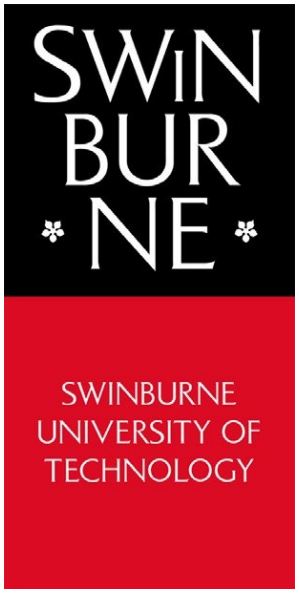
TNE10005/TNE60002

Network Administration

Lab 1

An Introduction to Network Administration Labs



Aim:

- To have an overview of the units' lab infrastructure and resources
- To learn how to use Hyper-V at an introductory level in ATC626 lab and Network Administration Azure lab

Preparation:

- View "*Lecture 01 Presentation – Topic 2: Network Devices"*
- Read "Lab Class Journal Submission requirements"

Resources:

- Network Administration Lab - Network Topology
  https://swinburne.instructure.com/courses/54080/files/25126972?module_item_id=3553708
- Microsoft Unit: Using Virtual Machines – Recommended Best Practices (Video)
  https://swinburne.instructure.com/courses/54080/files/25126713?module_item_id=3553711
- An Introduction to ATC626 Lab
  https://swinburne.instructure.com/courses/54080/pages/an-introduction-to-atc626-lab?module_item_id=3553709
- How to Connect to Network Administration's Azure Labs
  https://swinburne.instructure.com/courses/54080/files/25126976?module_item_id=3553710
- Accessing and Downloading Software from Microsoft Azure for Education
  https://azureforeducation.microsoft.com/devtools
- "Get Started with Windows Server 2022"
  https://docs.microsoft.com/en-us/windows-server/get-started/server-basics
- Windows Server 2022, Versions: Standard or Datacenter, 64-bit (English) iso image at
  https://azureforeducation.microsoft.com/devtools

Introduction to Network Administration - Practice Environment

Network Administration students, to practice weekly, can use a computer in ATC626 computer lab and/or the virtual machine allocated to them in this unit's Azure lab. A computer in ATC626 lab or an allocated virtual machine in the unit Azure lab is called the ***Host Machine*** since it will host other virtual machines used for practice.

In order to understand network concept and technologies learnt in the units, there is a set of machines with different operating systems installed, and with different roles as in *Fig.1 Network Administration Lab – Network Topology*.

- **sWin22RTR** is a machine that is installed with Windows Server 2022 and functions as a Router.
- **sWin22DC1** is a machine that is installed with Windows Server 2022 and functions as a DHCP server, a DNS server and a Domain Controller.
- ***sWin10PC201*** is a machine that is installed with Windows 10 in a Workgroup.
- ***sWin10CL101*** is a machine that is installed with Windows 10 in the domain sWin.Local.
- *etc.*

