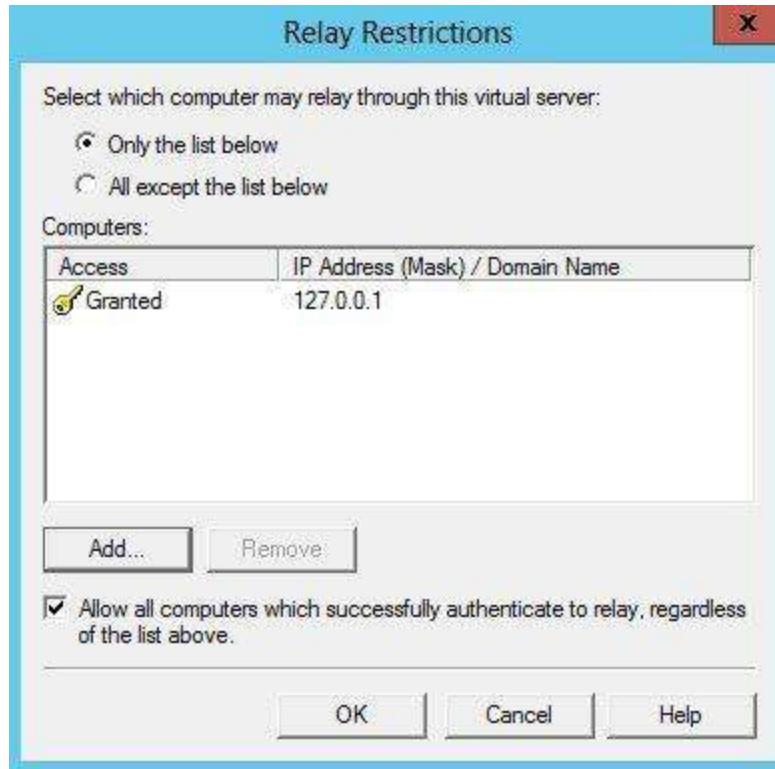
Step 12: Click on the Authentication button and ensure Anonymous access is checked and then click OK:



Step 13: Once back in the Access tab, click on the Connection button. Select only the list below and then click Add. Enter 127.0.0.1 as the IP address and then click OK:

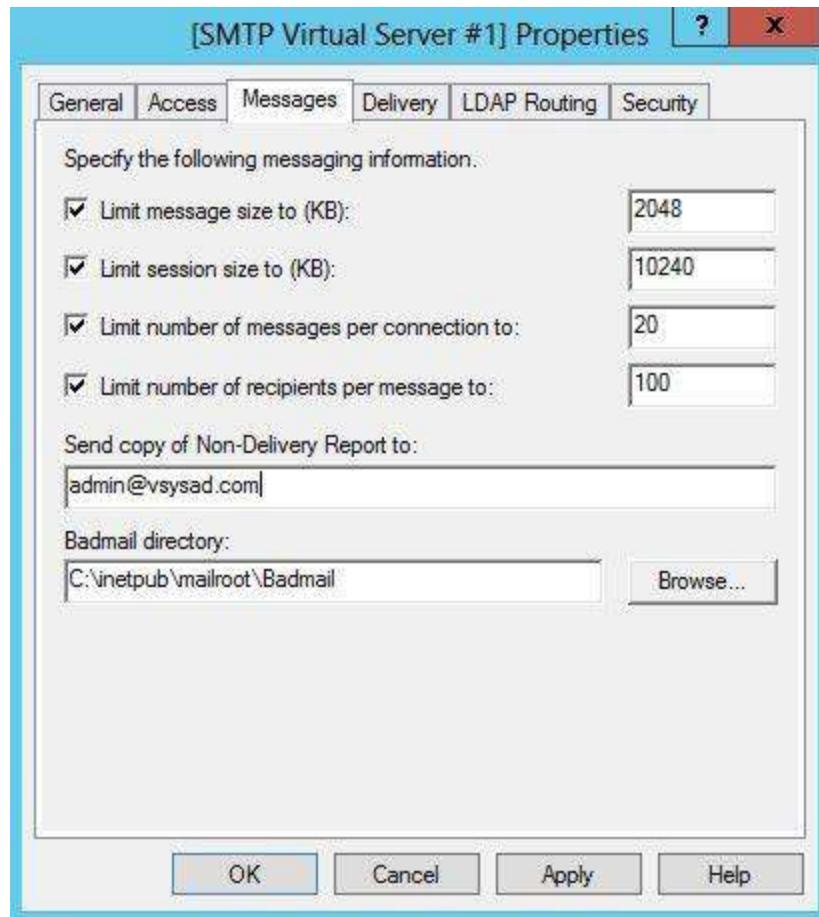


The Connection setting controls which computers can connect to the SMTP server and send mail. By granting only localhost (127.0.0.1) access, limits only the server itself the ability to connect to the SMTP server. This is a requirement for security. Click OK to return to the Access tab and then click on the Relay button. Enter 127.0.0.1 as the IP address and then click OK:

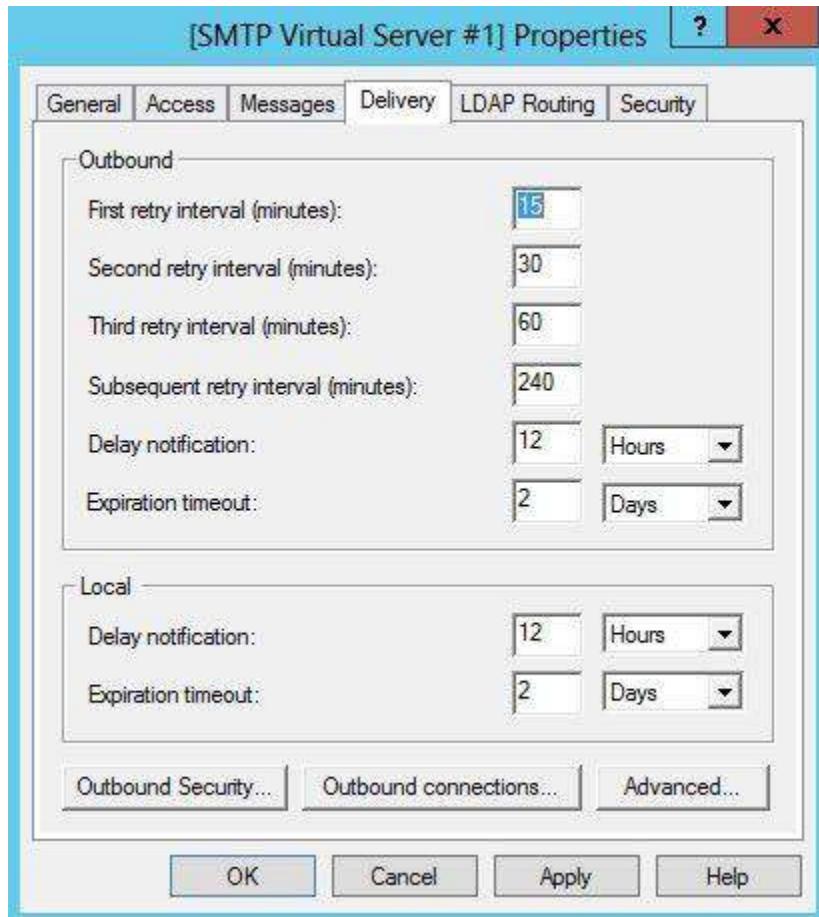


The Relay section determines which computers can relay mail through this SMTP server. By only allowing the localhost IP address (127.0.0.1) relay permissions it means that only the server itself can relay mail. Conversely, it prevents the SMTP server from being an open relay and being used to send unsolicited spam email by other computers on the internet, which could lead to the SMTP server being blacklisted.

Step 14: Next, go to the Messages tab. Here you can enter an email address where copies of non-delivery reports are sent to. You can also configure the location of the Badmail director, however, the default setting should suffice:



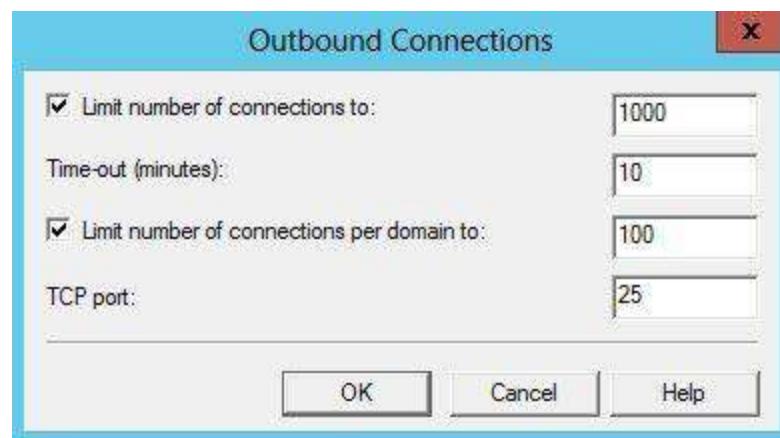
Step 15: Next, go to the Delivery tab:



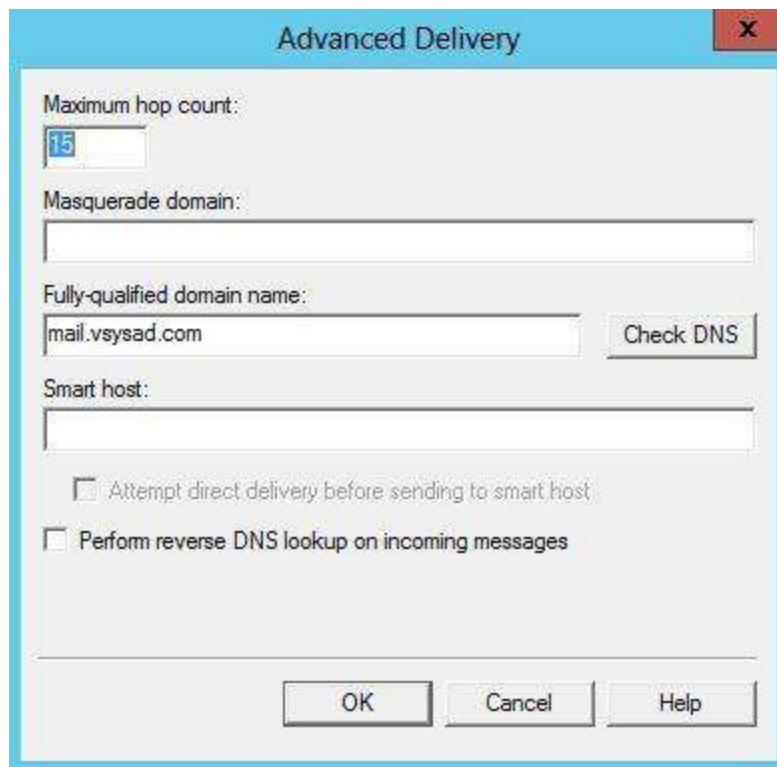
Step 16: Click on the Outbound Security button and ensure Anonymous access is selected. As the only server that can connect and relay mail through the SMTP server is local host this security settings is fine:



Step 17: Click OK to return to the Delivery tab and then click on Outbound Connections. Leave the defaults as they are:



Step 18: Click OK to return to the Delivery tab and then click on Outbound Connections, then click on the Advanced button:



Here you will need to enter the fully-qualified domain name of the SMTP server. This will be the host name or A record that has been created in your DNS zone file. This is straight-forward to do but you will have to confirm how you do this with the party that manages DNS for your domain. I have entered mail.vsysad.com as this is fully-qualified. If you click on the Check DNS button you can confirm whether your chosen name resolves successfully. In my case it does as I see the following:



Step 19: Click OK and then OK again to exit the SMTP Virtual Server Properties. You can also perform this test by running nslookup to confirm the existence of the host name as well as confirming the IP address it resolves to – which should be the IP address of your server:

References:

1. <https://docs.microsoft.com/en-us/exchange/plan-and-deploy/deploy-new-installations/install-mailbox-role?view=exchserver-2019>
2. <https://docs.microsoft.com/en-us/exchange/plan-and-deploy/deploy-new-installations/install-mailbox-role?view=exchserver-2019>

Activity 5

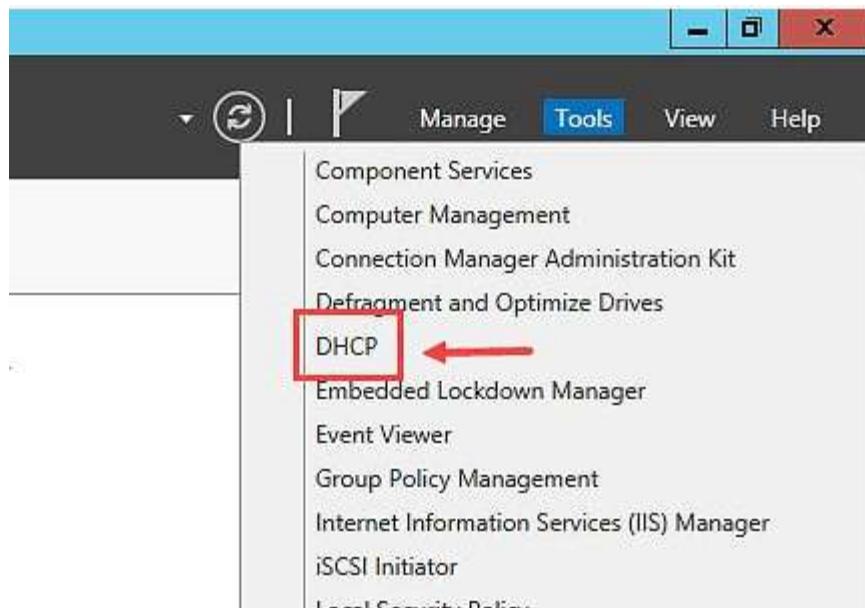
Aim: Backup and Restore ADS and DHCP

Learning Outcome: Able to Backup and Restore ADS and DHCP

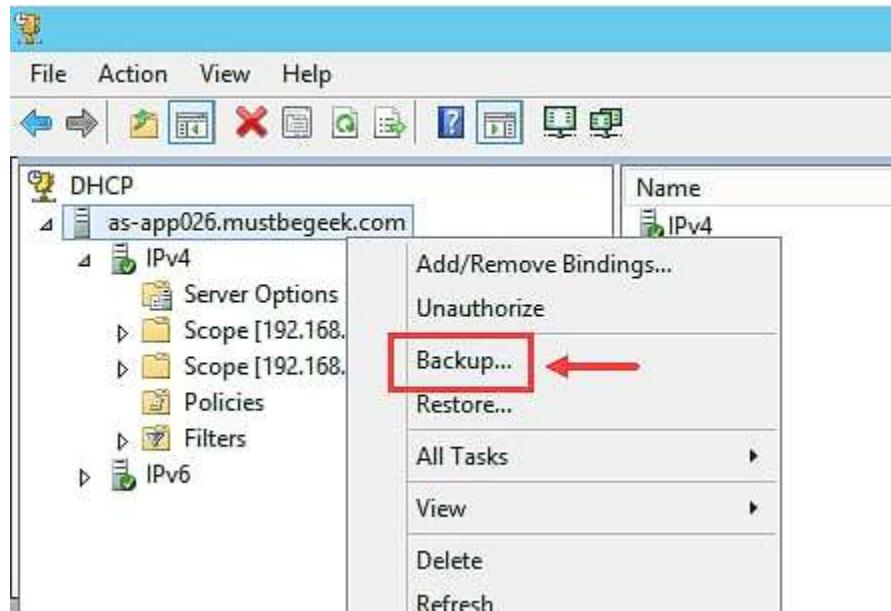
Duration: 3Hrs

Procedure:

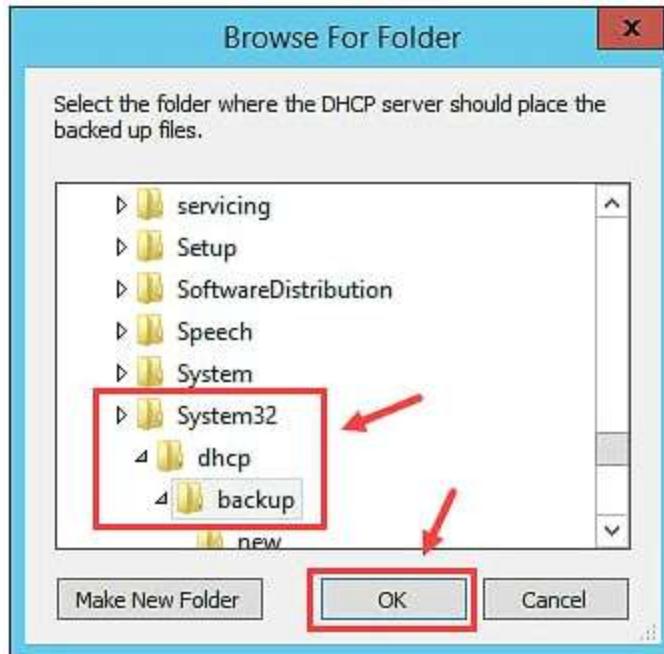
Step 1: To back up your DHCP server using GUI, open Server Manager then click Tools > DHCP to open up the DHCP manager console.



Step 2: In the DHCP manager console, right click on the server name and select “Backup” (in our case, the server name is as-app026.mustbegeek.com).



Step 3: The system will ask where to store the backup; by default it will be stored in C:\Windows\System32\dhcp\backup folder. You can choose whether to use the default location or specify your own preferred location, then click OK button to confirm.

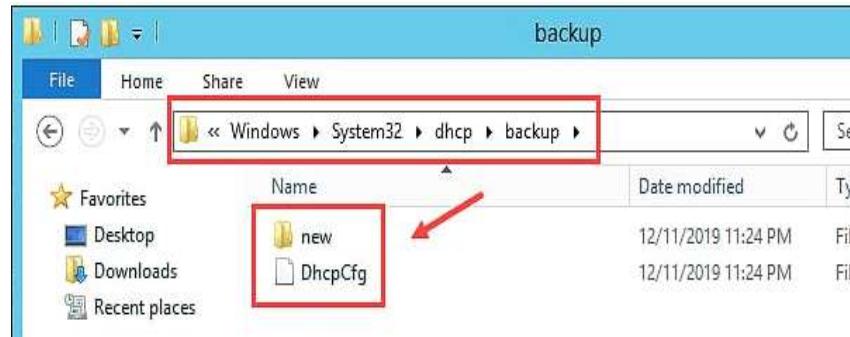


Step 4: The DHCP backup process will run, but unfortunately there is no confirmation box or message that appears when the backup is succeeded.

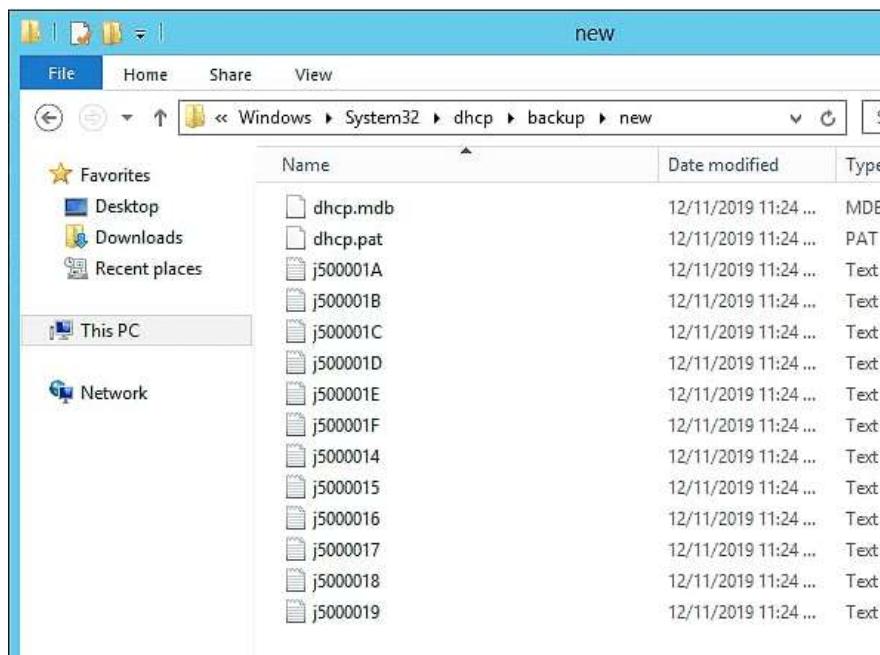
That's all the steps to backup your DHCP server using GUI.

Step 5: Verifying DHCP Server Backup Result

To verify if the backup success, browse to the directory where the backup is saved. You should see contents like the figures below:

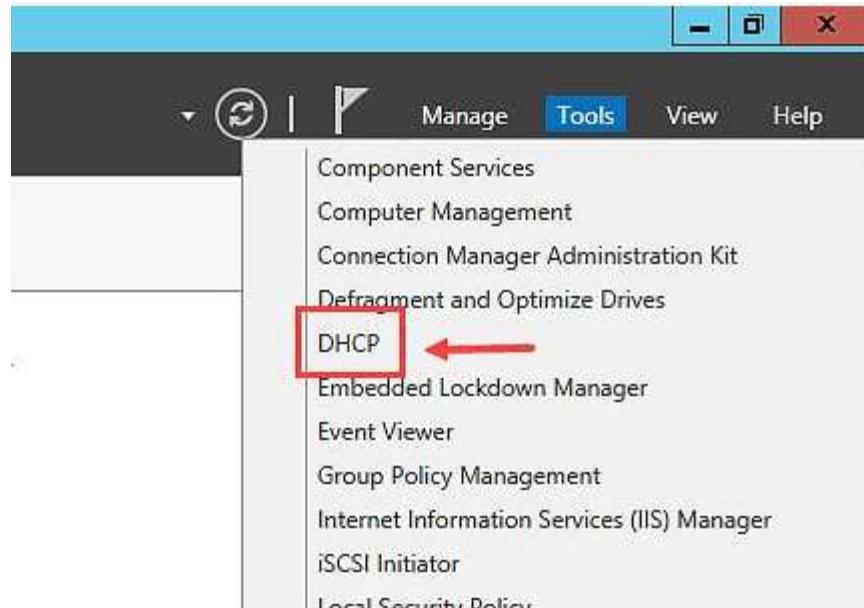


Step 6: In that folder there should be a file named “DhcpCfg” and a subfolder named “new”. If you look at the content of the subfolder, it will show you something like this:

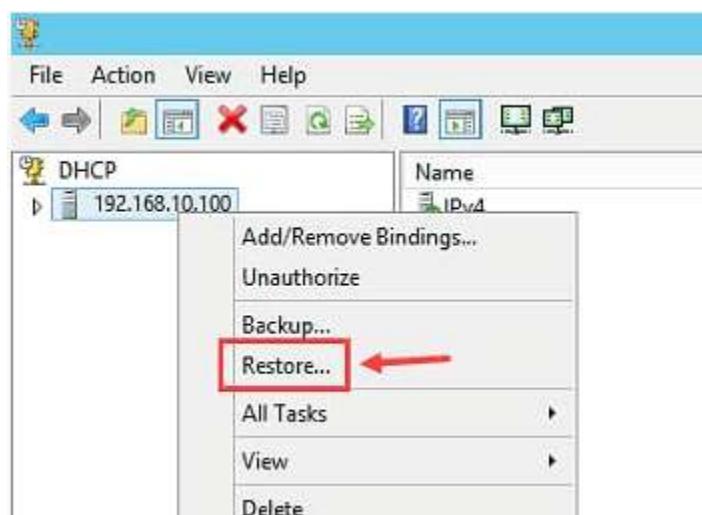


Restore DHCP Server

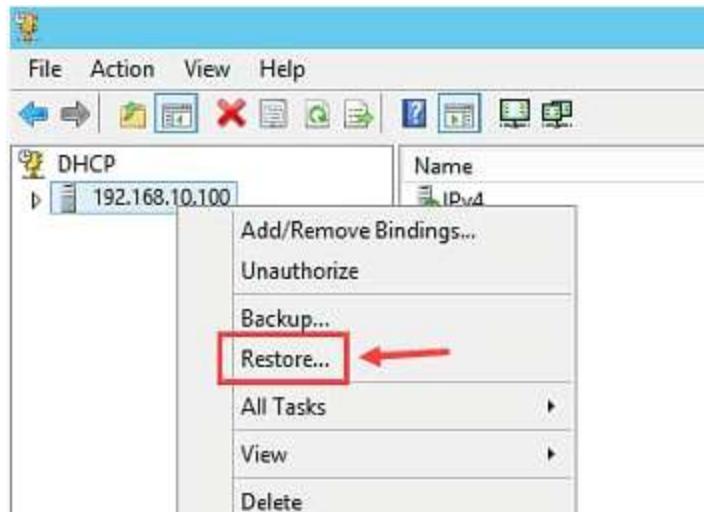
Step 7: To do it using GUI, in the target server, open Server Manager > Tools > DHCP.



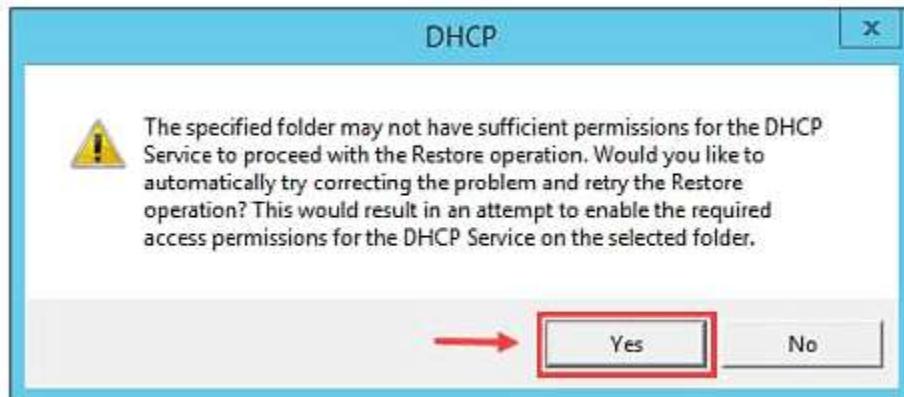
Step 8: In the DHCP Server console, right click the server name and select “Restore“.



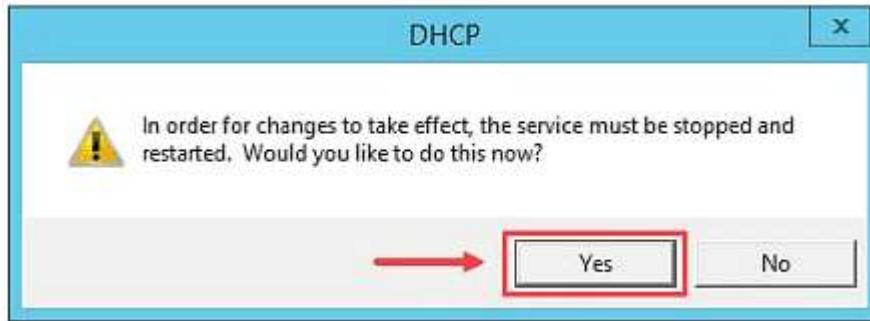
Step 9: Locate the folder where you put the DHCP backup files, and click OK. In this example we have the DHCP backup files in C:\Backup folder.



Step 10: If you copy the DHCP backup files from another server, you may be prompted with permission issue as shown in the figure below. Just click “Yes” button to automatically correct all the possible permission issues.



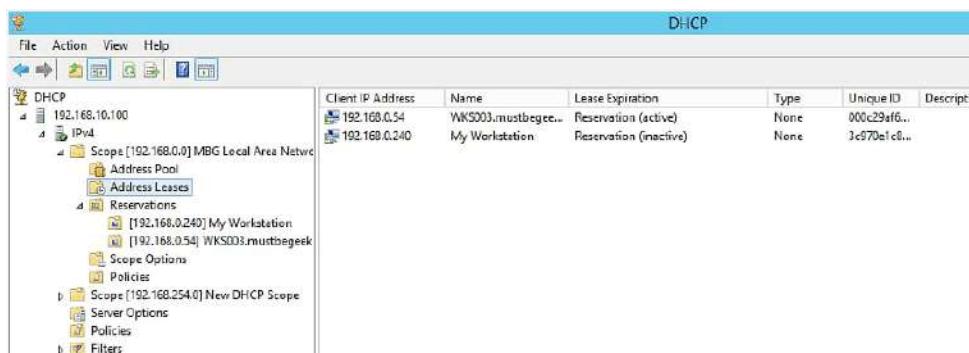
Step 11: The system will also ask if it's okay to restart the DHCP server service in order the perform restore. You must confirm it by clicking the “Yes” button again.



Step 12: Wait for a while (usually a few seconds – depending on your DHCP database size) and you will get notification that DHCP server data has been successfully restored. Click OK to confirm.



Step 13: After this, if you correctly follow all the steps, you will be able to see all the restored DHCP settings like the lease, reservation, filter, etc.

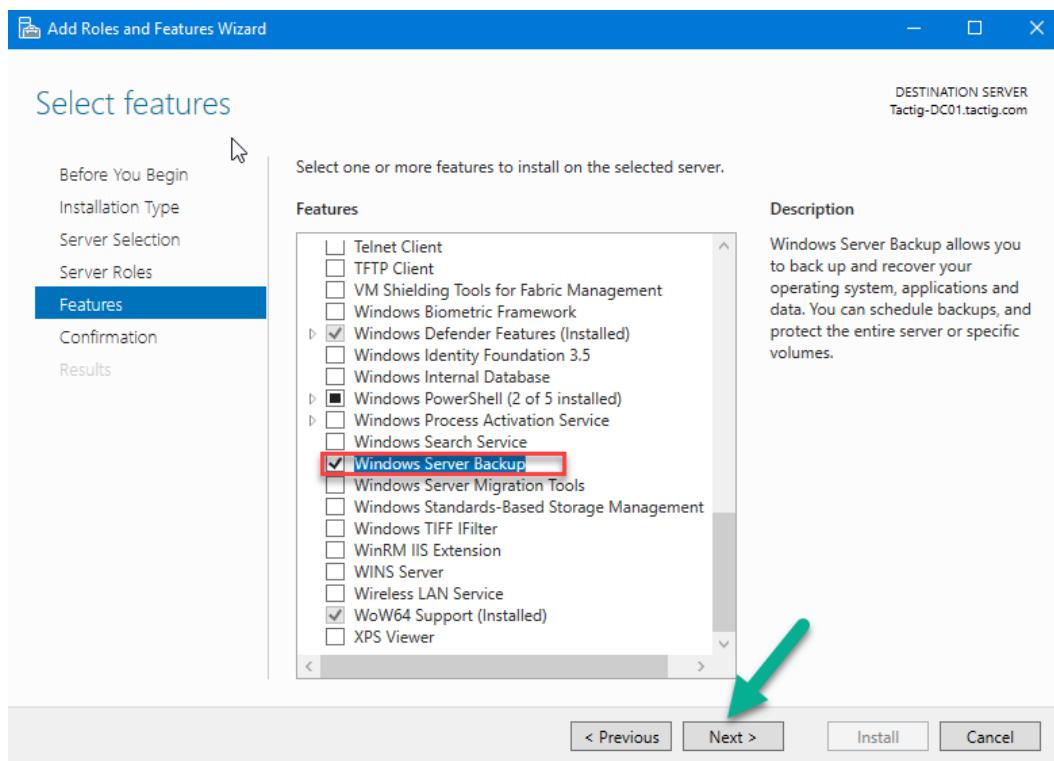


Client IP Address	Name	Lease Expiration	Type	Unique ID	Description
192.168.0.054	WKS003.mustbegreek	Reservation (active)	None	000c29af6..	
192.168.0.240	My Workstation	Reservation (inactive)	None	3c970e1c8..	

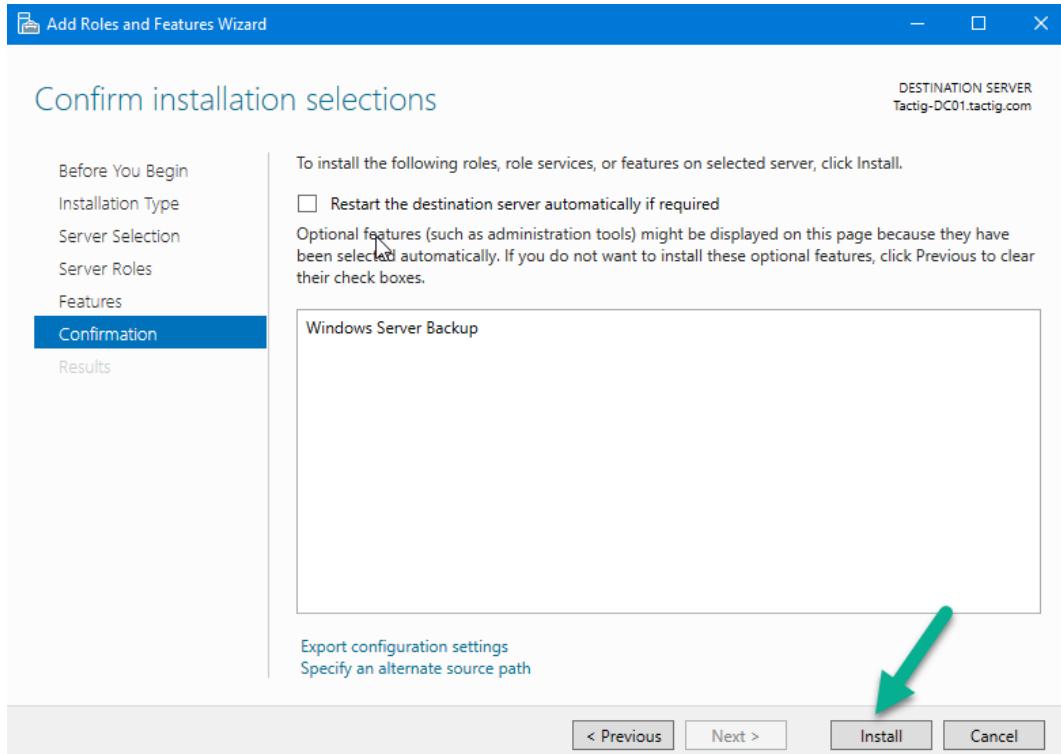
ADS Backup

First of all, you need to install the Windows Backup Server, using Server Manager.

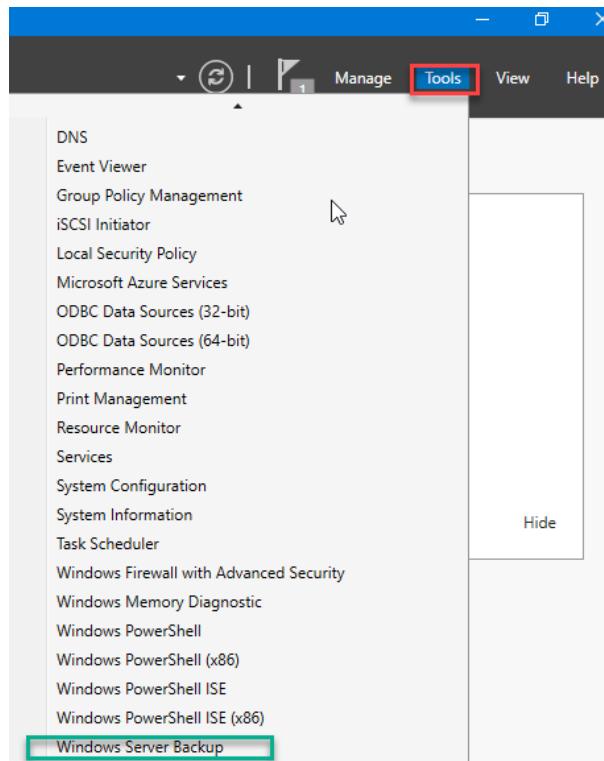
Step 1: Open Server Manager, click on Add roles and features, skip the Welcome page clicking on Next button, then select the server you want to install the backup server on, click on Next button. It is not the role; it is a feature, skip the select Server Roles page. In the feature page, scroll down and check the Windows Server Backup, click next!



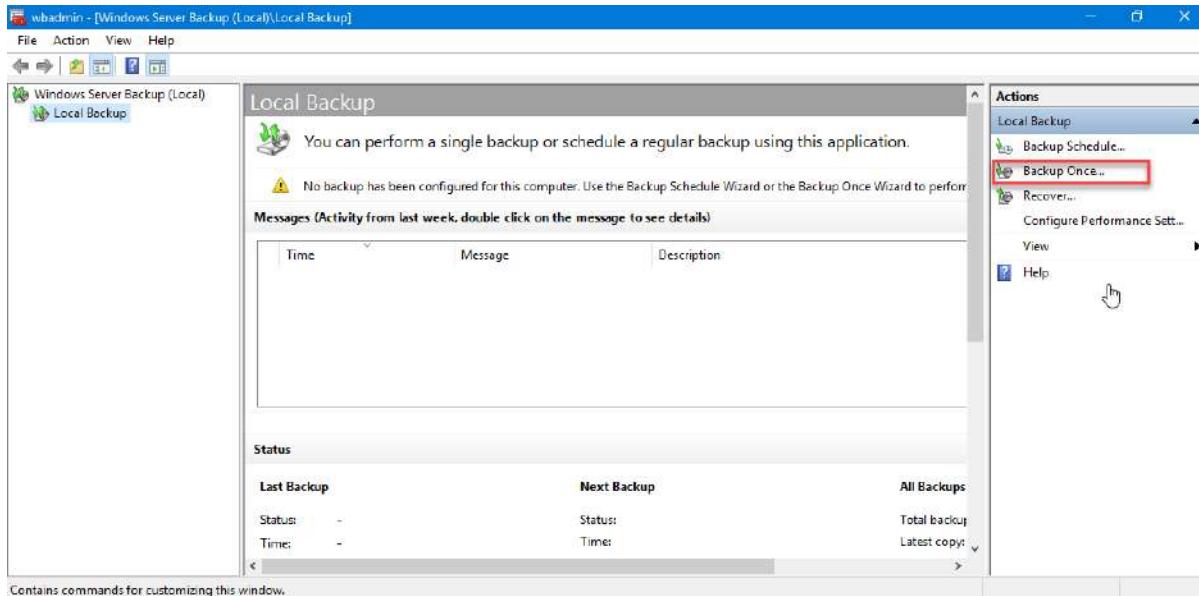
Step 2: In the Confirm installation selections page, click on Install button. It takes a while, no reboot is needed.



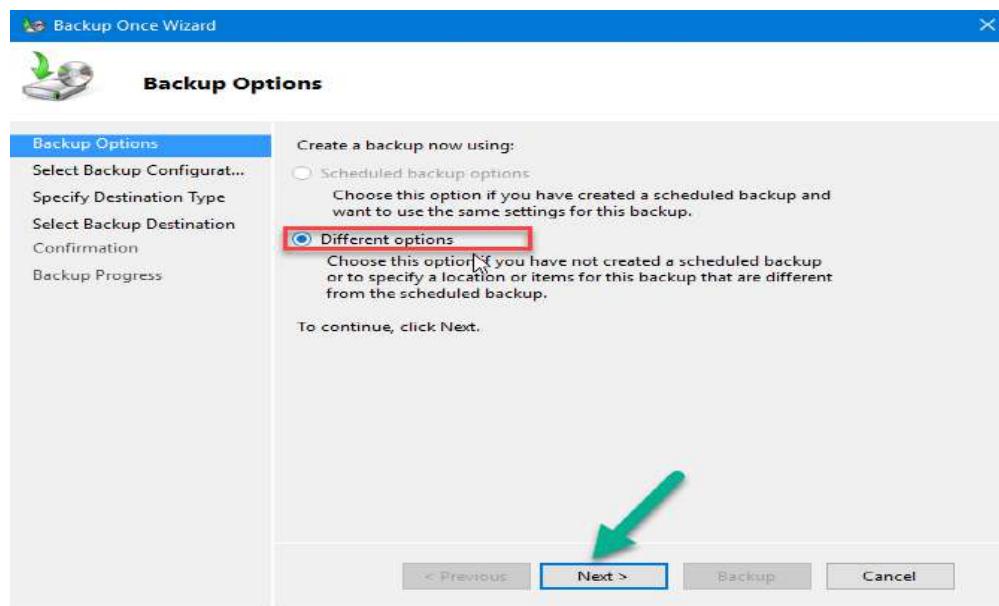
Step 3: Now on the Server Manager, click on Tools, and then click on Windows Server Backup at the end of the list to open the server.



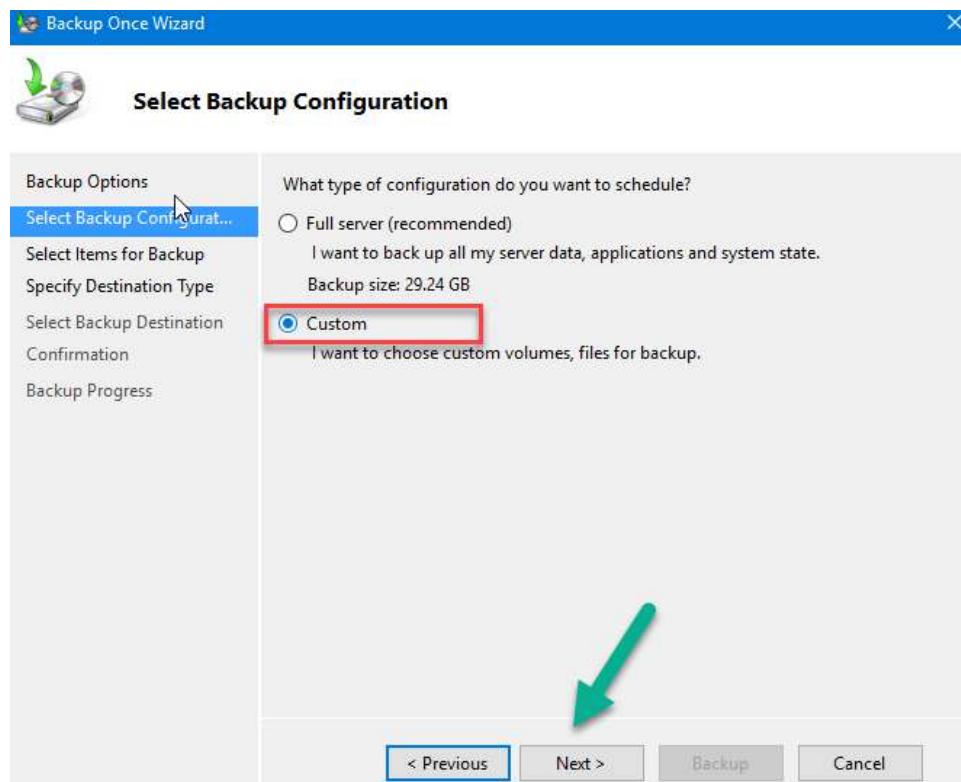
Step 4: Now the server backup is opened, click on backup once. If you like to make a schedule for active directory backup, so click on Backup schedule.



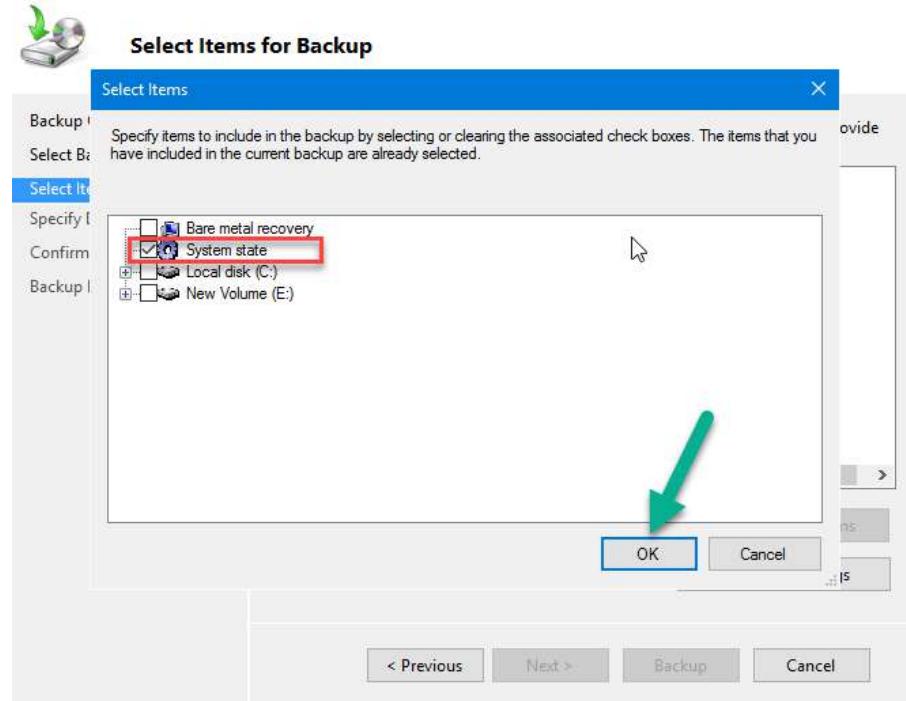
Step 5: Select Different options, click on Next button because Different options are used while we don't have any schedule for backup.



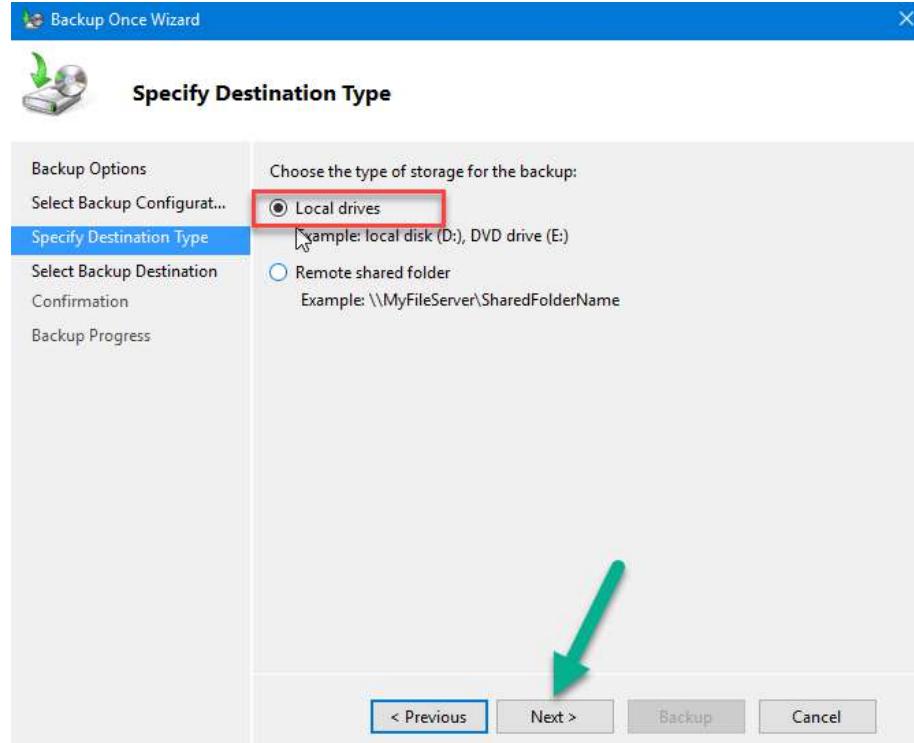
Step 6: On the Select backup configuration page, two options are available, Full Server and Custom. We just want to take backup of the active directory, so we choose the second option.



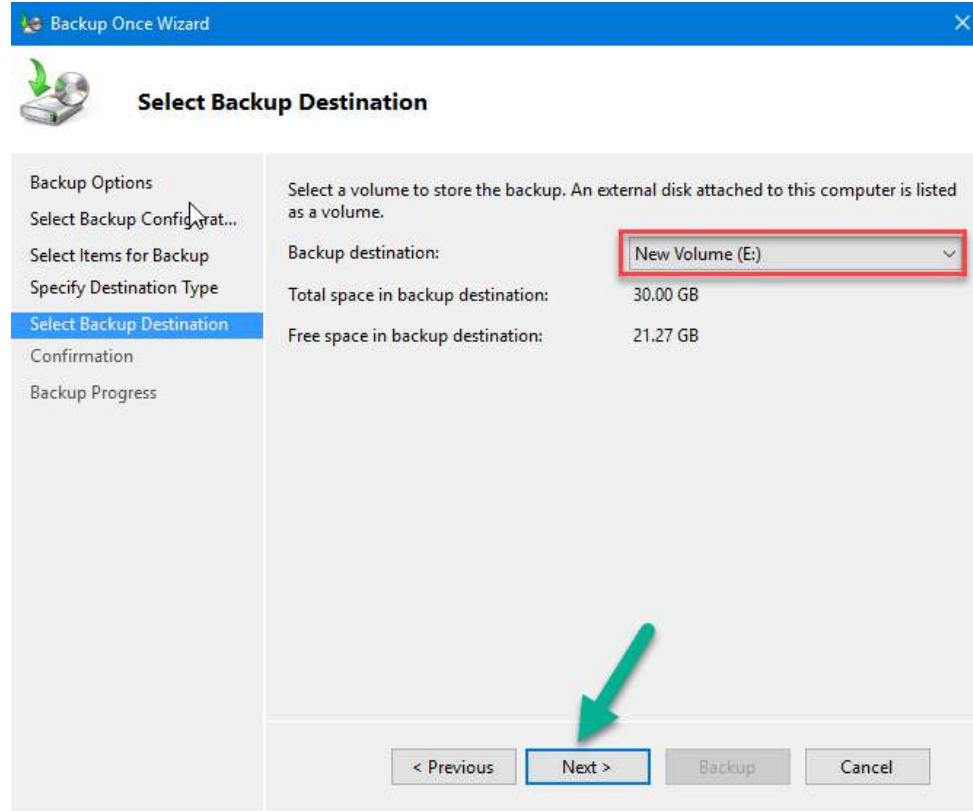
Step 7: In the Select items for the backup page, click on Add items button, select system state option and click on Ok button.



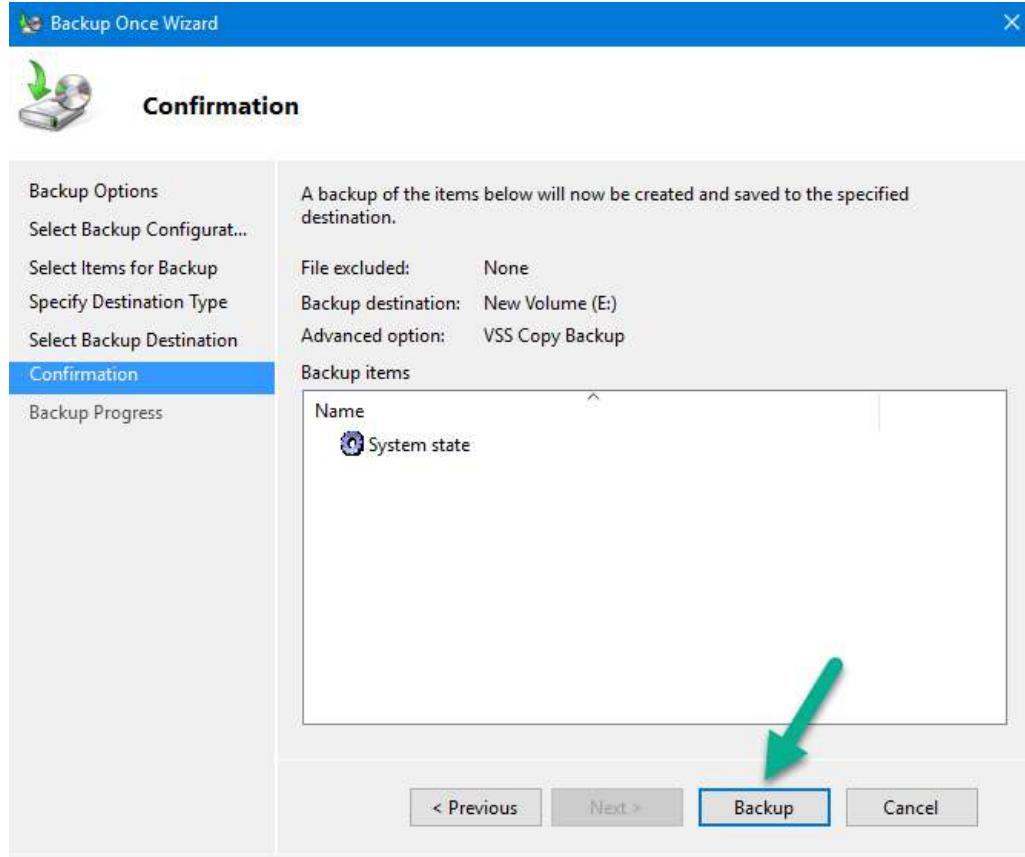
Step 8: It is the time to decide where to restore the backup files, Local drives or shared folder; I choose the local drive.



Step 9: In the Select backup destination page, the place for backup files restoration is specified.



Step 11: We are done, so click on the Backup button. Let the server do its work.

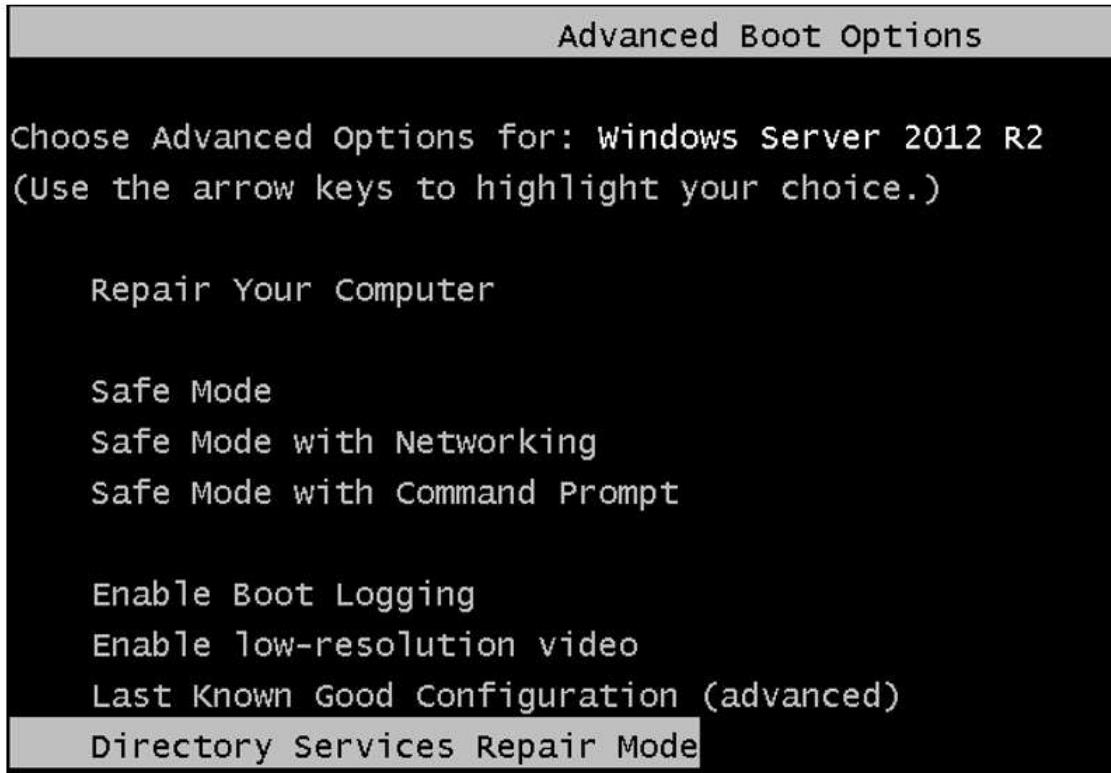


Make sure that you installed ADS, and then promoted it as a domain controller; make sure to use the same names.

You also need your backup in a special Hard Drive, (Like when we created the backup on the Backup drive).

When you are sure that everything's okay. Restart your Server and Spam the F8 key to get into the Advanced Boot Options.

Step 11: Once you are on this screen, get into the “Directory Services Repair Mode” (DSRM).



Once your server is restarted, you will see that you are in safe mode. If you have some difficulties to log on (Try to log on the local Administrator account):



Step 12: Once you are signed in, you will see that you are in safe mode, (it is normal).

Now, you need to go back on the Windows Server Backup screen, once you are here, click on Recovery, (Just under the Backup Once button).

Getting Started	You can use this wizard to recover files, applications, volumes, or the system state from a backup that was created earlier.
Specify Location Type	Where is the backup stored that you want to use for the recovery?
Select Backup Location	<input type="radio"/> This server (WIN-1ND88EP8TJL)
Select Backup Date	<input checked="" type="radio"/> A backup stored on another location
Select Recovery Type	
Select Items to Recover	
Specify Recovery Options	
Confirmation	
Recovery Progress	

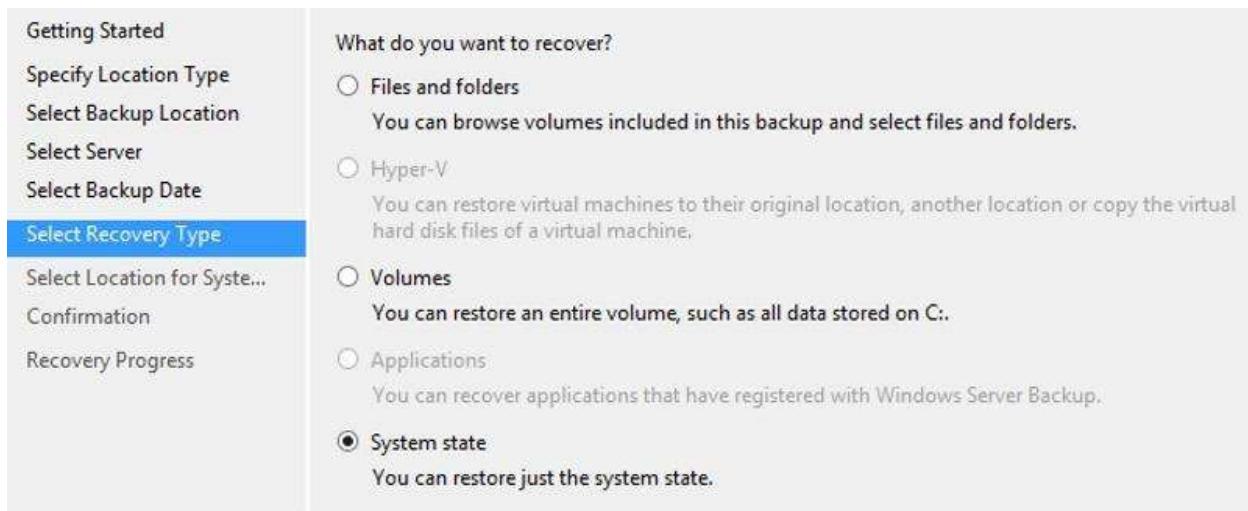
Step 13: On this first screen, choose “A backup stored on another location”. Even if the backup is on this computer, it comes from another one. So the server says: “Hey! I don’t know this one!”

And on the Next Screen, select the hard drive where you putted the backup. Then Click Next.

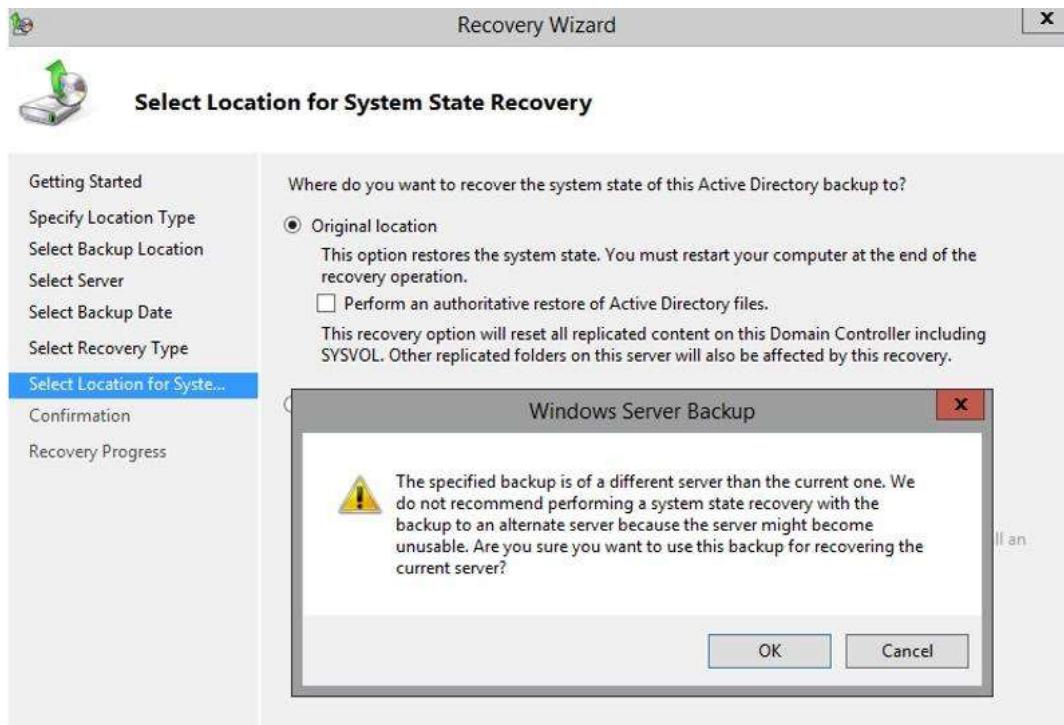
Getting Started	Please select which server's data you would like to recover.
Specify Location Type	Server:
Select Backup Location	
Select Server	<input type="radio"/> WIN-26P27USVT5E
Select Backup Date	
Select Recovery Type	
Select Items to Recover	
Specify Recovery Options	
Confirmation	
Recovery Progress	

Skip the Select Backup Date Screen.

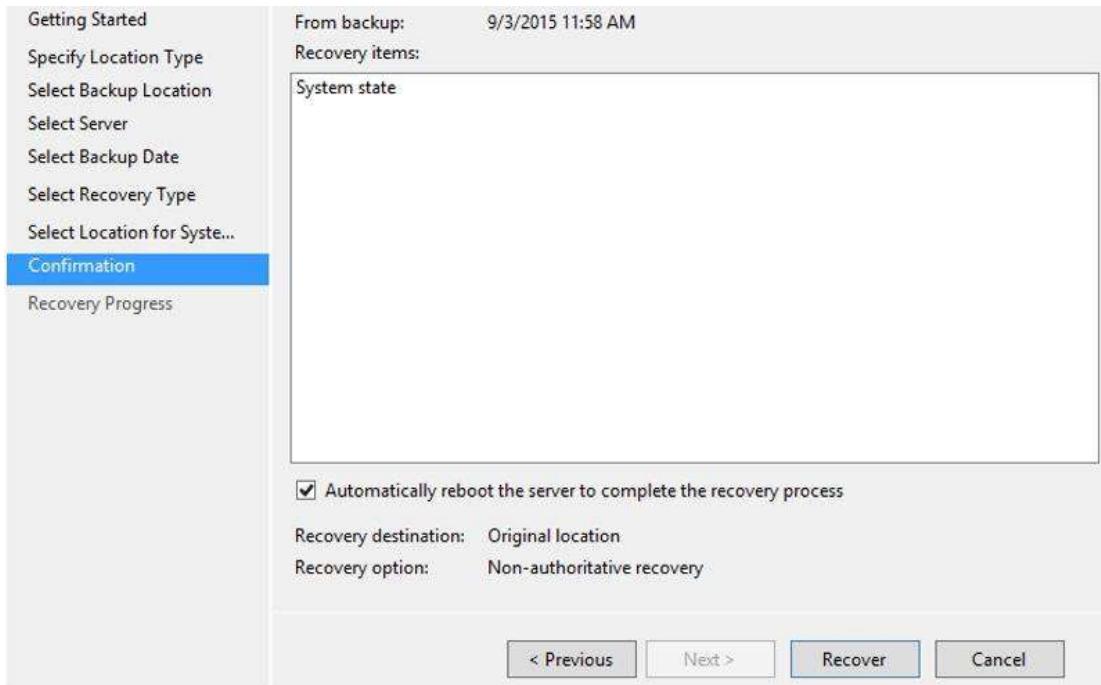
Step 14: On the Select Recovery Type, choose the System State (The backup type is a System State). Then Click Next.



Step 15: On the Next Screen, the Wizard asks us the location for the System State Backup, just choose the Original Location, (A Warning Window appears, Click OK, and then recover.



Step 16: For the last screen, check the box for “Automatically reboot the server to complete the recovery process” (or not, if you want to restart by yourself), and then click on recover.



Then, like for the backup, windows will work

Recovery Wizard

Recovery Progress

Getting Started
Specify Location Type
Select Backup Location
Select Server
Select Backup Date
Select Recovery Type
Select Location for Syste...
Confirmation
Recovery Progress

System state recovery progress:
Status: 2890 files found for recovery...

Estimated time: Computing ...

Recovery details:

Item	Destination	Status	Data transferred
Performan...	Original location	0% complete...	0 KB of 1.13 MB
DFS Replica...	Original location	0% complete...	0 KB of 8 KB
COM+ REG...	Original location	0% complete...	0 KB of 1.05 MB
VSS Metad...	Original location	0% complete...	0 KB of 12 KB
WMI Writer	Original location	0% complete...	0 KB of 26.93 MB
Registrv Wr...	Original location	0% complete...	0 KB of 94.81 MB

You cannot cancel the system state recovery operation once it has started.
 Automatically reboot the server to complete the recovery process

< Previous Next > Close Cancel

Recovery Wizard

Recovery Progress

Getting Started
Specify Location Type
Select Backup Location
Select Server
Select Backup Date
Select Recovery Type
Select Location for Syste...
Confirmation
Recovery Progress

System state recovery progress:
Status: 15% complete...

Estimated time: 5 minutes left ...

Recovery details:

Item	Destination	Status	Data transferred
Performan...	Original location	Completed.	1.13 MB of 1.13 MB
DFS Replica...	Original location	Completed.	8 KB of 8 KB
COM+ REG...	Original location	Completed.	1.05 MB of 1.05 MB
VSS Metad...	Original location	Completed.	12 KB of 12 KB
WMI Writer	Original location	Completed.	26.93 MB of 26.93...
Registrv Wr...	Original location	Completed.	94.81 MB of 94.81...

You cannot cancel the system state recovery operation once it has started.
 Automatically reboot the server to complete the recovery process

< Previous Next > Close Cancel

Once it's done. The server will restart. It can take an abnormal long time to reboot, but don't worry, Windows set up everything.

References:

1. <https://www.prajwaldesai.com/windows-server/windows-server-2012-r2-windows-server/>
2. <https://blogs.technet.microsoft.com/teAMDHCP/2012/08/31/installing-and-configuring-dhcp-role-on-windows-server-2012/>
3. <https://www.thegeekstuff.com/2014/11/install-active-directory/>

Activity 6

Aim: Backup and Restore User Data

Learning Outcome: Able to Backup and Restore User Data

Duration: 2Hrs

Procedure:

You can manually back up data or use the Backup Wizard, which is included in the Backup feature. You can back up the whole contents of the server, selected portions of the server, or the system state data (the system configuration information).

To Back Up Selected Files or Folders

Step 1: Click Start, point to All Programs, point to Accessories, point to System Tools, and then click Backup. The Backup or Restore Wizard starts.

Step 2: Click Advanced Mode.

Step 3: Click the Backup tab.

Step 4: On the Job menu, click New.

Step 5: Expand the drive or folder that contains the items that you want to back up. Click to select the check boxes next to the files, folders, or drives that you want to back up.

Step 6: In the Backup destination box, specify the destination for the new job. To do so, do one of the following:

Step 7: If you want to back up files and folders to a file, click File.

Step 8: If you want to back up to tape, click a tape device.

NOTE: If a tape device is not connected to your computer, File is the only backup media type that is available in the

Restoring Data to the Server

If a data loss occurs, you can restore your backup data manually or by using the Restore Wizard, which is included in the Backup feature.

To Restore the System State Data (Including Registry Information)

Step 9: Click Start, point to All Programs, point to Accessories, point to System Tools, and then click Backup. The Backup or Restore Wizard starts.

Step 11: Click Advanced Mode.

Step 12: Click the Restore and Manage Mediatab.

Step 13: In the Items to restore box, expand the media that you want to restore, and then click to select the System State check box.

Step 14: Click to select the check boxes next to any other drives, folders, or files that you want to restore.

Step 15: In the Restore file to box, specify the location where you want to restore the files by doing one of the following:

Step 16: If you want to restore the files or folders to the same location in which they were when you backed up the data, click Original location, and then go to step 8.

Step 17: If you want to restore the files or folders to a new location, click Alternate location.

This option preserves the folder structure of the backed up data.

Step 18: If you want to restore the files and folders to a single location, click Single folder.

NOTE: If you do not designate an alternate location for the restored data, the restore operation erases the current system state data and replaces it with the information that you are restoring.

References:

1. <https://support.microsoft.com/en-in/help/17127/windows-back-up-restore>

Activity 7

Aim: Permit FAT and NTFS Sharing

Learning Outcome: Able to configure file sharing

Duration: 3Hrs

Procedure

Log on to Windows Server with a local administrator account:

Step 1: Open Server Manager using the icon on the desktop taskbar, or from the Start screen.

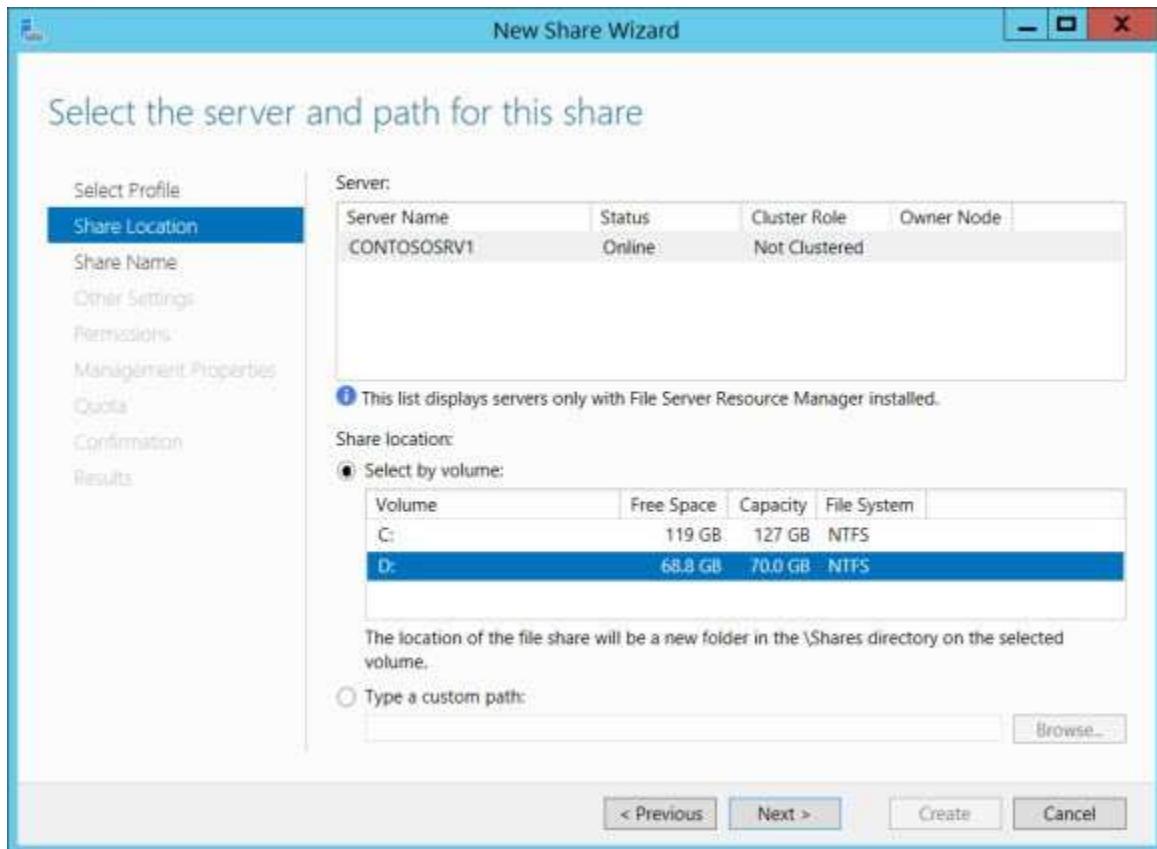
Step 2: In the left pane of Server Manager, click File and Storage Services.

Step 3: In the column to the right, click Shares.

Step 4: To the right of Shares in the main window, click the Tasks menu and New Share.

Step 5: In the New Share Wizard, select the SMB Share – Advanced profile and click Next.

Step 6: On the Select the server and path for this share screen, make sure that Select by volume is selected under Share location, and then chose the volume where you want to create the new share. Now click next.



Create a new file share using Server Manager.

Step 7: On the Specify share name screen, type a name for the new share in the Share name box and click next. The local and remote paths will be generated automatically.

Step 8: On the Configure share settings screen, check or deselect any of the additional options for the share as required, such as Enable access-based enumeration and Encrypt data access.

Click Next to continue.

Step 9: To change the default NTFS folder or share permissions, click Customize permissions on the Specify permissions to control access screen, set the permissions as required in the dialog box and click OK when you're done. Now click Next to continue.

Step 11: On the Management Properties screen, you can optionally select a folder usage value for the share if you plan to use classification rules. Click Next to continue

Step 12: Finally, on the Apply a quota to a folder or volume screen, you can chose to apply a quota template to the share. Click next when you're done.

Step 13: Click Create on the Confirmation screen.

Step 14: Click Close when the share has been successfully created.

References:

1. <https://www.petri.com/create-file-share-windows-server-2012-r2-with-server-manager>
2. <https://www.techrepublic.com/blog/data-center/how-to-share-a-folder-in-windows-server-2012/>

L

Learning Outcome 3 - Able to configure different protocol services

After achieving this learning outcome, a student will be able to configure different protocol services. In order to achieve this learning outcome, a student has to complete the following:

1. Add Account (1Hr)
2. ImplementAGDLPPProcess (2Hrs.)
3. Implement User Authentication Strategy (2 Hrs)
4. Plan and Implement OU Structure (1Hr)
5. Plan and Maintain Group Policies (2Hrs)
6. Configure User Environment (2Hrs)
7. Install andConfigureActive Directory Services (2 Hrs)
8. Installation and Configuring DNS Services (3Hrs)
9. Installation and Configuring DHCP Services (2Hrs)
10. Install and Configure FTP Services. (3Hrs)
11. Install and Configure HTTP Services (2Hrs)
12. Configure IIS Services (3 Hrs)

Activity 1

Aim: Add user Account

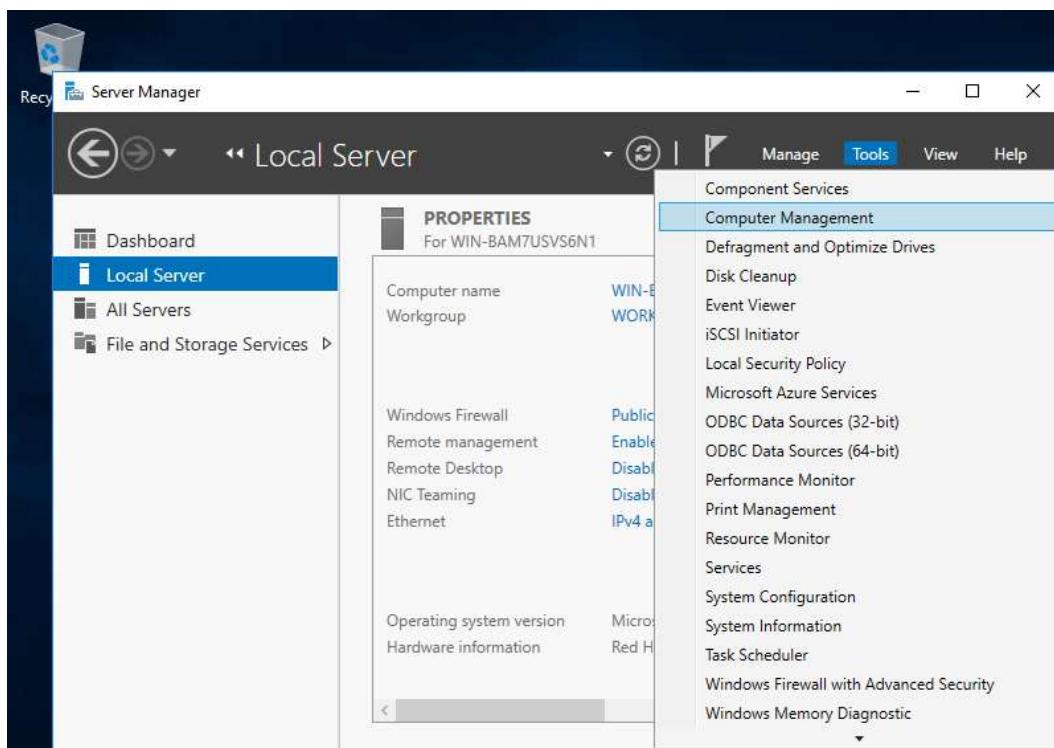
Learning Outcome: Able to Add user Account

Duration: 1Hr

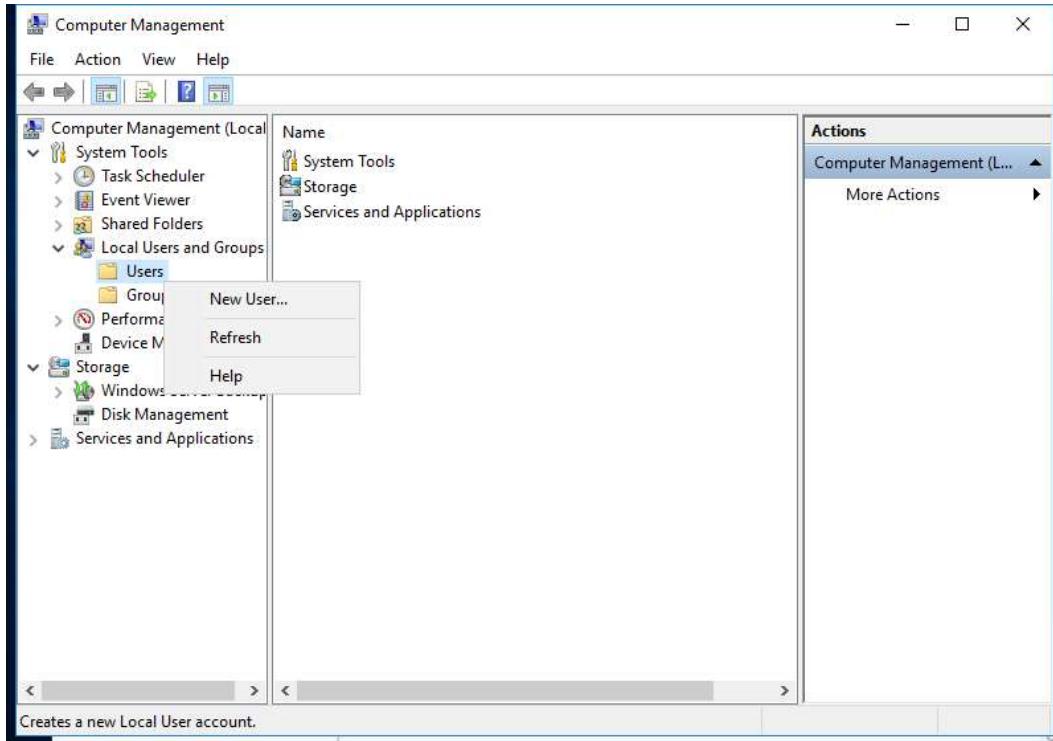
Procedure

Add Local User

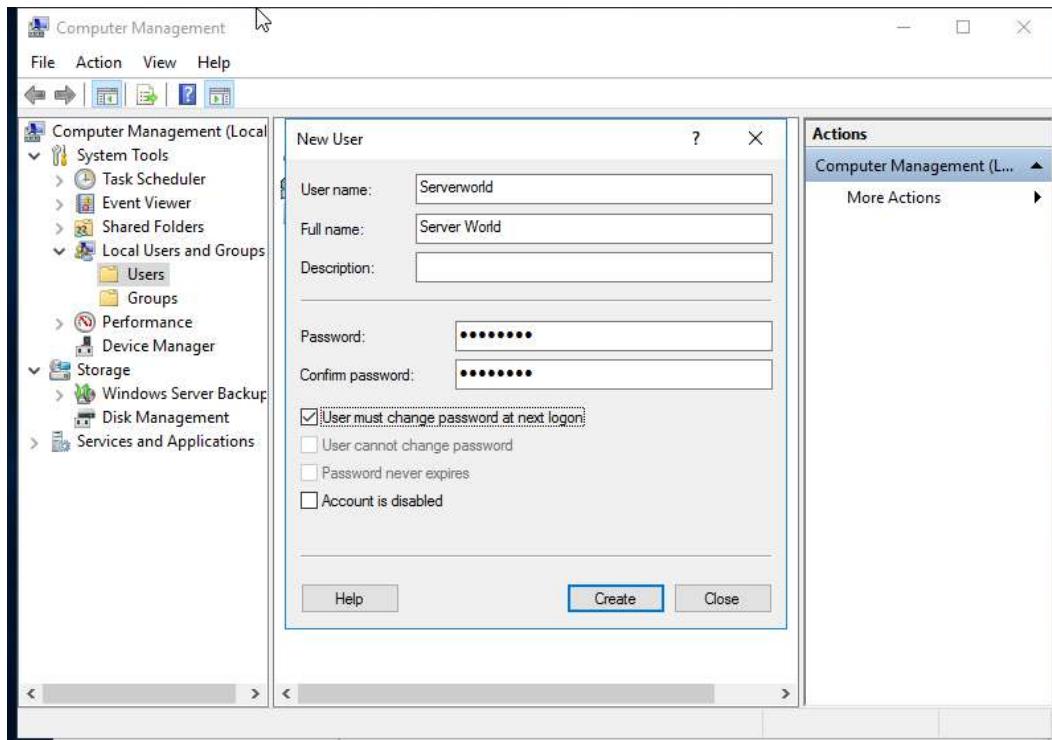
Step 1: Run [Server Manager] and Open [Tools] - [Computer Management].



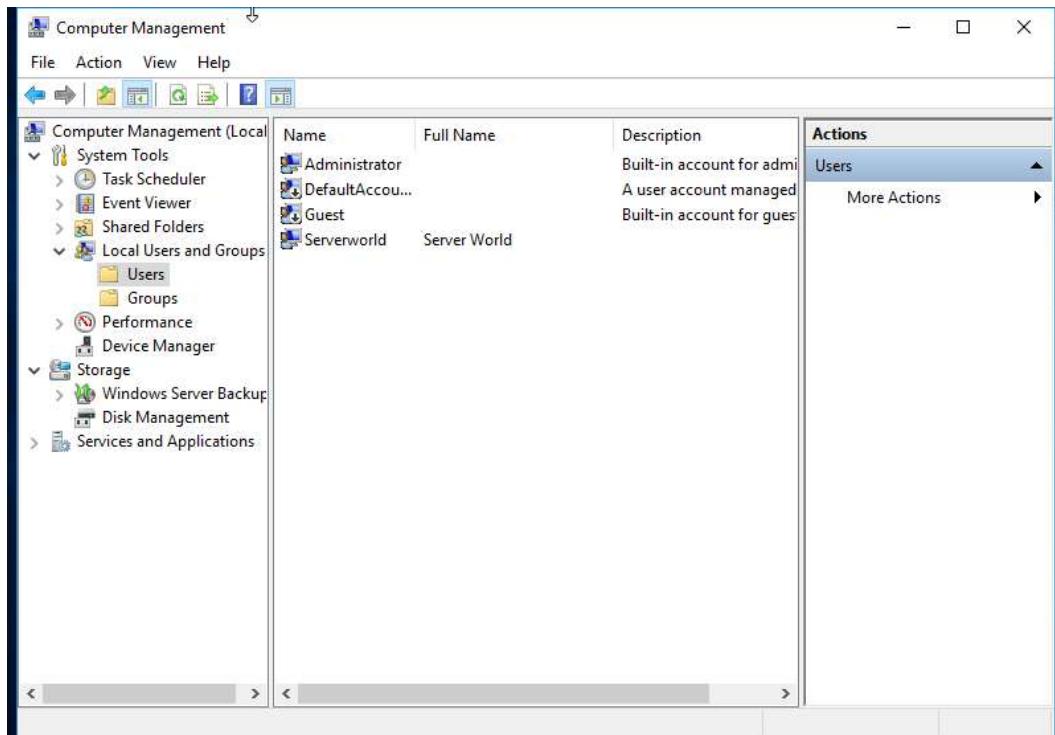
Step 2: Right-Click [Users] under the [Local Users and Groups] on the left pane and select [New User].



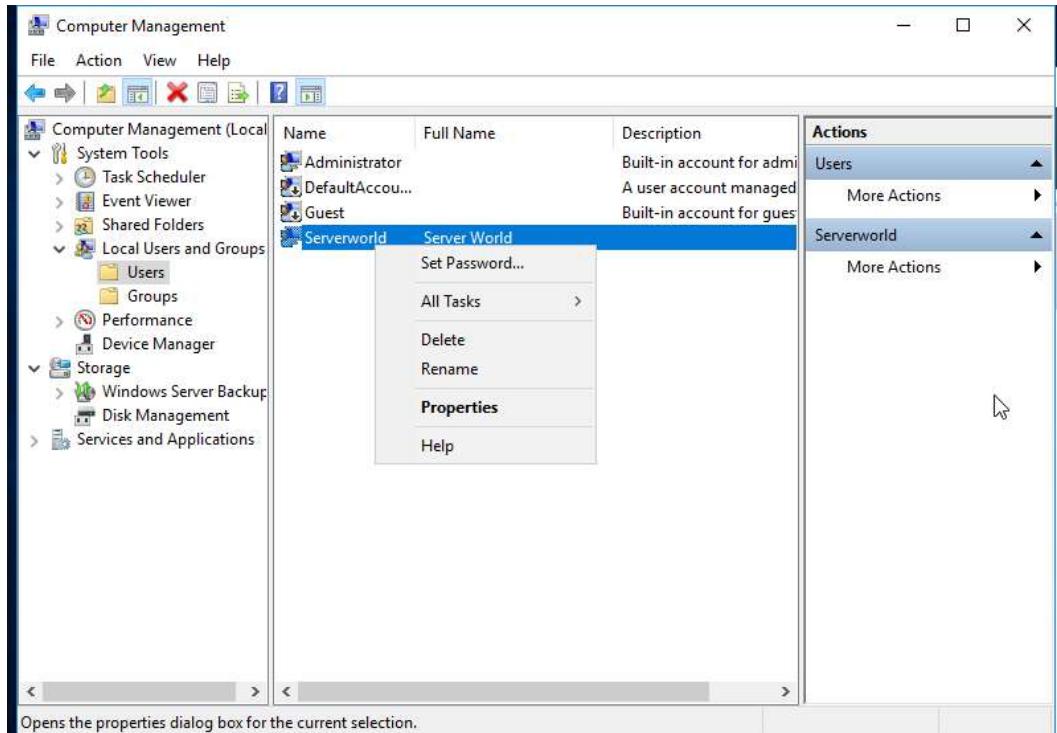
Step 3: Input UserName and Password for a new user and click [Create] button. Other items are optional to set.



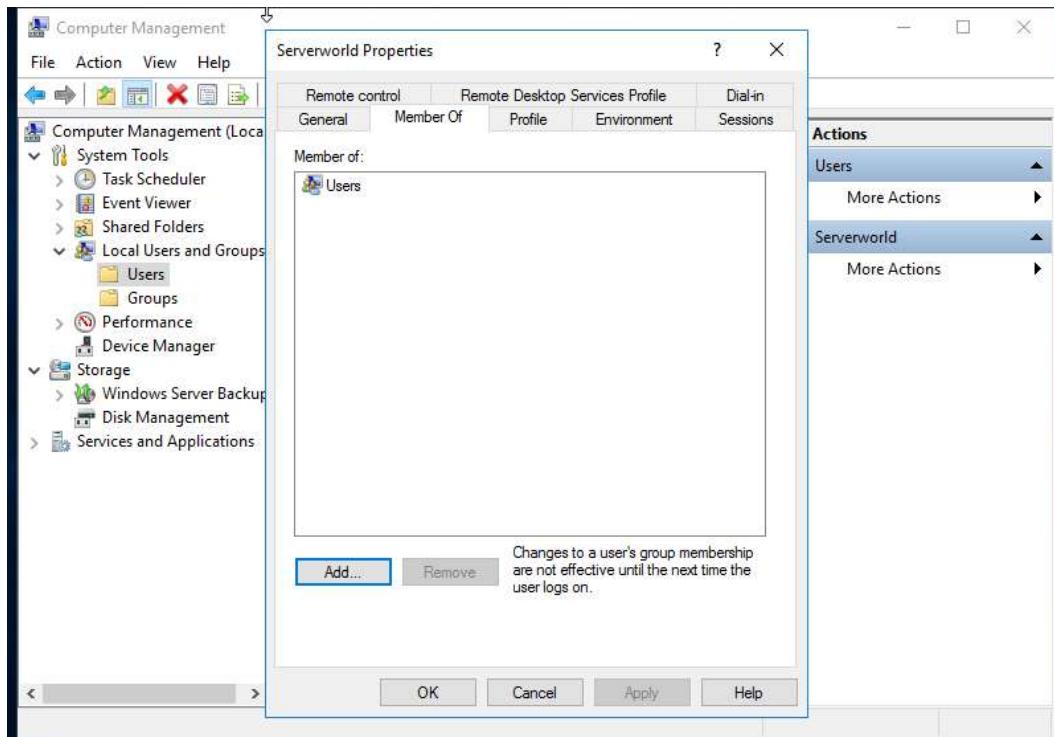
Step 4: After creating normally, New user is shown on the list like follows.



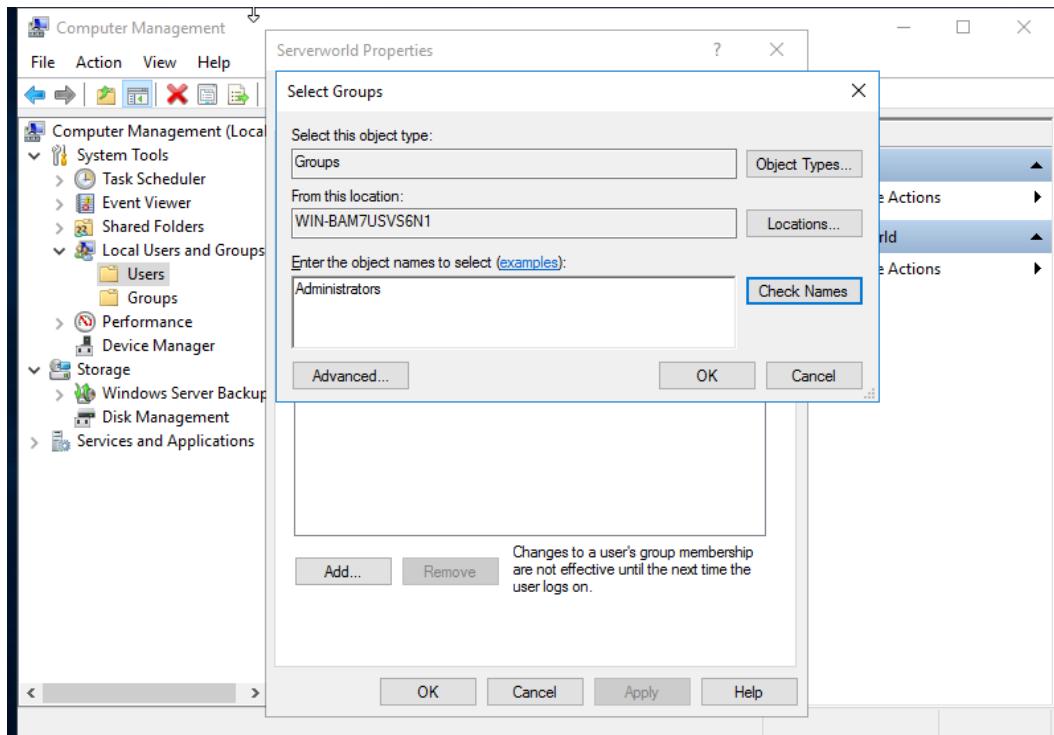
Step 5: If you'd like to set administrative privilege to the new user, Right-click the user and open [Properties].



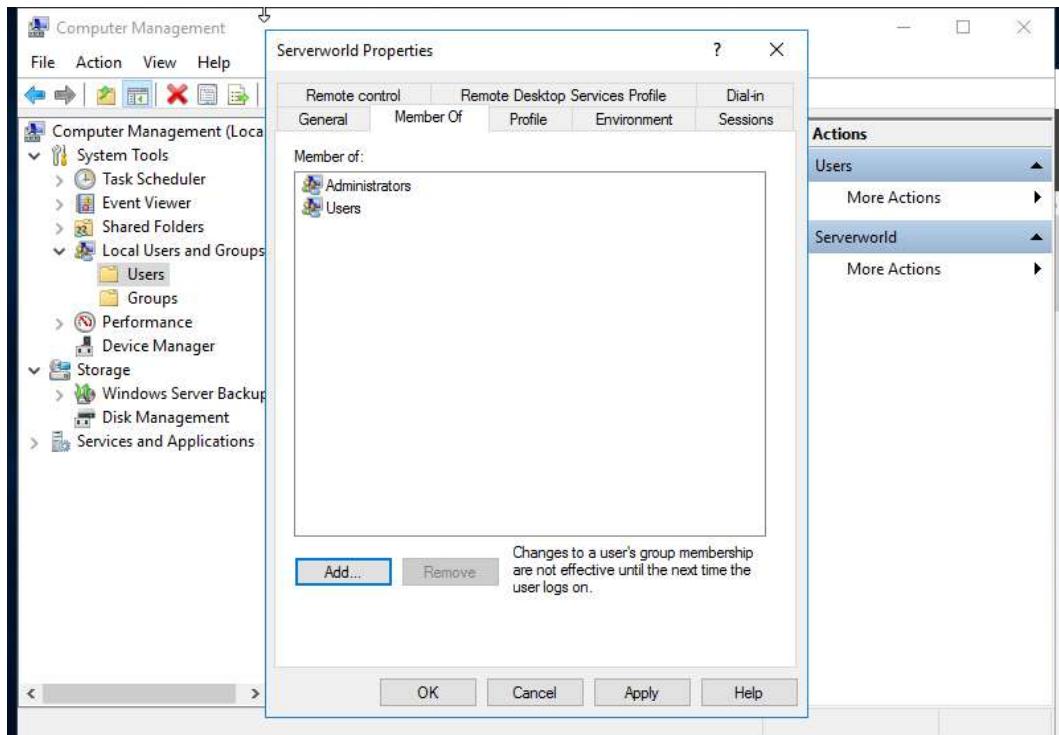
Step 6: Move to [Member of] tab and click [Add] button.



Step 7: Specify [Administrators] group like follows.



Step 8: Make sure [Administrators] group is added on the list and click [OK] button to finish settings.



References:

1. https://www.server-world.info/en/note?os=Windows_Server_2016&p=active_directory&f=3
2. <https://ittutorials.net/microsoft/windows-server-2016/create-a-new-local-user-account-in-windows-server-2016/>

Activity 2

Aim: Implement AGDLP Process

Learning Outcome: Able to configure and Implement AGDLP Process

Duration: 2Hrs

Procedure

Step 1: A: Create a user Account(s)

Step 2: G: Create a global group and add the user account(s) you created in step as members

Step 3: DL: Create a Domain Local group in the domain that contains the resource you wish to give access to and then add the global group from step 2 as a member of this Domain Local group

Step 4: P: Assign permissions on the resource using the domain local group created in a step.

References:

1. <https://ignitedsoul.com/2013/01/18/agdlp-accounts-global-groups-domain-local-groups-permissions/>
2. <https://www.networkedminds.com/70-410-objective-5-3-group-scope-nesting-groups-windows-server-2012-r2/>

Activity 3

Aim: Implement User Authentication Strategy

Learning Outcome: Able to configure and Implement User Authentication Strategy

Duration: 2Hrs

Procedure

Prerequisites

- Before you can configure authentication policies and silos in your domain, there are several requirements that must be met.

Domain Functional Level

Step 1: Protected Users Group - To remove an account from the Domain Admins group, use the PowerShell cmdlet below. In my domain, the default domain administrator account is contosodc1admin.

```
Remove-ADGroupMember -Identity 'Domain Admins' -Member contosodc1admin
```

Step 2: To quickly add members of the Domain Admins group to the Protected Users group, use the cmdlet below.

```
$DomainAdmins = Get-ADGroupMember -Identity 'Domain Admins'
```

```
Add-ADGroupMember -Identity 'Protected Users' -Members $DomainAdmins
```

Step 3: Quickly adding members to the Protected Users group.

Enable Support for Claims, Compound Authentication and Kerberos Armoring

There are two group policy settings that must be configured to enable Kerberos support for authentication policies and silos in a domain. The KDC support for claims, compound authentication, and Kerberos armoring setting under Computer Configuration > Policies > Administrative Templates > System > KDC must be set to Supported for domain controllers. Link the GPO to the Domain Controllers OU.

The Group Policy Management dialog screen.

- For all domain members (Windows 8 and Windows Server 2012 or later), Kerberos client support for claims, compound authentication, and Kerberos armoring should be set to Enabled under Computer Configuration > Policies > Administrative Templates > System > Kerberos. Link the GPO to the domain.

```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\CONTOSO\DC1\admin> Get-ADGroupMember -Identity 'Protected Users'

distinguishedName : CN=domainadmin 2,CN=Users,DC=ad,DC=contoso,DC=com
name              : domainadmin 2
objectClass       : user
objectGUID        : 3c728b53-edc6-4285-9425-77f865b7ad79
SamAccountName   : domainadmin2
SID               : S-1-5-21-1428797457-1620164863-807756529-1104

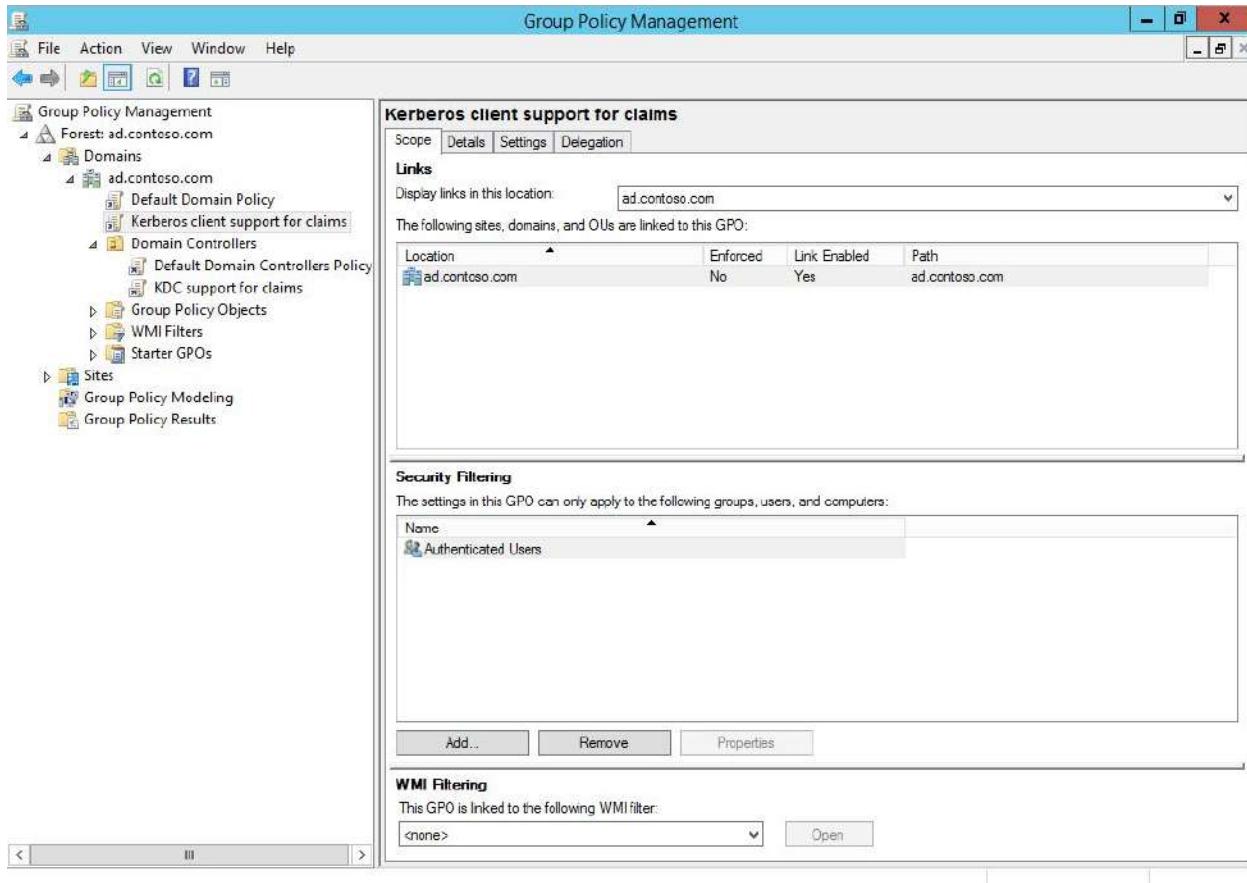
PS C:\Users\CONTOSO\DC1\admin> Get-ADGroupMember -Identity 'Domain Admins'

distinguishedName : CN=domainadmin 2,CN=Users,DC=ad,DC=contoso,DC=com
name              : domainadmin 2
objectClass       : user
objectGUID        : 3c728b53-edc6-4285-9425-77f865b7ad79
SamAccountName   : domainadmin2
SID               : S-1-5-21-1428797457-1620164863-807756529-1104

PS C:\Users\CONTOSO\DC1\admin> .
```

Enable Support for Claims, Compound Authentication and Kerberos Armoring

- There are two group policy settings that must be configured to enable Kerberos support for authentication policies and silos in a domain. The *KDC support for claims, compound authentication, and Kerberos armoring* setting under *Computer Configuration > Policies > Administrative Templates > System > KDC* must be set to Supported for domain controllers. Link the GPO to the *Domain Controllers* OU.



- For all domain members (Windows 8 and Windows Server 2012 or later), *Kerberos client support for claims, compound authentication, and Kerberos armoring* should be set to Enabled under *Computer Configuration > Policies > Administrative Templates > System > Kerberos*. Link the GPO to the domain.

Create an Authentication Policy and Silo

- Before creating a silo, we'll define an authentication policy that sets the lifetime of the Kerberos Ticket Granting Ticket (TGT). Domain accounts must have a configured TGT lifetime for silos to work. The cmdlets in this article can be run from a domain controller as a domain administrator or from a domain-joined device where the Active Directory

Module for Windows PowerShell is installed. You should run these commands as a domain administrator.