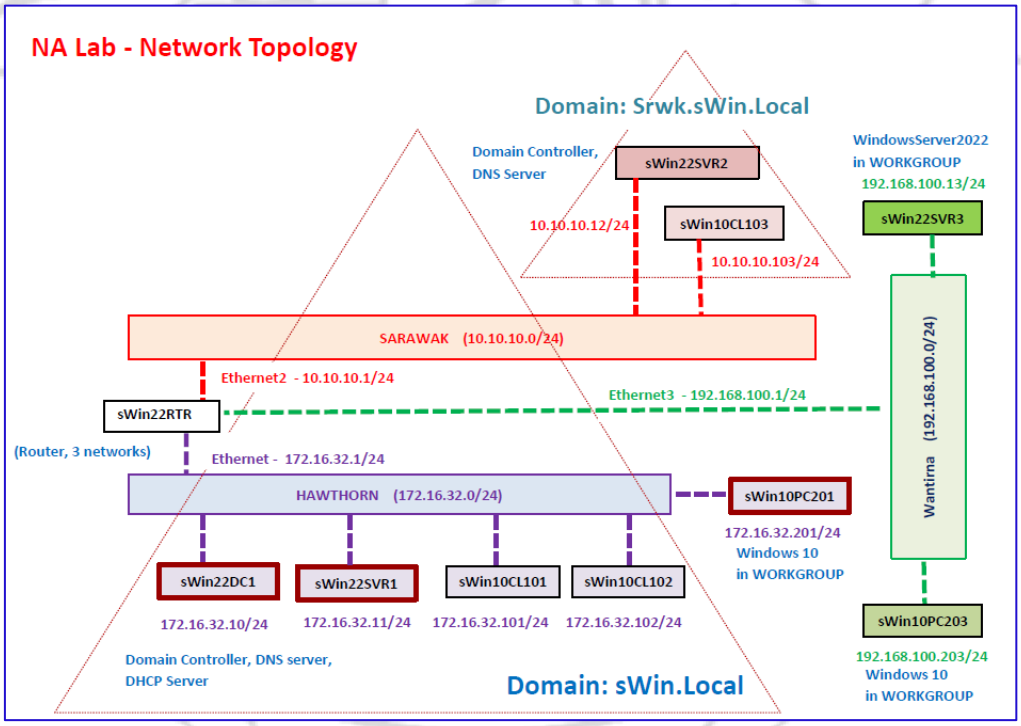


Figure 1: Network Administration Lab – Network Topology

Please be reassured that you will learn such concepts and technologies as DHCP, DNS, Domain, and so on, in the coming weeks, i.e. you will be exploring all components presented in the Network Topology in the following week lab. It is very common that at this stage you might find the Network Topology is complex or you do not know what DHCP server, or DNS server, or Domain Controller is.

Now, by observing the machine names sWin22DC1, sWin22RTR, sWin10PC201, sWinCL101 and the operating system installed in these machines, what operating system do you think is installed in the following virtual machines?

- sWin22SVR1 **Windows Server 2022**
- sWin22SVR2 **Windows Server 2022**
- sWin22SVR3 **Windows Server 2022**
- sWin10CL102 **Windows 10**
- sWin10PC203 **Windows 10**

In *Fig.1 Network Administration Lab – Network Topology,* there are 3 switches named **Hawthorn**, **Sarawak** and **Wantirna**.

- What are the functions of these switches?

  Facilitate communication between the virtual machines (VMs) connected to them
- Which virtual machines are connected to the Hawthorn Switch?

  not listed, have to check Hyper - V manager
- Which virtual machines are connected to the Sarawak Switch?

  same
- Which virtual machines are connected to the Wantirna Switch?

  same

The **sWin22RTR** is a machine that is installed with Windows Server 2022 and functions as a Router.

- What are the functions of routers in general?

Routers manage traffic between networks and direct data packets to their correct destinations.

- What are the functions of the sWin22RTR router?

Routes traffic between virtual machines and provides DHCP services for dynamic IP address assignment.

In the following week lab, we will be exploring further the roles/functions of these machines, switches, and router.

Introduction to Hyper-V.

There are 10 computers/machines required in the **NA lab – Network Topology** for each student using in their practice. It is definitely NOT cost, time, space neither technical efficient for deploying and maintaining 10 physical computers for each student to practise. Hence, we have used Hyper-V virtualisation platform in deploying Microsoft unit labs.

Hyper-V is Microsoft's software is installed and enabled within a computer/machine called **host machine,** for running multiple and independent computers/machines so that they can share the same host machine hardware. The part of the host's operating system that allows the virtual machines to share the hardware is called the *hypervisor*, and this is where Hyper-V gets its name. Computers/Machines that run within the Hyper-V software are called virtual computers, virtual machines, or guests. Hence, using Hyper-V, within a single host computer in the ATC626 lab or within a single virtual host machine in the unit Azure lab, the 10 ***Guest Virtual Machines*** (sWin22DC1, sWin22RTR, sWin10CL101, etc.) are hosted.

Most current computers (i.e. those built since 2012) have processors that support virtualisation with hypervisors. Microsoft Windows Server 2008 or above with Windows 8 Professional or above can all function as a guest operating system for Hyper-V. Unfortunately, the home editions of Windows 8 & Windows 10 do not support Hyper-V.

It is optional for this unit, but if you would like to learn how to install Hyper-V:

- on Windows 10 Professional, click here, or
- on Windows Server, click here

Click here to learn how to set up Hyper-V and create a virtual machine in Hyper-V.

However, keep in mind that you need lots of RAM, and lots of free disk space.

If you do not have a host operating system that supports Hyper-V then you may be able to use VMware, but remember that the tutors in this unit may not have the experience to help you with these products.

Introduction to Using Hyper-V.

Exercise 1. Using Hyper-V in Network Administration Azure Lab

We will start with using Hyper-V in the *Network Administration Azure lab*.

Please read the document How to Connect to Network Administration's Azure Labs in the Module ***Laboratory Exercises*** on Canvas.

Note: You must have received an invitation email from Microsoft with your link to your Host Virtual Machine. If this email is not in you student email, please first check your junk mail folder and if it is not in your email, post a request in an appropriate thread in Ed Discussions.

1. Loading the Hyper-V Manager

The Hyper-V Manager icon should appear on your desktop or toolbar.

Figure 2: Hyper-V Manager Icon

Double clicking the Hyper-V Manager icon will launch it. If the icon is missing on your computer press the **Win** key (⊞) and then select **Hyper-V Manager.**

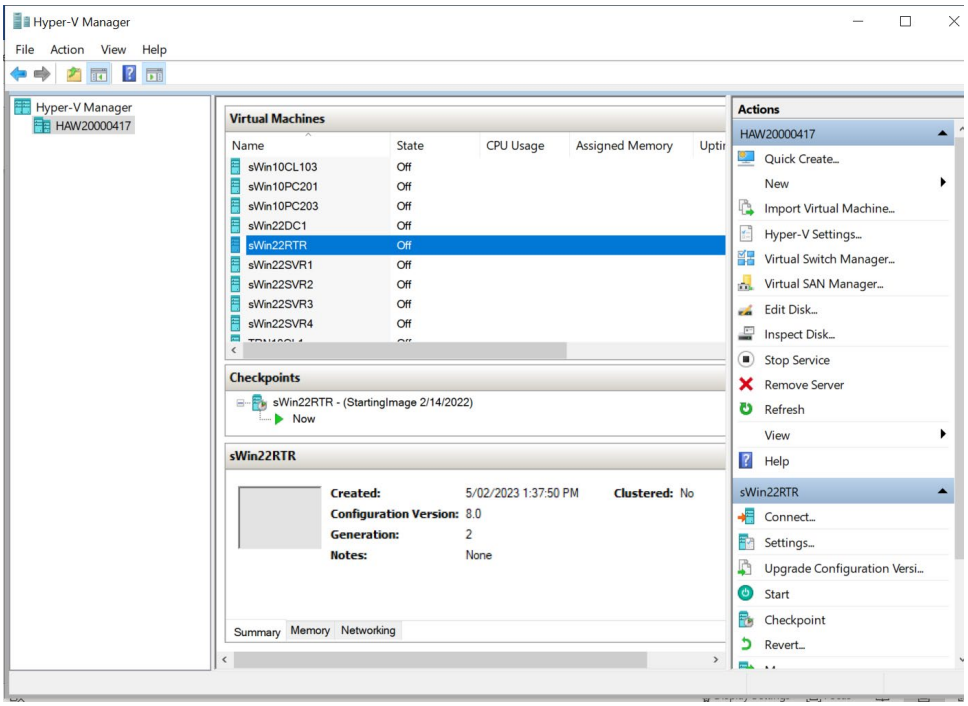


Figure 3: Hyper-V Manager Interface

In the Hyper-V manager interface, notice the panes Virtual Machines and Actions. We will be mainly using these panes in this lab.