- First let's create a new authentication policy and set the TGT lifetime for the policy to two hours using the *New-ADAuthenticationPolicy* cmdlet. After a two hour period, users must re-authenticate. The default TGT lifetime in AD is four hours.

```
New-ADAuthenticationPolicy -Name 2hr_Admin_TGT -Description '2hr TGT for admins'  
-UserTGTLifetimeMins 120 -Enforce -ProtectedFromAccidentalDeletion $true
```

- If you're experimenting with silos and authentication policies for the first time, you might want to omit the *-enforce* parameter from both the *New-ADAuthenticationPolicy* and *New-ADAuthenticationPolicySilo* cmdlets so that both are set to audit only mode.
- Before setting the access conditions for the policy, let's create a new silo that applies the previously created authentication policy to computer, service, and user accounts:

```
New-ADAuthenticationPolicySilo -Name Restricted_Admin_Logon -Description 'Restrict  
admins to DCs' -UserAuthenticationPolicy 2hr_Admin_TGT -ComputerAuthenticationPolicy  
2hr_Admin_TGT -ServiceAuthenticationPolicy 2hr_Admin_TGT -Enforce  
-ProtectedFromAccidentalDeletion $true
```

Now set the access control conditions to restrict the devices that can request a TGT for the user accounts assigned to the policy. In other words, the following configuration restricts users to

which our authentication policy applies, to only interact with computer accounts associated with the Restricted_Admin_Logon silo.

```
PS C:\Users\CONTOSO\DC1\administrator> New-ADAuthenticationPolicy -Name '2hr_Admin_TGT' -Description '2hr TGT for admins' -UserTGTLifetimeMins 120 -ProtectedFromAccidentalDeletion $true  
PS C:\Users\CONTOSO\DC1\administrator> New-ADAuthenticationPolicySilo -Name 'Restricted_Admin_Logon' -Description 'Restrict admins to DCs' -UserAuthenticationPolicy '2hr_Admin_TGT' -ComputerAuthenticationPolicy '2hr_Admin_TGT' -ServiceAuthenticationPolicy '2hr_Admin_TGT' -ProtectedFromAccidentalDeletion $true  
PS C:\Users\CONTOSO\DC1\administrator> Set-ADAuthenticationPolicy -Identity '2hr_Admin_TGT' -UserAllowedToAuthenticateFrom 'O:SYG:SYD:(XA;OICI;CR;;WD;(@USER.ad://ext/AuthenticationSilo = "Restricted_Admin_Logon"))'
```

There will be no user accounts linked directly to our authentication policy, but instead they are assigned indirectly in the silo.

- We will also associate our domain controller computer accounts with the Restricted_Admin_Logon silo later. And don't worry, I'll translate the SDDL in the cmdlet below into plain English in the second part of this series.

```
Set-ADAuthenticationPolicy -Identity 2hr_Admin_TGT -UserAllowedToAuthenticateFrom 'O:SYG:SYD:(XA;OICI;CR;;WD;(@USER.ad://ext/AuthenticationSilo == "Restricted_Admin_Logon"))'
```

- Before continuing, let's check the configuration of the authentication policy. In the output, you should see the *UserAllowedToAuthenticateFrom* and *UserTGTLifetimeMins* AD attributes populated according to the values we assigned using PowerShell.

```
Get-ADAuthenticationPolicy -identity 2hr_admin_tgt
```

```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\CONTOSO\DC1\administrator> Get-ADAAuthenticationPolicy -identity 2hr_admin_tgt

ComputerAllowedToAuthenticateTo      :
ComputerTGTLifetimeMins           :
DistinguishedName                 : CN=2hr_Admin_TGT,CN=AuthN Policies,CN=AuthN Policy
                                         Configuration,CN=Services,CN=Configuration,DC=ad,DC=contoso,DC=com
Enforce                           : True
Name                             : 2hr_Admin_TGT
ObjectClass                       : msDS-AuthNPolicy
ObjectGUID                         : 39a951ba-d76e-4b94-858e-173e15bac125
ServiceAllowedToAuthenticateFrom   :
ServiceAllowedToAuthenticateTo     :
ServiceTGTLifetimeMins           :
UserAllowedToAuthenticateFrom      : O:SYG:SYD:(XA;OICI;CR;;;WD;(@USER.ad://ext/AuthenticationSilo ==
                                         "Restricted_Admin_Logon"))
UserAllowedToAuthenticateTo        :
UserTGTLifetimeMins             : 120

PS C:\Users\CONTOSO\DC1\administrator>
```

Enforce Policy and Silo

- If you decide to omit the *-Enforce* parameter from the *New-ADAAuthenticationPolicy* and *New-ADAAuthenticationPolicySilo* cmdlets at this stage, you can always enforce the authentication policy and silo later using the cmdlets below:

```
Set-ADAAuthenticationPolicy -Identity 2hr_Admin_TGT -Enforce $true
```

```
Set-ADAAuthenticationPolicySilo –Identity Restricted_Admin_Logon –Enforce $true
```

- In part two of this series, I'll show you how the mysterious SDDL that appears in the *Set-ADAAuthenticationPolicy* cmdlet above was determined, and then complete the configuration by associating the necessary AD account objects with the silo, and testing the results on a member server in the domain.

References:

1. <https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/authentication-policies-and-authentication-policy-silos>
2. <https://ittutorials.net/microsoft/>

Activity 4

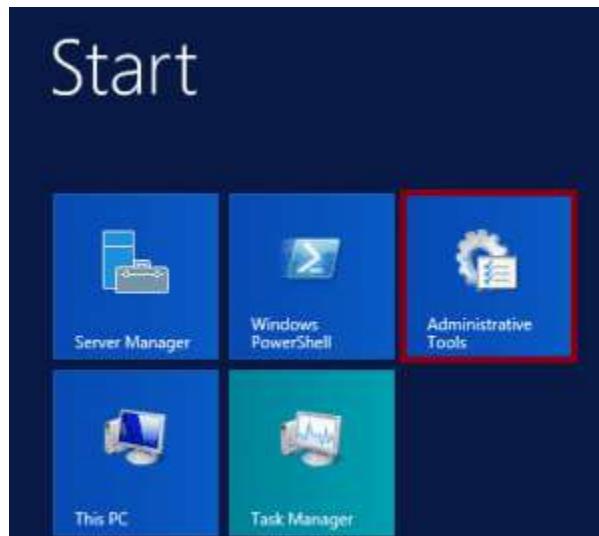
Aim: Creating Organizational Unit (OU) in Active Directory

Learning Outcome: Able to configure and Creating Organizational Unit (OU) in Active Directory

Duration: 2Hrs

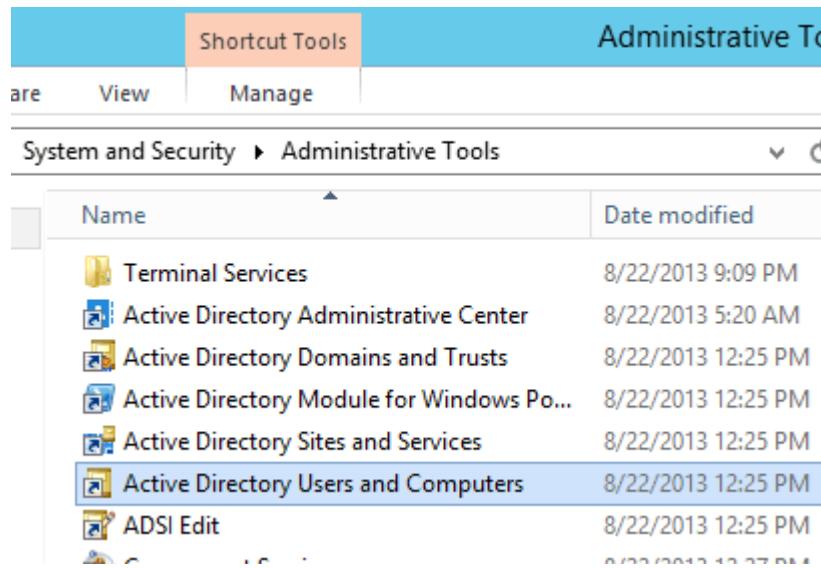
Procedure

Step 1: To create OU in Active Directory, we need to open “Active Directory Users and Computers”. Click on Start button and click administrative tools or you can run “dsa.msc” command in Run.

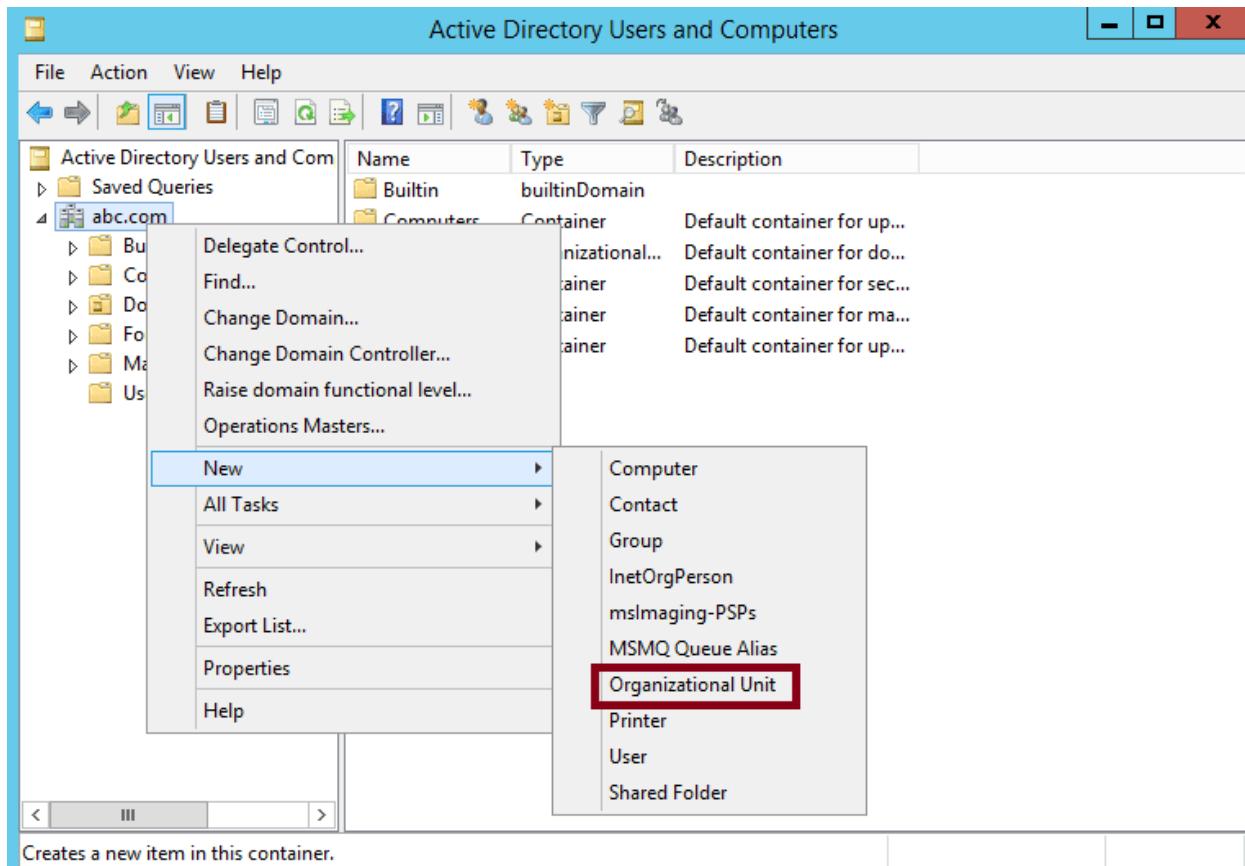


Step 2: In Administrative Tools Window, Click on Active Directory Users and Computers. Active Directory Users and Computers can also be open by clicking on Start, click on down

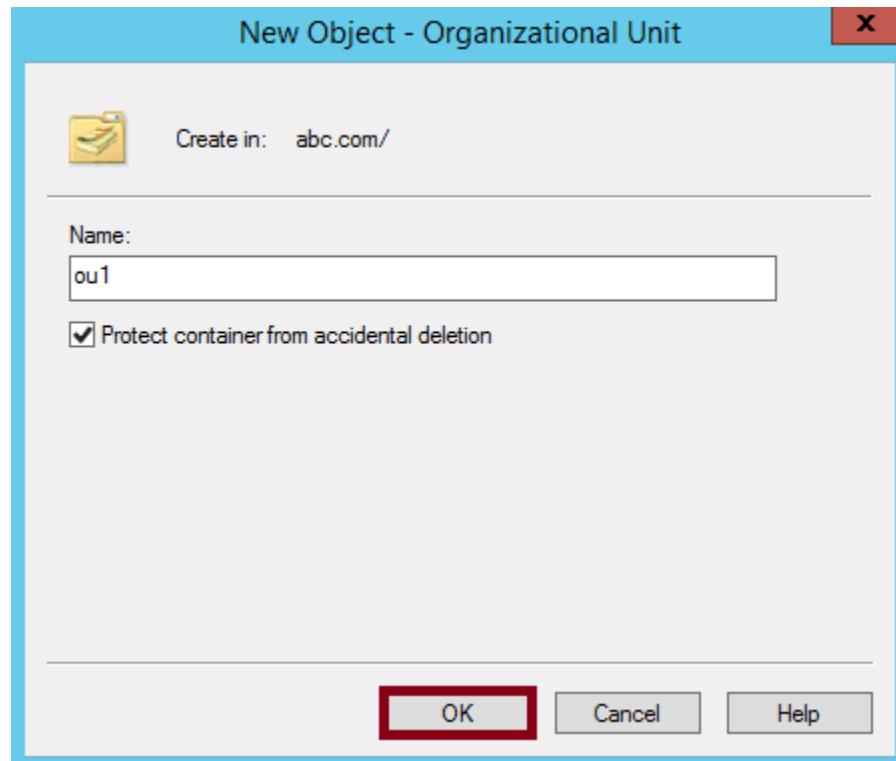
arrow and select “Active Directory User and Computer” or right click on Start, select run and type “DSA.MSC” and hit enter.



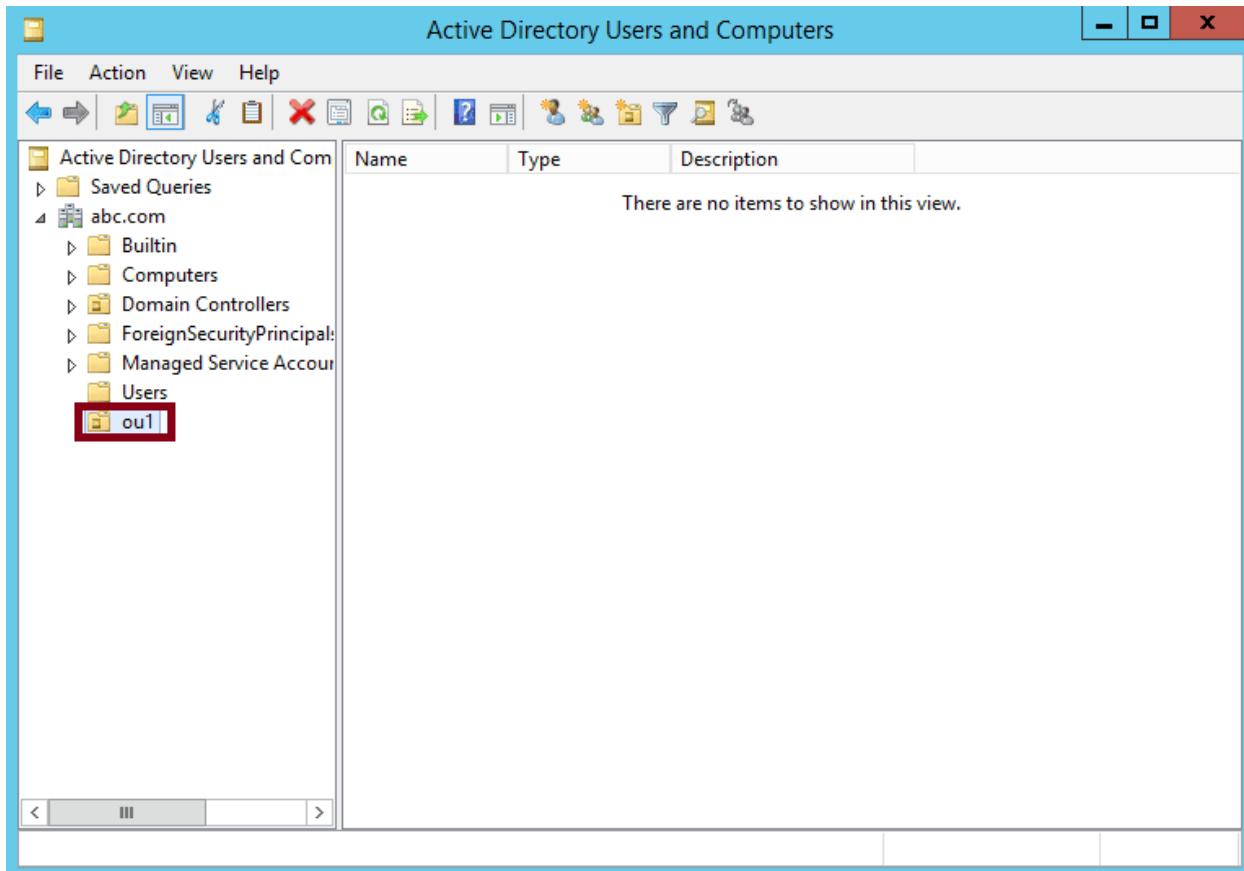
Step 3: In Active Directory Users and Computers window, right click on Domain. In this example domain name is ABC.COM. Click on “New”, it shows various options for creating new objects. We’ll talk about other options in future posts. To create an OU, click on “Organizational Unit”.



Step 4: It will open “New Object-Organizational Unit console”, type OU name in name tab. Select an option “protect the container from accidental deletion”, it will use enhance security and prevent accidental deletion of OU. We’ll cover the steps to delete an OU by removing extra protection in future articles. Click on OK to close the window.

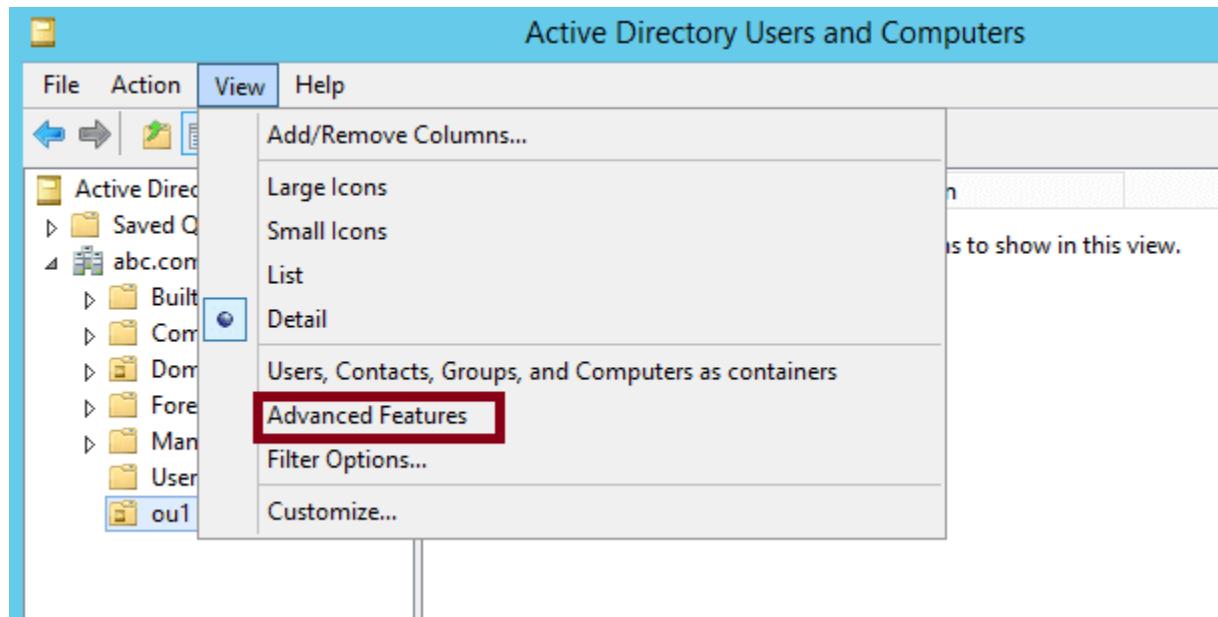


Step 5: Here we can see that the Organizational Unit (ou1) is created. Similarly we can create nested OUs by selecting an OU in which we want nested OU to be created.

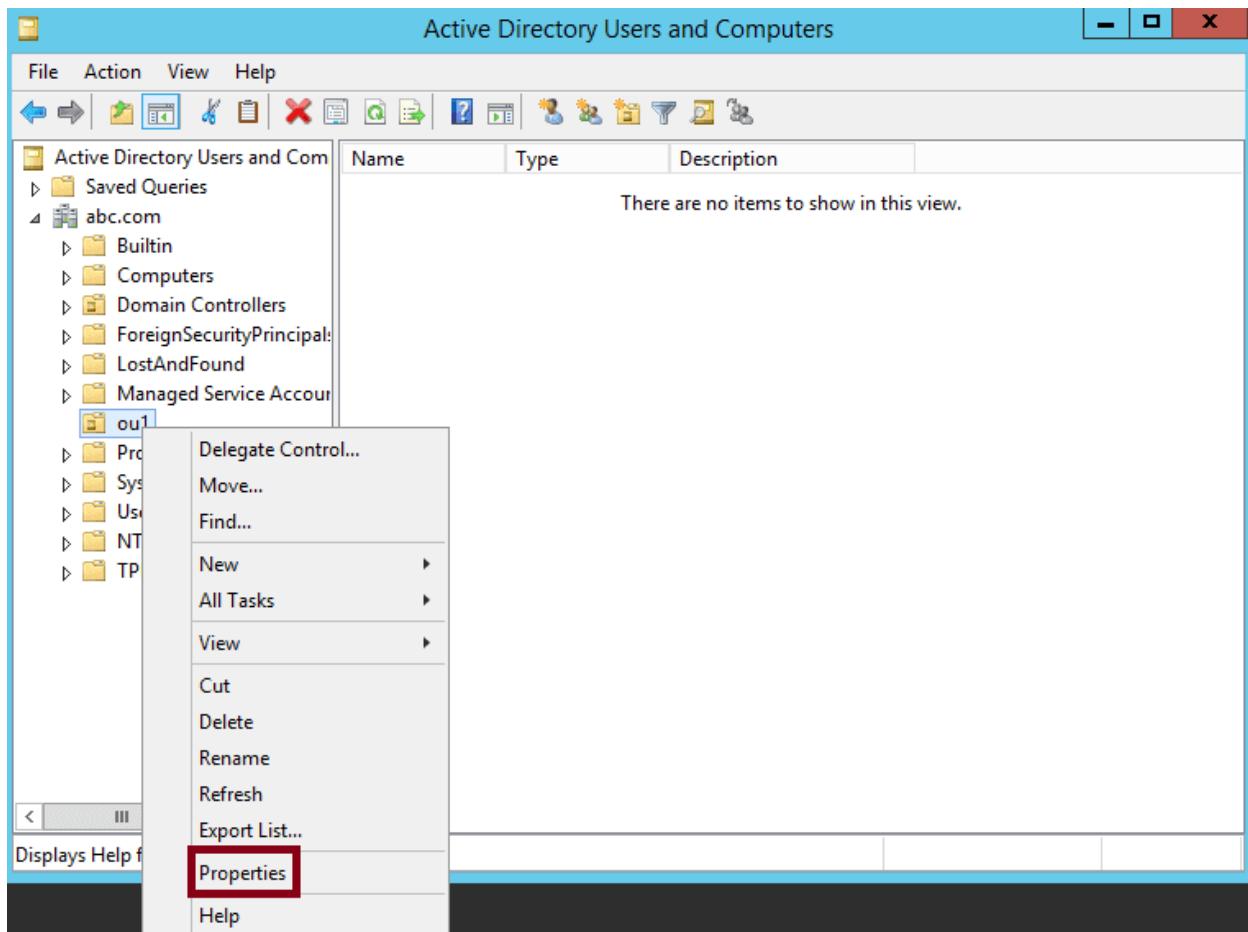


Steps to Delete Active Directory OU

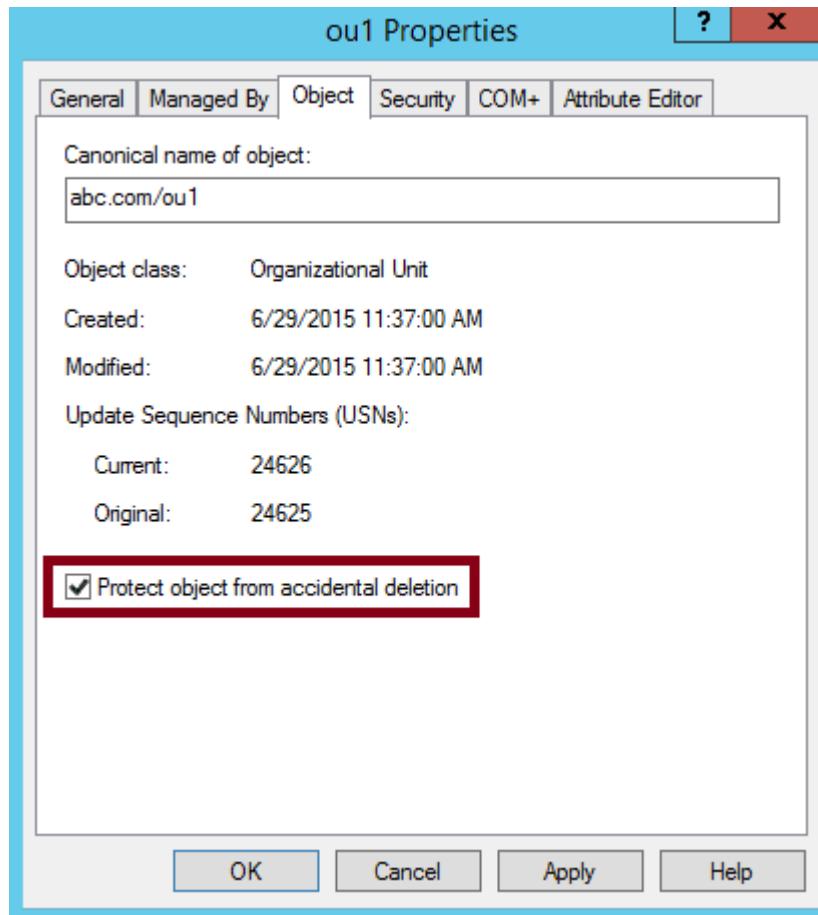
Step 6: For deleting an OU with enhanced security, first we have to disable “Protection from accidental deletion”. To disable accidental deletions click on ‘View’ and then select Advanced Features. Please ensure that you disable Advanced Features once you are done with the task.



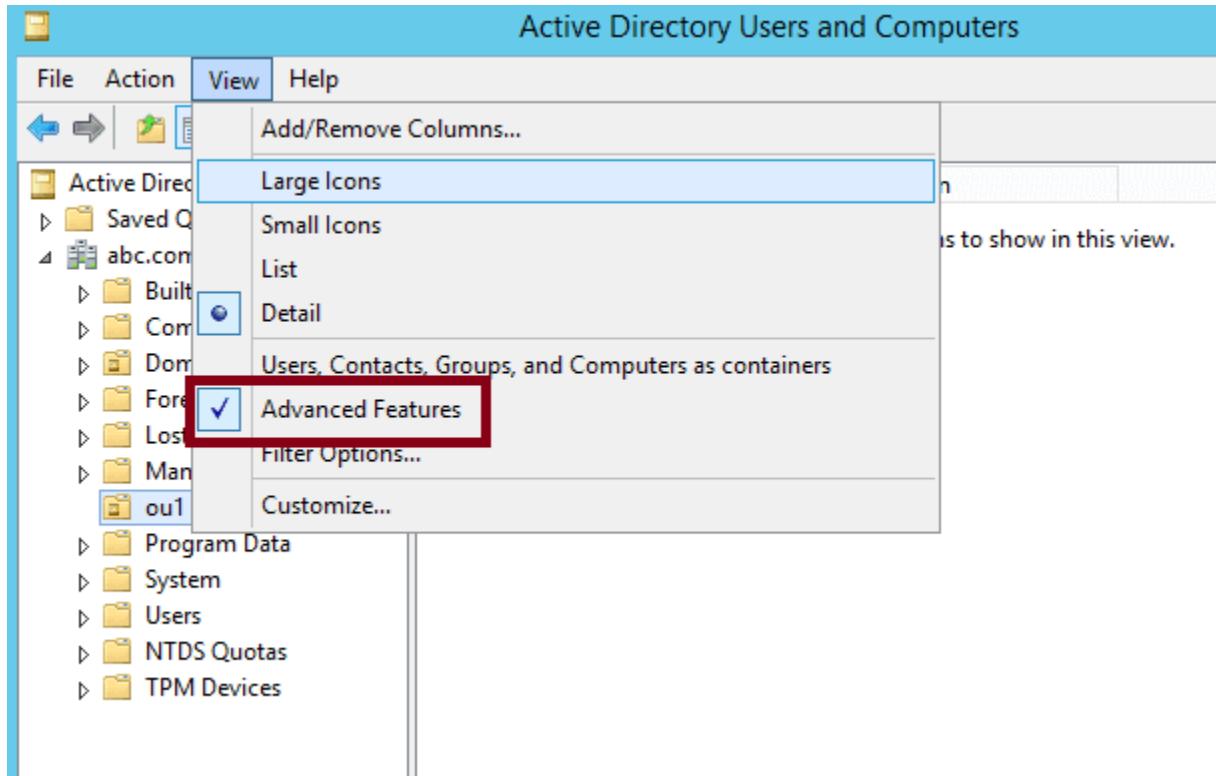
Step 7: After enabling Advanced Features, right click on Organizational Unit (ou1) i.e. the Active Directory OU for which you want to disable “Protection from accidental deletion” and click on Properties.



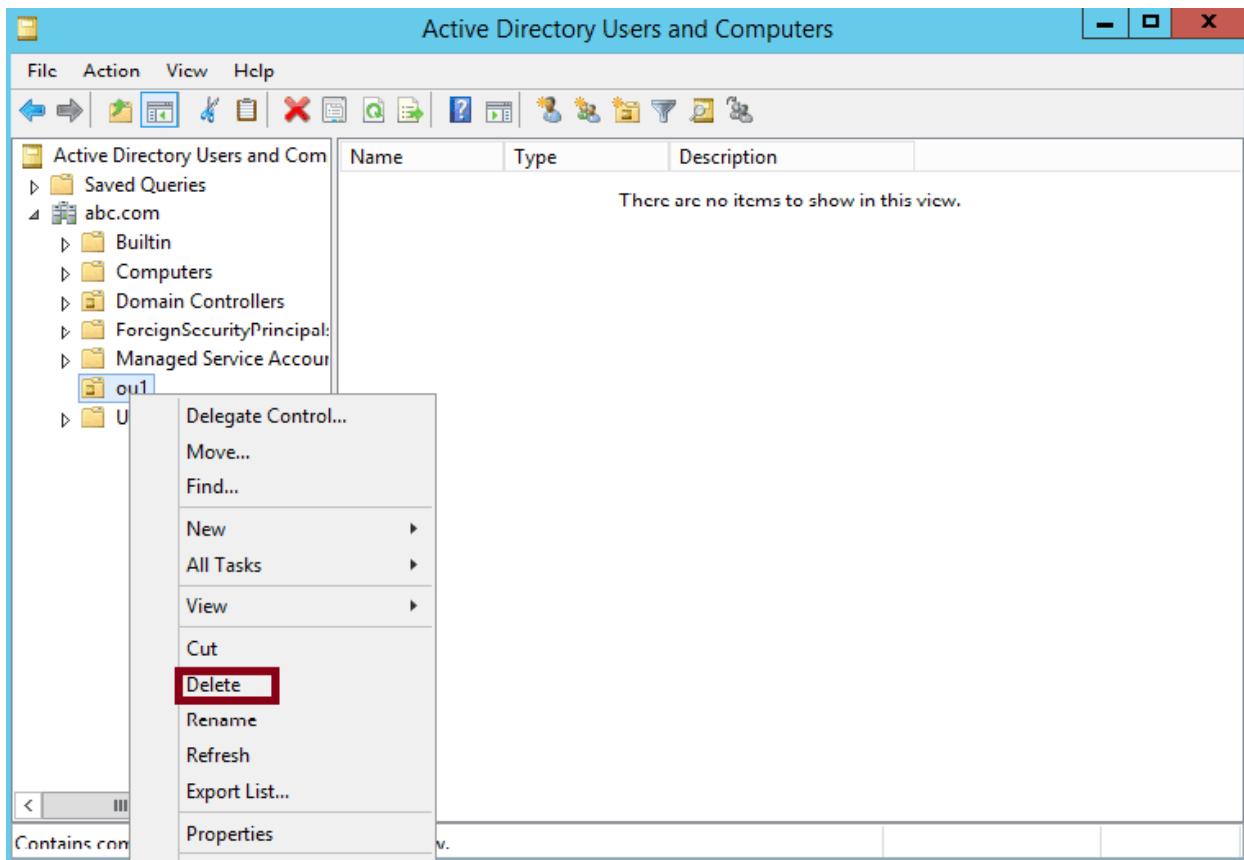
Step 8: In OU1 properties window, click on ‘object’ tab, here we can see an option checked for “Protect object from accidental deletion” option. Uncheck that enhanced security options and click OK. This option will not be visible if Advanced Feature is not enabled (step 6).



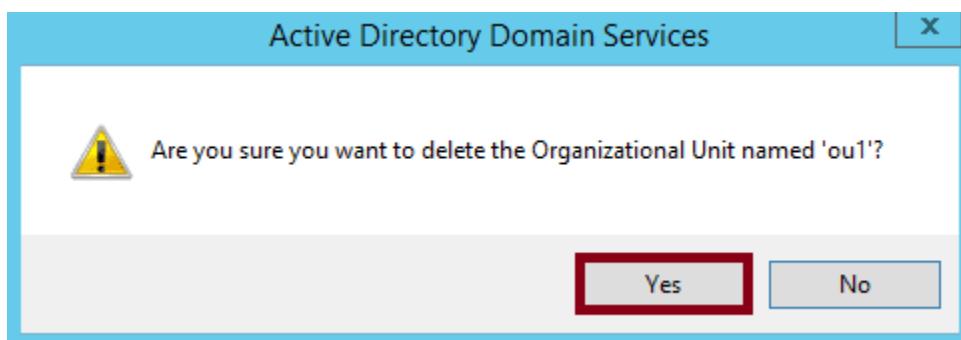
Step 9: Please ensure that advanced feature is not enable all the time and it's disabled once you are done with the task. To disable advanced feature click on View and uncheck the Advanced Feature option.



Step 10: Now when “Protection from accidental deletion” is disabled, for deleting OU, right click on OU and click on Delete.



Step 11: Here, we have to confirm that we want to delete the Organizational Unit named 'ou1' by click on YES.



Step 12: Now we can verify that Organizational Unit (ou1) is deleted.

The screenshot shows the 'Active Directory Users and Computers' management console. The left pane displays the navigation tree for the 'abc.com' domain, which includes 'Saved Queries', 'Builtin', 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipals', 'Managed Service Accounts', and 'Users'. The right pane is a table titled 'Active Directory Users and Computers' with columns 'Name', 'Type', and 'Description'. The table lists several objects:

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Con...	Organizational...	Default container for do...
ForeignSecu...	Container	Default container for sec...
Managed Se...	Container	Default container for ma...
Users	Container	Default container for up...

References:

1. <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/creating-an-organization-unit-design>
2. <https://johnkeen.tech/windows-server-2016-006-organizational-units-and-group-policy-objects/>
3. https://www.server-world.info/en/note?os=Windows_Server_2016&p=active_directory&f=5

Activity 5

Aim: Plan and Maintain Group Policies

Learning Outcome: Able to configure Plan and Maintain Group Policies

Duration: 2Hrs

Procedure

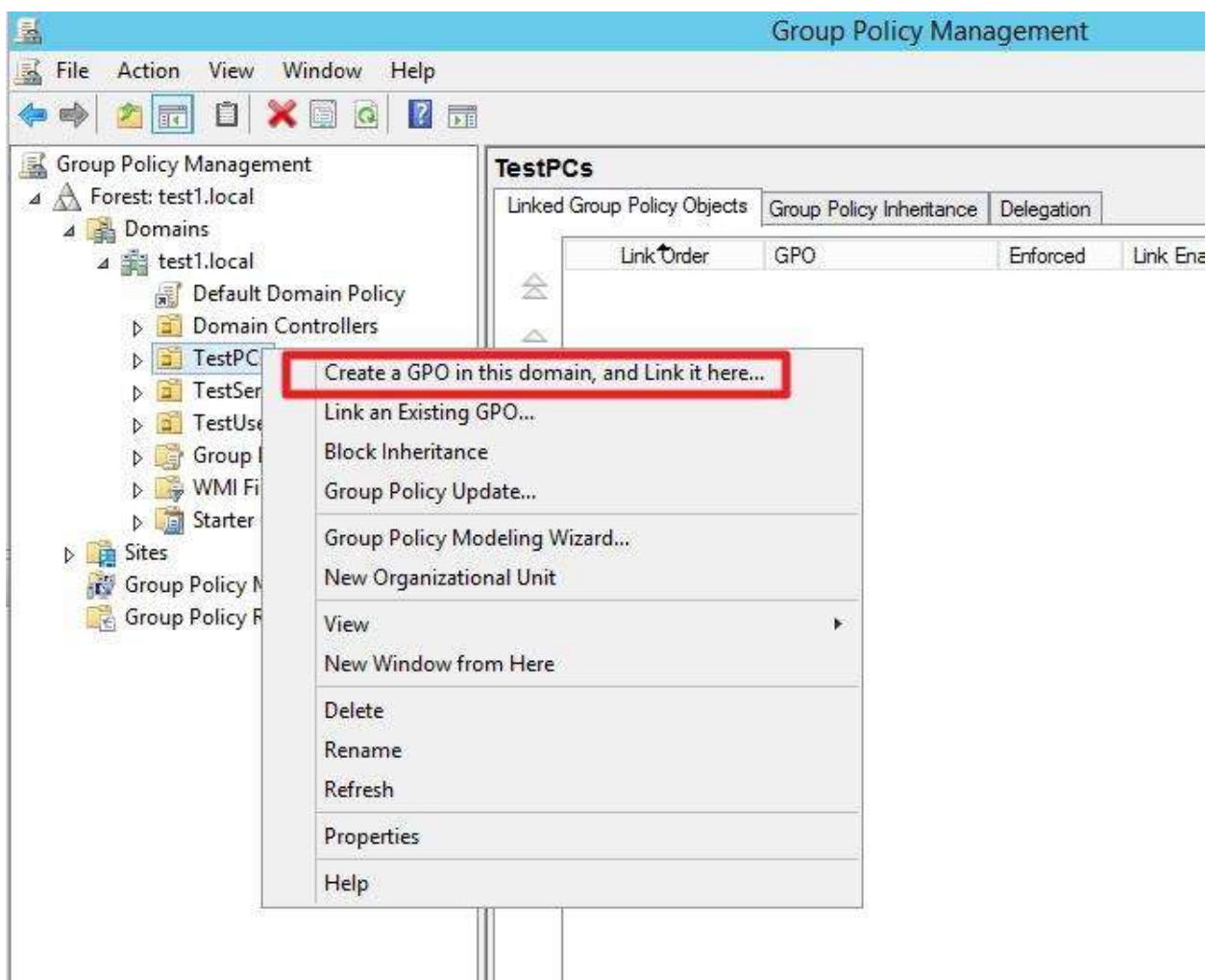
Step 1: On your domain controller open search (or run) and type in gpmc.msc

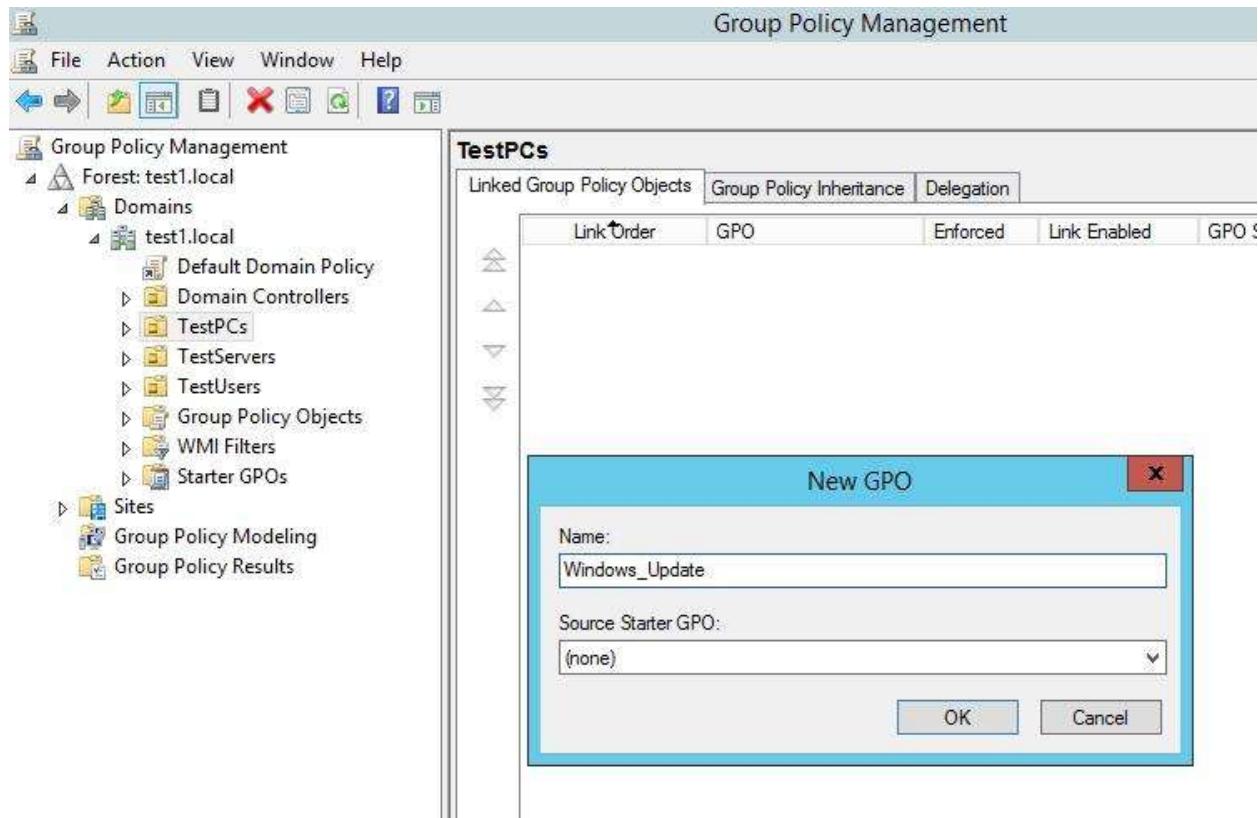
Step 2: Click on gpmc



Create different Organizational Units for different types of computers and users in your environment so you can fine tune your group policy and permissions also.

Step 2: You can create new organization unit in Active Directory Users and Computers | right click on domain name | New – Organizational Unit

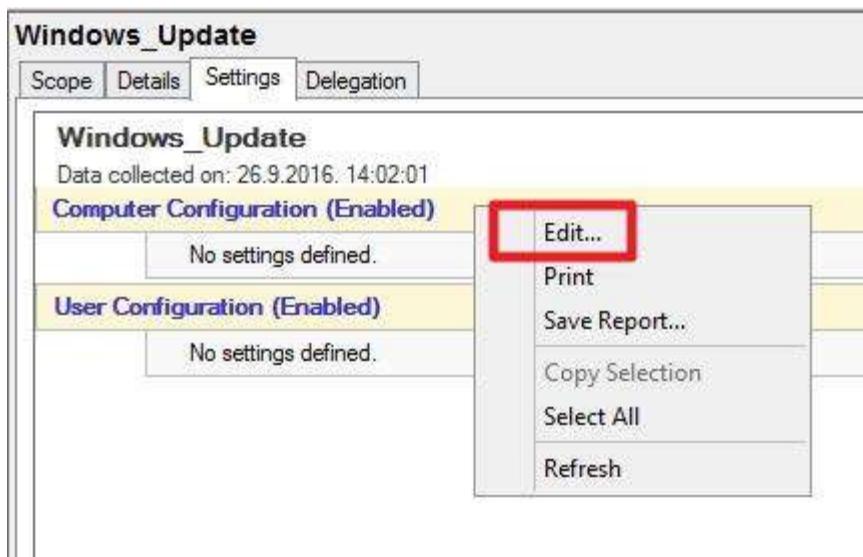




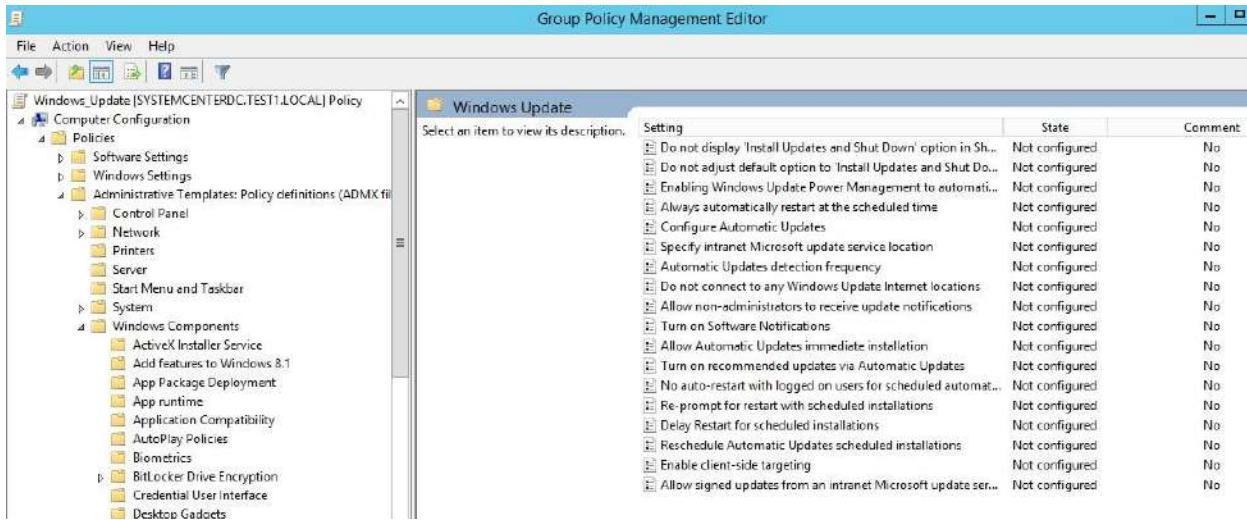
Step 4: Select created Windows_Update GPO (group policy object) and click on Settings tab on the right part of the screen



Step 5: Right click on Computer Configuration |Edit

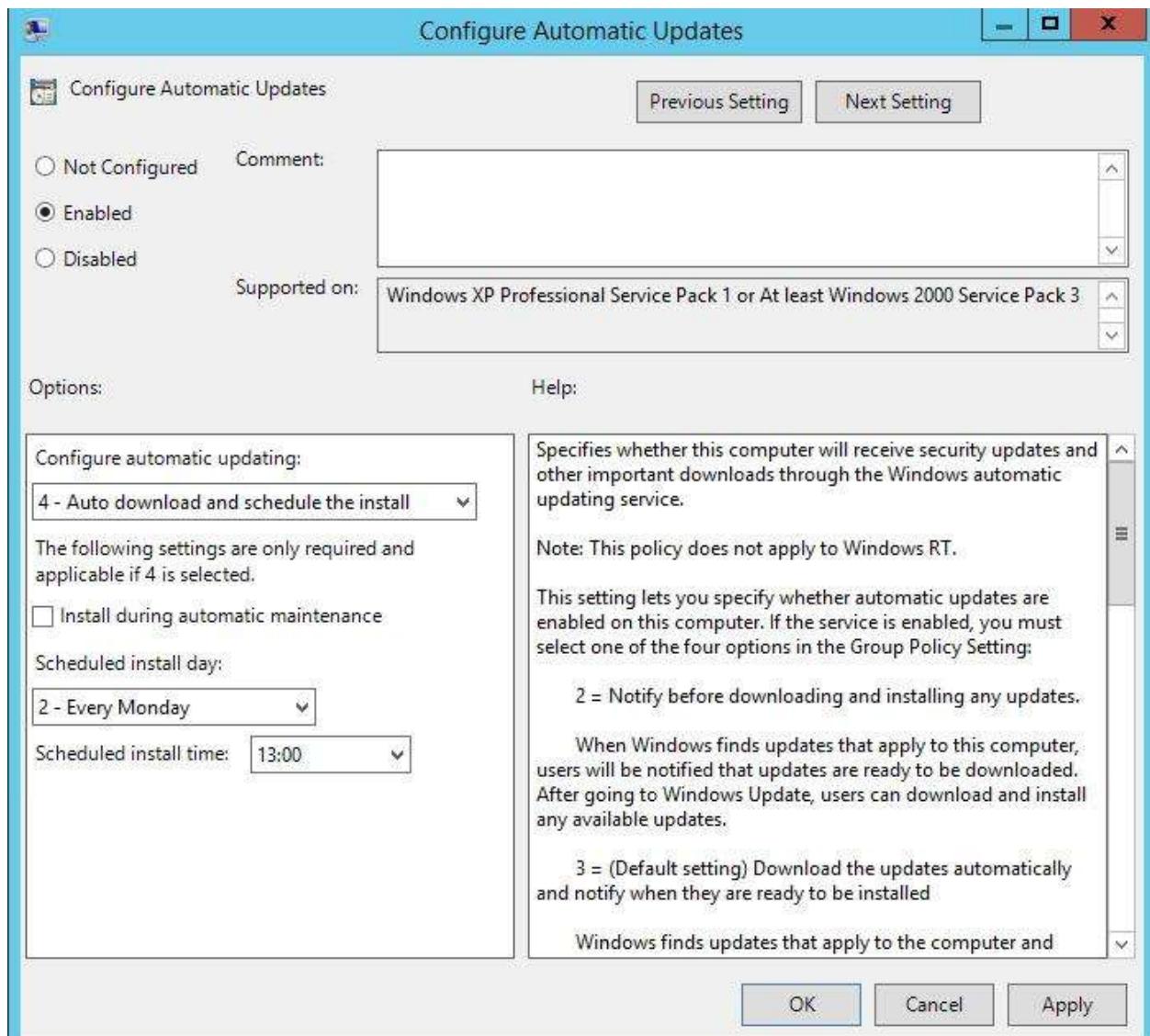


Step 6: Click on Computer Configuration | Policies | Administrative Templates | Windows Components | Windows Update



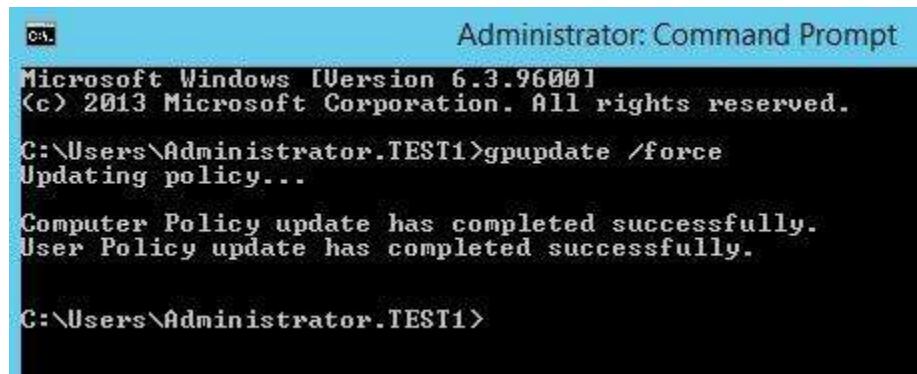
Step 7: Double click on Configure Automatic Updates |Enabled | under Options define how you would like your updates to work. You choose following

- Configure automatic updating: 4 – Auto download and schedule the install
- Schedule install day: 2 – Every Monday at 13:00h
- Apply |OK



- In order to confirm that this setting is working we need to test on one of the PCs that are affected by this policy.

Step 8: Log on onto the PC – command prompt with administrative privileges (run as administrator) : gpupdate /force



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.TEST1>gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\Administrator.TEST1>
```

Step 9: After that if we check under Control Panel | Windows Update | Change settings (right part of the screen) we see that update settings are changed



References:

1. <https://www.microsoftpressstore.com/articles/article.aspx?p=2217265&seqNum=2>
2. <https://support.microsoft.com/en-in/help/324802/how-to-configure-group-policies-to-set-security-for-system-services-in>
3. <https://www.techrepublic.com/blog/data-center/whats-new-for-group-policy-in-windows-server-2012/>

Activity 6

Aim: Configure User Environment

Learning Outcome: Able to configure add and remove user Environment

Duration: 2Hrs

Procedure

Add a user account

.Step 1: Open the Windows Server Dashboard.

Step 2: On the navigation bar, click Users.

Step 3: In the Users Tasks pane, click Add a user account. The Add a User Account Wizard appears.

Step 4: Follow the instructions to complete the wizard.

Remove a user account

Step 1: Open the Windows Server Essentials Dashboard.

Step 2: On the navigation bar, click Users.

Step 3: In the list of user accounts, select the user account that you want to remove.

Step 4: In the <User Account> Tasks pane, click Remove the user account. The Delete a User Account Wizard appears.

On the Do you want to keep the files? page of the wizard, you can choose to delete the user's files, including File History backups and the redirected folder for the user account. To keep the user's files, leave the check box empty. After making your selection, click Next.

Step 5: Click Delete account.

References:

1. <https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/set-up-the-lab-environment-for-ad-fs-in-windows-server-2012-r2>
2. <https://docs.microsoft.com/en-us/windows-server/storage/folder-redirection/deploy-roaming-user-profiles>

Activity 7

Aim: Install and Configure Active Directory Services

Learning outcome: Able to configure different protocol services

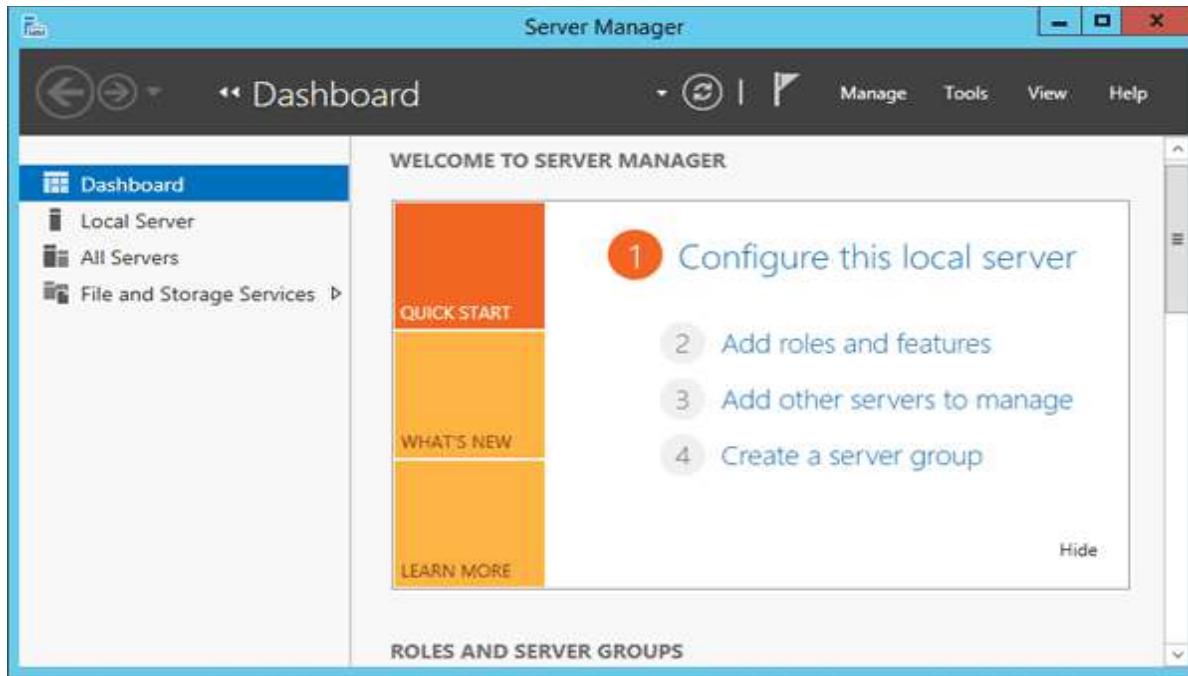
Duration: 2 hour

List of Hardware/Software requirements:

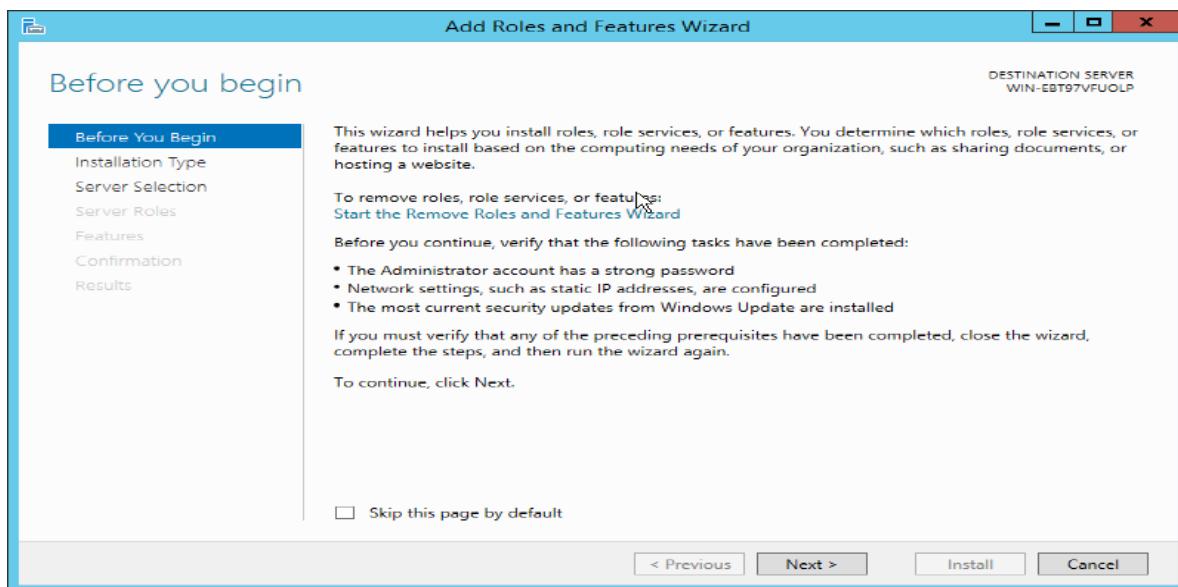
1. Windows Server 2012 R2
2. VMWare Workstation
3. Computer with 8GB RAM/500 GB HD

Code/Program/Procedure (with comments):

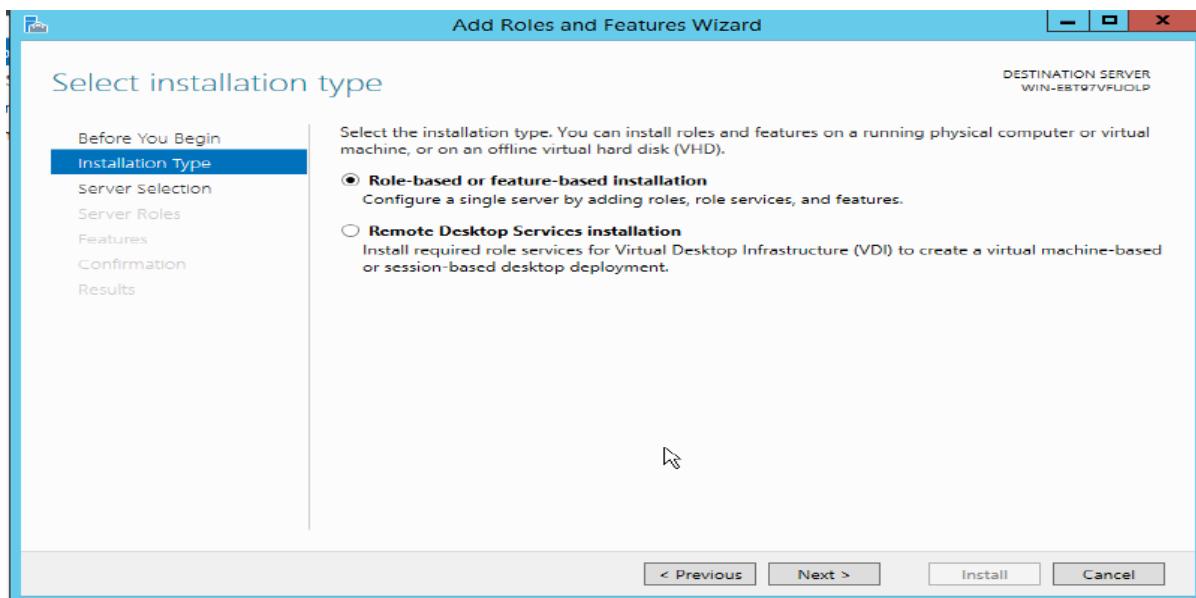
1. Open Server Manager Console and select Manage > Add Roles and Features.



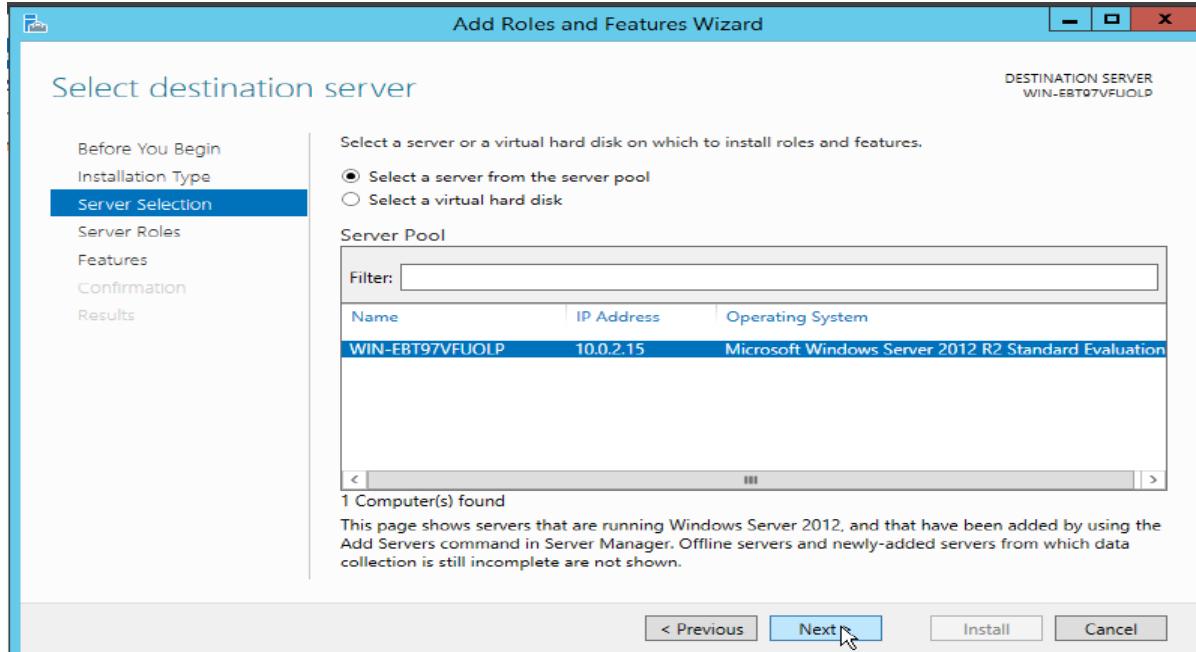
2. In Server Manager, go to Manage, and click Add Roles and Features. It opens the Add Roles and Features Wizard. Click Next.



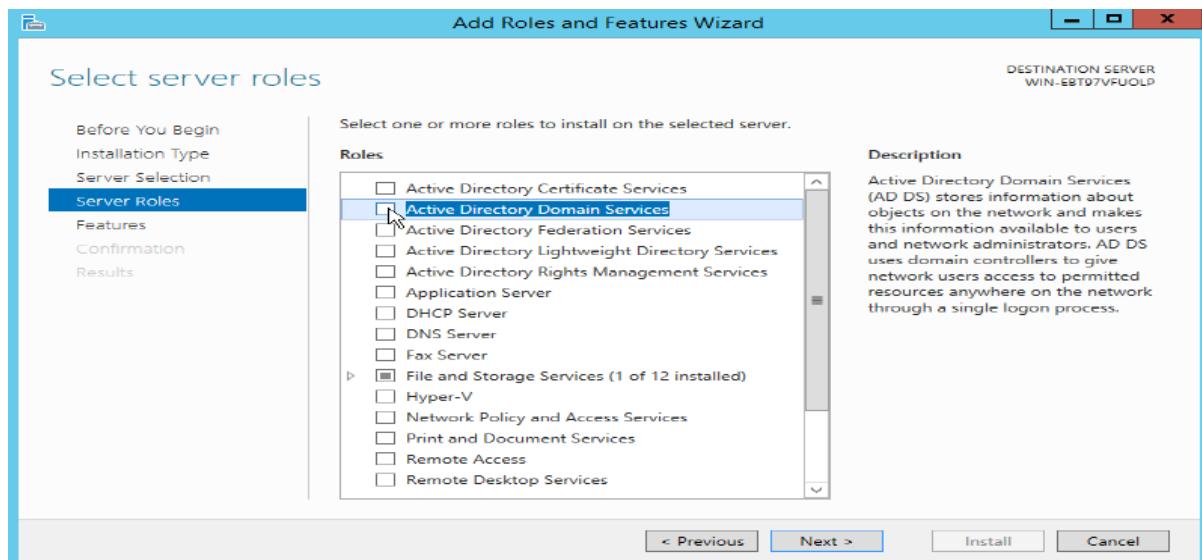
3. In Select Installation Type, select Role-based or feature-based installation and click Next.



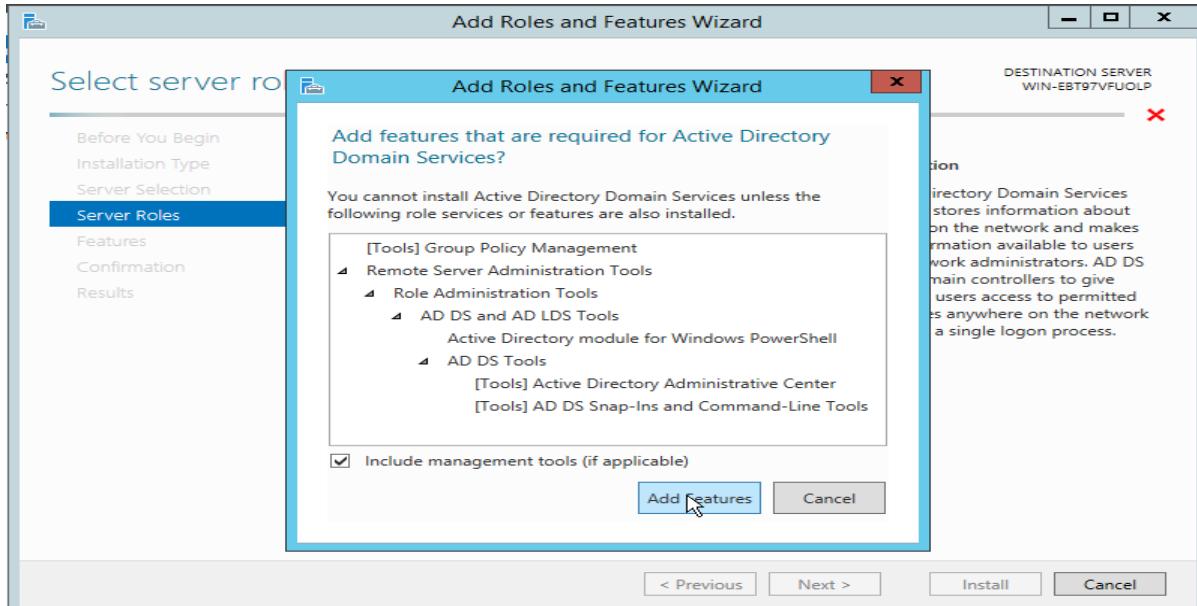
4. Select “Select a server from the server pool”. In Server Pool, ensure that the local computer is selected and click Next.



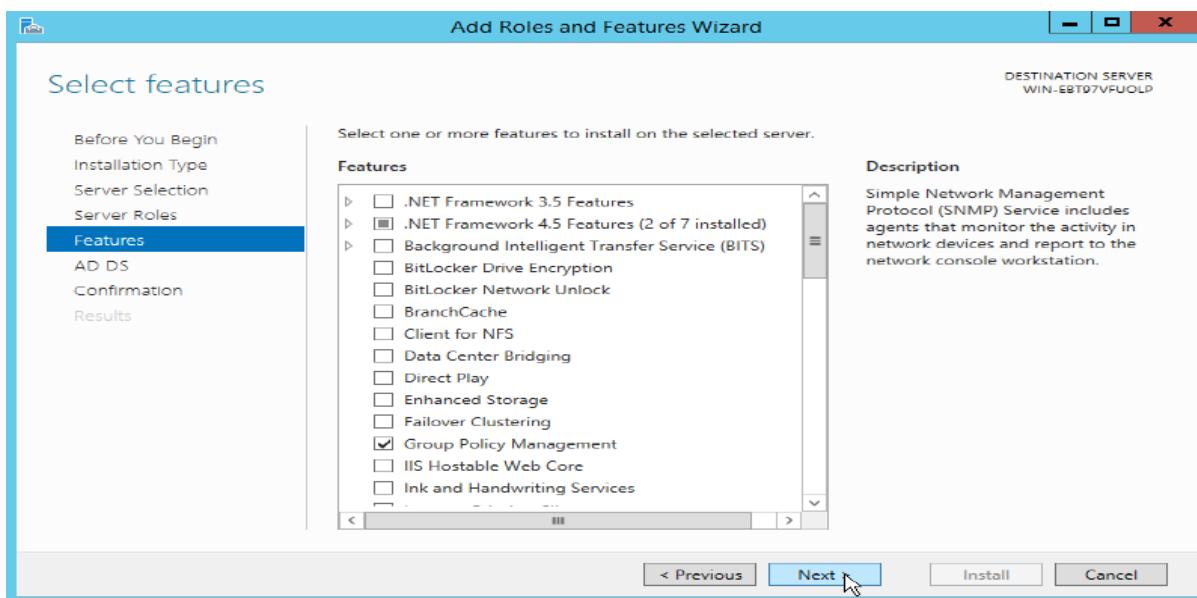
5. Select Active Directory Domain Services from Roles.



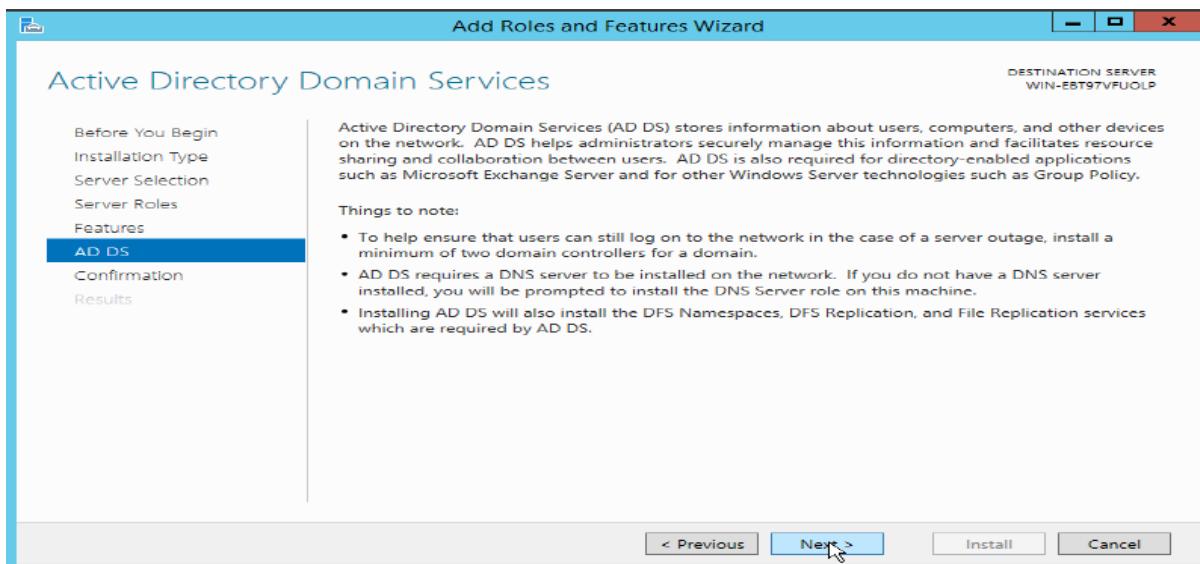
6. You will be prompted to add required features. Click Add Features and then click Next.



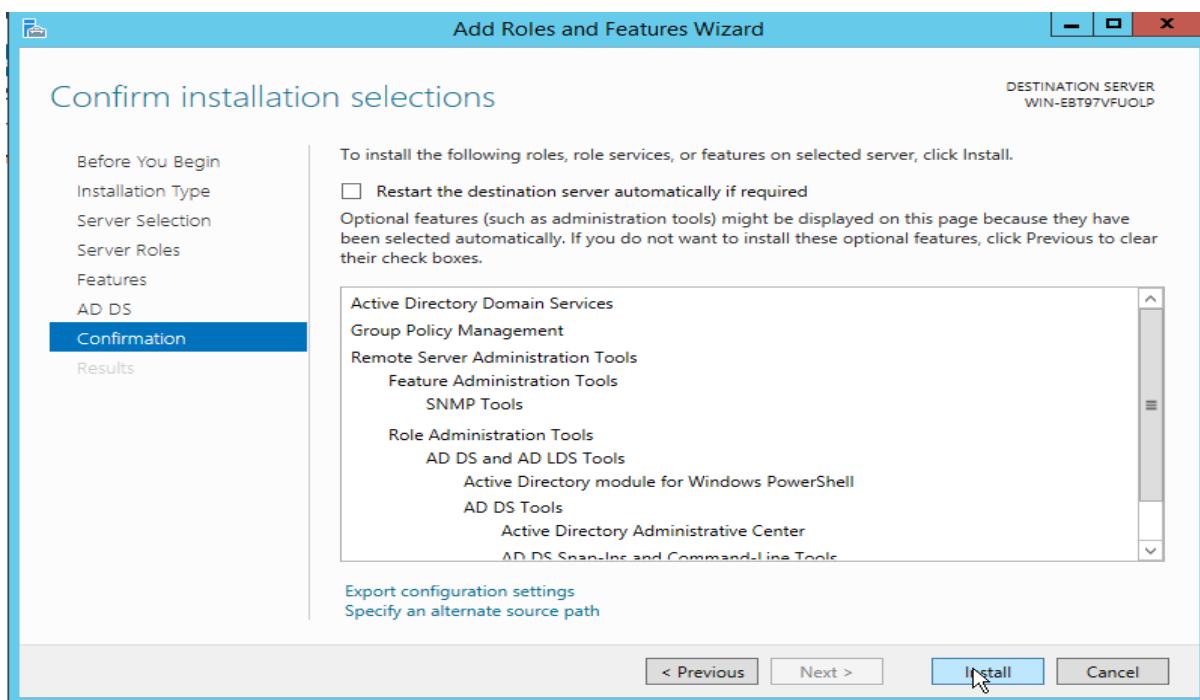
7. In Features, select Next.



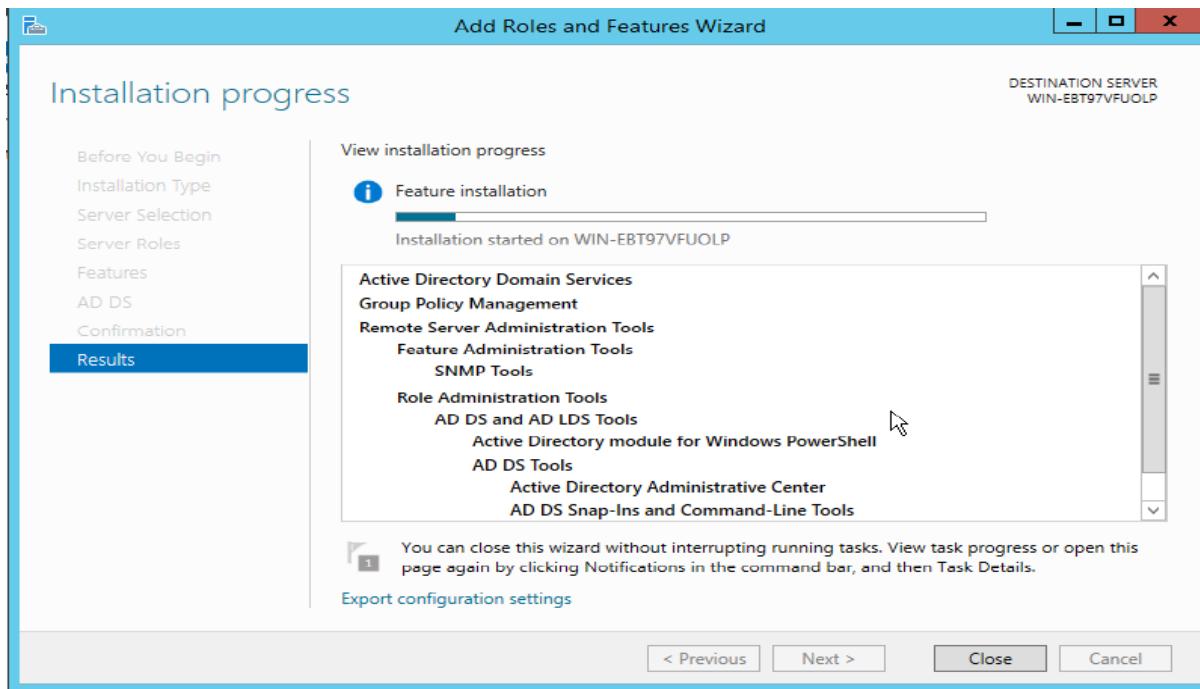
8. Read the information in Active Directory Domain Services page and click Next.



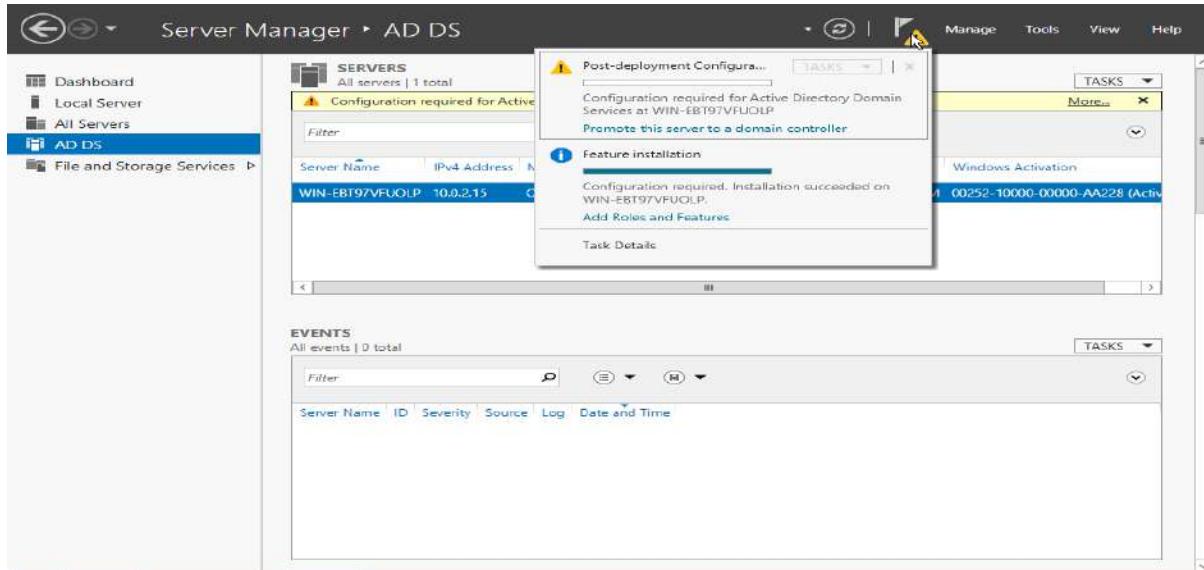
9. In the Confirmation page, click Install to install the roles, role services, or features on the server.



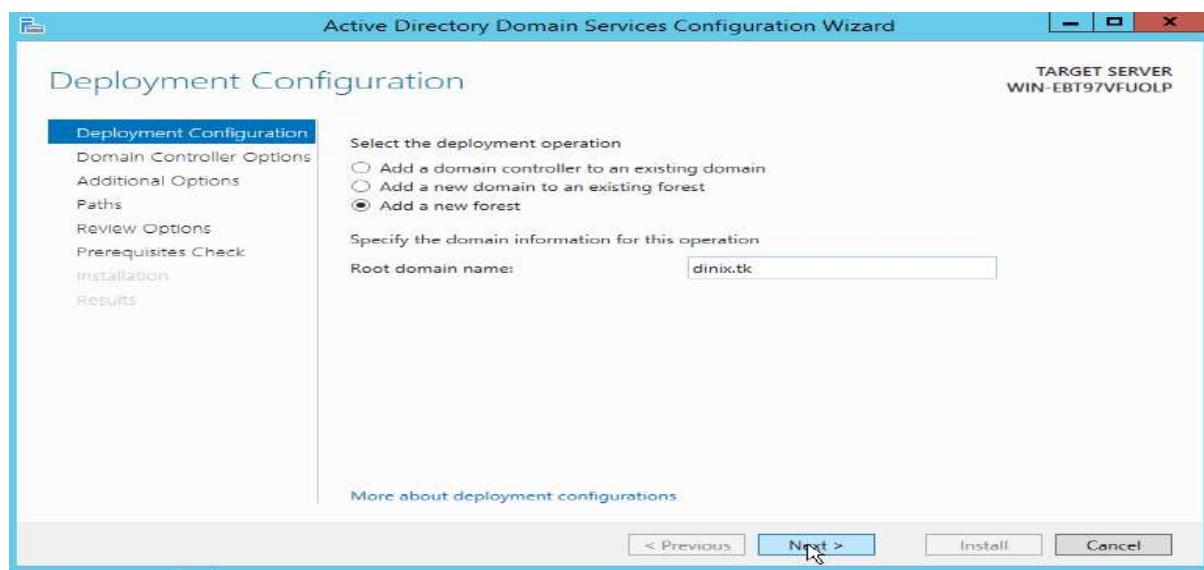
10. The installation process will start. You may close the wizard.



11. When the installation is completed, click on Notifications in Server Manager, and click on the link Promote this server to a domain controller.

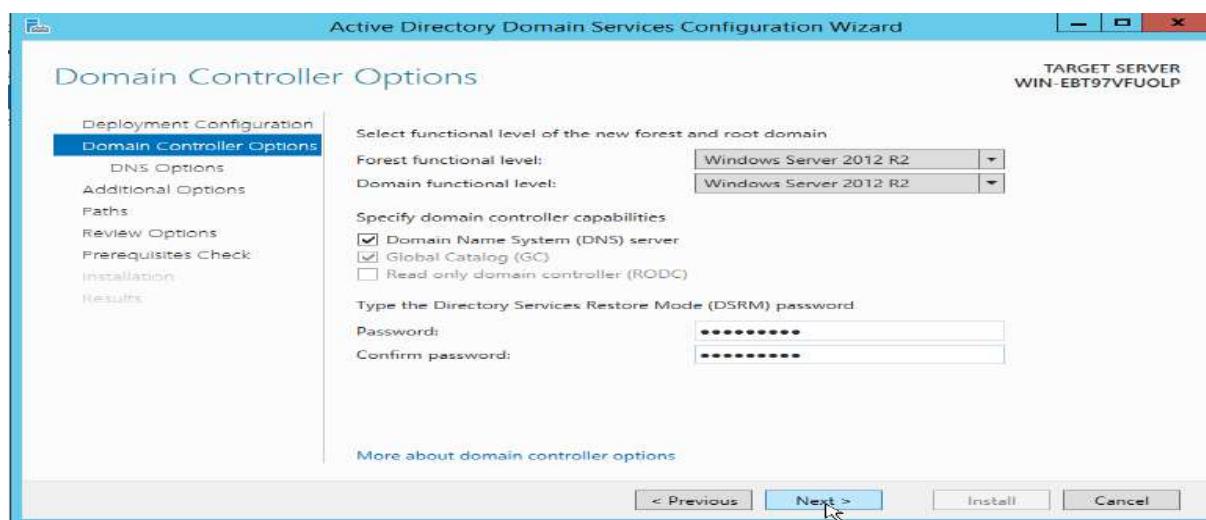


- When the Active Directory Domain Services Configuration Wizard opens, select Add a new forest and enter Root domain name. Then click Next.

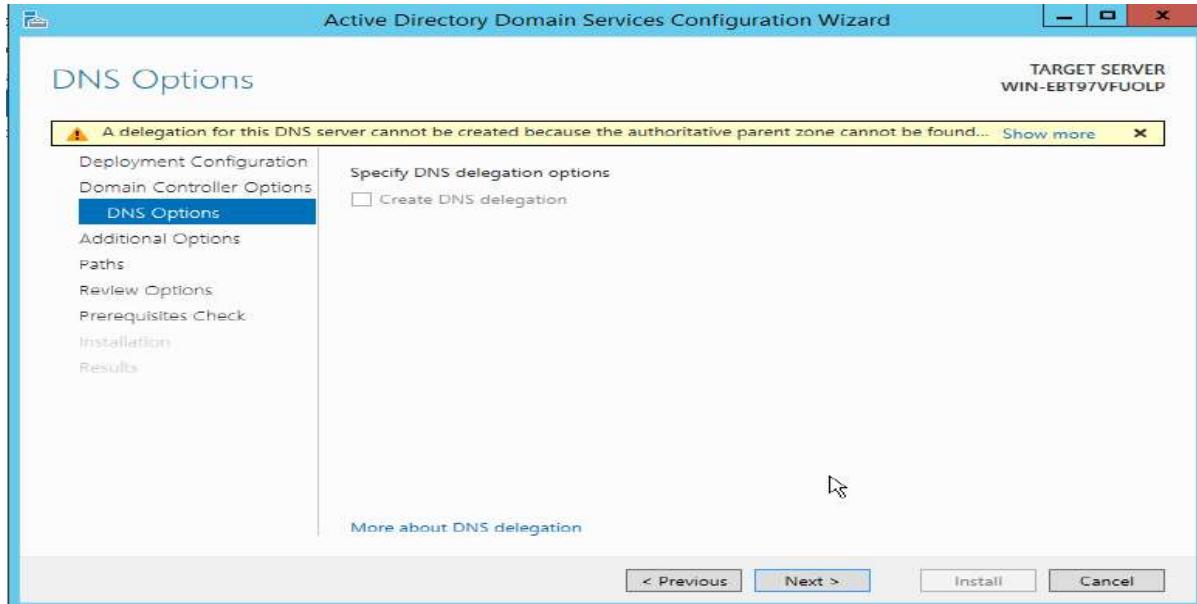


-
13. In Domain Controller Options, leave Forest functional level and Domain functional level as default. Leave Domain Name System (DNS) server checked. Provide a password for Directory Services Restore Mode and click Next.

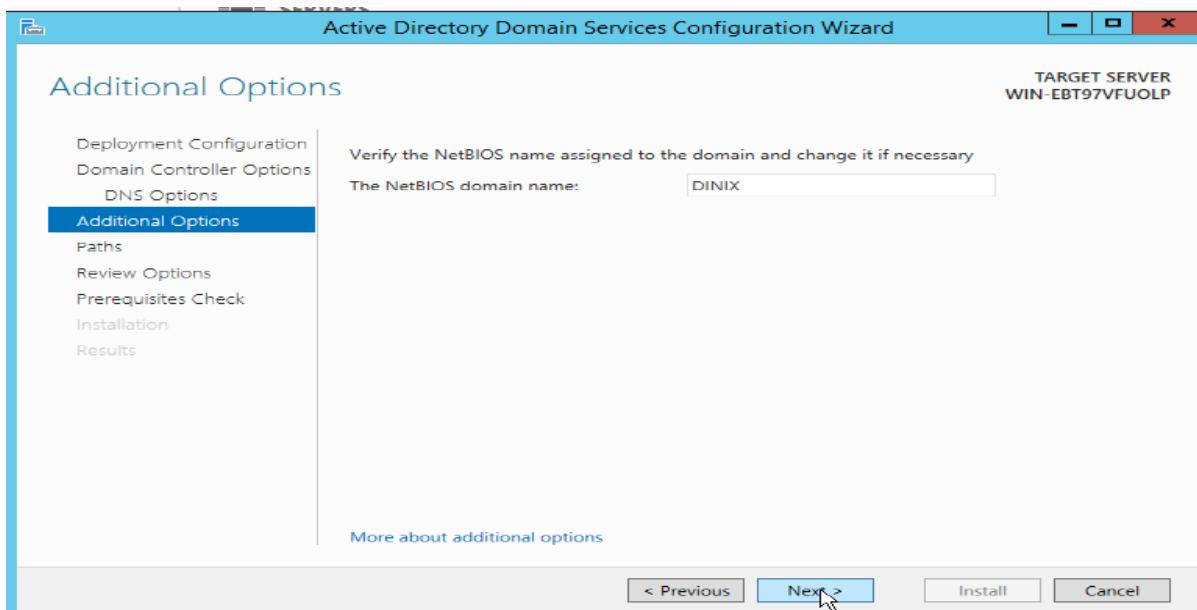
(Note: DSRM password is required when booting the domain controller into recovery mode)



14. Ignore the warning given in DNS Options page. Click Next.

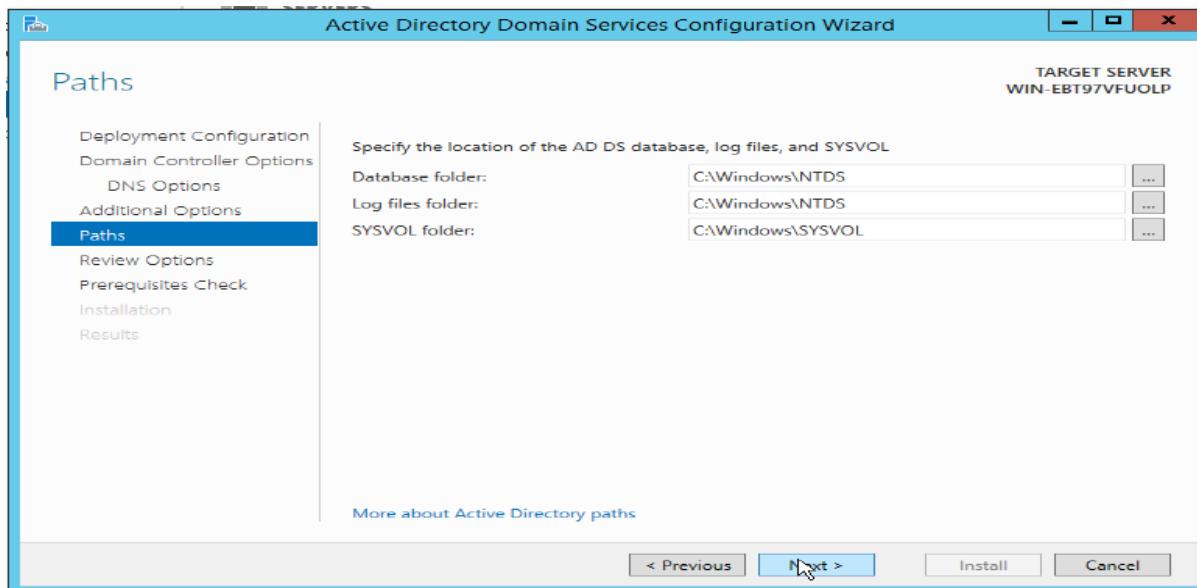


15. Verify NetBIOS domain name. Click Next.

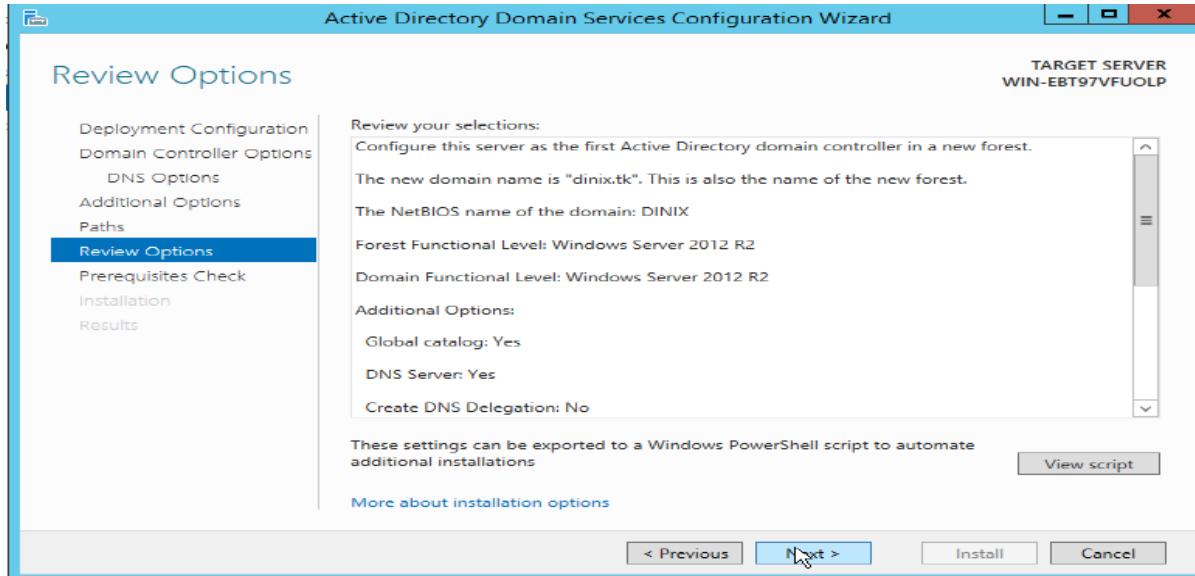


16. Specify locations for AD DS Database folder, Log Files folder, and SYSVOL folder.

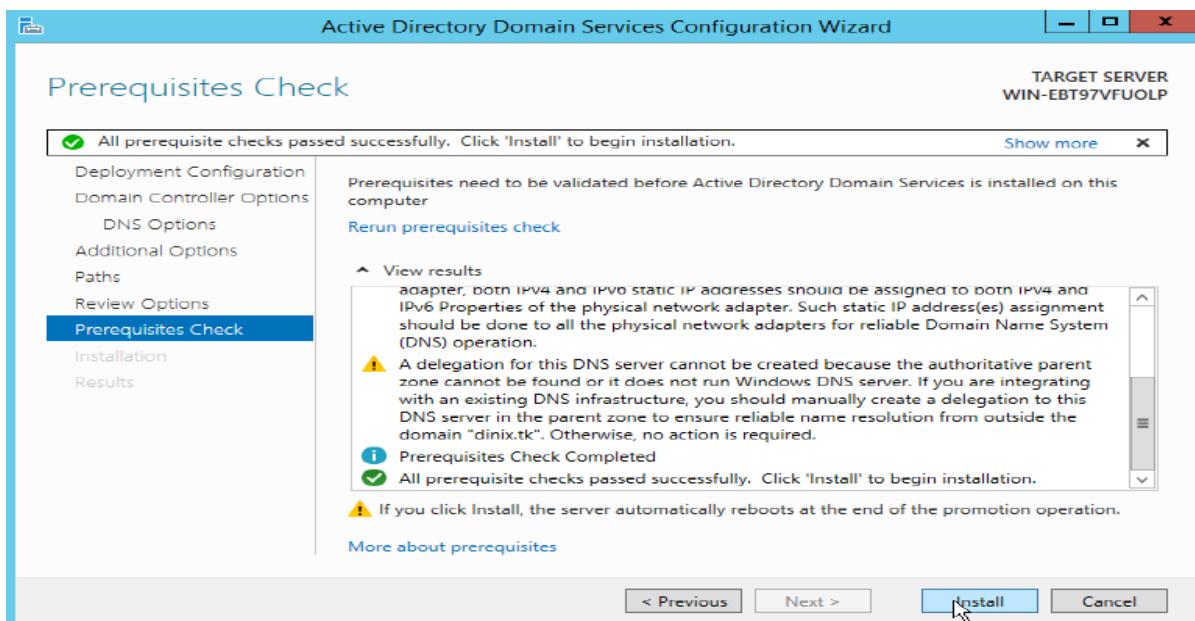
(Note: It is recommended to leave these as defaults). Click Next.



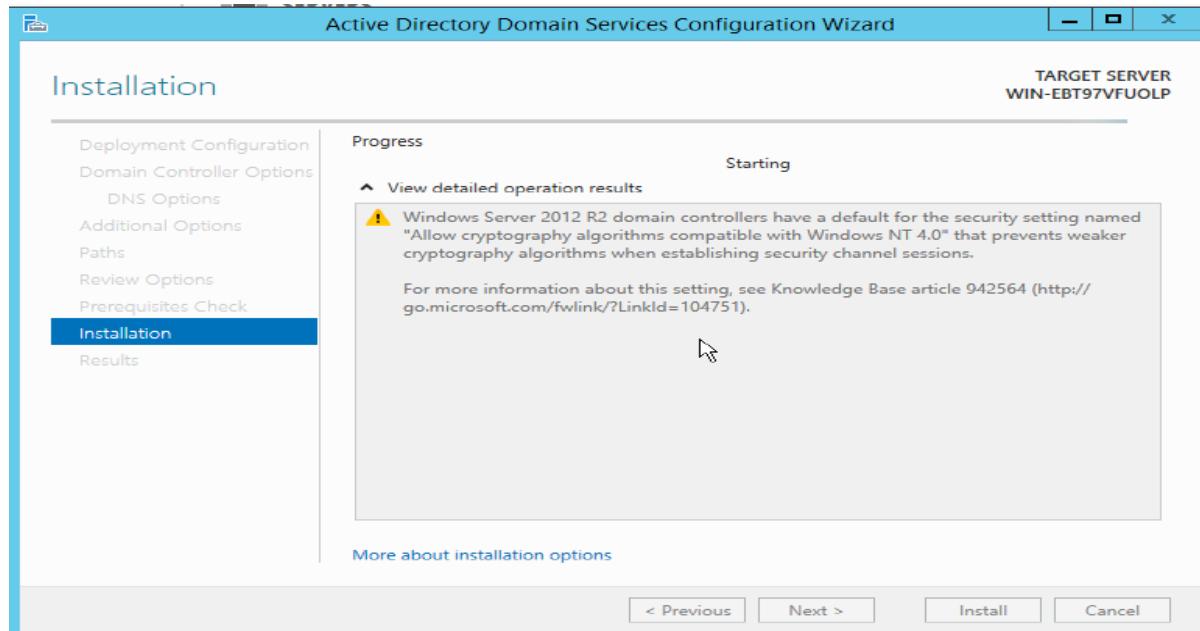
17. Review your selections and click Next.



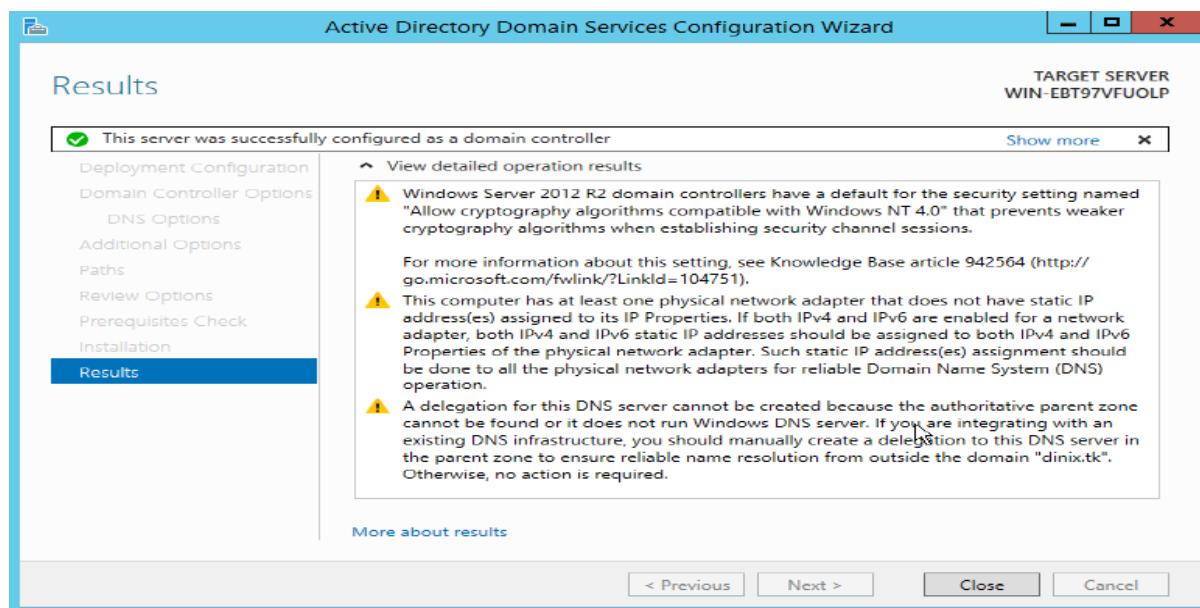
18. The wizard will validate the prerequisites before installing AD DS. When all checks are passed successfully, click Install.



19. The installation will be started.



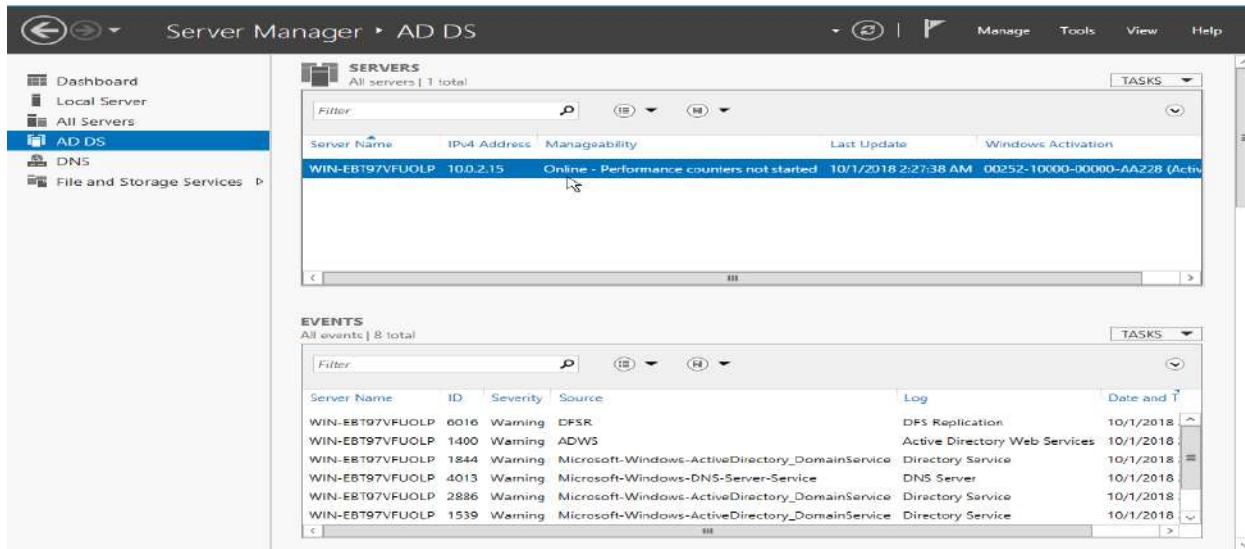
20. When the installation is completed, click Close to finish the wizard.



-
21. Active Directory Domain Services have been successfully installed. Your machine will be rebooted automatically.

Output/Results snippet:

Now we have set up Active Directory on your Windows Server 2012 R2 successfully. You can use Active Directory Users and Computers tool to access your newly created active directory.



The screenshot shows the Windows Server Manager interface. The left navigation pane is collapsed. The main content area has two tabs: 'SERVERS' and 'EVENTS'. The 'SERVERS' tab is selected, displaying a table with one row for 'WIN-EBT97VFUOLP' (IP 10.0.2.15) which is 'Online - Performance counters not started'. The 'EVENTS' tab is also visible below it, showing a table of 8 events from 10/1/2018, all of which are 'Warning' level events related to DFSR, ADWS, and Directory Service.

Server Name	ID	Severity	Source	Log	Date and Time
WIN-EBT97VFUOLP	6016	Warning	DFSR	DFS Replication	10/1/2018
WIN-EBT97VFUOLP	1400	Warning	ADWS	Active Directory Web Services	10/1/2018
WIN-EBT97VFUOLP	1844	Warning	Microsoft-Windows-ActiveDirectory_DomainService	Directory Service	10/1/2018
WIN-EBT97VFUOLP	4013	Warning	Microsoft-Windows-DNS-Server-Service	DNS Server	10/1/2018
WIN-EBT97VFUOLP	2886	Warning	Microsoft-Windows-ActiveDirectory_DomainService	Directory Service	10/1/2018
WIN-EBT97VFUOLP	1539	Warning	Microsoft-Windows-ActiveDirectory_DomainService	Directory Service	10/1/2018

References:

- <https://docs.microsoft.com/en-us/windows-server/administration/server-manager/server-manager>

Activity 8

Aim: Installation and Configuring DNS Services

Learning outcome: Able to configure different protocol services

Duration: 3 hour

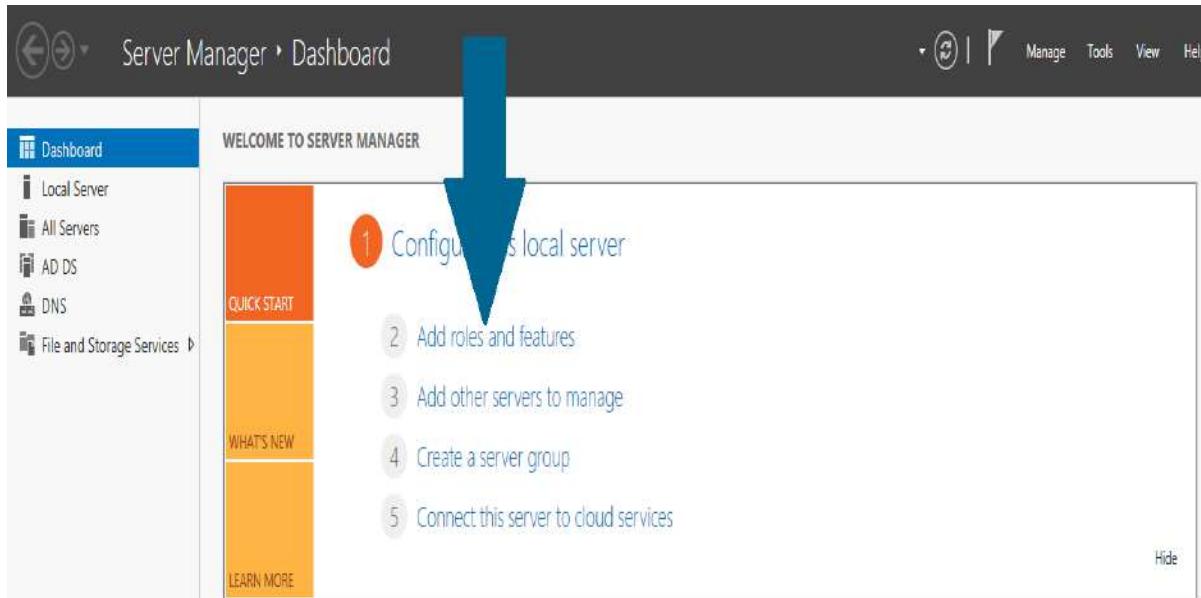
List of Hardware/Software requirements:

1. Windows Server 2012 R2
2. VMWare Workstation
3. Computer with 8GB RAM/500 GB HD

Code/Program/Procedure (with comments):

Installing DNS Server Role

Step 1: From task bar, open server manager dashboard



1. Read the notes and meet the prerequisites. Click Next when you are done

This screenshot shows the 'Before You Begin' step of the 'Add Roles and Features Wizard'. The left sidebar lists steps: Before You Begin, Installation Type, Server Selection, Server Roles, Features, Confirmation, and Results. The main content area describes the wizard's purpose: installing roles, role services, or features based on organizational needs like sharing documents or hosting a website. It also provides instructions for removing existing features and lists prerequisites for the administrator account, network settings, and security updates. A large blue arrow points downwards from the top of the image towards the 'Next >' button at the bottom of the wizard page.

DESTINATION SERVER
AD.pel.com

Before You Begin

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
[Start the Remove Roles and Features Wizard](#)

Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

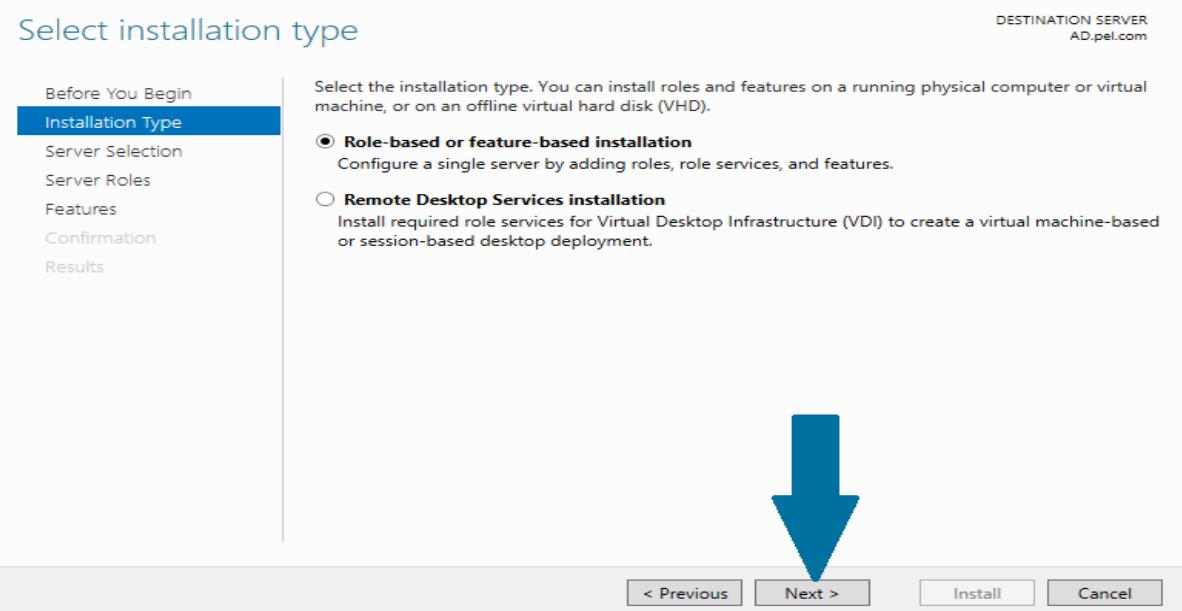
If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

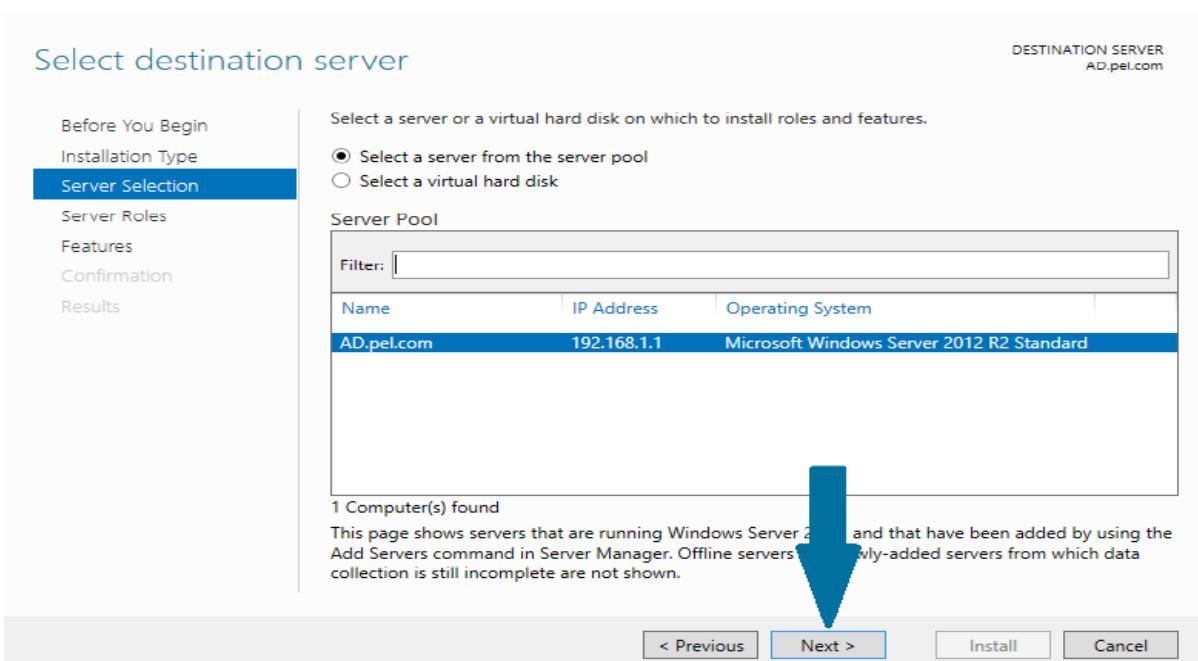
Skip this page by default

< Previous **Next >** Install Cancel

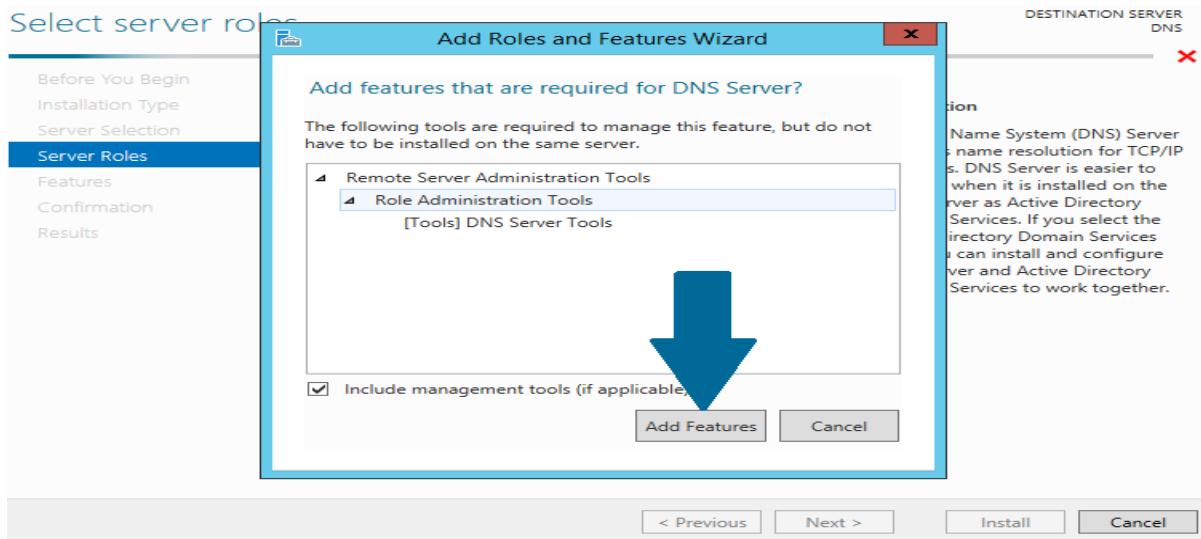
2. Choose **Role-based or feature-based installation** and click **Next**



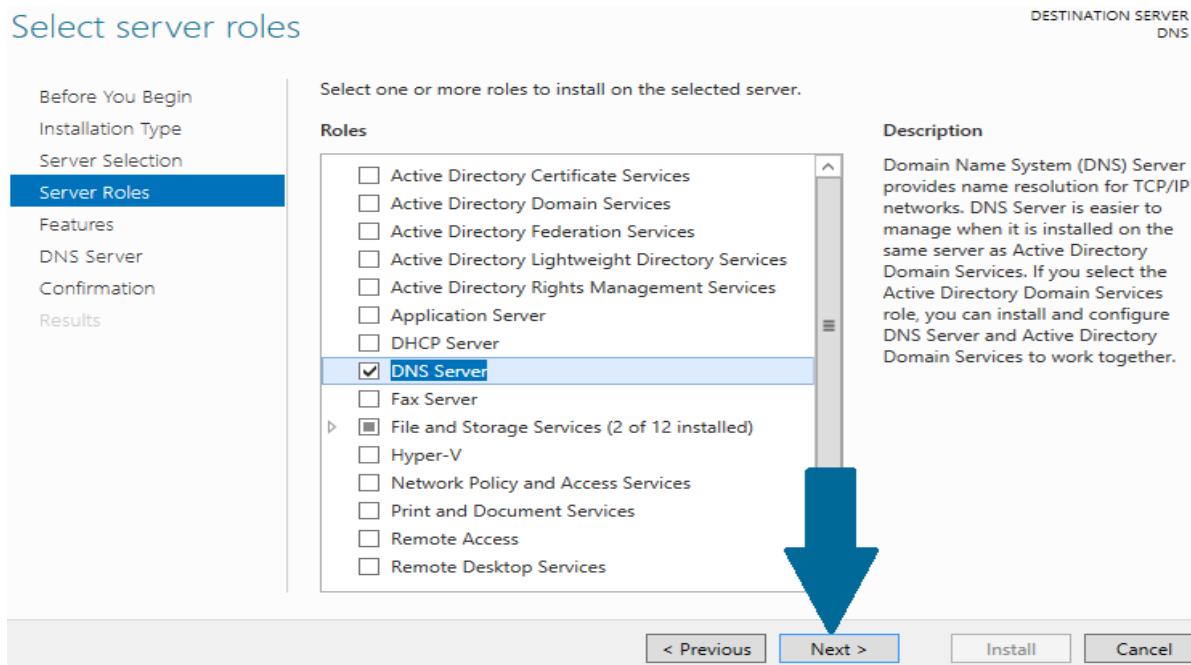
3. Select the destination server from server pool on which you want to configure DNS and click **Next**



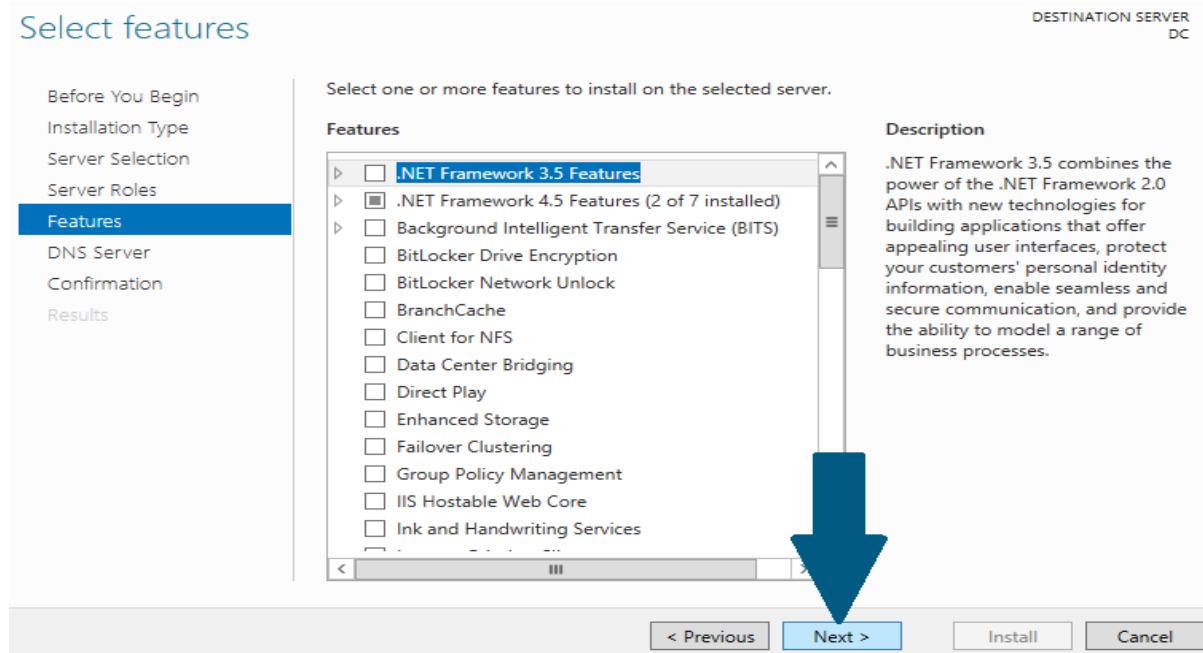
4. Choose DNS Server from server roles. When prompted to install additional necessary features along with DNS server, click **Add Features**



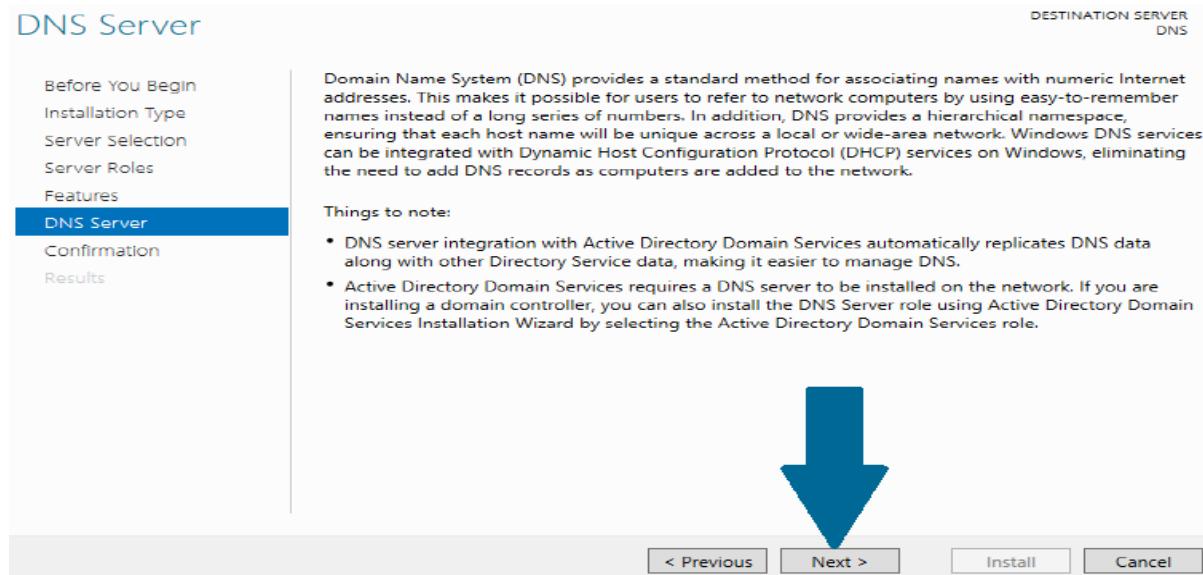
5. Click **Next**



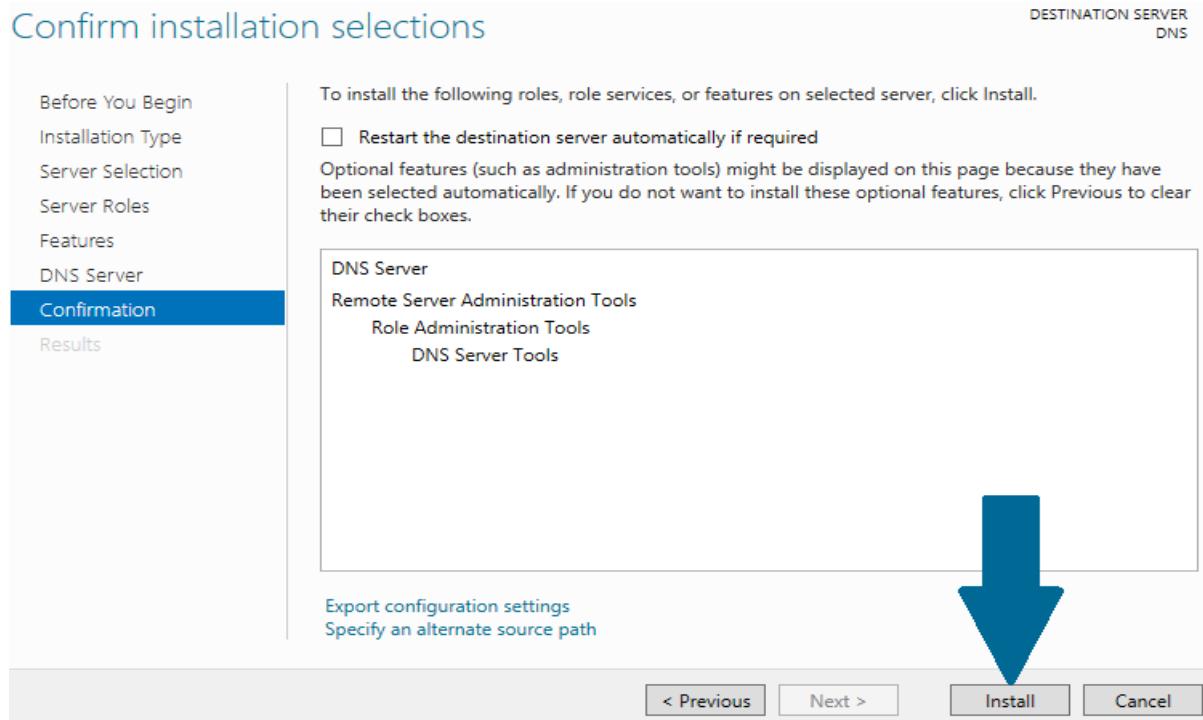
6. Keep default selections and click Next



7. Read the important notes and click Next

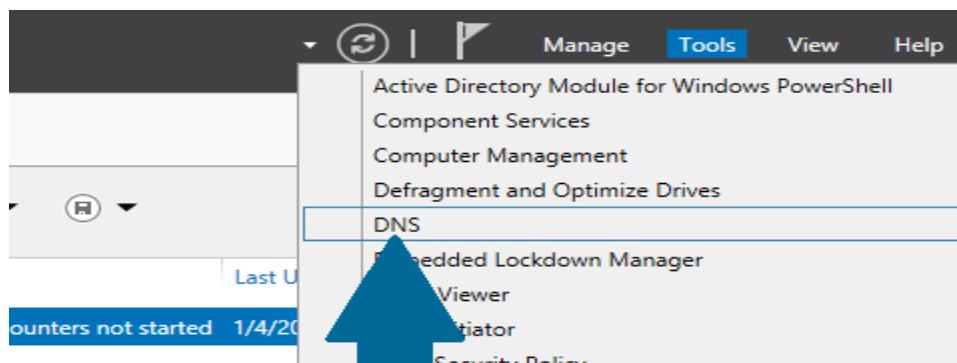


8. Click **Install**. Wait for a moment before DNS role is installed

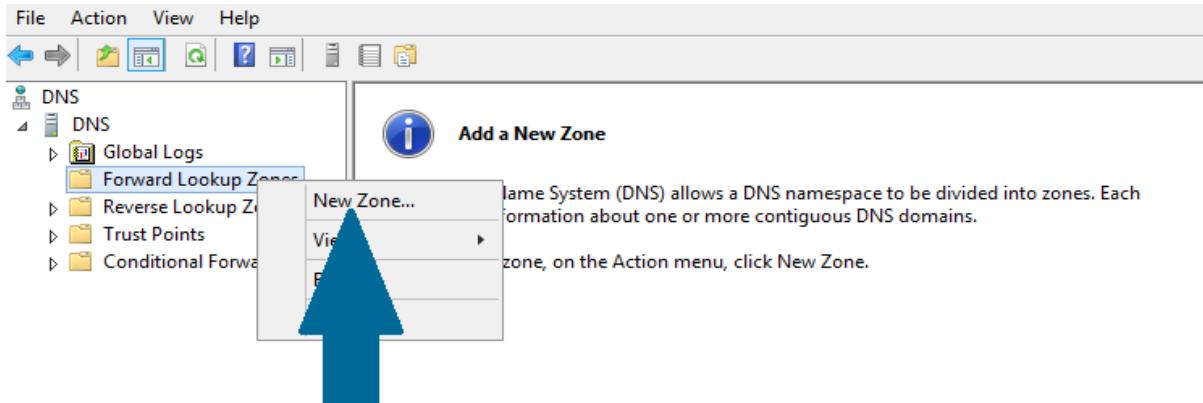


Configuring Forward Look Up Zone:

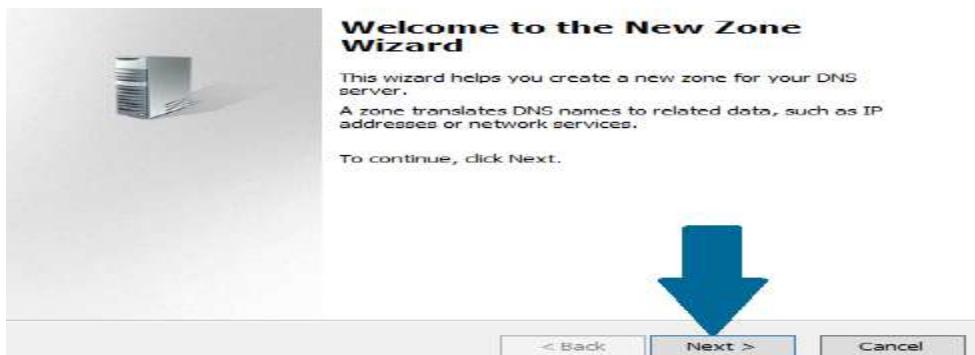
1. Open server manager dashboard, and then open tools. Scroll to DNS and click it



2. Right-click **Forward Lookup Zones** and click **New Zone**



3. Click Next



4. Provide the zone name and click Next

Zone Name

What is the name of the new zone?



The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.

Zone name:



< Back Next > Cancel

5. Choose Create a new file with this file name and click Next**Zone File**

You can create a new zone file or use a file copied from another DNS server.



Do you want to create a new zone file or use an existing file that you have copied from another DNS server?

Create a new file with this file name:

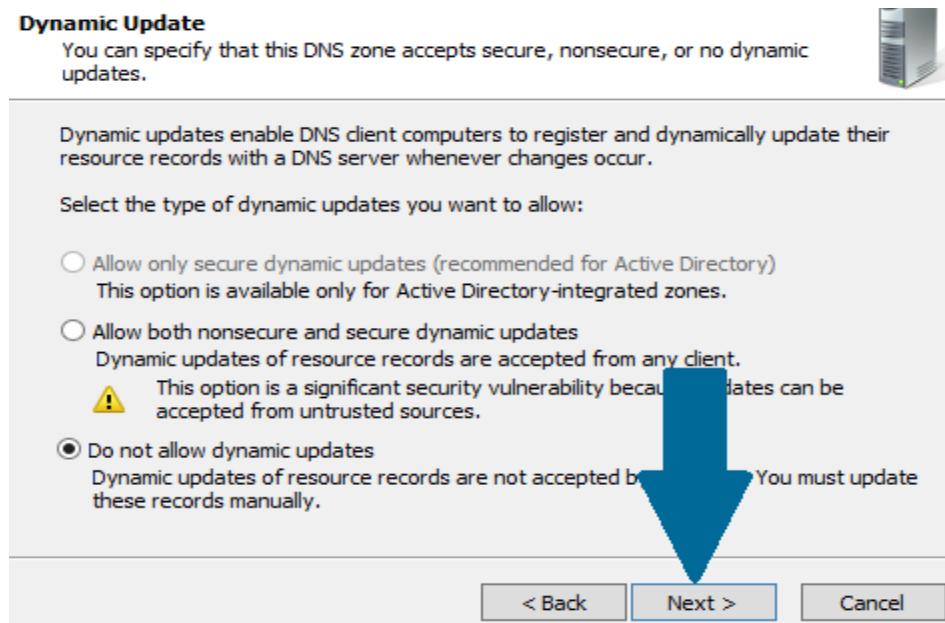
Use this existing file:

To use this existing file, ensure that it has been copied to the %SystemRoot%\system32\dns on this server, and then click Next >

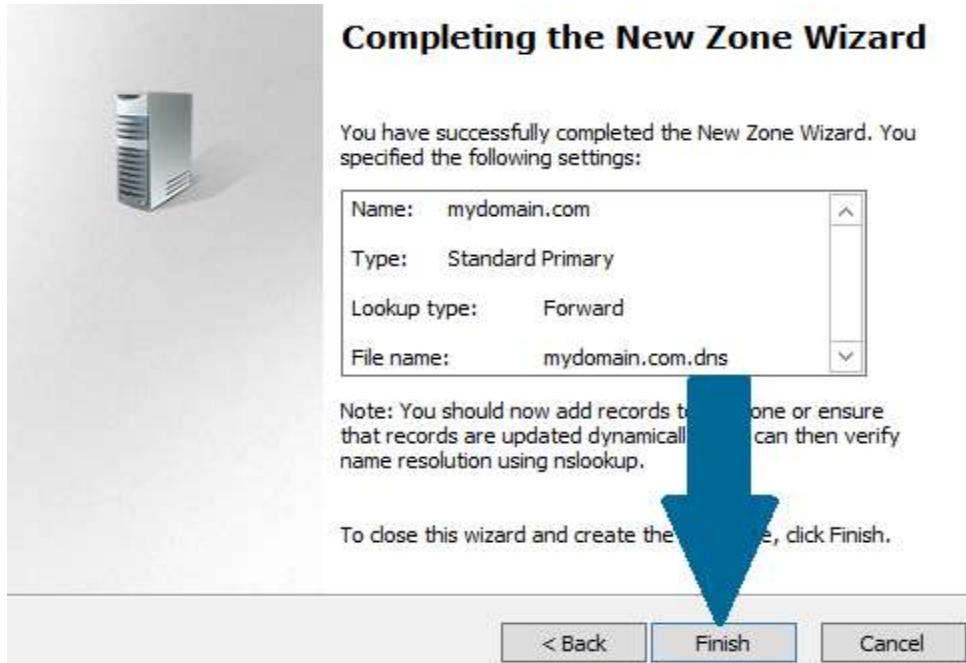


< Back Next > Cancel

6. Choose **Do not allow dynamic updates** and click **Next**

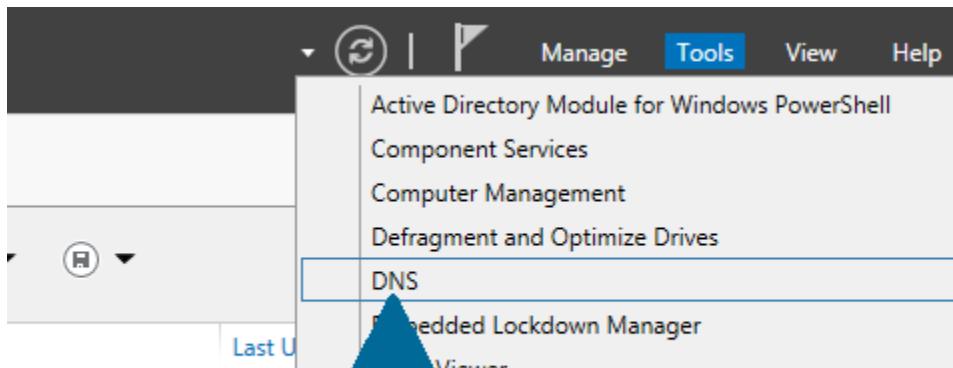


7. Click **Finish** to successfully create the new zone

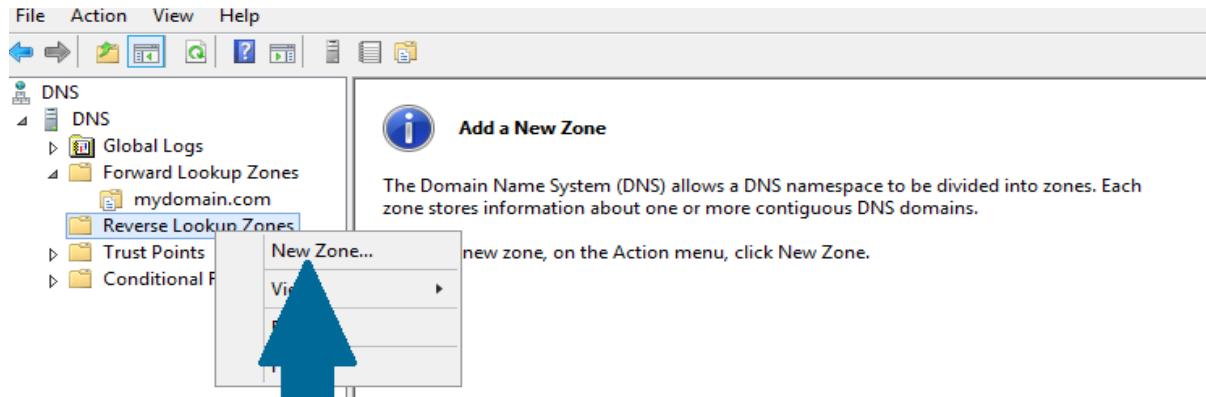


Configuring Reverse Look Up Zone

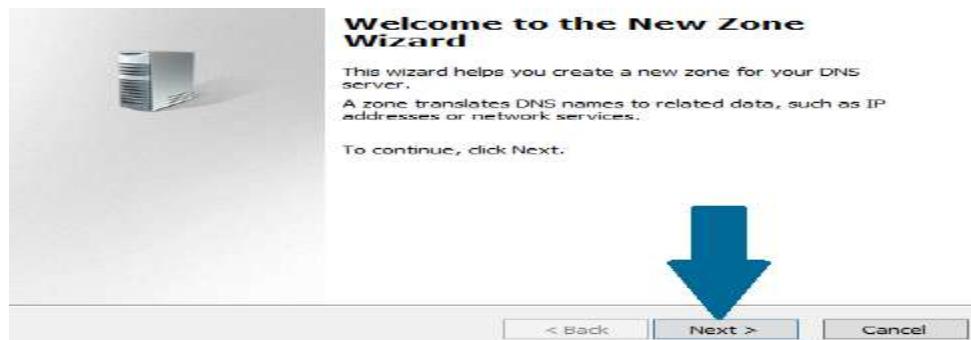
1. Open server manager from task bar and click on Tools. Scroll to DNS and then click on it



2. Right-click Reverse Lookup Zones and then click New Zone



3. Click Next



4. Choose Primary zone and click Next

Zone Type

The DNS server supports various types of zones and storage.



Select the type of zone you want to create:

 Primary zone

Creates a copy of a zone that can be updated directly on this server.

 Secondary zone

Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.

 Stub zone

Creates a copy of a zone containing only Name Server (NS) (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.

Store the zone in Active Directory (available only if DNS service is running on a writeable domain controller)



< Back

Next >

Cancel

5. Choose IPv4 Reverse Lookup Zone and click Next**Reverse Lookup Zone Name**

A reverse lookup zone translates IP addresses into DNS names.



Choose whether you want to create a reverse lookup zone for IPv4 addresses or IPv6 addresses.

 IPv4 Reverse Lookup Zone IPv6 Reverse Lookup Zone

< Back

Next >

Cancel

6. Provide **network ID** and click **Next**

Reverse Lookup Zone Name
A reverse lookup zone translates IP addresses into DNS names.

To identify the reverse lookup zone, type the network ID or the name of the zone.

Network ID:

The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.

If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.

Reverse lookup zone name:



< Back **Next >** **Cancel**

7. Choose **Create a new file with this file name:** and click **Next**

Zone File

You can create a new zone file or use a file copied from another DNS server.



Do you want to create a new zone file or use an existing file that you have copied from another DNS server?

- Create a new file with this file name:

1.168.192.in-addr.arpa.dns

- Use this existing file:

To use this existing file, ensure that it has been copied to the %SystemRoot%\system32\DNS folder on this server, and then click Next.



< Back

Next >

Cancel

8. Choose Do not allow dynamic updates and click Next**Dynamic Update**

You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.



Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

Select the type of dynamic updates you want to allow:

- Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.

- Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
 This option is a significant security vulnerability because dynamic updates can be accepted from untrusted sources.

- Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this server. You must update these records manually.

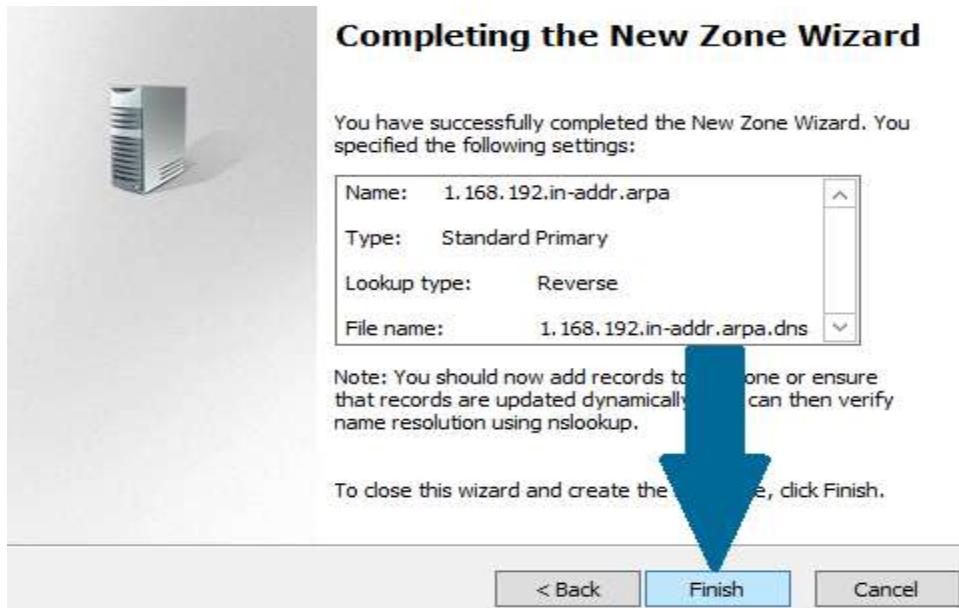


< Back

Next >

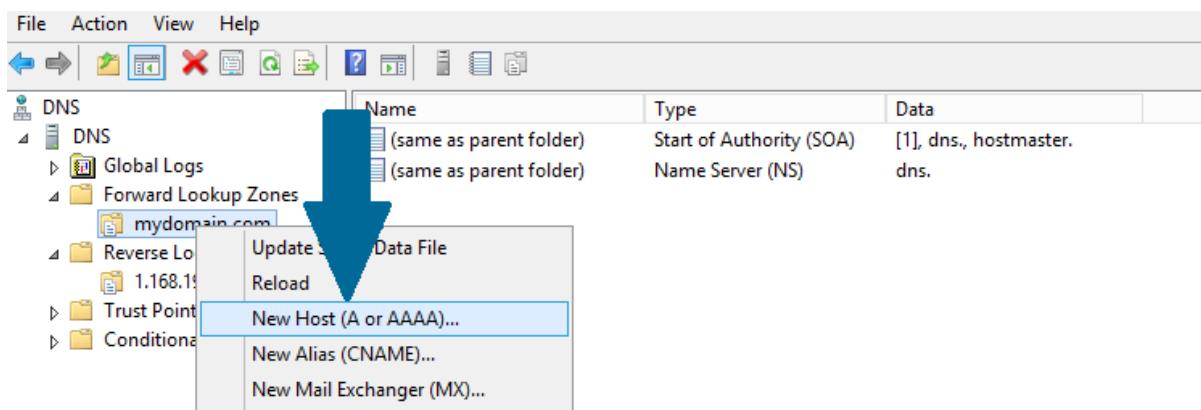
Cancel

9. Click **Finish** to end the wizard

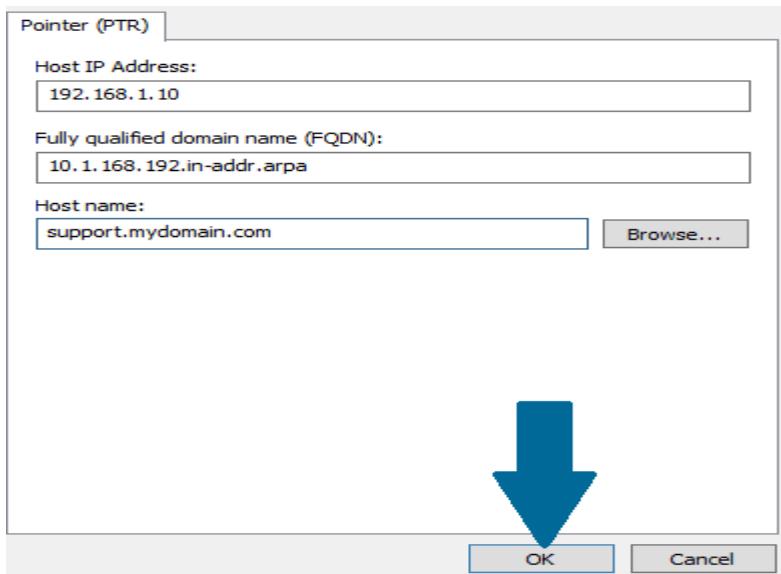


Adding a New Host Record in Forward Look Up Zone

1. Locate the zone in forward lookup zones and right-click on it. Scroll to New Host (A or AAAA) and click on it



2. Provide the name and click Add Host



3. To determine DNS Server ->Open **Command Prompt in Windows Server and type **ipconfig /all**.**

Output/Results snippet:

```
ca: C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.16299.98]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\In te>ipconfig /all
Windows IP Configuration

Host Name . . . . . : NOTENMAC12WIN10
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : hsd1.wa.comcast.net

Ethernet adapter Ethernet 2:

Connection-specific DNS Suffix . : hsd1.wa.comcast.net
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address. . . . . : 00-1C-42-65-BE-FA
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IPv6 Address. . . . . : 2603:3023:11d:3100::49d6(Preferred)
  Lease Obtained. . . . . : Wednesday, December 6, 2017 3:01:06 PM
  Lease Expires . . . . . : Wednesday, December 13, 2017 3:01:06 PM
  IPv6 Address. . . . . : 2603:3023:11d:3100:f8ee:9367:4300:ef2e(Preferred)
```

References:

- <https://www faqforge com/windows/configure-dns-windows-server-2012-r2-2/>

Activity 9

Aim: Installation and Configuring DHCP Services

Learning outcome: Able to configure different protocol services

Duration: 2 hour

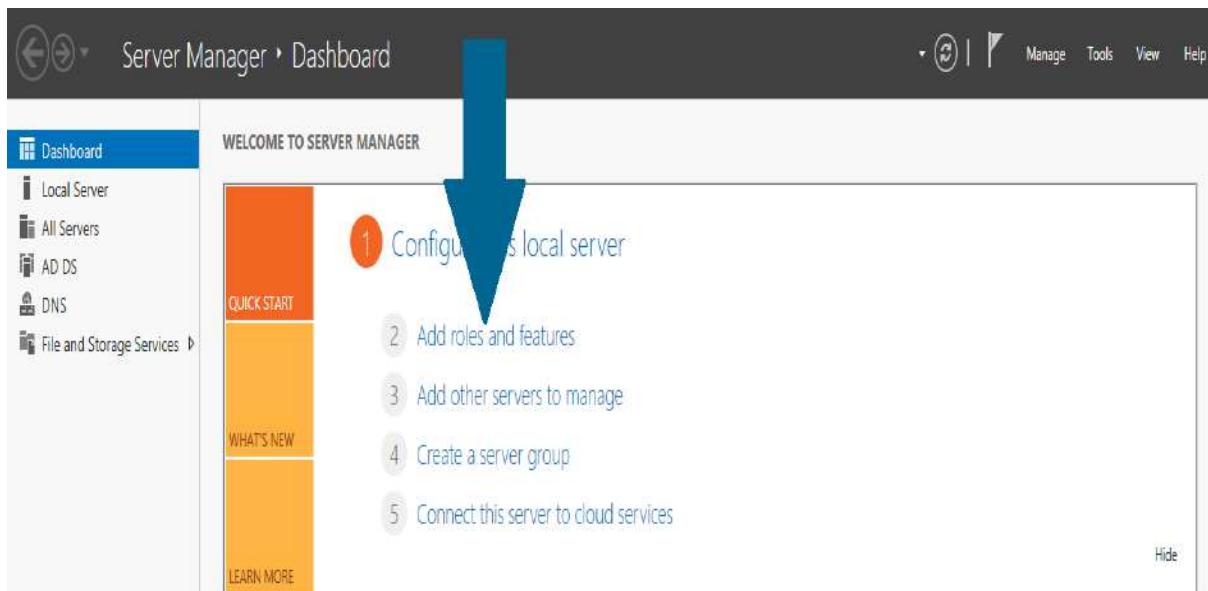
List of Hardware/Software requirements:

1. Windows Server 2012 R2
2. VMWare Workstation
3. Computer with 8GB RAM/500 GB HD

Code/Program/Procedure (with comments):

Installing DHCP Server

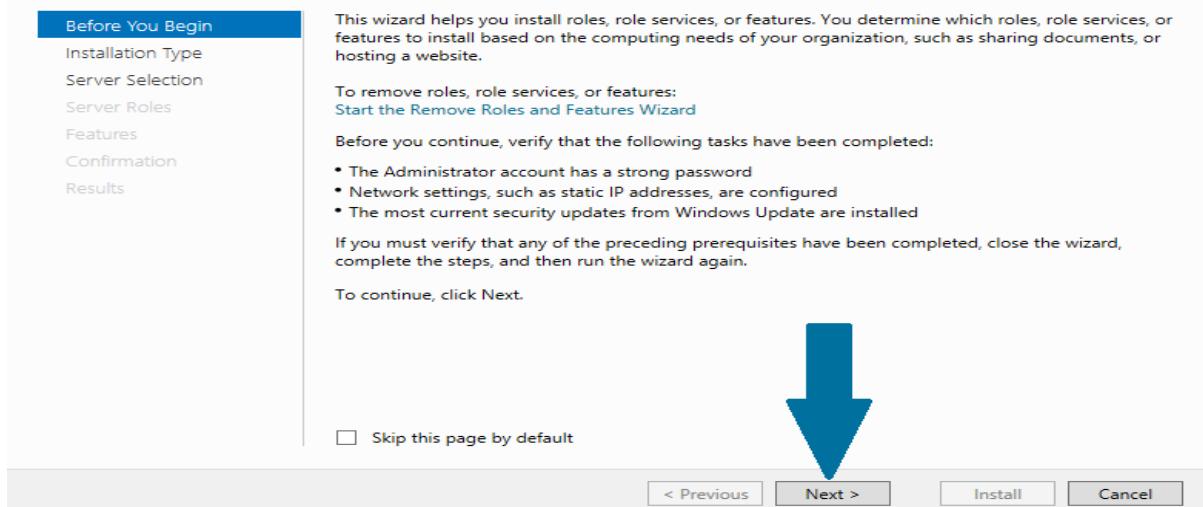
1. Open **Server Manager** from task bar and click **Add roles and features**



2. Before you run the installation wizard, make sure that an administrator account has a strong password, static IP is configured, and security updates from Windows updates are installed. When you are done, click **Next**

Before you begin

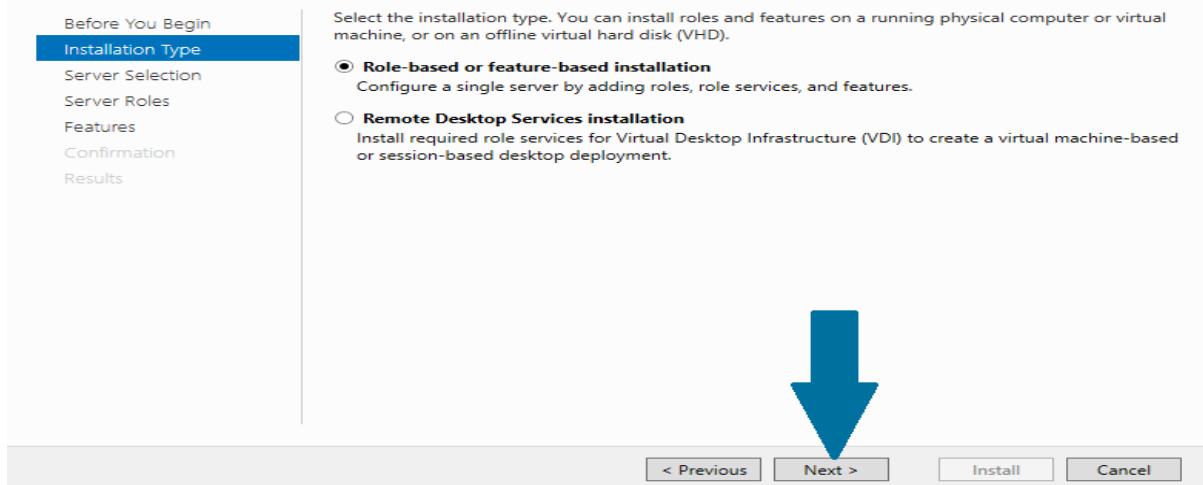
DESTINATION SERVER
AD.pel.com



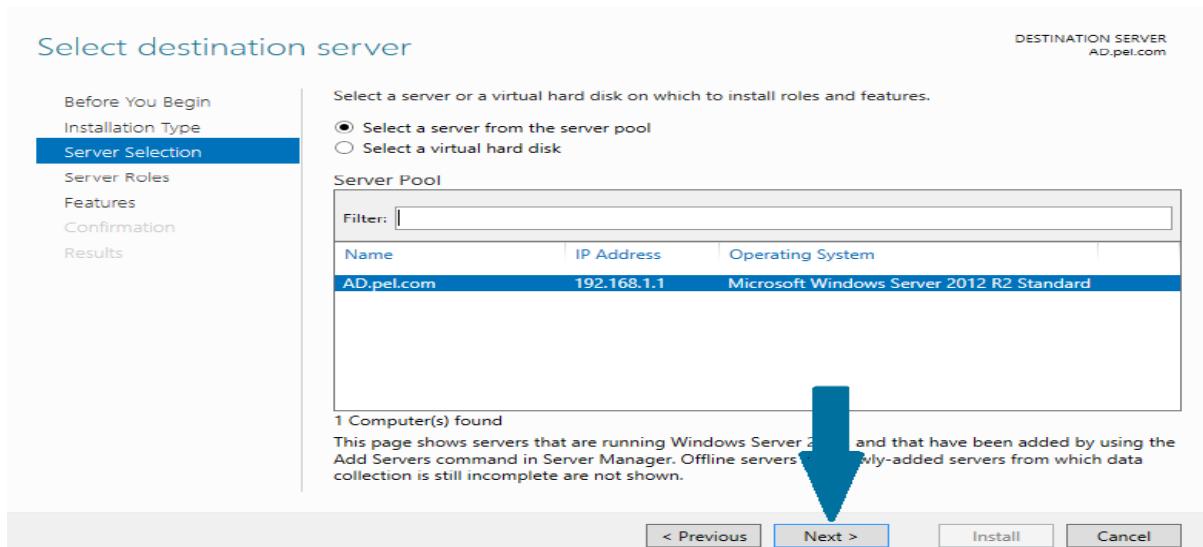
3. Select **Role-based or feature-based installation** and click **Next**

Select installation type

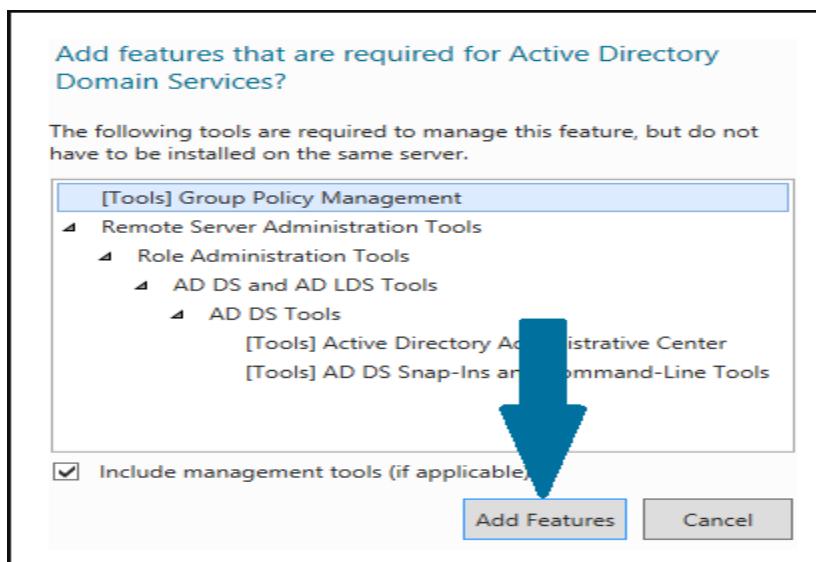
DESTINATION SERVER
AD.pel.com

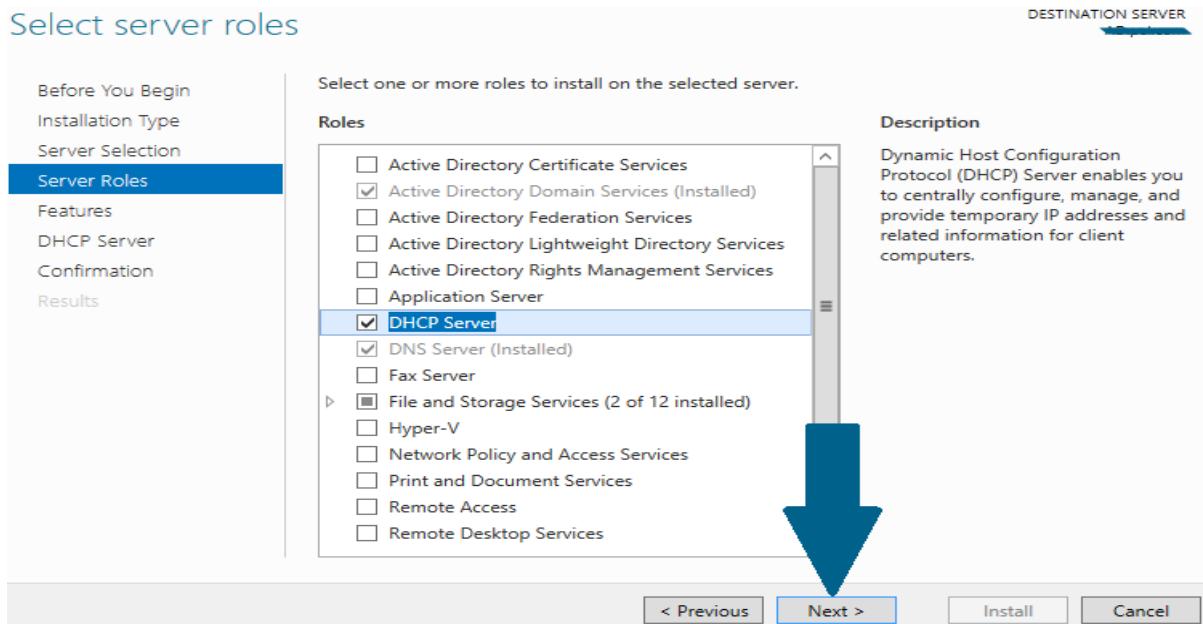


4. Select a destination server on which you want to install the DHCP server. In our case, there is only one server which is local server and it is selected by default. Click **Next**

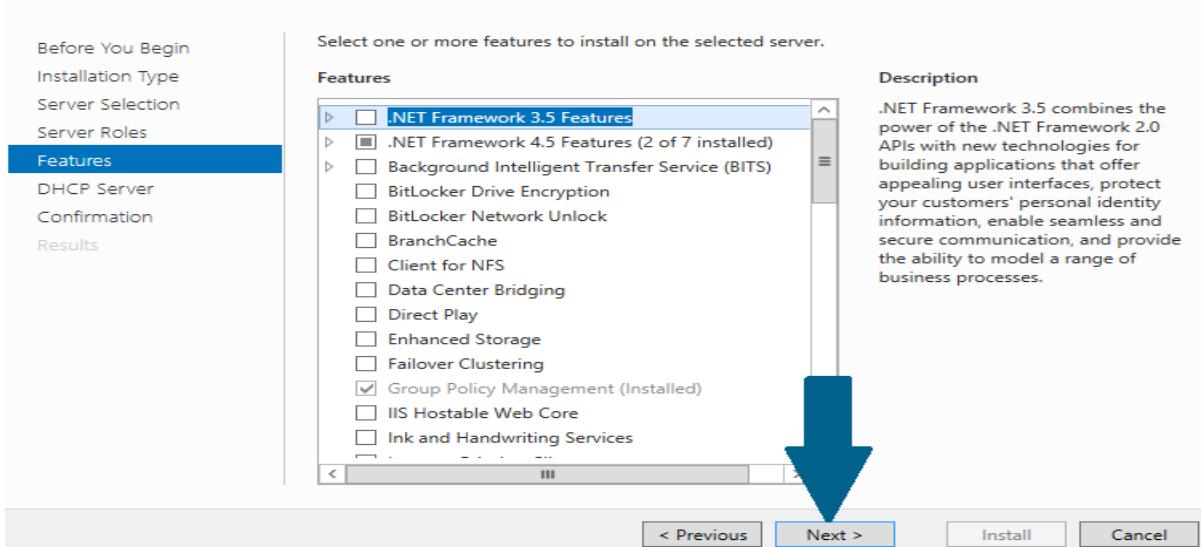


5. Select DHCP server role by checking the appropriate box. As soon as you check the box, a small window will pop up alerting you that there are some other features which are also required to be installed along with DHCP server. Click **Add Features**

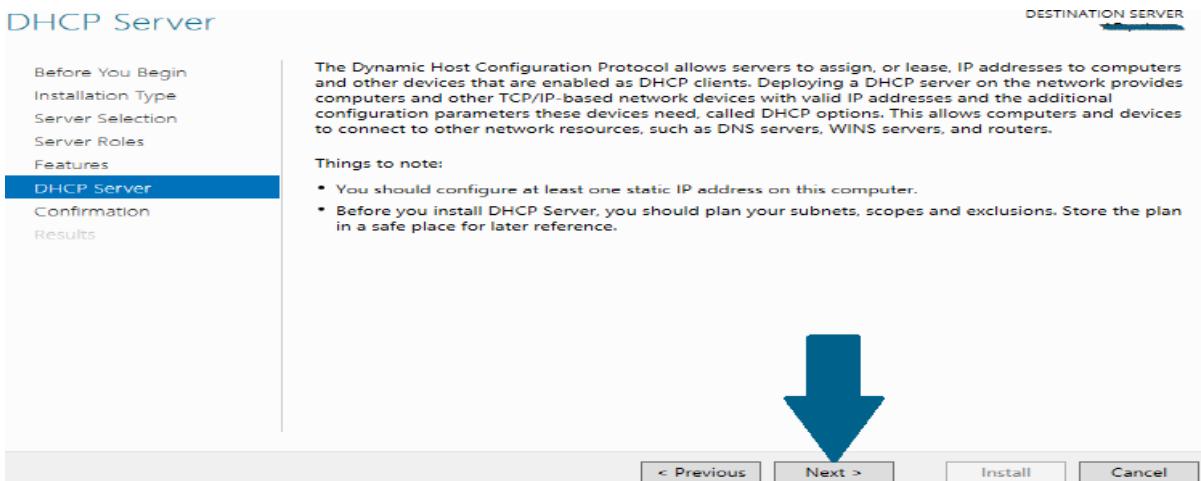


6. Click Next**7. Click Next**

Select features



8. Note the things outlined in the screen and click **Next**



9. Confirm your installation selections and click **Install**

Confirm installation selections

DESTINATION SERVER

Before You Begin

Installation Type

Server Selection

Server Roles

Features

DHCP Server

Confirmation

Results

To install the following roles, role services, or features on selected server, click Install.

Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

DHCP Server

Remote Server Administration Tools

Role Administration Tools

DHCP Server Tools

Export configuration settings
Specify an alternate source path

< Previous

Next >

Install

Cancel



10. Click **Close** to finish the installation

Installation progress

DESTINATION SERVER

Before You Begin

Installation Type

Server Selection

Server Roles

Features

DHCP Server

Confirmation

Results

View installation progress

Feature Installation

Configuration required. Installation succeeded on AD.pel.com.

DHCP Server

Launch the DHCP post-install wizard

Complete DHCP configuration

Remote Server Administration Tools

Role Administration Tools

DHCP Server Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task List.

Export configuration settings

< Previous

Next >

Close

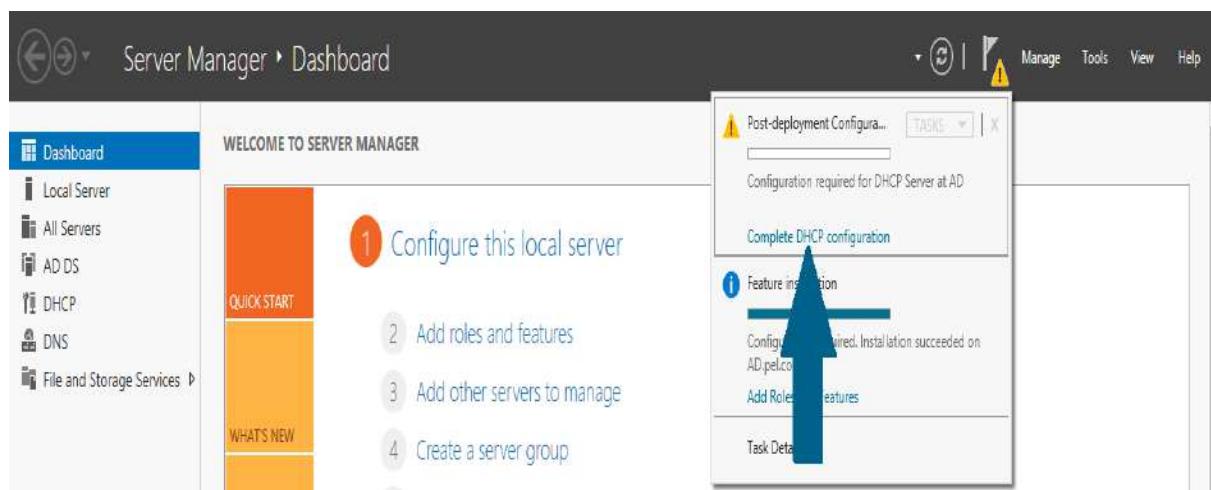
Cancel



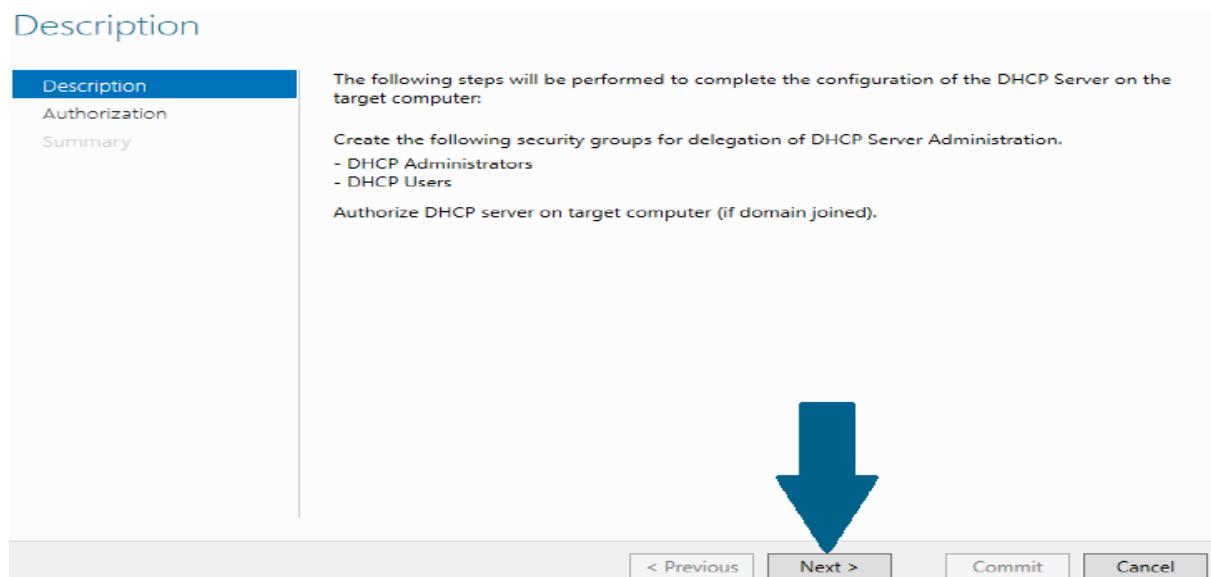
Configuring DHCP Server and Creating Scope

11. Open Server Manager and click **notifications icon**. A small window will appear.

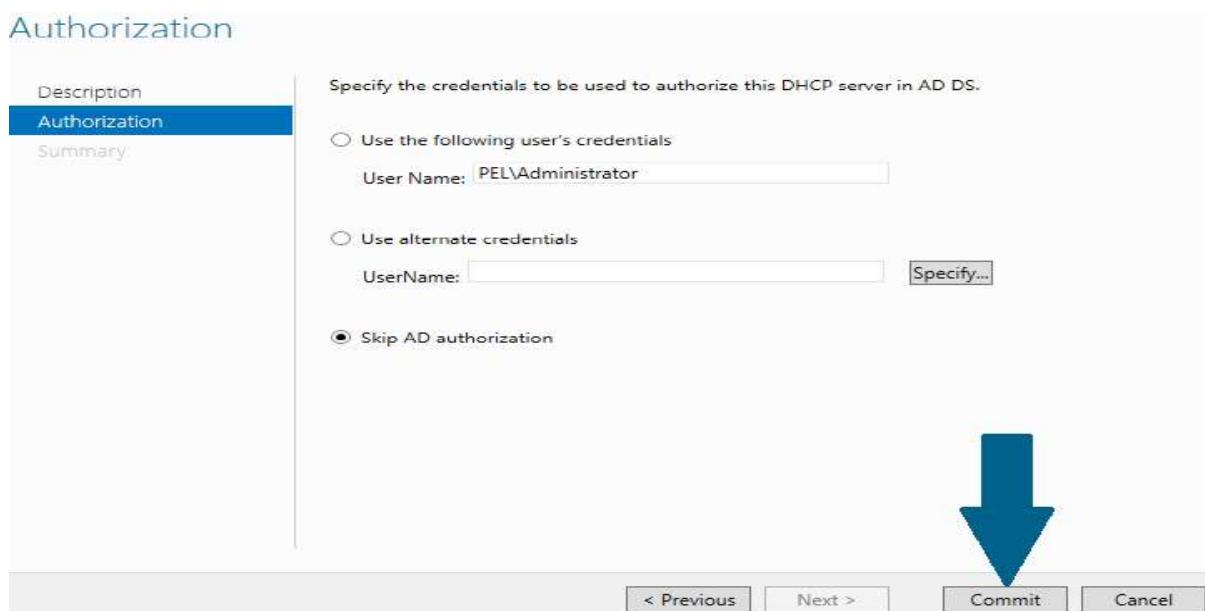
Click **Complete DHCP configuration**



12. Click **Next**



13. Choose Skip AD authorization since we do not have any AD configured and click **Commit**



14. Read the summary and click **Close**

Summary

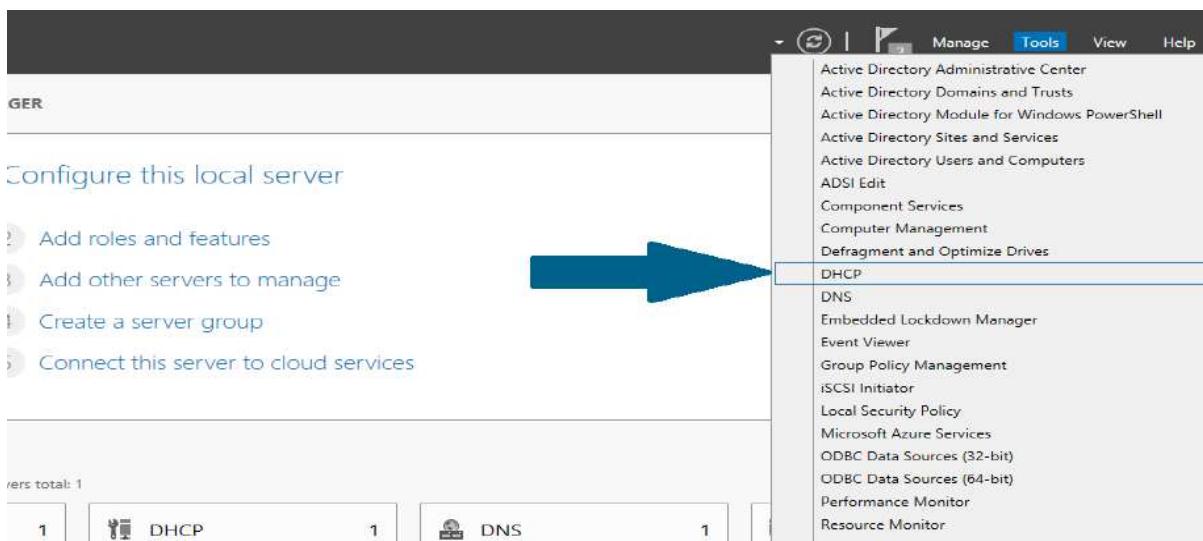
Description
Authorization
Summary

The status of the post install configuration steps are indicated below:

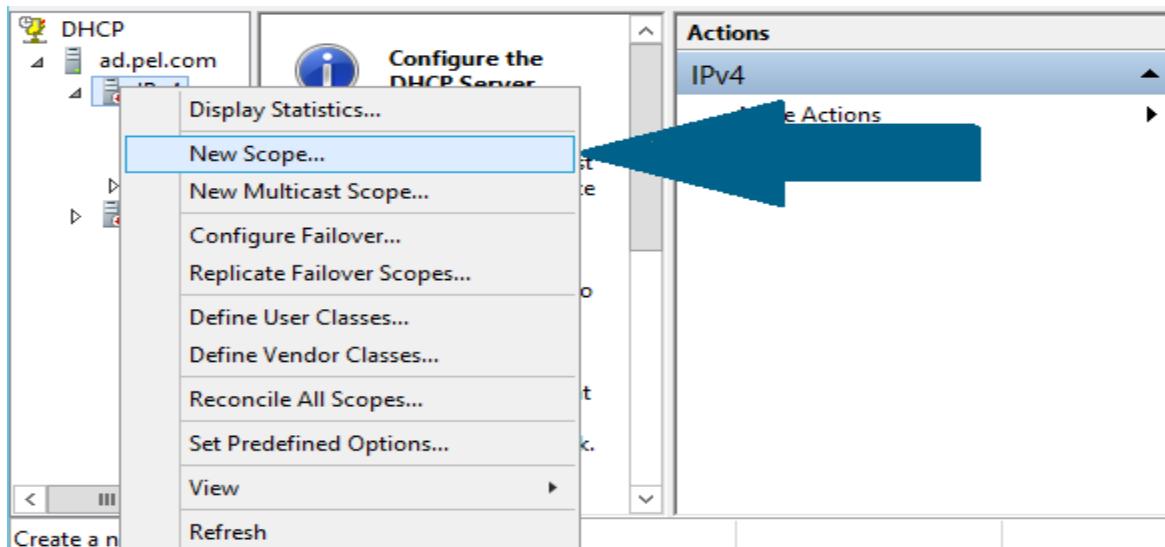
Creating security groups	Done
Please restart the DHCP server service on the target computer for the security groups to be effective.	

< Previous | Next > | **Close** | Cancel

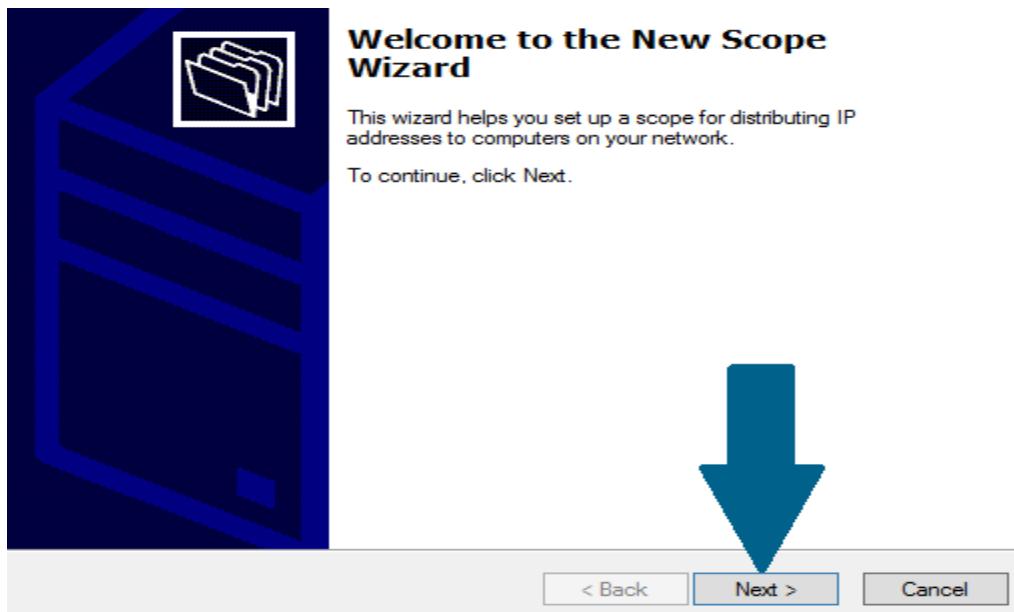
15. Open Server Manager and click on **Tools**. When a small window appear, scroll to **DHCP** and click it



16. In management console, right click on **IPv4** and scroll to **New Scope** and click it.



17. Click Next



18. Provide name and meaningful description of this new scope and click **Next**

Scope Name
You have to provide an identifying scope name. You also have the option of providing a description.

Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name: Description:



19. Provide IP address range along with sub net you need to distribute to client machines and click **Next**

IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.

Configuration settings for DHCP Server
Enter the range of addresses that the scope distributes.

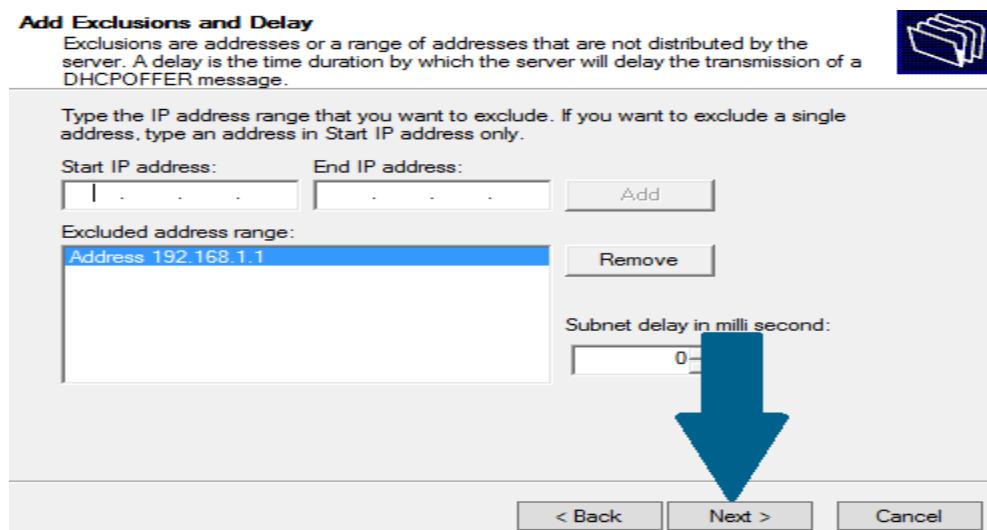
Start IP address:
End IP address:

Configuration settings that propagate to DHCP Client

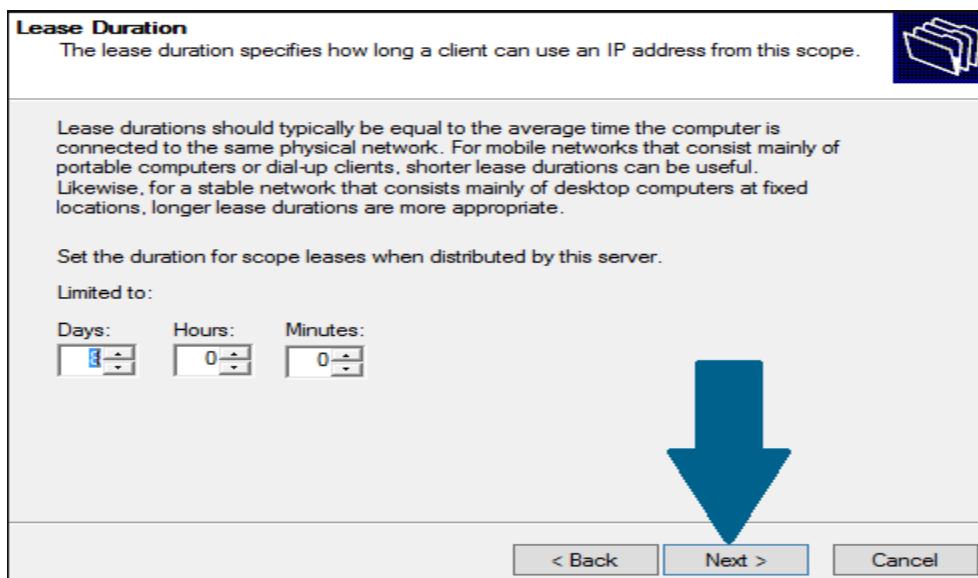
Length:
Subnet mask:



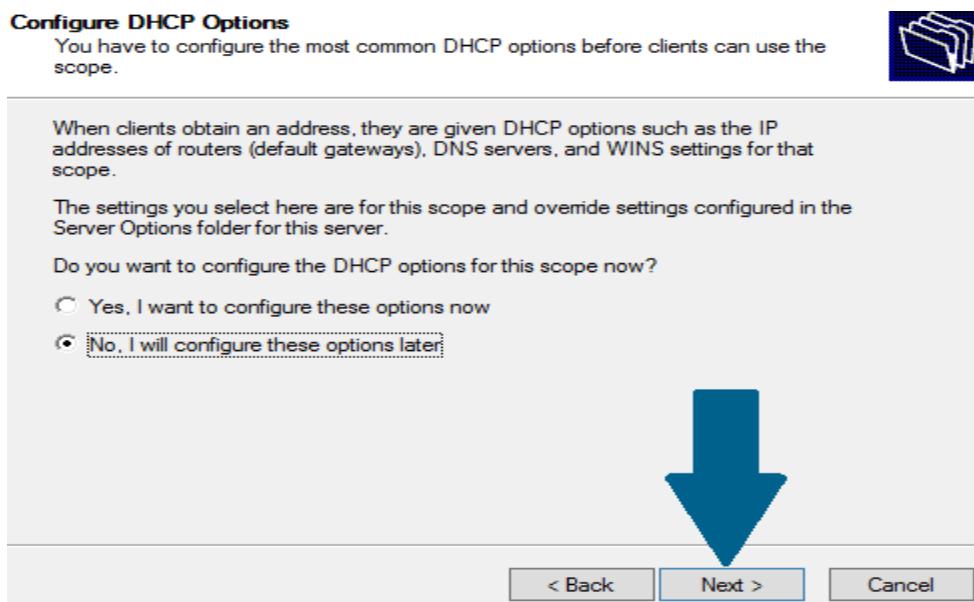
20. Provide any IP addresses you need to exclude from pool and click **Add**. I have excluded a first IP address which is statically assigned to my DHCP server. Click **Next**



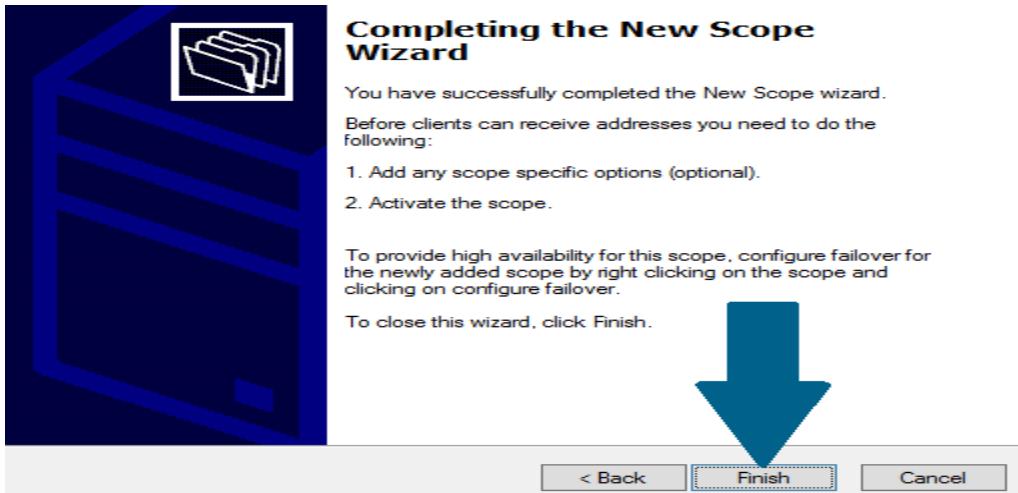
21. Keep lease duration as 8 days and click **Next**



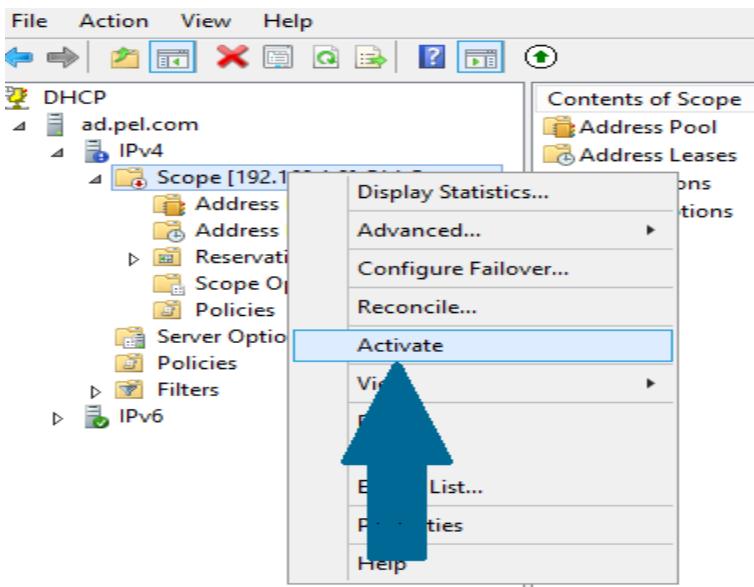
22. Choose **No, I will configure these options later** and click **Next**



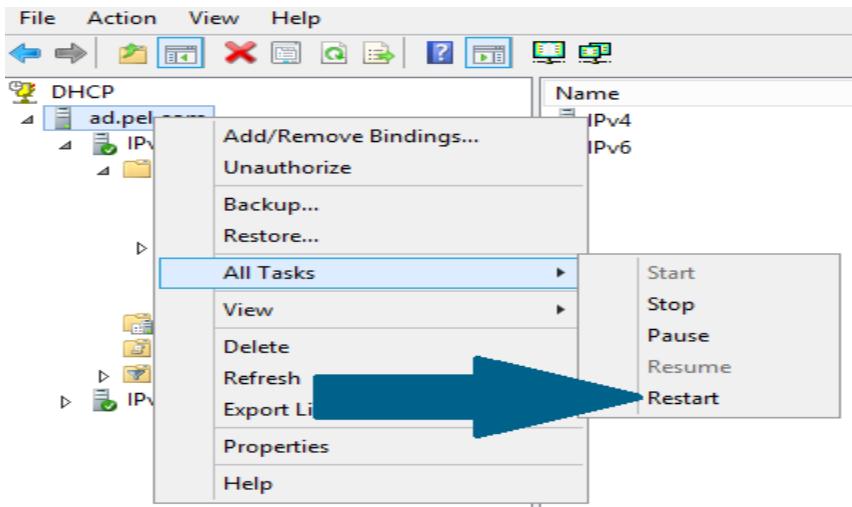
23. Click **Finish** to end the new scope wizard



24. Right-click on new scope you just created in above step and click **Activate**



25. Right-click on your server, scroll to **All Tasks** and then click **Restart** to finish with configuration



Output:

Open Command Prompt and Type : ipconfig /all

```
Windows IP Configuration

IP Routing Enabled : No
WINS Proxy Enabled : No
DNS Suffix Search List : ittaster.local

Ethernet adapter Ethernet:

Connection-specific DNS Suffix : ittaster.local
Description : Intel(R) 82574L Gigabit Network Connection
Physical Address : 00-0C-29-1A-C8-E5
DHCP Enabled : Yes
Autoconfiguration Enabled : Yes
IPv4 Address : 192.0.2.11<Preferred>
Subnet Mask : 255.0.0.0
Lease Obtained : 19 April 2013 22:53:29
Lease Expires : 27 April 2013 22:53:30
Default Gateway : 10.0.0.1
DHCP Server : 10.0.0.2
DNS Servers : 10.0.0.2
NetBIOS over Tcpip : Enabled

Tunnel adapter Teredo Tunneling Pseudo-Interface:

Media State : Media disconnected
Connection-specific DNS Suffix : ittaster.local
Description : Teredo Tunneling Pseudo-Interface
Physical Address : 00-00-00-00-00-00-E8
DHCP Enabled : No
Autoconfiguration Enabled : Yes

Tunnel adapter isatap.ittaster.local:

Media State : Media disconnected
Connection-specific DNS Suffix : ittaster.local
Description : Microsoft ISATAP Adapter #2
Physical Address : 00-00-00-00-00-00-E8
DHCP Enabled : No
Autoconfiguration Enabled : Yes