2. Viewing and Creating Virtual Switches

a. From the Actions pane of **Hyper-V Manager** select **Virtual Switch Manager…**

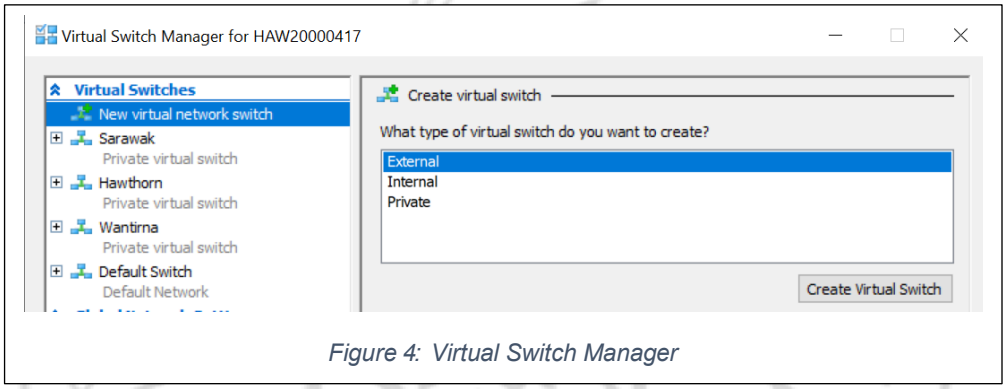


Figure 4: Virtual Switch Manager

Notice that at the top left, under Virtual Switches, you can see the existing virtual switches, i.e. Sarawak, Hawthorn and Wantirna switches created as parts of the unit's Network topology.

b. Now, let's create a new virtual switch for computers in Croydon location to connect to, from the **Create virtual switch** windows, click the button **Create Virtual Switch**.

In the **Name:** field, enter the name **Croydon**. In the **Notes:** field, enter a note that lets others know that you created the switch for this lab. Configure the **Connection type** to be a **Private network.** Click **OK.**

3. Examining the Properties of a Virtual Machine (VM)

a. In the most left pane, click on <*ComputerName*> (i.e. **23s1NetAd-Host**) beneath the Hyper-V Manager.

b. In the Virtual Machines pane, right-click any VM, i.e. ***sWin22SVR3***. You will see the options Connect, Settings, Start, Checkpoint and Revert.

c. To view the properties of the VM, click on **Settings**.

- How much RAM has been allocated to this VM: **1024 mb**
- Which controller has the VM's hard disk attached? **SCSI Controller**
- What network is the VM attached to: **Wantima**

Notice that at the top left of the settings window you can change the VM focus, i.e. you can choose other VMs to change the settings of.

d. Click on **Cancel**.

4. Virtual Machine – Checkpoints and Reverting

Each guest VM in a computer in ACT626 lab or in a host VM allocated to each student in the unit Azure lab has been deployed with a Checkpoint, named **StartingImage,** in which the VM has been configured with correct settings and roles as designed and detailed in the Lab Network topology.