C:\Users\administrator>
```

References:

-
- <https://www faqforge com/windows/configure-dhcp-server-windows-server-2012-r2/>

Activity 10

Aim: Install and Configure FTP Services.

Learning outcome: Able to configure different protocol services

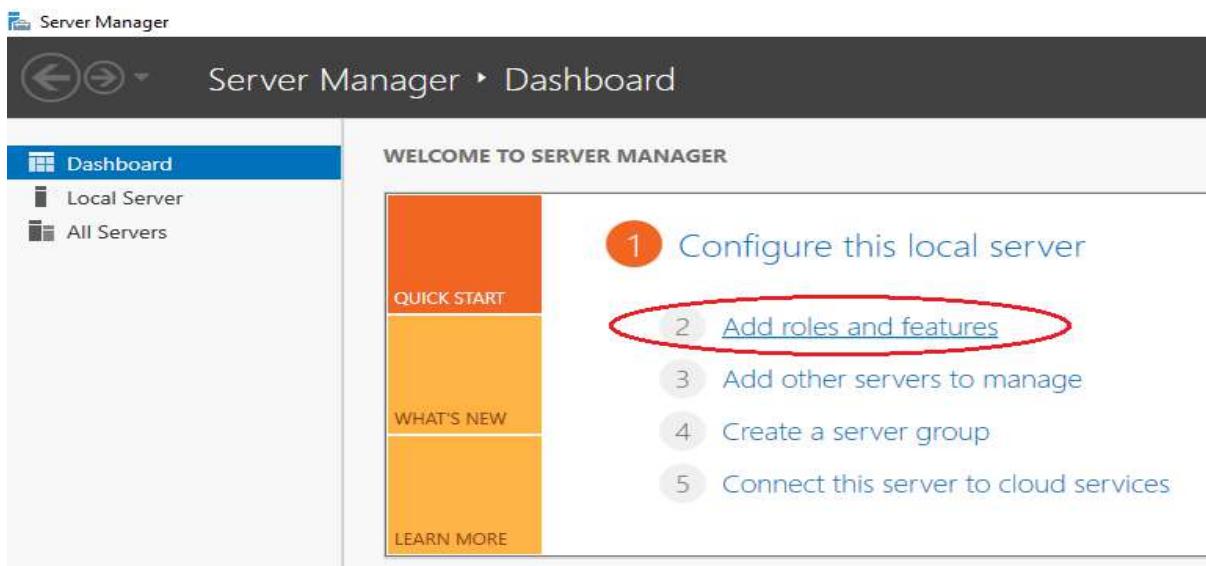
Duration: 3 hour

List of Hardware/Software requirements:

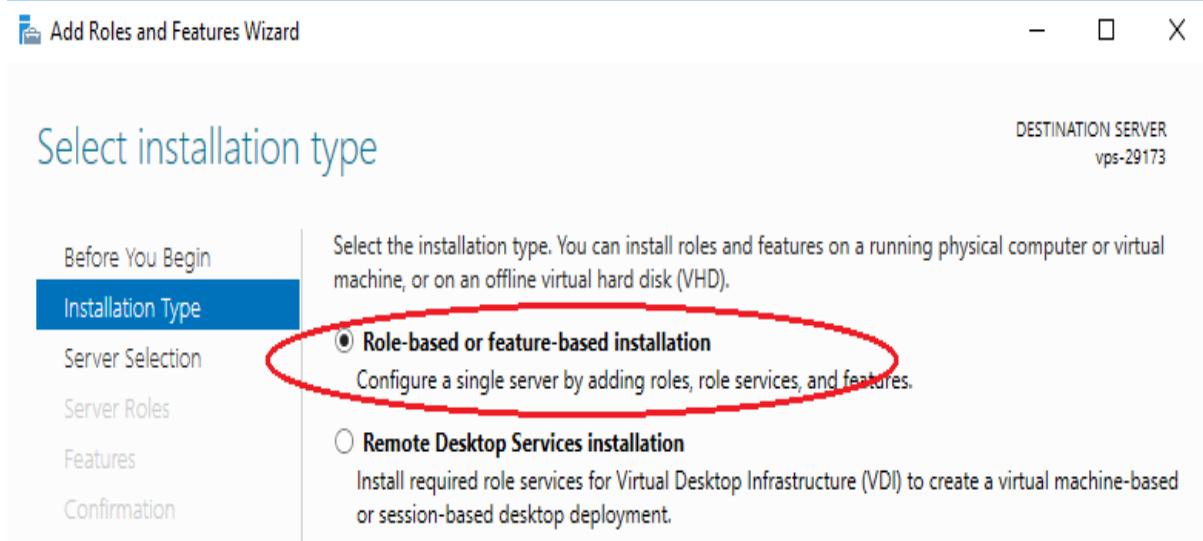
1. Windows Server 2012 R2
2. VMWare Workstation
3. Computer with 8GB RAM/500 GB HD

Code/Program/Procedure (with comments):

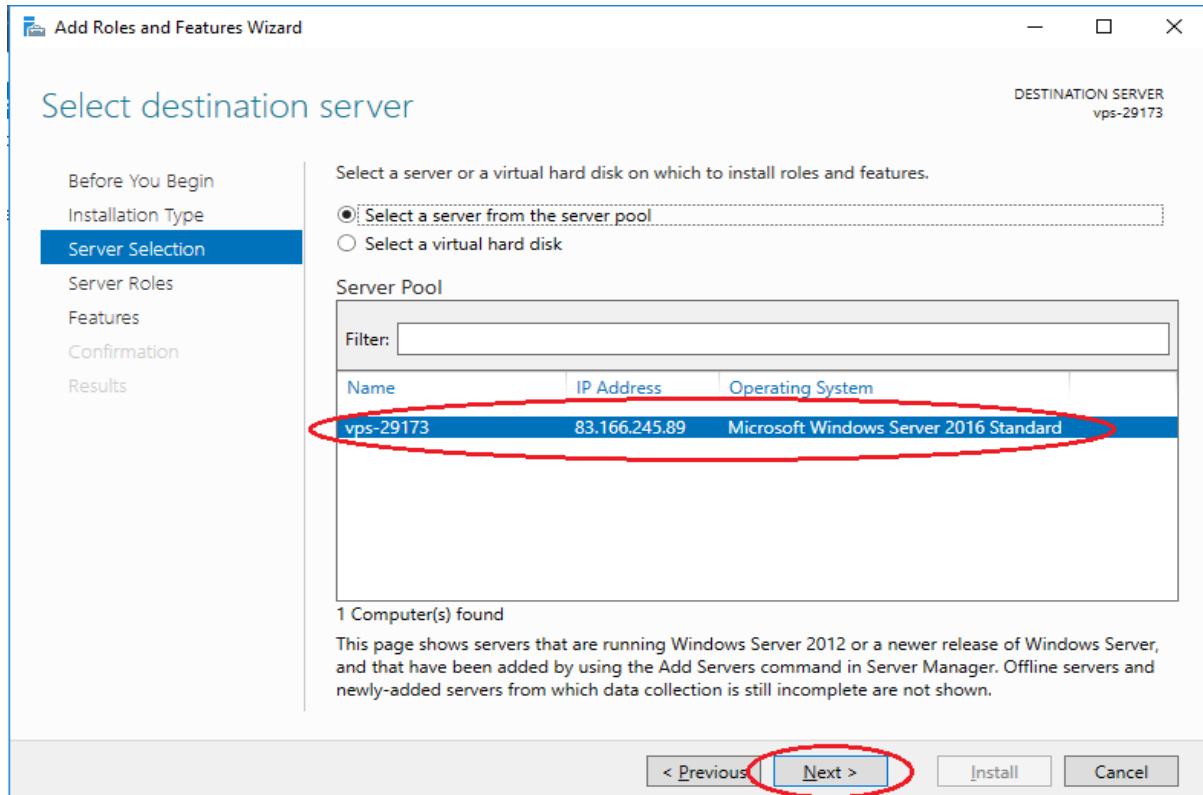
1. Open the Windows Server Control Panel and find the **Add roles and features**.



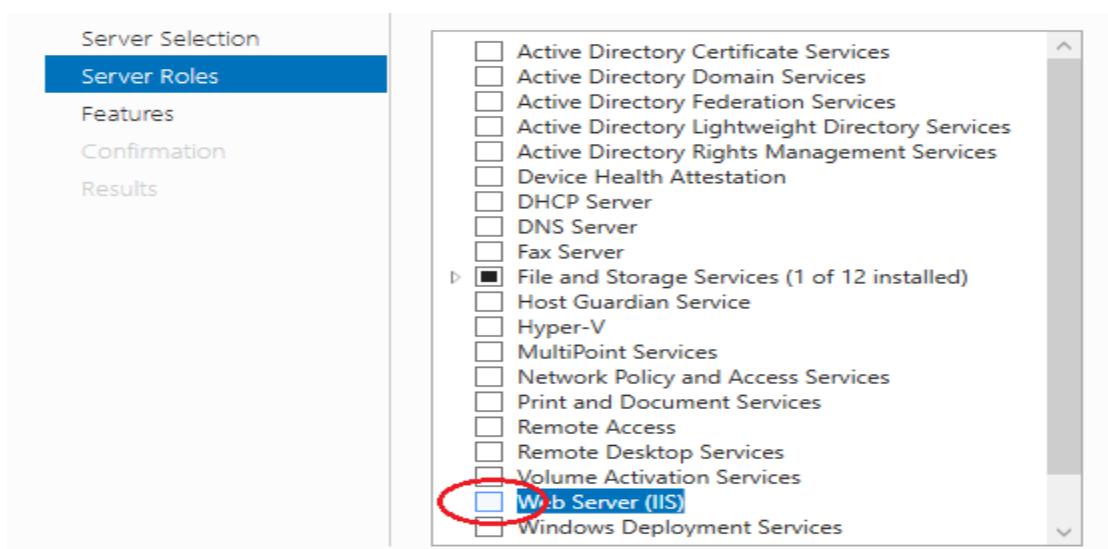
2. As the installation type, specify **Role-based or feature-based installation**.



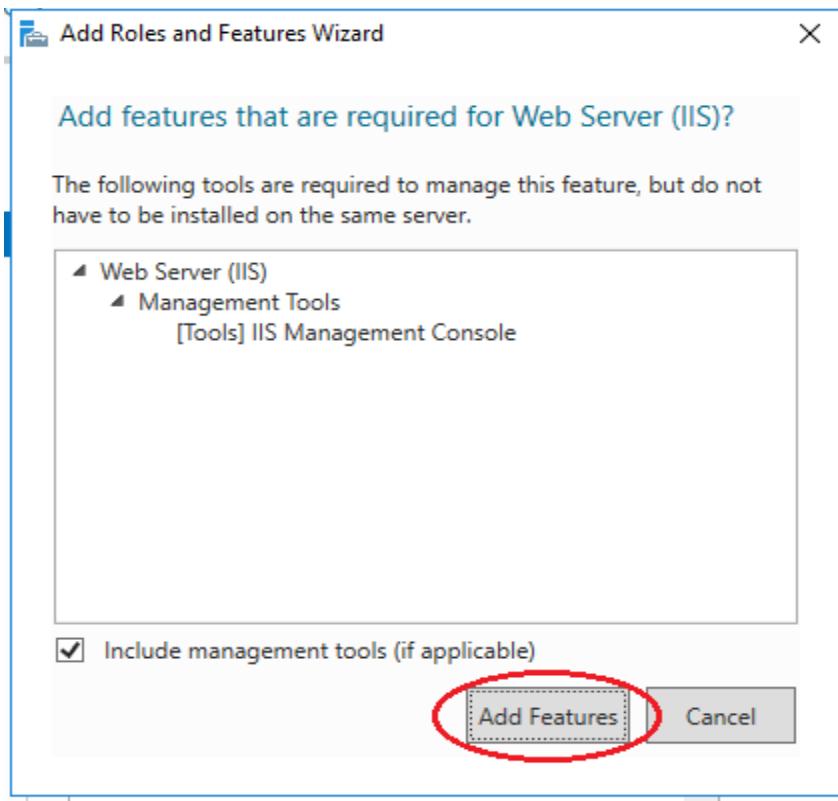
3. Select your server from the server pool.



4. In the next window, check the IIS web server

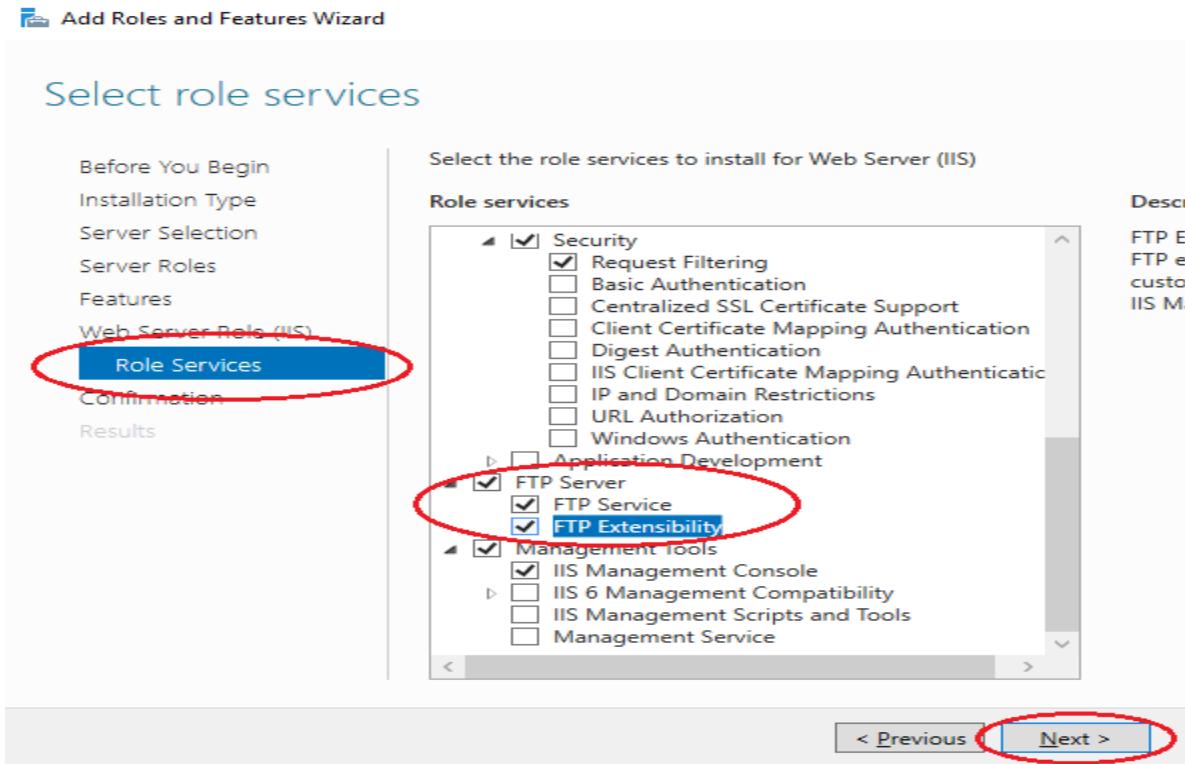


5. In the window that opens, click **Add features**.

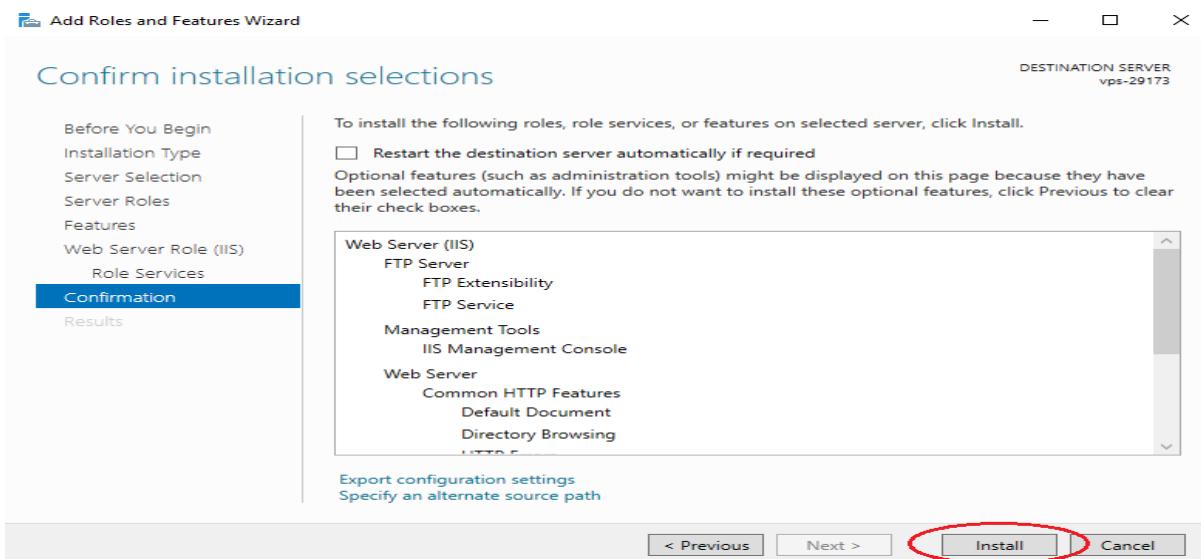


6. In the next window **Features** do not select anything.

Next in the **Role services** window, check the **FTP server**.

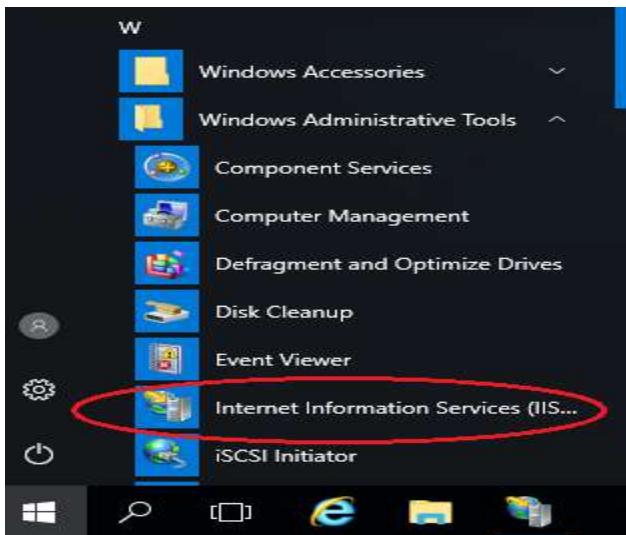


7. Install all selected features on the server using the **Install** button.

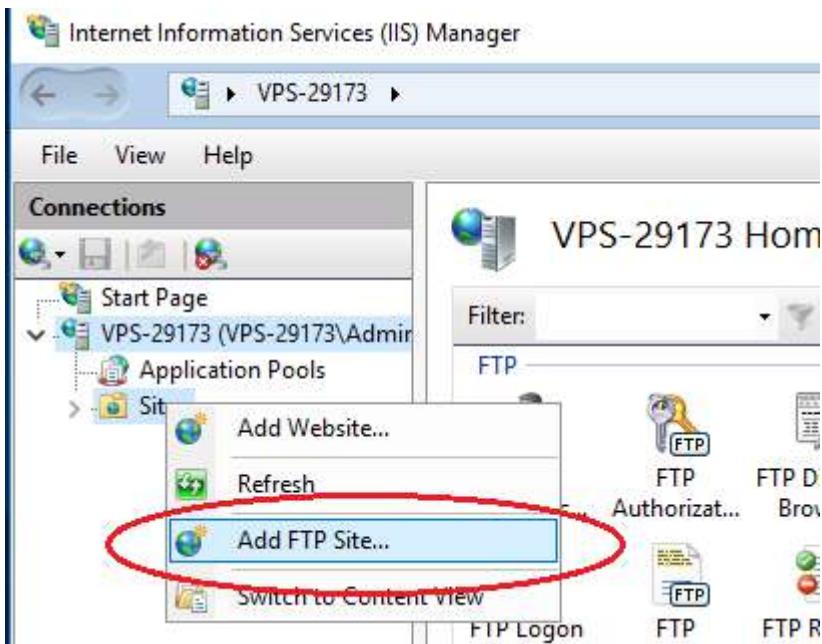


Creating an FTP site on a Windows server

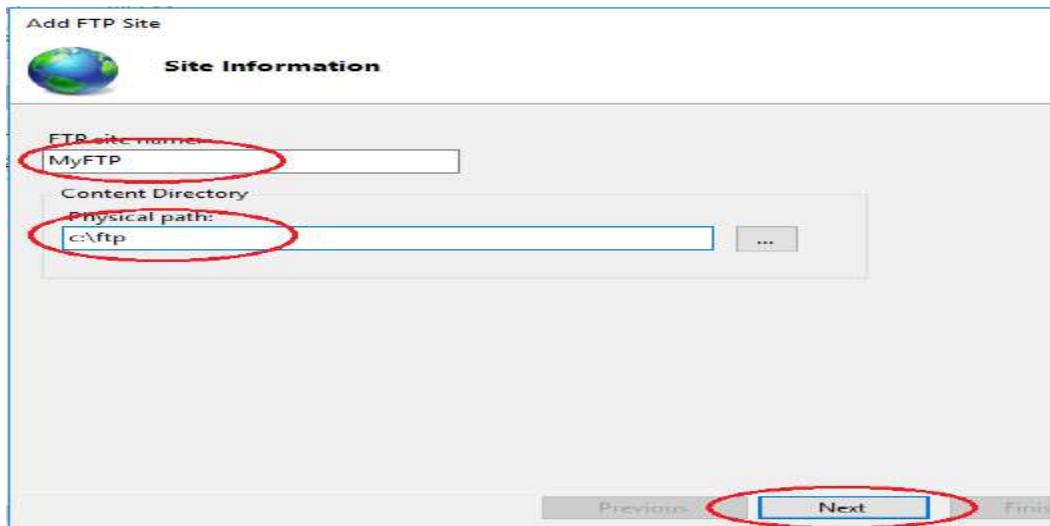
8. Open IIS Manager.



9. Right-click on Sites and select Add FTP Site from the menu.



10. Enter the site name and path to the directory.



11. Next, select your IP address in the drop-down list. For encryption, check No SSL.

Add FTP Site

Binding and SSL Settings

Binding

IP Address: 83.166.245.89 Port: 21

Enable Virtual Host Names:
Virtual Host (example: ftp.contoso.com):

Start FTP site automatically

SSL

No SSL
 Allow SSL
 Require SSL

SSL Certificate:

Not Selected

12. In the next window, select Basic for authentication. **Authorization** - Specified roles or groups, enter the name of the group of FTP users (example of creation below). Check the desired read and write permissions and click the **Finish** button.

Add FTP Site

Authentication and Authorization Information

Authentication

Anonymous
 Basic

Authorization

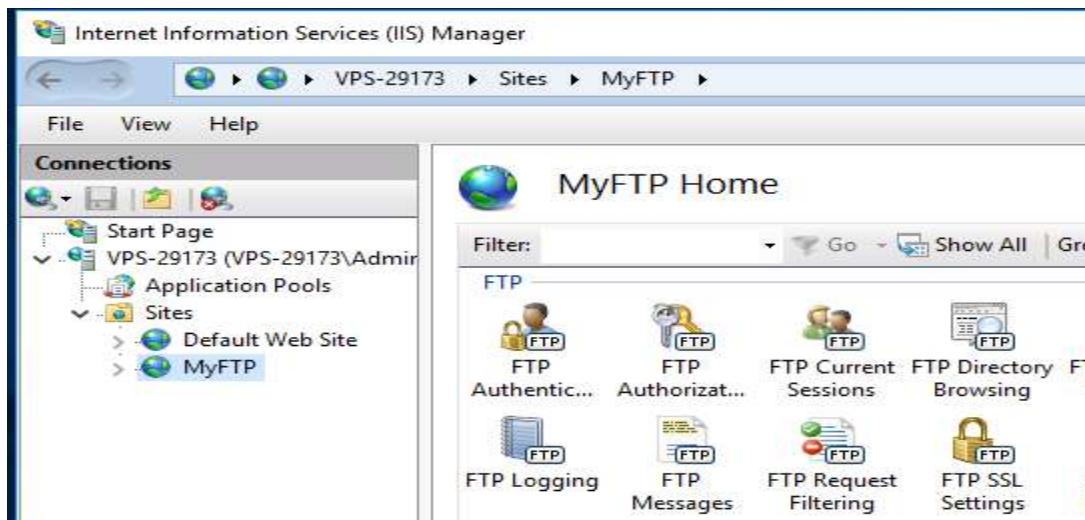
Allow access to:

Specified roles or user groups
ftp-group

Permissions

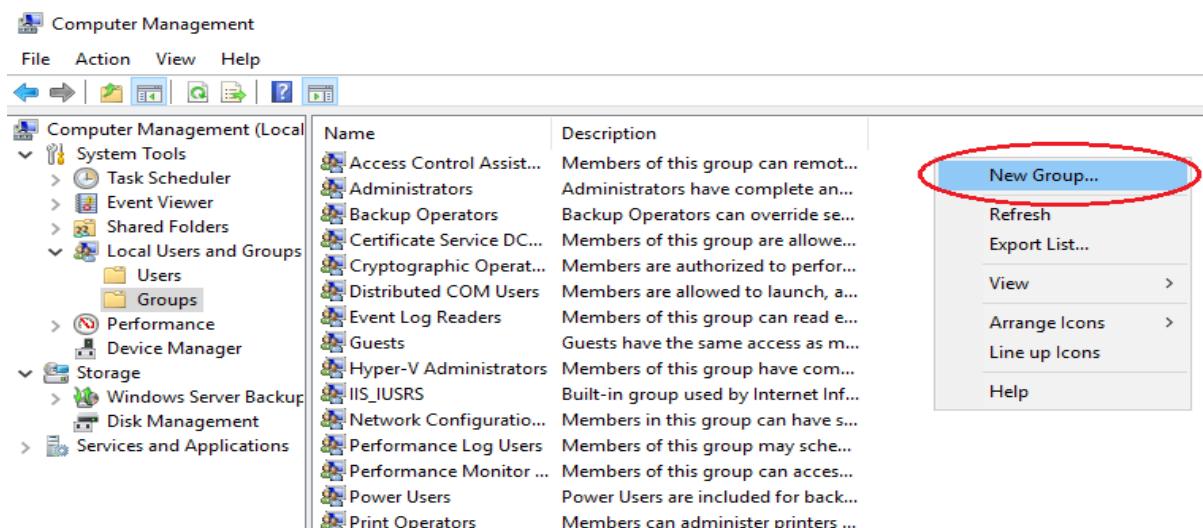
Read
 Write

13. Your website will appear in the tree structure of the Windows web server

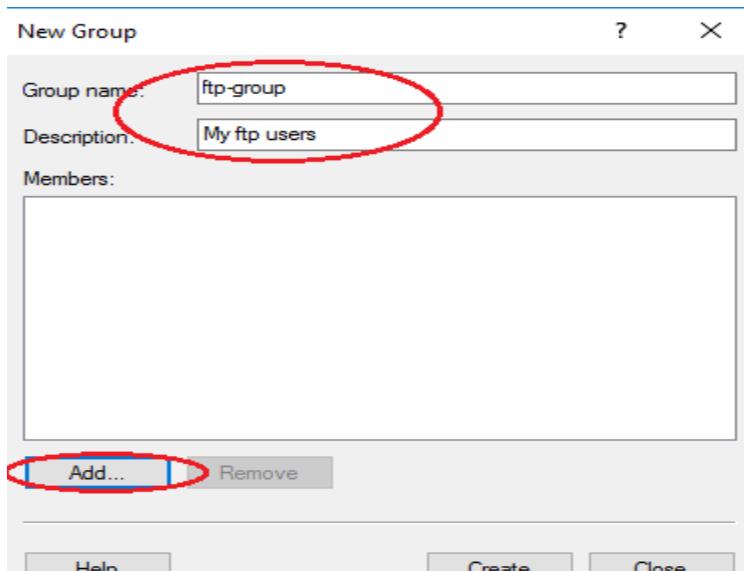


Create user group

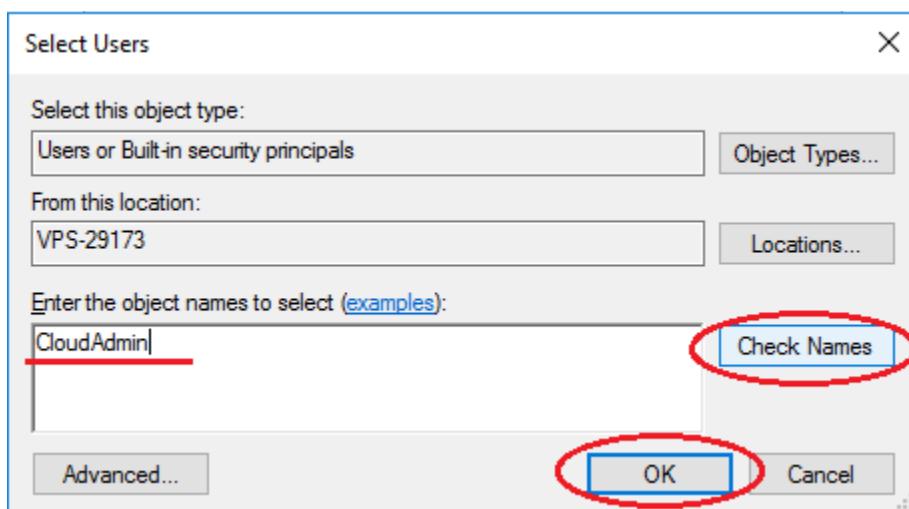
14. Creating a Windows group is necessary to determine the users who will have access to the ftp server. Open Computer Management. In the menu on the right, select Groups. Use the right mouse button to create a new group (New Group).



15. In the window that opens, enter the name of the group, a description if necessary. To add a user, click **Add**.

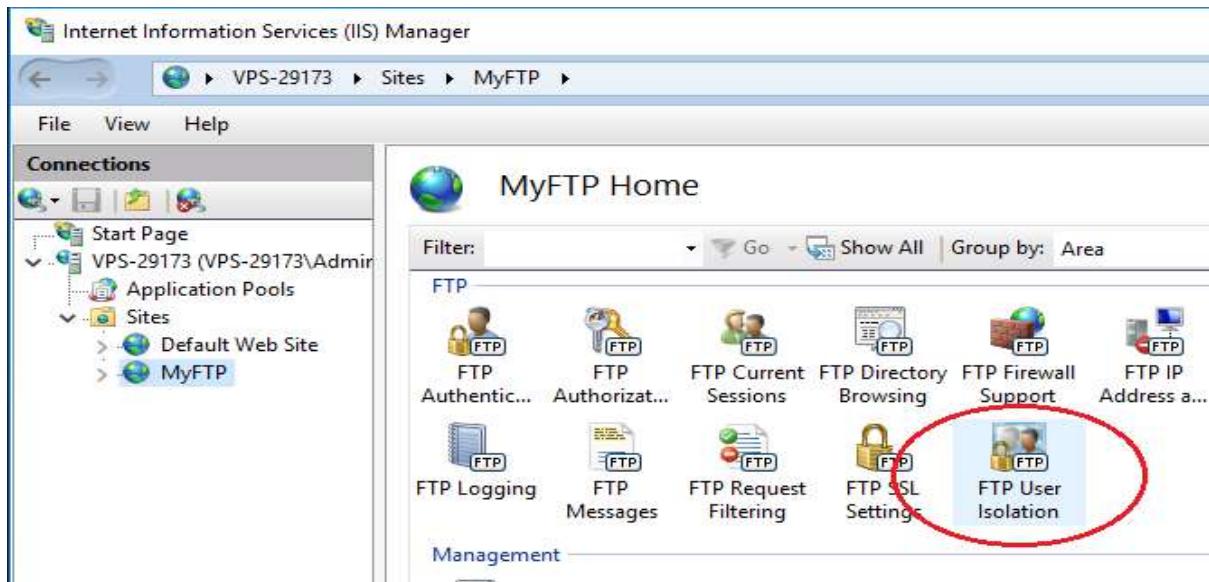


16. Enter a name in the input field, to check it, click **Check Names**. If Windows users exist, click **Ok**.

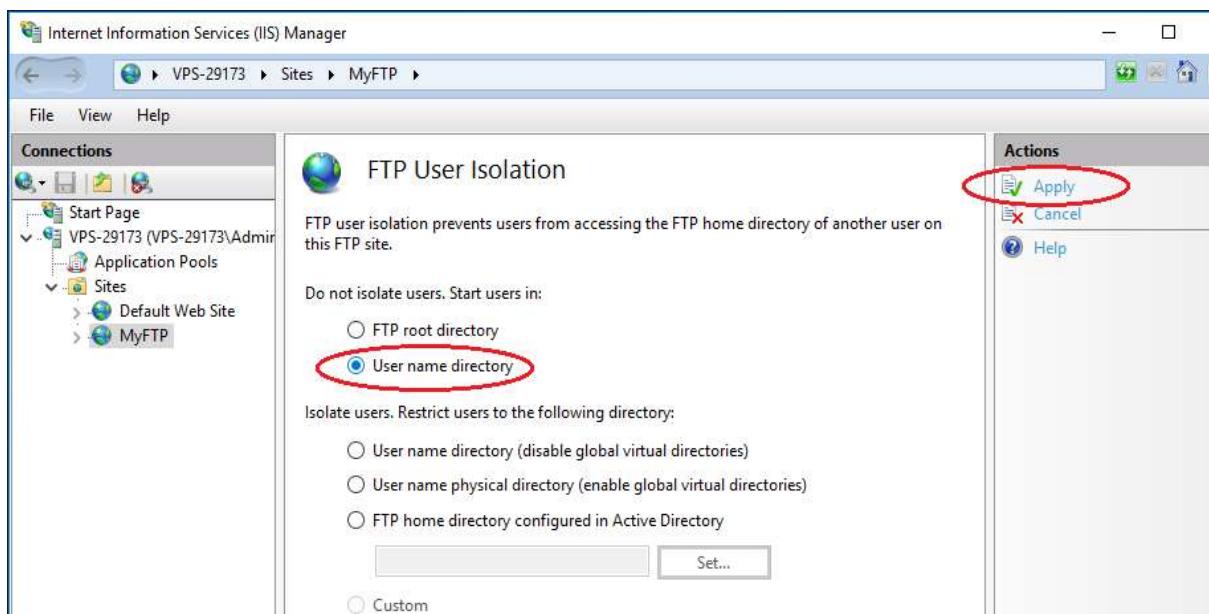


User isolation

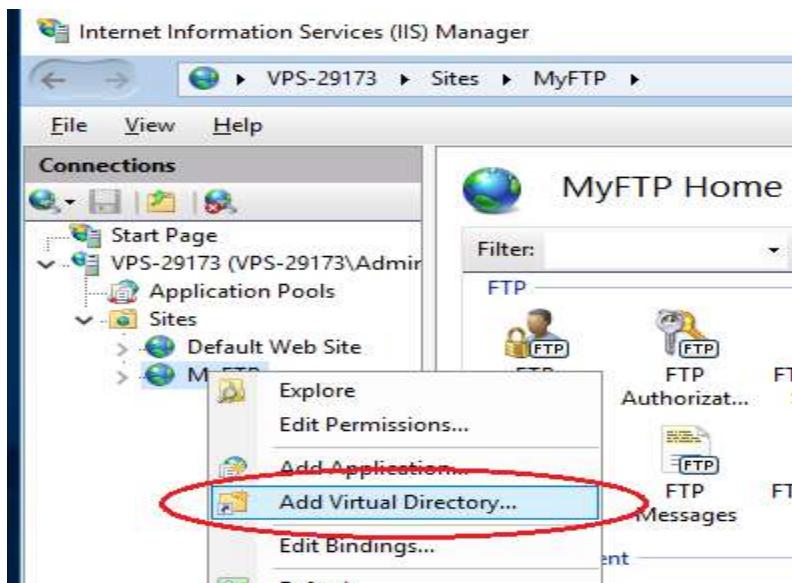
17. In order for each user to get to his own directory and not have access to other files after connecting to the server, it is necessary to set up isolation. To do this, open your ftp site settings and select **FTP User Isolation**.



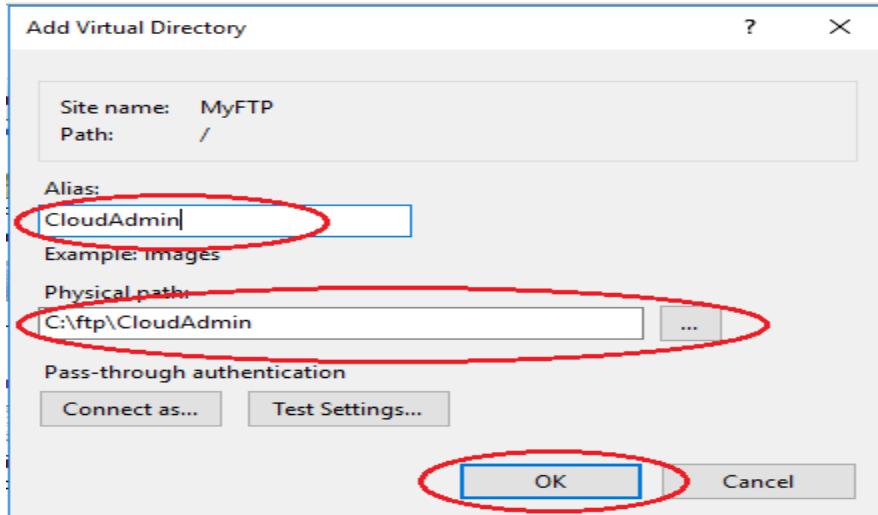
18. Select the **User name directory** and click **Apply**.



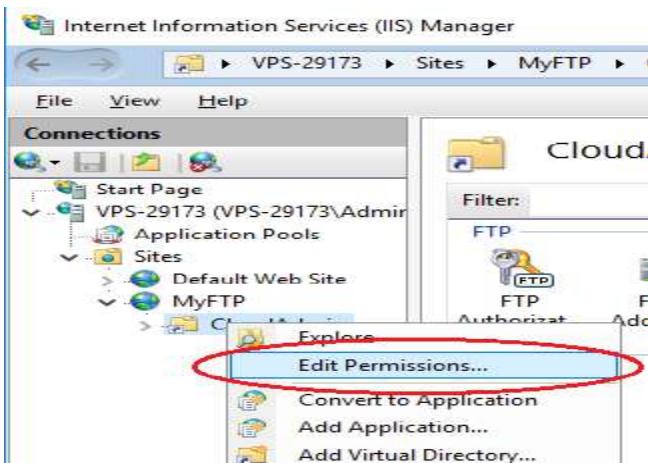
-
19. Then, using the right mouse button, open the menu of your ftp site and select Add Virtual Directory.



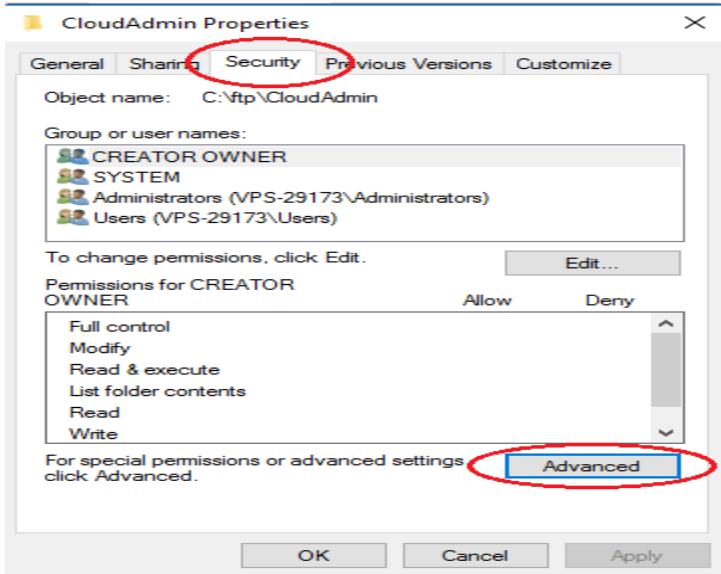
20. In the Alias field, enter a nickname or name, in the path field enter the path to the user directory, to do this, create a subdirectory in the ftp site directory on your Windows server. Click Ok.



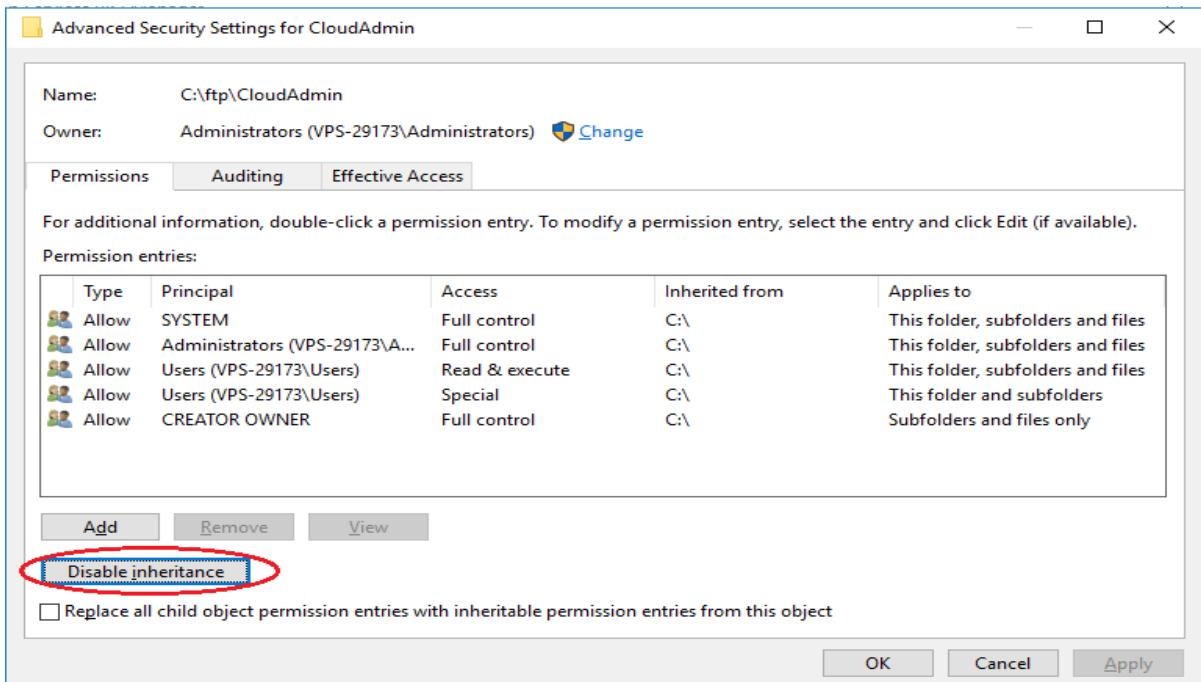
21. To configure permissions in IIS Manager, expand the hierarchical structure of your ftp server. Using the right mouse button, open the Windows virtual directory menu and select **Edit Permission**.

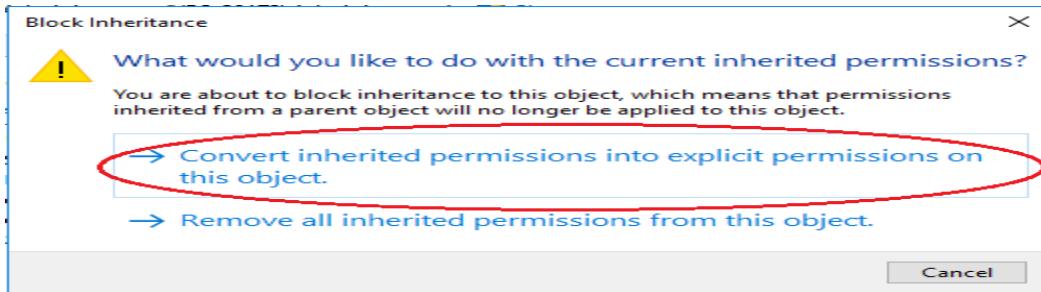


22. Click the **Security** tab and click the **Advanced** button.

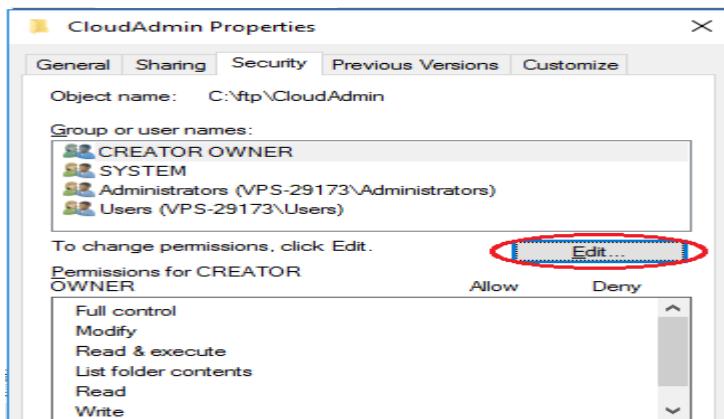


23. In the window that opens, click the **Disable inheritance** button, select the first option in the new window, and then click **Apply - Ok**.

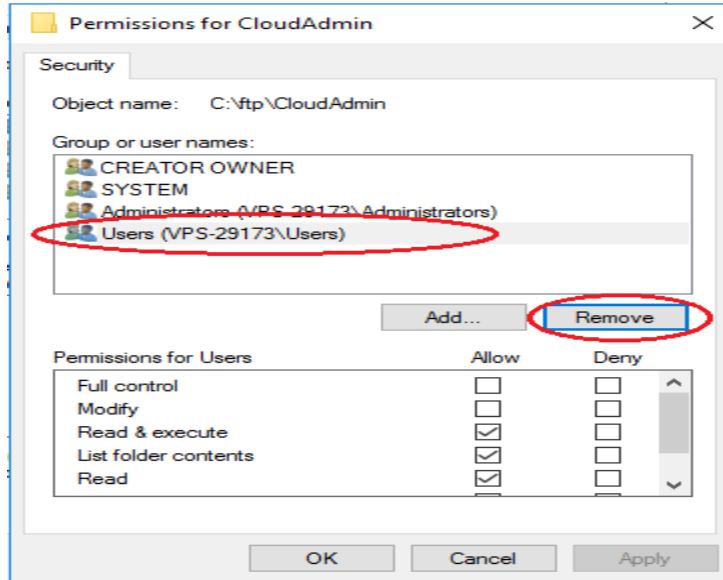




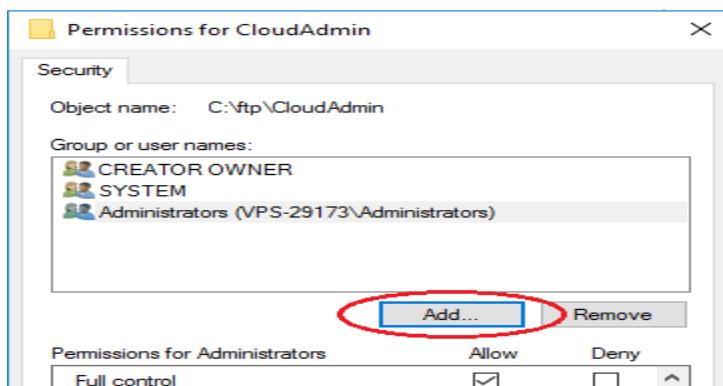
24. Return to the **Security** tab and click the **Edit** button.



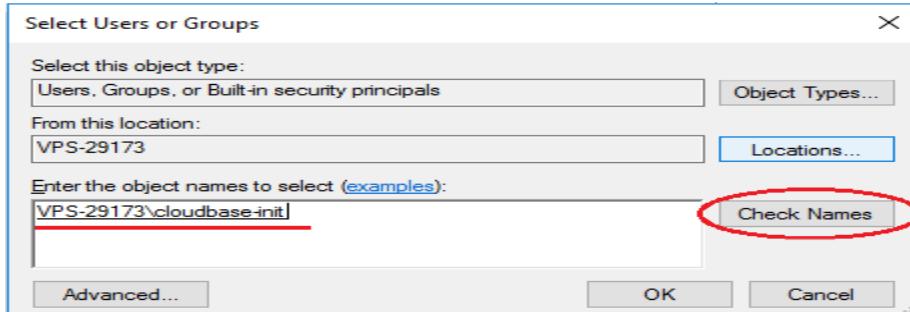
25. Select the **Users** group in which all users are located and click the **Remove** button. This is necessary so that only the owner of the directory has access to it.



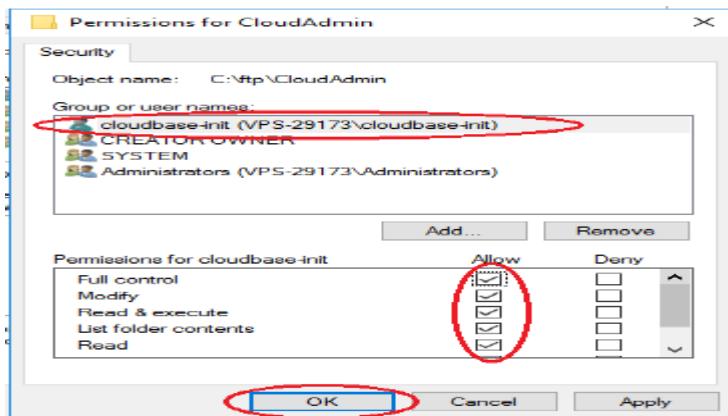
26. Now add a Windows user who will have full access to the directory. Click the **Add** button.



27. Enter the username of the virtual directory in the input field, to check it, click **Check Names**. If users exist, click **Ok**.



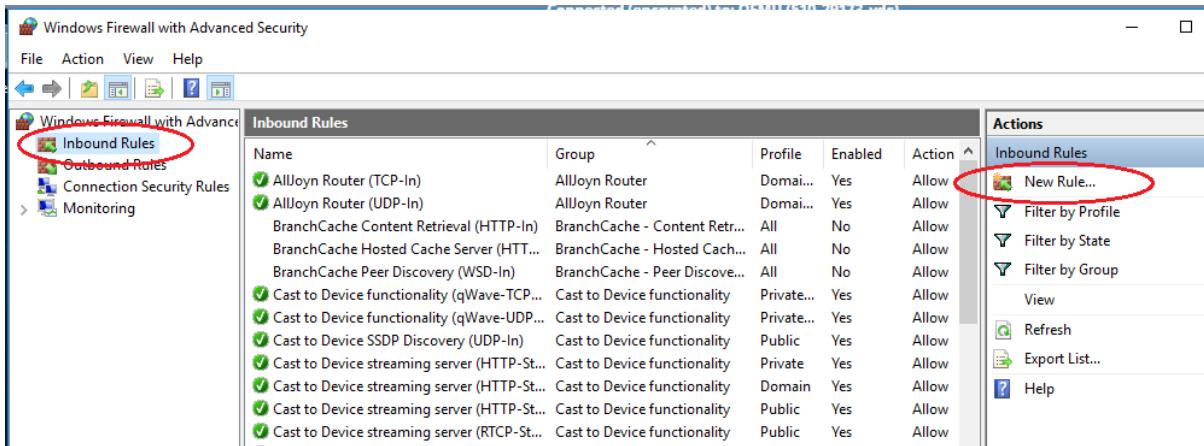
28. Next you need to add rights for complete control of the directory. Select the created user and check all fields Allow (Permissions).



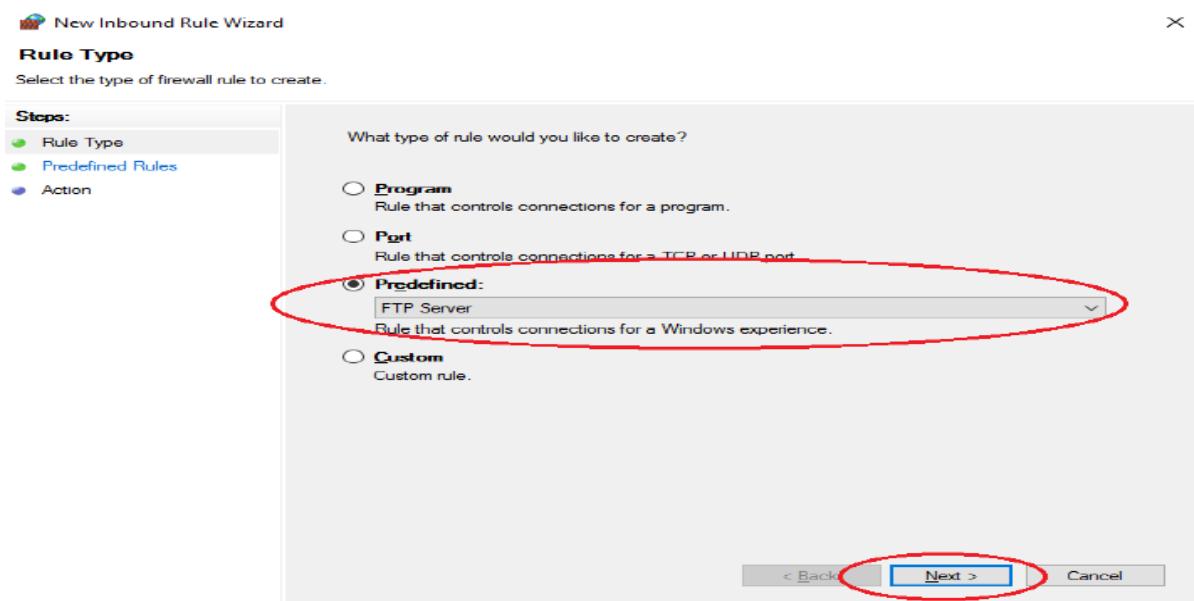
29. Next, click **Apply - Ok**.

Firewall Setup

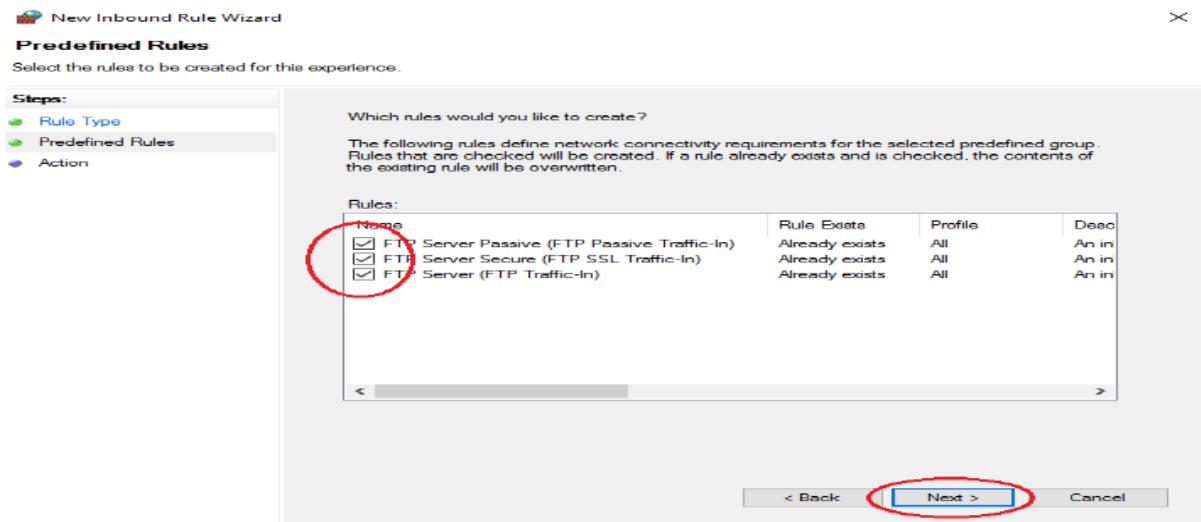
30. For an external connection to the ftp server, you must configure the firewall. To do this, open **Windows Firewall with Advanced Security**. In the vertical menu on the left, select **Inbound rules**, then in the vertical menu on the right **New Rule**.



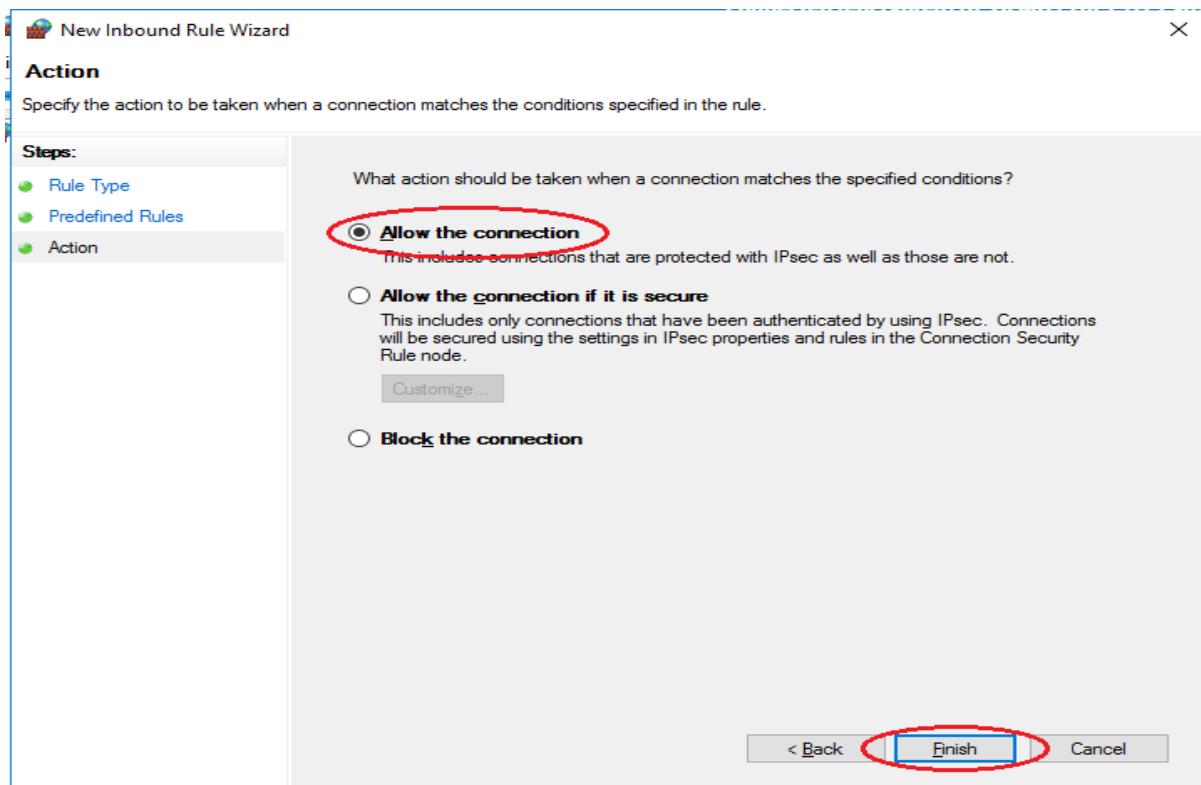
31. In the window that opens, check the **Predefined** type and select FTP Server from the drop-down list. Click **Next**.



32. Select and Mark all the lines and click **Next**.



33. In the next step, select **Allow the connection** and click **Finish**. For these rules to take effect - restart the server.



Connect to an FTP server

34. You can connect to an FTP server in several ways, for example, through the standard Windows utility - Explorer, or through the FileZilla program.

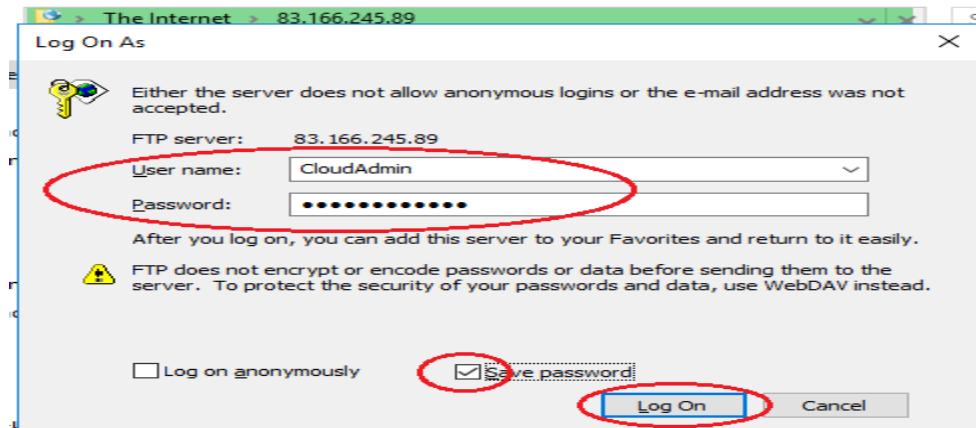
Consider connecting through Explorer. In the address bar, enter:

ftp://ipaddress

For example,

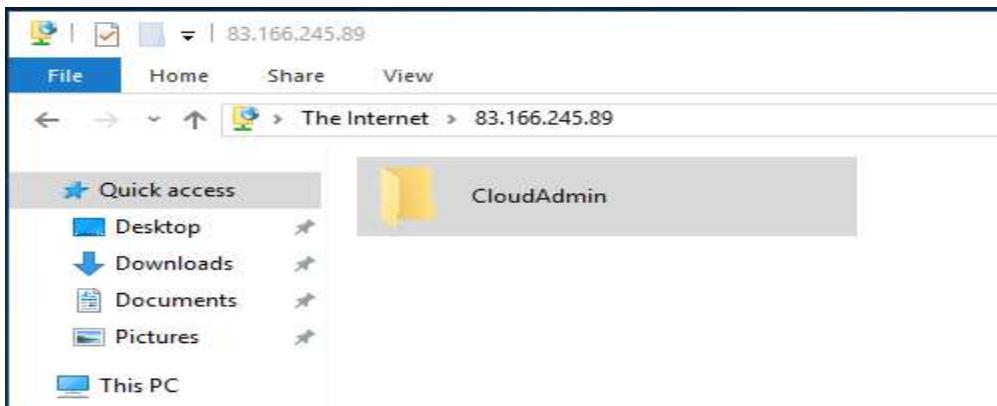
ftp://83.166.245.89

35. The login and password input window will open, specify the connection data from the server control panel.



Output:

As a result, you will see the contents of the FTP server folder:

**References:**

- <https://neoserver.site/help/setting-ftp-server-windows-server-2016>

Activity 11

Aim: Install and Configure HTTP Services

Learning outcome: Able to configure different protocol services

Duration: 2 hour

List of Hardware/Software requirements:

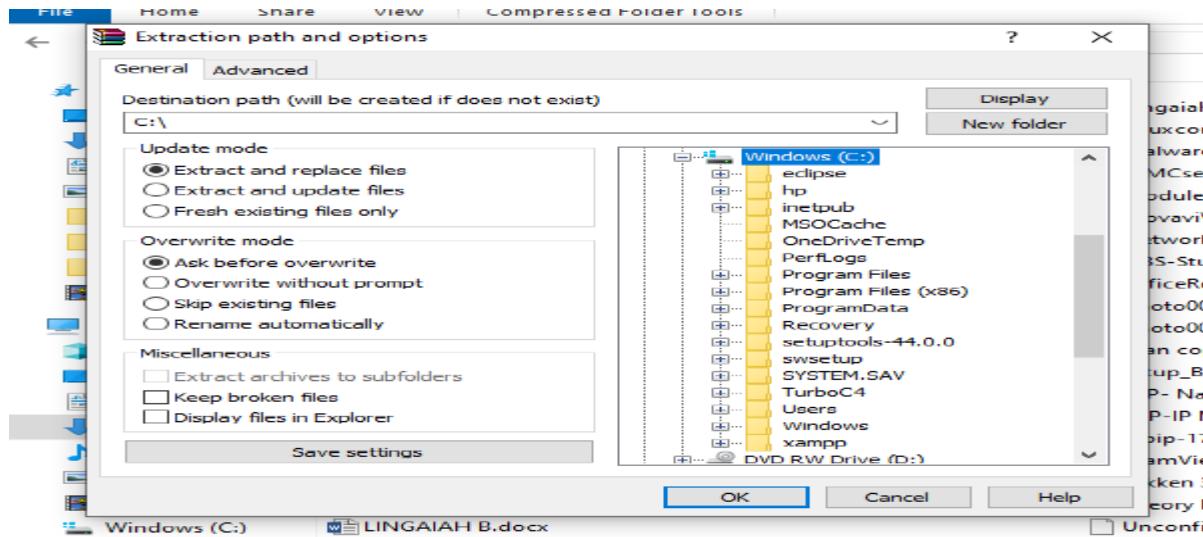
1. Windows Server 2012 R2
2. VMWare Workstation
3. Computer with 8GB RAM/500 GB HD

Code/Program/Procedure (with comments):

1. Download the Apache Software form <https://www.apachelounge.com/download/> and select the Operating system type 32-bit or 64-bit.

The screenshot shows the Apache Lounge website with the title "Apache Lounge Webmasters". On the left, there's a sidebar with links for Home, VS16, VC15, and Additional. The main content area is titled "Apache 2.4 VS16 Windows Binaries and Modules". It contains a brief history of the build, mentioning improvements over VC15 in areas like Performance, Memory Management, and Stability. It also notes that the binaries are backward compatible with VC15 modules. Below this, there are two sections: "Apache 2.4.43 Win64" and "Apache 2.4.43 Win32", each listing a file with its PGP signature and size. A note at the bottom encourages users to verify the integrity of their downloads using PGP.

2. Go to Downloads and extract the ZIP file to the root of the C: drive



3. Open "C:/Apache24/conf" and select httpd.conf and open with notepad.

If there is no any other web services running on your machine then keep "Listen 80" otherwise change it to "Listen 81".

```
httpd.conf - Notepad
File Edit Format View Help

#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 80|


#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding 'LoadModule' lines at this location so the
# "LoadModule module_name module_file" line is valid.
```

4. Test your installation open command prompt and type C:\Apache24\bin press enter and Next-> type httpd -t in command prompt.

```
C:\windows\system32\cmd.exe
C:\Apache24\bin>cd C:\Apache24\bin
C:\Apache24\bin>httpd -t
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using fe80::804:f159:9cc4:e765. Set the 'ServerName' directive globally to suppress this message
Syntax OK
C:\Apache24\bin>
```

5. To Start Apache in the command prompt type:

httpd.exe

```
C:\Windows\system32\cmd.exe - httpd.exe
Microsoft Windows [Version 10.0.18362.720]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\LUCKY>C:\
'C:' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\LUCKY>cd C:\
C:\>cd Apache24
C:\Apache24>cd bin
C:\Apache24\bin>httpd.exe
AH00558: httpd.exe: Could not reliably determine the server's fully qualified domain name
5. Set the 'ServerName' directive globally to suppress this message
```

6. We can test your installation by opening up your Browser and typing in the address:
<http://localhost>



It works!

7. To stop the apache service press **Ctrl+C** in Command Propmpt.

```
cmd Select C:\windows\system32\cmd.exe
Microsoft Windows [Version 10.0.18362.720]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\LUCKY>C:\
'C:' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\LUCKY>cd C:\
C:\>cd Apache24

C:\Apache24>cd bin

C:\Apache24\bin>httpd.exe
AH00558: httpd.exe: Could not reliably determine the server's fully qual
5. Set the 'ServerName' directive globally to suppress this message

C:\Apache24\bin>
```

8. To install as a service. Open command prompt as Administrator and type:

>httpd.exe -k install

```
Administrator: Command Prompt

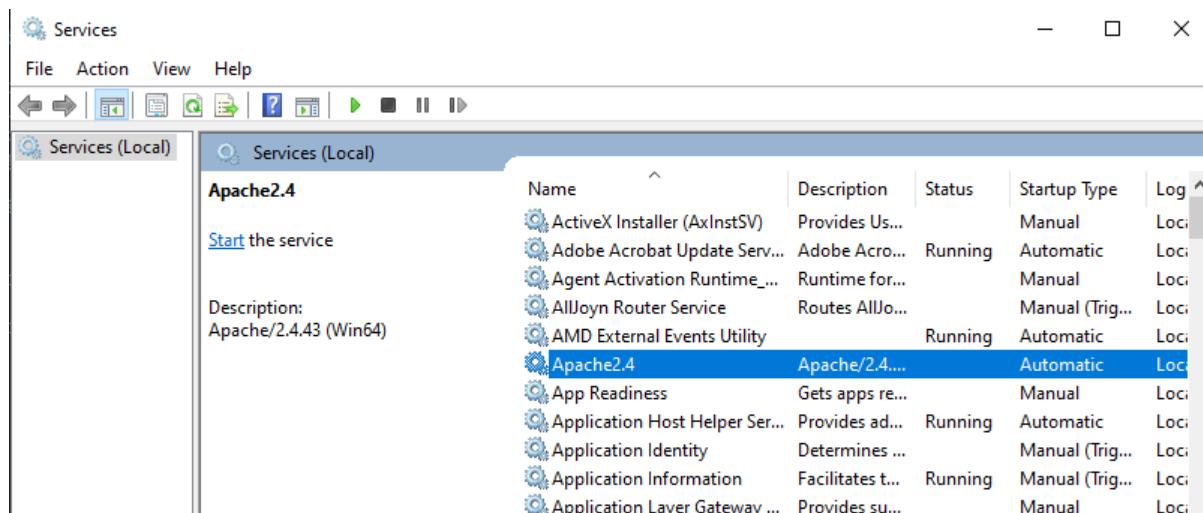
C:\windows\system32>cd C:\Apache24\bin

C:\Apache24\bin>httpd.exe -k install
Installing the 'Apache2.4' service
The 'Apache2.4' service is successfully installed.
Testing httpd.conf....
Errors reported here must be corrected before the service can be started.
AH00558: httpd.exe: Could not reliably determine the server's fully qualified do
5. Set the 'ServerName' directive globally to suppress this message

C:\Apache24\bin>
```

9. we can start/stop the service with the command:

>services.msc



Output:

← → ⌂ ⓘ localhost:81

It works!

Reference:

- <https://www.sitepoint.com/how-to-install-apache-on-windows/>

Activity 12

Aim: Configure IIS Services

Learning outcome: Able to configure different protocol services

Duration: 3 hour

List of Hardware/Software requirements:

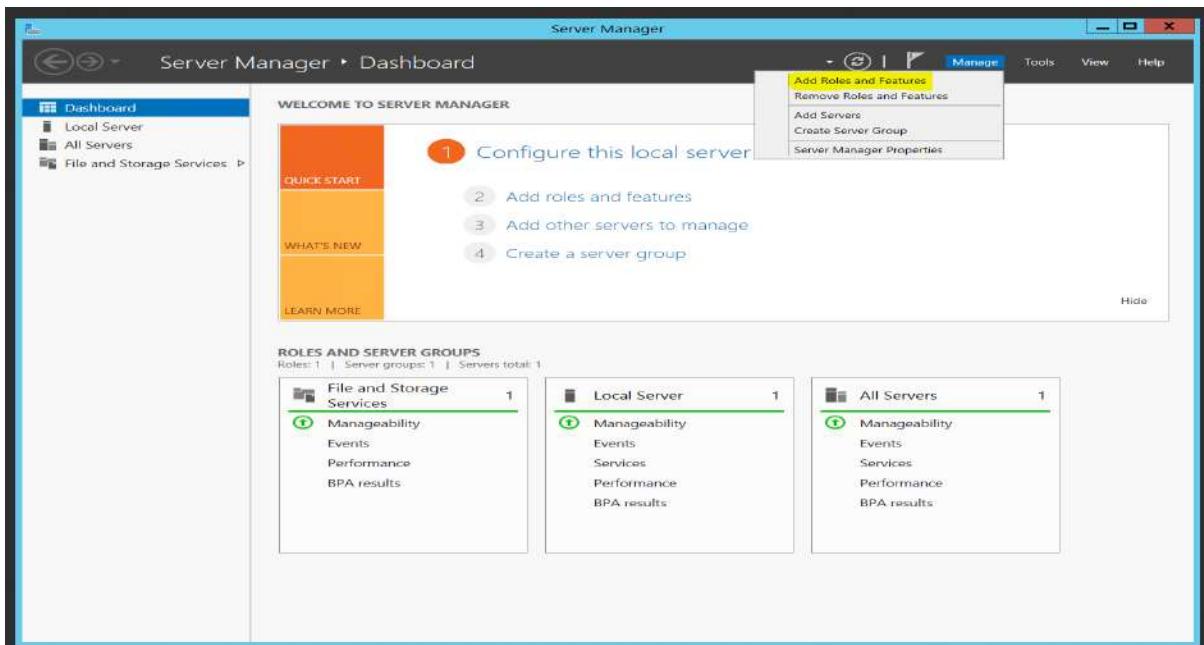
1. Windows Server 2012 R2
2. VMWare Workstation
3. Computer with 8GB RAM/500 GB HD

Code/Program/Procedure (with comments):

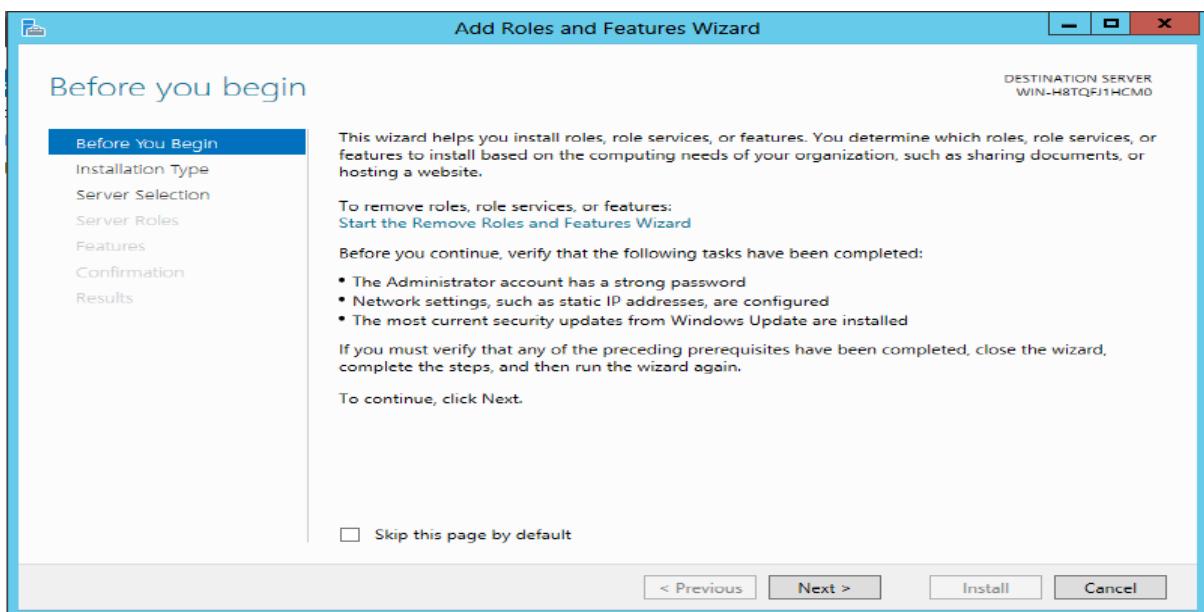
1. Open the **Start Menu** and select the **Server Manager** icon.



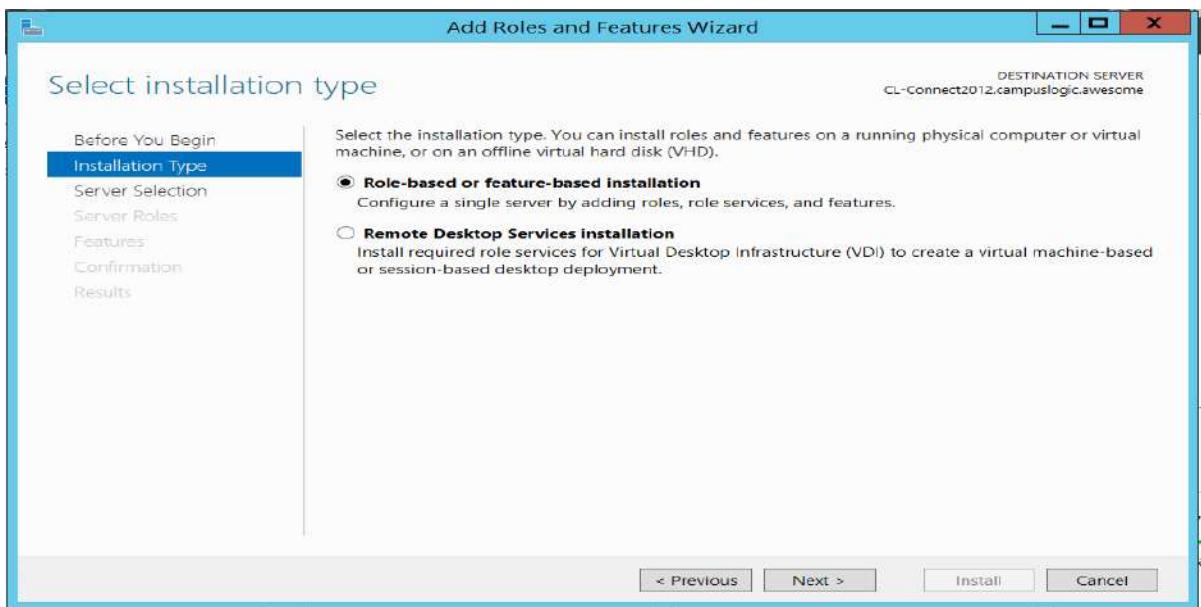
2. In the Server Manager click **Manage** in the upper right hand corner, then **Add Roles and Features**.



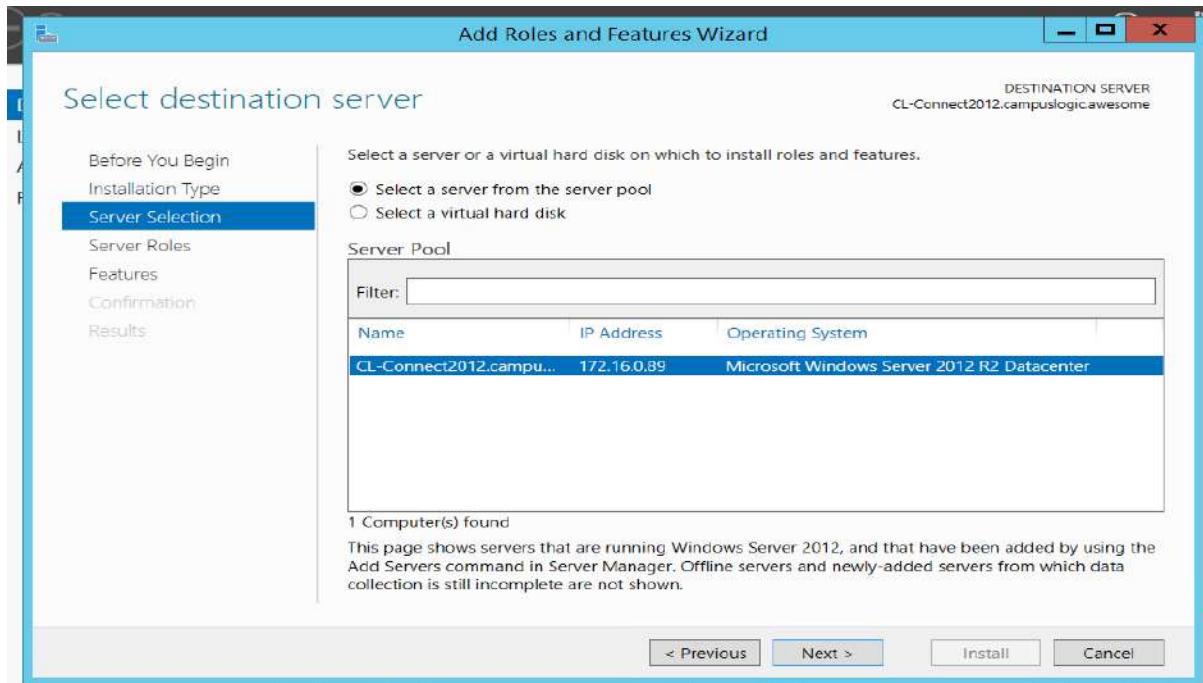
3. Click **Next**



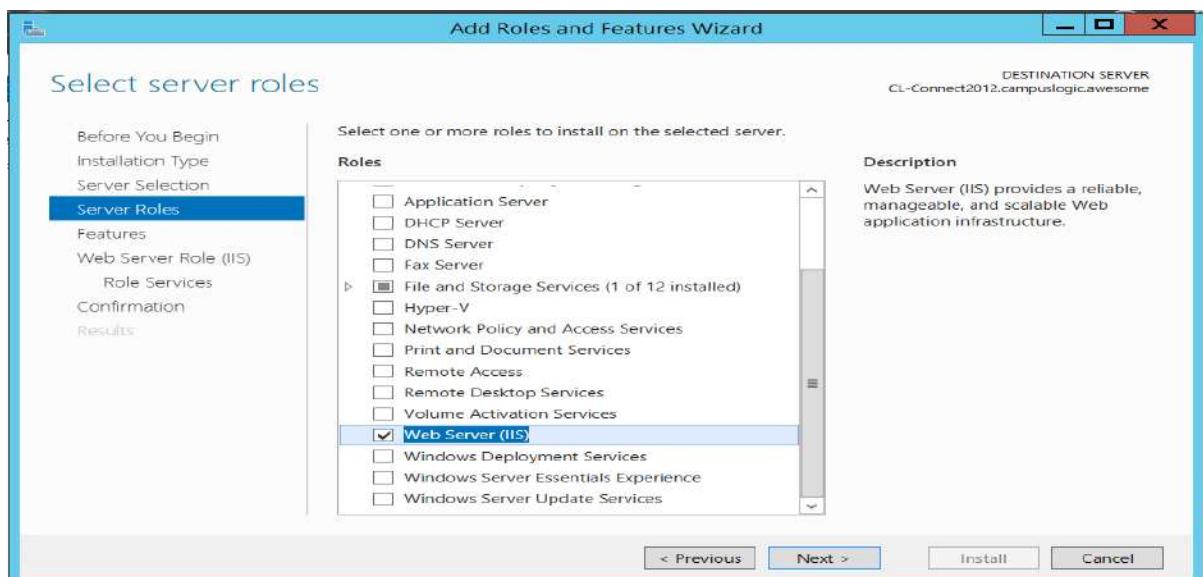
4. On the left hand side, select **Installation Type** and ensure **Role-based or feature-based installation** is selected. Click **Next**.



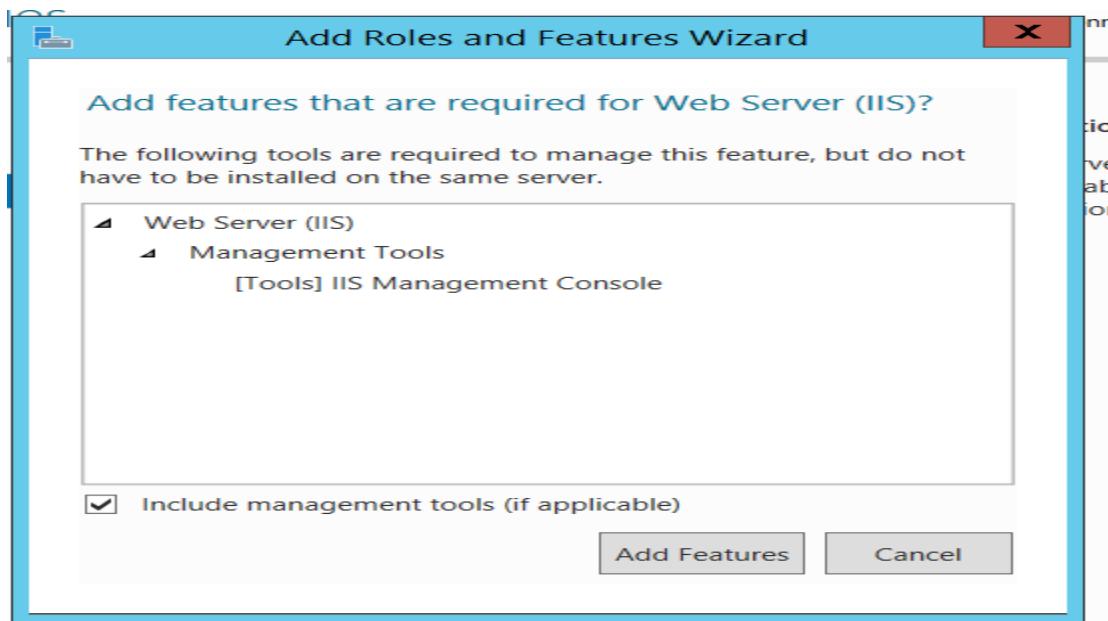
5. Select the appropriate server and hit **Next**



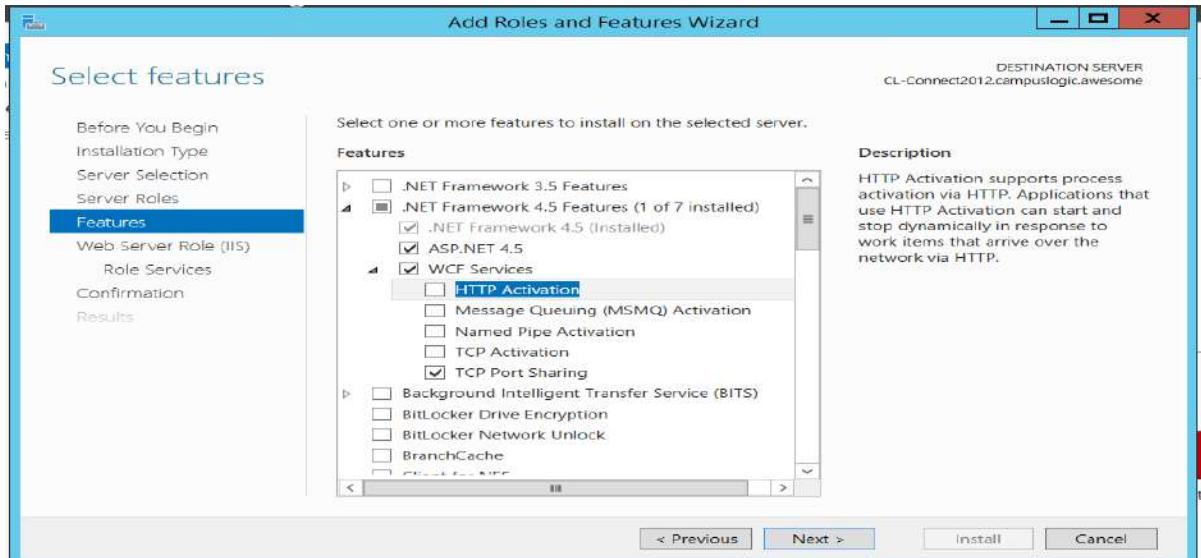
6. Scroll down to **Web Server(IIS)** and check the checkbox



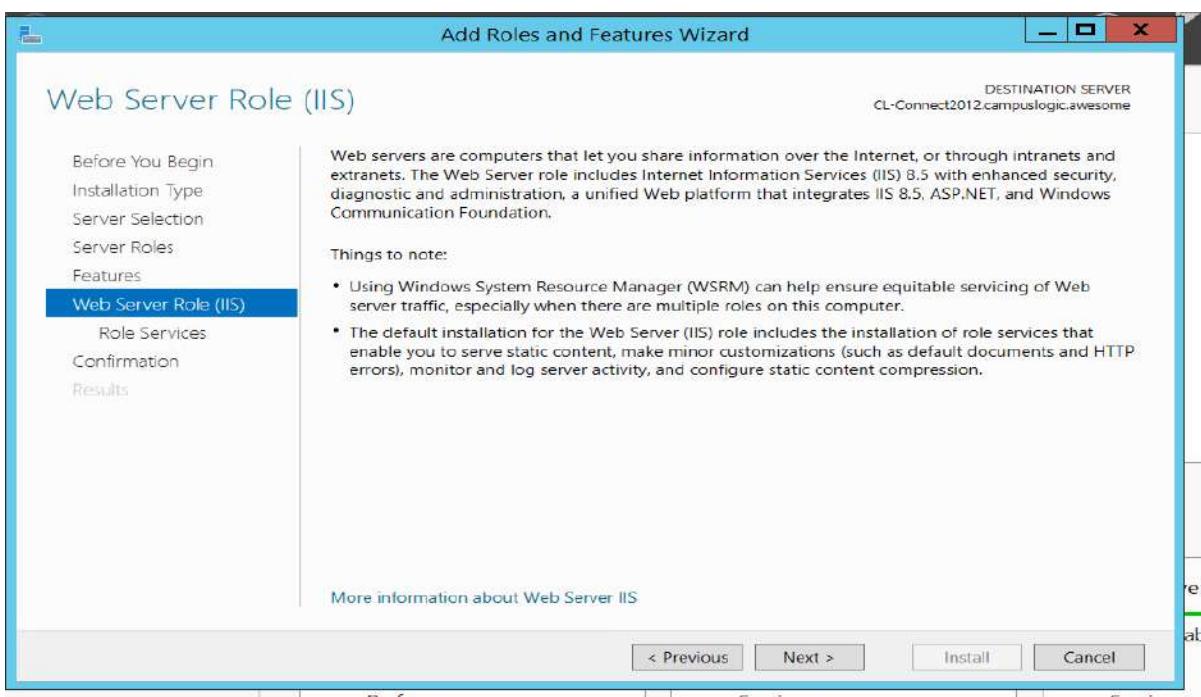
-
7. This will create a pop-up, **check the Include Management tools box**, and click **Add Features**. This will take you back to the Add Roles and Features Wizard. Click **Next**.



8. After IIS Server installed, open the server manager and click on 'Manage'. Then, select 'Add Roles and Features' and then click the 'Next' button until you reach the "Select Features" screen shown below.

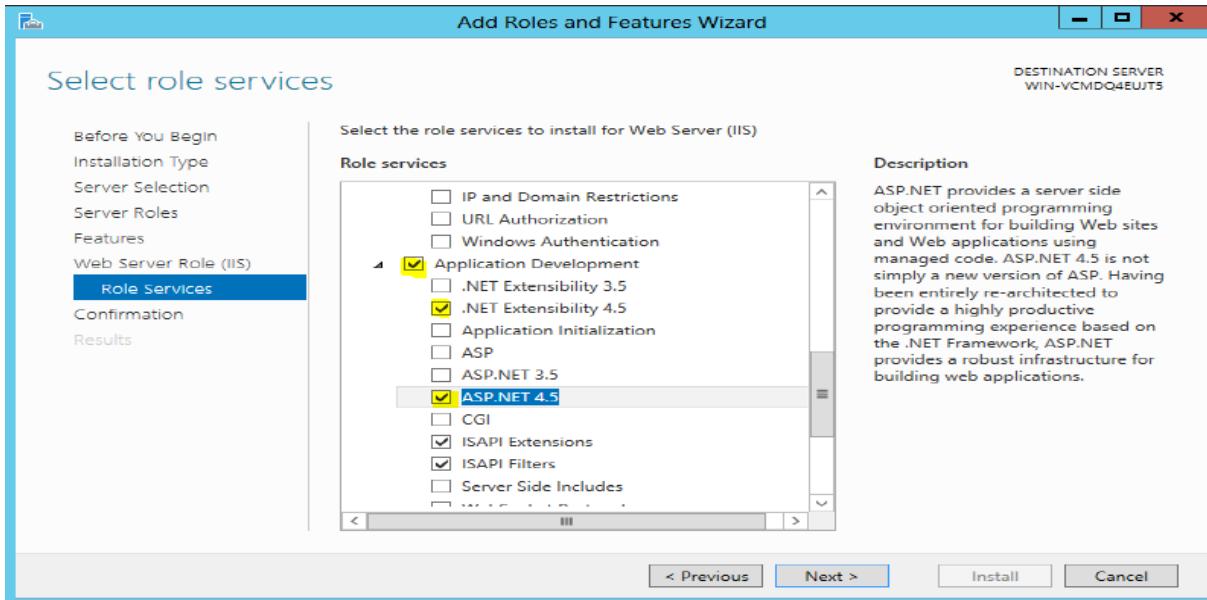


9. Click Next

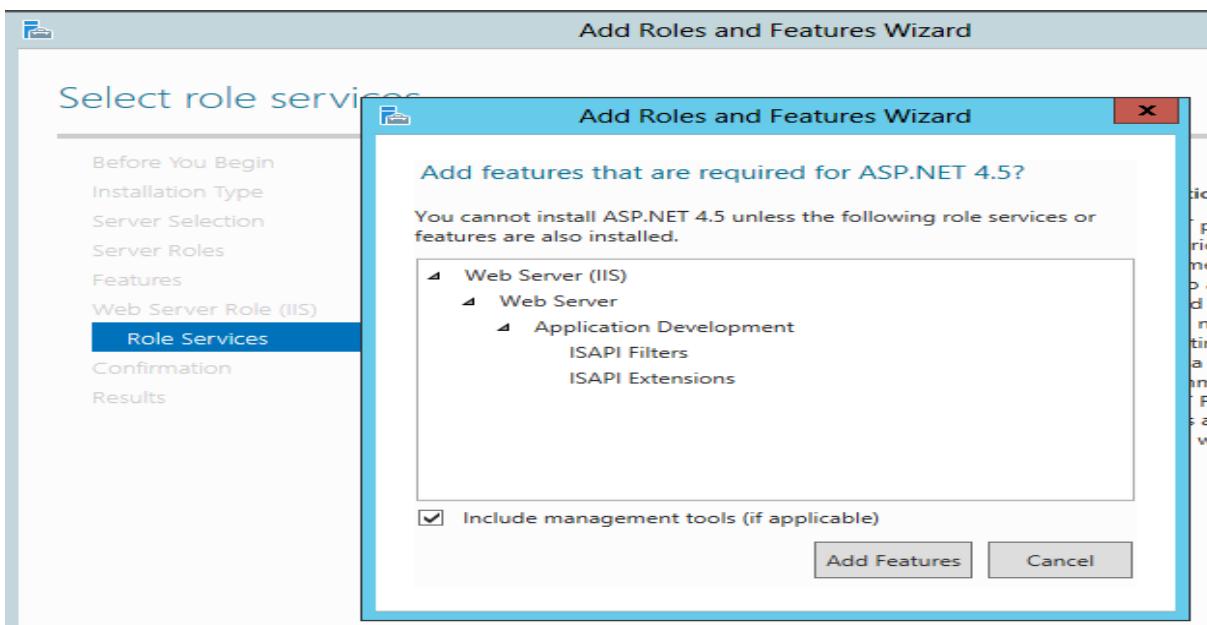


10. On Role Service, scroll down to the Application Development option and expand it.

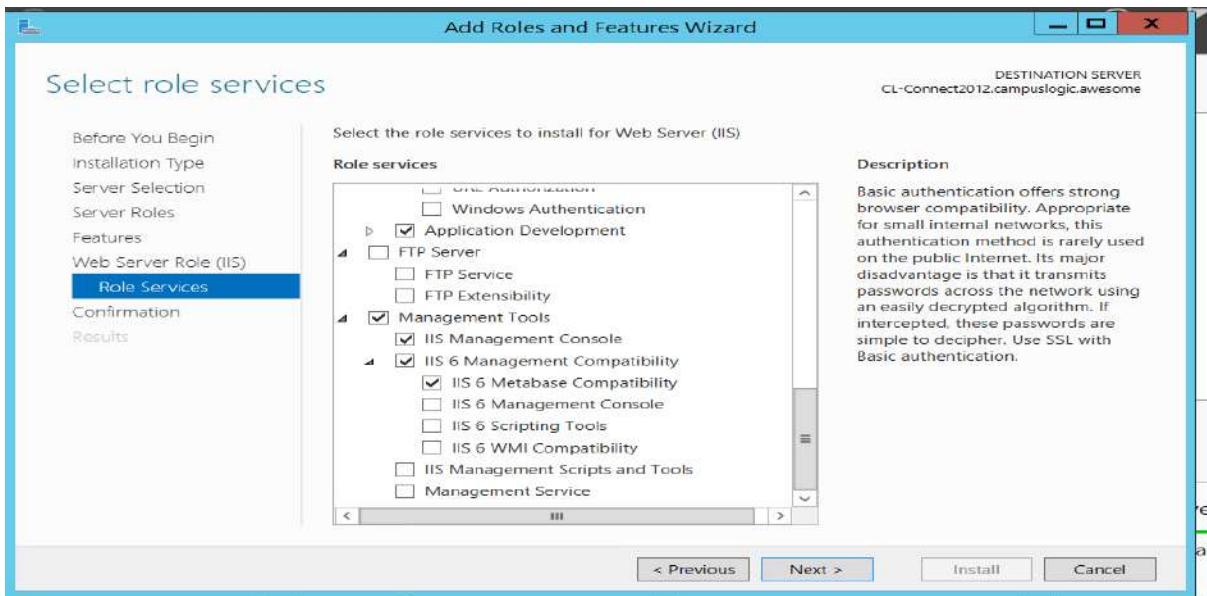
Then select .NET Extensibility 4.5 and ASP.NET4.5.



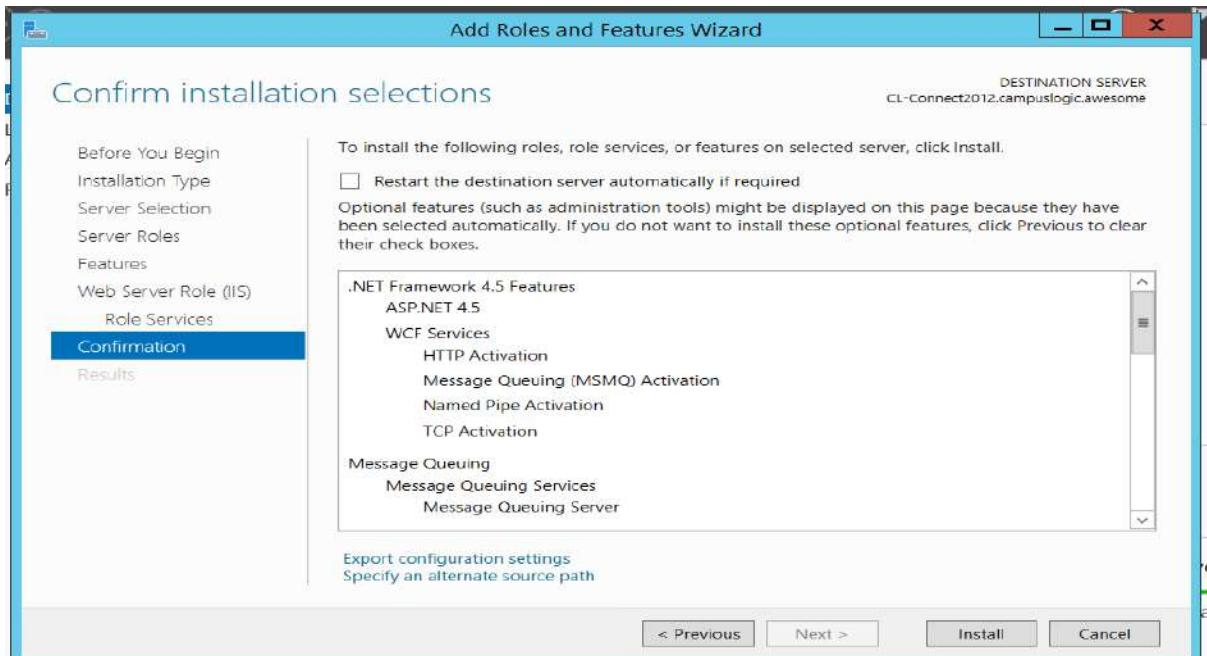
11. If prompted, select "Add Features".



12. Then scroll down and select **IIS Management Console** and **IIS 6 Metabase Compatibility**. Click Next.

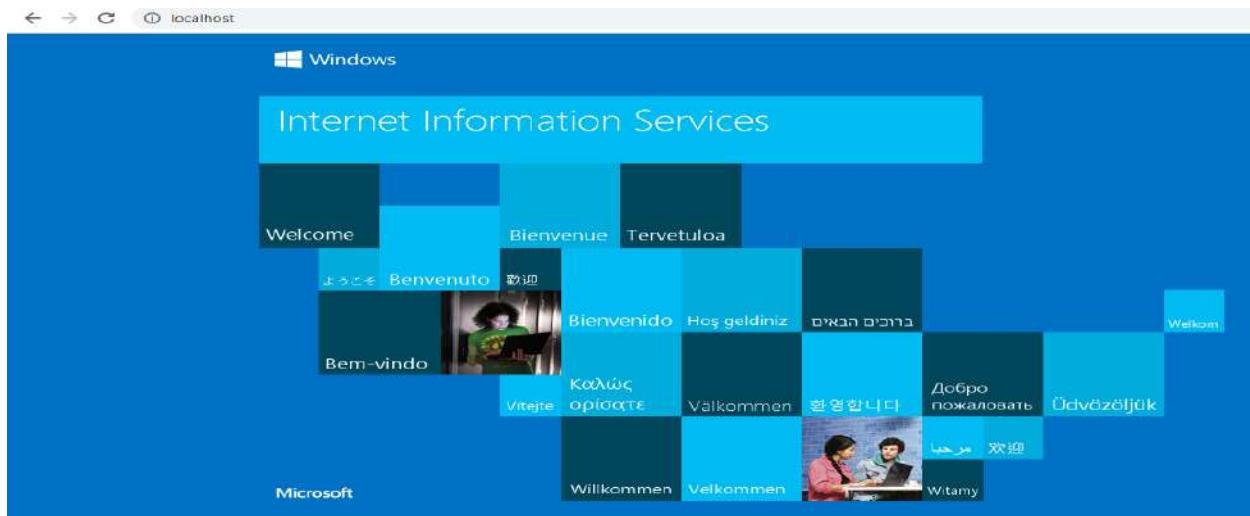


13. Click Install



Output:

Open Browser and enter <http://localhost> in URL.

**References:**

- <https://docs.microsoft.com/en-us/iis/install/installing-iis-85/installing-iis-85-on-windows-server-2012-r2>

Learning Outcome 4 - Able to Install and configure Linux server environment

After achieving this learning outcome, a student will be able to install and configure the Linux server environment. In order to achieve this learning outcome, a student has to complete the following:

1. Install Linux Server (3Hrs)
2. Create new user and group (2 Hrs)
3. Create public and data directory (2 Hrs)
4. Create an lmlhosts file (3 Hrs.)
5. InsCheck host file (2Hrs)
6. Filter ports (3Hrs)
7. Secure and run SWAT (5 Hrs)
8. Install and configure Telnet (5 Hrs)

Activity 1

Aim: Install Linux Server.

Learning outcome: Able to understand Linux Installation

Duration: 3 hour

List of Hardware/Software requirements:

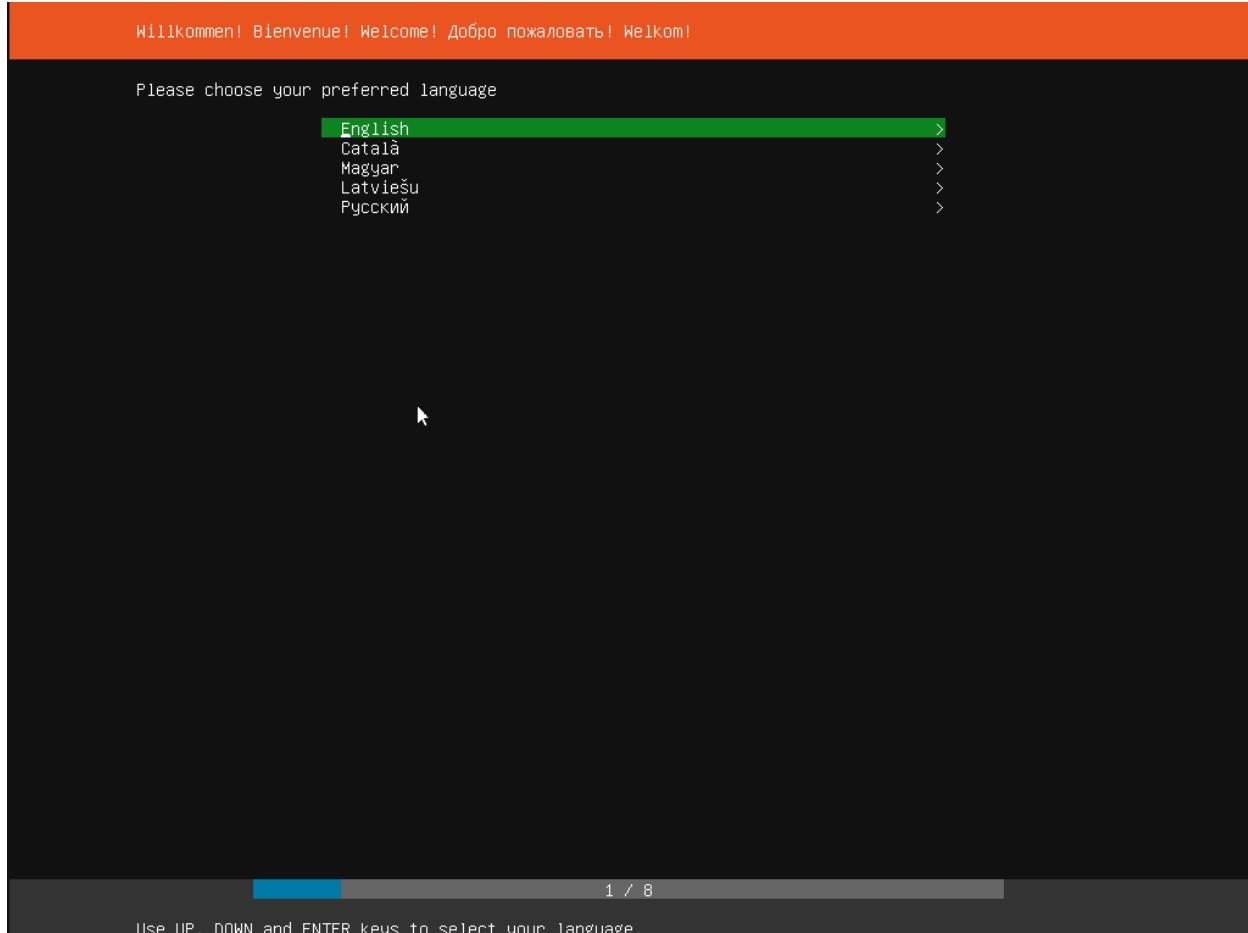
1. Ubuntu Server 19.0 Bootable Image or CD
2. VMWare or Oracle Virtual Box Software

Code/Program/Procedure (with comments):

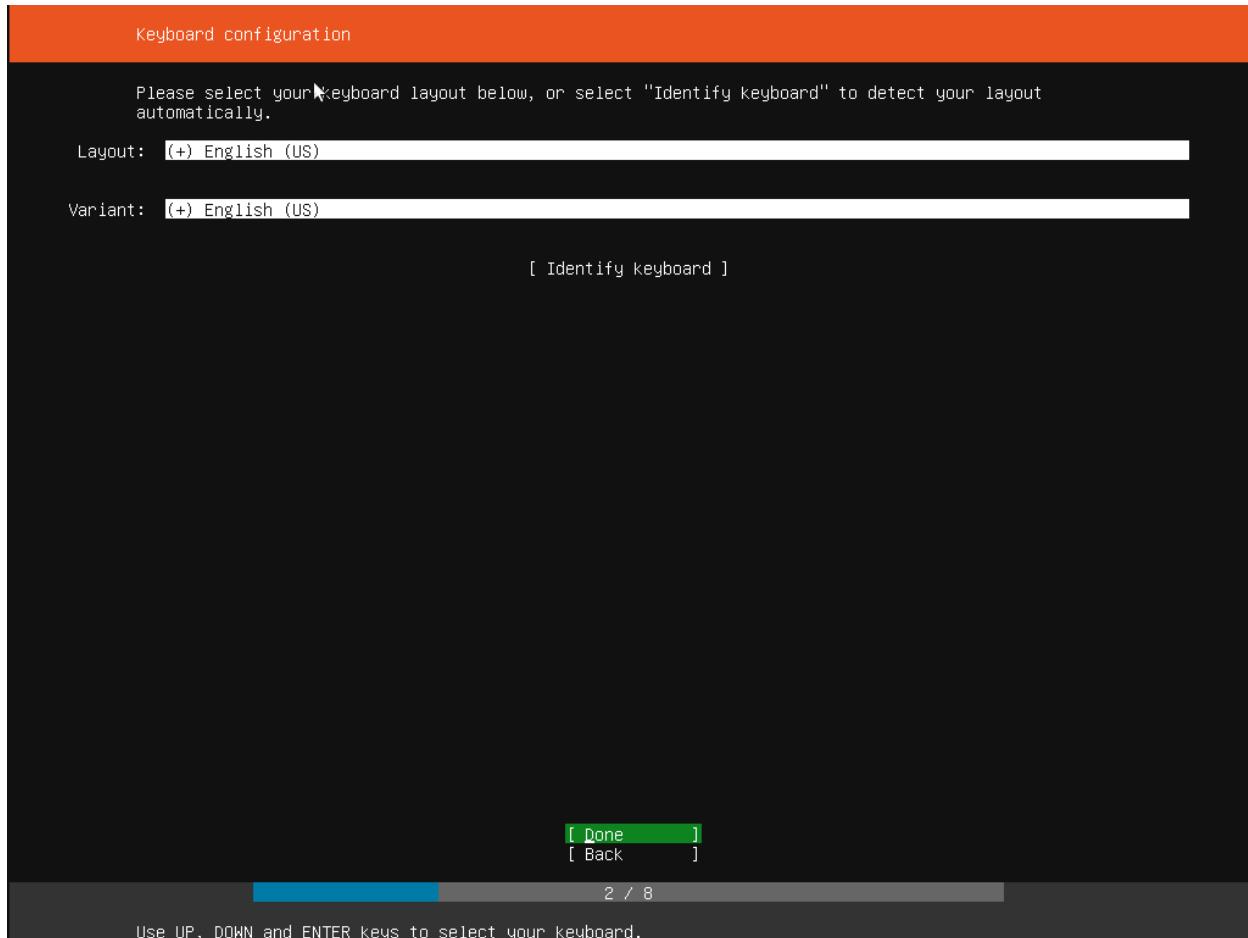
1. Put the Ubuntu DVD into your DVD drive (or insert the USB stick or other install media).
2. Restart your computer.