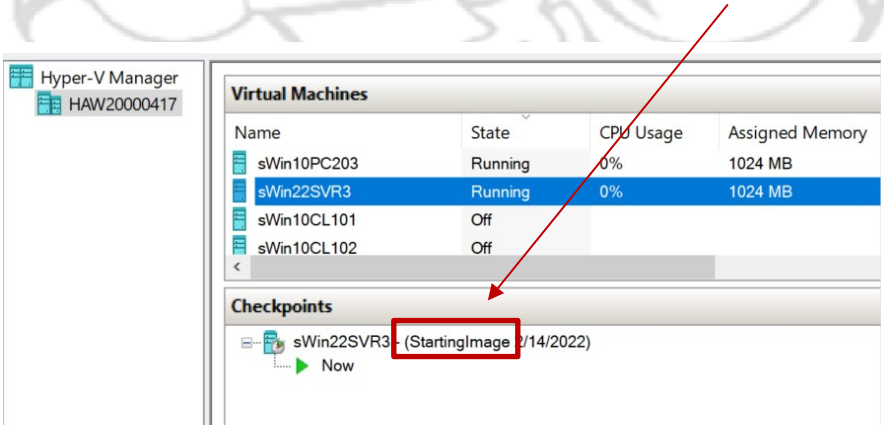


*Figure 5: The **StartingImage** Checkpoint*

Please note that we will not be creating any additional checkpoints in ATC626 lab neither in Azure labs, but it is very useful if you have the VM set deployed in your own computer. A checkpoint will save the state of a virtual machine at a particular point of time, hence it enables to revert the VM back to that point of time configuration.

During the semester, students will likely practise on different learnt concepts and technologies by configuring different settings and roles. These practice require VMs without unwanted errors or pre-configured (i.e.by previous lab class students). Hence, to prevent unwanted and unknown errors, students are instructed to successfully **revert (**i.e. reverting returns without errors) a VM prior to launching it for using.

Reverting deletes the changes and reverts the VM back to the state when **the last Checkpoint** was made. Since there is only one checkpoint (the *StartingImage* checkpoint) was created for each VM when the lab was deployed, the **revert** action in the unit lab instructions means reverting a VM back to its StartingImage.

Now, let's try this Revert feature!

We will first launch/start a VM (i.e. **sWin22SVR3)** that has been reverted to its StartingImage, observe the original settings; make some changes; then revert the VM back to its original state (its StartingImage).

a. Right click **sWin22SVR3**, and select **Settings**.
   Which virtual switch that this VM is connected to? **Wantirna**
   (Hints: Look under **Hardware – Network Adapter)**

b. Now change the Network Adapter to connect to a different virtual switch, i.e. Hawthorn.
   In Settings for sWin22SVR3, under Hardware, click to select **Network Adapter.**
   In the **Network Adapter** window, pull down the **Virtual switch:** and select **Hawthorn,** then click **OK.**

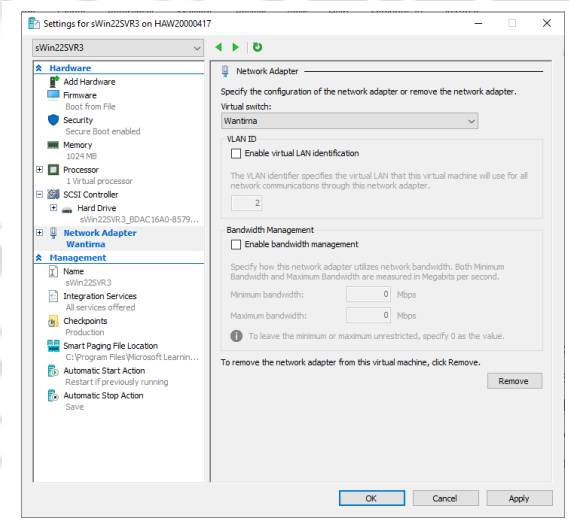


Figure 6: Change Network Adapter settings

c. Right click on **sWin22SVR3**, and select **Start**.

Notice that no window opens, but in the **sWin22SVR3** pane notice there is a thumbnail image of the virtual machine and this shows it is running.

It is important to remember that virtual machines can run in the background. But if we want to interface with it then we need to connect to it.

d. Right click on **sWin22SVR3**, and select **Connect**. A window will now open.

e. Type in the password (**Pa55w.rd**) and either press **Enter** or click on the **Submit** icon (i.e. "→").
*The password **Pa55w.rd** will be the standard password for all user accounts in all labs and exams this semester – so remember it!*

f. When the log in is complete, right- click the **Win** key on the tool bar at the bottom left of the window, the **Start Menu** will pop up.

Figure 7: Windows Start Menu

g. Select **Run**. In the **Open** box, type **cmd** and click **OK**.