```
chroot: can't execute 'glib-compile-schemas': No such file or directory
Using CD-ROM mount point /cdrom/
Identifying... [92043204992947830abda80987b766a7-2]
Scanning disc for index files...
Found 2 package indexes, 0 source indexes, 0 translation indexes and 1 signatures
Found label 'Ubuntu-Server 18.04 LTS _Bionic Beaver_ - Beta amd64 (20180404)'
This disc is called:
'Ubuntu-Server 18.04 LTS _Bionic Beaver_ - Beta amd64 (20180404)'
Copying package lists...[ TIME ] Timed out waiting for device dev-disk-by\x2duuid-00c629d6\x2d06ab\x2d4dfd\x2db21e\x2dc3186f3410
5d.device.
[DEPEND] Dependency failed for /subiquity_config.
[ OK ] Started Uncomplicated firewall.
[ OK ] Started Create list of required static device nodes for the current kernel.
      Starting Create Static Device Nodes in /dev...
[ OK ] Mounted POSIX Message Queue File System.
[ OK ] Mounted Kernel Debug File System.
[ OK ] Started Remount Root and Kernel File Systems.
      Starting Load/Save Random Seed...
[ OK ] Mounted Huge Pages File System.
[ OK ] Started Load/Save Random Seed.
[ OK ] Started Create Static Device Nodes in /dev.
      Starting udev Kernel Device Manager...
[ OK ] Started Journal Service.
      Starting Flush Journal to Persistent Storage...
[ OK ] Started udev Kernel Device Manager.
[ OK ] Started Load Kernel Modules.
      Mounting Kernel Configuration File System...
      Mounting FUSE Control File System...
      Starting Apply Kernel Variables...
[ OK ] Started Flush Journal to Persistent Storage.
[ OK ] Mounted FUSE Control File System.
[ OK ] Mounted Kernel Configuration File System.
[ OK ] Started LVM2 metadata daemon.
[ OK ] Started udev Coldplug all Devices.
[ OK ] Started Monitoring of LVM2 mirrors, snapshots etc. using dmeventd or progress polling.
[ OK ] Started Apply Kernel Variables.
-
```

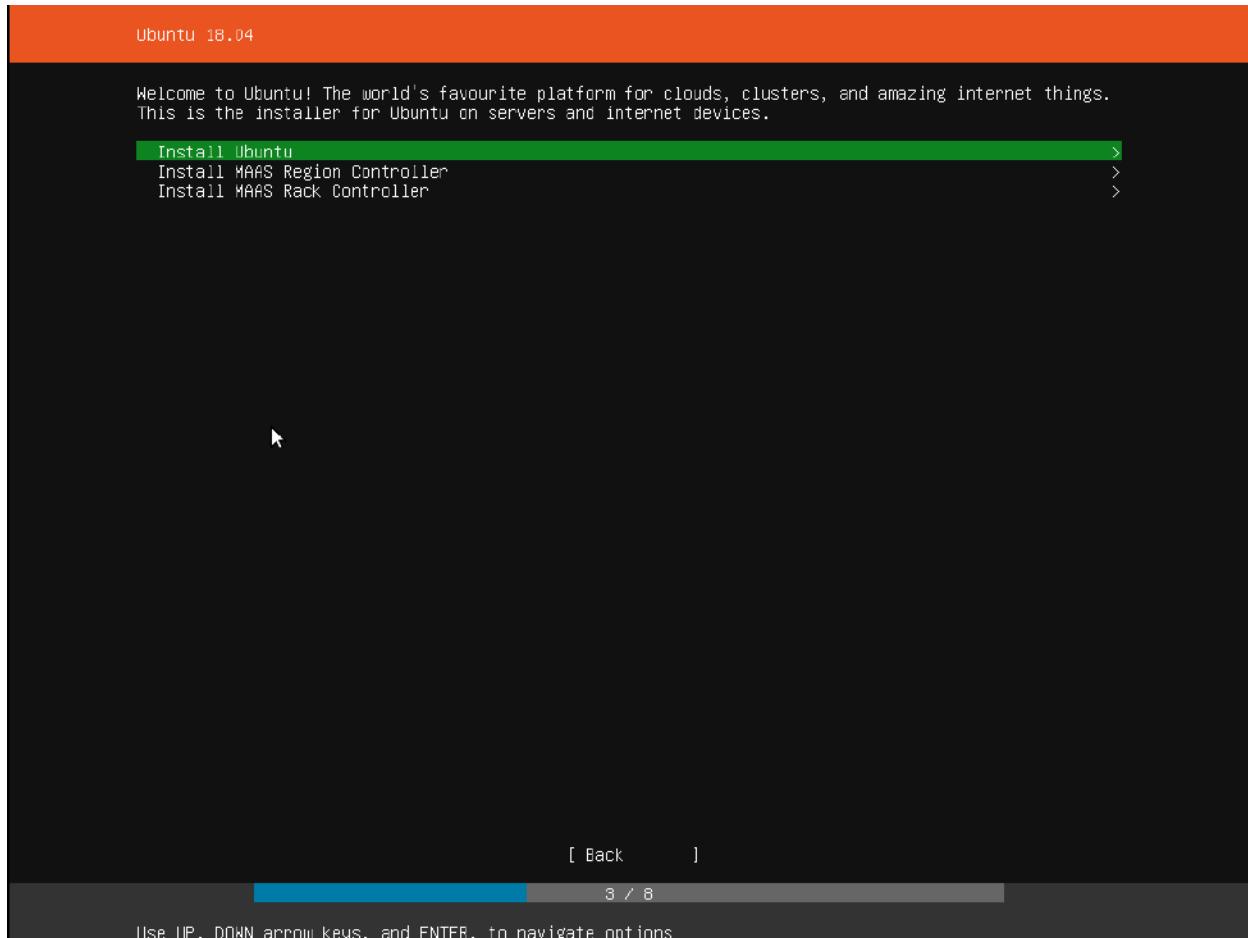
3. Choose your language



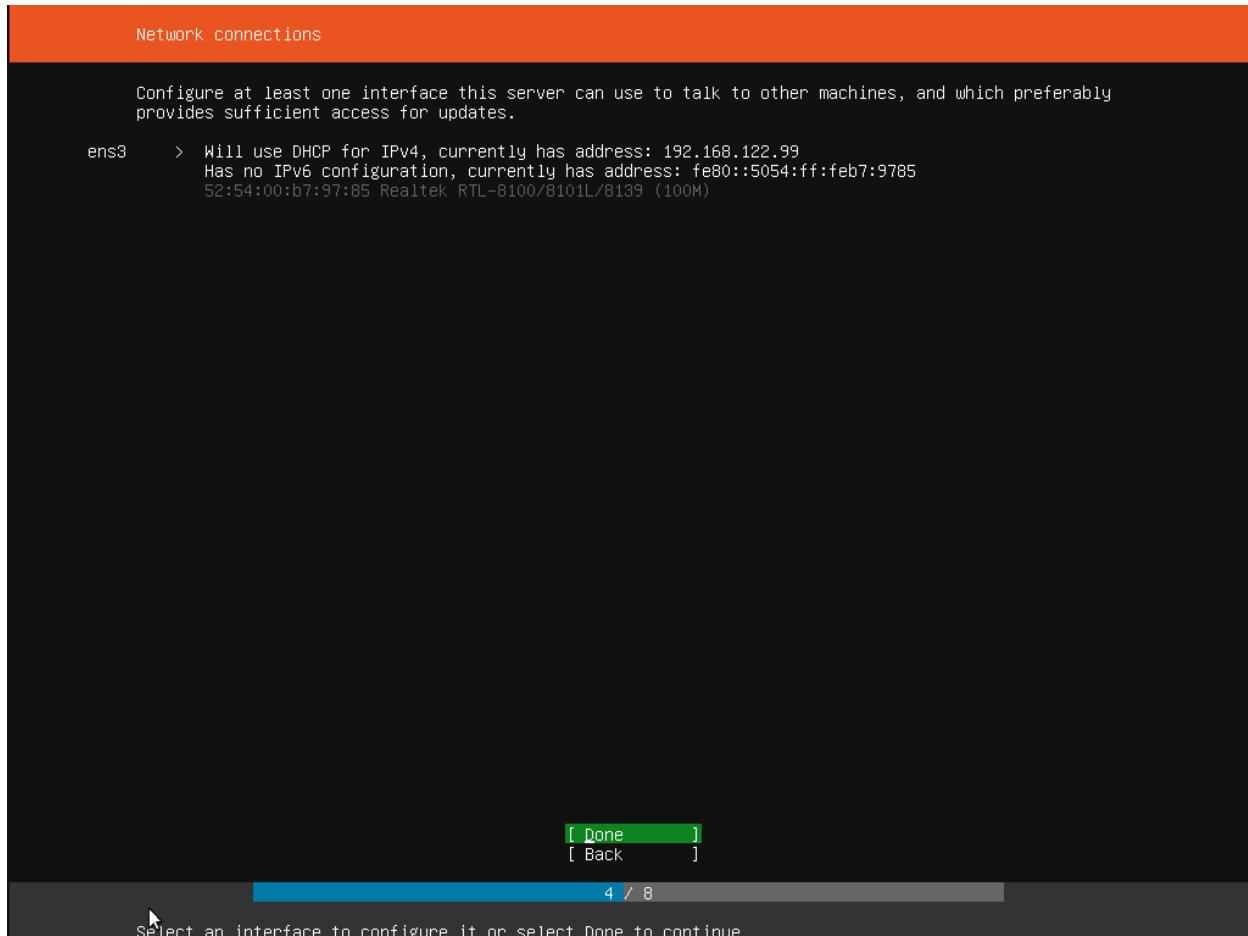
4. Choose the correct keyboard layout



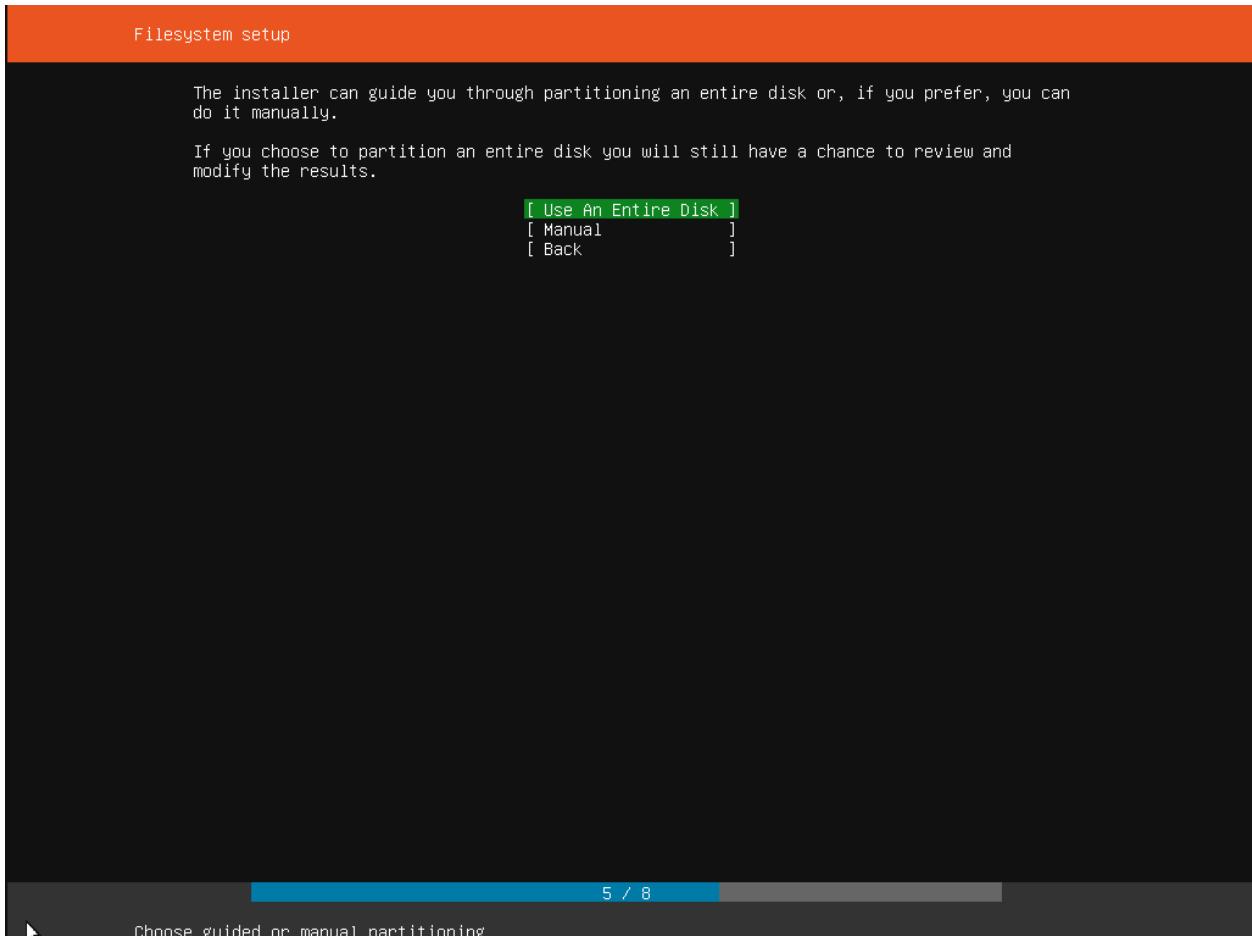
5. Choose your install



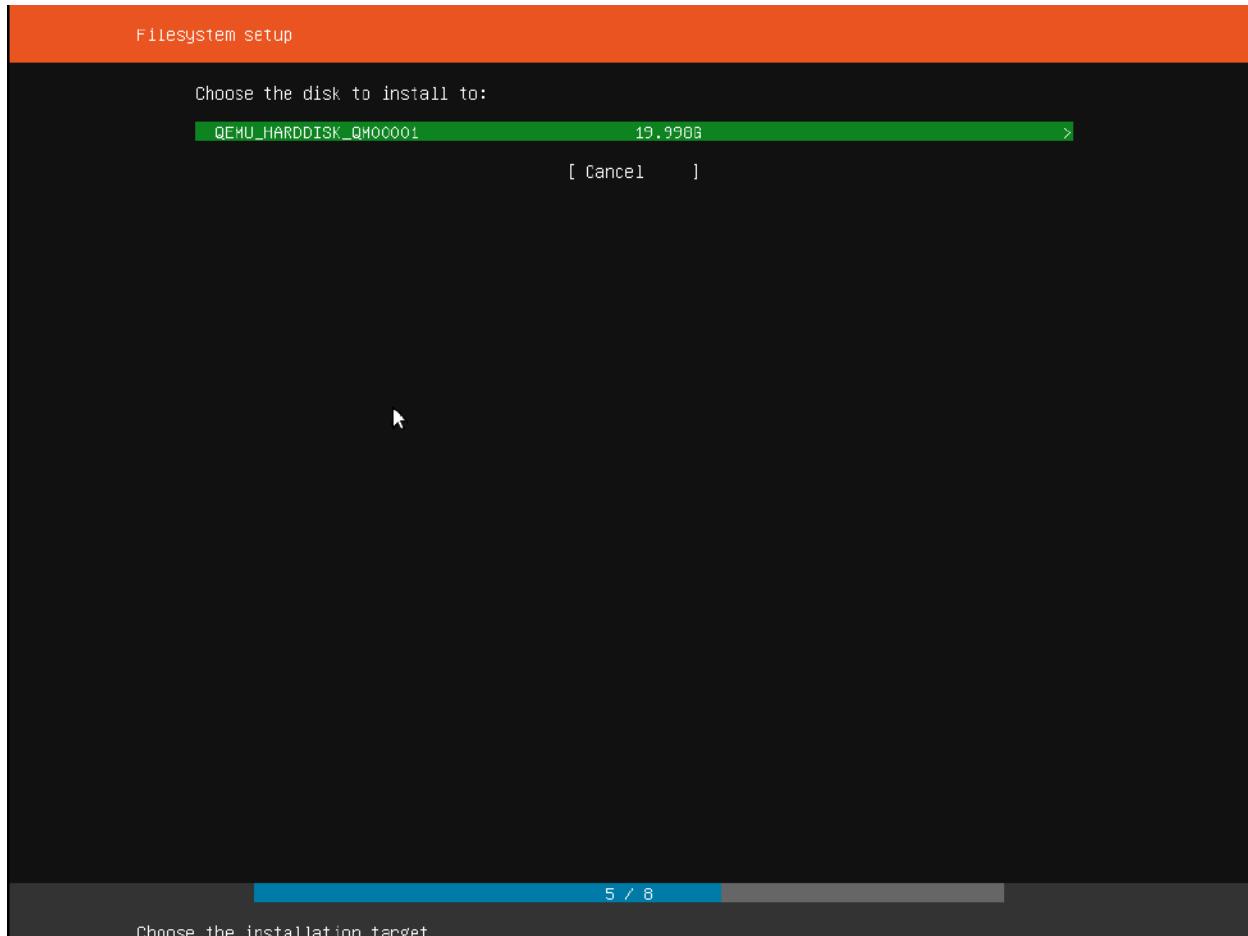
6. Networking



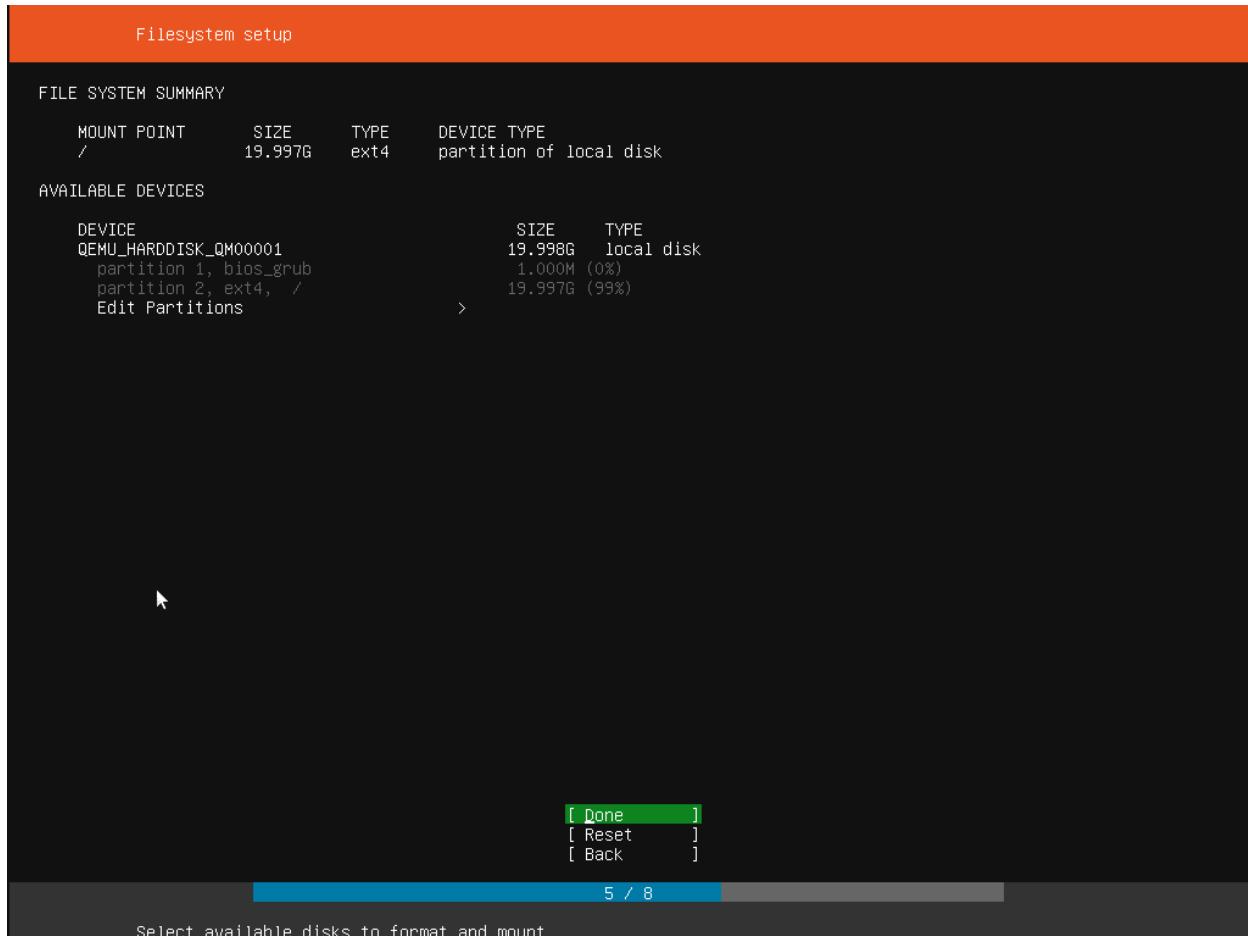
7. Configure storage



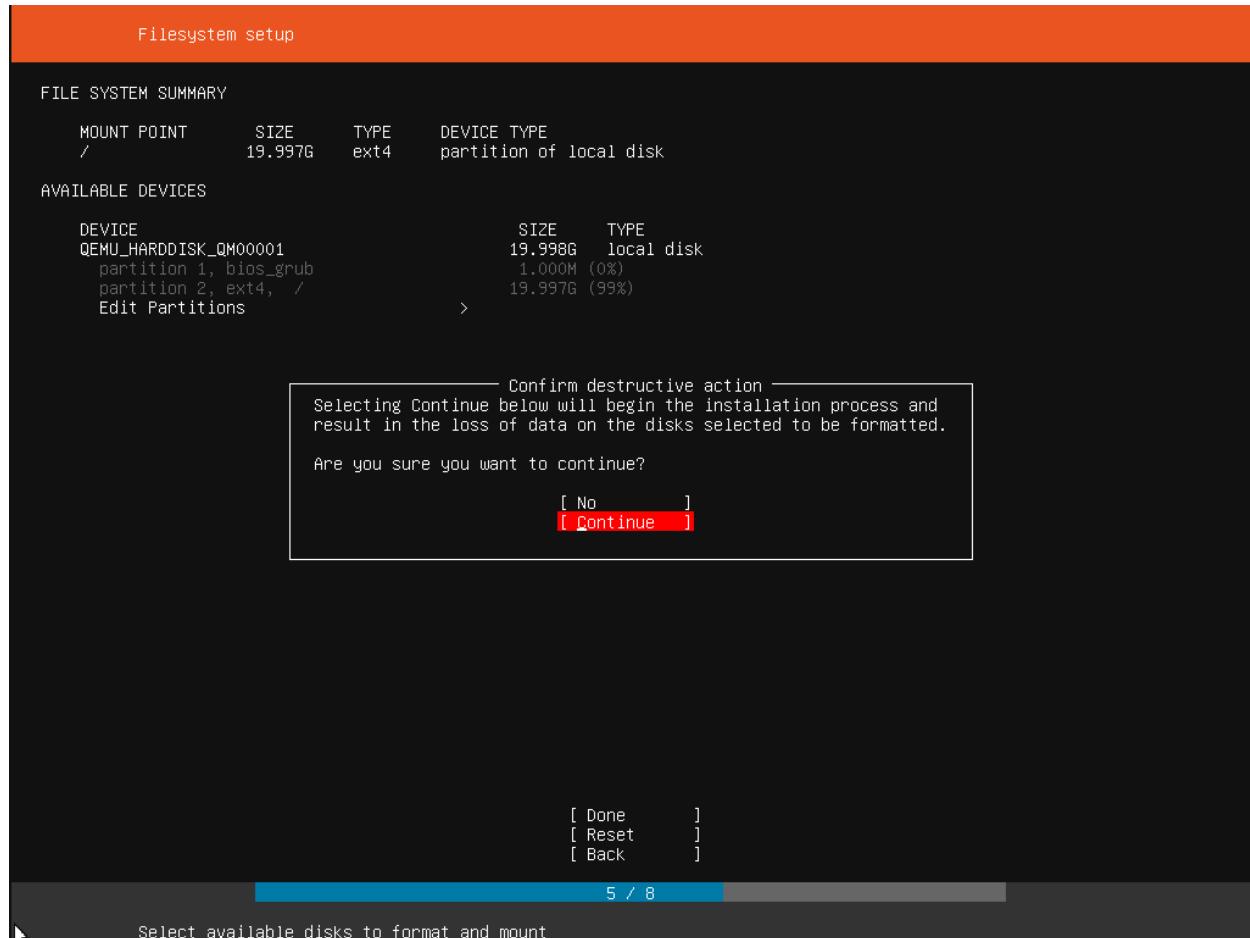
8. Select a device



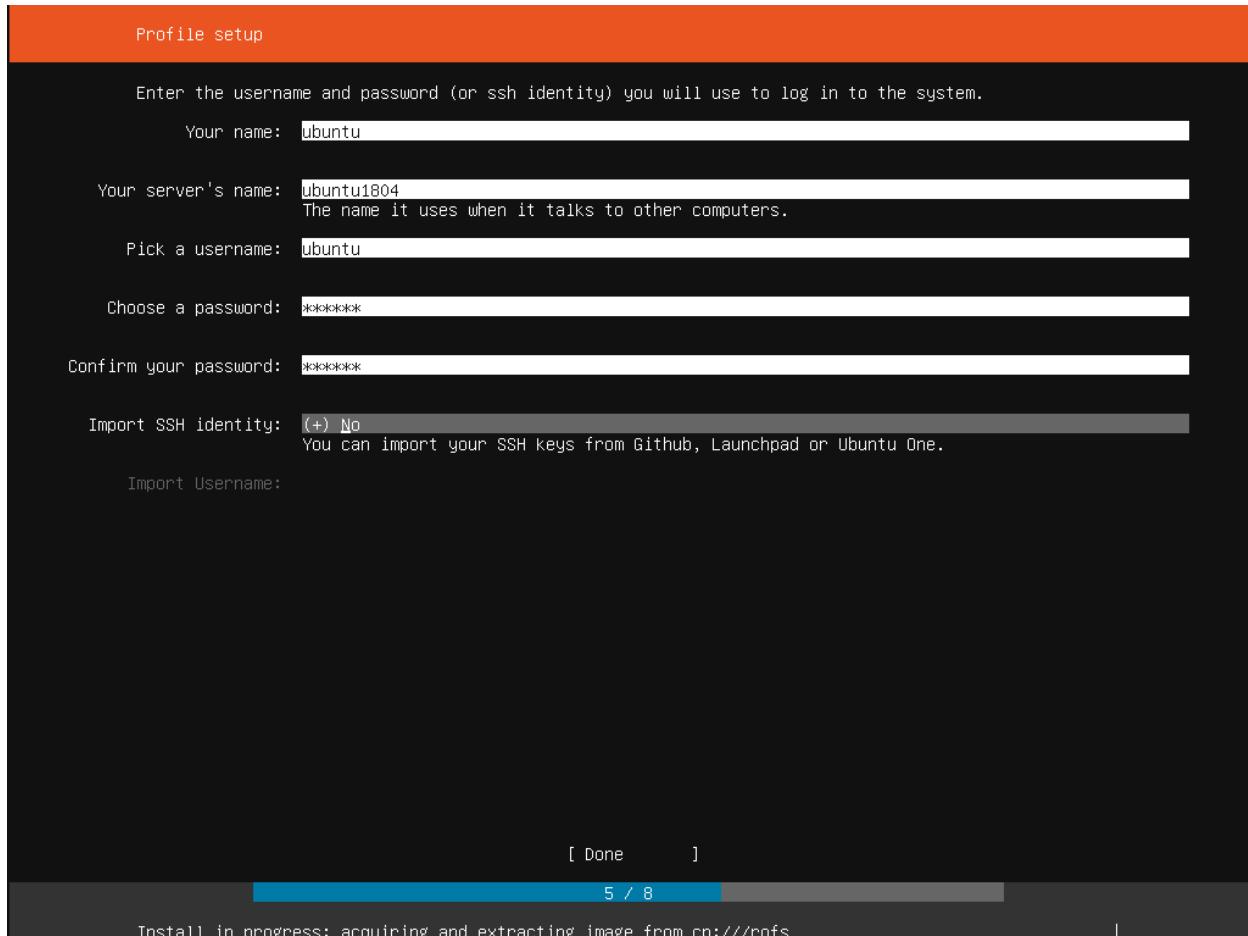
9. Confirm partitions



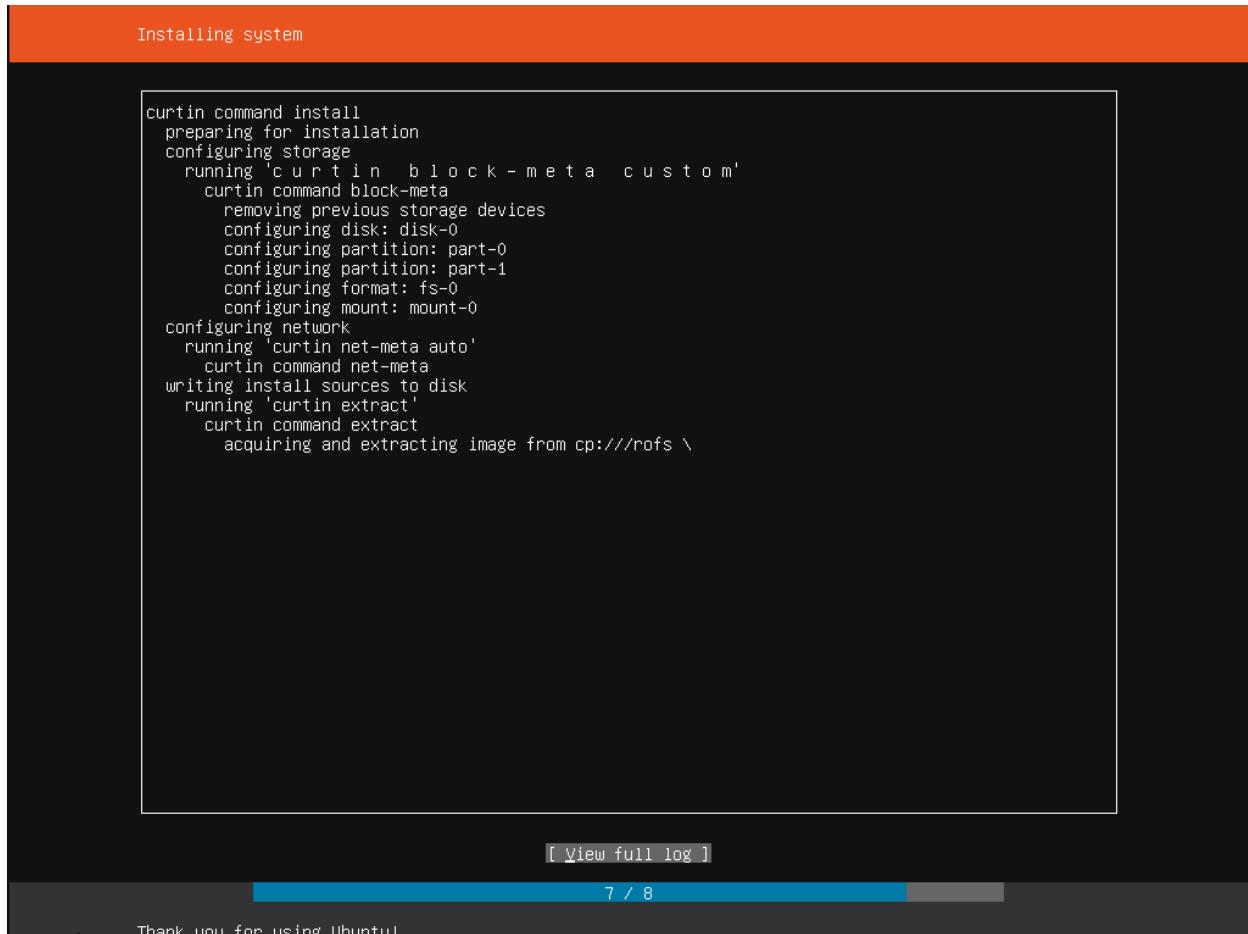
10. Confirm changes



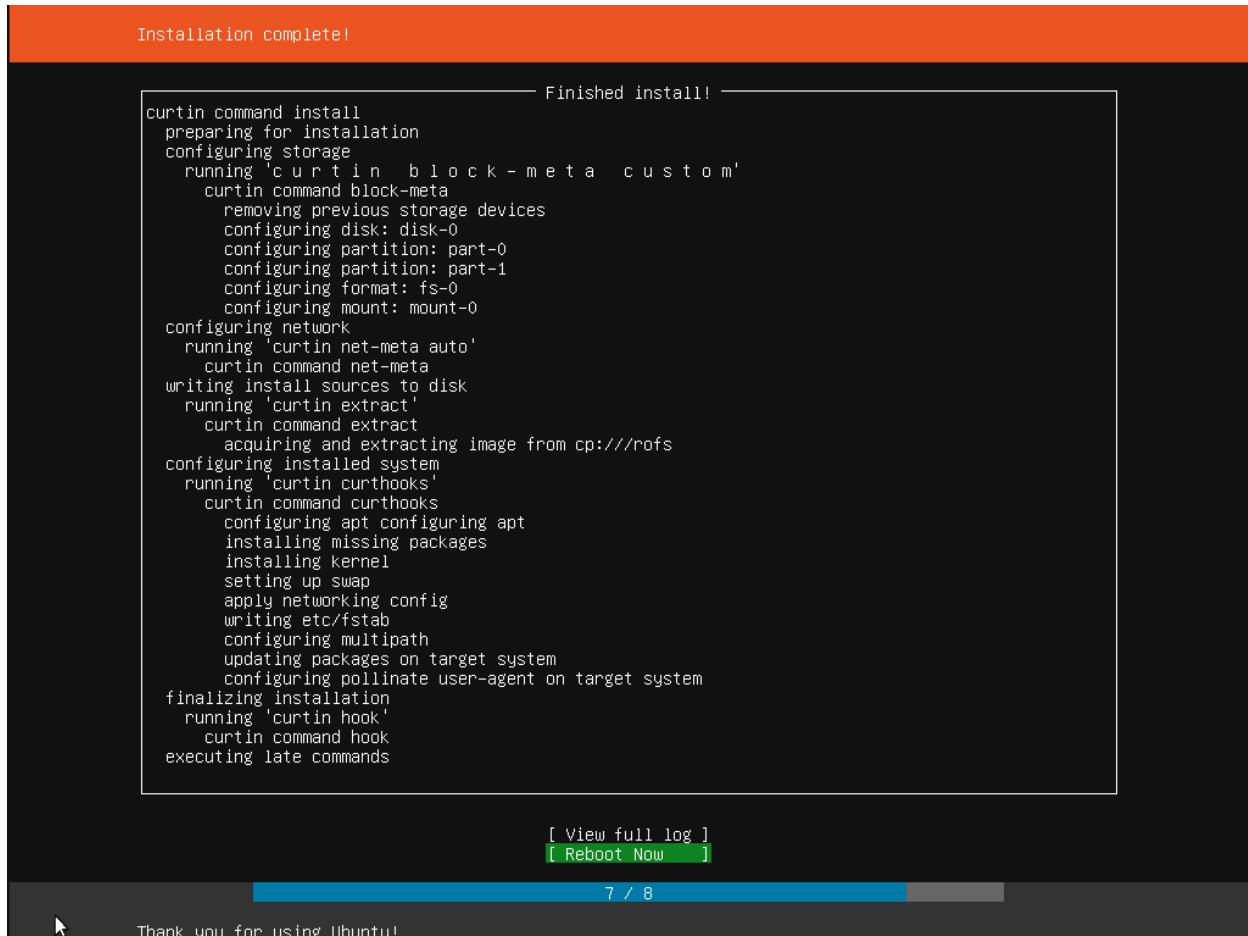
11. Set up a Profile



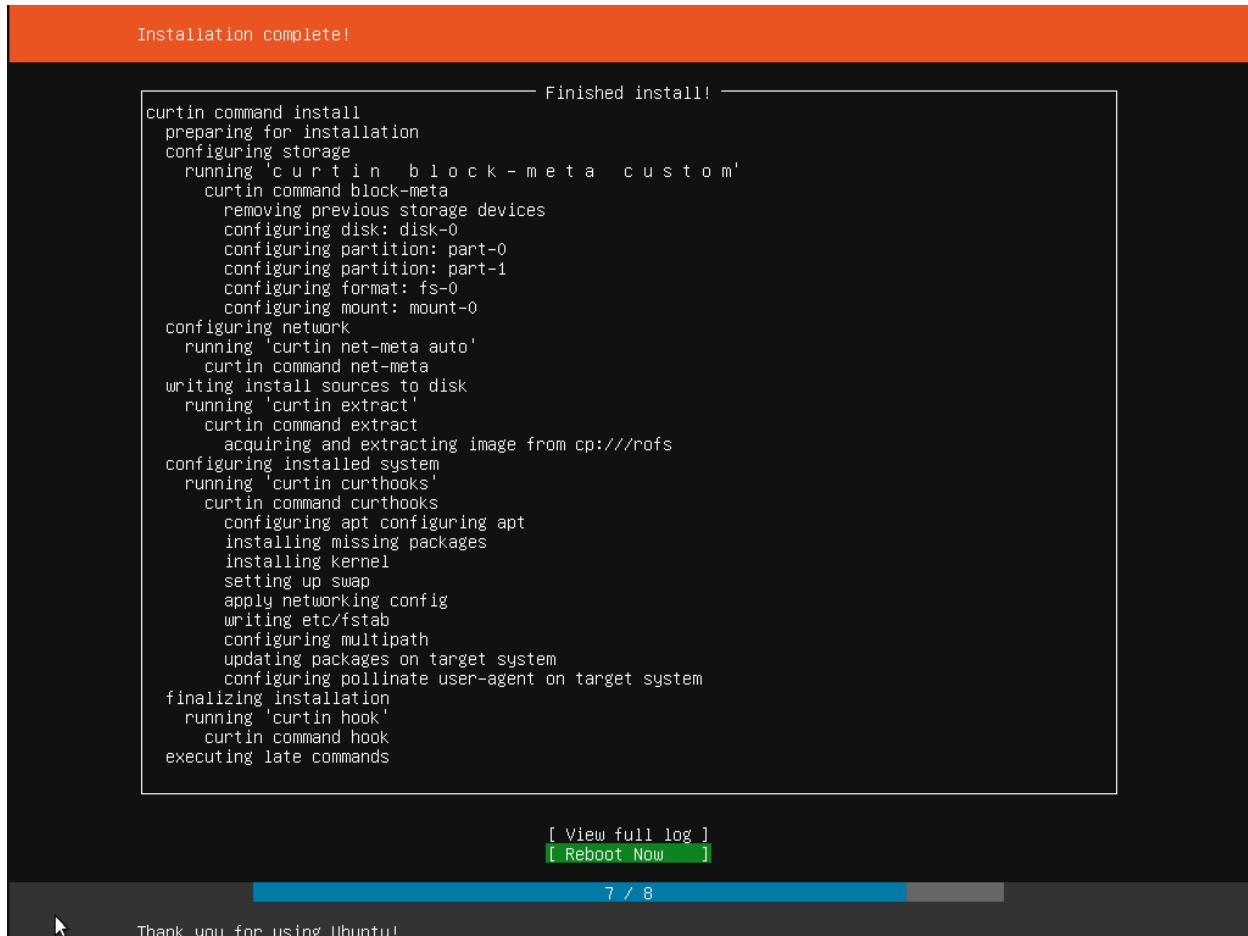
12. Install software



13. Installation complete



Output/Results snippet:



Installation complete!

```
----- Finished install! -----
curtin command install
preparing for installation
configuring storage
  running 'curtin in block-meta custom'
    curtin command block-meta
      removing previous storage devices
      configuring disk: disk-0
      configuring partition: part-0
      configuring partition: part-1
      configuring format: fs-0
      configuring mount: mount-0
configuring network
  running 'curtin net-meta auto'
    curtin command net-meta
writing install sources to disk
  running 'curtin extract'
    curtin command extract
      acquiring and extracting image from cp:///rofs
configuring installed system
  running 'curtin curthooks'
    curtin command curthooks
      configuring apt
      configuring apt
      installing missing packages
      installing kernel
      setting up swap
      apply networking config
      writing etc/fstab
      configuring multipath
      updating packages on target system
      configuring pollinate user-agent on target system
finalizing installation
  running 'curtin hook'
    curtin command hook
executing late commands

[ View full log ]
[ Reboot Now ]
```

7 / 8

Thank you for using Ubuntu!

References:

- <https://ubuntu.com/server/docs>

Activity 2

Aim: Create new user and group

Learning outcome: Able to understand users and groups

Duration: 2 hours

List of Hardware/Software requirements:

1. Ubuntu Server 19.0

Code/Program/Procedure (with comments):

Linux also provides the **useradd**, **usermod**, and **userdel** commands to manage user accounts.

Syntax -

useradd <i>username options</i>	//Adds a user
userdel <i>username</i>	//Deletes a user
usermod <i>username options</i>	//Modifies user properties
groupadd <i>groupname options</i>	//Adds a group
groupdel <i>groupname</i>	//Deletes a group
groupmod <i>groupname options</i>	//Modifies a group name

Adding a new user -

`useradd [options] username`

Examples -

Log in as root

Create a User

`# useradd edunet`

Create a User with Specific User ID

`useradd -u 999 edunet1`

Create a User with Specific Group ID

```
#useradd -u 1000 -g 500 training // adding training user need group ID 500
```

Add a User to Multiple Groups

```
#useradd -G admins,webadmin,developers backupoperator //groups mush present in system
```

Create a User with Account Expiry Date

```
# useradd -e 2020-04-30 sandip
```

Create a User with Password Expiry Date

```
# useradd -e 2020-04-30 -f 45 anip
```

Modifying User using Usermod

Syntax -

```
usermod [options] LOGIN
```

Change User Home Directory

```
# usermod -d /var/www/ tecmint
```

Set User Account Expiry Date

```
# usermod -e 2020-04-30 tecmint
```

```
# chage -l tecmint
```

Change User Primary Group

```
# usermod -g babin tecmint_test
```

```
# id tecmint_test
```

Adding Group to an Existing User

```
# usermod -G tecmint_test0 tecmint
```

```
# id tecmint
```

Change User Login Name

```
# usermod -l tecmint_admin tecmint
```

Deleting User using Userdel

Syntax –

```
#userdel username
```

```
# userdel -r tecmint
```

passwd and chpasswd

A quick way to change just the password for a user is the passwd command:

Syntax – Passwd username

```
# passwd test
```

Managing Groups Using groupadd, groupmod, and groupdel

Creating new groups

The groupadd command allows you to create new groups on your system:

Syntax

```
groupadd [options] group
```

Example –

```
#groupadd newgroup
```

Modifying groups

The groupmod command allows you to change the GID (using the -g parameter) or the group name (using the -n parameter) of an existing group:

Modify a user security group.

Syntax

```
groupmod [options] GROUP
```

Examples :

1. Change the group “newgroup” to “bettergroup”.

```
# groupmod -n bettergroup newgroup
```

2. Change groupid of a group

This command changes the groupid of abc group to 777

```
# groupmod -g 777 abc
```

3. When -o is used with -g option we can give non unique values

```
# groupmod -g 777 -o abc1
```

groupdel

Delete a user security group.

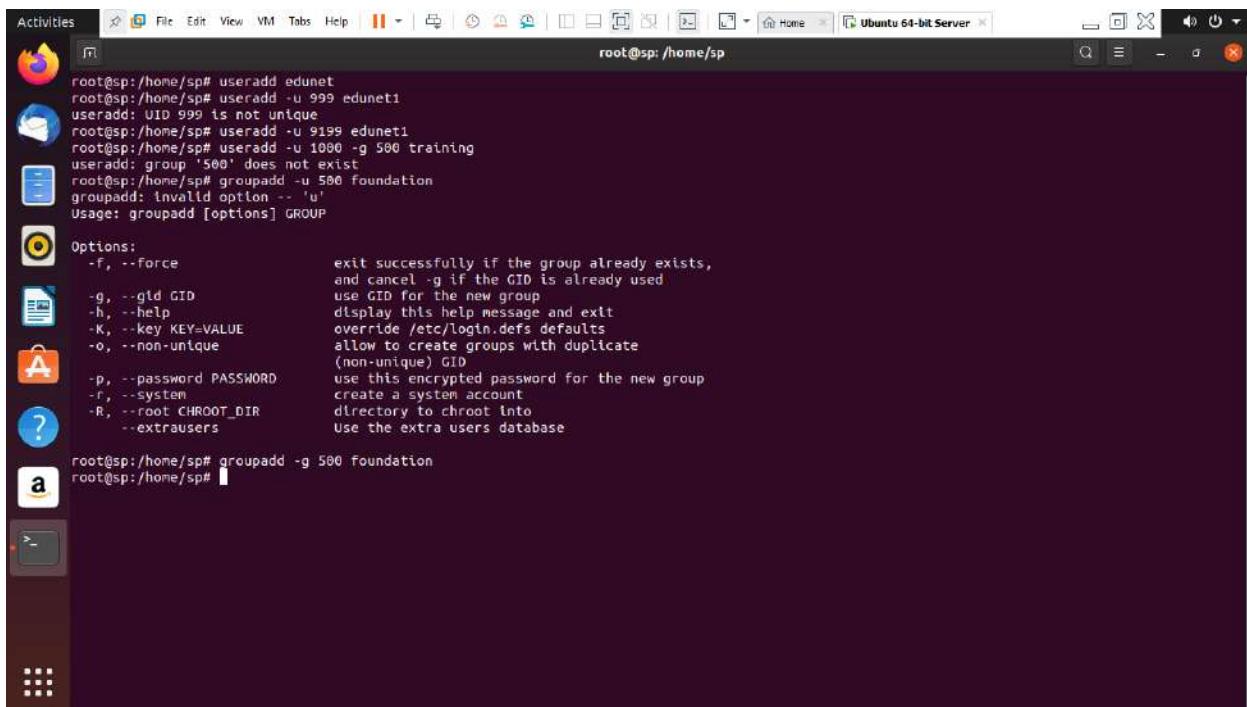
Syntax

groupdel *group*

Example –

```
#groupdel abc1
```

Output/Results snippet:



The screenshot shows a terminal window on an Ubuntu 64-bit Server. The terminal title is "root@sp:/home/sp#". The user has run several commands related to user and group management:

```
root@sp:/home/sp# useradd edunet
root@sp:/home/sp# useradd -u 999 edunet1
useradd: UID 999 is not unique
root@sp:/home/sp# useradd -u 9199 edunet1
root@sp:/home/sp# useradd -u 1090 -g 500 training
useradd: group '500' does not exist
root@sp:/home/sp# groupadd -u 500 foundation
groupadd: invalid option -- 'u'
Usage: groupadd [options] GROUP

Options:
  -f, --force          exit successfully if the group already exists,
                       and cancel -g if the GID is already used
  -g, --gid GID        use GID for the new group
  -h, --help            display this help message and exit
  -K, --key KEY=VALUE  override /etc/login.defs defaults
  -o, --non-unique      allow to create groups with duplicate
                       (non-unique) GID
  -p, --password PASSWORD
  -r, --system          create a system account
  -R, --root CHROOT_DIR
  --extrausers          Use the extra users database

root@sp:/home/sp# groupadd -g 500 foundation
root@sp:/home/sp#
```

References:

- http://manpages.ubuntu.com/manpages/xenial/man8/useradd.8.html?_ga=2.108577930.922876392.1588315806-228537118.1588315806

Activity 3

Aim: Create public and data directory.

Learning outcome: Able to understand directory and permission.

Duration: 2 hours

List of Hardware/Software requirements:

1. Ubuntu Server 19.0

Code/Program/Procedure (with comments):

Login to super user mode or use sudo command

```
sudo mkdir reports //Create Directory reports  
sudo groupadd project //Create Group project  
sudo usermod -a -G project edunet //modify existing user edunet with group project
```

The flags and arguments used in the above command are:

-a – which adds the user to the supplementary group.

-G – specifies the group name.

project – group name.

edunet – existing username.

Changing permissions

The chmod command allows you to change the security settings for files and directories. The format of the chmod command is:

Syntax

chmod options mode file

Reference	Class	Description
u	owner	file's owner
g	group	users who are members of the file's group
o	others	users who are neither the file's owner nor members of the file's group
a	all	All three of the above, same as ugo
r		Permission to read the file.
w		Permission to write (or delete) the file.
x		Permission to execute the file, or, in

Example

```
sudo chgrp -R project reports
```

```
sudo chmod -R 2775 reports
```

Explaining the permissions 2775 in the chmod command above:

2 – turns on the setGID bit, implying–newly created subfiles inherit the same group as the directory, and newly created subdirectories inherit the set GID bit of the parent directory.

7 – gives rwx permissions for owner.

7 – gives rwx permissions for group.

5 – gives rx permissions for others.

You can create more system users and add them to the directory group as follows:

```
sudo useradd -m -c "Satish Pise" -s/bin/bash -G project satishpise
```

```
sudo useradd -m -c "Anip Sharma" -s/bin/bash -G project anipsharma
```

```
sudo useradd -m -c "Surandar Sharma" -s/bin/bash -G project surandar
```

Then create subdirectories where the new users above will store their project reports:

```
sudo mkdir reports/satishpise
```

```
sudo mkdir reports/anipsharma
```

```
sudo mkdir reports/surandar
```

Output/Results snippet:

Ubuntu 64-bit Server - VMware Workstation

File Edit View VM Tabs Help

Library Type here to search

Activities Terminal May 1 07:49

root@sp:/home/sp# sudo mkdir reports
root@sp:/home/sp# sudo groupadd project
root@sp:/home/sp# sudo usermod -a -G project edunet
root@sp:/home/sp# sudo chgrp -R project reports
root@sp:/home/sp# sudo chmod -R 2775 reports
root@sp:/home/sp# sudo useradd -m -c "Satisf Pise" -s/bin/bash _G project antip
Usage: useradd [options] LOGIN
 useradd -D
 useradd -D [options]

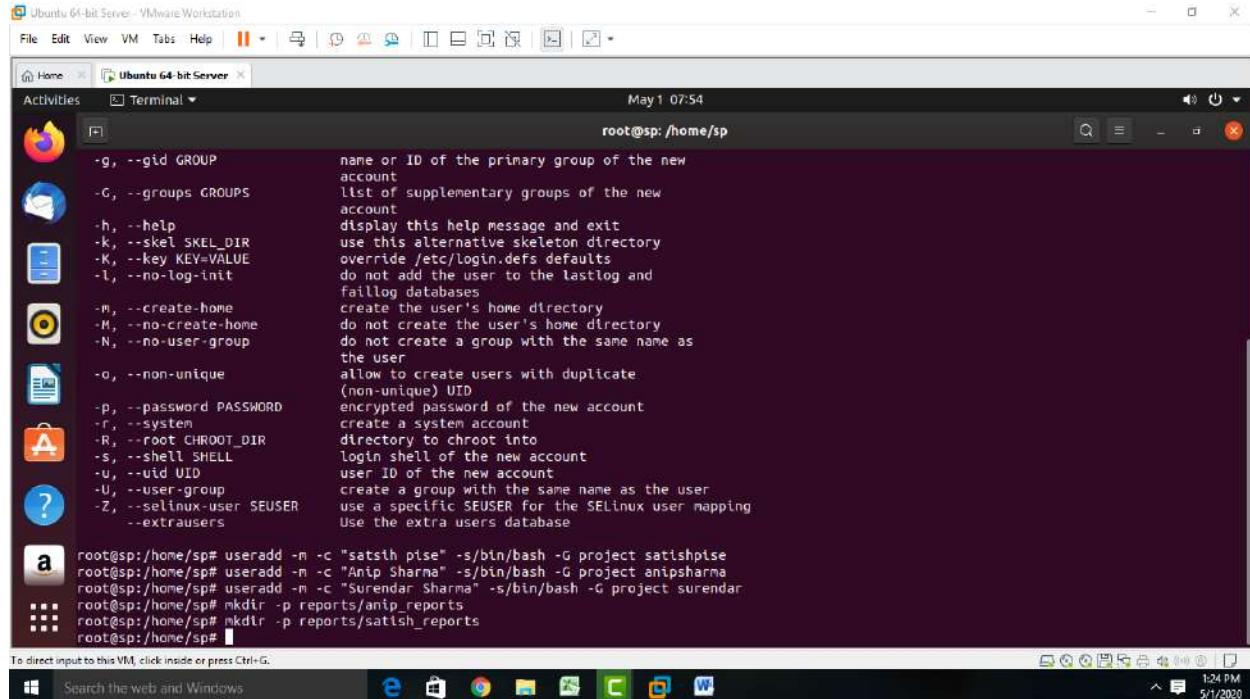
Options:

- b, --base-dir BASE_DIR base directory for the home directory of the new account
- c, --comment COMMENT GECOS field of the new account
- d, --home-dir HOME_DIR home directory of the new account
- D, --defaults print or change default useradd configuration
- e, --expiredate EXPIRE_DATE expiration date of the new account
- f, --inactive INACTIVE password inactivity period of the new account
- g, --gid GROUP name or ID of the primary group of the new account
- G, --groups GROUPS list of supplementary groups of the new account
- h, --help display this help message and exit
- k, --skel SKEL_DIR use this alternative skeleton directory
- K, --key KEY:VALUE override /etc/login.defs defaults
- l, --no-log-init do not add the user to the lastlog and failing databases
- m, --create-home create the user's home directory
- M, --no-create-home do not create the user's home directory
- N, --no-user-group do not create a group with the same name as

To direct input to this VM, click inside or press Ctrl+G.

Search the web and Windows

1:19 PM 5/1/2023



The screenshot shows a Linux terminal window titled "Ubuntu 64-bit Server - VMware Workstation". The terminal is running as root, indicated by the prompt "root@sp:/home/sp#". The user is executing the "useradd" command with various options to create new user accounts. The output of the command is displayed, listing the usage information for "useradd" and the creation of three new users: "satishpise", "anipsharma", and "surendar". The terminal window is part of a desktop environment with icons for various applications like a browser, file manager, and system tools.

```
-g, --gid GROUP          name or ID of the primary group of the new account
-G, --groups GROUPS      list of supplementary groups of the new account
-h, --help                display this help message and exit
-k, --skel SKEL_DIR       use this alternative skeleton directory
-K, --key KEY=VALUE       override /etc/login.defs defaults
-l, --no-log-init         do not add the user to the lastlog and faillog databases
-m, --create-home         create the user's home directory
-M, --no-create-home      do not create the user's home directory
-N, --no-user-group       do not create a group with the same name as the user
-o, --non-unique          allow to create users with duplicate (non-unique) UID
-p, --password PASSWORD   encrypted password of the new account
-r, --system               create a system account
-R, --root CHROOT_DIR     directory to chroot into
-s, --shell SHELL          login shell of the new account
-u, --uid UID              user ID of the new account
-U, --user-group           create a group with the same name as the user
-Z, --selinux-user SEUSER  use a specific SEUSER for the SELinux user mapping
--extrausers               Use the extra users database

root@sp:/home/sp# useradd -m -c "satish pise" -s/bin/bash -G project satishpise
root@sp:/home/sp# useradd -n -c "Anip Sharma" -s/bin/bash -G project anipsharma
root@sp:/home/sp# useradd -n -c "Surendar Sharma" -s/bin/bash -G project surendar
root@sp:/home/sp# mkdir -p reports/anip_reports
root@sp:/home/sp# mkdir -p reports/surendar_reports
root@sp:/home/sp#
```

References:

- <https://www.geeksforgeeks.org/chmod-command-linux/>

Activity 4

Aim: Create an lmhosts file.

Learning outcome: Able to create lmhosts.

Duration: 3 hours

List of Hardware/Software requirements:

1. Ubuntu Server 19.0

Code/Program/Procedure (with comments):

Installing Samba

```
sudo apt update
```

```
sudo apt install samba
```

We can check if the installation was successful by running:

```
whereis samba
```

Configure your /etc/lmhosts file. The lmhosts file is the Samba Net BIOS name to IP address mapping file. It is very similar to the /etc/hosts file format, except that the hostname component must correspond to the Net BIOS naming format.

Create the lmhosts file, **touch /etc/lmhosts** and add your client hosts:

```
# Sample Samba lmhosts file.
```

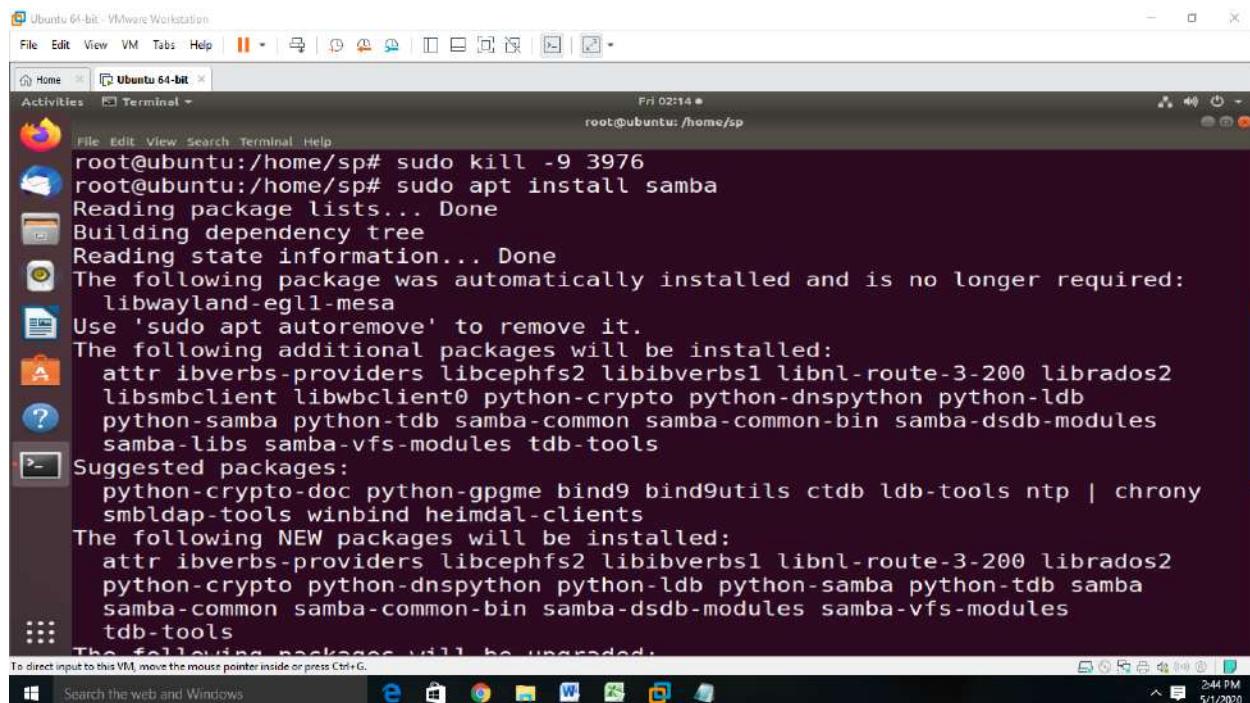
```
#
```

```
127.0.0.1      localhost
```

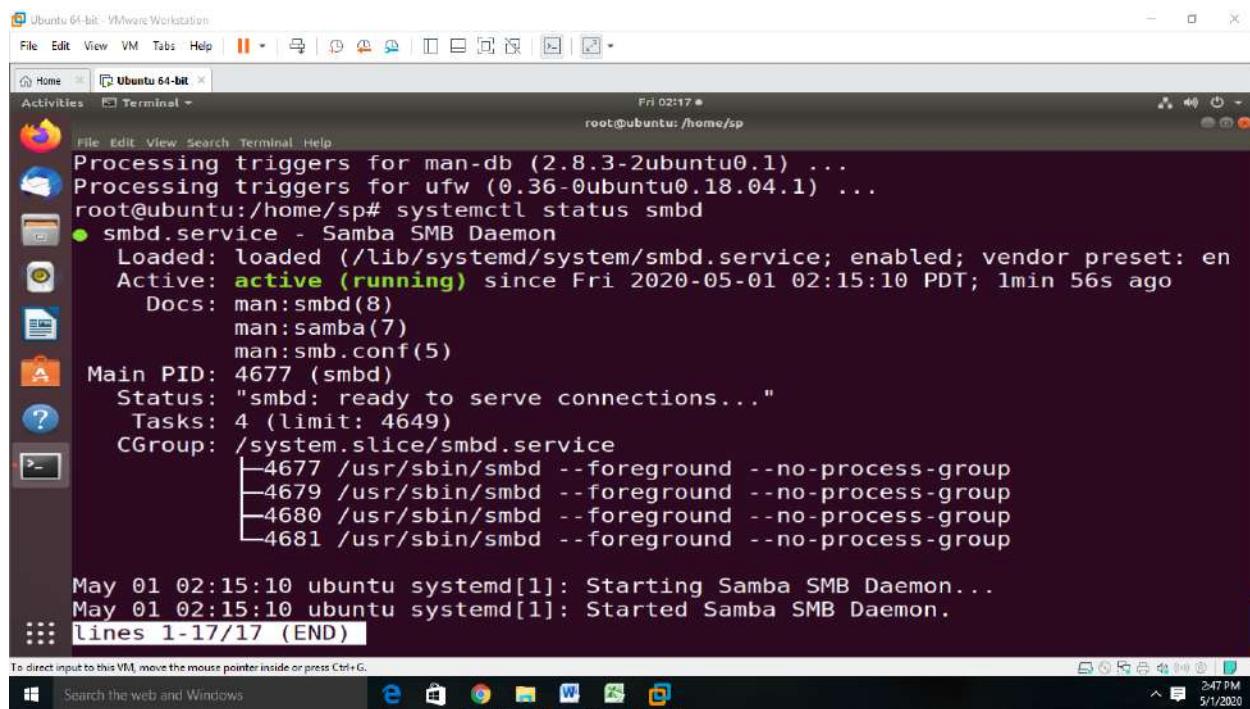
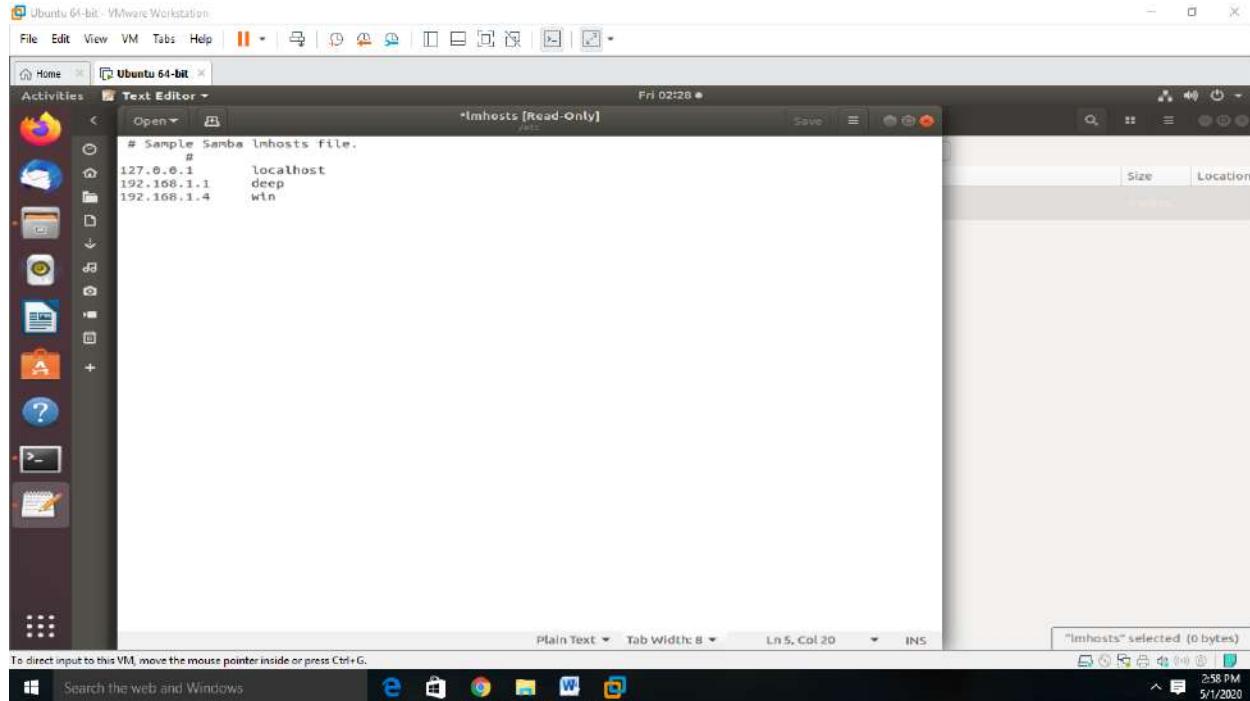
192.168.1.1 deep
192.168.1.4 win

In our example, this file contains three IP to Net BIOS name mappings. The localhost, 127.0.0.1, client named deep, 192.168.1.1 and client named win, 192.168.1.4.

Output/Results snippet:



```
root@ubuntu:/home/sp# sudo kill -9 3976
root@ubuntu:/home/sp# sudo apt install samba
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libwayland-egl1-mesa
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  attr ibverbs-providers libcephfs2 libibverbs1 libnl-route-3-200 librados2
  libsmbclient libwbclient0 python-crypto python-dnspython python-ldb
  python-samba python-tdb samba-common samba-common-bin samba-dsdb-modules
  samba-libs samba-vfs-modules tdb-tools
Suggested packages:
  python-crypto-doc python-gpgme bind9 bind9utils ctdb ldb-tools ntp | chrony
  smbldap-tools winbind heimdal-clients
The following NEW packages will be installed:
  attr ibverbs-providers libcephfs2 libibverbs1 libnl-route-3-200 librados2
  python-crypto python-dnspython python-ldb python-samba python-tdb samba
  samba-common samba-common-bin samba-dsdb-modules samba-vfs-modules
  tdb-tools
The following packages will be upgraded:
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Windows Search the web and Windows 2:44 PM 5/1/2020
```



Activity 5

Aim: Check host file

Learning outcome: Understand host file configuration

Duration: 2 hours

List of Hardware/Software requirements:

1. Ubuntu Server 19.0

Code/Program/Procedure (with comments):

File entry format

IPAddress DomainName [DomainAliases]

Example

192.168.1.10 foo.mydomain.org

Open File /etc/hosts

Sudo nano /etc/hosts

Adding entries

Change permission

Sudo u+x /etc/hosts

u – user

x – execute permission

Add entries

127.0.0.1 localhost

192.168.1.10 foo.mydomain.org foo

192.168.1.13 bar.mydomain.org

146.82.138.7 master.debian.org

Hosts.deny file

/etc/hosts.deny: list of hosts that are not allowed to access the system.

Hosts.allow file

/etc/hosts.allow: list of hosts that are allowed to access the system.

See the manual pages hosts_access(5) and hosts_options(5).

Example: ALL: LOCAL @some_netgroup

ALL: .foobar.edu EXCEPT terminalserver.foobar.edu

Output/Results snippet:

The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "hosts" and it displays the contents of the hosts file. The file contains the following entries:

```
127.0.0.1 localhost
127.0.1.1 ubuntu

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

The terminal window is running the "GNU nano 2.9.3" editor. At the bottom of the window, there are several keyboard shortcut keys listed: ^G Get Help, ^O Write Out, ^R Read File, [Read 9 lines], ^W Where Is, ^\ Replace, ^K Cut Text, ^U Uncut Text, ^J Justify, ^T To Spell, and ^X Exit. The status bar at the bottom of the screen shows the date and time as "Fri 02:35" and the IP address "root@ubuntu:/etc".

References:

- <http://manpages.ubuntu.com/manpages/trusty/man5/hosts.5.html#example>

Activity 6

Aim: Filter ports

Learning outcome: Able to apply filter in ports

Duration: 3 hours

List of Hardware/Software requirements:

1. Ubuntu Server 19.0

Code/Program/Procedure (with comments):

Install net-tool

Sudo apt-get install net-tools

sudo netstat -tunlp

The options used in this command have the following meaning:

- t - Show TCP ports.
- u - Show UDP ports.
- n - Show numerical addresses instead of resolving hosts.
- l - Show only listening ports.
- p - Show the PID and name of the listener's process. This information is shown only if you run the command as root or sudo user.

sudo lsof -nP -iTCP -sTCP:LISTEN

The options used are as follows:

- n - Do not convert port numbers to port names.

-p - Do not resolve hostnames, show numerical addresses.

-iTCP -sTCP:LISTEN - Show only network files with TCP state LISTEN.

To find what process is listening on a particular port, for example, port 3306 you would use:

```
sudo lsof -nP -iTCP:3306 -sTCP:LISTEN
```

Listing all the LISTENING Ports of TCP and UDP connections

```
netstat -a | more
```

Listing TCP Ports connections

```
netstat -at
```

Listing UDP Ports connections

```
netstat -au
```

Listing all LISTENING Connections

```
netstat -l
```

Listing all UNIX Listening Ports

```
netstat -lx
```

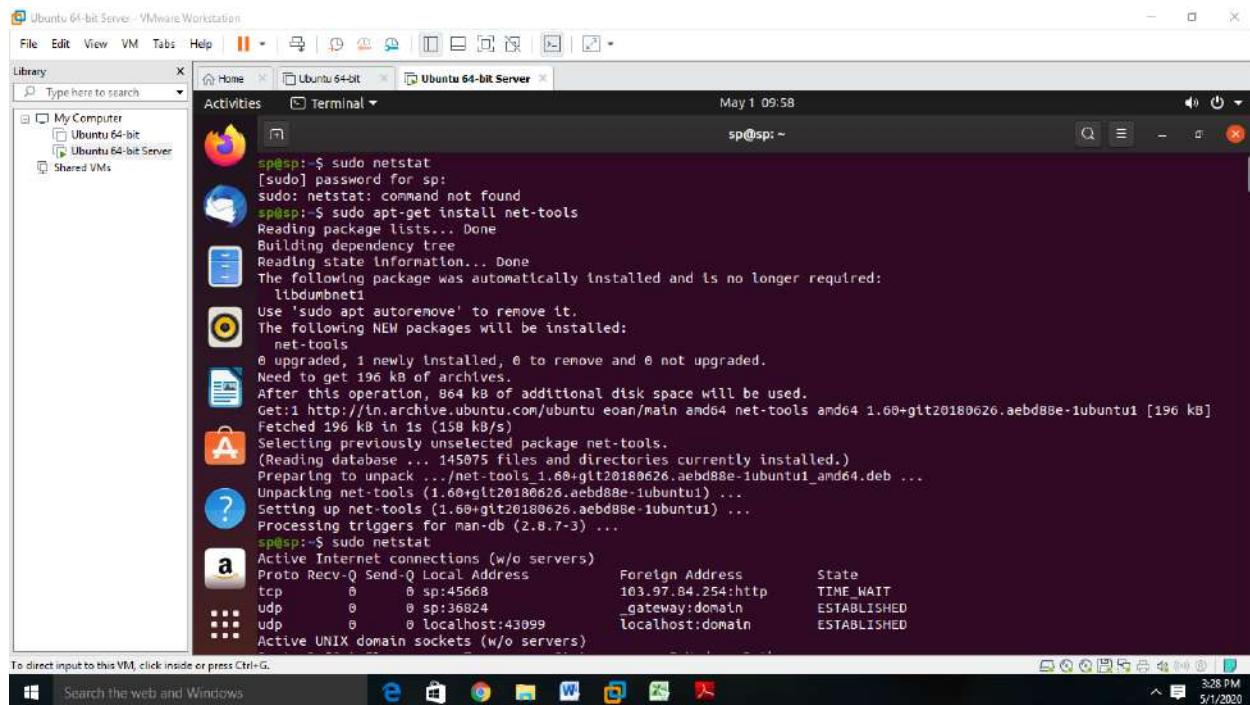
Showing Statistics by Protocol

```
netstat -s
```

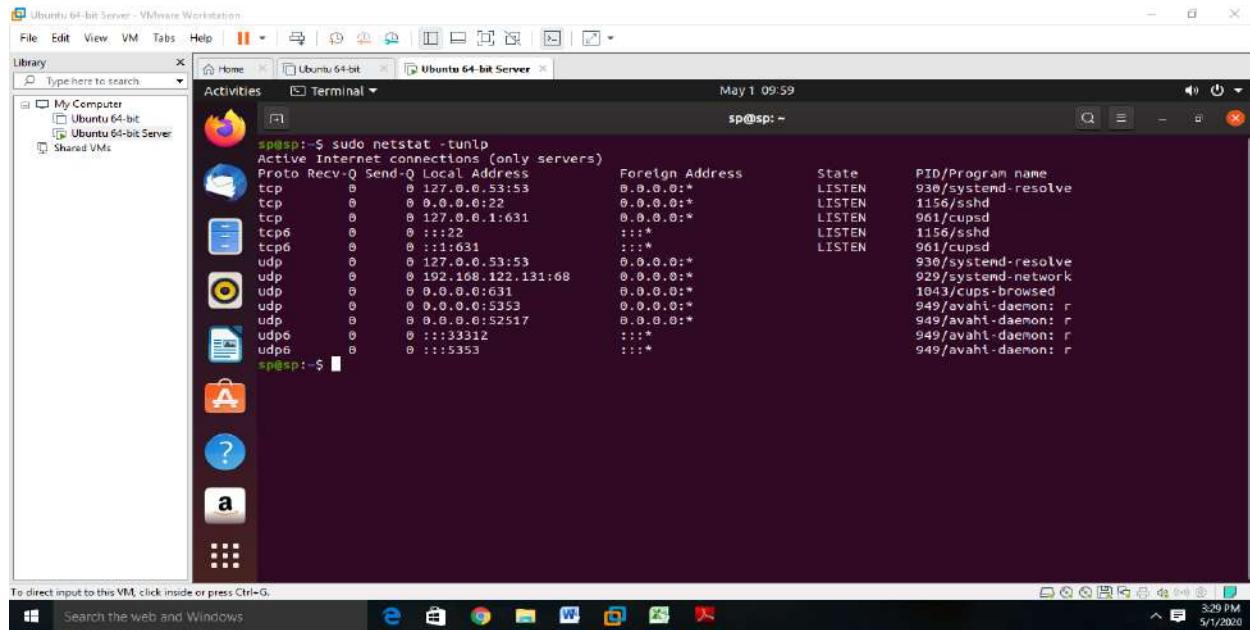
Showing Statistics by TCP Protocol

```
netstat -st
```

Output/Results snippet:



```
sp@sp:~$ sudo netstat
[sudo] password for sp:
sudo: netstat: command not found
sp@sp:~$ sudo apt-get install net-tools
Reading package lists... Done
Building dependency tree...
Reading state information... Done
The following package was automatically installed and is no longer required:
  libdumbnet1
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  net-tools
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 196 kB of archives.
After this operation, 864 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu eoan/main amd64 net-tools amd64 1.60+git20180626.aebdb88e-1ubuntu1 [196 kB]
Fetched 196 kB in 1s (158 kB/s)
Selecting previously unselected package net-tools.
(Reading database ... 145075 files and directories currently installed.)
Preparing to unpack .../net-tools_1.60+git20180626.aebdb88e-1ubuntu1_amd64.deb ...
Unpacking net-tools (1.60+git20180626.aebdb88e-1ubuntu1) ...
Setting up net-tools (1.60+git20180626.aebdb88e-1ubuntu1) ...
Processing triggers for man-db (2.8.7-3) ...
sp@sp:~$ sudo netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp     0      0  sp:45668                103.97.84.254:http    TIME_WAIT
      0      0  sp:36824                _gateway:domain      ESTABLISHED
      0      0  localhost:43099             localhost:domain    ESTABLISHED
Active UNIX domain sockets (w/o servers)
```



References:

- <https://www.tecmint.com/20-netstat-commands-for-linux-network-management/>
- <https://ubuntu.com/server/docs/security-firewall>

Activity 7

Aim: Secure and install SWAT server.

Learning outcome: Able to install samba server and run application.

Duration: 5 hours

List of Hardware/Software requirements:

1. Ubuntu Server 19.0

Code/Program/Procedure (with comments):

Overview

A Samba file server enables file sharing across different operating systems over a network. It lets you access your desktop files from a laptop and share files with Windows and macOS users.

This guide covers the installation and configuration of Samba on Ubuntu.

What you'll learn

How to set up a Samba file server

How to share files across a local network

What you'll need

Ubuntu 18.04 LTS

A Local Area Network (LAN) to share files over

Installing Samba

To install Samba, we run:

sudo apt update

sudo apt install samba

We can check if the installation was successful by running:

whereis samba

The following should be its output:

```
samba: /usr/sbin/samba /usr/lib/samba /etc/samba /usr/share/samba  
/usr/share/man/man7/samba.7.gz /usr/share/man/man8/samba.8.gz
```

Setting up Samba

Now that Samba is installed, we need to create a directory for it to share:

mkdir /home/sp/sambashare/

The command above creates a new folder sambashare in our home directory which we will share later.

The configuration file for Samba is located at /etc/samba/smb.conf. To add the new directory as a share, we edit the file by running:

sudo nano /etc/samba/smb.conf

At the bottom of the file, add the following lines:

[sambashare]

comment = Samba on Ubuntu

path = /home/sp/sambashare

read only = no

browsable = yes

Then press Ctrl-O to save and Ctrl-X to exit from the nano text editor.

What we've just added

comment: A brief description of the share.

path: The directory of our share.

read only: Permission to modify the contents of the share folder is only granted when the value of this directive is no.

browsable: When set to yes, file managers such as Ubuntu's default file manager will list this share under "Network" (it could also appear as browseable).

Now that we have our new share configured, save it and restart Samba for it to take effect:

sudo service smbd restart

Update the firewall rules to allow Samba traffic:

sudo ufw allow samba

Setting up User Accounts and Connecting to Share

Since Samba doesn't use the system account password, we need to set up a Samba password for our user account:

sudo smbpasswd -a username

Note

Username used must belong to a system account, else it won't save.

Connecting to Share

On Ubuntu: Open up the default file manager and click Connect to Server then enter:

On Ubuntu: Open up the default file manager and click Connect to Server then enter:

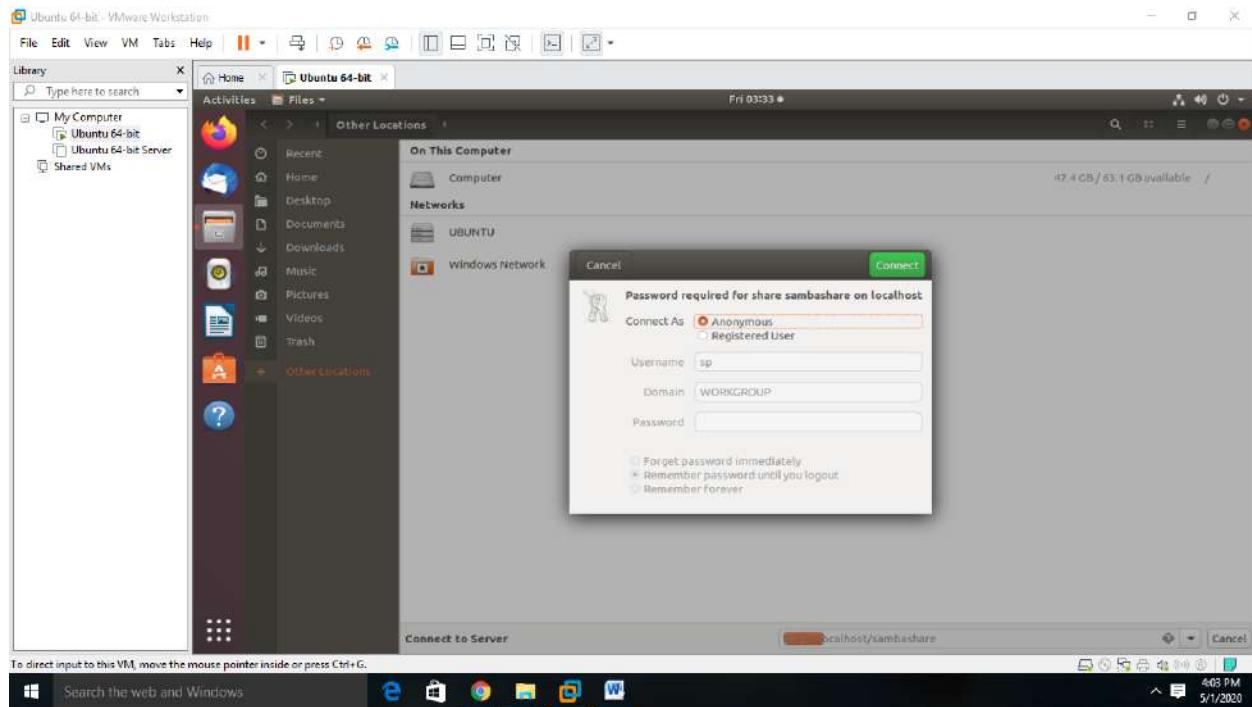
Open other location

Pass server address

Smb://localhost/sambashare

And click on connect

Output/Results snippet:



References:

- <https://ubuntu.com/tutorials/install-and-configure-samba>

Activity 8

Aim: Install and configure Telnet

Learning outcome: Able to install and configure telnet server.

Duration: 5 hours

List of Hardware/Software requirements:

1. Ubuntu Server 19.0

Code/Program/Procedure (with comments):

Server Configuration

//Install telnet server files

Step 1. sudo apt-get install xinetd

Step 2. sudo apt-get install telnetd

//Configure file /etc/inetd.conf

Step 3. sudo nano /etc/inetd.conf

telnet stream tcp nowait telnetd /usr/sbin/tcpd /usr/sbin/in.telnetd

//Configure file /etc/xinetd.conf

Step 4. sudo nano /etc/xinetd.conf

Simple configuration file for xinetd

#

Some defaults, and include /etc/xinetd.d/

```
defaults
```

```
{
```

```
# Please note that you need a log_type line to be able to use log_on_success
```

```
# and log_on_failure. The default is the following :
```

```
# log_type = SYSLOG daemon info
```

```
instances = 60
```

```
log_type = SYSLOG authpriv
```

```
log_on_success = HOST PID
```

```
log_on_failure = HOST
```

```
cps = 25 30
```

```
}
```

//Configure file /etc/xinetd.d/telnet

```
Step 5. sudo nano /etc/xinetd.d/telnet
```

```
# default: on
```

```
# description: The telnet server serves telnet sessions; it uses
```

```
# unencrypted username/password pairs for authentication.
```

```
service telnet
```

```
{
```

```
    disable = no
```

```
    flags = REUSE
```

```
    socket_type = stream
```

```
    wait = no
```

```
user = root  
  
server = /usr/sbin/in.telnetd  
  
log_on_failure += USERID  
  
}  
  
6. sudo /etc/init.d/xinetd restart  
  
7. sudo apt install net-tools  
  
8. sudo ifconfig
```

See your ip address

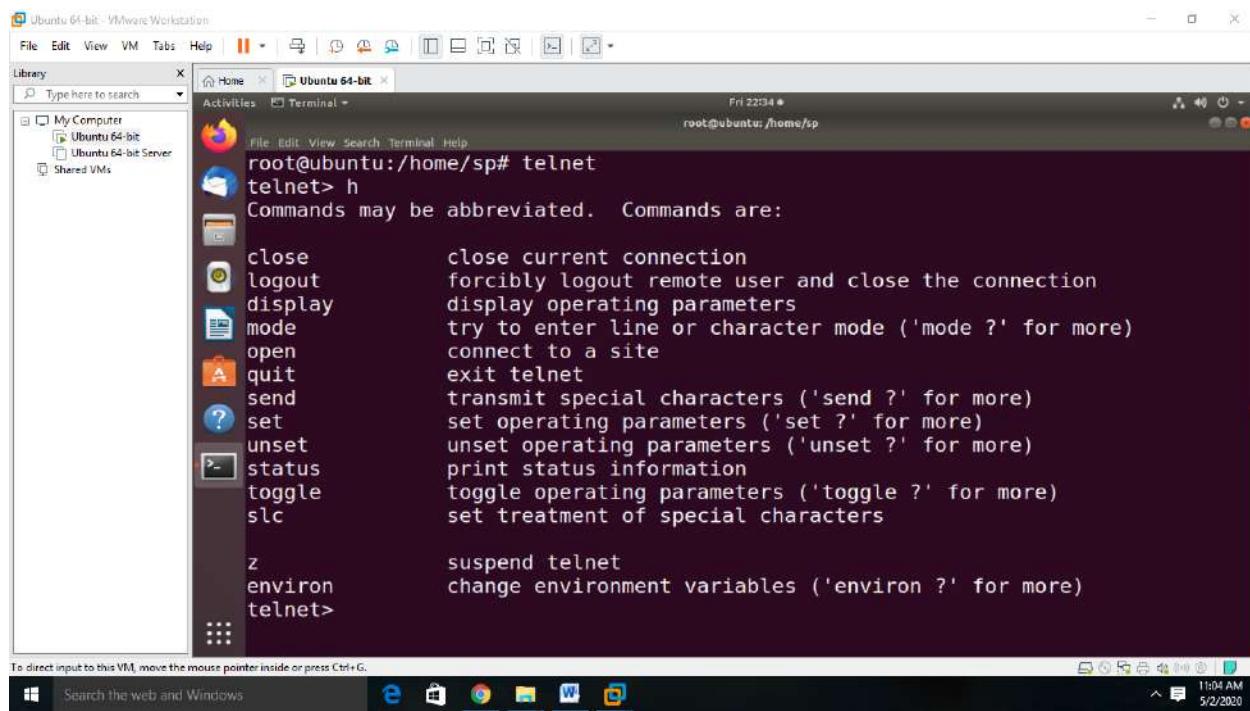
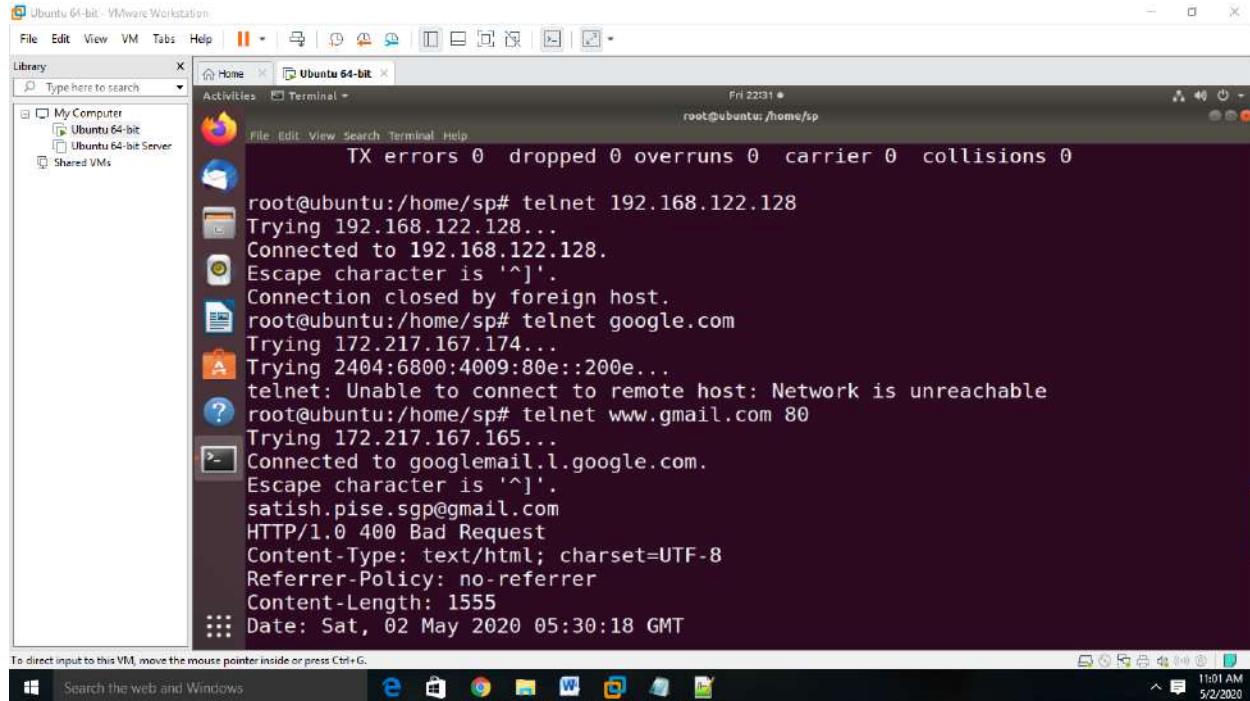
Client Configuration

Open terminal and type telnet server ip address

telnet 192.168.0.1

type your username and password

Output/Results snippet:



References:

<http://manpages.ubuntu.com/manpages/xenial/man1/telnet-ssl.1.html>

Learning Outcome 5 - Able to install & configure the different types of network devices in a network

After achieving this learning outcome, a student will be able to install & configure the different types of network devices in a network. In order to achieve this learning outcome, a student has to complete the following:

1. Configure & Implement Unmanageable Network Switch (3Hrs)
2. Configure & Implement Manageable Network Switch (2Hrs)
3. Install and configure router, bridges and HUB (3Hrs)
4. Configure Wireless Access Point (2Hrs)
5. Install and Configure Wire Network (2Hrs)
6. Install and Configure Wireless Network (2Hrs)
7. Install of AD-hoc Wireless Network (1Hr)
8. Configure Gateway Service for Internet Connectivity (3 Hrs)
9. Configure ADSL+2 Router for ISP Internet Connectivity (2Hrs)
10. Troubleshoot Internet Connectivity (5Hrs)

Activity 1

Aim: Configure & Implement Unmanageable Network Switch.

Learning outcome: Able to install & configure the different types of network devices in a network.

Duration: 3 hours

List of Hardware/Software requirements:

1. Unmanaged network switch
2. Ethernet cables with connectors
3. Computers/Digital Devices with pre-installed operating system (Windows, Linux, etc)

Code/Program/Procedure (with comments):



Figure 1: Configure & Implement Unmanageable Network Switch

- It allows for networking of Ethernet devices for data communication.

- The dedicated path between the sender and the receiver for the exchange of data at full speed.
- Forward broadcasts.
- No user configuration.
- Compatible with other switches.

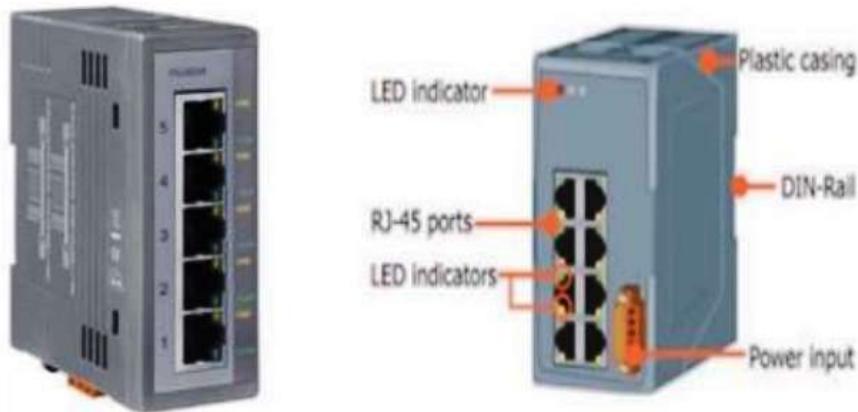


Figure 2: Ethernet Devices for data communication

- Five Ethernet ports 10/100 Base-TX.
- Din rail mountable.
- Automatic MDI//MDI-X crossover for plug-and-play.
- Supports=10~+30 VDC voltage input reverse polarity protection.
- Supports operating temperatures from -40~+75*C (-40F~ 167F).
- Full-duplex IEEE 802.3x and half-duplex backpressure movement control.
- Each port reinforcement 10/100mbps speed auto negotiation store-and-forward architecture.

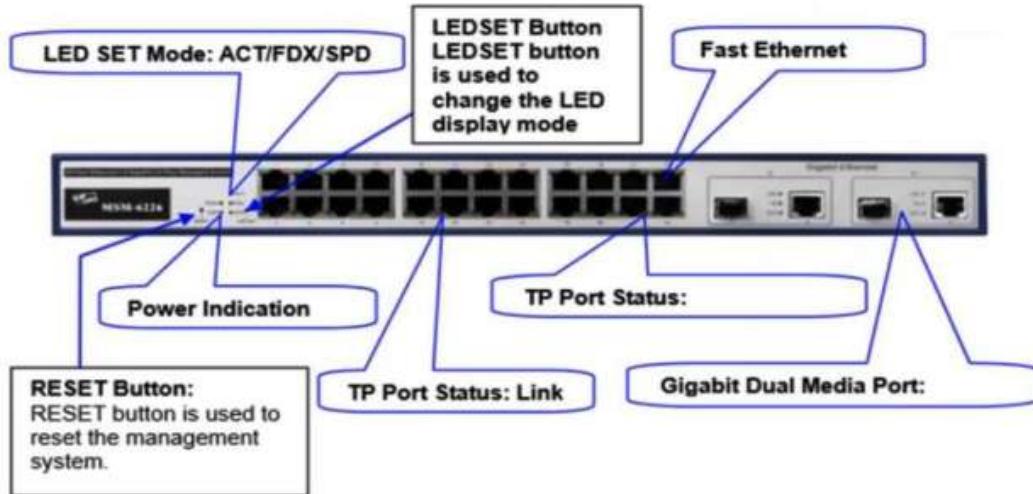


Figure 3: Ethernet ports

References:

<https://ipc2u.com/articles/knowledge-base/what-is-the-difference-between-managed-and-unmanaged-switch/>

Activity 2

Aim: Configure & Implement Manageable Network Switch.

Learning outcome: Able to install & configure the different types of network devices in a network.

Duration: 2 hours

List of Hardware/Software requirements:

1. Managed network switch
2. Ethernet cables with connectors
3. Computers/Digital Devices with pre-installed operating system (Windows, Linux, etc)

Code/Program/Procedure (with comments):

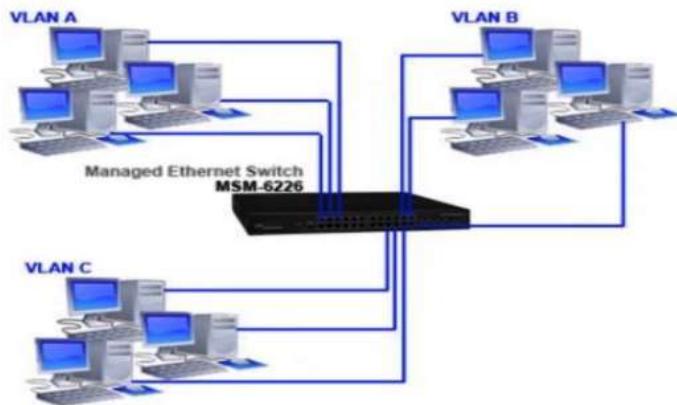


Figure 9: Configure & Implement Manageable Network Switch



Figure 10: Manageable Network Switch

- IEEE 802.3ab 10000BASE-T Gigabit Ethernet.
- L2+features provide good manageability, security, QoS, and performance.
- Network redundant ring failover protection.
- Multicasting support IGMP v1/v2/v3, proxy and snooping.
- Multicast/flooding/broadcast storm control.



Figure 11: Ethernet ports

- Two dual-media for flexible fiber connection.
- Port mirroring helps supervisor monitoring network.
- IEEE802.1Q tag base VLAN for performance and security and 4094 VLAN entries.
- IEEE802.1X access control improves network security.
- IEEE802.1D compatible, IEEE802.1w rapid spanning tree and IEEE802.1s multiple spanning tree.

- Unknown unicast/broadcast/multicast storm control.
- Multicast VLAN management for IPTV.
- IP-MAC port binding for LAN security.
- QCL based on application traffic for QoS and speed limitation management.
- Support IGMPv3 snooping and IGMP proxy.
- Support DHCP snooping.

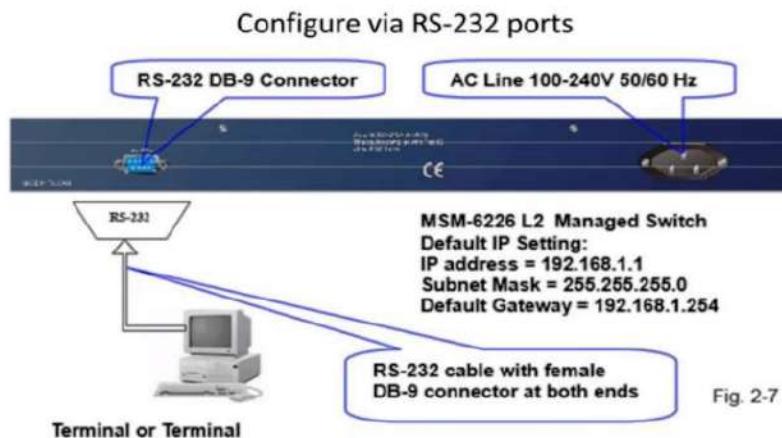
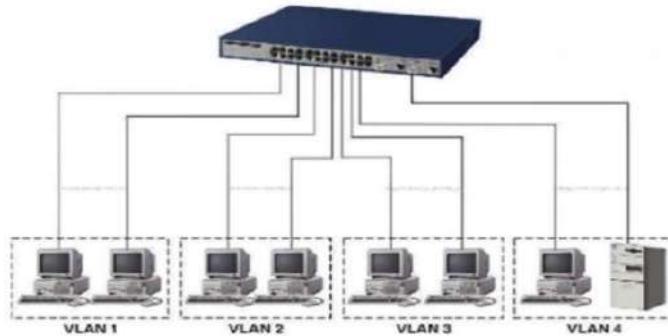


Figure 12: RS-232 Ports

Port-Based VLAN Configuration

**Procedure:**

Step 1: Connect the computer to the unmanaged switch (e.g. Dlink DGS 1210) with ethernet cable connected to any port of the switch.

Step 2: Set the IP address of the computer with a static IP address of the range 10.90.90.X

Step 3: Power on the switch. Type the default IP address of the switch (Dlink DGS 1210) – 10.90.90.90 in the URL of the browser to open the login of the switch.

Output/Results snippet:

Figure 4: Type the default password as ‘admin’ to get into the dashboard of the configuration page of the switch.



Figure 5: After logging in to the homepage of Dlink DGS 1210 switch



Figure 6: The system contains many options like Port Settings where the different ethernet ports of the switch could be configured.

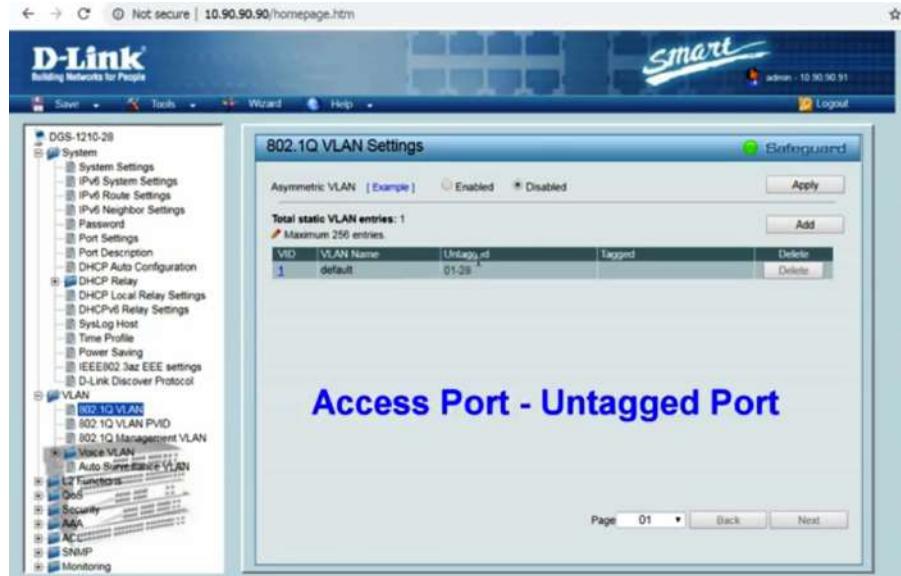


Figure 7: 802.1Q VLAN settings

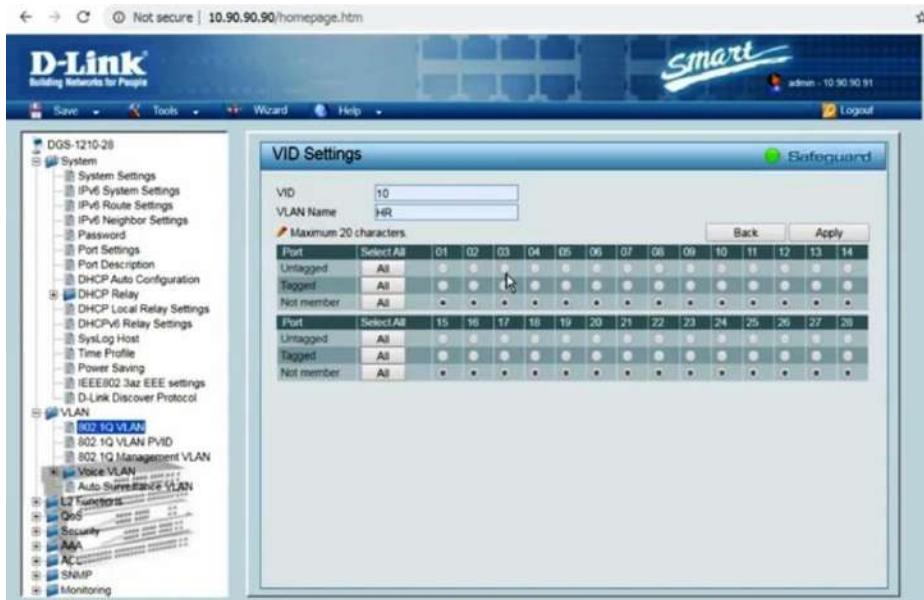


Figure 8: The VLAN options could be used to setup vlans.

References:

- <https://youtu.be/mYJInHyhU-s>

Activity 3

Aim: Install and configure router, bridges and HUB.

Learning outcome: Able to install & configure the different types of network devices in a network.

Duration: 3 hours

List of Hardware/Software requirements:

1. Router, Bridge, HUB
2. Ethernet cables with connectors
3. Computers/Digital Devices with pre-installed operating system (Windows, Linux, etc)
4. Cisco Packet Tracer Software

Code/Program/Procedure (with comments):

1. Provide power to the switch, if required. For a stand-alone switch, this means plugging in the power supply. For rack-mounted switches, this means using a slot that has power provided to it.
2. Connect the incoming network cable to the switch. Although any time can be used on most network switches, it is a good idea to use the first slot so anyone can quickly identify the incoming cable. For home and small office software, the incoming cable will be the one coming from your modem.
3. Connect a Cat5 or Cat6 cable to another slot in the network switch. Connect the other end to a computer you want to be connected to the network. Provide power to the switch, if required. For a stand-alone switch, this means plugging in the power supply.

For rack-mounted switches, means using a slot that has power supplied to it.

4. Connect the incoming network cable to the switch. Although any time can be used on most network switches, it is a good idea to use the first slot so anyone can quickly identify the incoming cable. For home and small office applications, the arriving cable will be the one coming from your modem.
5. Connect a Cat5 or Cat6 cable to another slot in the network switch. Connect the other end to a computer you want to be connected to the network.

Need to install pocket tracer software

- Press RETURN to get started
- Router>Enabled
- Router#configure t
- Enter configuration commands, one per line. End with CNTL/Z
- Router? (?) select which router from 0 to many)(config-if)#shot down.

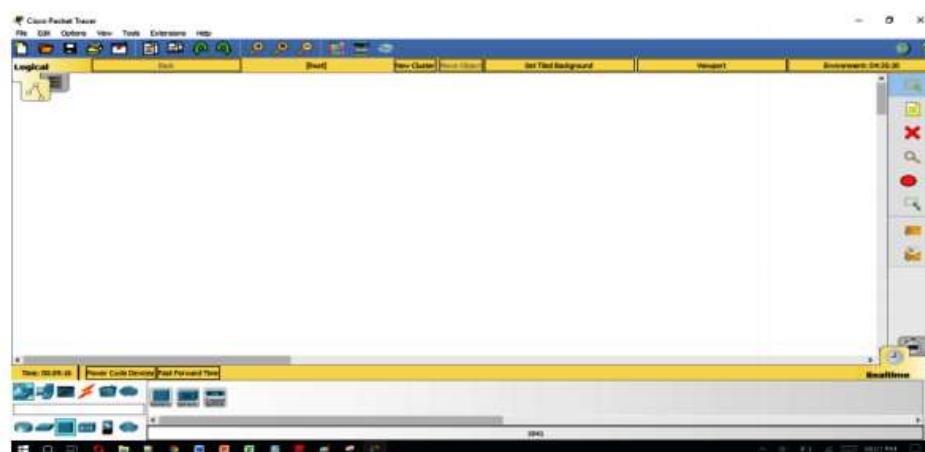


Figure 9: Packet Tracer Software

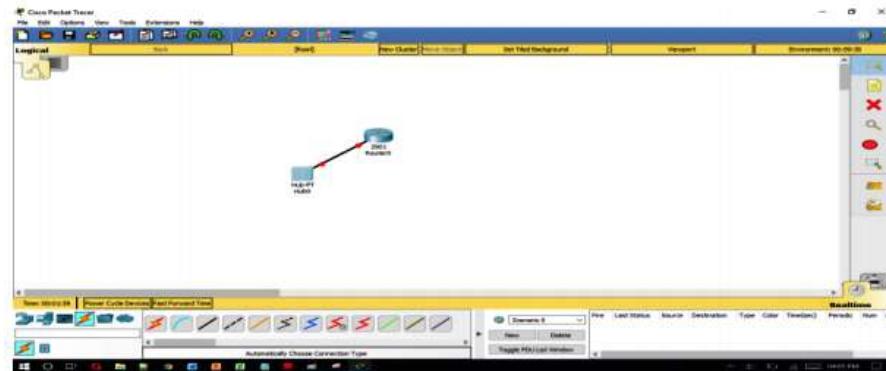


Figure 10: configure router, bridges, and HUB

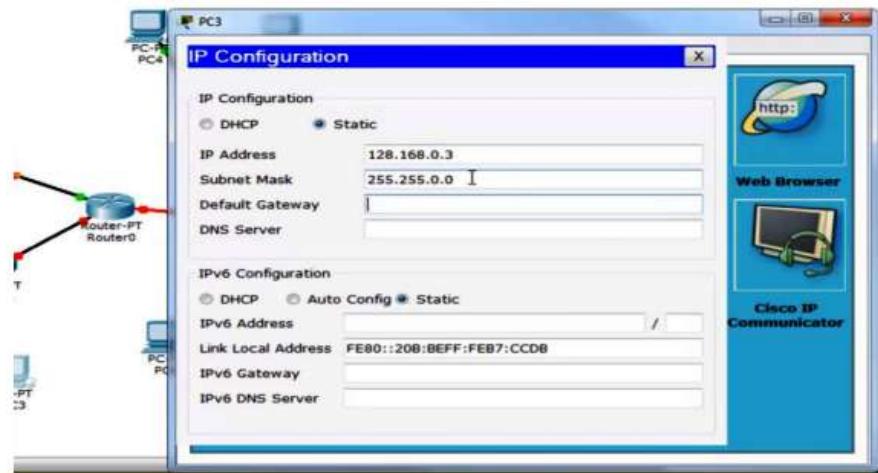


Figure 11: IP Configure

References:

- <https://www.examcollection.com/certification-training/network-plus-how-to-install-and-configure-routers-and-switches.html>
- <https://electricalacademia.com/computer/install-configure-routers-switches/>

Activity 4

Aim: Configure Wireless Access Point.

Learning outcome: Able to install & configure the different types of network devices in a network.

Duration: 2 hours

List of Hardware/Software requirements:

1. Computer with pre-installed operating system (Windows, Linux, etc)
2. Access point

Code/Program/Procedure (with comments):

Configure a wireless access point (By taking DLink access point). These guidelines are provided for illustrative purposes and do not represent an endorsement of the DLink access point over other competing products.

Please take the following steps:

1. Change the default admin password.
2. Change the default SSID to something of your picking.
3. Enable encryption.
4. Disable the DHCP Server task, if your access point has this feature.
5. Register the hardware (MAC) address of the wireless card.

By using these steps while connecting wireless access point there will be no problem.

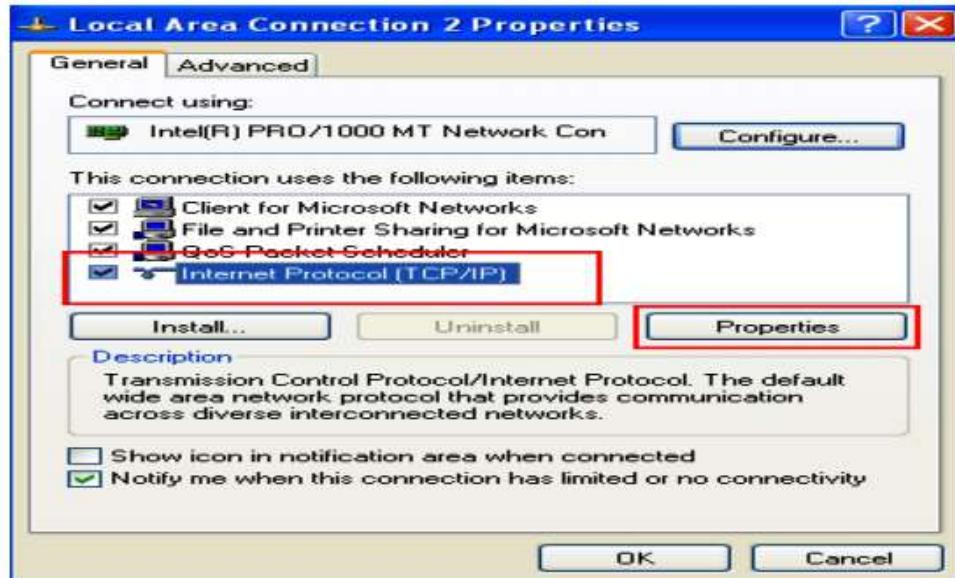


Figure 12: TCP/IP Properties

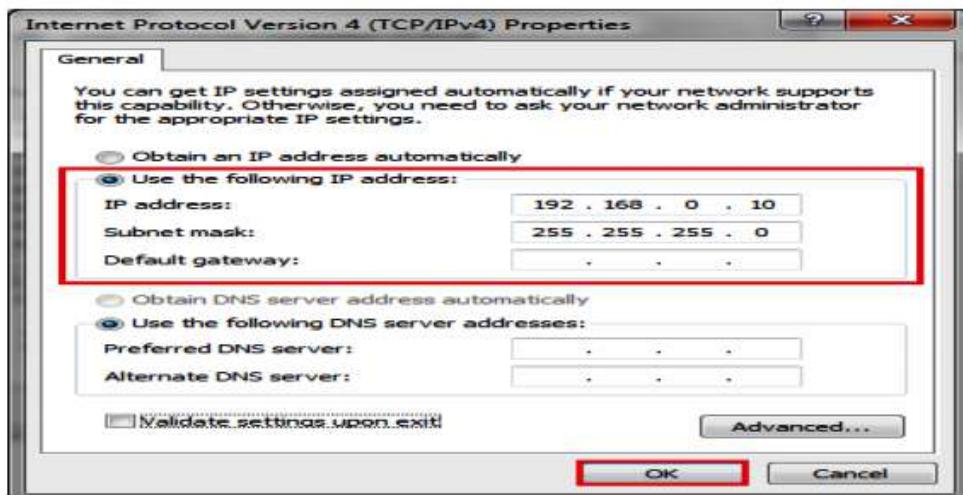


Figure 13: IP Address



Figure 14: Wireless access point Setup

References:

- <https://www.linksys.com/us/support-article?articleNum=136548>
- <https://www.dummies.com/programming/networking/configuring-a-wireless-access-point/>

Activity 5

Aim: Install and Configure Wire Network.

Learning outcome: Able to install & configure the different types of network devices in a network.

Duration: 2 hours

List of Hardware/Software requirements:

1. Computer with pre-installed operating system (Windows, Linux, etc)
2. Ethernet cable with connector
3. Router

Code/Program/Procedure (with comments):

1. Take the router to connect the Modem and router with the help of cables.



Figure 15: Connection between Modem and Router

2. Connect the router to the modem. Routers and wireless routers enable to share broadband internet connection with multiple devices. Will need to connect broadband modem to the router. For better results, place your router near your

modem. Fix the router and the modem with an Ethernet cable.



Figure 16: Modem with an Ethernet cable

3. The arrow mark shows the LAN is not connected, Or a problem with your LAN connection.

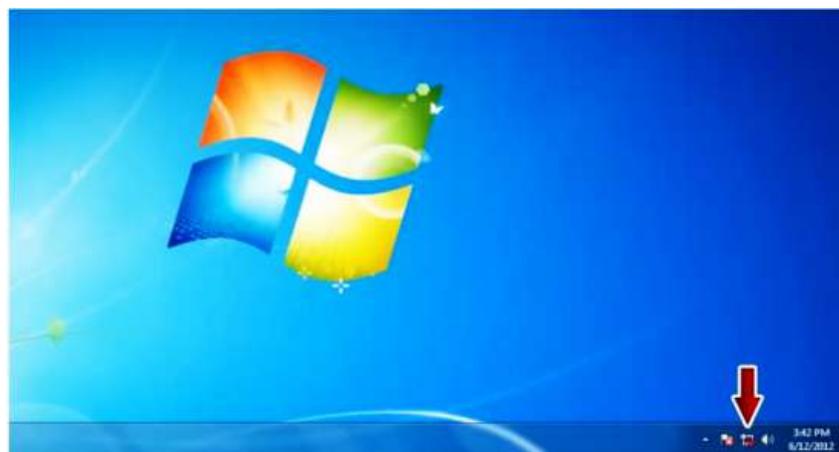


Figure 17: LAN connection

1. Select the Local area connection, right click on that and select the status option.

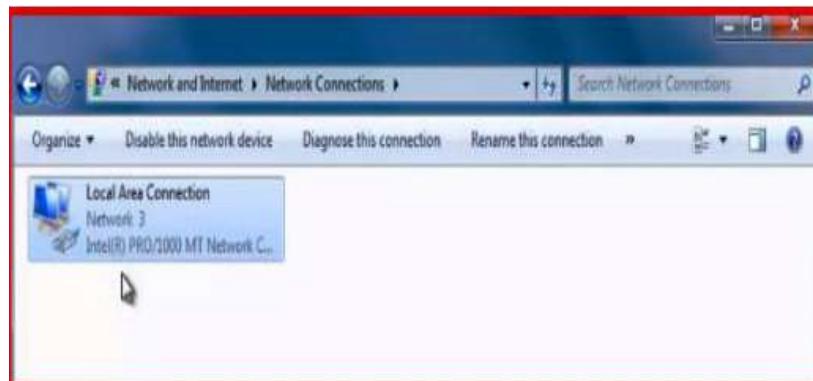


Figure 18: Status Option

4. Check the IPv4 connection and click on properties.

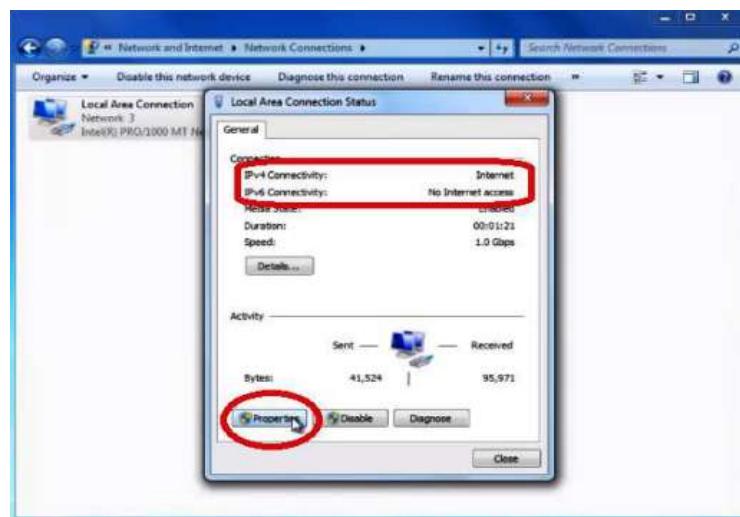


Figure 19: IPv4 connection

3. After that select the internet protocol version TCP/IPv4 and click on ok.

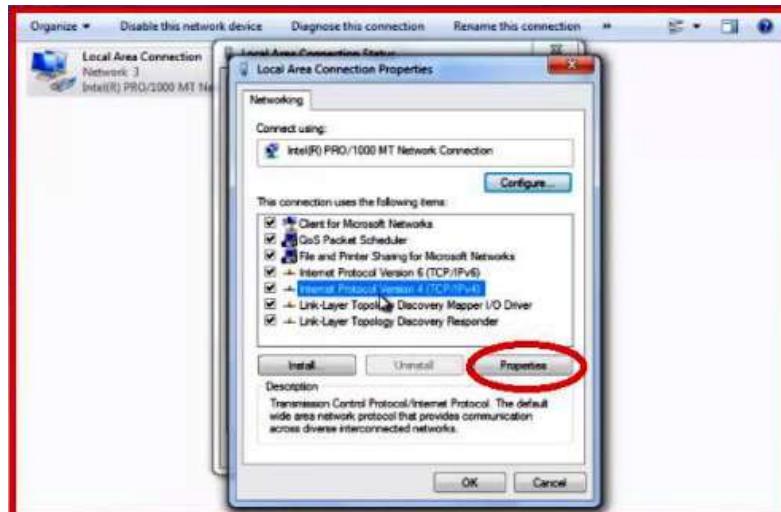


Figure 20: Version of TCP/IPv4



Figure 21: LAN Status Icon

References:

- <https://www.dummies.com/computers/operating-systems/windows-xp-vista/install-a-wireless-network/>
- <https://stevessmarthomeguide.com/build-home-network/>

Activity 6

Aim: Install and Configure Wireless Network.

Learning outcome: Able to install & configure the different types of network devices in a network.

Duration: 2 hours

List of Hardware/Software requirements:

1. Computer with pre-installed operating system (Windows, Linux, etc)
2. Wireless router

Code/Program/Procedure (with comments):

1. When you power on the router, it will only generate its wi-fi network, and the device will be connected to the router's wi-fi connection, not the internet. To connect the router to the internet need a MAC address to the internet service provider's website.

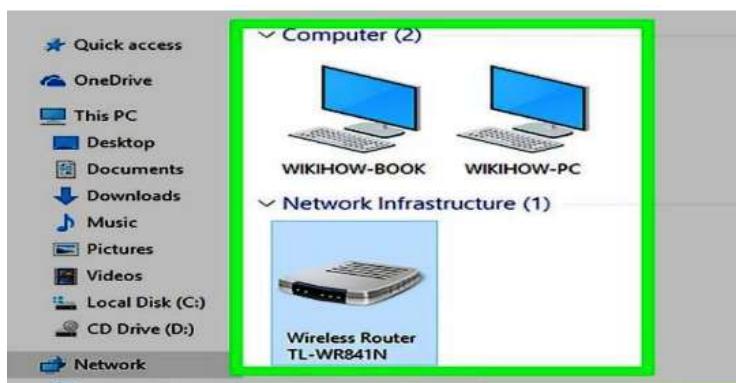


Figure 22: MAC address

2. The MAC address will display already the old one need to Reset the MAC address

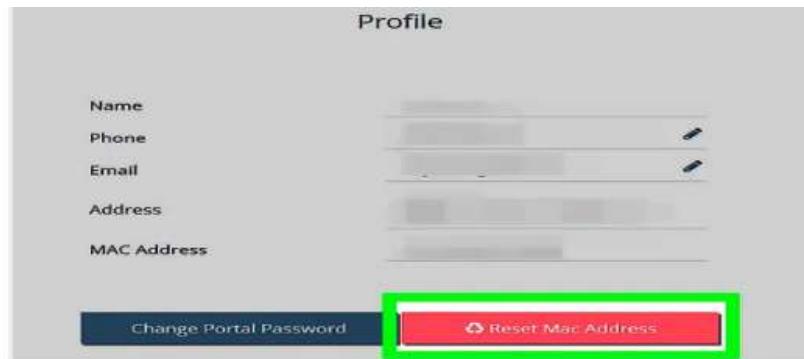


Figure 23: Reset MAC Address

3. Enter the administrator name and password and click on login



Figure 24: Administrator Name and Password



Figure 25: Wireless Tools

4. Select the wireless network name and select the enable the wireless router radio and SSID broadcast

The screenshot shows a configuration page for a wireless network. At the top, the 'Wireless Network Name' is set to 'www.wikihow.com'. The 'Region' is set to 'United States'. A warning message states: 'Ensure you select a correct country to conform local law. Incorrect settings may cause interference.' Below these, the 'Mode' is set to '11bgn mixed', 'Channel Width' is 'Auto', and 'Channel' is 'Auto'. At the bottom, there are three checkboxes: 'Enable Wireless Router Radio' (checked), 'Enable SSID Broadcast' (checked), and 'Enable WDS Bridging' (unchecked).

Figure 26: Wireless Router Radio and SSID broadcast

1. Select the WPA/WPA2 and fill all the fields.

The screenshot shows a 'Wireless Security' configuration page. It includes two radio button options: 'Disable Security' (unchecked) and 'WPA/WPA2 - Personal (Recommended)' (checked). Under 'WPA/WPA2 - Personal', the 'Version' is set to 'Automatic', 'Encryption' is 'AES', and the 'Wireless Password' field is empty. A note says: '(You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)'. The 'Group Key Update Period' is set to '0 Seconds'. Below this, there is another radio button for 'WPA/WPA2 - Enterprise', which has 'Version' set to 'Automatic', 'Encryption' set to 'Automatic', and 'Radius Server IP' and 'Radius Port' fields both set to '1812'. A note for the radius port says: '(1-65535, 0 stands for default port 1812)'.

Figure 27: WPA/WPA2

2. Enter the wireless password and click on the save button.

Disable Security

WPA/WPA2 - Personal(Recommended)

Version: Automatic

Encryption: AES

Wireless Password:

(You can enter ASCII characters between 0 and 8 and 64.)

Group Key Update Period: 0 Seconds

(Keep it default if you are not sure, minimum is 30.)

WPA/WPA2 - Enterprise

Version: Automatic

Encryption: Automatic

Figure 28: Wireless Password

Radius Server IP:

Radius Port: 1812 (1-65535, 0 stands for default port 1812)

Radius Password:

Group Key Update Period: 0 (in second, minimum is 30, 0 means no update)

WEP

Type: Automatic

WEP Key Format: Hexadecimal

Key Selected	WEP Key	Key Type
Key 1: <input checked="" type="radio"/>	<input type="text"/>	Disabled
Key 2: <input type="radio"/>	<input type="text"/>	Disabled
Key 3: <input type="radio"/>	<input type="text"/>	Disabled
Key 4: <input type="radio"/>	<input type="text"/>	Disabled

Figure 29: Save the Features

3. Gave old administrator name and password and a new username and password then click on save.

The user name and password can contain between 1 - 15 characters and may not include spaces.

Old User Name:	administrator
Old Password:	*****
New User Name:	wikihow
New Password:	*****
Confirm New Password:	*****

Figure 30: Administrator Name and Password

The Schedule is based on the time of the Router. The time can be set in "System Tools -> [Time Schedules](#)".

MAC Address of Children's PC:	<input type="text"/>
All MAC Address In Current LAN:	<input type="text"/> --Please Select-- <input type="button" value="▼"/>
Website Description:	<input type="text"/>
Allowed Website Name:	<input type="text"/> wikihow.com <input type="text"/> google.com <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Effective Time:	<input type="text"/> Anytime <input type="button" value="▼"/>
<p>The time schedule can be set in "Access Control -> Schedule"</p>	
Status:	<input type="text"/> Enabled <input type="button" value="▼"/>

Figure 31: Administration Information

4. Open the WIFI portal see the name is displaying then click on connect.

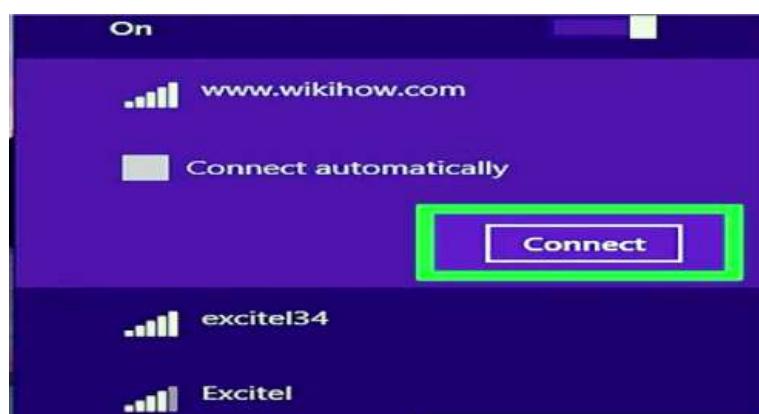


Figure 32: WIFI portal

5. Enter the password or security key which was given before and click on next button.



Figure 33: Password/Security Key

6. The WIFI is connected finally it is displaying in WIFI portal.

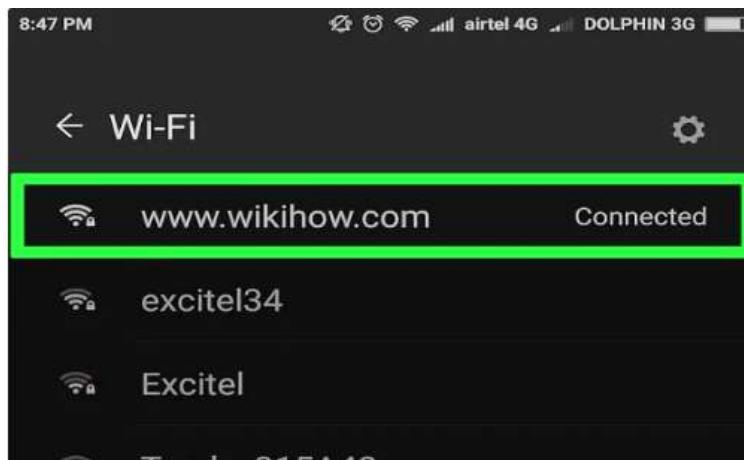


Figure 34: Check Connected or not

References:

- <https://support.microsoft.com/en-in/help/17137/windows-setting-up-wireless-network>

-
- [https://www.wikihow.com/Set-up-a-Wireless-Network-\(WiFi\)-Connection](https://www.wikihow.com/Set-up-a-Wireless-Network-(WiFi)-Connection)

Activity 7

Aim: Installation of AD-hoc Wireless Network.

Learning outcome: Able to install & configure the different types of network devices in a network.

Duration: 1 hour

List of Hardware/Software requirements:

1. Computer with pre-installed operating system (Windows, Linux, etc)
2. WinLAN software

Code/Program/Procedure (with comments):

First, need to install WinLAN.exe software, and double-click on that it will open WinLAN.exe.

1. Give your network name and password in the fields SSID and PASS respectively.

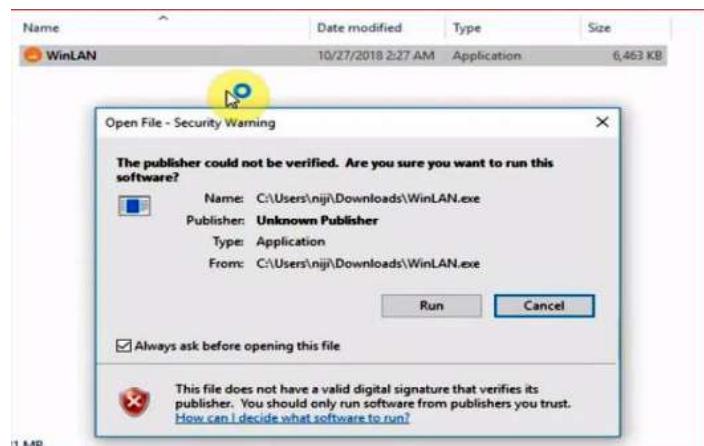


Figure 35: AD-hoc Wireless

2. Enter the SSID and PASS and click on create button.



Figure 36: Enter the SSID and PASS

3. See in the network and security center portal and will get the created LAN.

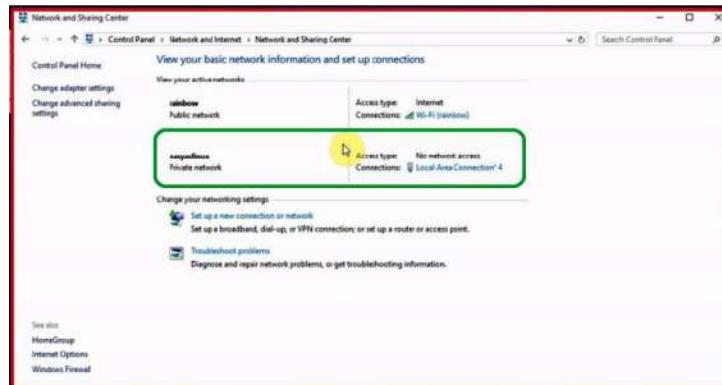


Figure 37: Network and Security Center Portal

References:

- <https://www.dummies.com/computers/computer-networking/wireless/how-to-set-up-a-wireless-ad-hoc-network/>
- <https://www.lifewire.com/set-up-an-ad-hoc-peer-wifi-network-818272>

Activity 8

Aim: Configure Gateway Service for Internet Connectivity.

Learning outcome: Able to install & configure the different types of network devices in a network.

Duration: 3 hours

List of Hardware/Software requirements:

1. Router
2. Broadband modem
3. Computer with pre-installed operating system (Windows, Linux, etc)
4. Ethernet cables

Code/Program/Procedure (with comments):

To configure your NETGEAR router (gateway) for cable internet connection with Smart Wizard:

- Connect your modem to the internet port of the NETGEAR router and your PC to any of the four LAN ports.

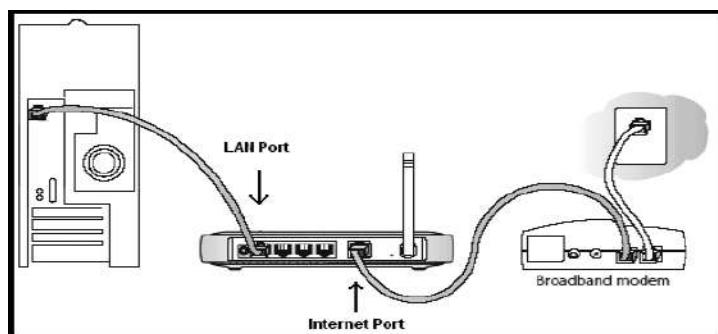


Figure 38: NETGEAR router

- Change the computer, router, and broadband/cable modem, off and on again. Pause for them all to finish booting up.
- Open a web browser and sort the router's IP address which would be either <http://192.168.0.1> or <http://192.168.1.1> in the address bar and press Enter.
- You are pressed to log into the router.
- The defaulting username is admin and the default password is password.
- The username and password are case-sensitive.
- If the default username and password are not functioning, you might have changed the password. Please try additional passwords that you might have changed too.
- Click the Setup Wizard.
- The Setup Wizard monitor displays.
- Select the Yes button and click Next.

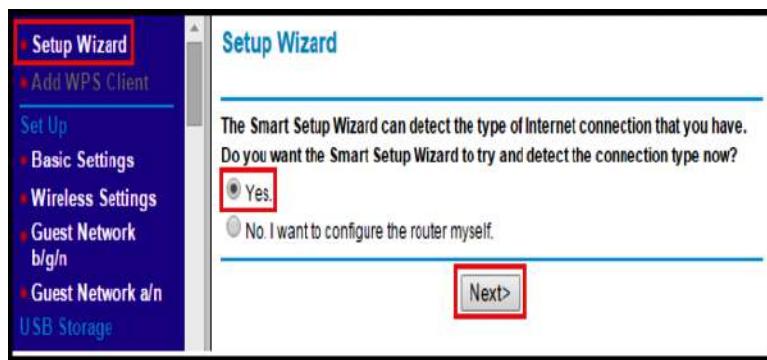


Figure 39: Setup for NETGEAR router

The Setup Wizard identifies the type of internet connection. For cable internet connections, the Setup Wizard identifies Dynamic IP.

- Click the Next. The router saves the settings.

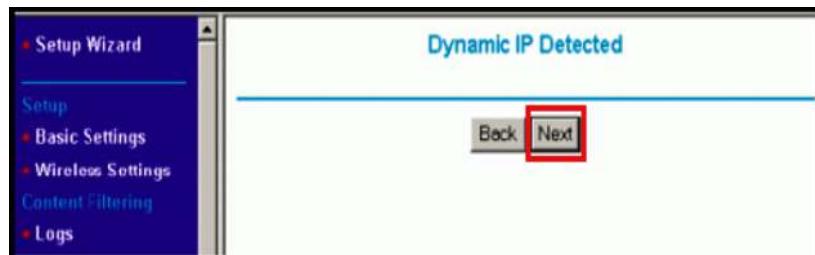


Figure 40: Save the settings

- Check that the internet connected, select Router Status under Maintenance.

Router Status	
Hardware Version	WNDR3700
Firmware Version	V1.0.4.26NA
GUI Language Version	V1.0.0.1
Internet Port	
MAC Address	00:22:3F:8C:F8:7F
IP Address	99.38.151.87
DHCP	PPPoE
IP Subnet Mask	255.255.255.255
Domain Name Server	68.94.156.1 68.94.157.1
LAN Port	
MAC Address	00:22:3F:8C:F8:7E
IP Address	192.168.1.1
DHCP	On
IP Subnet Mask	255.255.255.0
Wireless Port	
Wireless Settings a/n	
Name (SSID)	NETGEAR-5G
Region	United States

Figure 41: Router Status

- Appearance at the IP Address field to see if you have a valid IP address (that is, not blank or filled with zeroes, such as 0.0.0.0).

References:

https://media.distributordatasolutions.com/Leviton/files/File_47611-GT4_Programming_Guide.pdf

Activity 9

Aim: Configure ADSL+2 Router for ISP Internet Connectivity.

Learning outcome: Able to install & configure the different types of network devices in a network.

Duration: 2 hours

List of Hardware/Software requirements:

1. Computer with pre-installed operating system (Windows, Linux, etc)
2. ADSL+2 Router
3. Broadband modem
4. Ethernet cables

Code/Program/Procedure (with comments):

1. Open a web browser and enter the IP address of the DSL-300T. Press Enter.
2. Type the Login name and password. Click on login.
3. Click on the Setup at the top. Click on Connection on the left.
4. Configure the following for your connection:
 - Type - Set the connection to PPPoA
 - Name – Enter the name on name field for the connection.
 - Encapsulation - set the encapsulation as suggested by ISP.

- Username - Enter ISP login username
 - Password – Enter the login password
 - Keep alive - leave the default
 - MAX Fail - left the field as default
 - MTU - leave as default
 - MRU - leave the default
 - Set Route - enable set route(default)
 - VPI - set to ISP suggested settings (i.e. 0)(UK ADSL commonly uses VPI=0 and VCI=38)
 - VCI - set to ISP recommended settings (i.e.38) (UK ADSL usually uses VPI=0 and VCI=38)
 - QoS - leave the default
 - PCR - leave the default
 - SCR - leave default
- Click on Apply when done.
5. Click on the Status tab at the top and then click on Connection Position on the left side. The Connection data can be seen in the WAN section of the page. After connecting, the machine will now get the IP address from the ISP.
6. Click on Tools at the top. Click on System Commands on the left. Click on Save to permanently save the changes.

References:

-
- <https://eu.dlink.com/uk/en/support/faq/modems/dsl-modems/dsl-series/how-do-i-setup-my-adsl-router-for-internet-access>
 - <https://www.tp-link.com/lk/support/faq/618/>

Activity 10

Aim: Troubleshoot Internet Connectivity

Learning outcome: Able to configure and manage network security.

Duration: 5 hour

List of Hardware/Software requirements:

- Computer with 500GB Hard Disk
- 8 GB Ram
- Windows Server 2016 / 2019

Procedure:

Troubleshooting using IPCONFIG Command

If you are trying to diagnose and fix a network problem, you should know about the Ipconfig program as one of the troubleshooting arrows in your quiver.

Ipconfig can be used to display TCP/IP network configuration values, discard the current IP and DHCP settings for a device, and renew the DHCP settings for a device.

If your computer is connecting to the Internet or your local network properly, an easy thing to try is to use Ipconfig to release (meaning, discard) its current settings and then renew itself with new settings.

Ipconfig is a command-line program. To see the results of the program, you should run it from a Command Prompt box. To open a Command Prompt box, select the Command Prompt icon in the Accessories program group from the Windows XP Start menu.

Next, at the command line, type the command you want to run. Here are some of the most important ways you can use Ipconfig.

The command Ipconfig /? displays all the Ipconfig commands and the syntax of the program. So this is the command to run if you want to learn more about what Ipconfig can do, and how to use it.

The command Ipconfig /all displays the network settings for a TCP/IP device on the network, as you can see in Figure 15.10. You can use this information to track the IP addresses assigned to computers on your network, and make sure that there is no conflict caused by two computers having been assigned the same address. You can also use the IP address of a device on the network to access the device directly without knowing its name.

The command Ipconfig /release sends a message to the DHCP server to release the current IP address for a device on the network.

The command Ipconfig /renew sends a message to the DHCP server to renew the IP address of your computer, provided your computer is set up to automatically obtain its IP address. The results of running this command on my computer are shown in Image.

Troubleshooting using PING Command

1. Open a DOS command window. To do this, click Start, click Run, type cmd, and then press Enter.
2. At the command prompt, type the following command. Replace *example.com* with the domain that you want to test:
3. “ping *example.com*” write on the command prompt.
4. Interpret the output from ping.

Troubleshooting using TRACERT Command

1. Open a DOS command window. To do this, click Start, click Run, type cmd, and then press Enter.
2. At the command prompt, type the following command. Replace *example.com* with the domain that you want to test:
“tracert *example.com*”

3. Interpret the output from tracert:

- Tracert displays each hop, indicated by a number in the left column. It also displays the domain and IP address at each hop, as well as the time spent.

Troubleshooting using NSLOOKUP Command

Run the following command and check whether the DNS server is reachable from client computers.

Cmd

```
nslookup <client name> <server IP address>
```

- If the resolver returns the IP address of the client, the server does not have any problems.
- If the resolver returns a "Server failure" or "Query refused" response, the zone is probably paused, or the server is possibly overloaded. You can learn whether it's paused by checking the General tab of the zone properties in the DNS console.

If the resolver returns a "Request to server timed out" or "No response from server" response, the DNS service probably is not running. Try to restart the DNS Server service by entering the following at a command prompt on the server:

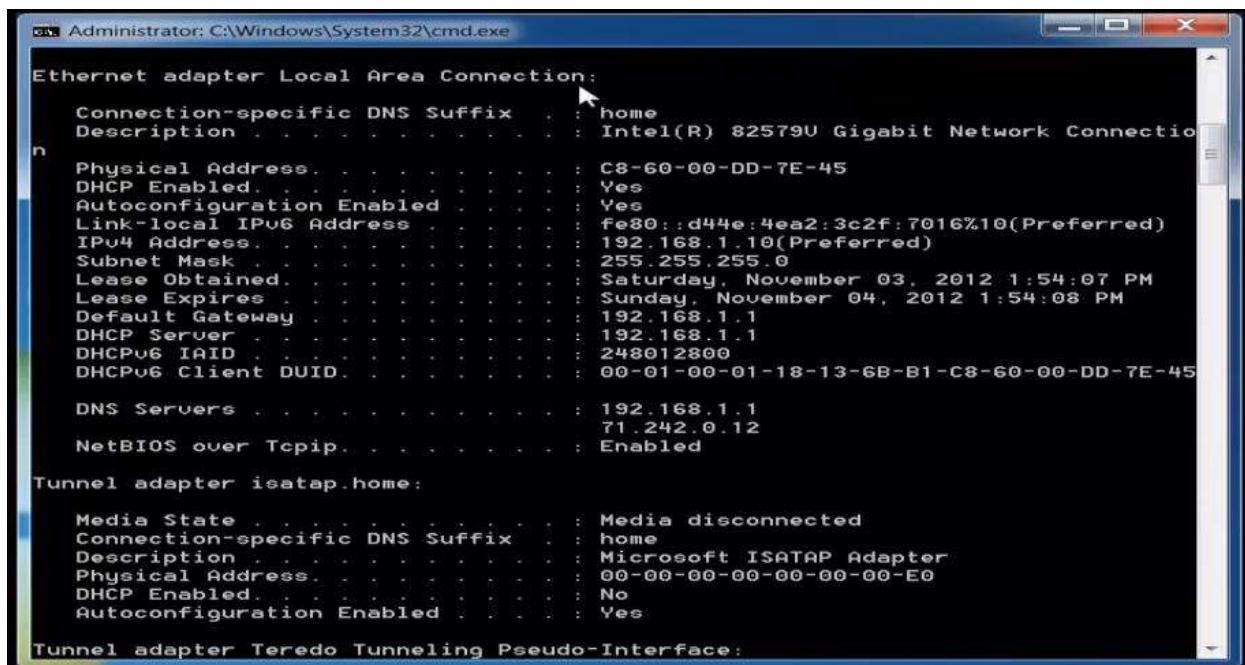
Cmd

```
net start DNS
```

If the issue occurs when the service is running, the server might not be listening on the IP address that you used in your nslookup query. On the **Interfaces** tab of the server properties page in the DNS console, administrators can restrict a DNS server to listen on only selected addresses. If the DNS server has been configured to limit service to a specific list of its configured IP addresses, it's possible that the IP address that's used to contact the DNS server is not in the list. You can try a different IP address in the list or add the IP address to the list.

1. In rare cases, the DNS server might have an advanced security or firewall configuration. If the server is located on another network that is reachable only through an intermediate host (such as a packet filtering router or proxy server), the DNS server might use a non-standard port to listen for and receive client requests.

Output/Results snippet:



The screenshot shows a Windows Command Prompt window titled "Administrator: C:\Windows\System32\cmd.exe". It displays the configuration for several network adapters:

- Ethernet adapter Local Area Connection:**
 - Connection-specific DNS Suffix : home
 - Description : Intel(R) 82579U Gigabit Network Connection
 - Physical Address : C8-60-00-DD-7E-45
 - DHCP Enabled : Yes
 - Autoconfiguration Enabled : Yes
 - Link-local IPv6 Address : fe80::d44e:4ea2:3c2f:7016%10 (Preferred)
 - IPv4 Address : 192.168.1.10 (Preferred)
Subnet Mask : 255.255.255.0
 - Lease Obtained : Saturday, November 03, 2012 1:54:07 PM
 - Lease Expires : Sunday, November 04, 2012 1:54:08 PM
 - Default Gateway : 192.168.1.1
 - DHCP Server : 192.168.1.1
 - DHCPv6 IAID : 248012800
 - DHCPv6 Client DUID : 00-01-00-01-18-13-6B-B1-C8-60-00-DD-7E-45
 - DNS Servers : 192.168.1.1
71.242.0.12
 - NetBIOS over Tcpip : Enabled
- Tunnel adapter isatap.home:**
 - Media State : Media disconnected
 - Connection-specific DNS Suffix : home
 - Description : Microsoft ISATAP Adapter
 - Physical Address : 00-00-00-00-00-00-E0
 - DHCP Enabled : No
 - Autoconfiguration Enabled : Yes
- Tunnel adapter Teredo Tunneling Pseudo-Interface:**


```
Administrator: C:\Windows\System32\cmd.exe
C:\Windows\system32>tracert google.com

Tracing route to google.com [74.125.228.34]
over a maximum of 30 hops:

 1  <1 ms    <1 ms    <1 ms  Wireless_Broadband_Router.home [192.168.1.1]
 2   6 ms     9 ms     9 ms  L100.PHLAPA-UFTTP-104.verizon-gni.net [98.111.16.
7.1]
 3   9 ms    11 ms   16 ms  G0-9-3-5.PHLAPA-LCR-22.verizon-gni.net [130.81.1.
39.154]
 4   8 ms     9 ms   19 ms  so-3-1-0-0.PHIL-BB-RTR2.verizon-gni.net [130.81.
22.60]
 5  13 ms     8 ms   10 ms  0.so-7-0-0.XL4.PHL6.ALTER.NET [152.63.3.81]
 6  14 ms    19 ms   28 ms  0.xe-3-1-0.XL4.IAD8.ALTER.NET [152.63.5.38]
 7  21 ms    19 ms   27 ms  TenGigE0-5-0-0.GW7.IAD8.ALTER.NET [152.63.37.158
]
 8  27 ms    18 ms   19 ms  google-gw.customer.alter.net [152.179.50.106]
 9  28 ms    18 ms   19 ms  216.239.46.250
10  20 ms    29 ms   19 ms  72.14.238.175
11  17 ms    20 ms   28 ms  iad23s06-in-f2.1e100.net [74.125.228.34]

Trace complete.

C:\Windows\system32>
```

```
Administrator: C:\Windows\System32\cmd.exe
C:\Windows\system32>ping www.google.com

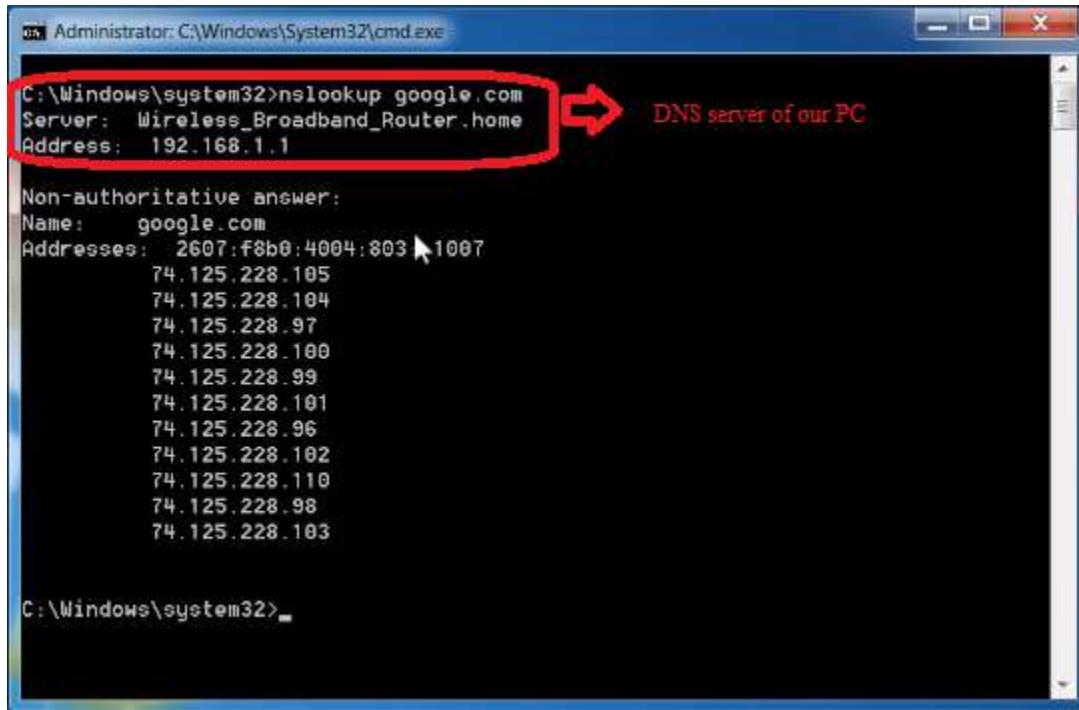
Pinging www.google.com [74.125.131.106] with 32 bytes of data:
Reply from 74.125.131.106: bytes=32 time=29ms TTL=252
Reply from 74.125.131.106: bytes=32 time=29ms TTL=252
Reply from 74.125.131.106: bytes=32 time=32ms TTL=252
Reply from 74.125.131.106: bytes=32 time=30ms TTL=252

Ping statistics for 74.125.131.106:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 29ms, Maximum = 32ms, Average = 30ms

C:\Windows\system32>ping 192.168.2.200

Pinging 192.168.2.200 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.200:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Windows\system32>
```



```
C:\Windows\system32>nslookup google.com
Server: Wireless_Broadband_Router.home
Address: 192.168.1.1

Non-authoritative answer:
Name: google.com
Addresses: 2607:f8b0:4004:803`1007
          74.125.228.105
          74.125.228.104
          74.125.228.97
          74.125.228.100
          74.125.228.99
          74.125.228.101
          74.125.228.96
          74.125.228.102
          74.125.228.110
          74.125.228.98
          74.125.228.103

C:\Windows\system32>
```

References:

- etutorials.org/Networking/
- <https://www.thewindowsclub.com/>

Learning Outcome 6 - Able to configure and manage network security

After achieving this learning outcome, a student will be Able to configure and manage network security. In order to achieve this learning outcome, a student has to complete the following:

1. Managing Server Network Security (3Hrs)
2. Set up security base line (2 Hrs)
3. Configure Audit Policy (2 Hrs)
4. Monitor and Troubleshoot Network protocol (3Hrs)
5. Configure Protocol Security (2 Hrs)
6. Plan security for Wireless Network (1Hr)
7. Install and Configure Different Antivirus Software (2 Hrs)
8. Install and Configure Admin Console (3Hrs)
9. Configure a Local Security Policies (2Hrs)
10. Configure Domain Security Policies (3Hrs)
11. Configure RRAS Policies (2Hrs)

Activity 1

Aim: Managing Server Network Security

Learning outcome: Able to configure and manage network security.

Duration: 3 hour

List of Hardware/Software requirements:

- Computer with 500GB Hard Disk
- 8 GB Ram
- Windows Server 2016 / 2019

Procedure:

There are two important things to understand about virtual secure mode. First, virtual secure mode doesn't really provide any security by itself. Instead, virtual secure mode is more of an infrastructure- level component of the operating system, and is the basis for other security features which will be discussed later on.

The other thing that must be understood about virtual secure mode is that the word virtual is there for a reason. As you probably know, modern CPUs include on-chip virtualization extensions. Historically, these virtualization extensions have been the basis of server virtualization. The hypervisor sits on top of the CPU and acts as an intermediary between the virtual machines and the hardware.

One of the big advantages to using this approach to server virtualization is that the hypervisor is able to ensure that virtual machines are truly isolated from one another. Virtual secure mode uses a similar technique to create a virtualized space on top of the hypervisor. Sensitive operations can be securely performed within this space, without being exposed to the host operating system.

Feature No. 1: Credential Guard

As previously noted, virtual secure mode is not a security feature itself, but rather a platform that can be used by other security features. Credential Guard is one of the security features that relies on virtual secure mode. As its name implies, Credential Guard is designed to prevent user credentials from being compromised.

The authentication process used by the Windows operating system is a function of the Local Security Authority (LSA). Not only does the LSA provide interactive authentication services, but it also generates security tokens, manages the local security policy and manages the system's audit policy. Credential Guard works by moving the LSA into Isolated User Mode, the virtualized space created by virtual secure mode.

Although the operating system must be able to communicate with the LSA in order to perform authentication services, Microsoft has designed the operating system to protect the integrity of the LSA. First, the memory used by the LSA is isolated, just as a virtual machine's memory is isolated. Microsoft also limits the LSA to running only the bare minimum binaries, and strict signing of those binaries is enforced. Finally, Microsoft prevents other code, such as drivers, from running in Isolated User Mode.

Feature No. 2: Device Guard

Device Guard is another operating system feature that leverages virtual secure mode. Device Guard isn't really a feature per se, but rather a collection of three security features that fall collectively under the Device Guard label. These three features include Configurable Code Integrity, VSM Protected Code Integrity, and Platform and UEFI Secure Boot (which has been around since Windows 8). Collectively, these three features work together to prevent malware infections.

The Device Guard component that is designed to work with virtual secure mode is VSM Protected Code Integrity. This component ensures the integrity of code running at the kernel level. Although moving kernel mode code integrity into virtual secure mode goes a long way toward protecting the operating system, the Configurable Code Integrity feature is equally noteworthy. This feature is designed to ensure that only trusted code is allowed to run. Administrators can use the PowerShell New-CIPolicy cmdlet to create integrity policies that essentially act as whitelists for applications.

In case you are wondering, these policies are based on application signatures. Since not all applications are signed, Microsoft provides a tool called SignTool.exe that can create a catalog (a signature) for unsigned applications.

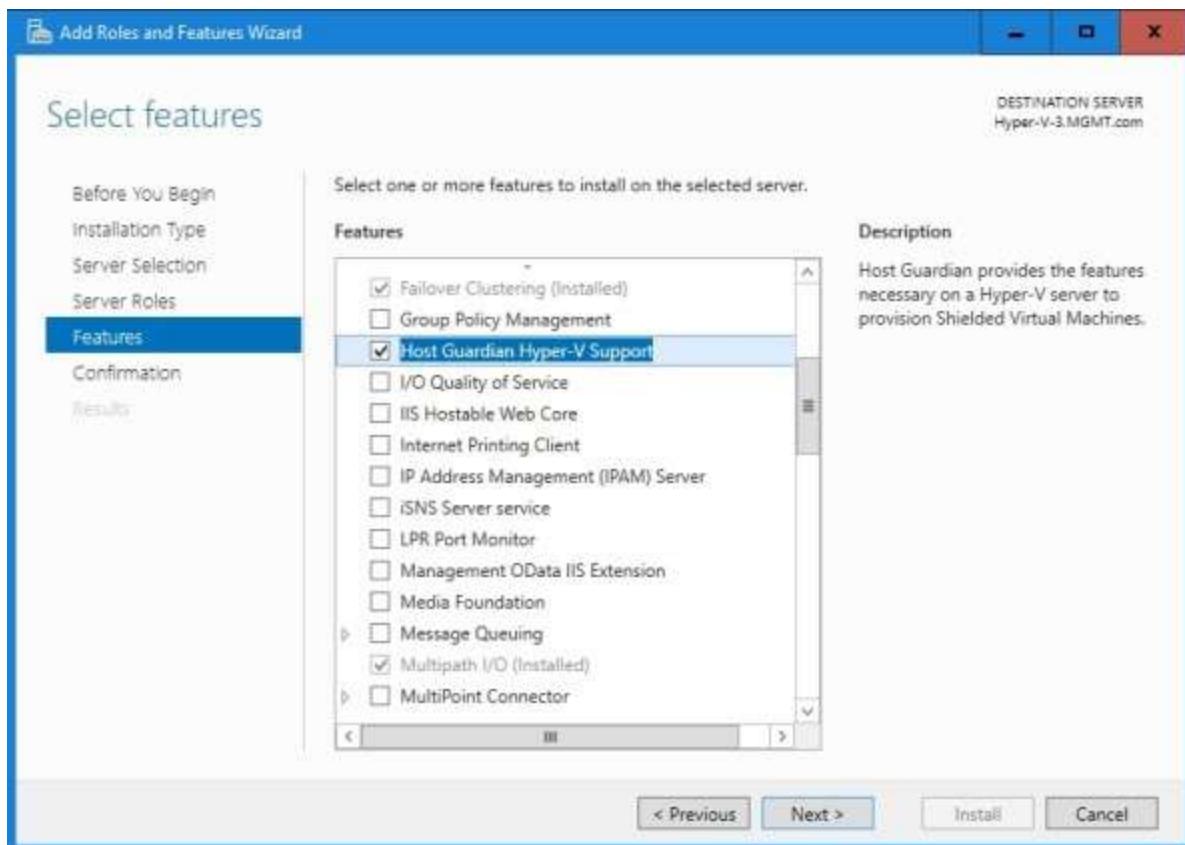
Feature No. 3: Host Guardian and Shielded Virtual Machines

Although server virtualization has been proven to be relatively secure, it has always had one major Achilles heel: virtual machine portability. Today, there is little to prevent a virtualization administrator, or even a storage administrator for that matter, from copying a virtual machine's virtual hard disk to removable media. The rogue administrator would then be able to take the media home, mount the virtual hard disks on his own computer and gain full access to the virtual hard disk's contents. If necessary, the administrator could even go so far as to set up their own host server and actually boot the stolen virtual machine. Microsoft's Host Guardian Service is designed to prevent this from happening by allowing the creation of shielded virtual machines.

The Host Guardian Service is a Windows Server 2016 attestation and key protection service that allows a Hyper-V host to be configured to act as a guarded host. A guarded host must be positively identified on the network and attested at the Active Directory and/or TPM level. If TPM trusted attestation is being used, then Windows goes so far as to verify the host's health by comparing its configuration against a known good baseline configuration. It is worth noting, however, that Active Directory trusted attestation does not support host configuration verification.

The Host Guardian Service enables the use of shielded virtual machines. A shielded virtual machine is a virtual machine whose virtual hard disks are encrypted via virtual TPM. This encryption prevents a shielded virtual machine from running on any Hyper-V server other than a designated guarded host. If a virtual hard disk is removed from the organization, its contents cannot be accessed and the virtual machine cannot be run.

Shielded virtual machines are BitLocker encrypted. BitLocker makes use of a virtual TPM device, residing on the host server. The virtual TPM is encrypted using a transport key, and the transport key is in turn protected by the Host Guardian Service.

Output/Results snippet:**References:**

12. etutorials.org/Networking/
13. <https://www.thewindowsclub.com/>

Activity 2

Aim: Set up security baseline

Learning outcome: Able to configure and manage network security.

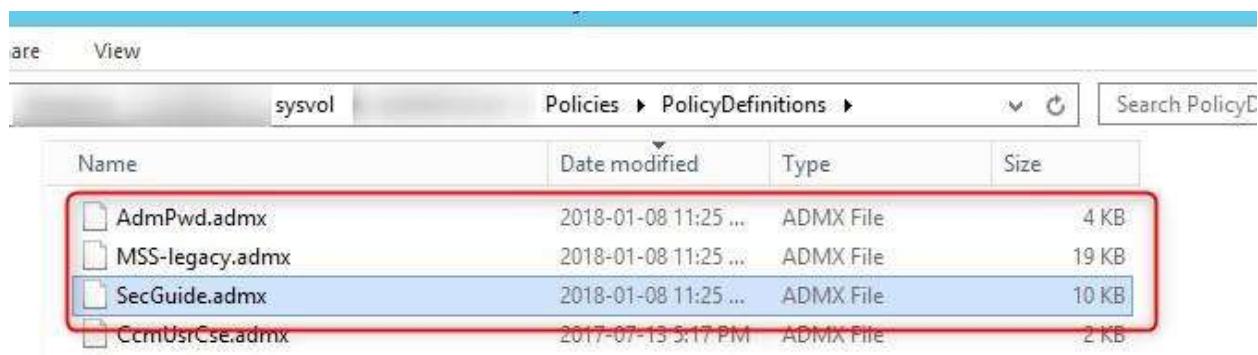
Duration: 2 hour

List of Hardware/Software requirements:

- Computer with 500GB Hard Disk
- 8 GB Ram
- Windows Server 2016 / 2019

Procedure:

Copy the ADMX from the Templates to the GPO Central Store



Name	Date modified	Type	Size
AdmPwd.admx	2018-01-08 11:25 ...	ADMX File	4 KB
MSS-legacy.admx	2018-01-08 11:25 ...	ADMX File	19 KB
SecGuide.admx	2018-01-08 11:25 ...	ADMX File	10 KB
CcmUsrCse.admx	2017-07-13 5:17 PM	ADMX File	2 KB

Duplicate the ADML from the templates to the GPO Central Store EN-US subfolder

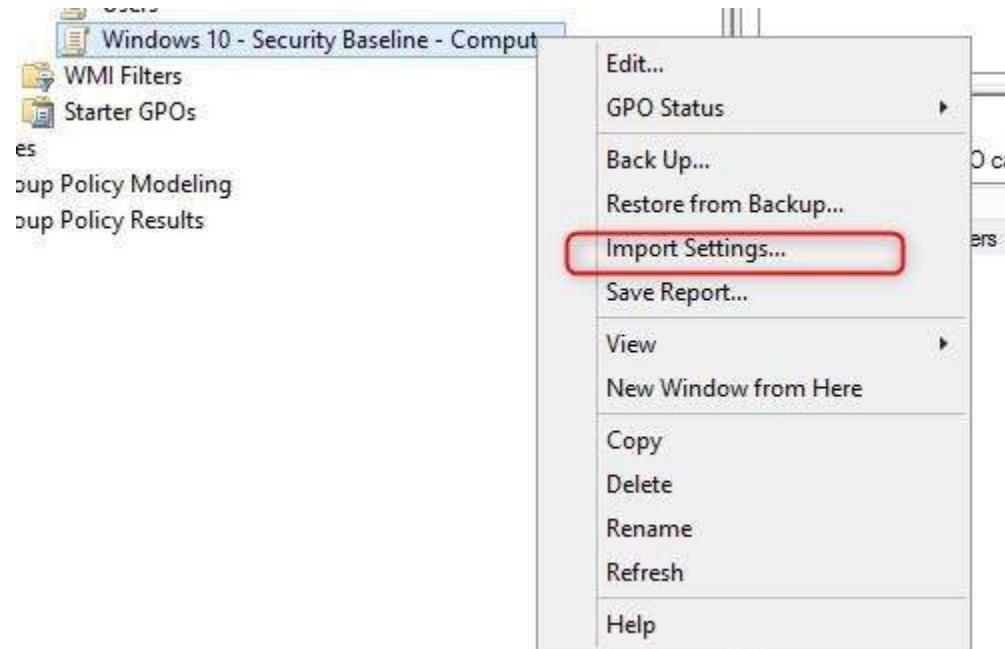
Name	Date modified	Type	Size
MSS-legacy.adml	2018-01-08 11:25 ...	ADML File	17 KB
SecGuide.adml	2018-01-08 11:25 ...	ADML File	9 KB
AdmPwd.adml	2018-01-08 11:25 ...	ADML File	4 KB
CcmUsrCse.adml	2017-07-13 5:17 PM	ADML File	1 KB

IMPORT GPOS

- Create a new blank GPO



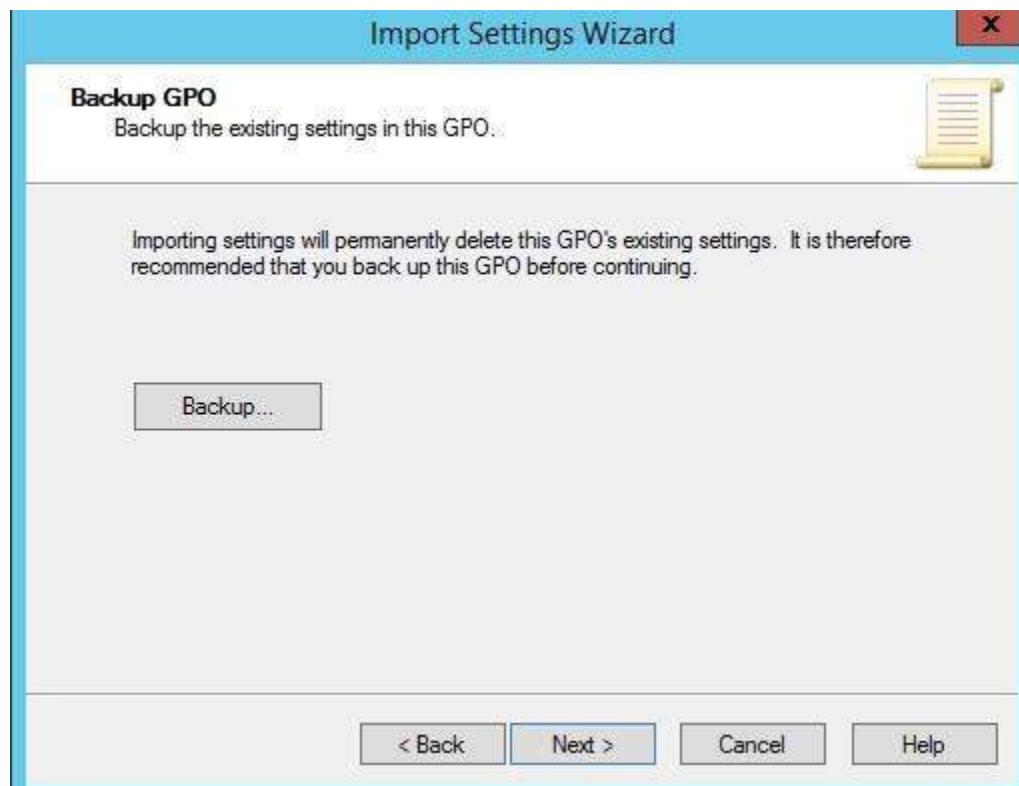
- Right-click on the GPO, and click on Import Settings



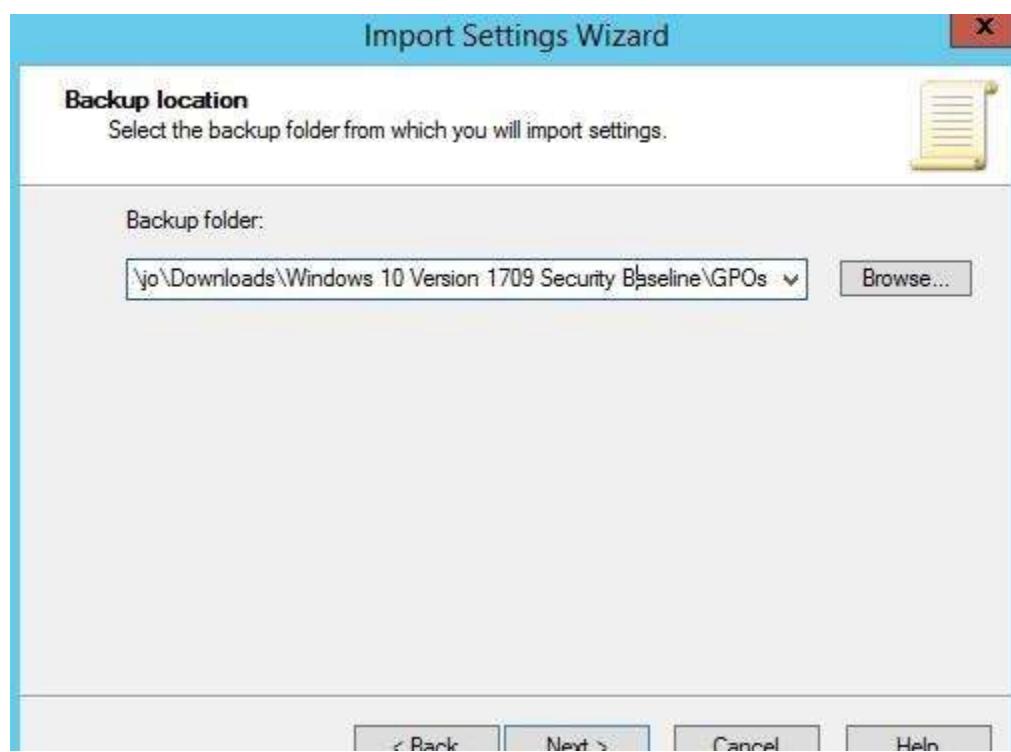
- Click Next



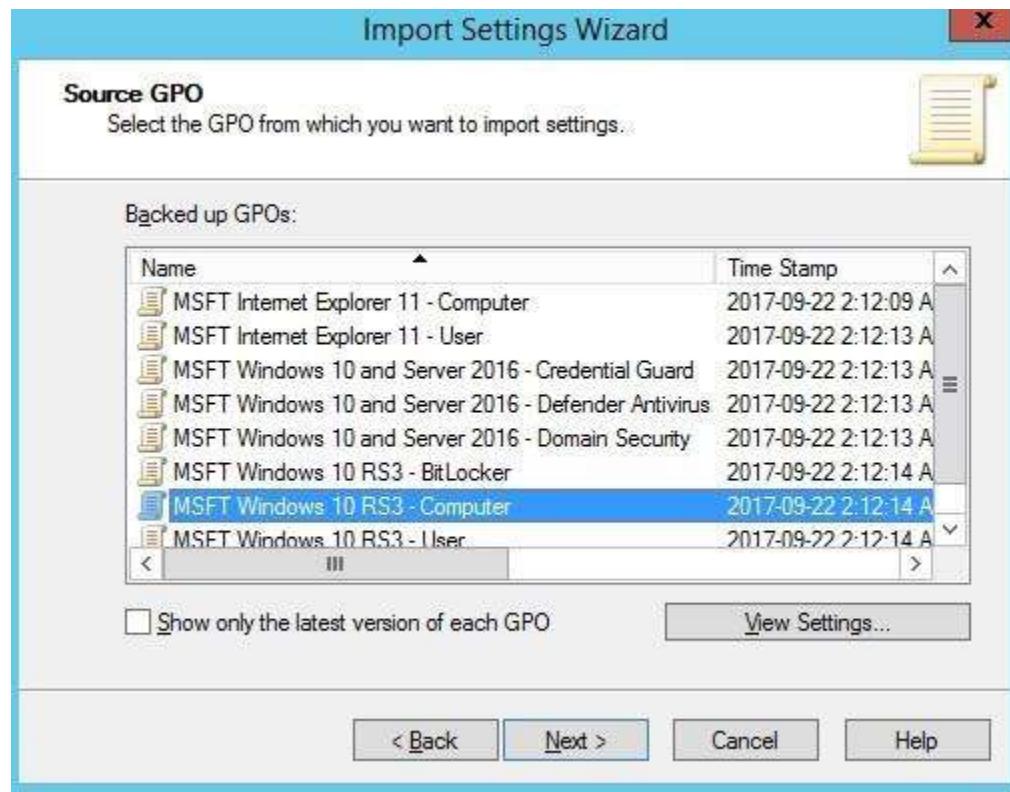
- Click Next, no need of backup of a new blank GPO.



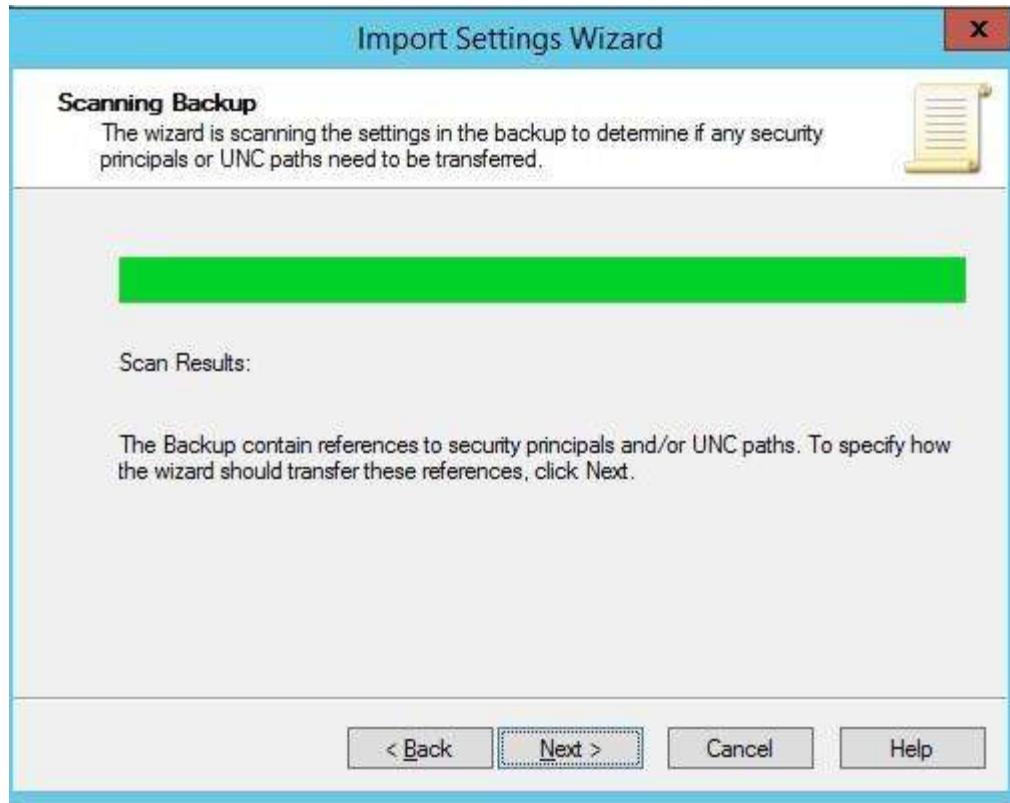
- Browse to the GPOs file and click Next.



- Select the GPO to be imported, built on the name and click Next.



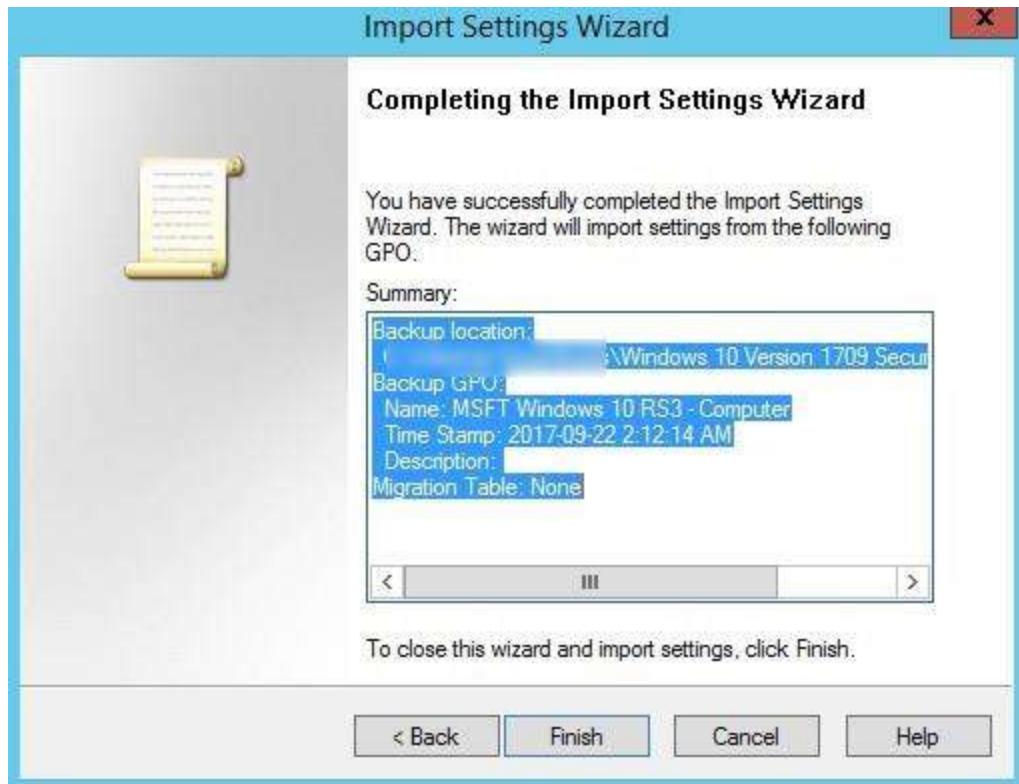
- Click Next



- Select Copying them identically from the source and click on next



- Click Finish



Output/Results snippet:

The Output as follows in the security baseline.

Windows 10 - Security Baseline - Computer	
Scope	Details
Settings	Delegation
Status	
Windows 10 - Security Baseline - Computer	
Data collected on: 2018-03-24 23:16 PM	
Computer Configuration (Enabled)	
Policies	show_all
Windows Settings	hide
Security Settings	hide
Administrative Templates	hide
Policy definitions (ADMX files) retrieved from the central store.	hide
Control Panel/Personalization	
LAPS	show
MS Security Guide	show
MSS (Legacy)	show
Network/Lanman Workstation	show
Network/Network Connections	show
Network/Network Connections/Windows Firewall/Domain Profile	show
Network/Network Provider	show
Network/Windows Connection Manager	show
Network/WLAN Service/WLAN Settings	show
System/Credential Delegation	show
System/Early Launch Antimalware	show
System/Group Policy	show
System/Internet Communication Management/Internet Communication settings	show
System/Logon	show
System/Power Management/Sleep Settings	show
System/Remote Assistance	show
System/Remote Procedure Call	show
Windows Components/App runtime	show
Windows Components/AutoPlay Policies	show
Windows Components/Biometric/Facial Features	show
Windows Components/Cloud Content	show
Windows Components/Credential User Interface	show
Windows Components/Event Log Service/Application	show
Windows Components/Event Log Service/Security	show
Windows Components/Event Log Service/System	show
Windows Components/File Explorer	show
Windows Components/Microsoft Edge	show
Windows Components/Remote Desktop Services/Remote Desktop Connection Client	show
Windows Components/Remote Desktop Services/Remote Desktop Session Host/Device and Resource Redirection	show

References:

14. etutorials.org/Networking/
15. <https://www.thewindowsclub.com/>

Activity 3

Aim: Configure Audit Policy

Learning outcome: Able to configure and manage network security.

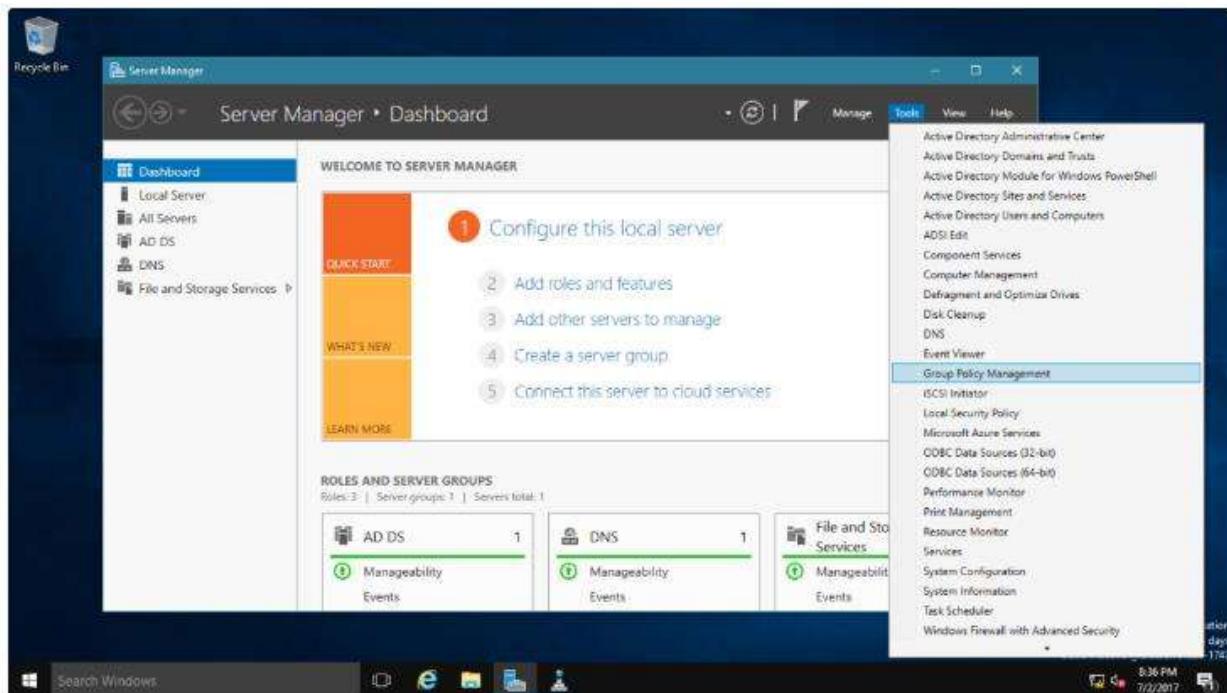
Duration: 2 hour

List of Hardware/Software requirements:

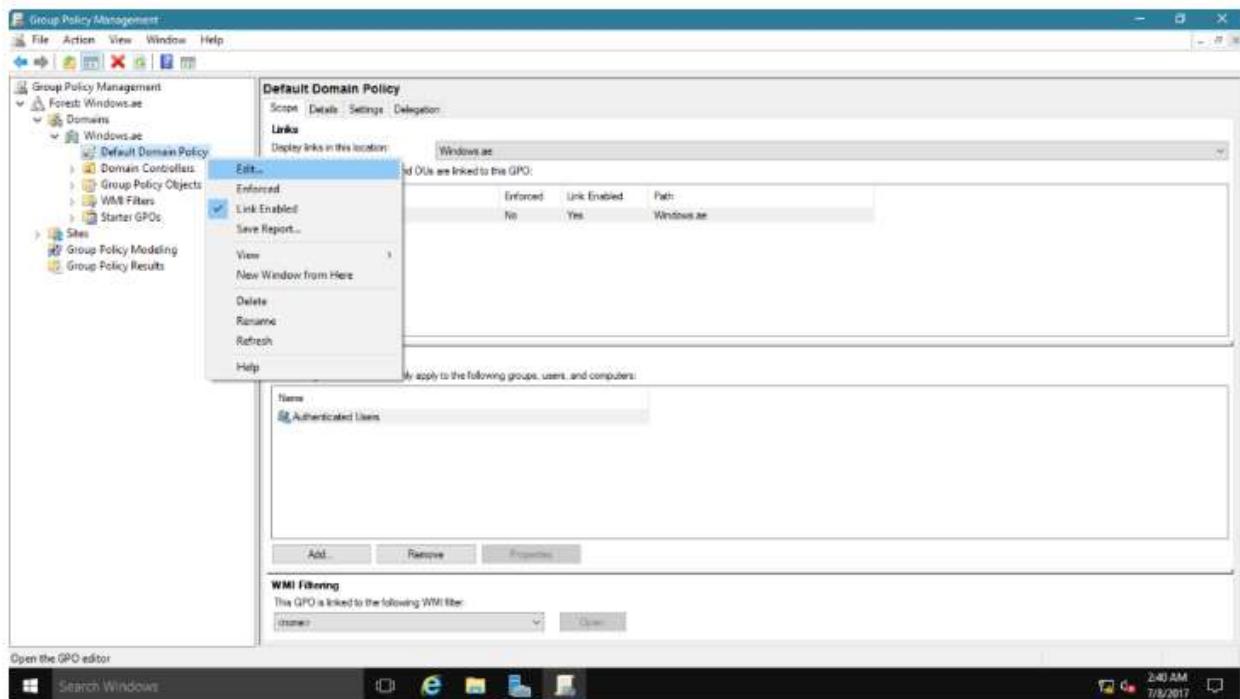
- Computer with 500GB Hard Disk
- 8 GB Ram
- Windows Server 2016 / 2019

Procedure:

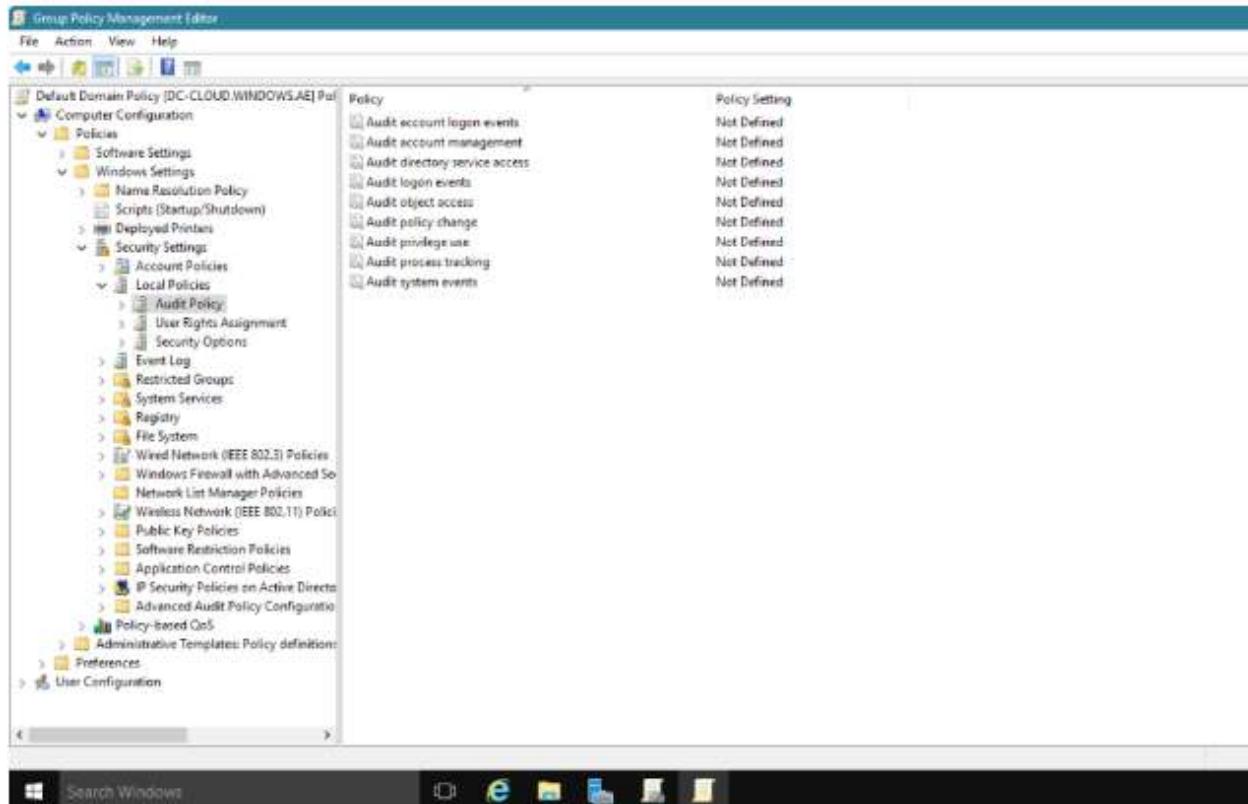
Open the server manager, click on tools and select the group policy management.



Select forest windows ae from group policy management, then select domain from their windows ae from their select default domain controller policy then right-click and select edit.

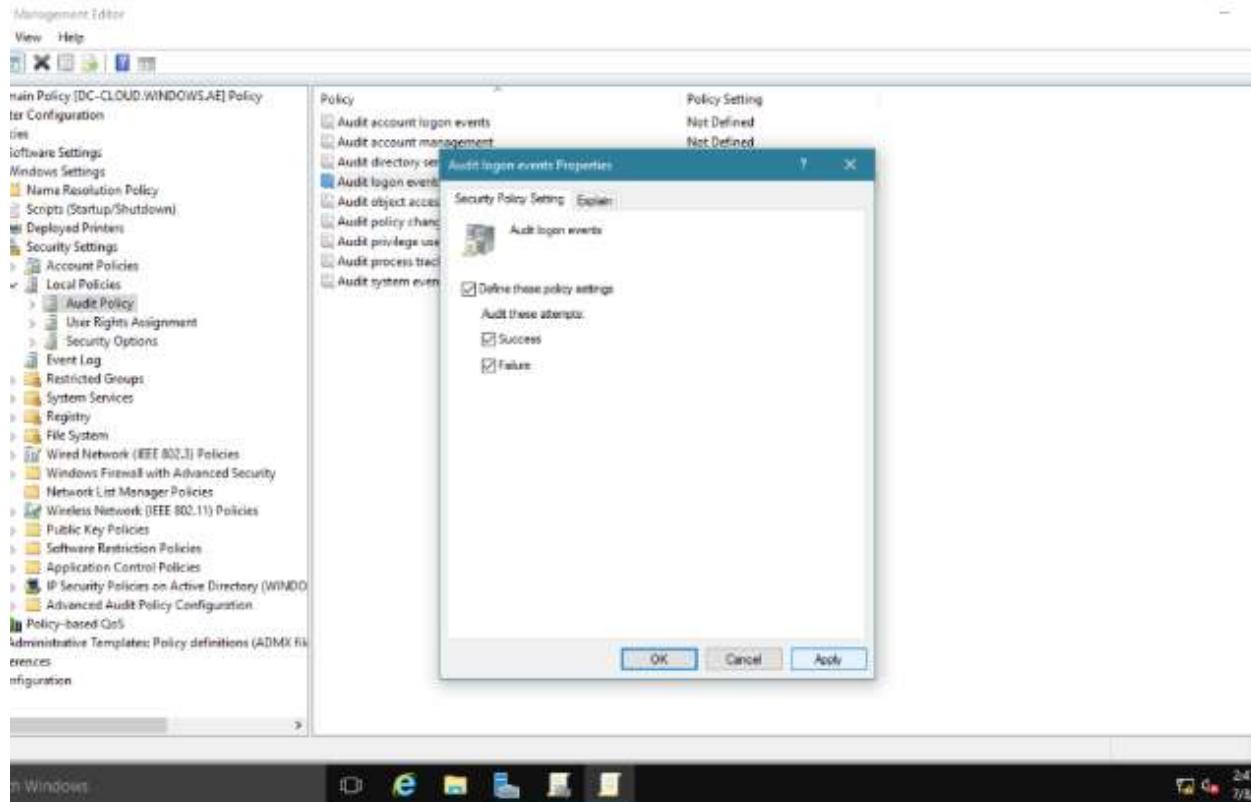


After that select the computer configuration.

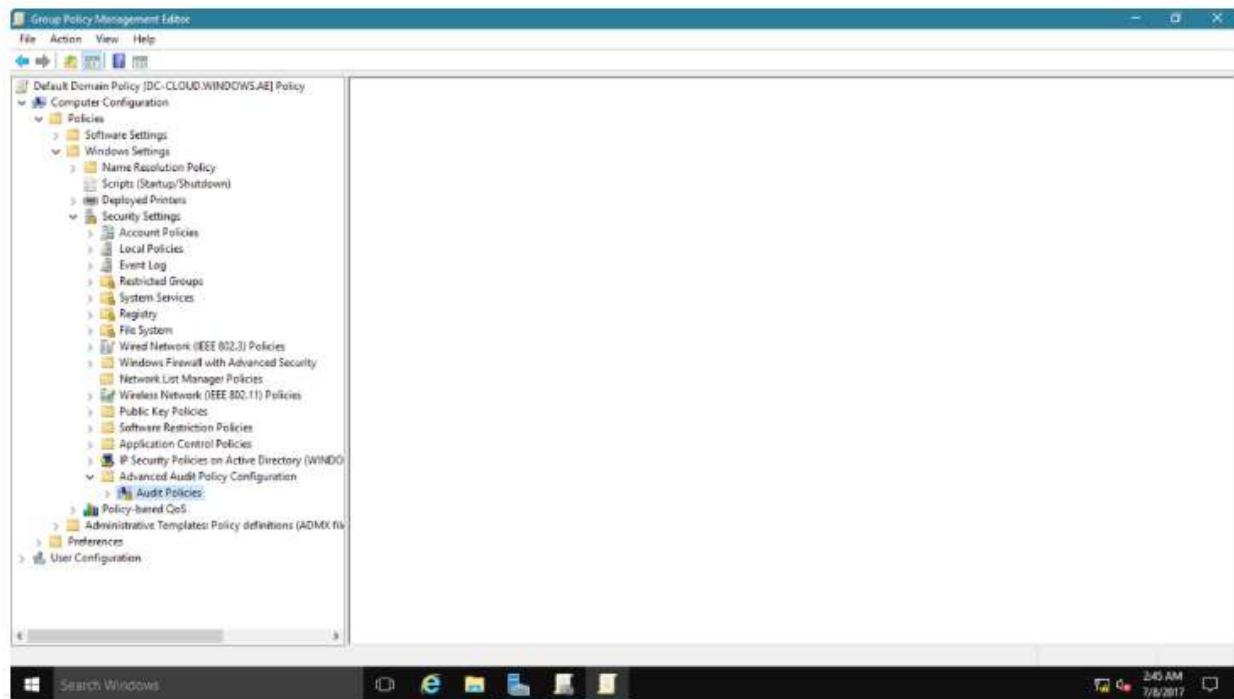


Double click on audit account logon events,

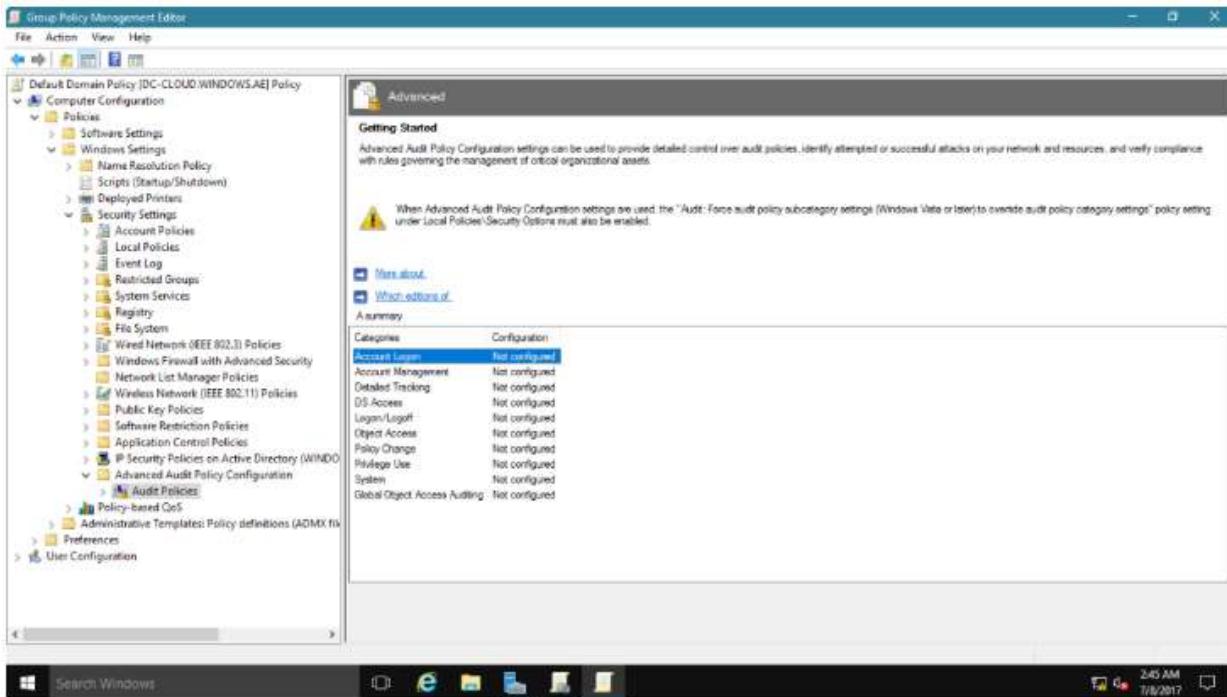
- If you select the Define these policy settings check box, the policy is applied.
- If you select Success, only success audits are logged.
- If you select Failure, only failure audits are logged.



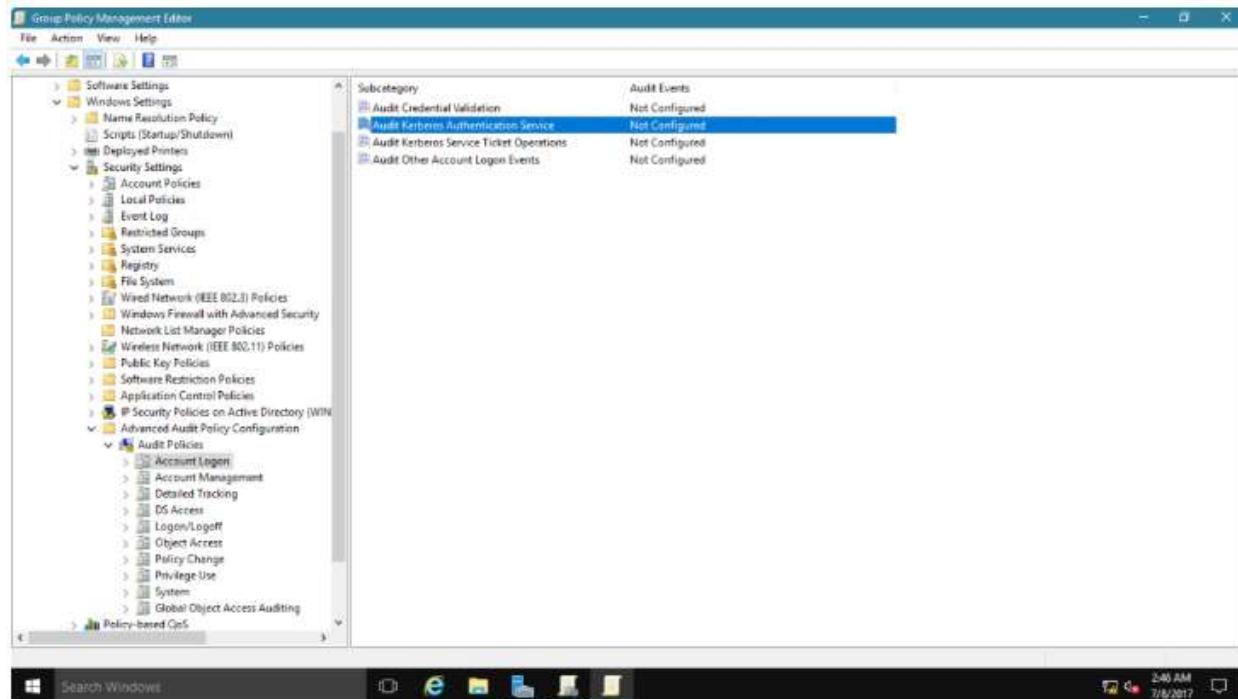
Repeat the step 1 and 3, then click Audit policies.



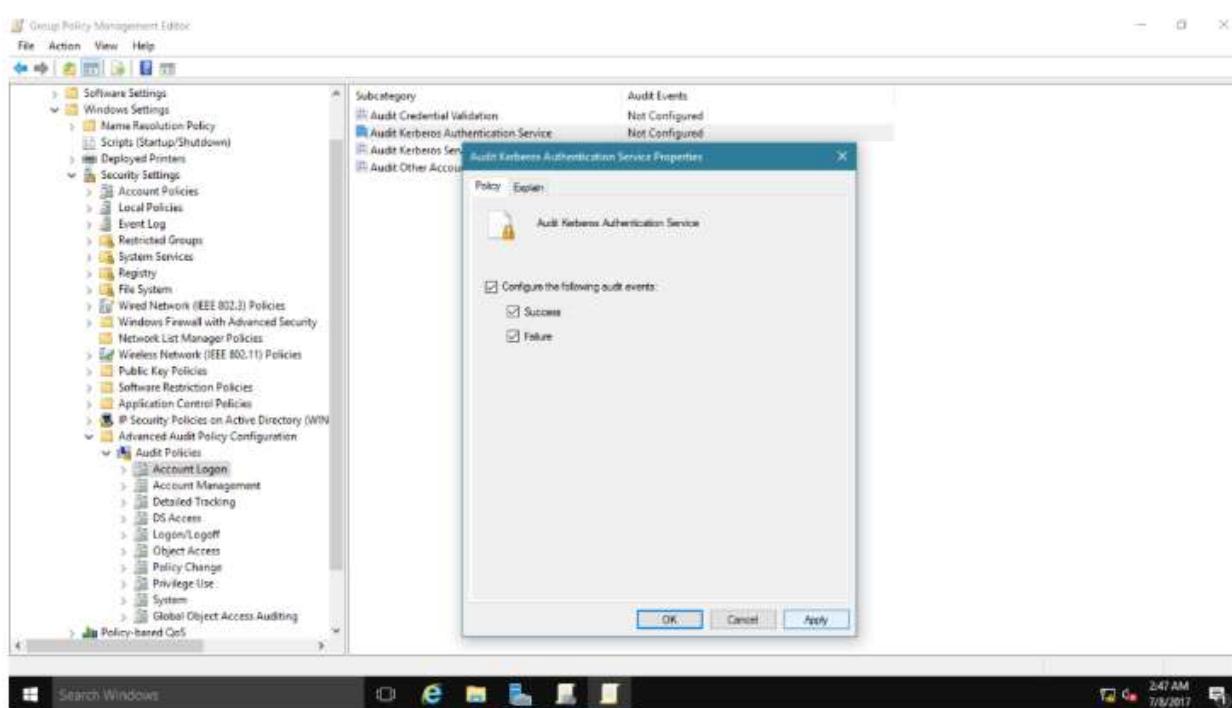
After that ten categories will display, then select account logon



In that four subcategories will display



Select Configure the following audit events, select Success, select Failure, and then click Apply.

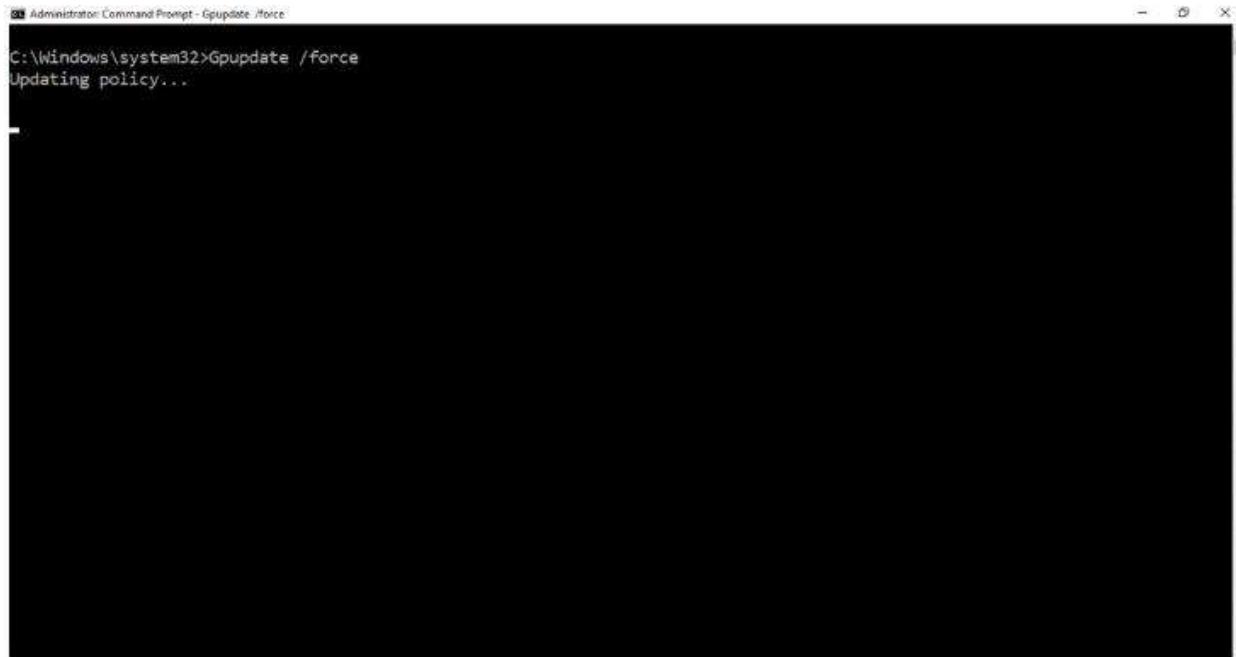


Close the Audit Kerberos Authentication Service Properties dialog box, click OK.

Output/Results snippet:

On DC-CLOUD, in the Right-Click Start, then click Command Prompt.



**References:**

16. etutorials.org/Networking/
17. <https://www.thewindowsclub.com/>

Activity 4

Aim: Monitor and Troubleshoot Network protocol

Learning outcome: Able to configure and manage network security.

Duration: 3 hour

List of Hardware/Software requirements:

- Computer with 500GB Hard Disk
- 8 GB Ram
- Windows Server 2016 / 2019

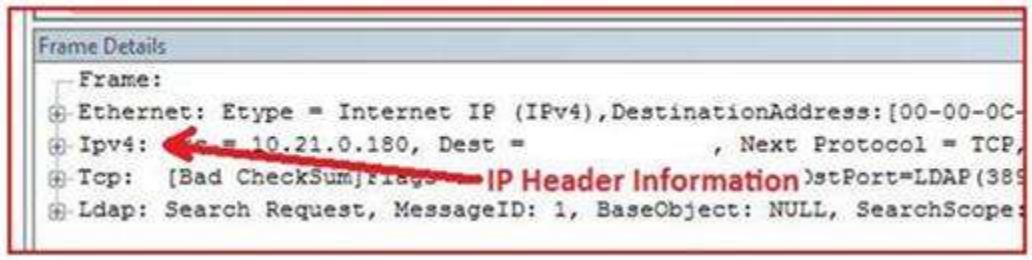
Procedure:

This is from the Frame Summary pane and is a general overview of each frame sent on

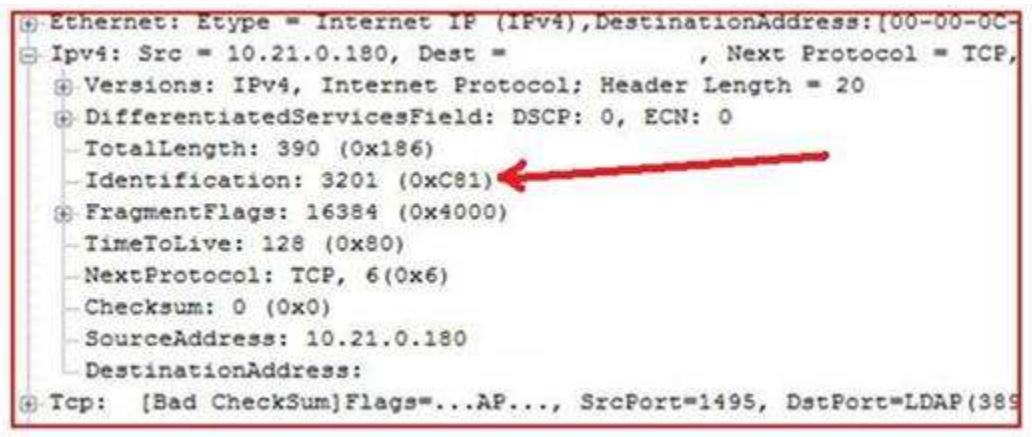
the wire.

51	77.01...	{SMB:11,... Workstation	Domain Controller	SMB	SMB:C; Read Andx, FID = 0x000C (\lsarpc\$
52	77.01...	{MSRPC:... Domain Controller	Workstation	MSRPC	MSRPC:c/o Bind Ack: Call=0x1 Assoc Grp=
53	77.21...	{MSRPC:... Workstation	Domain Controller	LsaRpc	LsaRpc:LsaOpenPolicy2 Request, Target C
54	77.21...	{MSRPC:... Domain Controller	Workstation	LsaRpc	LsaRpc:LsaOpenPolicy2 Response, PolicyH
55	77.43...	{MSRPC:... Workstation	Domain Controller	LsaRpc	LsaRpc:LsaQueryInformationPolicy2 Request
56	77.43...	{MSRPC:... Domain Controller	Workstation	LsaRpc	LsaRpc:LsaQueryInformationPolicy2 Response
57	77.64...	{MSRPC:... Workstation	Domain Controller	LsaRpc	LsaRpc:LsaQueryInformationPolicy Request
58	77.64...	{MSRPC:... Domain Controller	Workstation	LsaRpc	LsaRpc:LsaQueryInformationPolicy Response
59	78.00...	(TCP:5, ...	Workstation	Domain Controller	TCP
60	78.35...	{SMB:13,... Workstation	Domain Controller	SMB	SMB:C; Nt Create Andx, FileName = \samr\
61	78.35...	{SMB:13,... Domain Controller	Workstation	SMB	SMB:B; Nt Create Andx, FID = 0x000A (\sa
62	78.54...	{MSRPC:... Workstation	Domain Controller	MSRPC	MSRPC:c/o Bind: UUID{12345778-1234-AB
63	78.54...	{SMB:13,... Domain Controller	Workstation	SMB	SMB:B; Write Andx, FID = 0x000A (\samr@
64	78.73...	{SMB:13,... Workstation	Domain Controller	SMB	SMB:C; Read Andx, FID = 0x000A (\samr@
65	78.73...	{MSRPC:... Domain Controller	Workstation	MSRPC	MSRPC:c/o Bind Ack: Call=0x1 Assoc Grp=
66	78.93...	{MSRPC:... Workstation	Domain Controller	Samr	Samr:SamrConnect5 Request, ServerName=
67	78.93...	{MSRPC:... Domain Controller	Workstation	Samr	Samr:SamrConnect5 Response, OutVersion=
68	79.12...	{MSRPC:... Workstation	Domain Controller	Samr	Samr:SamrEnumerateDomainsInSamServer

These are the connection points involved in a domain join between a workstation and a domain controller.



Expand the IPv4 header information, the attribute named Identification with a value of 3201.



Line up the conversation of two traces taken simultaneously is to compare the Sequence and Acknowledgement numbers.

```

e: ipv4: Src = 10.21.0.180, Dest =
      Next Protocol = TCP,
e: Tcp: [Bad CheckSum]Flags=...AP..., SrcPort=1495, DstPort=LDAP(389)
  - SrcPort: 1495
  - DstPort: LDAP(389)
  - SequenceNumber: 4167329214 (0xF86465BE) ←
  - AcknowledgementNumber: 1946363494 (0x74032666) ←
⊕ DataOffset: 80 (0x50)
⊕ Flags: ...AP...
⊕ TCPKeyProperties: 0x1
⊕ TCPConversationProperties:
  - Window: 65535 (scale factor 0) = 65535
  - Checksum: 0xDDE6, Bad
  - UrgentPointer: 0 (0x0)
  - TCPPayload:
e: Ldap: Search Request, MessageID: 1, BaseObject: NULL, SearchScope:

```

The last packet sequence number sent in this frame is 4167329214, and the last packet that received from a partner in this communication is 1946363494.

Frame Summary				
F...	Source	Destination	Pro...	Description
126	Workstation	Domain Controller	LDAP	LDAP:Search Request, Me
127	Domain Controller	Workstation	Kerb...	KerberosV5:
128	Workstation	Domain Controller	TCP	TCP: [Bad CheckSum]Flag
129	Domain Controller	Workstation	NbtSS	NbtSS:SESSION KEEP ALI
130	Workstation	Domain Controller	TCP	TCP: [Bad CheckSum]Flag
131	Workstation	Domain Controller	ICMP	ICMP: [Bad CheckSum]Flag
132	Domain Controller	Workstation	ICMP	ICMP: [Bad CheckSum]Flag
133	Workstation	Domain Controller	LDAP	LDAP:Abandon Request, I
134	Domain Controller	Workstation	TCP	TCP:Flags=...A...., SrcPo
135	Workstation	Domain Controller	LDAP	LDAP:Search Request, Me

Frame Summary				
F...	Source	Destination	Prot...	Description
123	Workstation	Domain Controller	LDAP	LDAP:Search Request, Mess
124	Domain Controller	Workstation	TCP	TCP:[Continuation to #145]
125	Domain Controller	Workstation	TCP	TCP:[Continuation to #139]
126	Workstation	Domain Controller	TCP	TCP:Flags=...A...., SrcPort=
127	Domain Controller	Workstation	TCP	TCP:[ReTransmit #124][Con
128	Domain Controller	Workstation	TCP	TCP:[ReTransmit #124][Con
129	Domain Controller	Workstation	NbtSS	NbtSS:SESSION KEEP ALIVE,
130	Workstation	Domain Controller	TCP	TCP:Flags=...A...., SrcPort=
131	Domain Controller	Workstation	TCP	TCP:...
132	Domain Controller	Workstation	TCP	TCP:...
133	Domain Controller	Workstation	TCP	TCP:[ReTransmit #124][Con

Output/Results snippet:

By using Network Monitor, you can avoid time spent troubleshooting the wrong component.

References:

18. etutorials.org/Networking/
19. <https://www.thewindowsclub.com/>

Activity 5

Aim: Configure Protocol Security

Learning outcome: Able to configure and manage network security.

Duration: 2 hour

List of Hardware/Software requirements:

- Computer with 500GB Hard Disk
- 8 GB Ram
- Windows Server 2016 / 2019
- RV34x Series Cisco Router

Procedure:

Step 1. Log in to the web-based utility of the router and choose **VPN > IPSec Profiles**



Step 2. The IPsec Profiles Table shows the existing profiles. Click Add to create a new profile.

IPSec Profiles

IPsec Profiles Table			
	Name	Policy	In Use
<input type="radio"/>	Amazon_Web_Services	Auto	<input type="checkbox"/>
<input type="radio"/>	Default	Auto	<input checked="" type="checkbox"/>
<input type="radio"/>	Microsoft_Azure	Auto	<input type="checkbox"/>

Add **Edit** **Clone** **Delete**

Apply **Cancel**



Step 3. Create a name for the profile in the *Profile Name* field. The profile name must contain only alphanumeric characters and an underscore (_) for special characters.

Note: In this example, IPSec_VPN is used as the IPSec profile name.

Add a New IPSec Profile

Profile Name: **IPSec_VPN**

Keying Mode Auto Manual



Configure the Auto Settings

Step 1. In the Phase 1 Options area, choose the appropriate Diffie-Hellman (DH) group to be used with the key in Phase 1 from the DH Group drop-down list. Diffie-Hellman is a cryptographic key exchange protocol which is used in the connection to exchange pre-shared key sets. The strength of the algorithm is determined by bits. The options are:

- Group2 - 1024 bit — Computes the key slower, but is more secure than Group1.
- Group5 - 1536-bit — Computes the key the slowest, but is the most secure.

Note: In this example, Group2-1024 bit is chosen.

Phase I Options

DH Group:

✓ Group2 - 1024 bit

Group5 - 1536 bit

Encryption:

AES256

Step 2. From the Encryption drop-down list, choose the appropriate encryption method to encrypt and decrypt Encapsulating Security Payload (ESP) and Internet Security Association and Key Management Protocol (ISAKMP). The options are:

- 3DES — Triple Data Encryption Standard.
- AES-128 — Advanced Encryption Standard uses a 128-bit key.
- AES-192 — Advanced Encryption Standard uses a 192-bit key.
- AES-256 — Advanced Encryption Standard uses a 256-bit key.

Note: AES is the standard method of encryption over DES and 3DES for its greater performance and security. Lengthening the AES key will increase security with a drop-in performance. For this example, AES-256 is chosen.

Phase I Options

DH Group:

3DES

AES-128

AES-192

✓ AES-256

Encryption:

MD5

Authentication:

Step 3. From the Authentication drop-down menu, choose an authentication method that will determine how ESP and ISAKMP are authenticated. The options are:

- MD5 — Message Digest Algorithm has a 128-bit hash value.
- SHA-1 — Secure Hash Algorithm has a 160-bit hash value.
- SHA2-256 — Secure Hash Algorithm with a 256-bit hash value.

Note: MD5 and SHA are both cryptographic hash functions. They take a piece of data, compact it, and create a unique hexadecimal output that is typically not reproducible. In this example, SHA2-256 is chosen.

DH Group:	Group2 - 1024 bit
Encryption:	MD5
Authentication:	SHA1
	✓ SHA2-256

Step 4. In the *SA Lifetime* field, enter a value ranging between 120 to 86400. This is the length of time the Internet Key Exchange (IKE) Security Association (SA) will remain active in this phase. The default value is 28800.

Note: In this example, 28801 is used.

Authentication:	SHA2-256
SA Lifetime:	28801
Perfect Forward Secrecy:	<input checked="" type="checkbox"/> Enable

Step 5. (Optional) Check the **Enable Perfect Forward Secrecy** check box to generate a new key for IPSec traffic encryption and authentication.

Authentication:	SHA2-256
SA Lifetime:	28801
Perfect Forward Secrecy:	<input checked="" type="checkbox"/> Enable

Step 6. From the Protocol Selection drop-down menu in the Phase II Options area, choose a protocol type to apply to the second phase of the negotiation. The options are:

- ESP — If this is chosen, skip to [Step 7](#) to choose an encryption method on how the ESP packets will be encrypted and decrypted. A security protocol which provides

data privacy services and optional data authentication, and anti-replay services. ESP encapsulates the data to be protected.

- AH — Authentication Header (AH) is a security protocol which provides data authentication and optional anti-replay services. AH is embedded in the data to be protected (a full IP datagram). Skip to [Step 8](#) if this was chosen.



Step 7. If ESP was chosen in Step 6, choose the appropriate encryption method to encrypt and decrypt ESP and ISAKMP from the Encryption drop-down list. The options are:

- 3DES — Triple Data Encryption Standard.
- AES-128 — Advanced Encryption Standard uses a 128-bit key.
- AES-192 — Advanced Encryption Standard uses a 192-bit key.
- AES-256 — Advanced Encryption Standard uses a 256-bit key.

Note: In this example, AES-256 is chosen.



Step 8. From the Authentication drop-down menu, choose an authentication method that will determine how ESP and ISAKMP are authenticated. The options are:

- MD5 — Message Digest Algorithm has a 128-bit hash value.
- SHA-1 — Secure Hash Algorithm has a 160-bit hash value.
- SHA2-256 — Secure Hash Algorithm with a 256-bit hash value.

Note: In this example, SHA2-256 is used.



Step 9. From the DH Group drop-down list, choose the appropriate Diffie-Hellman (DH) group to be used with the key in Phase 2. The options are:

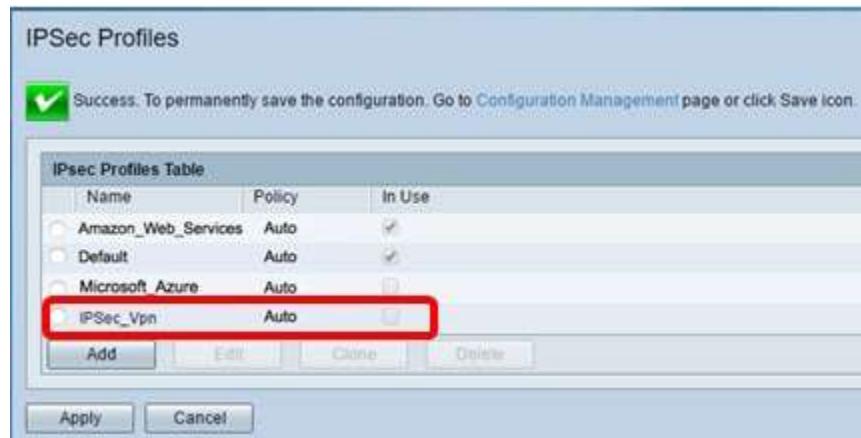
- Group2 – 1024 bit — Computes the key slower, but is more secure than Group1.
- Group5 – 1536 bit — Computes the key the slowest, but is the most secure.

Note: In this example, Group5 – 1536 bit is chosen.



Output/Results snippet:

Note: You will be taken back to the IPSec Profiles Table and the newly-created IPSec profile should now appear.



References:

20. etutorials.org/Networking/
21. <https://www.cisco.com/>
22. <https://www.thewindowsclub.com/>

Activity 6

Aim: Plan security for Wireless Network

Learning outcome: Able to configure and manage network security.

Duration: 1 hour

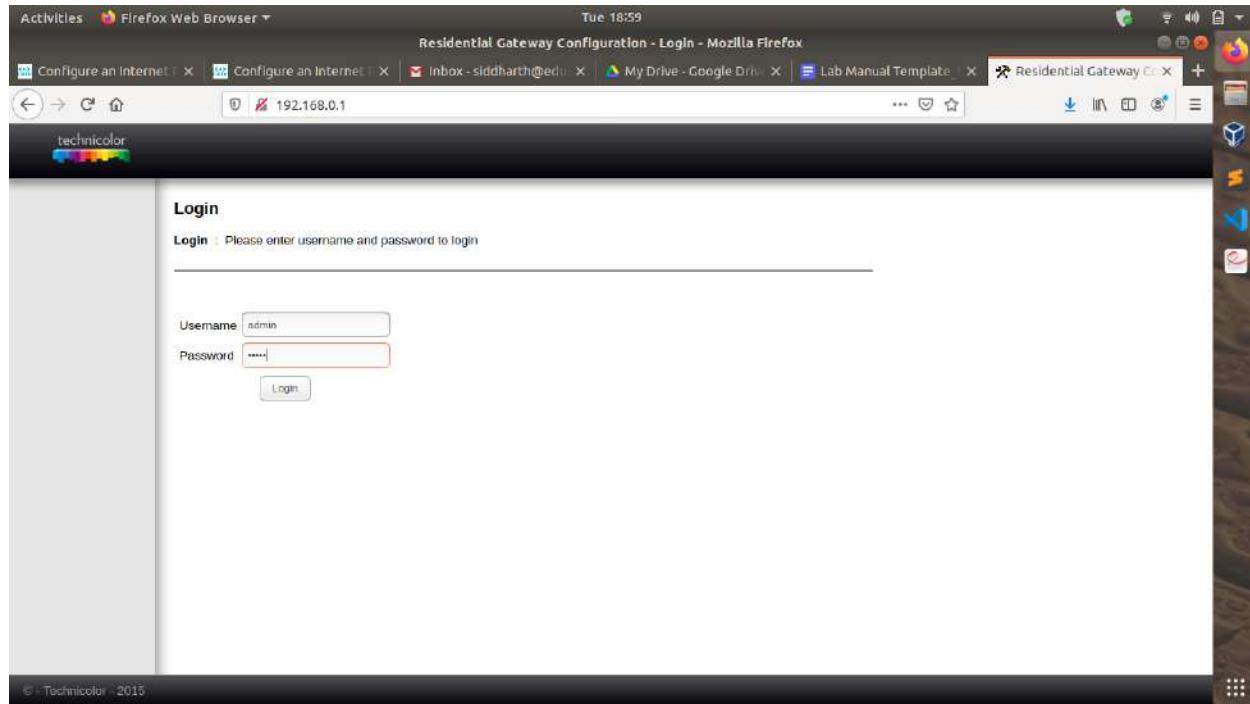
List of Hardware/Software requirements:

- Computer with 500GB Hard Disk
- 8 GB Ram
- Hathway Wifi Router

Procedure:

- Ensure that no one can easily connect to your wireless network and use the Internet without any permission.
- Personalize access on who can configure your wireless settings.
- Protect all data that is transmitted through the wireless network

1. Open the browser enter url on Address bar, enter your router's local IP Address then press enter. When the login credential appears, enter your router's Username and Password.



You will now be redirected to the main screen of the status page.

The screenshot shows the 'Software' section of the gateway's configuration interface. The left sidebar includes links for Software, Connection, Password, Diagnostics, Event Log, Initial Scan, Switch Mode, and Backup/Restore. The main content area displays the following information:

Information	
Standard Specification Compliant	DOCSIS 3.0
Hardware Version	1.0
Software Version	STFL.86.02
Cable Modem MAC Address	50:09:59:ef:6e:9d
Cable Modem Serial Number	00040836501911
CM Certificate	Installed

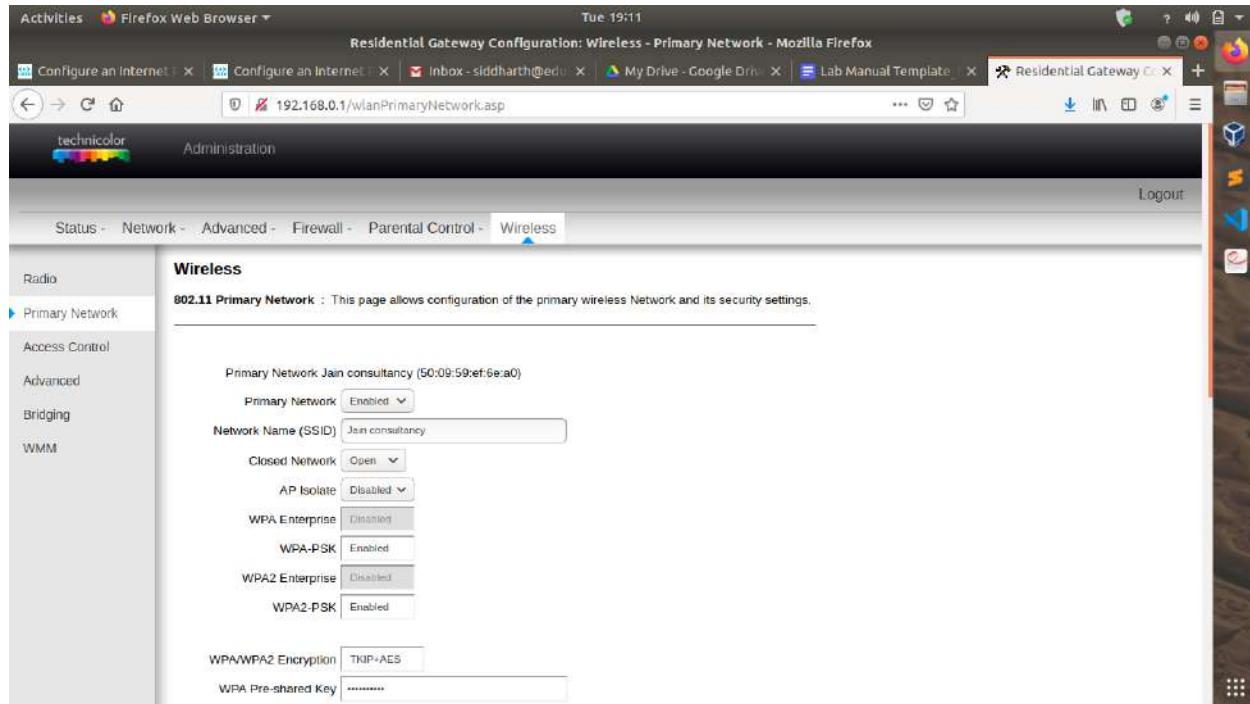
Status	
System Up Time	0 days 02h:29m:08s
Network Access	Allowed
Cable Modem IP Address	-----,----,----

After clicking on the Wireless Tab

The screenshot shows a Mozilla Firefox browser window titled "Residential Gateway Configuration: Wireless - Radio Configuration - Mozilla Firefox". The address bar displays "192.168.0.1/wlanRadio.asp". The main content area shows the "Wireless" configuration page for a "Radio" interface. The left sidebar lists options: Primary Network, Access Control, Advanced, Bridging, and WMM. The main panel displays various configuration parameters for the 802.11 Radio:

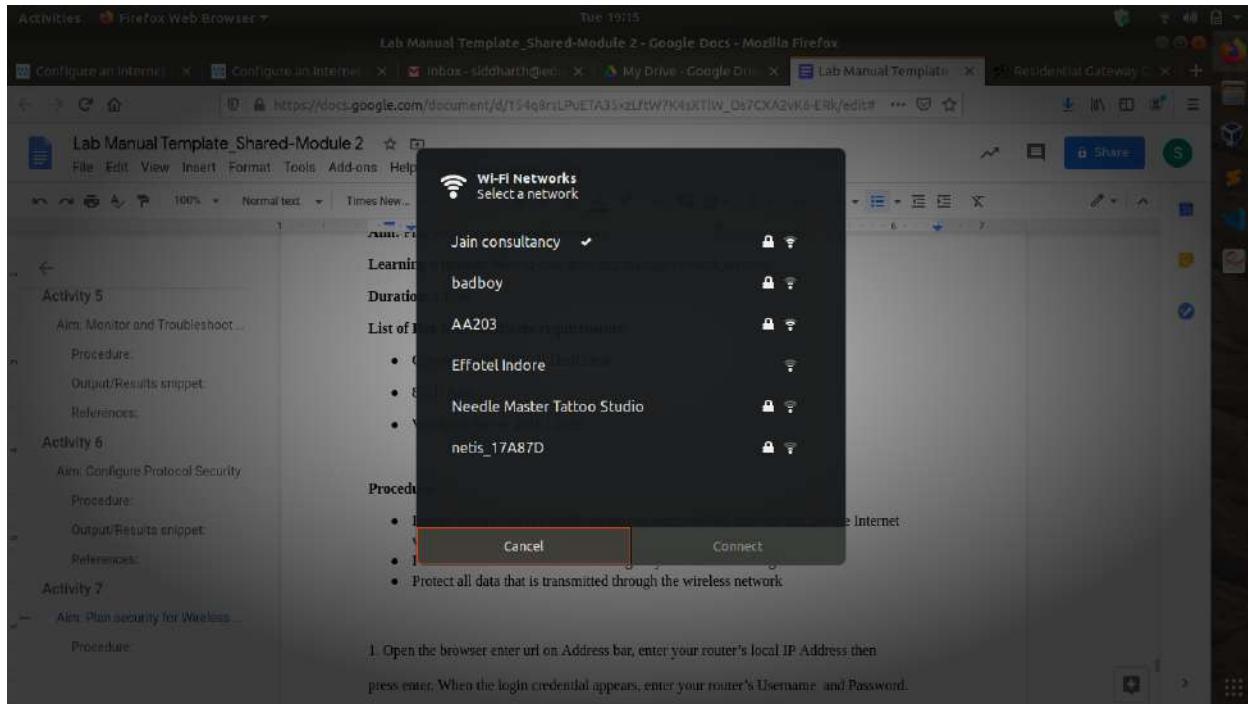
- Interface: Embedded
- Wireless MAC Address: 50:09:59:EF:8E:A0
- Output Power: 100%
- 802.11 Band: 2.4 GHz (Current: 2.4 GHz)
- 802.11 n-mode: Auto
- Bandwidth: 40 MHz (Current: 20MHz)
- Sideband for Control Channel (40 MHz only): Upper (Current: Lower)
- Channel: 11
- Current Channel: 11
- Interference Level: Acceptable
- TPC Mitigation (dB): 0 (Off)
- OBSS Coexistence: 1 (Enabled)
- ETCS TV: Auto

You can now select Primary Network modes which you can choose from WEP, WPA Personal, WPA2 Personal, and WPA2/WPA Mixed Mode.



Output/Results snippet:

Note: Your wifi Network will appear as secured when you set password.



References:

23. etutorials.org/Networking/
24. <https://www.hatway.com/>
25. <https://www.thewindowsclub.com/>

Activity 7

Aim: Install and Configure Different Antivirus Software

Learning outcome: Able to configure and manage network security.

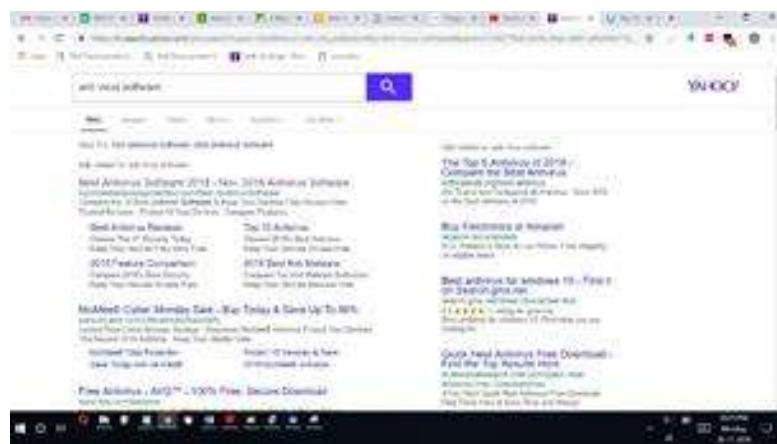
Duration: 2 hour

List of Hardware/Software requirements:

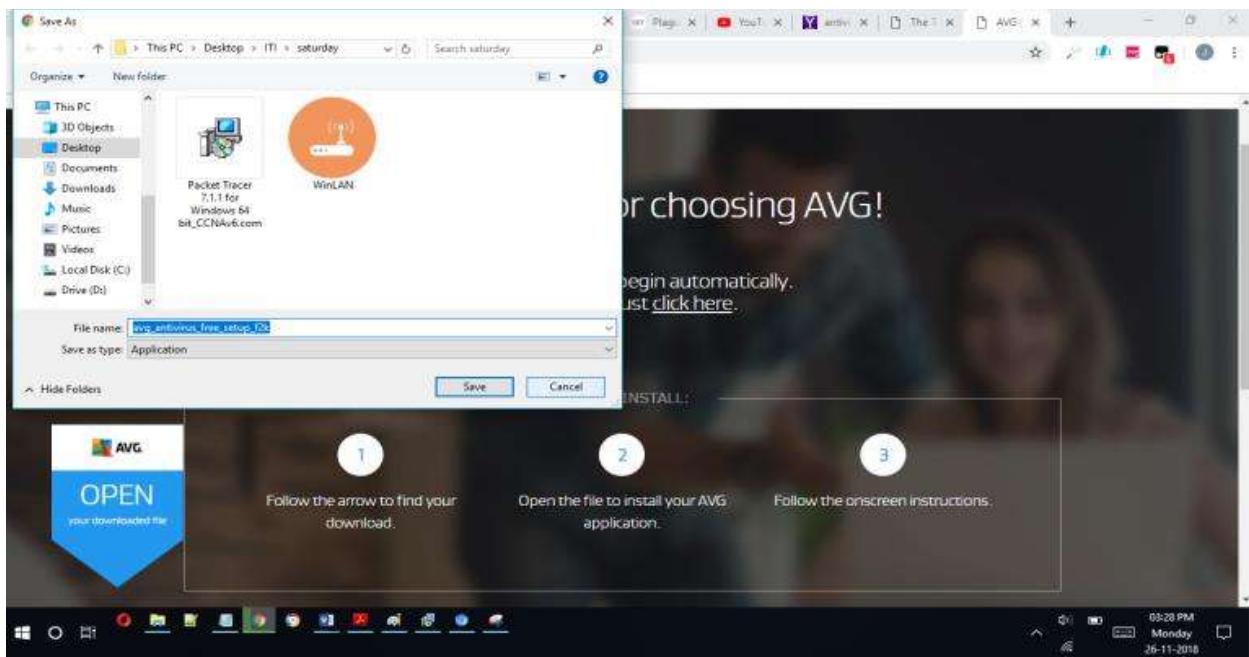
- Computer with 500GB Hard Disk
 - 8 GB Ram
 - Windows Server 2016 / 2019

Procedure:

Browse for the antivirus software and click on any software which you feel comfortable.



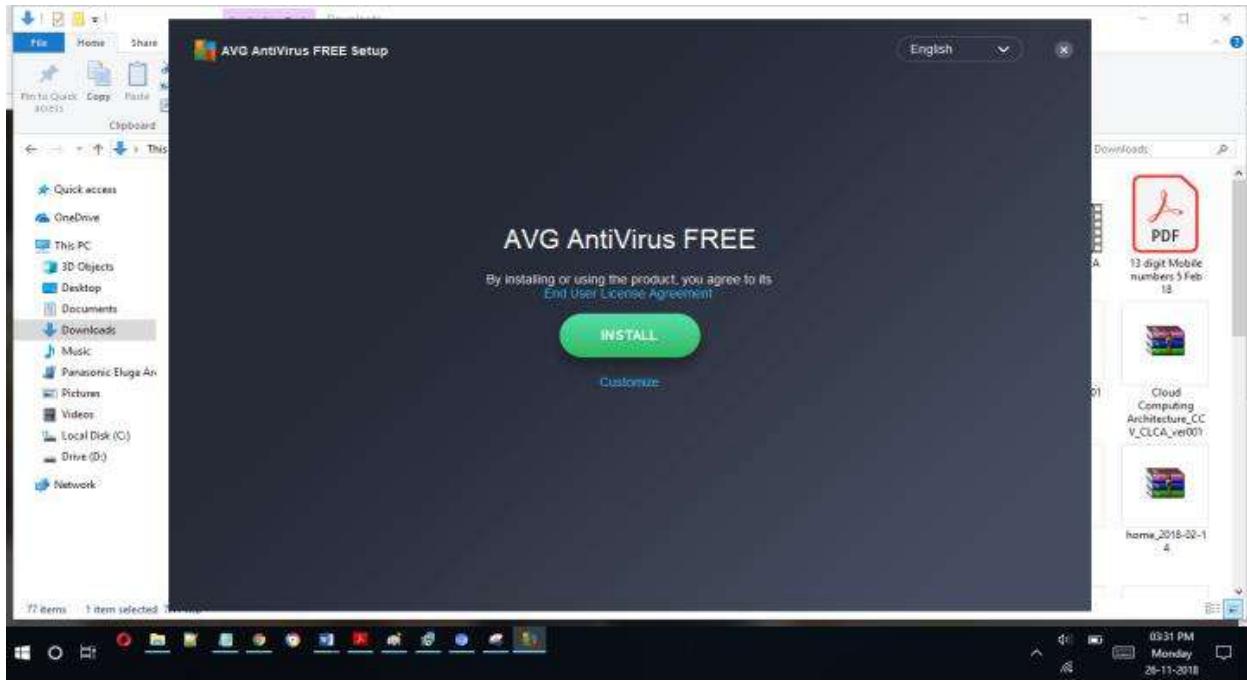
Click on free download and save the file. After that double click on that file.



Click on install, it will ask to restart the computer.

Output/Results snippet:

Note: Now the antivirus software is installed in your computer.



References:

26. etutorials.org/Networking/
27. <https://www.avast.com/>
28. <https://www.thewindowsclub.com/>

Activity 8

Aim: Install and Configure Admin Console

Learning outcome: Able to configure and manage network security.

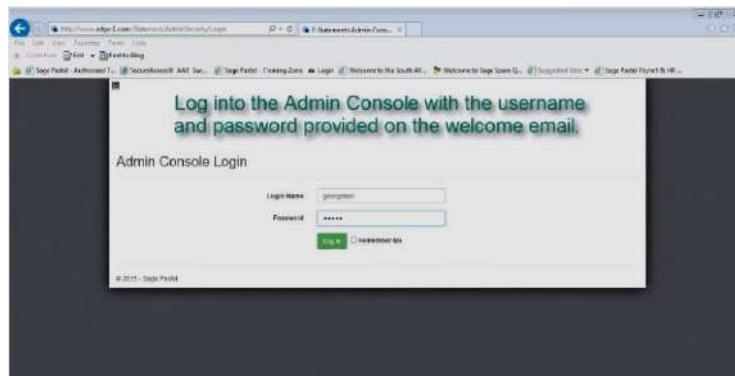
Duration: 3 hour

List of Hardware/Software requirements:

1. Personal Computer
2. Microsoft Windows 10 operating system

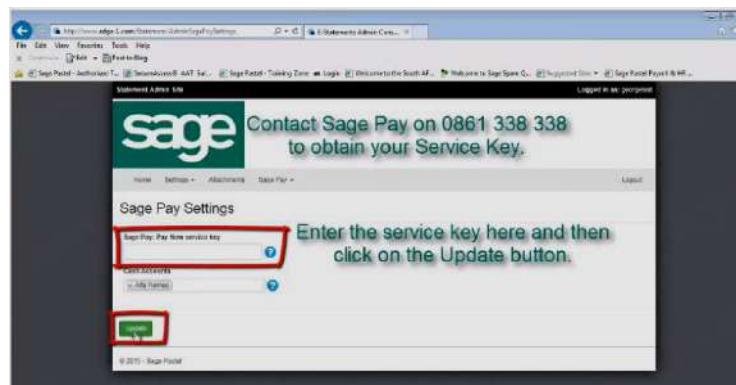
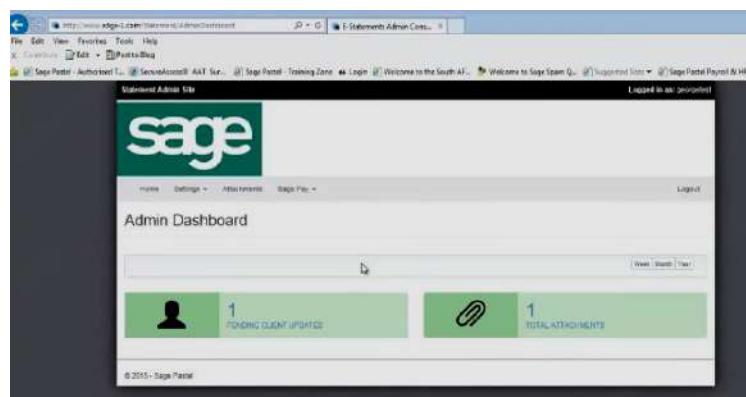
Code/Program/Procedure (with comments):

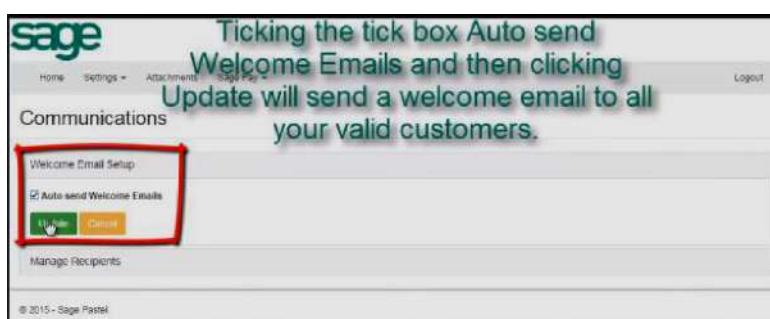
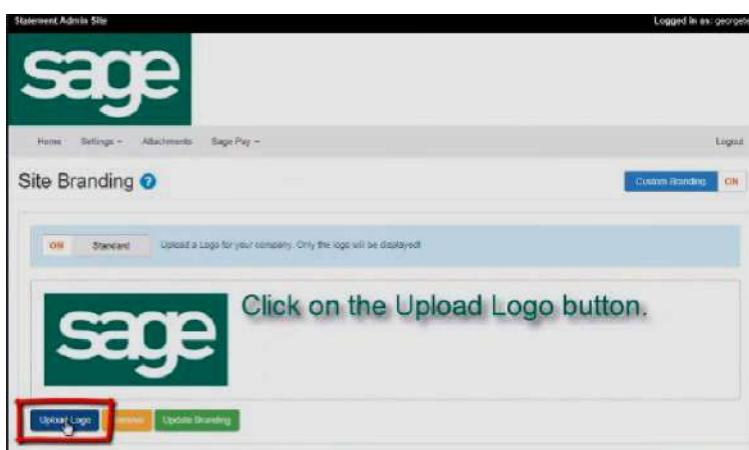
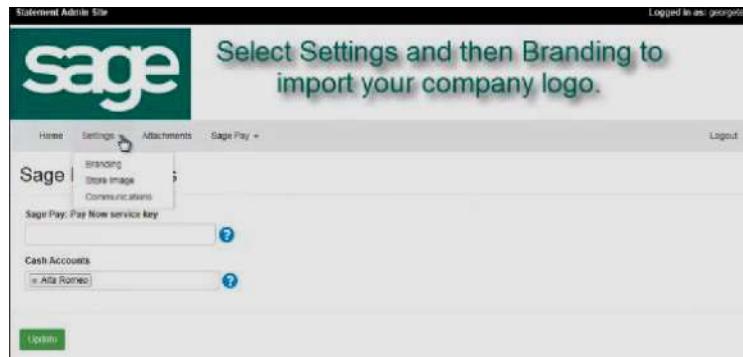
1. First need to Login the Admin console, enter valid credential and click on login.

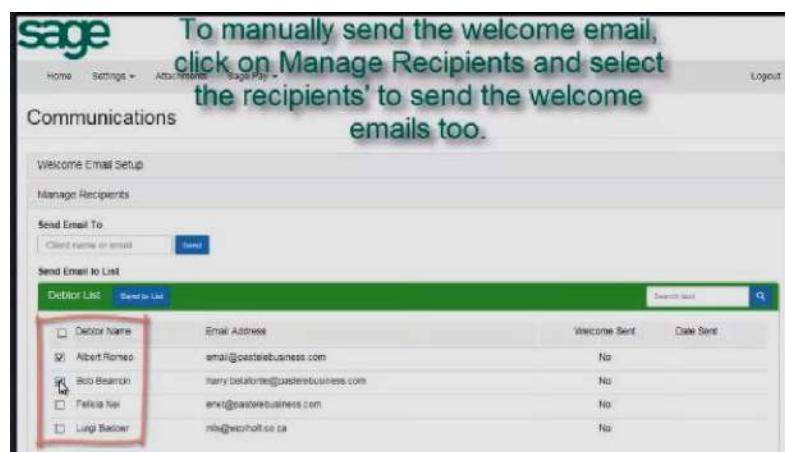




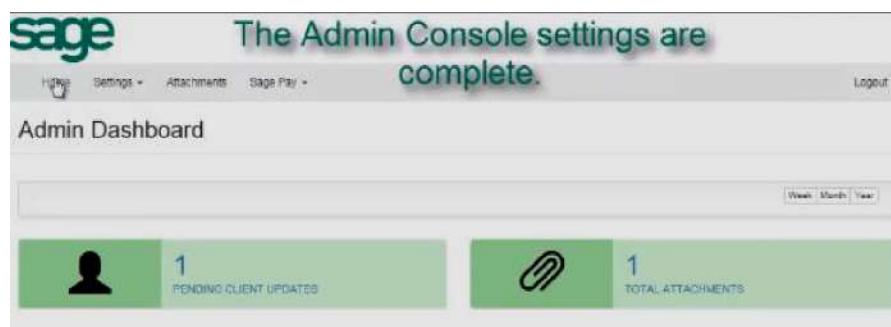
2. Select the sage pay from the menu and then select the settings.







Output/Results snippet:



References:

29. <https://www.sagepay.co.uk/support/test-your-integration/log-in-to-test-my-sage-pay>

Activity 9

Aim: Configure a Local Security Policies

Learning outcome: Able to configure and manage network security.

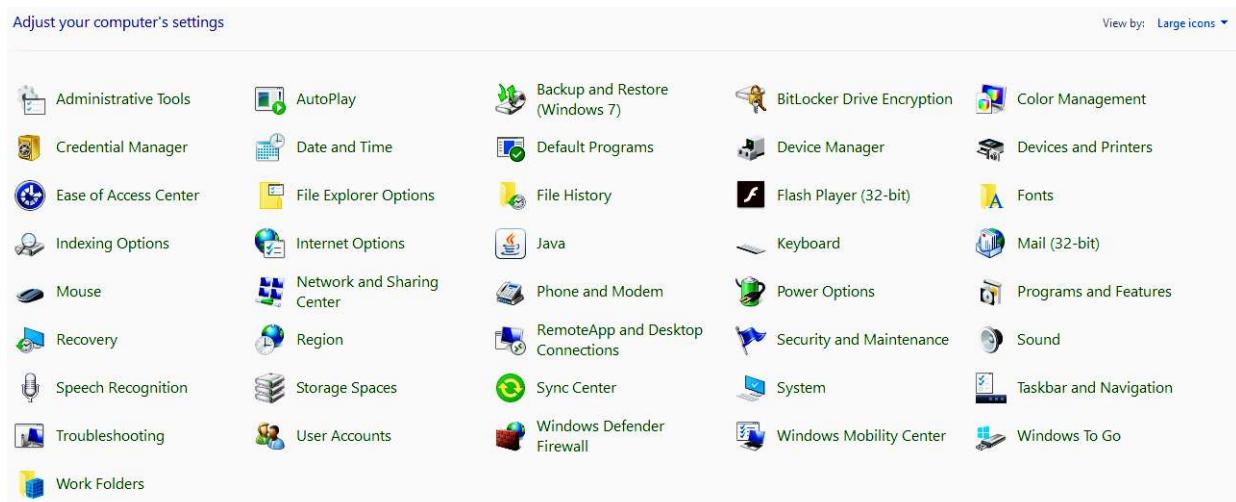
Duration: 2 hour

List of Hardware/Software requirements:

1. Personal Computer with minimum 4 GB RAM & 50 GB HDD
2. Microsoft Windows 10 operating system

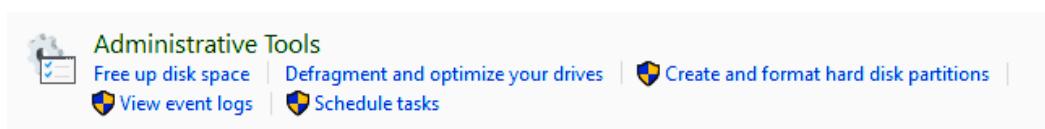
Code/Program/Procedure (with comments):

1. Open Control Panel.
2. The Control Panel items should be listed as "Large" or "Small icons", click on Administrative Tools.





3. If the Control Panel items are displayed by "Category", click System and Security, and then click Administrative Tools.

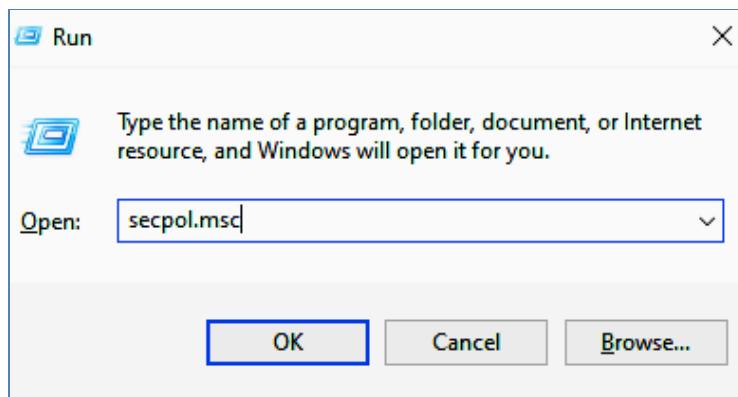


4. In the list of the tools find and double-click the Local Security Policy shortcut.

Name	Date modified	Type	Size
Component Services	3/19/2019 10:15 AM	Shortcut	2 KB
Computer Management	3/19/2019 10:15 AM	Shortcut	2 KB
Defragment and Optimize Drives	3/19/2019 10:15 AM	Shortcut	2 KB
Disk Cleanup	3/19/2019 10:15 AM	Shortcut	2 KB
Event Viewer	3/19/2019 10:15 AM	Shortcut	2 KB
iSCSI Initiator	3/19/2019 10:15 AM	Shortcut	2 KB
Local Security Policy	3/19/2019 10:16 AM	Shortcut	2 KB
ODBC Data Sources (32-bit)	3/19/2019 10:16 AM	Shortcut	2 KB
ODBC Data Sources (64-bit)	3/19/2019 10:15 AM	Shortcut	2 KB
Performance Monitor	3/19/2019 10:15 AM	Shortcut	2 KB
Print Management	3/19/2019 10:16 AM	Shortcut	2 KB
Recovery Drive	3/19/2019 10:15 AM	Shortcut	2 KB
Registry Editor	3/19/2019 10:15 AM	Shortcut	2 KB
Resource Monitor	3/19/2019 10:15 AM	Shortcut	2 KB
Services	3/19/2019 10:15 AM	Shortcut	2 KB
System Configuration	3/19/2019 10:15 AM	Shortcut	2 KB
System Information	3/19/2019 10:15 AM	Shortcut	2 KB
Task Scheduler	3/19/2019 10:14 AM	Shortcut	2 KB
Windows Defender Firewall with Advanc...	3/19/2019 10:14 AM	Shortcut	2 KB
Windows Memory Diagnostic	3/19/2019 10:15 AM	Shortcut	2 KB

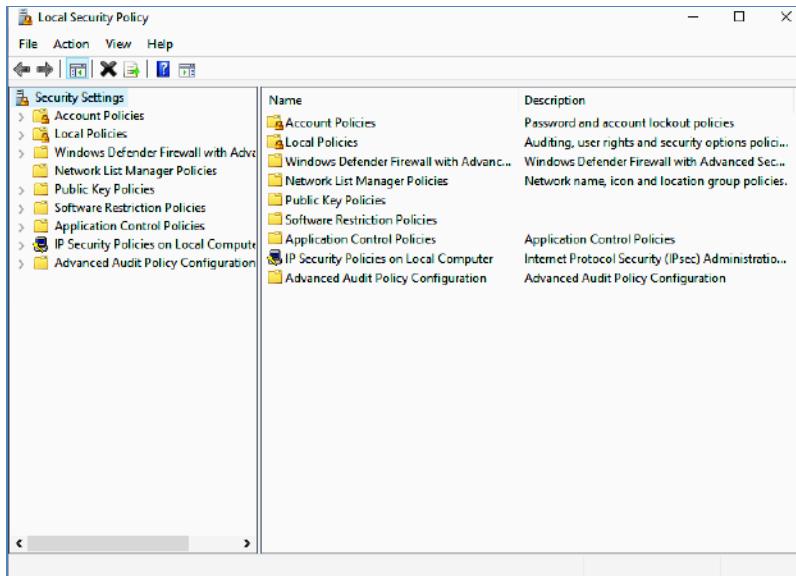


- Also, as a shortcut you can open Run or Command Prompt and type **secpol.msc** and press enter.



- You will get Local Security Policy access for further activities of configuration.

Output/Results snippet:



References:

30. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/how-to-configure-security-policy-settings>

Activity 10

Aim: Configure Domain Security Policies

Learning outcome: Able to configure and manage network security.

Duration: 3 hour

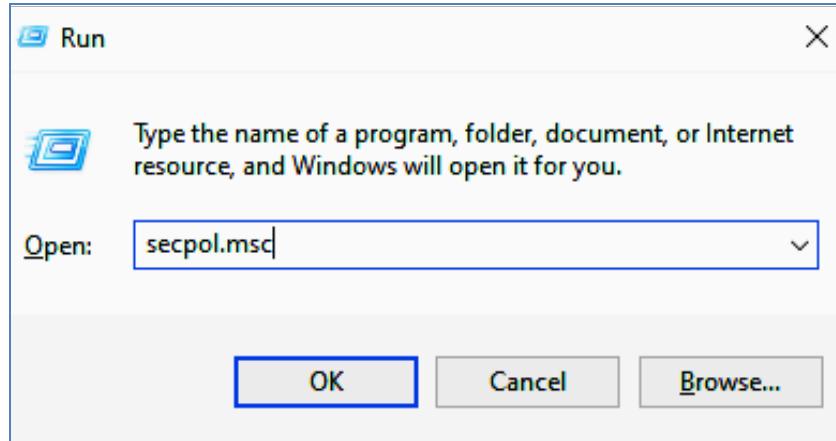
List of Hardware/Software requirements:

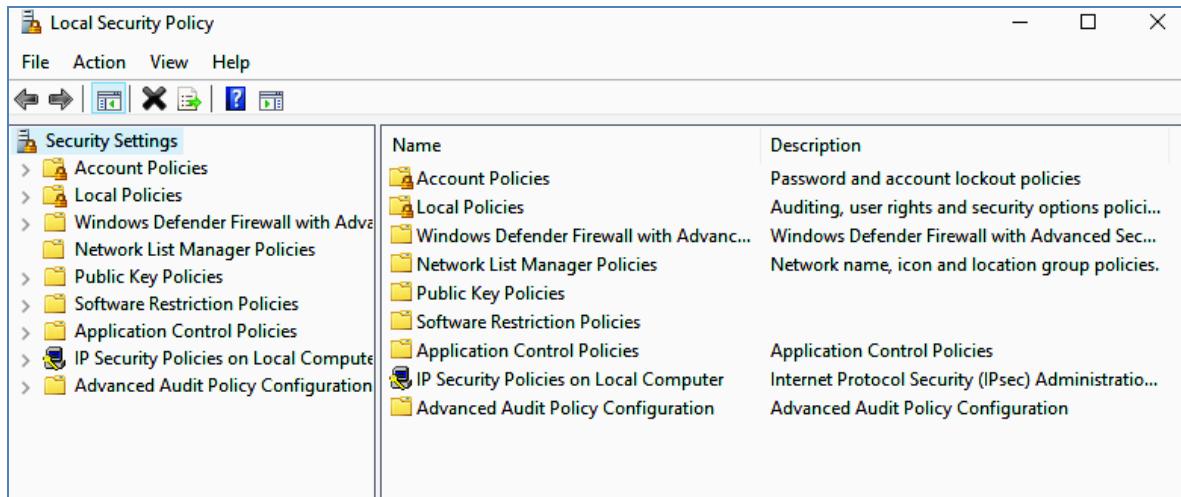
1. Personal Computer
2. Microsoft Windows operating system

Code/Program/Procedure (with comments):

The following procedure describes how to configure a security policy setting for only a domain controller (from the domain controller).

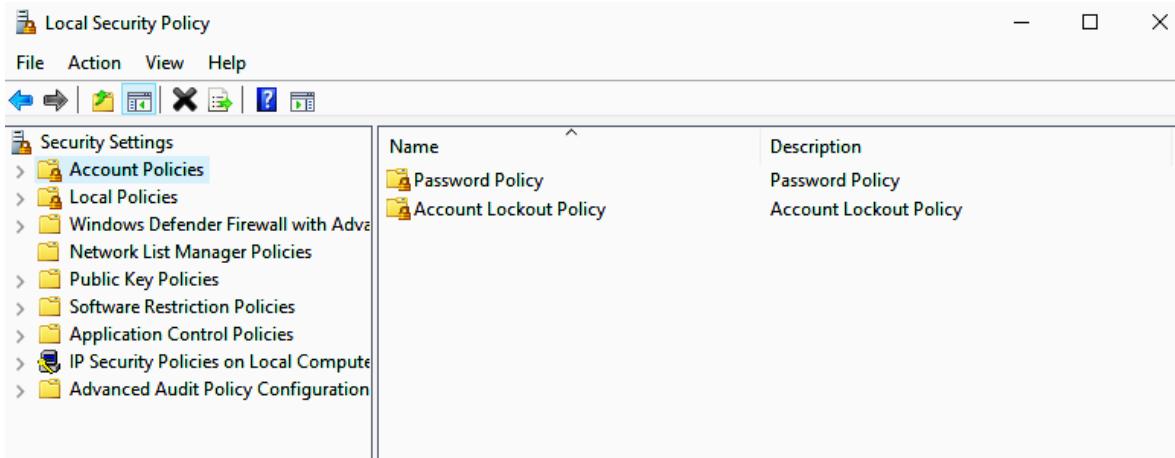
1. To open the domain controller security policy, in the console tree, locate GroupPolicyObject [ComputerName] Policy, click Computer Configuration, click Windows Settings, and then click Security Settings.
2. Alternatively, open Run and type **secpol.msc** and press enter.

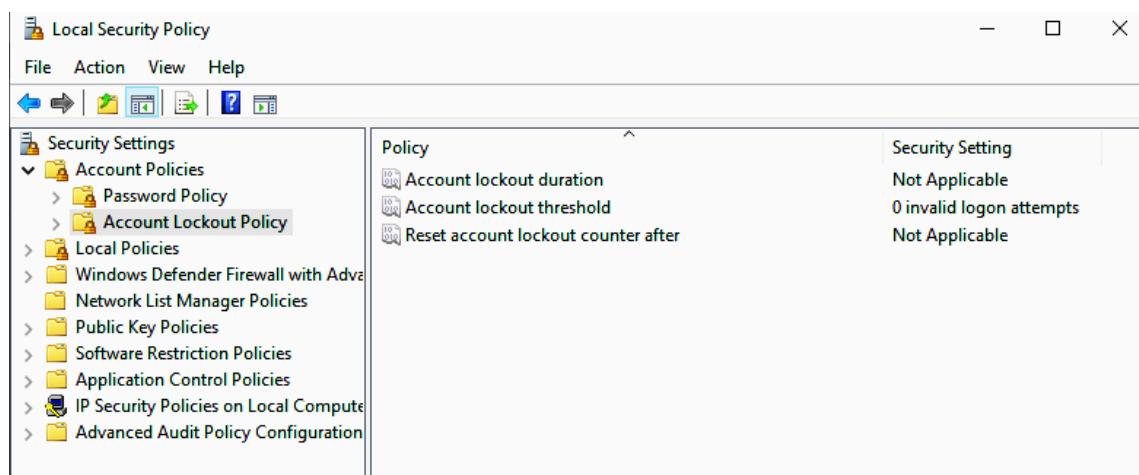
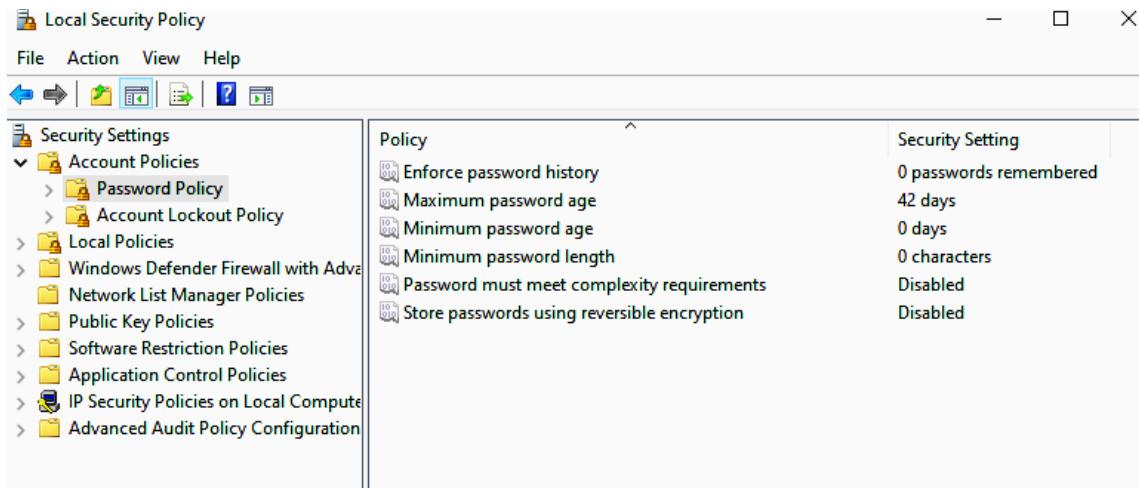




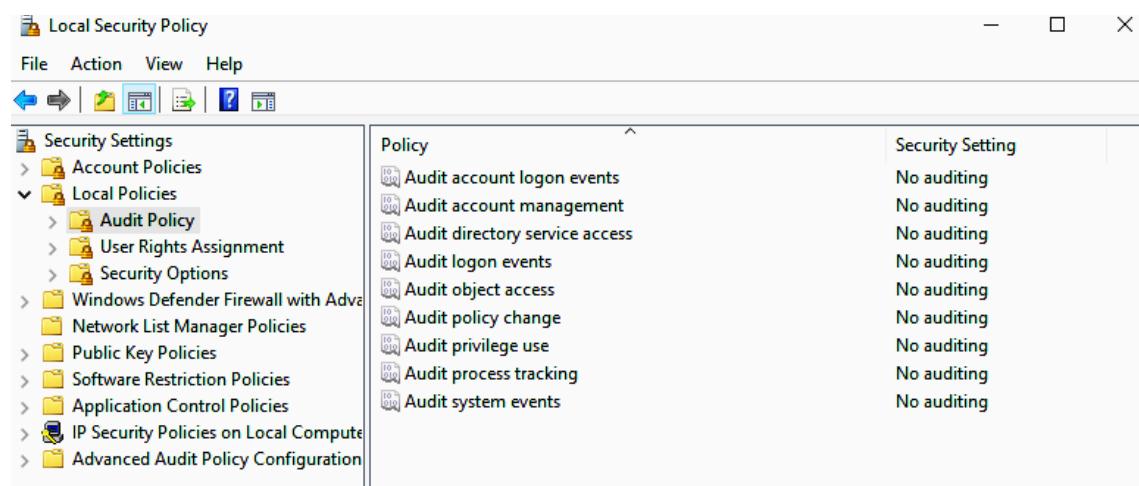
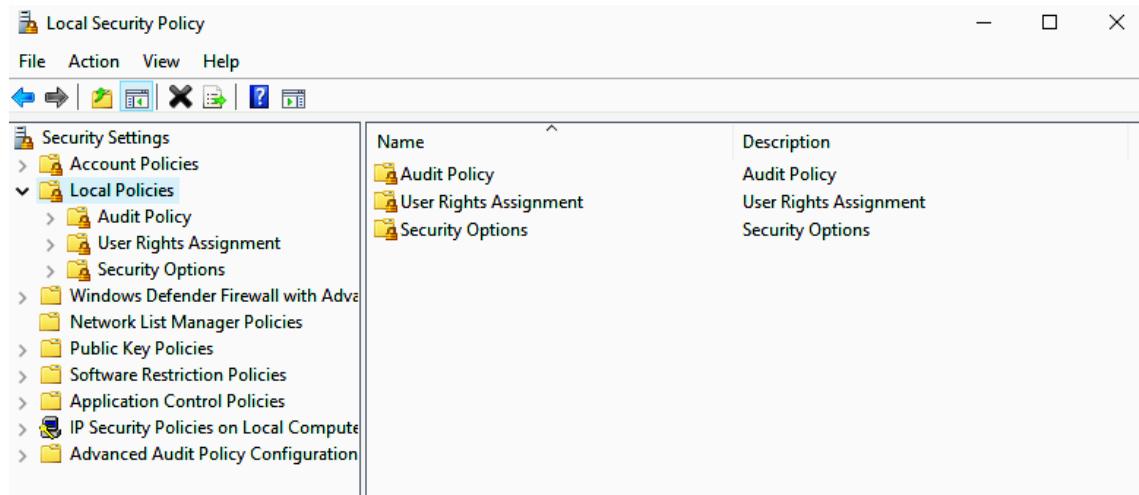
3. Do one of the following:

- Double-click Account Policies to edit the Password Policy, Account Lockout Policy, or Kerberos Policy.





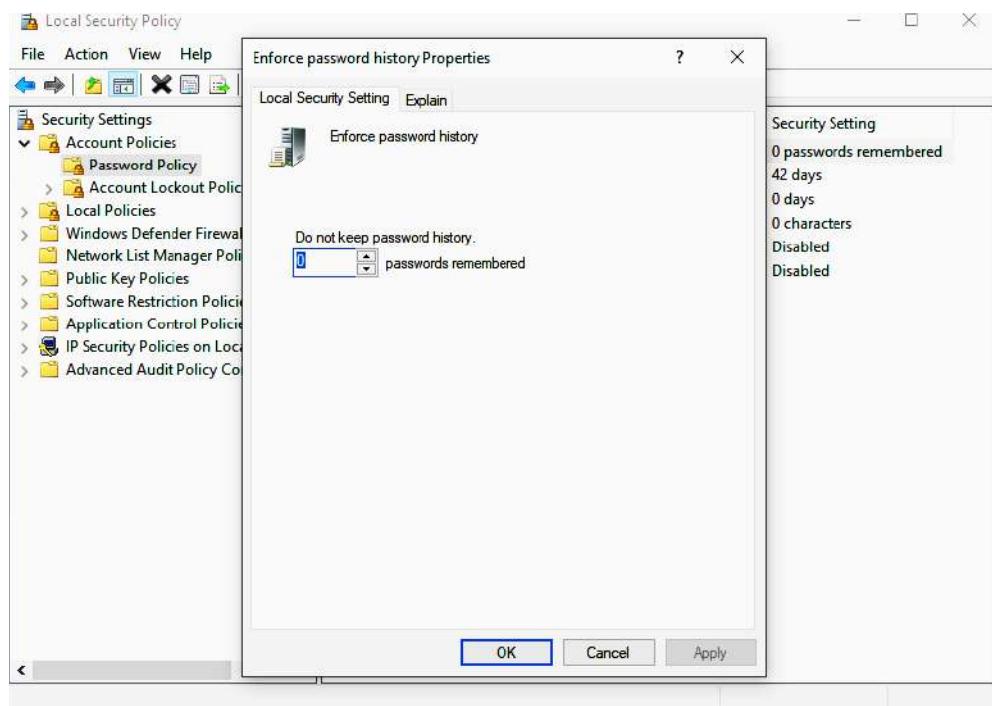
- Click Local Policies to edit the Audit Policy, a User Rights Assignment, or Security Options.



Local Security Policy		
	Policy	Security Setting
>	Access Credential Manager as a trusted caller	Everyone,Administrators...
>	Access this computer from the network	
>	Act as part of the operating system	
>	Add workstations to domain	
>	Adjust memory quotas for a process	LOCAL SERVICE,NETWO...
>	Allow log on locally	Guest,Administrators,U...
>	Allow log on through Remote Desktop Services	Administrators,Remote ...
>	Back up files and directories	Administrators,Backup ...
>	Bypass traverse checking	Everyone,LOCAL SERVIC...
>	Change the system time	LOCAL SERVICE,Admini...
>	Change the time zone	LOCAL SERVICE,Admini...
>	Create a pagefile	Administrators
>	Create a token object	LOCAL SERVICE,NETWO...
>	Create global objects	
>	Create permanent shared objects	
>	Create symbolic links	Administrators
>	Debug programs	Administrators
>	Deny access to this computer from the network	Guest
>	Deny log on as a batch job	
>	Deny log on as a service	
>	Deny log on locally	Guest
>	Deny log on through Remote Desktop Services	
>	Enable computer and user accounts to be trusted for delegation	

Local Security Policy		
	Policy	Security Setting
>	Accounts: Administrator account status	Disabled
>	Accounts: Block Microsoft accounts	Not Defined
>	Accounts: Guest account status	Disabled
>	Accounts: Limit local account use of blank passwords to co...	Enabled
>	Accounts: Rename administrator account	Administrator
>	Accounts: Rename guest account	Guest
>	Audit: Audit the access of global system objects	Disabled
>	Audit: Audit the use of Backup and Restore privilege	Disabled
>	Audit: Force audit policy subcategory settings (Windows Vis...	Not Defined
>	Audit: Shut down system immediately if unable to log secur...	Disabled
>	DCOM: Machine Access Restrictions in Security Descriptor D...	Not Defined
>	DCOM: Machine Launch Restrictions in Security Descriptor ...	Not Defined
>	Devices: Allow undock without having to log on	Enabled
>	Devices: Allowed to format and eject removable media	Not Defined
>	Devices: Prevent users from installing printer drivers	Disabled
>	Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
>	Devices: Restrict floppy access to locally logged-on user only	Not Defined
>	Domain controller: Allow server operators to schedule tasks	Not Defined
>	Domain controller: LDAP server signing requirements	Not Defined
>	Domain controller: Refuse machine account password chan...	Not Defined
>	Domain member: Digitally encrypt or sign secure channel d...	Enabled
>	Domain member: Digitally encrypt secure channel data (wh...	Enabled
>	Domain member: Digitally sign secure channel data (when ...	Enabled

4. In the details pane, double-click the security policy that you want to modify. If this security policy has not yet been defined, select the Define these policy settings check box.
5. Modify the security policy setting, and then click OK.

Output/Results snippet:**References:**

31. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/how-to-configure-security-policy-settings>

Activity 11

Aim: Configure RRAS Policies

Learning outcome: Able to configure and manage network security.

Duration: 2 hour

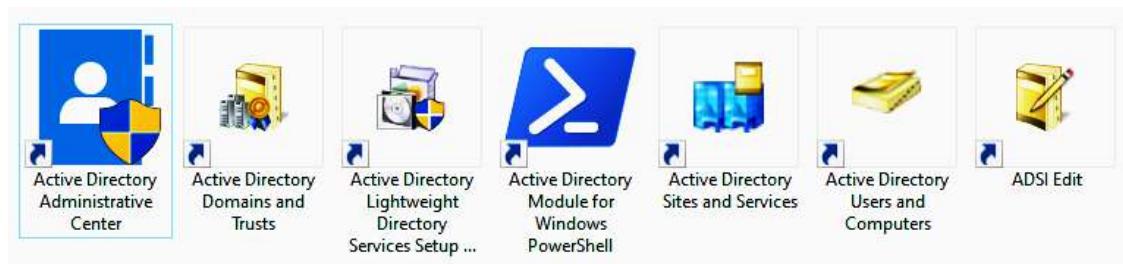
List of Hardware/Software requirements:

1. Personal Computer
2. Microsoft Windows 10 operating system

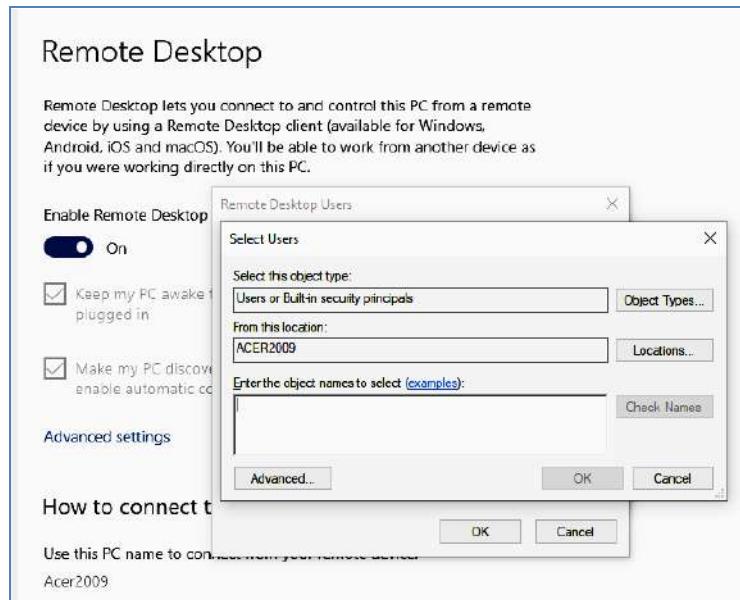
Code/Program/Procedure (with comments):

It uses policies to create and stored in Network Policy Server to finely control remote access.

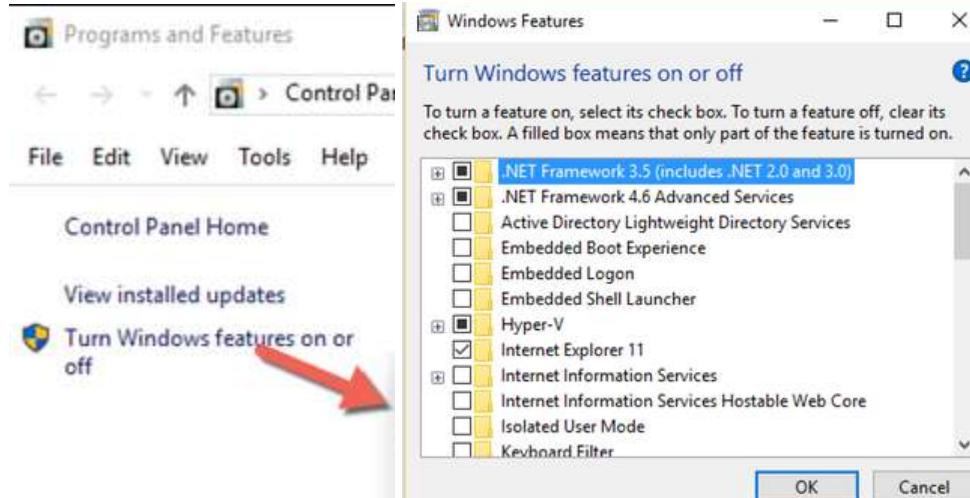
1. Configure the user accounts to use remote access policy for dial-in access.
2. Click Start > Programs > Administrative Tools > Active Directory Users and Computers.



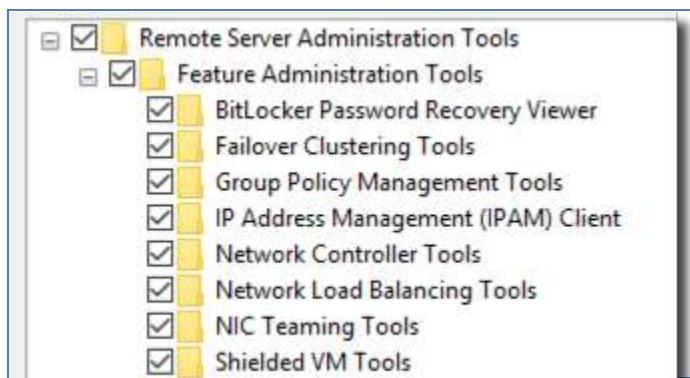
3. Verify that the user accounts have the Remote Access Permission (Dial-in or VPN) option set to Control access through Remote Access Policy.
4. Open the Routing and Remote Access management console to configure the policy, then click Start > Programs > Administrative Tools > Routing and Remote Access.



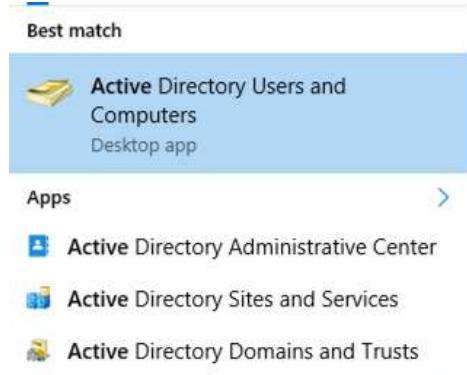
5. If necessary, double-click Routing and Remote Access and the server name.
6. In the left pane, right-click Remote Access Policies, then click New Remote Access Policy.
7. Select the appropriate policy settings as discussed above.
8. Delete the default policies.
9. Head over to Programs and Features in the Control Panel and click on Turn Windows features on or off.



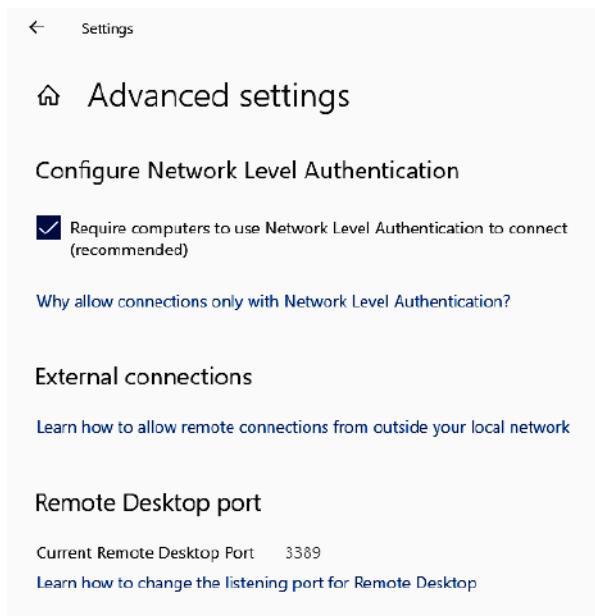
10. At this point, scroll down until you see the Remote Server Administration Tools section.
Under this, you'll see lots of different tools to enable.



11. From here, you can enable and disable any of the toolsets that you want or would rather not have. Once you've done this, you can then find any of these tools by typing a subset of the name into the Cortana search bar.



Output/Results snippet:



References:

32. <https://docs.microsoft.com/en-us/windows-server/remote/remote-access/ras/manage-remote-clients/install/step-1-configure-the-remote-access-infrastructure>
33. <https://www.businessnewsdaily.com/10996-windows-10-remote-server-administration-tools-rsat.html>

34. <https://blog.netwrix.com/2017/01/30/active-directory-users-and-computers-aduc/>

Learning Outcome 7 - Able to configure and perform remote accessing & routing

After achieving this learning outcome, a student will be Able to configure and perform remote accessing & routing. In order to achieve this learning outcome, a student has to complete the following:

1. Manage TCP/IP Routing (5 Hrs)
2. Configure Remote Access Authentication Protocol (5 Hrs)
3. Connect remote Desktop using RemoteAssistance(5 Hrs)
4. Connect Remote Desktop using Telnet (3Hrs)
5. Connect Remote Desktop using HyperTerminal (2 Hrs)
6. Connect Remote Desktop using Team Viewer (5Hrs)

Activity 1

Aim: Manage TCP/IP Routing

Learning outcome: Able to configure and perform remote accessing & routing.

Duration: 5 hour

List of Hardware/Software requirements:

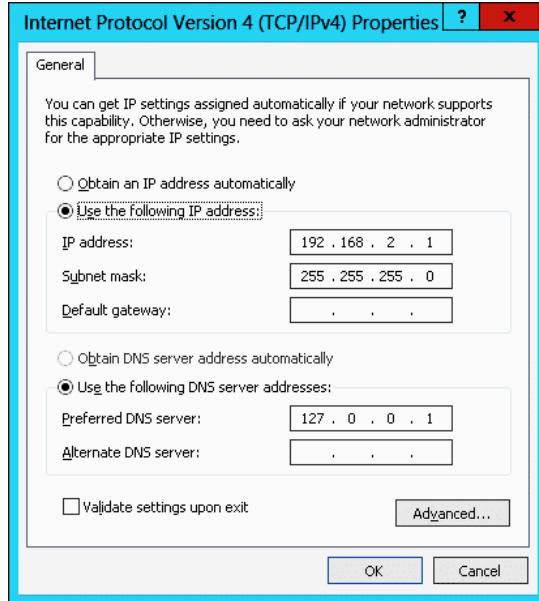
1. Personal Computer
2. Microsoft Windows Server

Code/Program/Procedure (with comments):

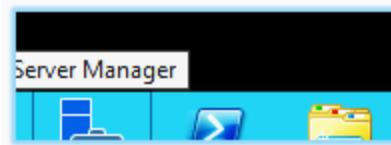
Instead of spending a hardware-based router from a vendor like Cisco, Windows Server 2003 can be used as a software-based router. It supports both static routing and dynamic routing with Open Shortest Path First (OSPF) which uses link state routing and Routing Information Protocol (RIP V2) which uses distance vector routing.

One of the advantages is that a hardware-based router usually has over a Windows router is the number and types of interfaces offered. A Windows router is narrow by its number of network cards, and other interfaces, that may be installed. Before to use Windows Server 2003 as a router, the user must enable Routing and Remote Access. All of the routing utilities in Windows can be configured with the RRAS MMC snap-in.

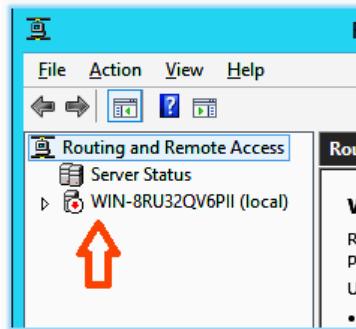
1. Open PowerShell, type 'control panel' and press enter. Select network and sharing center.
2. Click on change adapter settings. Right click on the Ethernet adapter that's connected to your switch and select rename. Change its name to LAN.
3. Now double click on the LAN adapter and select properties. Next, highlight TCP/IPv4 and change the configuration to the one shown below. Note: Do not enter a default gateway for the LAN. Only the WAN should have a default gateway. Make sure the LAN interface is connected to a switch.



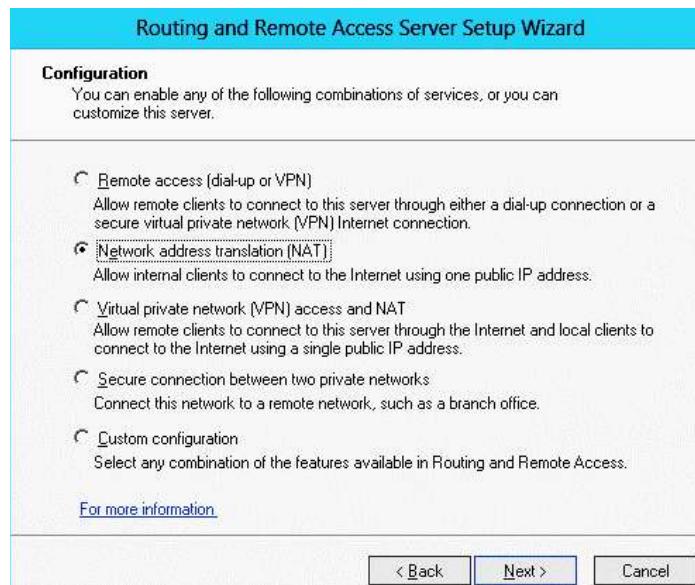
4. Next, click on the server manager icon on the bottom left hand side of the desktop.



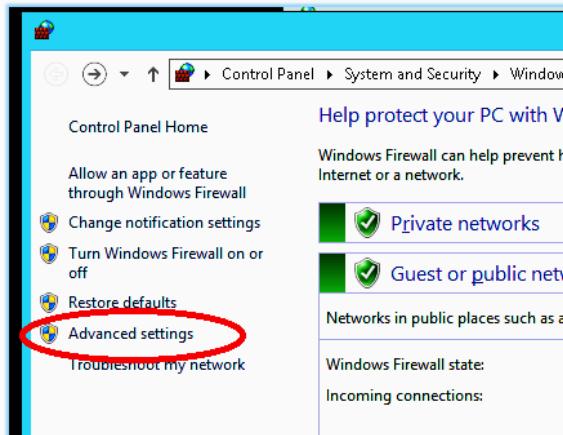
5. In the server manager, click on manage > add roles and features.
6. From the server list, select your server. Finally, add the server roles:
 - a. DHCP Server
 - b. DNS Server
 - c. Remote Access
7. Click next until you reach Remote Access role services. Place a checkmark by DirectAccess and VPN as well as by Routing. Finish the installation.



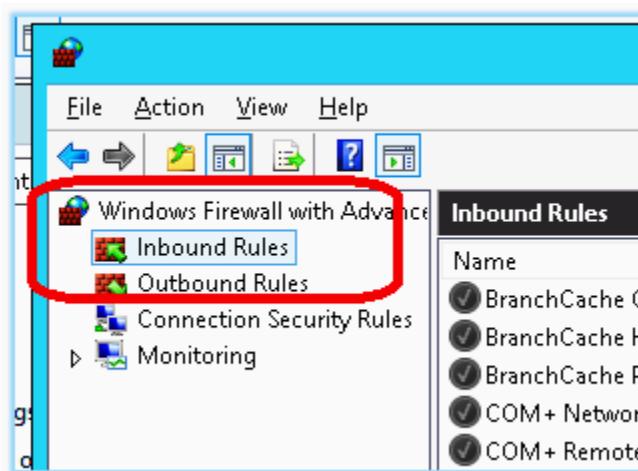
8. Right click on the server name and select configure and enable routing and remote access.
9. In the setup wizard, select network address translation (NAT)



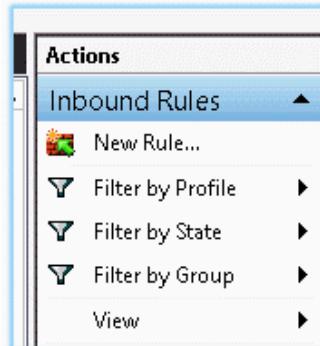
10. Open PowerShell and type firewall and press enter. Windows firewall console will display. Click Advanced Settings.



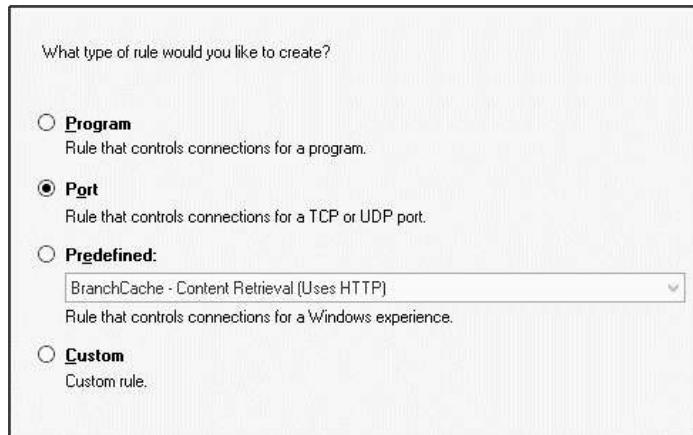
11. In Windows Firewall with Advanced Security, click on inbound rules.



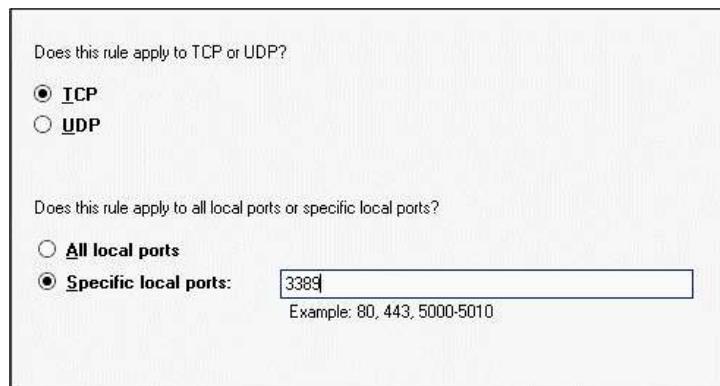
12. To add an inbound rule, highlight inbound rule and select new rule from the actions pane.



13. The new inbound rule wizard will appear. Follow these steps to add a rule for Remote Desktop: Select a port to allow.



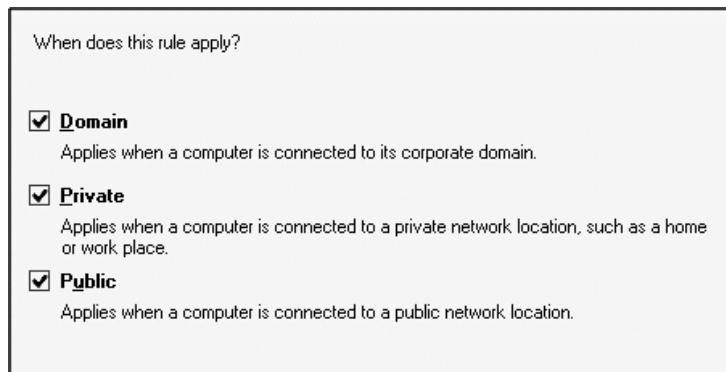
14. Select the protocol and port number.



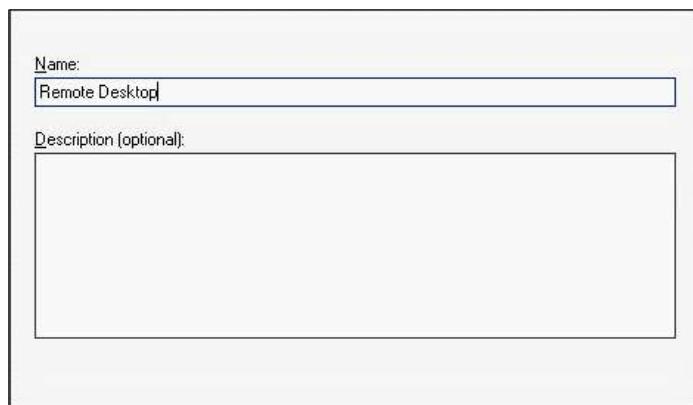
Does this rule apply to all local ports or specific local ports?

- All local ports
 Specific local ports:
Example: 80, 443, 5000-5010

15. Select the zone where the firewall will allow traffic to traverse.



16. Give the rule a friendly name and click finish.



17. After finishing, it's a good idea to run NMap to make sure that only the specified ports are open.

Output/Results snippet:

Hosts	Services	Nmap Output	Ports / Hosts	Topology	Host Details	Scans
OS	Host					
	██████████		Port Protocol State Service Version			
			3389 tcp open			

References:

- <https://www.falconitservices.com/support/KB/Lists/Posts/Post.aspx?ID=77>

Activity 2

Aim: Configure Remote Access Authentication Protocol

Learning outcome: Able to configure and perform remote accessing & routing.

Duration: 5 hour

List of Hardware/Software requirements:

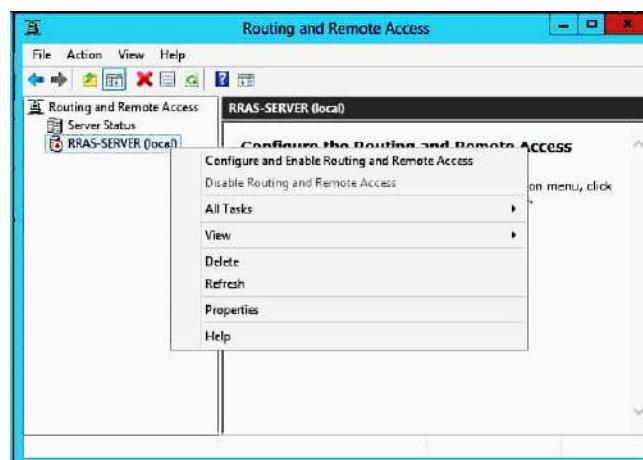
3. Personal Computer
4. Microsoft Windows Server

Code/Program/Procedure (with comments):

The authentication methods can be selected from the Routing and Remote Access > Remote Access Policies folder by double-clicking a policy, then selecting to edit that policy's settings, and finally working to the Authentication tab for the policy as shown below.

Configuring Authentication Protocols:

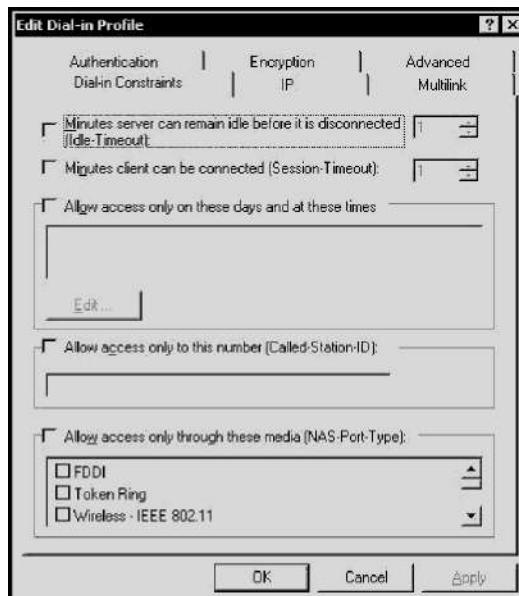
1. Open the RRAS MMC snap-in by selecting Start > Administrative Tools > Routing And Remote Access.



2. Navigate to the server whose authentication support you want to change. Choose the server and then select Action > Properties to open the server Properties dialog box.

3. Switch to the Security tab and make sure that Windows Authentication is selected in the Authentication Provider drop-down.
4. Click the Authentication Methods button. When the Authentication Methods dialog box looks, Extensible Authentication Protocol (EAP).
5. Select the two MS-CHAP checkboxes, then select the CHAP checkbox and verify that the SPAP and PAP checkboxes are cleared.
6. Verify that Allow Remote Systems To Connect Without Authentication checkbox is cleared and click OK.
7. When the server Properties dialog box reappears, click OK.
8. When asked if you want to view the help files associated with configuring authentication protocols click No to finish this activity.

Output/Results snippet:



References:

- <https://www.serverbrain.org/security-administration-2003/configuring-rras-authentication-protocols.html>

Activity 3

Aim: Connect remote Desktop using RemoteAssistance.

Learning outcome: Able to configure and perform remote accessing & routing.

Duration: 5 hour

List of Hardware/Software requirements:

1. Any kind of Laptop/ Desktop with internet connection
2. Windows 8 OS

Code/Program/Procedure (with comments):

1 - On the Computer That the user Wants To CONNECT TO Open the Windows 8 System folder. In Windows 8, swipe in from the right edge of the screen. Tap Search.



Image: Desktop

2. Type remote in the Search Text Box field.
3. Click Settings, located on the right.

-
4. Click Allow Remote Access to your computer, located on the left

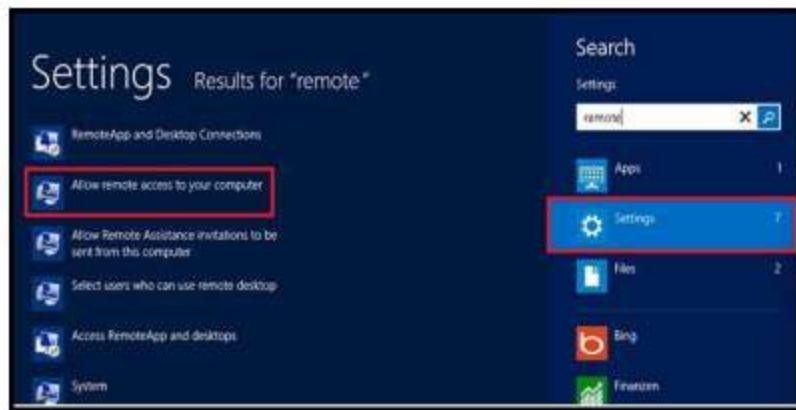


Image: Settings

5. Enter the system Admin Password or confirm your Choice, if requested.
6. Select the checkbox - Allow users to connect remotely to this computer, located in the lower section.
7. Uncheck the checkbox option, allow connection only from computers running Remote Desktop with Network Level Authentication (recommended).
8. Click the Select Users button of the window. (FWindow Remote Assistance)

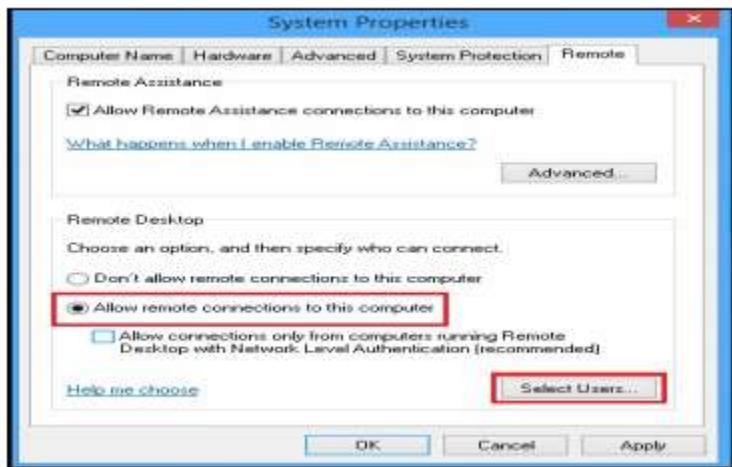


Image: Select user button

9. Add your PAWS ID and any other users that need access to remotely connect to your computer using Remote Desktop.

10. Click the OK button to save your changes that have added all necessary Remote Desktop Users.



Image:Remote Desktop Users

Output/Results snippet:

The connection will now be established. According to the Quick Assist dialog, it may take a few minutes before the devices connect, so you may have to be patient.

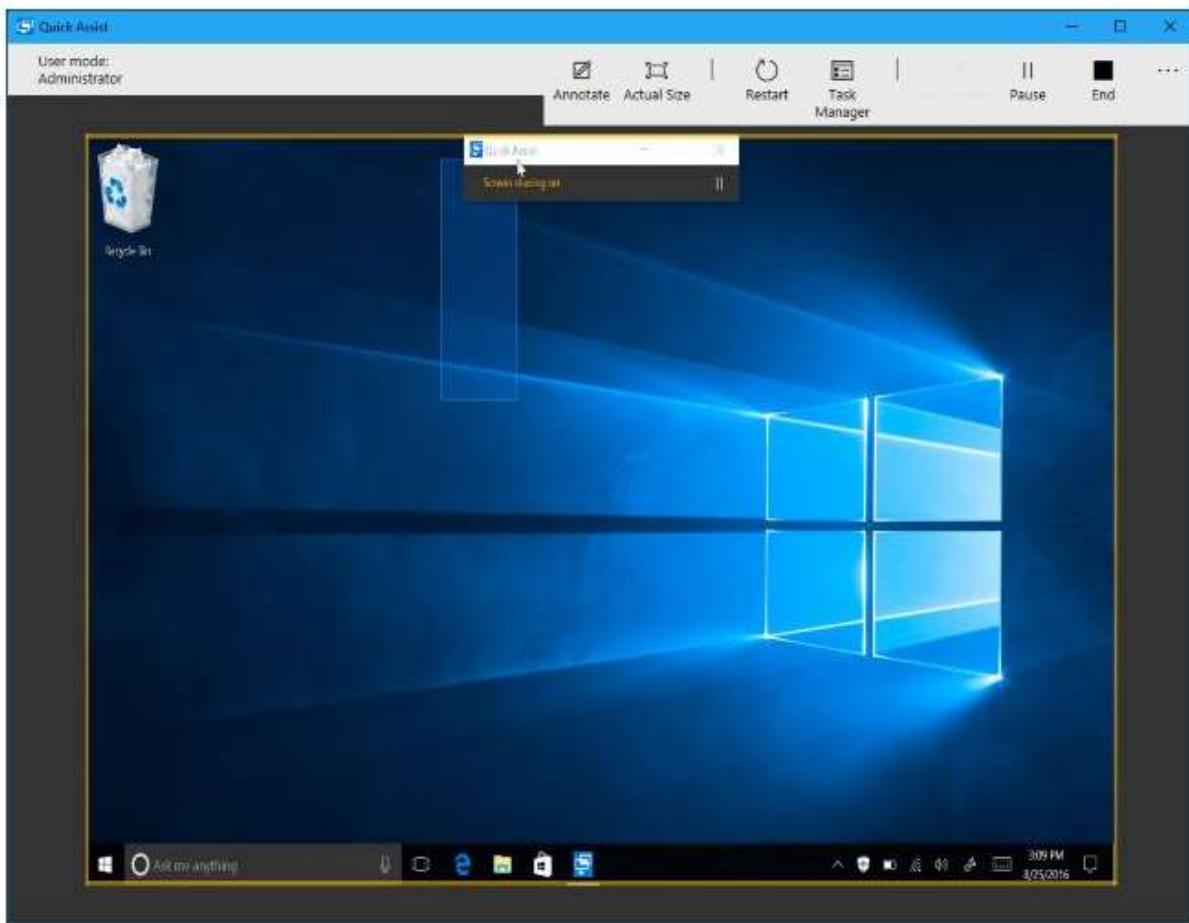


Image:Remote Desktop Screen

References:

35. NSTI Lab manual on Module 2

Activity 4

Aim: Connect Remote Desktop using Telnet

Learning outcome: Able to configure and perform remote accessing & routing.

Duration: 3 hour

List of Hardware/Software requirements:

1. Any kind of Laptop/ Desktop with internet connection
2. Windows 8 OS

Code/Program/Procedure (with comments):

Step 1: Press Windows- X and select the search from the context menu and enter the control panel in the search field.

Step 2: Click the Programs and features and then click Turn Windows Features On or Off.

Step 3: Select the Telnet Client checkbox and then click OK to install telnet to Windows 8.

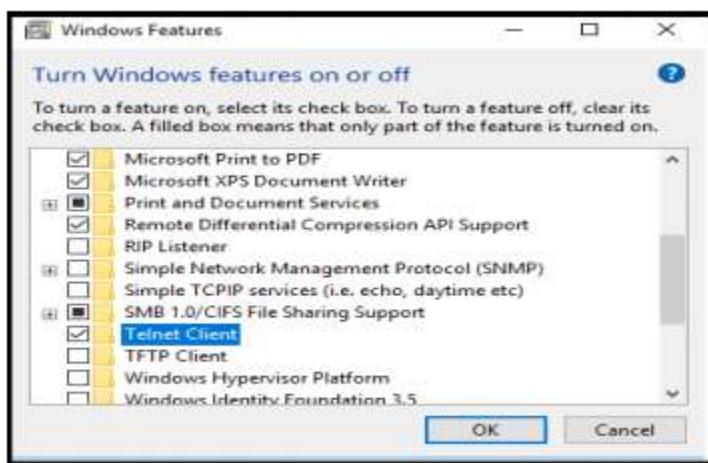


Image:Install Telnet

It may take some time to install telnet.

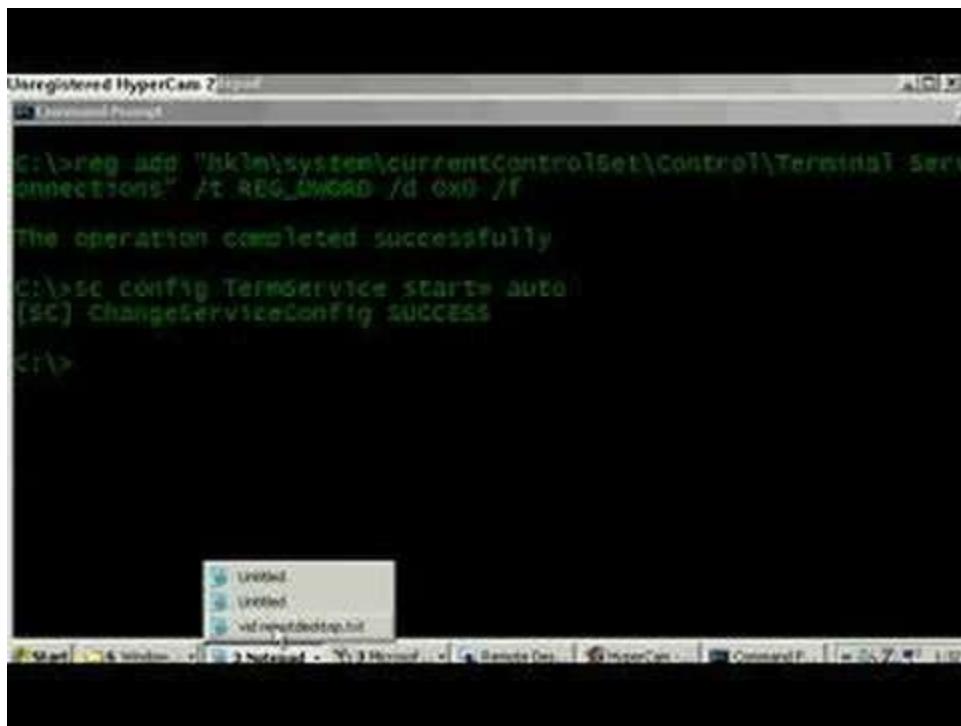
Step 4: Enter cmd in the search field and click Command Prompt from the context menu.

Step 5: Type the command- telnet [IP Address or host name] [port-number] Determine the IP Address or hostname of the server and the TCP port number required to establish a connection and press enter.

Step 6: Type the username and password, if applicable, to log in to the computer.

Output/Results snippet:

The connection will now be established. The telnet screen appears as follows:



The screenshot shows a Windows Command Prompt window titled "Unregistered HyperCam 2". The window contains the following text:

```
C:\>reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\TcService" /v fAllowRemoteDesktop /t REG_DWORD /d 0x0 /f  
The operation completed successfully.  
C:\>sc config TerminalService start= auto  
(SC) ChangeServiceConfig SUCCESS  
C:\>
```

At the bottom of the window, there is a small floating window titled "Untitled" with the text "Telnet" and "Telnet" repeated twice. The taskbar at the bottom of the screen shows icons for Start, Windows, Task View, Network, Task Manager, Remote Desktop, HyperCam, Command Prompt, and File Explorer.

Image: Telnet

References:

36. NSTI Lab manual on Module 2

Activity 5

Aim: Connect Remote Desktop using HyperTerminal

Learning outcome: Able to configure and perform remote accessing & routing.

Duration: 2 hour

List of Hardware/Software requirements:

1. Any kind of Laptop/ Desktop with internet connection
2. Windows XP OS

Code/Program/Procedure (with comments):

Activity 6

Aim: Connect Remote Desktop using Teamviewer

Learning outcome: Able to configure and perform remote accessing & routing.

Duration: 5 hour

List of Hardware/Software requirements:

1. Any kind of Laptop/ Desktop with internet connection
2. Windows 8 OS
3. Teamviewer Software

Code/Program/Procedure (with comments):

Step 1 First, install the team viewer software. Just open this team viewer page. Select Download Now button. It will automatically download the software for the particular user OS.



Image: Teamviewer Software

Step 2 After downloaded, install it and click on the run which appears as a pop-up window to start the setup program.



Image: Teamviewer Software Setup

Step 3 The setup window will open and select the necessary option and click the Accept-finish button.

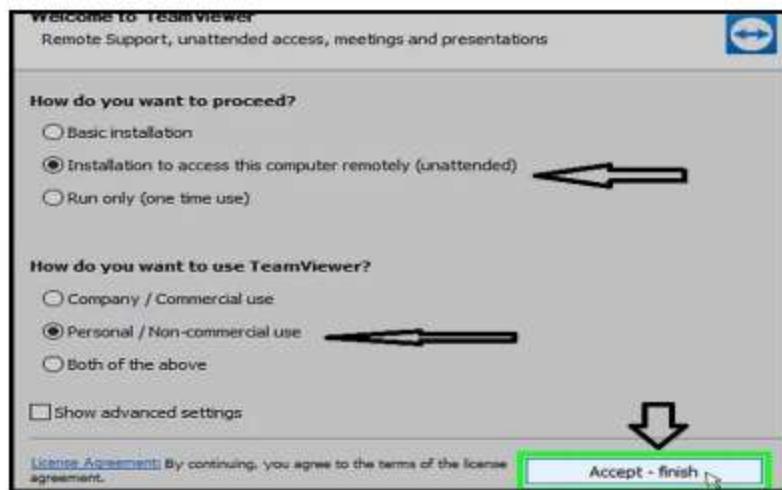


Image: Accept to Finish Setup

Step 4 Finally installing is done and Wait for the setup to finish downloading the files on your C: drive. Then, TeamViewer will automatically generate a random ID and password to be used to connect to other computers.

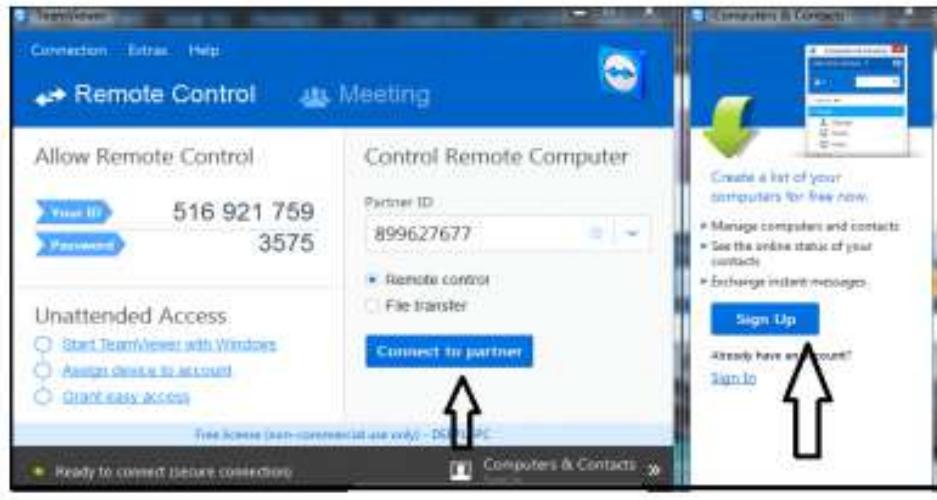


Image:Connect to other Computer

Step 5 It will take some time to connect and the screen blurs. After the while, the user can be able to see your partner screen, and the user can make changes to it as well.

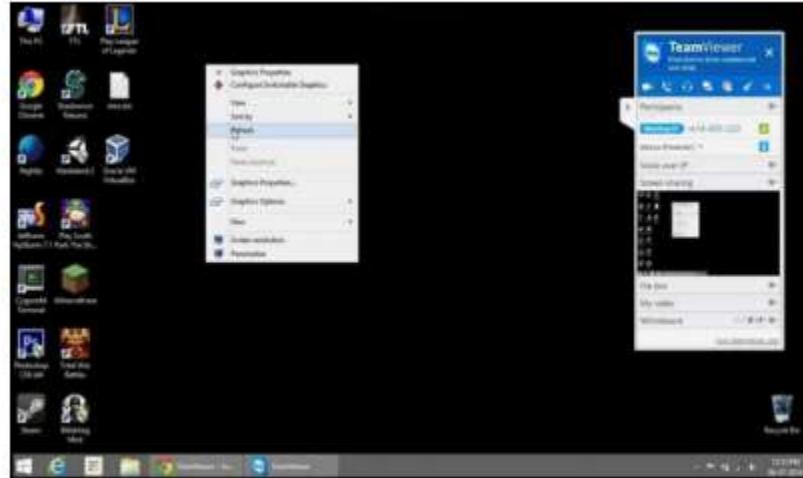


Image:Screen Blur

Step 6 Share a file remotely by using a team viewer. Just tick on “file transfer” instead of “remote control” and then connect to the partner by using his/her ID and Password. Just drag the files which are to be referred.

Step 7 And can have a conversation with the partner by using the simple chat box at the bottom of the right side. Once connected to the partner, the user can use chat effectively.

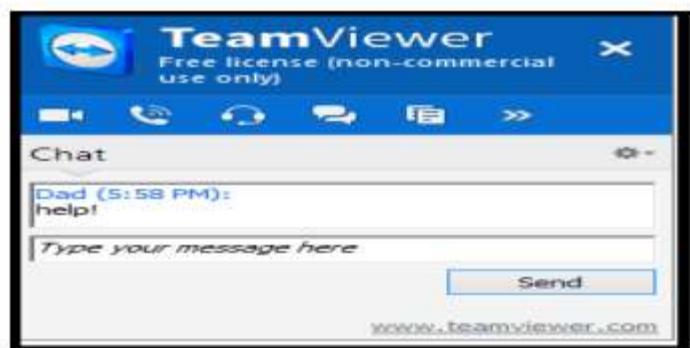


Image:Chat

Step 8 And even allowed to adjust the visuals of the screen by heading over to the “view” which is at the top of the screen

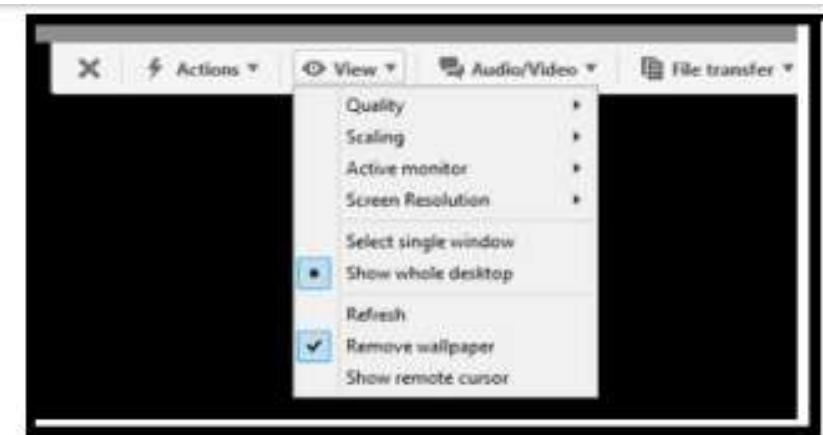


Image:Adjust the screen

Step 9 And the user may feel better to add some recorded videos of that team viewer session and it provides it too.

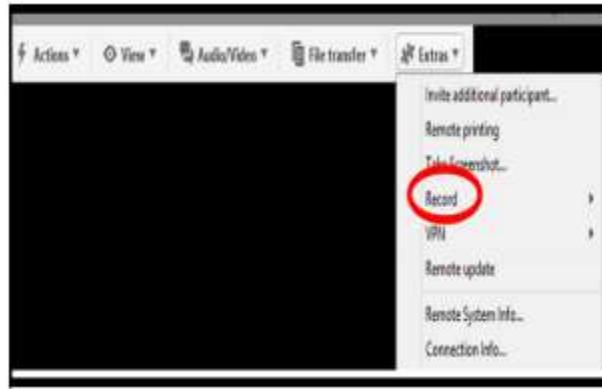


Image:Recording

Output/Results snippet:

The connection will now be established. The teamviewer screen appears as follows:

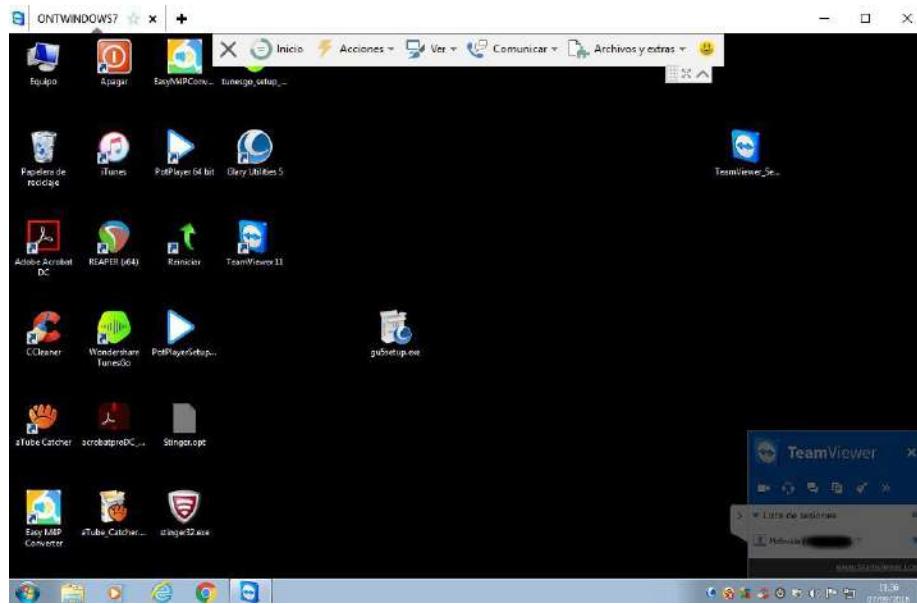


Image:Final Screen

References:

37. NSTI Lab manual on Module 2

Learning Outcome 8 - Able to get familiarized with internet and E- Commerce sites

After achieving this learning outcome, a student will be able to get familiarized with internet and E- Commerce sites. In order to achieve this learning outcome, a student has to complete the following:

1. Create and send e-mail, Reply to an e-mail message and Forward email message (3Hrs)
2. Send document/softcopy by email (1Hr)
3. Activate spell check using address book and Handle SPAM (1Hr)
4. Sorting and search emails. (2Hrs)
5. Block emails using filter (1 Hr)
6. Store download file in mail drives (2Hrs)
7. Communicate using text, video chatting and social networking sites (2Hrs)
8. Protect thecomputeragainst various internet threats (3Hrs)
9. Browse e-commerce websites (1 Hr)
10. Place order for items (1 Hr)
11. Add items to shopping Carts (1Hr)
12. Do online payment through payment gateways or other payment method (1Hr)
13. Do online Bill payment of service providers (1Hr)

Activity 1

Aim: Configure web browser.

Learning outcome: Able to get familiarized with internet and E- Commerce sites.

Duration: 2 hour

List of Hardware/Software requirements:

1. Any kind of Laptop/ Desktop with internet connection
2. Windows 8 OS
3. Chrome Web Browser

Code/Program/Procedure (with comments):

One of the easiest technologies to keep the information and computer safe is properly configuring the security settings on the web browser.

There are some setting suggestions to be configured in the web browser

- Limit Cookie Storage
- Do not Store Passwords or Allow Sites to Remember the Form Entries
- Disable the Pop-ups
- Limit the Plug-ins and Add-ons
- Enable the Automatic Site Checking
- Prompt for the Downloads
- Clear the Browsing Data/Temporary Internet Files

- Limit Cookie Storage

Cookies are the data files of web page put on the user computer that tracks information about the user. Cookies can be helpful like remembering what item the user put in their shopping cart while the user continues shopping.

To configure cookies,

Browser	How to configure
Chrome 64	<p>Chrome Menu → Settings → Show Advanced Settings → Privacy and then Security → Content settings. Under Cookies, set the following:</p> <ol style="list-style-type: none">1. Select the Keep local data only until I quit my browser or select Block sites for setting any data if you want to select which cookies to allow as you visit each site.2. Check the Block third-party cookies.
Internet Explorer	<p>Tools → Internet Options → Privacy → Advanced, and: Select the Prompt or Accept for first-party cookies and then Block for third-party cookies. If you select the Prompt, it will ask for each site what you want to keep, which is helpful for limiting cookie use but will have a lot of notifications.</p>

• **Do not Store Passwords or Allow Sites to Remember the Form Entries**

Browser	How to configure
Chrome	<p>Chrome Menu → Settings → Advanced → Privacy and Security, and:</p> <ul style="list-style-type: none">• Under the Privacy, click the Content settings. Under location, select Ask before accessing.• Under the Passwords and forms, uncheck the Autofill Settings and <p>uncheck Manage Passwords.</p>
Internet Explorer	<p>Tools → Internet Options, and:</p> <ol style="list-style-type: none">1. Select Advanced. Then under the Security, check Do not save encrypted pages to disk.2. Select Content. Then under Autocomplete, click Settings and uncheck all.3. Select Privacy and Then check Never allow websites to request your physical location.

- **Disable the Pop-ups**

Browser	How to configure
Chrome	Chrome Menu → Settings → Advanced, under Privacy, click Content settings. Select the Popups → Blocked.
Internet Explorer	Tools → Internet Options → Privacy and check the Turn on Pop-up Blocker.

- **Limit the Plug-ins and Add-ons**

Browser	How to configure
---------	------------------

Chrome	<p>Chrome Menu → Settings → Advanced → Privacy and Security. Under Privacy, click Content settings and:</p> <ol style="list-style-type: none">1. Under the JavaScript, uncheck JavaScript.2. Under the Plug-ins, select Block all (you can instead select Click to play to be prompted).3. Under the Sandboxed plug-in access, select the Ask me when a site wants to use a plug-in to access my computer.
Internet Explorer	<p>Tools → Internet Options → Advanced. Under Browsing, uncheck Enable third-party browser extensions (add-ons).</p> <p>You will also want to select the Security and click the Internet icon. Change the setting to the High for the Internet zone. Click on the Trusted Sites icon and set this to Medium and Add sites to the Trusted list as you go.</p>

- **Enable the Automatic Site Checking**

Browser	How to configure

Chrome	This feature may be automatically on. To verify that it's on, select Chrome Menu → Settings, and under the Privacy, check to Enable phishing/malware protection.
Internet Explorer	This feature is automatically on. To verify that it's on, select the Tools → Safety → Turn on SmartScreen Filter.

- **Prompt for the Downloads**

Browser	How to configure
Chrome	Chrome Menu → Settings, and under the Downloads, check to Ask where to save each file before downloading.
Internet Explorer	Tools → Internet Options → Security → Custom Level. Under the Downloads, select Enable for Automatic prompting for file downloads.

- **Clear the Browsing Data/Temporary Internet Files**

Browser	How to configure

Chrome	Chrome Menu → Tools → Clear the Browsing Data. In the drop-down list, change the amount of time you want to go back (recommended: The beginning of time). Check the items to remove and click the Clear browsing data.
Internet Explorer	Tools → Safety → Delete the browsing history. Check the items to remove and click Delete.

Output/Results snippet:

The chrome browser settings looks like as follows:

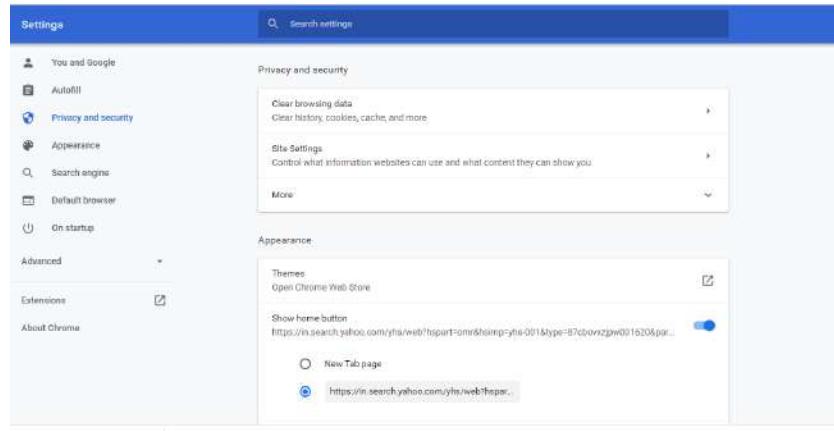


Image: Chrome Settings Tab

References:

- NSTI Lab manual on Module 2

Activity 2

Aim: Search for content using popular search engines.

Learning outcome: Able to get familiarized with internet and E- Commerce sites.

Duration: 1 hour

List of Hardware/Software requirements:

1. Any kind of Laptop/ Desktop with internet connection
2. Windows 8 OS
3. Chrome Web Browser

Code/Program/Procedure (with comments):

Step 1: Go to Google.com.

Step 2: Enter site:www.website.com search term into the search box.*

Google site:blog.hubspot.com facebook stat

Web Images Maps Shopping More Search tools

About 340 results (0.21 seconds)

[12 Revealing Marketing Stats About Facebook for Business](#)
blog.hubspot.com/.../12-Revealing-Marketing-Stats-...
 by Corey Eridon - in 132 Google+ circles - More by Corey Eridon
Sep 11, 2012 - Dig through some fascinating stats about how Facebook is used for businesses and marketers.

[The Ultimate List: 100+ Facebook Statistics \[Infographics\]](#)
blog.hubspot.com/.../The-Ultimate-List-100-Facebook-...
 by Kipp Bodnar - in 5,672 Google+ circles - More by Kipp Bodnar
Jun 24, 2010 - With more than 500 million users Facebook has become the dominant player in the social networking industry As marketers and business ...

...

[12 Essential Facebook Stats \[Data\]](#)
blog.hubspot.com/.../12-Essential-Facebook-Stats-Data.aspx
May 31, 2011 - It's no secret that Facebook has a massive and highly engaged audience But just because 93 of Americans are actively friending poking ...

[21 Internet Marketing Stats That Will Blow Your Mind](#)
blog.hubspot.com/.../21-Internet-Marketing-Stats-That-Will-Blow-Your-Mind.aspx
by Kipp Bodnar - in 5,672 Google+ circles - More by Kipp Bodnar
Jun 29, 2012 - Tweet This Stat! 9) In any given week, less than 0.5% of Facebook fans engage with the brand they are fans of. (Source: Marketing Science) ...

[19 Reasons You Should Include Visual Content in Your Marketing ...](#)
blog.hubspot.com/.../19-Reasons-You-Should-Include-Visual-Content-in-Your-Marketing.aspx
Aug 6, 2012 - (Source: SEOmoz) Tweet This Stat! 6) Visual content drives engagement. In fact, just one month after the introduction of Facebook timeline for ...

*Pay attention to the subdomain (the letters that precede a domain name, like www., blog., or info.) you enter. Which subdomain you enter, or even choosing not to enter one at all, will change your results.

For example, when I try to conduct a site:search for all the mentions of marketing automation on hubspot.com, I get way more results (about 9,500) when I enter site:hubspot.com marketing automation than I do if I enter site:www.hubspot.com marketing automation (about 2,300). Why?

Because the former is bringing up results for *all* the subdomains on hubspot.com. That means it returns results for mentions of marketing automation on, say, blog.hubspot.com, too.

Act Big To Get Big

www.hubspot.com/act-big-to-get-big/

... in the comments on this post and we will highlight the best discussions and links in two weeks on the HubSpot blog. Learn more about **Marketing Automation** ...

HubSpot Announces Death By Marketing Automation Upgrade ...

www.hubspot.com/.../HubSpot-Announces-Death-By...



by Kara Sassone - in 371 Google+ circles - More by Kara Sassone
Sep 1, 2011 – Inbound **marketing software** company HubSpot laid out a challenge to the industry with a **software trade-up program** it calls #DeathByMA.

3 Ways You're Not Using Marketing Automation (But Should Be)

blog.hubspot.com/.../3-Ways-You-re-Not-Using-Mar...



by Jeffrey Russo - in 22 Google+ circles - More by Jeffrey Russo
Dec 11, 2012 – A good first step is to set up some rules using your **marketing automation software** that put your leads into those various segmented buckets as ...

Death by Marketing Automation Webinar Download

www.hubspot.com/marketing-automation-webinar/

Originally only presented in two sold-out sessions at Dreamforce 2011, "Death by **Marketing Automation**" is presented by HubSpot CMO Mike Volpe on the topic ...

5 Disastrous Misconceptions About Marketing Automation

blog.hubspot.com/.../5-Disastrous-Misconceptions-A...



by Corey Eridon - in 132 Google+ circles - More by Corey Eridon
Nov 28, 2011 – **marketing automation software** There's a lot of buzz around whether **marketing automation software** is worth the investment of time and money, ...

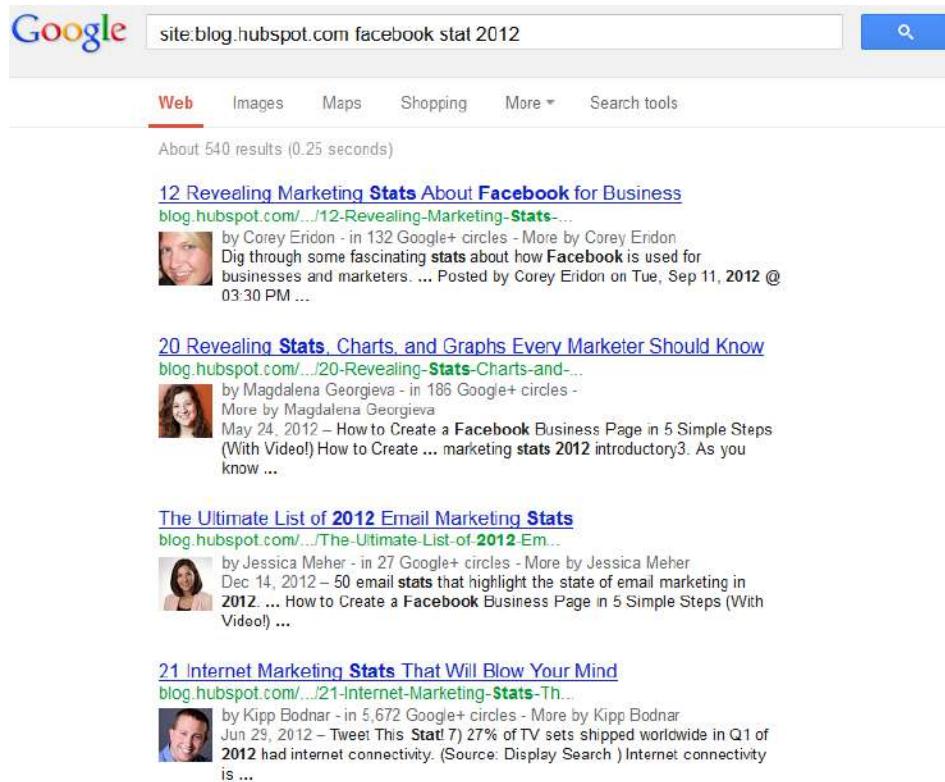
Entering site:www.hubspot.com marketing automation, however, returns results for only mentions of marketing automation on the www. subdomain. So the lesson here is, be specific about what domain and subdomain you want to search.

Step 3: Refine your search.

For instance, in Step 2 when I searched our blog for a Facebook stat, some results from a long time ago -- like 2010 -- came up. I could filter for only the most recent stats by refining my search to site:blog.hubspot.com facebook stat 2012.

Output/Results snippet:

The Google Search result looks like as follows:



A screenshot of a Google search results page. The search query in the bar is "site:blog.hubspot.com facebook stat 2012". The results are filtered to show only web pages from the specified blog. The first result is a blog post titled "12 Revealing Marketing Stats About Facebook for Business" by Corey Eridon. The second result is "20 Revealing Stats, Charts, and Graphs Every Marketer Should Know" by Magdalena Georgieva. The third result is "The Ultimate List of 2012 Email Marketing Stats" by Jessica Meher. The fourth result is "21 Internet Marketing Stats That Will Blow Your Mind" by Kipp Bodnar. Each result includes a small profile picture of the author, the date of publication, and a brief description of the content.

Google

site:blog.hubspot.com facebook stat 2012

Web Images Maps Shopping More Search tools

About 540 results (0.25 seconds)

[12 Revealing Marketing Stats About Facebook for Business](#)
blog.hubspot.com/...12-Revealing-Marketing-Stats-...
by Corey Eridon - in 132 Google+ circles - More by Corey Eridon
Dig through some fascinating stats about how Facebook is used for businesses and marketers. ... Posted by Corey Eridon on Tue, Sep 11, 2012 @ 03:30 PM ...

[20 Revealing Stats, Charts, and Graphs Every Marketer Should Know](#)
blog.hubspot.com/...20-Revealing-Stats-Charts-and-...
by Magdalena Georgieva - in 186 Google+ circles - More by Magdalena Georgieva
May 24, 2012 – How to Create a Facebook Business Page in 5 Simple Steps (With Video) How to Create ... marketing stats 2012 introductory3. As you know ...

[The Ultimate List of 2012 Email Marketing Stats](#)
blog.hubspot.com/...The-Ultimate-List-of-2012-Em...
by Jessica Meher - in 27 Google+ circles - More by Jessica Meher
Dec 14, 2012 – 50 email stats that highlight the state of email marketing in 2012. ... How to Create a Facebook Business Page in 5 Simple Steps (With Video) ...

[21 Internet Marketing Stats That Will Blow Your Mind](#)
blog.hubspot.com/...21-Internet-Marketing-Stats-Th...
by Kipp Bodnar - in 5,672 Google+ circles - More by Kipp Bodnar
Jun 29, 2012 – Tweet This Stat! 7) 27% of TV sets shipped worldwide in Q1 of 2012 had internet connectivity. (Source: Display Search) Internet connectivity is ...

References:

- <https://blog.hubspot.com/marketing/how-to-do-a-google-site-search>

Activity 3

Aim: Use favourite folder for browsing quickly

Learning outcome: Able to get familiarized with internet and E- Commerce sites.

Duration: 1 hour

List of Hardware/Software requirements:

1. Any kind of Laptop/ Desktop with internet connection
2. Windows 8 OS
3. Internet Explorer Web browser

Code/Program/Procedure (with comments):

Two way to use a favourite folder for browse quick. (Internet Explorer)

Step 1

Select organize favorites via the star button.

Click the top-right star icon (or press Alt+C) to view Favorites, click the down arrow on the right of Add to favorites and choose to Organize favorites in the drop-down list.

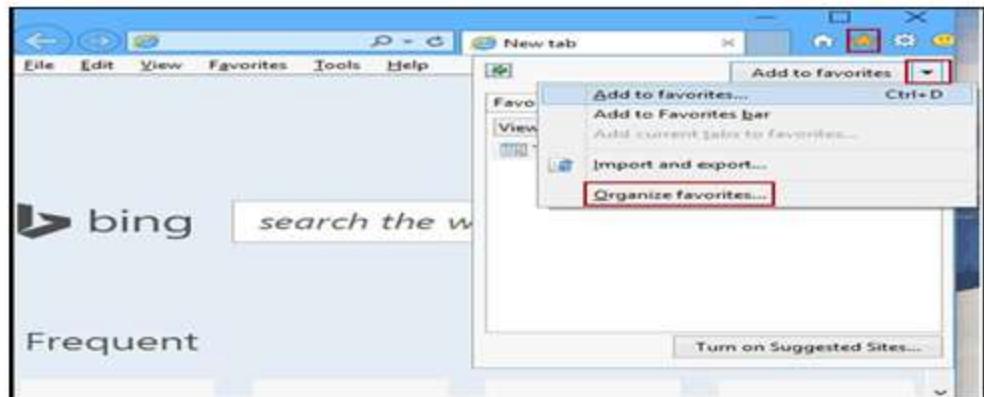


Image: organize favorites

Step 2

Select organize favorites via the Favorites menu.

Output/Results snippet:

The internet explorer screen looks like as follows:

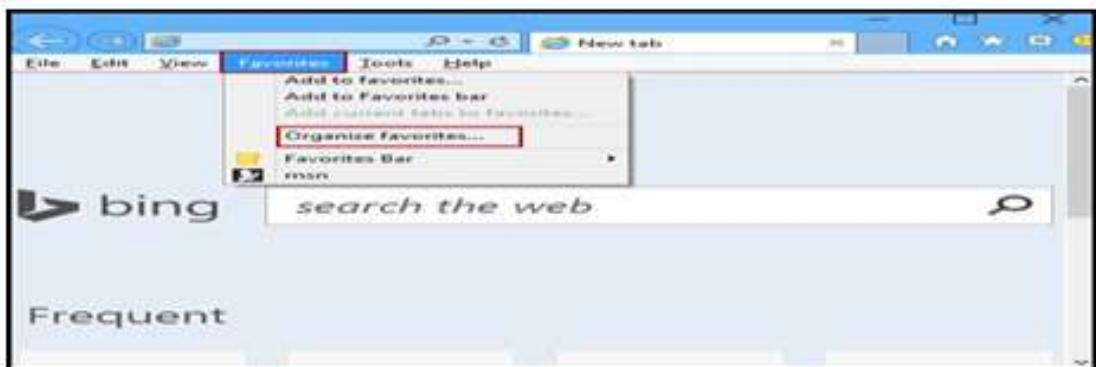


Image: Favorites menu

References:

- NSTI Lab manual on Module 2

Activity 4

Aim: Download & Print Webpages

Learning outcome: Able to get familiarized with internet and E- Commerce sites.

Duration: 1 hour

List of Hardware/Software requirements:

1. Any kind of Laptop/ Desktop with internet connection
2. Windows 8 OS
3. Chrome Web browser

Code/Program/Procedure (with comments):

Step 1

Open the Settings menu by clicking the three-dot icon in the top right-hand corner and then choose the Print. This will bring up a printing window. Alternatively, press Ctrl + P.



Image: Print Webpage

Step 2

In the printing window, look for the heading Destination and select Change. This will bring the user to select the Destination Under the heading, Print Destinations, and the user views an option to save as PDF checkbox and select it. That will load a preview of the pages and allow the user to select pages, change the layout, and so on.

Output/Results snippet:

The chrome window looks like as follows:



Image: Final Screen of Chrome

References:

NSTI Lab manual on Module 2

Activity 5

Aim: Create and send e-mail, Reply to an e-mail message and Forward email message

Learning outcome: Able to get familiarized with internet and E-Commerce sites.

Duration: 3 hours

List of Hardware/Software requirements:

1. Computer/Laptop/Mobile.
2. Internet Connection.
3. Sending person and receiving person.

Procedure:

Step 1:

Create an e-mail account with the Username and Password and enter all other details in the fields.

Step 2:

When the user signs in to Gmail, the user sees a list of any messages they received in their Inbox.

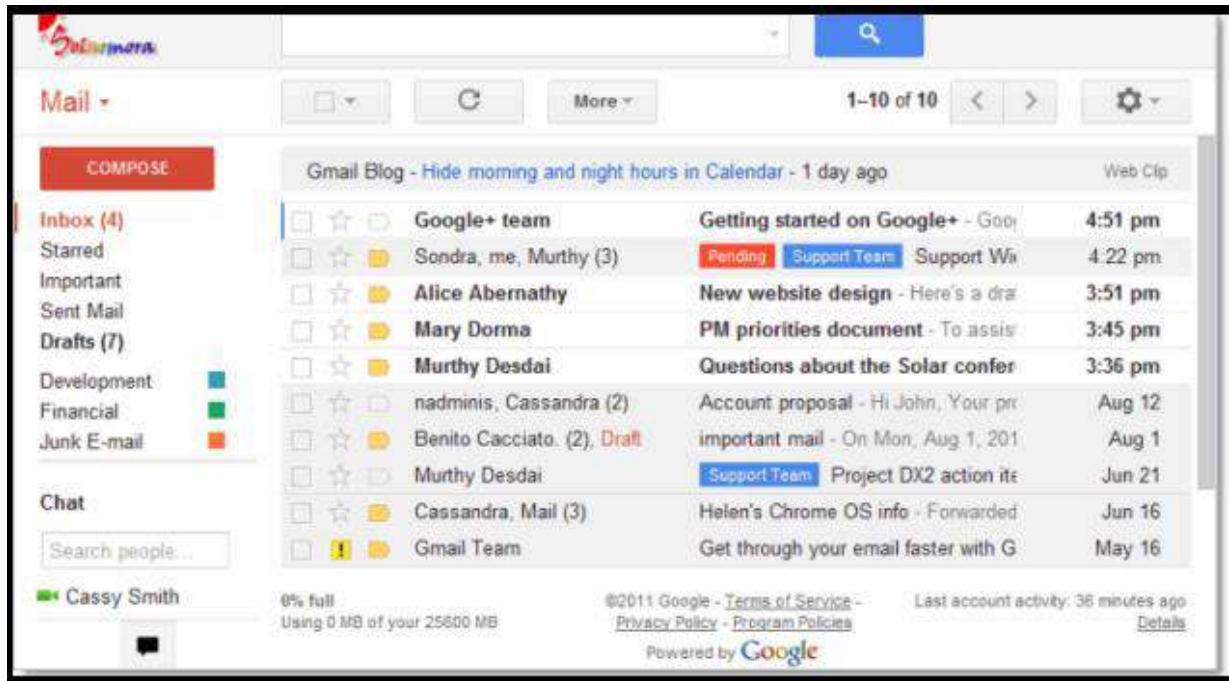


Figure 01: Inbox

Step 3: Compose a mail and send a mail.

In the pane on the left side, click on COMPOSE.



Figure 02: Compose

In the To field, a category is the first letter or letters of a recipient's name to look up their email address in your corporate directory.

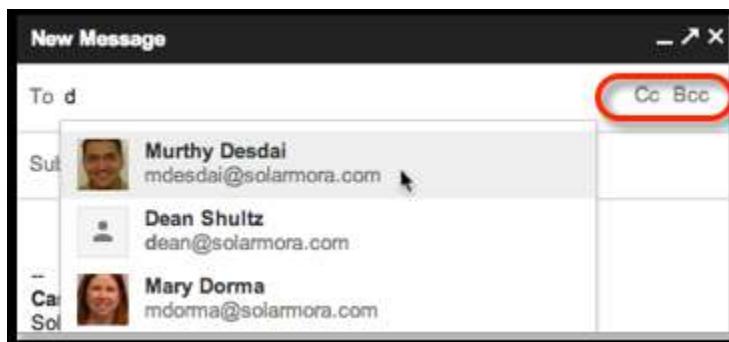


Figure 03: cc and Bcc field

To add a Cc or a Bcc, just click Cc or Bcc that shows up when the user is entering the addresses. The user can also drag and drop email addresses between To, Cc, and Bcc.

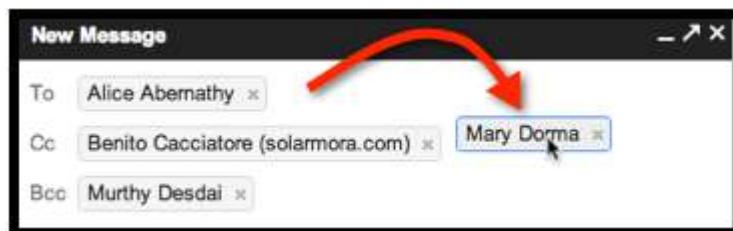


Figure 04: Drag and Drop Email Addresses between To, Cc, and Bcc

Enter a subject and the message text. The email pane will grow as the user type to fit their message

Step 4: Attach a file

Click on the paperclip icon and browse for the file on the computer or local network. After attached, the file appears at the bottom of the message.



Figure 05: Attaching the File

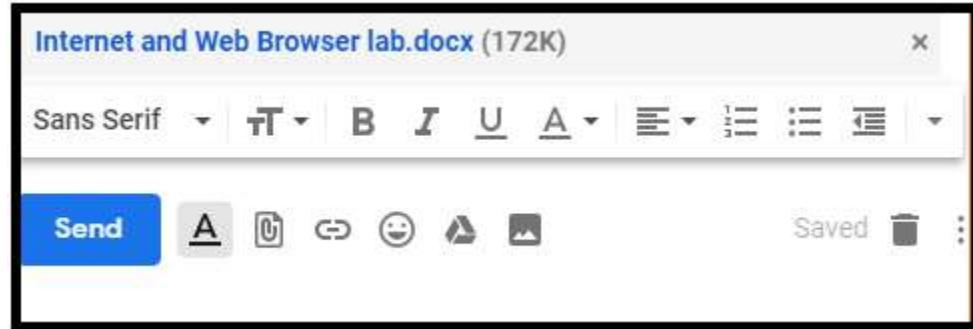


Figure 06: Send Button

.At the bottom of the message window, click the Send. A message appears at the top of the mail window, confirming that the message was sent.

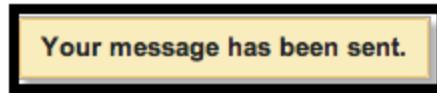


Figure 07: Confirmation Message

Step 5:

Reply to an e-mail message.

1. Open the conversation message and select the message that the user wants to reply to.
2. To reply to the sender, click on the Reply button.



Figure 08: Replay Button

3. And then at the bottom of the message, click Send.

Step 6:

Forward email message

1. Open the message. If the message is part of a chat, open the chat and select the message to forward.
2. At the bottom of the message, click the Forward.

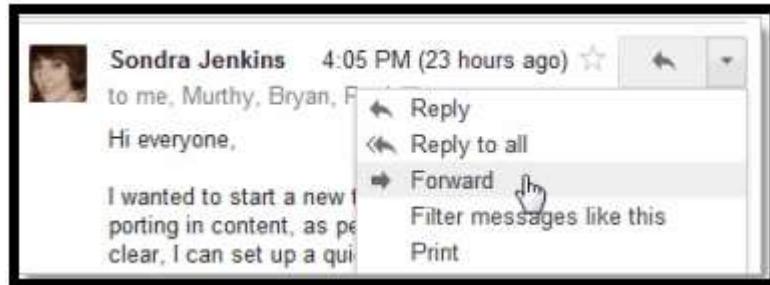


Figure 09: Forward email message

3. Enter the email addresses to which to forward the message and add any records in the message field.
4. If the message has an attachment that the user doesn't want to forward, uncheck the box next to the attachment file name, below the Subject field.
5. At the bottom of the message, click the Send.

References: <https://support.google.com/>

Activity 6

Aim: Send document/softcopy by email.

Learning outcome: Able to get familiarized with internet and E-Commerce sites.

Duration: 1 hour

List of Hardware/Software requirements:

1. Computer/Laptop/Mobile.
2. Internet Connection.
3. Sending person and receiving person.

Procedure:

Step 1:

In the pane on the left side, click on COMPOSE.



Figure 10: Compose

In the To field, a category is the first letter or letters of a recipient's name to look up their email address in your corporate directory.

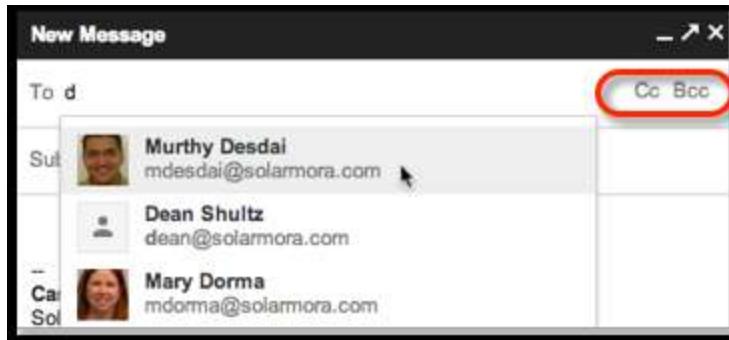


Figure 11: cc and Bcc field

To add a Cc or a Bcc, just click Cc or Bcc that shows up when the user is entering the addresses. The user can also drag and drop email addresses between To, Cc, and Bcc.



Figure 12: Drag and Drop Email Addresses between To, Cc, and Bcc

Enter a subject and the message text. The email pane will grow as the user type to fit their message.

Step 2:

Click on the paperclip icon and browse for the file on the computer or local network. After attached, the file appears at the bottom of the message.



Figure 13: Attaching the File

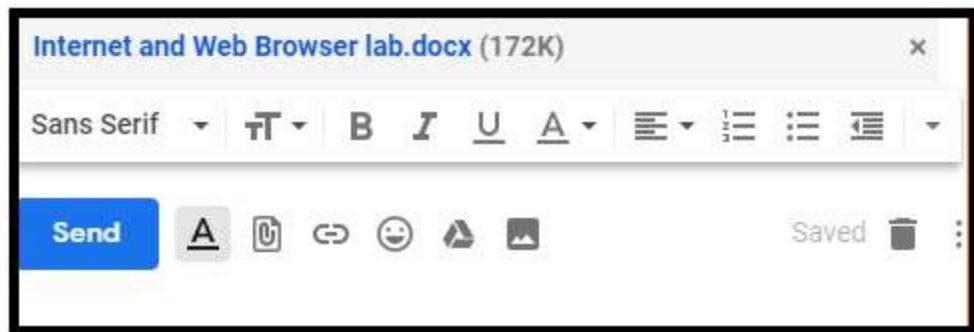


Figure 14: Send Button

At the bottom of the message window, click the Send. A message appears at the top of the mail window, confirming that the message was sent.

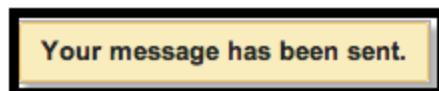


Figure 15: Confirmation Message

References: <https://support.google.com/>

Activity 7

Aim: Activate spell check using address book and Handle SPAM

Learning outcome: Able to get familiarized with internet and E-Commerce sites.

Duration: 1 hour

List of Hardware/Software requirements:

1. Computer/Laptop/Mobile
2. Internet connection

Procedure:

Step 1

In the Search, field enters the contacts name which is not stored in the address book. To connect to the mail conversation in the Inbox page and click on Add to Contacts option. Then the person's mail ID will be stored in the address book and enter the name in the search field.

Step 2

In the Gmail before send a mail check for the spell checking. So follow the below step to do a spell check.

- In the top left side, click Compose.
- Write the message, below the subject field.

- Click on the stacked, three-dotted menu at the bottom right-hand side of Compose Gmail's message box.
- Click on Check spelling.
 1. The spelling mistake is highlighted in red immediately.
- Click any misspelled word to get a list of optional alternative spellings.
- Click a different word to have Gmail automatically replace the misspelled word with a suitably spelled word.
 1. You can also click Ignore to avoid the spelling mistake.
- If the user types more words in the email and wants to check the spelling again, click on Recheck at the bottom of the message box.

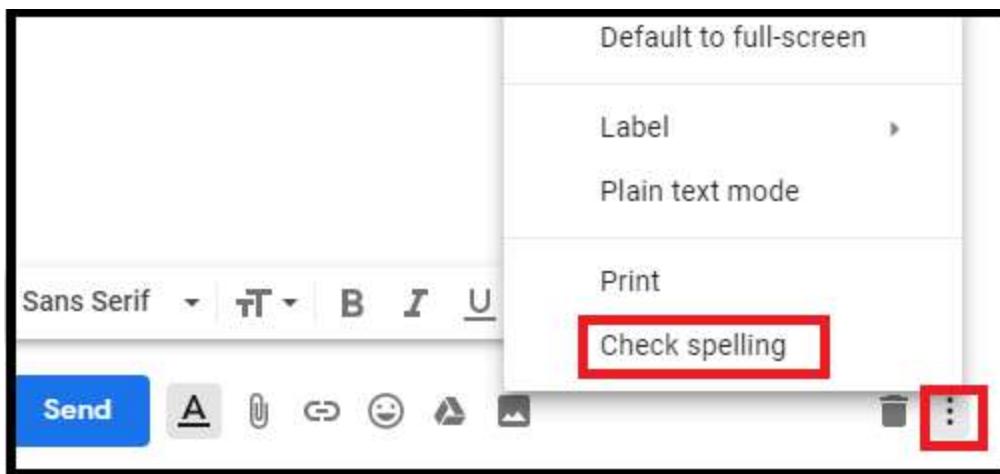


Figure 16: Checking Spelling in Message

How to handle Spam

The term spam refers to unwanted emails. Spam is often sent by mass mailing operations that use computers to send millions of emails in a short period of time.

There are some precautions to use mail and web to keep yourself from being a victim.

- Never respond to the spam.
- Be careful when using the unsubscribe directions at the bottom of emails.
- Do not include your major email address on your website.
- Do not share your major password on bulletin boards or online forums.
- Avoid using your major email address in online forms.

References: <https://support.google.com/>

Activity 8

Aim: Sorting and searching emails.

Learning outcome: Able to get familiarized with internet and E-Commerce sites.

Duration: 2 hours

List of Hardware/Software requirements:

1. Computer/Laptop/Mobile.
2. Internet Connection.

Procedure:

Sort mail by the sender and search emails.

Step 1:

Open Gmail and sign with the username and password and the Gmail Inbox page displayed on the screen.

Step 2:

Find the sender email address

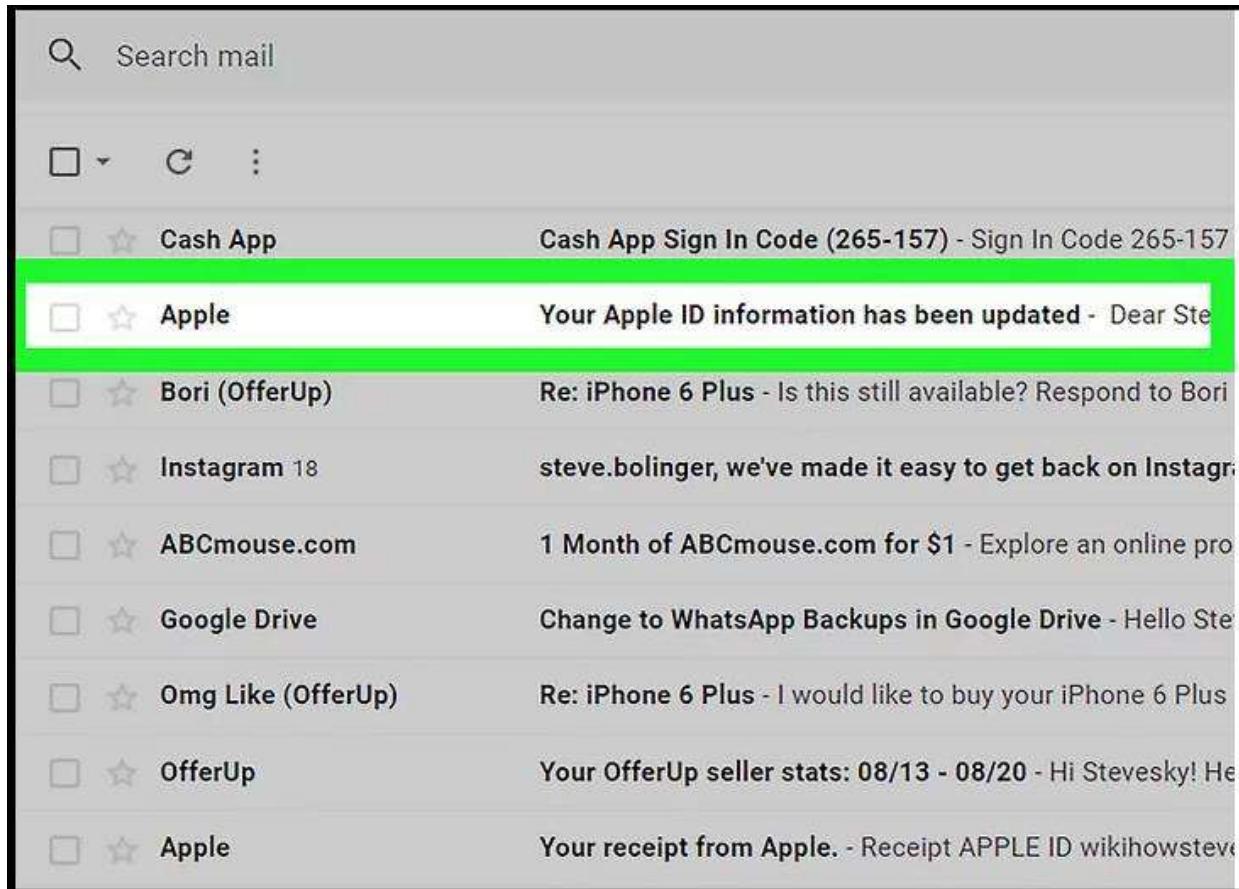


Figure 17: Find the sender email address

Step 3:

Copy the email address- Copy the Mail address

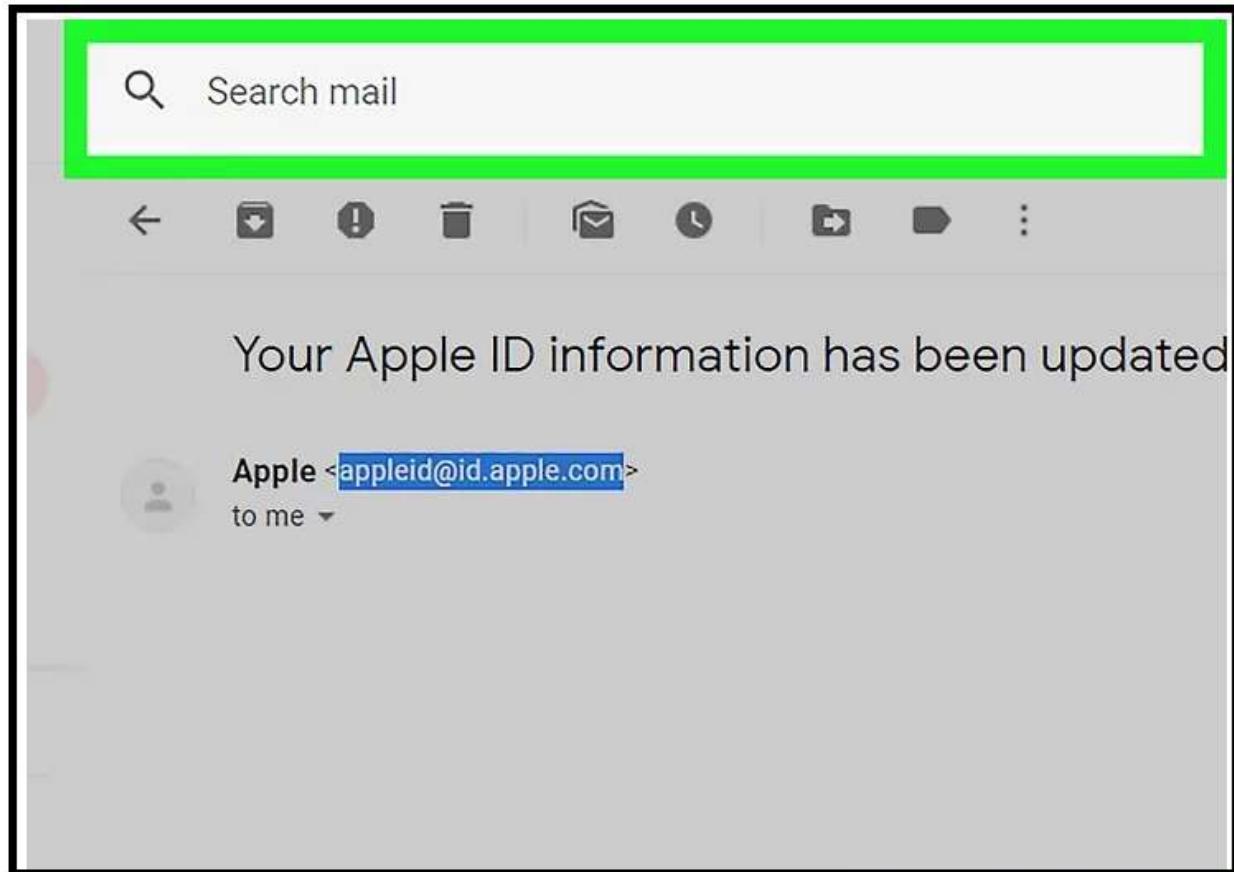


Figure 18: Copy the Mail address

Step 4:

Click on the Gmail search bar.

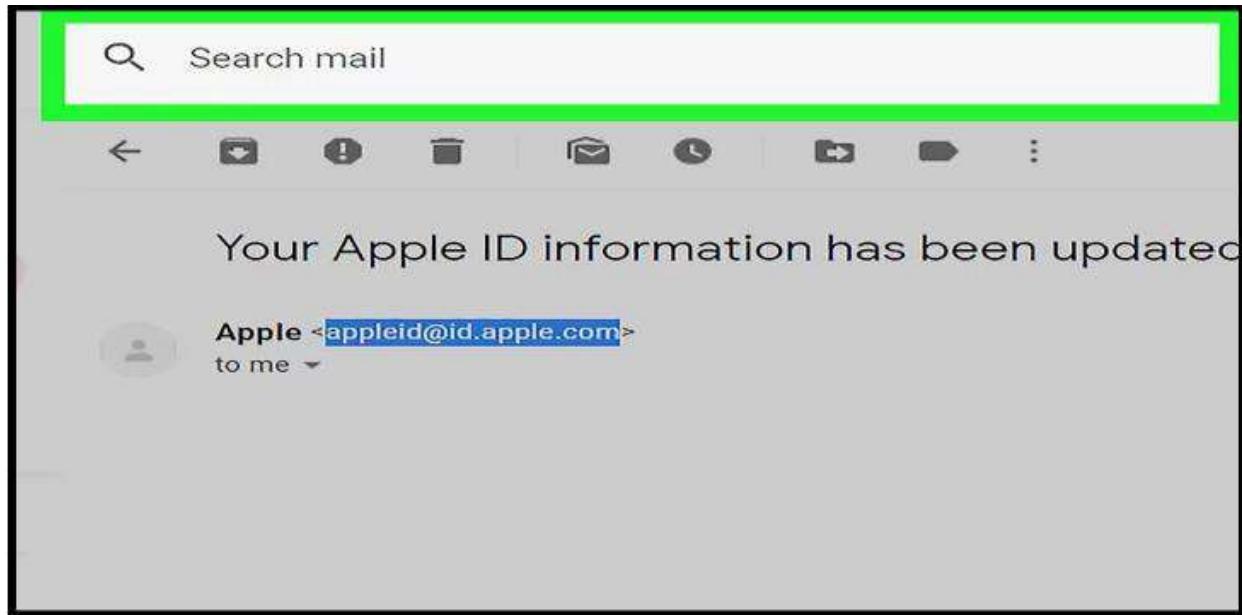


Figure 19: Gmail search bar

Step 5:

Enter the copied email address- Press Ctrl+V to paste in the copied address, then press Enter to view the list of email addresses.

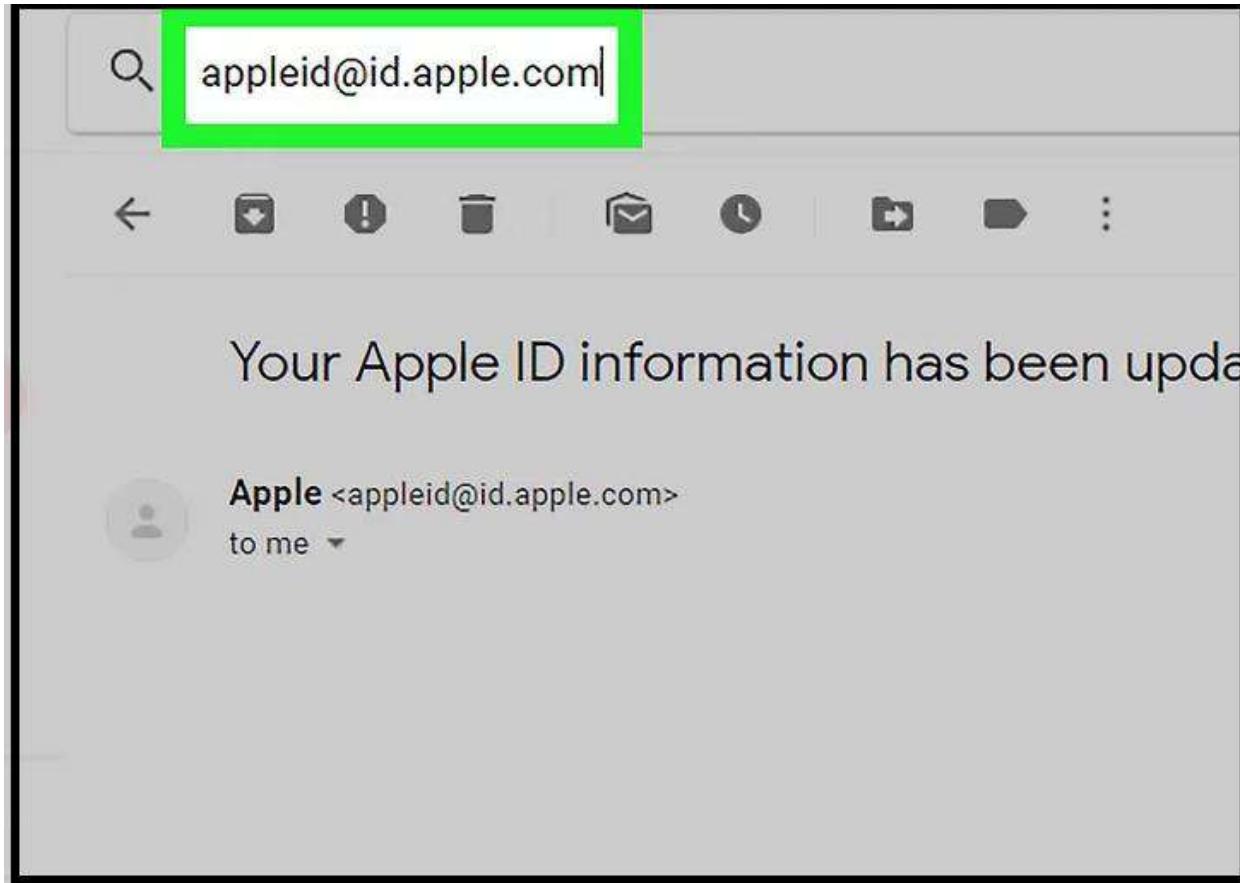


Figure 20: Enter to view the list of email address

Step 6:

Review the list of emails.

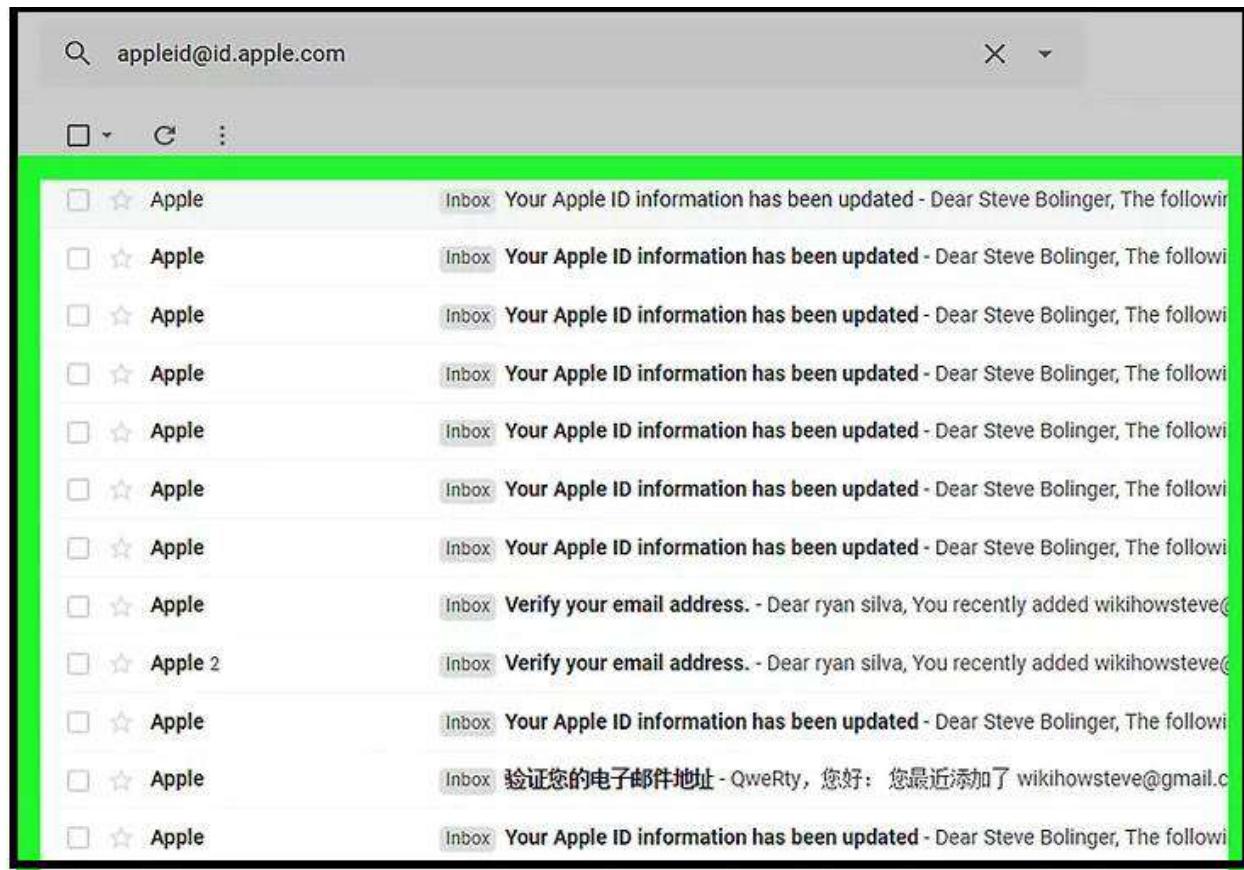


Figure 21: Review the list of emails

References: <https://support.google.com/>

Activity 9

Aim: Crimp Straight Cable using Different Color Codes.

Learning outcome: Able to understand basic computer network technology.

Duration: 5 hour

List of Hardware/Software requirements:

1. Computer/Laptop/Mobile
2. Internet connection

Procedure:

The use of Block Sender frequently.

Select the spam email, right-click, choose the Junk from the drop menu, and click on Block Sender. Or, Select Home > Junk > Block Sender. The Outlook marks it and relocates it immediately.

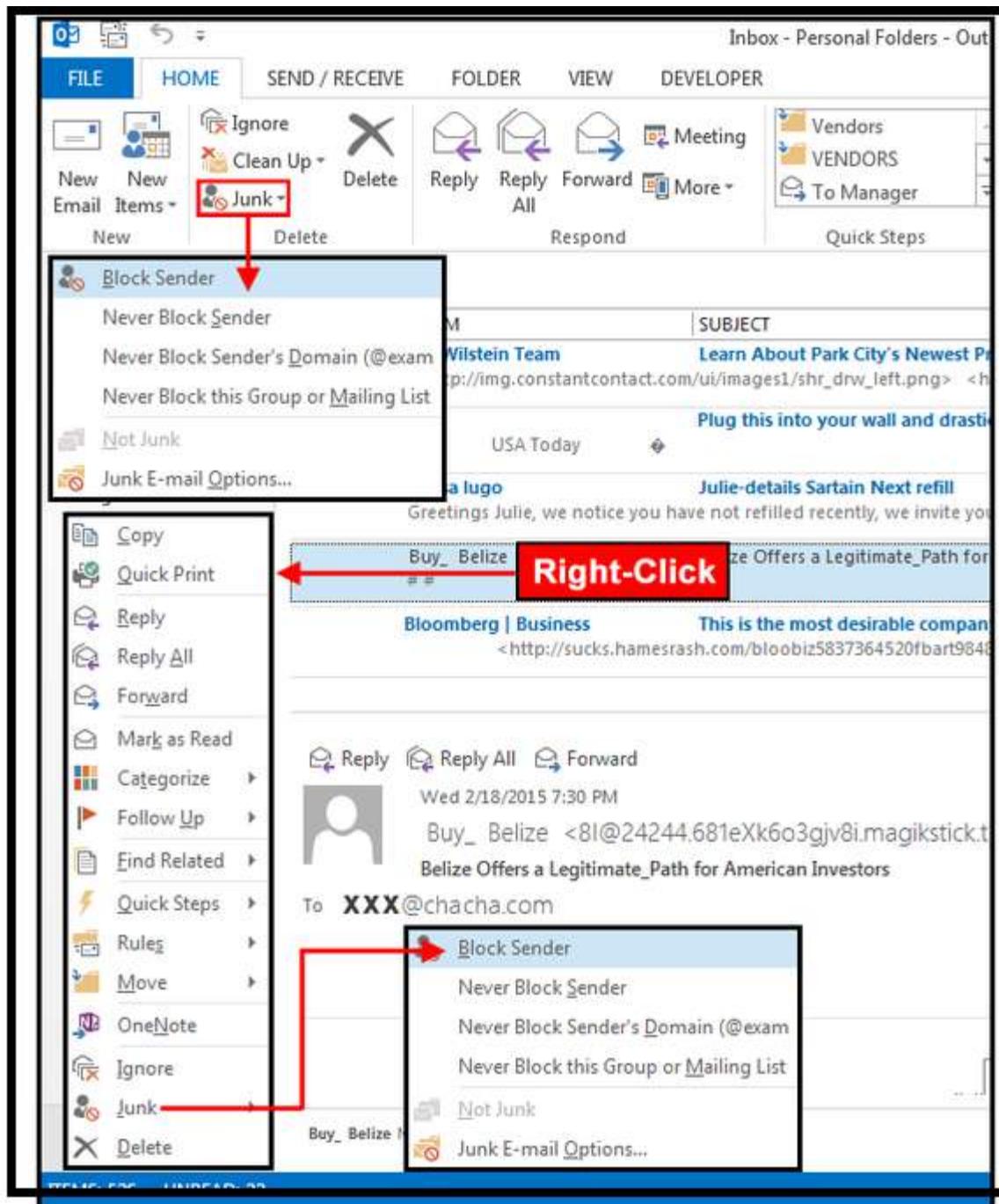


Figure 22: Forward email message

Use Block Sender frequently to automatically increase the senders to Junk Email folder.

Second Procedure:

Step 1:

Select the email address to block and open it.

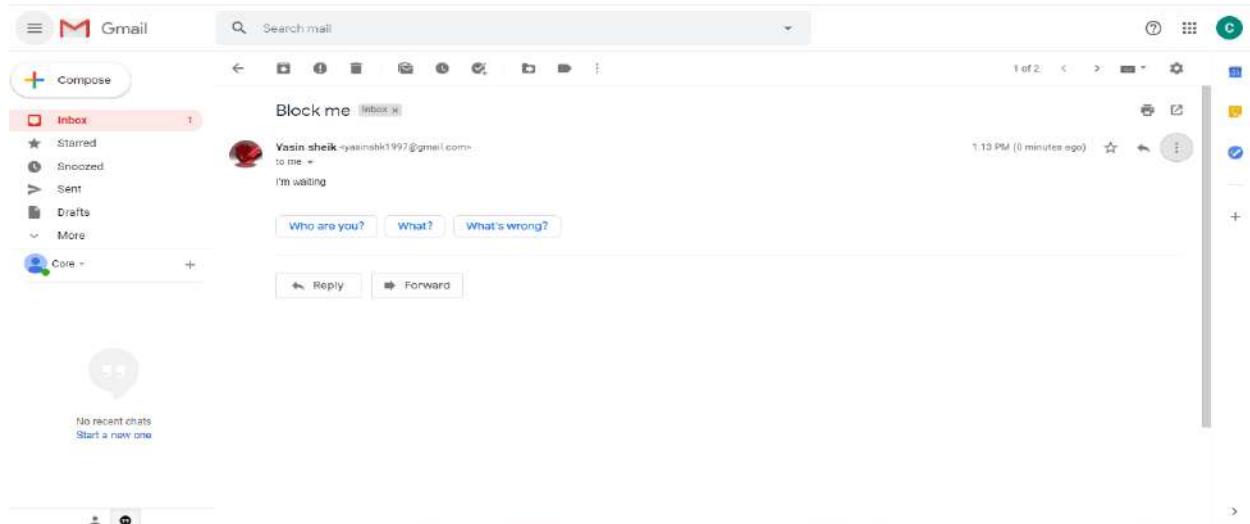


Figure 23: Selecting and opening the blocking email address

Step 2:

Click on 3dots from the right top corner.

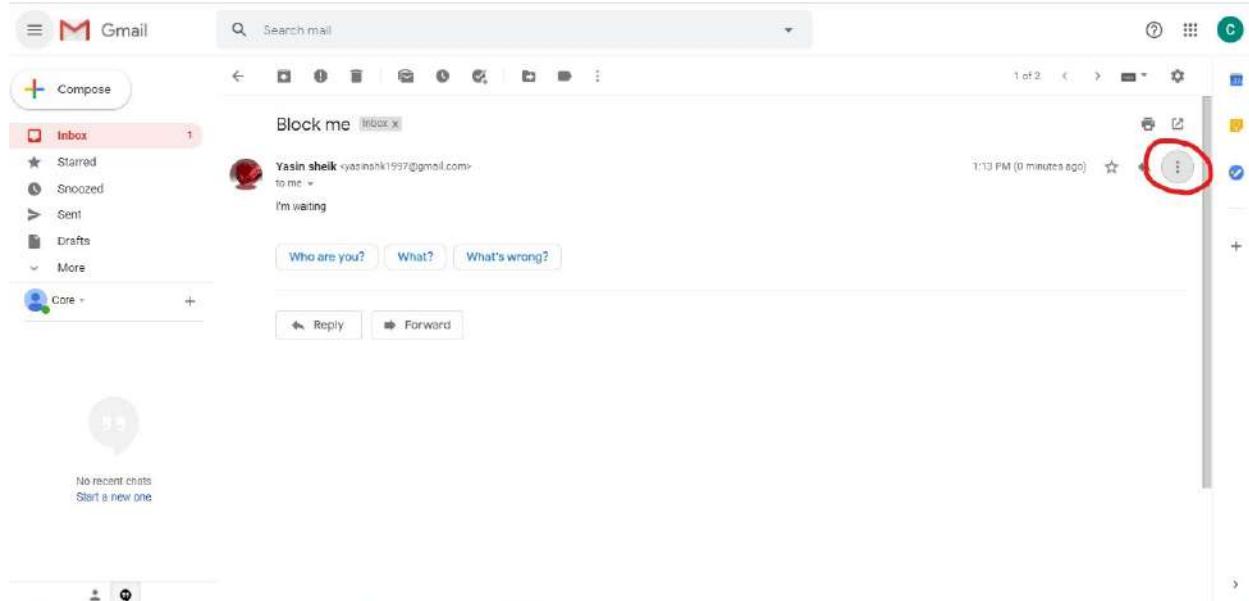


Figure 23: Click on the 3dots

Step 3:

Select the Block from the drop down menu. Once you select the block from the drop down menu. The selected email address will be block.

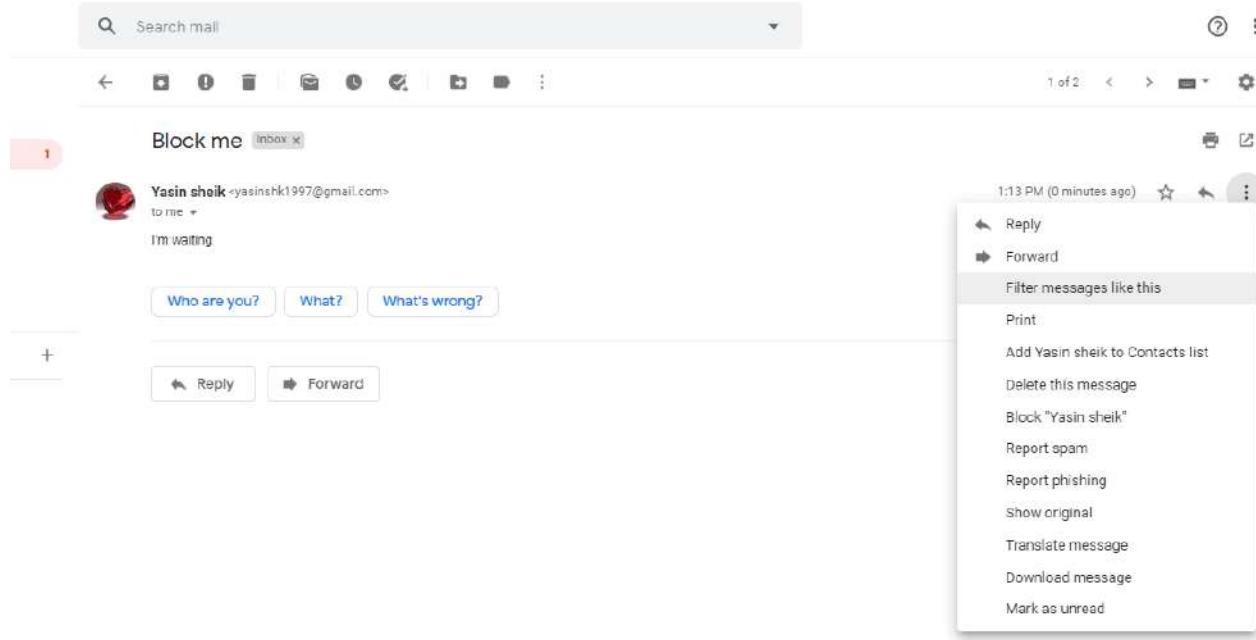


Figure 24: Select block

Step 4:

Confirm the blocking. By clicking the Block again.

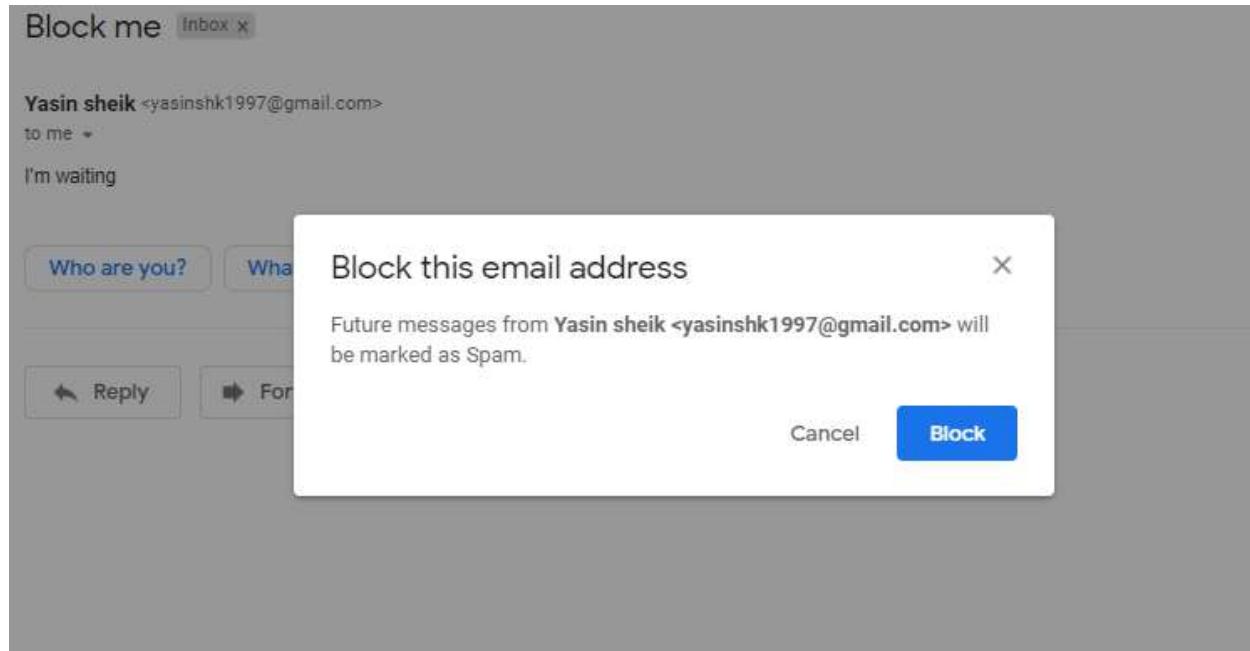


Figure 25: Confirm Blocking

After the blocking you can see the confirmation like this

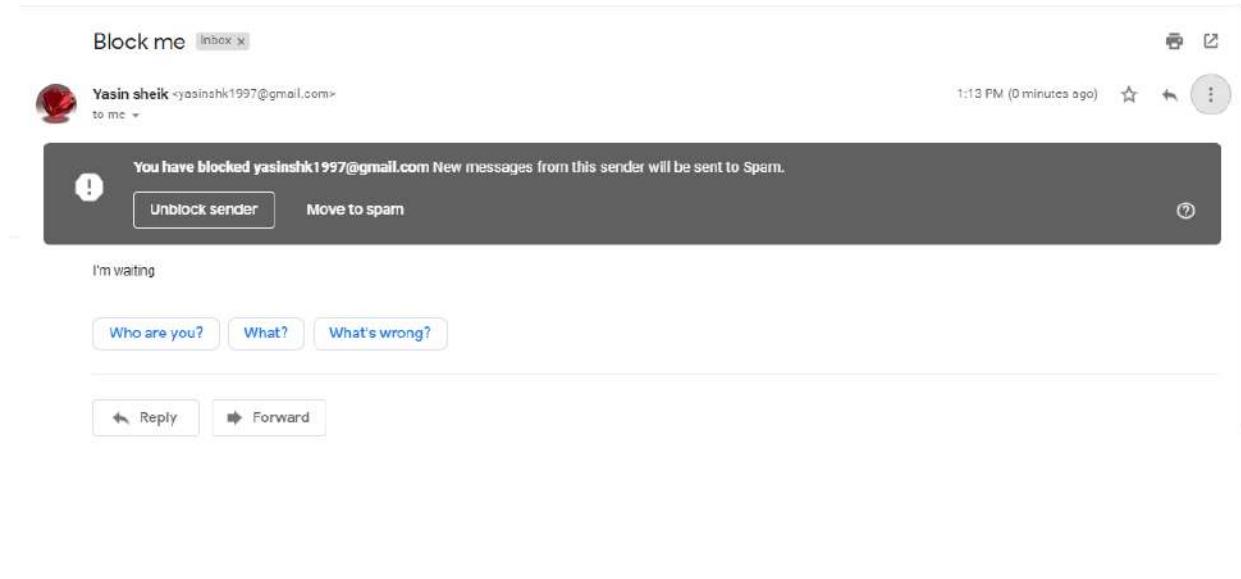


Figure 26: Blocking Message

Step 5:

You can click setting's icon on top right corner

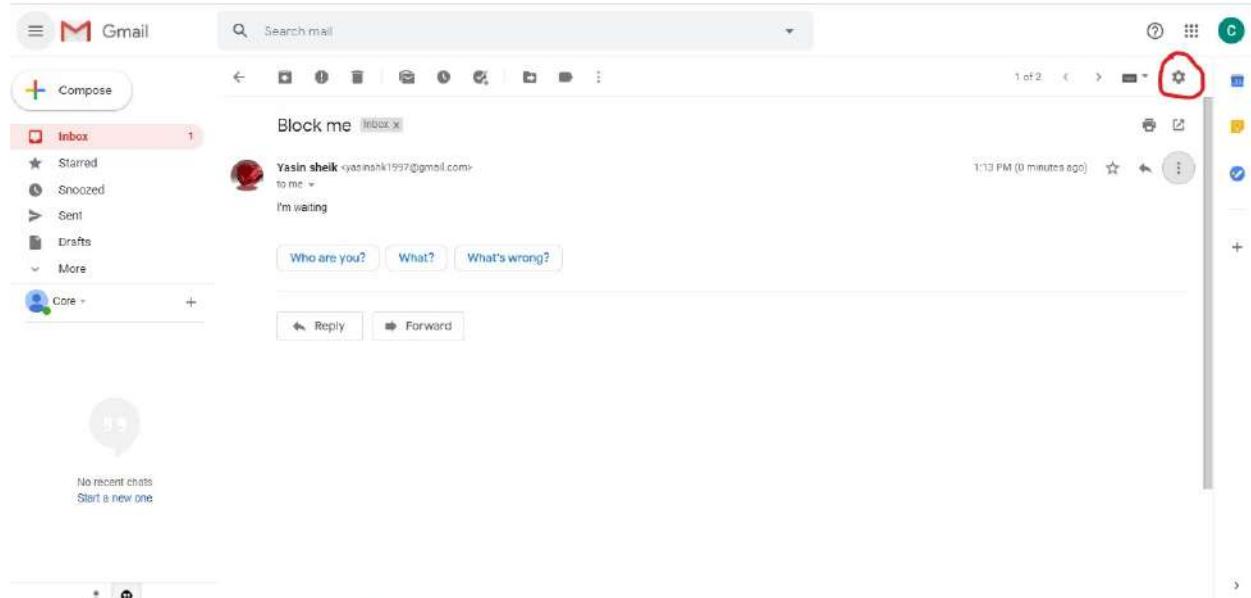


Figure 27: Click on setting's icon

Step 6:

Choose settings from drop down menu

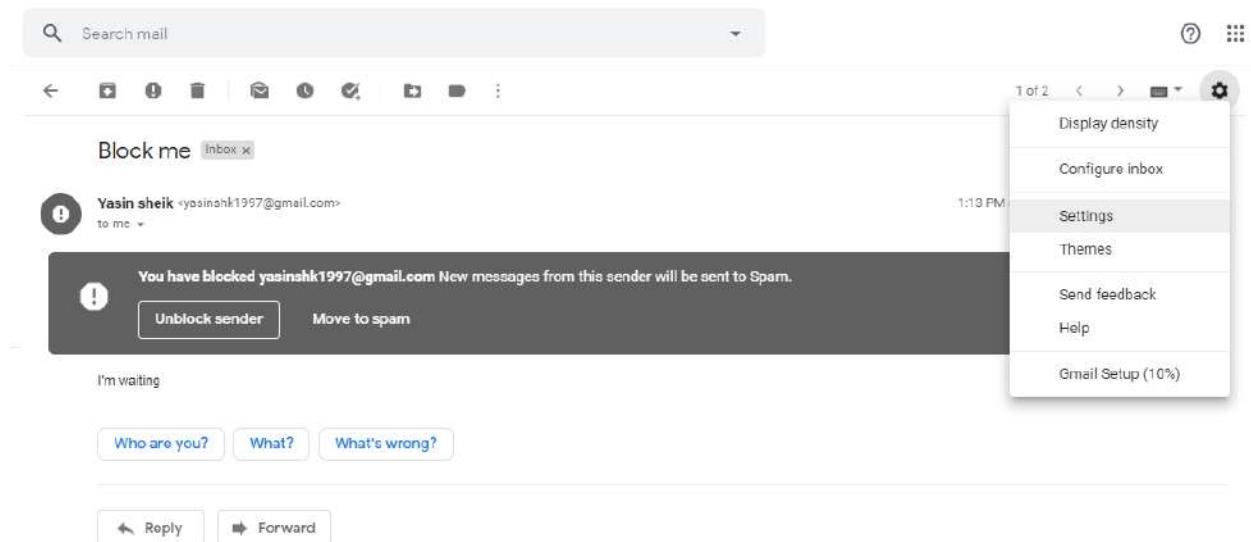
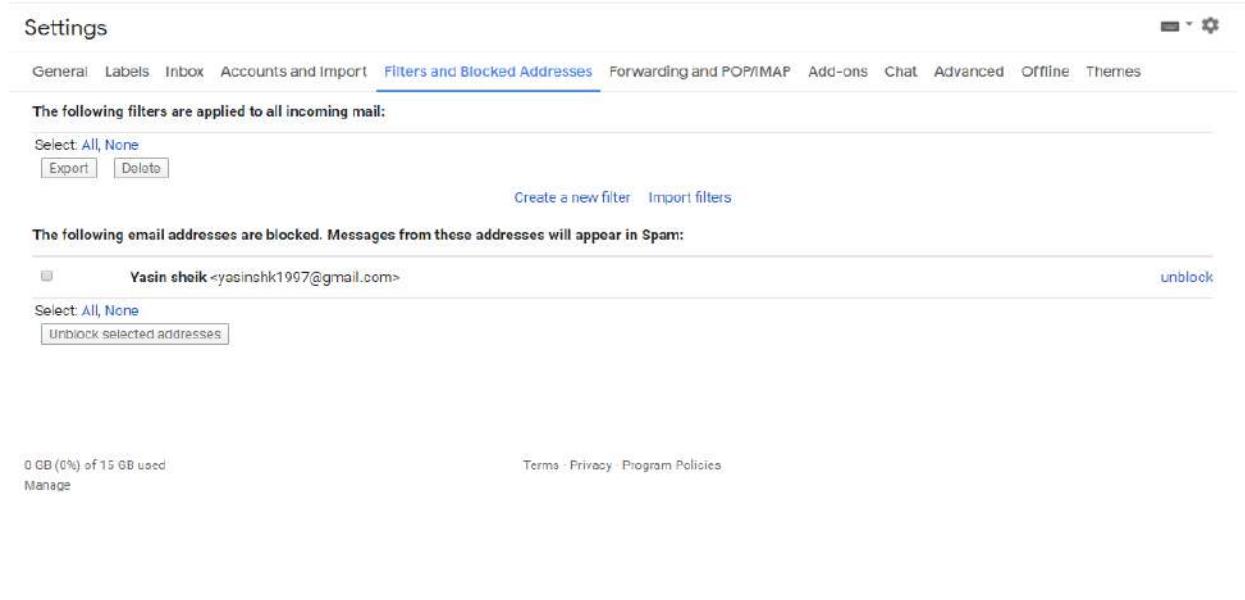


Figure 28: select settings

Step 7:

Select Filters and Blocked Addresses from the navigation menu. You can find all blocked email addresses over there. You unblock the email address from there itself.



The following filters are applied to all incoming mail:
Select: All, None

The following email addresses are blocked. Messages from these addresses will appear in Spam:
 Yasin sheik <yasinshk1997@gmail.com>
Select: All, None

0.000 GB (0%) of 15 GB used [Manage](#) [Terms](#) [Privacy](#) [Program Policies](#)

Figure 29: Checking Filters

References: <https://support.google.com/>

Activity 10

Aim: Store download file in mail drives

Learning outcome: Able to get familiarized with internet and E-Commerce sites.

Duration: 2 hour

List of Hardware/Software requirements:

1. Computer/Laptop/Mobile
2. Internet connection

Procedure:

Downloading a file from Gmail

1. Open your gmail account and search for the email address from where you want to download a file.

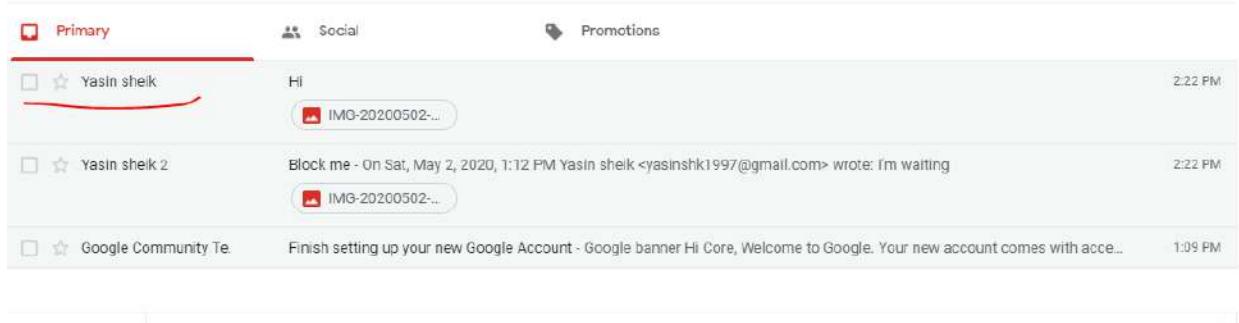


Figure 30: Select the email address.

-
2. Open that particular email address and locate the attachment/file you want to download.

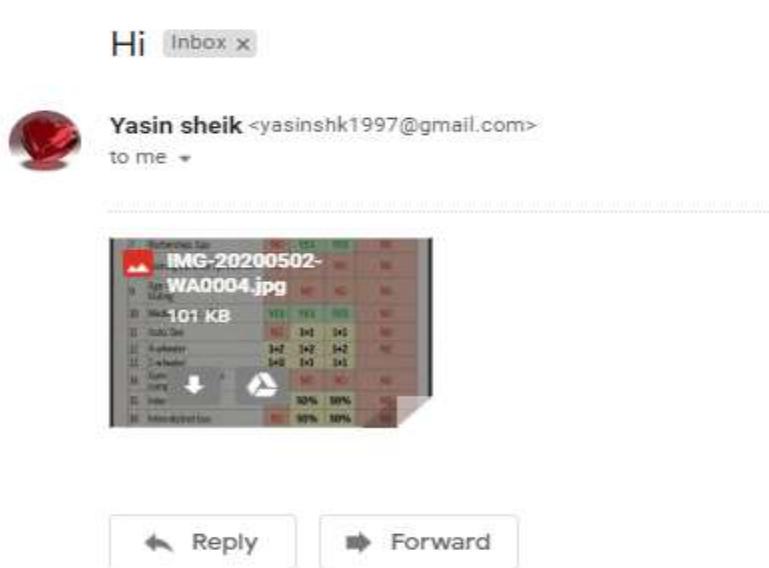


Figure 31: Locating the attachment/file

3. Keep your mouse on that attachment and find the download icon.

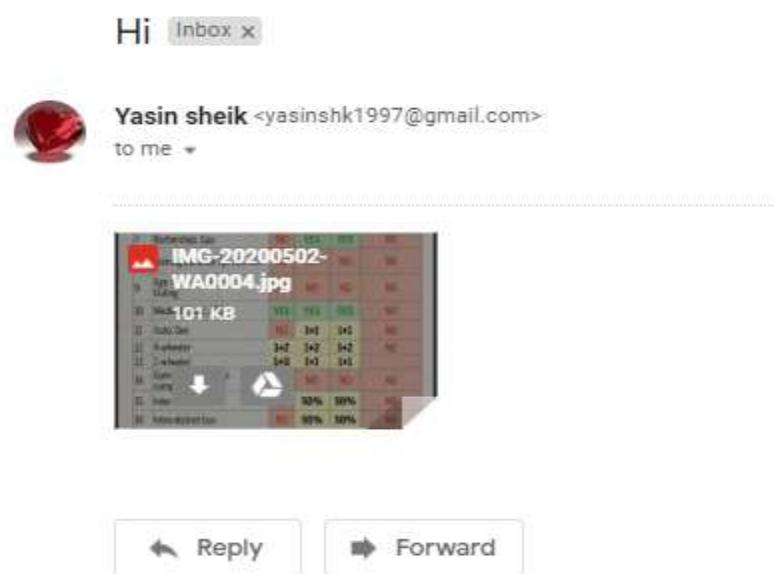


Figure 32: Keep the mouse on the attachment/file

4. Click on the download icon
5. Once you click on the download, it will ask you the location to save the file.

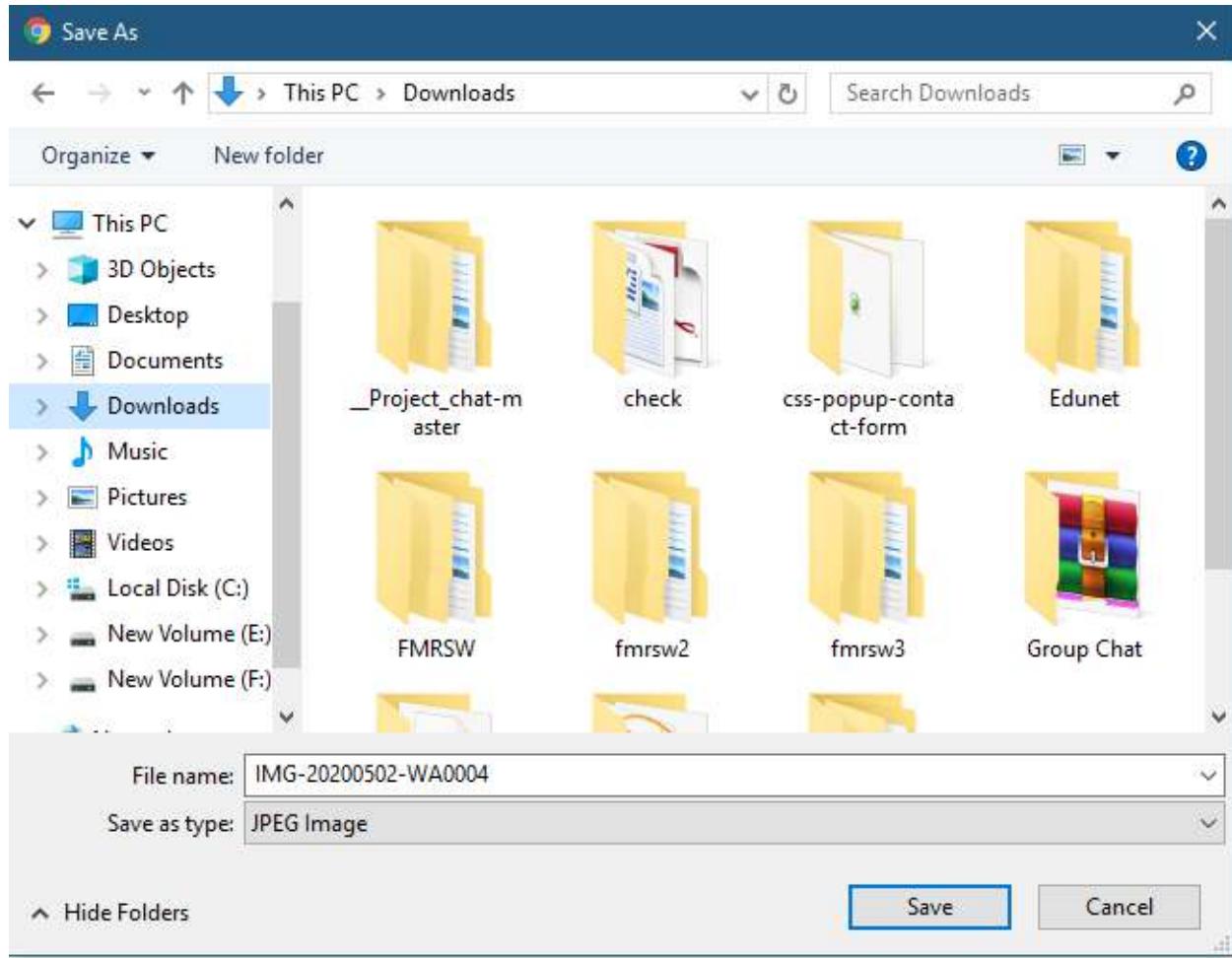


Figure 33: Choosing the file location

6. Choose the location to save the file and click on save

Saving a file to drive from Gmail

1. Open your gmail account and search for the email address from where you want to save a file to drive.

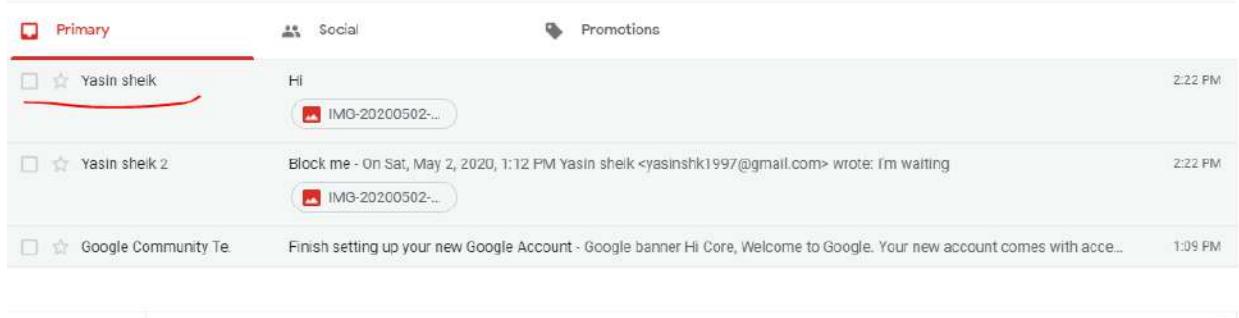


Figure 34: Select the email address.

2. Open that particular email address and locate the attachment/file you want to save to drive.

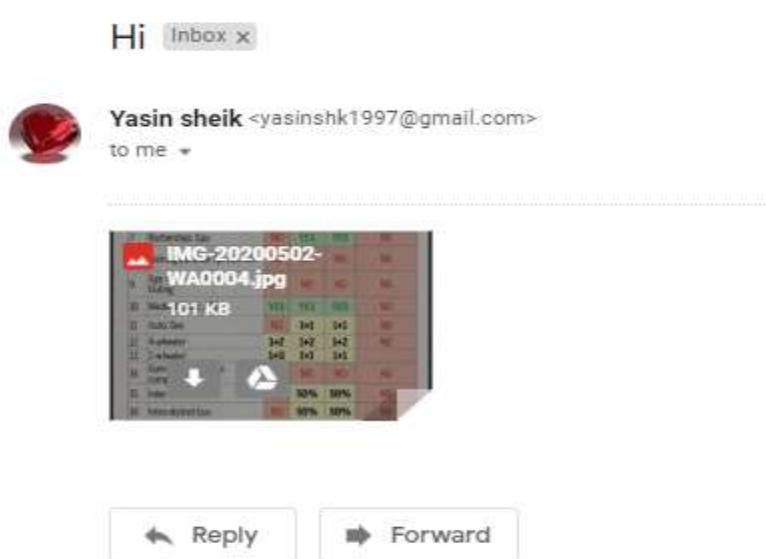


Figure 35: Locating the attachment/file

-
3. Keep your mouse on that attachment and find the save to drive icon.

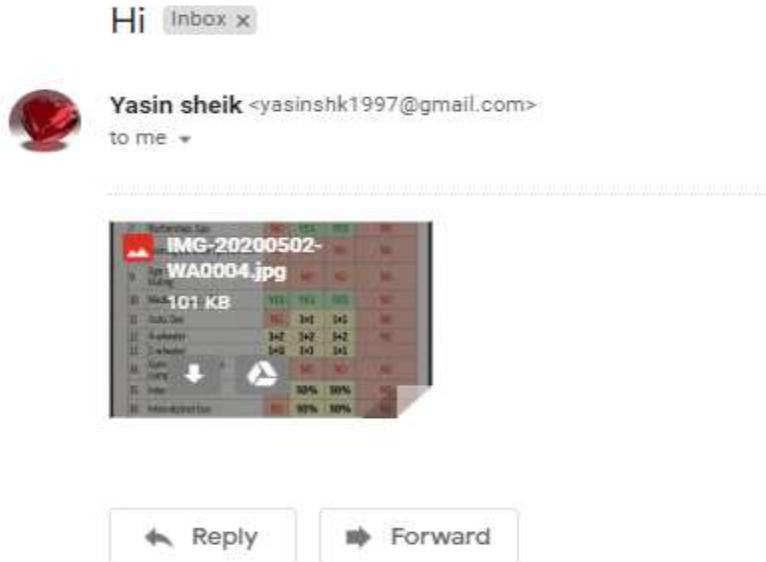


Figure 36: Keep the mouse on the attachment/file

4. Click on the save to drive icon
5. Once you click on that you will get a confirmation message as shown below.

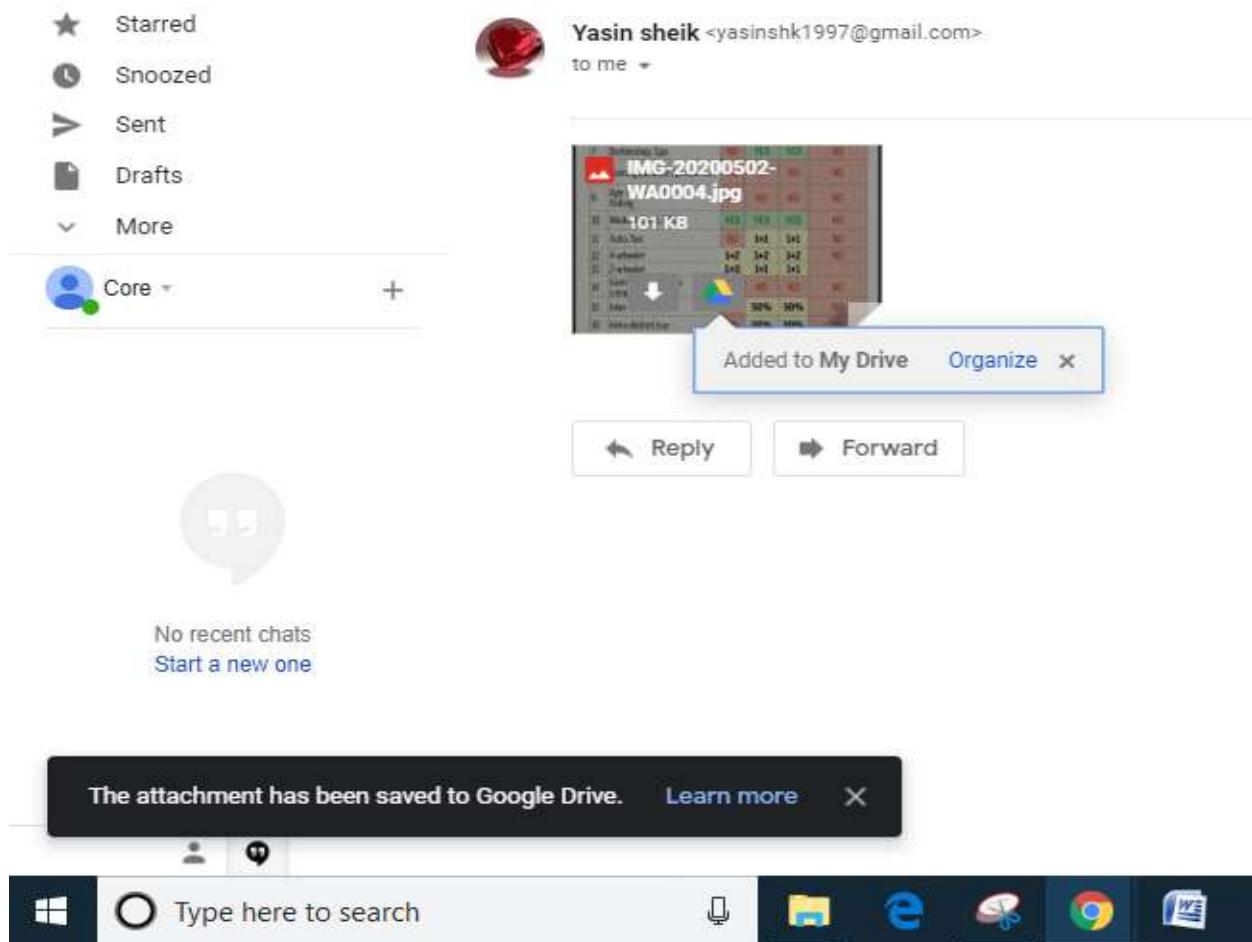


Figure 37: Confirmation message.

References: <https://support.google.com/>

Activity 11

Aim: Communicate using text, video chatting and social networking sites

Learning outcome: Able to get familiarized with internet and E-Commerce sites.

Duration: 2 hours

List of Hardware/Software requirements:

1. Computer/Laptop/Mobile
2. Internet connection.

Procedure:

Communicate using Text

- In a hangout application the communication using text.

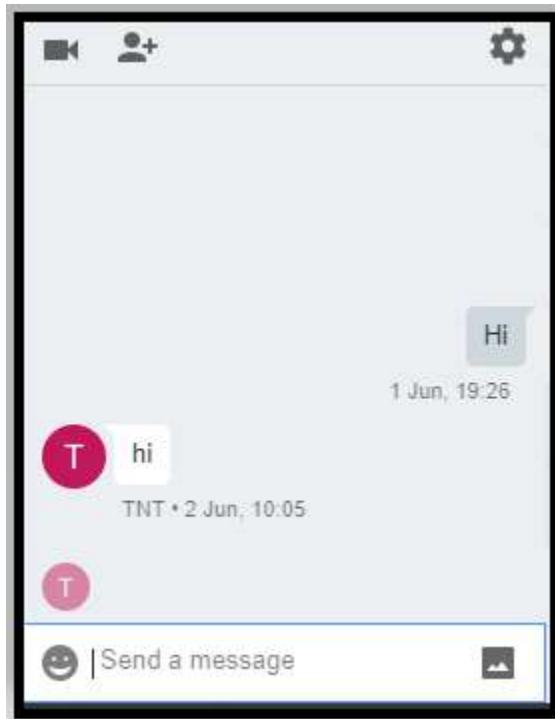


Figure 38: Communication using Text

Video Chatting



Figure 39: Video Chat

Social Networking sites

The social networking sites are

- Facebook
- Twitter
- LinkedIn
- YouTube
- Instagram
- WhatsApp

Reference: <https://support.google.com/search?q=how+to+chat+through+hangouts>

Activity 12

Aim: Protect the computer against various internet threats

Learning outcome: Able to get familiarized with internet and E-Commerce sites.

Duration: 3 hours

List of Hardware/Software requirements:

Procedure:

To protect the computer from the above threats certain rules to be followed.

Never disclose the LastPass master password to anyone.

- Always use and make sure the anti-virus, anti-malware, and firewall software are up-to-date.
- Not ever click on any links in emails unless you specifically requested that the email is sent to you. Even then, if it looks out of character, double-check with the sender before opening a link or attachment.
- Never accept that any email you receive was sent by the recipient listed as the sender.
- Avoid using untrusted PCs or untrusted PC networks.
- Only download apps from main companies and check all approvals before completing the download.
- Use LastPass to automatically fill login identifications for websites you visit to avoid the risk of phishing attacks.
- Use multifactor confirmation for increased security.

Reference:

<https://support.google.com/search?q=Protect+the+computer+against+various+internet+threats>

Activity 13

Aim: Browse ecommerce website.

Learning outcome: Able to get familiarized with internet and E-Commerce sites.

Duration: 1 hour

List of Hardware/Software requirements:

1. Computer/Laptop/Mobile
2. Internet connection

Procedure:

Step 1

Browse e-commerce website – type has <https://www.amazon.in/> in the URL. Create an account and Sign In with the account and the Amazon home page appears on the screen.

Step 2

Place order for items – In the search field enter the item name and press enter. The list of the items displayed on the screen and select an item from the list.

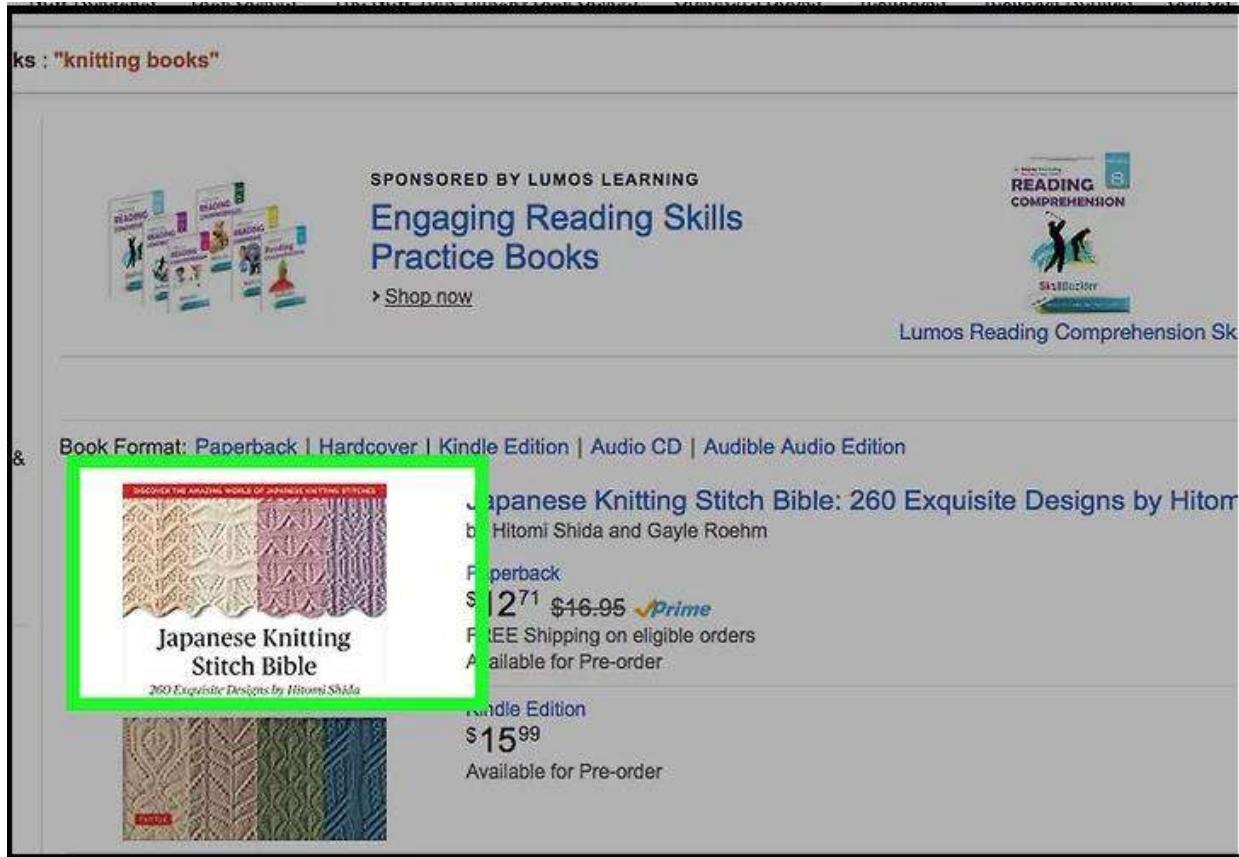


Figure 40: Place order for items

Step 3

Add items to shopping Carts –This will take to a page confirming that the item is in your cart. Amazon will also show the related items that user may be interested in purchasing.

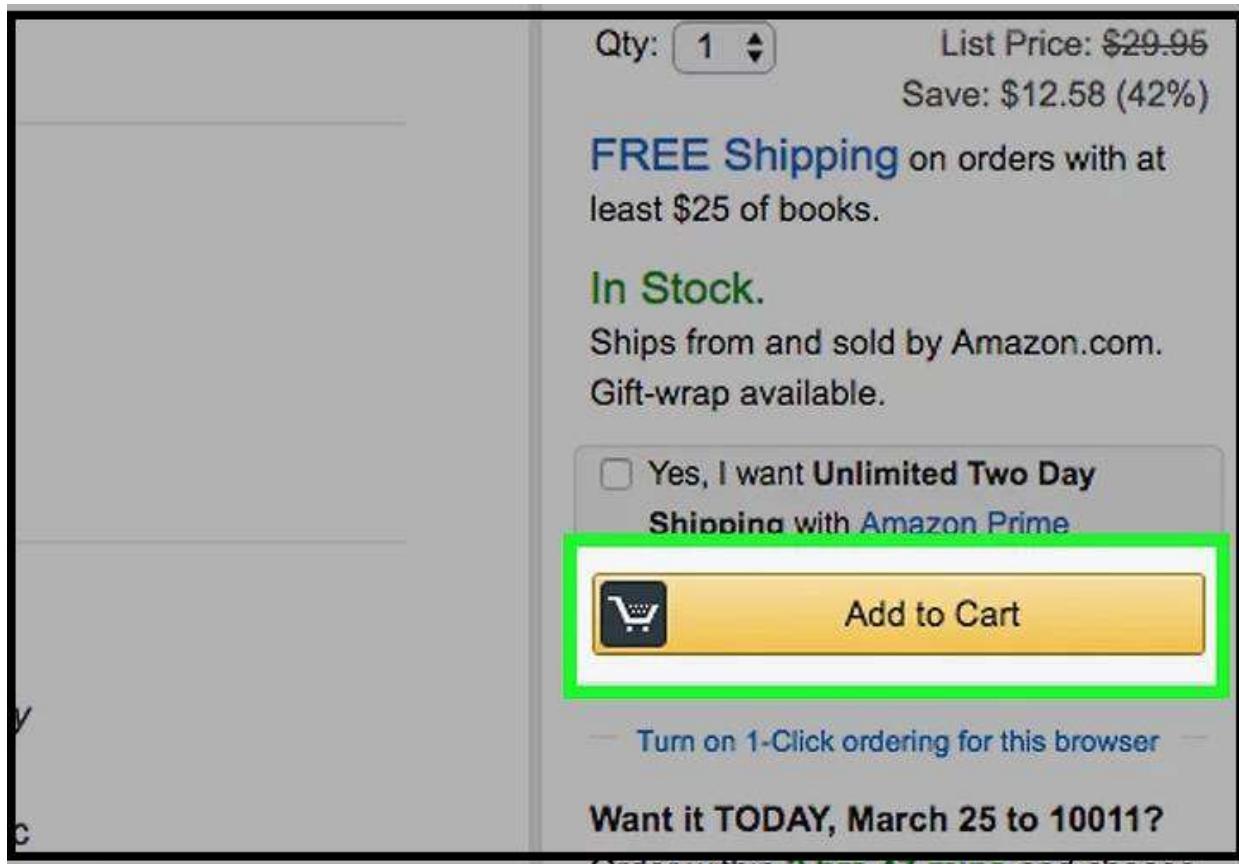


Figure 41: Add items to shopping Cart

- Click on the Cart icon- Review all the items that you are ordering. If you need to change or remove items, you can type the correct number you want into the Quantity box.

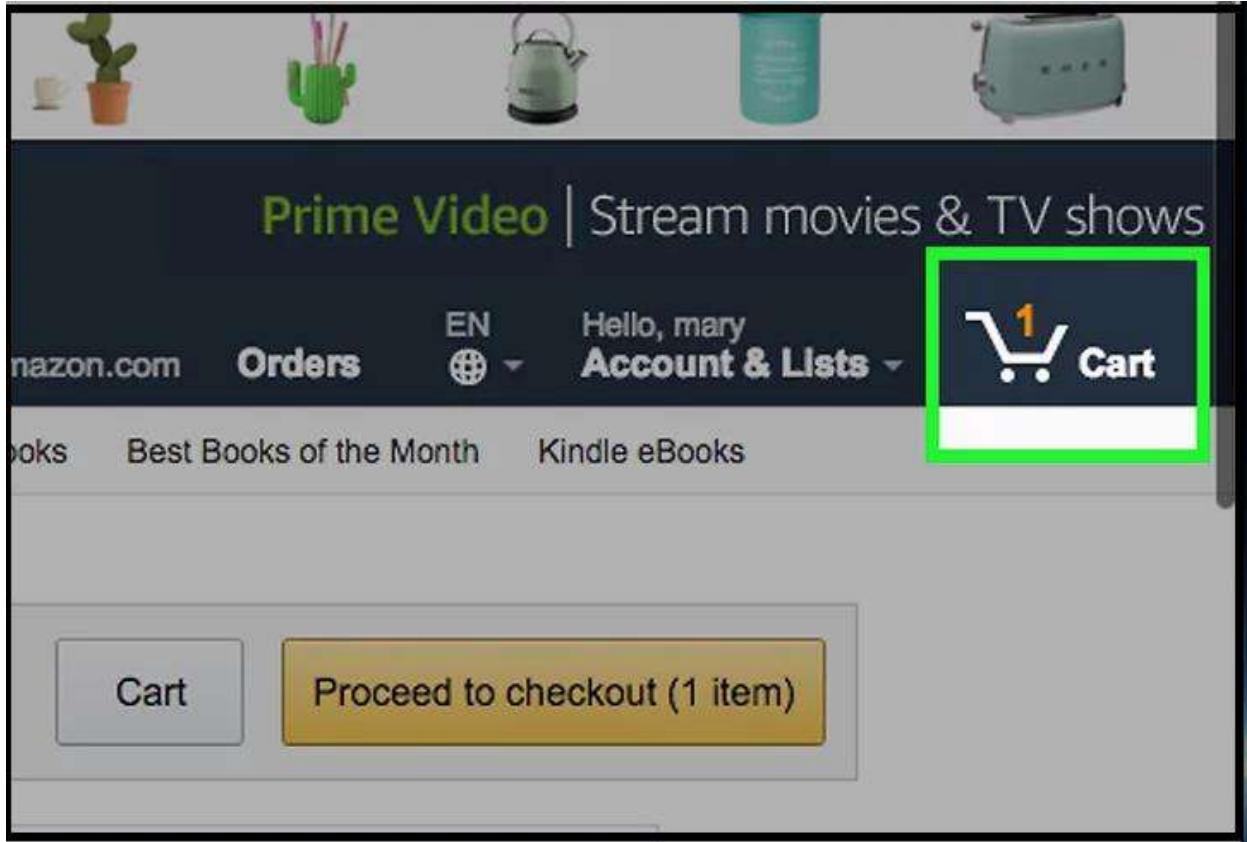


Figure 42: Cart icon- Review

- Click on Proceed to Checkout- Amazon will ready you to choose the correct address and payment method for your order.



Figure: 43: Proceed to Checkout

Choose the shipping address.

The form is titled "Add a new address". It contains fields for Full name, Address line 1 (Street address, P.O. box, company name, c/o), Address line 2 (Apartment, suite, unit, building, floor, etc.), City, State/Province/Region, and ZIP. A green border highlights the entire form area.

Figure 44: Shopping Address

- Click on Deliver to this address button.

Step 4

Do online payment through payment gateways or another payment method

- Select the payment method.

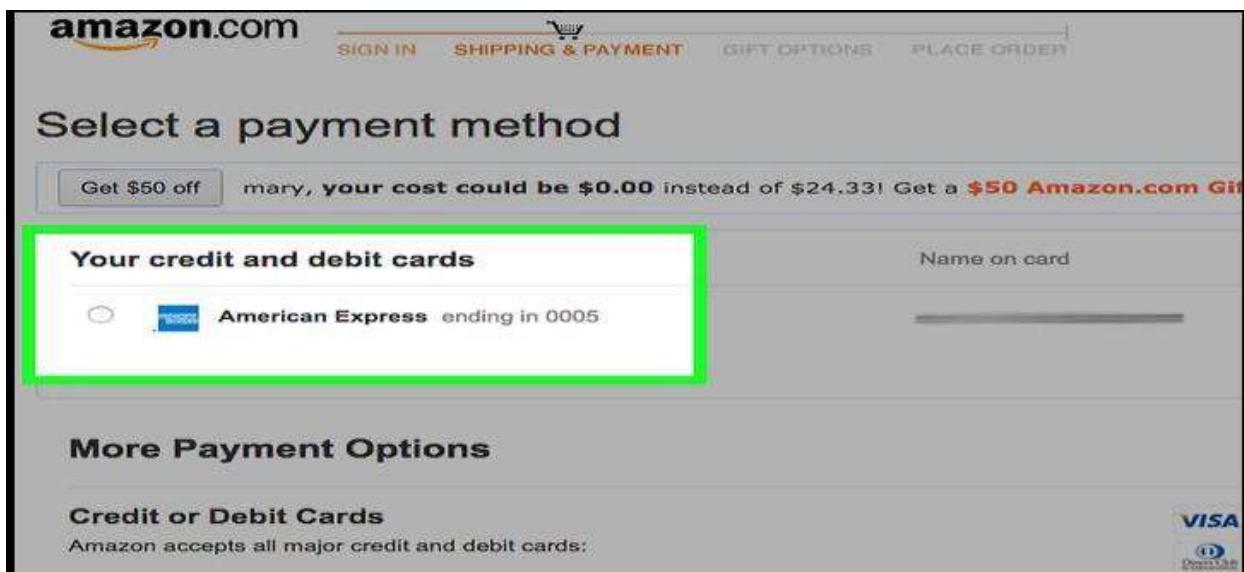


Figure 45: Online Payment

- Click on Place your Order- After you have finished your order, Amazon will show you your confirmation details. Moreover, each item's estimated arrival date will appear.
- Check the mail- Amazon will send a confirmation email to the address.

Step 5

End with Logout

Reference: <https://www.amazon.in/gp/help/customer/display.html?ie=UTF8&nodeId=508510>