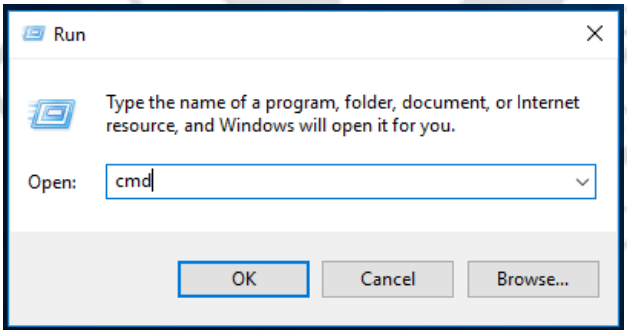


Figure 8: To Launch Command Prompt

h. In the **Command Prompt**, type **ipconfig** and press **Enter**.

i. Record the output for the **Ethernet Adapter** here:

IPv4 Address: **192.168.100.13**

Subnet Mask: **255.255.255.0**

Do not close the **Command Prompt** window since we will use it in the later steps to verify IP settings changes. Hence, just minimise it, click on the – icon on the top right corner of the Window.

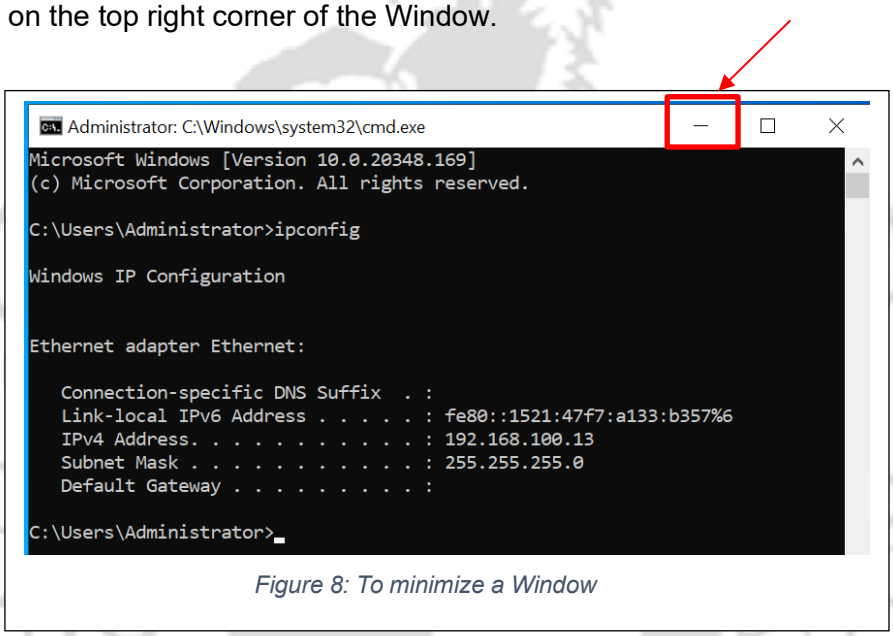


Figure 8: To minimize a Window

We are now going to configure sWin22SRV3's IP settings with IP address of 172.16.32.13 and subnet mask 255.255.0.0

j. On **WsWin22SVR3,** in **Server Manager** Window, click **Local Server** in the most left pane. Below the **properties** section, click the link next to **Ethernet.** In the **Network Connections**, right click **Ethernet** and select **Properties**

Without removing the tick, click on **Internet Protocol Version 4 (TCP/IPv4)**, and select the **Properties** button.

Select **Use the following IP address:** and enter the following details:

- IP address: 172.16.32.13
- Subnet mask: 255.255.0.0

Click **OK** twice.

k. To verify that the IP settings have been changed, click **Command Prompt**  icon on the tool bar, then in the **Command Prompt**, type **ipconfig** and press **Enter**.

Confirm that the IP settings are as what you configured in step (j).

You have made 2 changes to sWin22SVR3:

- Change the Network Adapter connection: from Wantirna to Hawthorn
- IP settings: from IP=192.168.100.13 , SM=255.255.255.0
  to IP=172.16.32.13, SM=255.255.0.0

Assuming that we have completed all practice and would like to delete all changes made to sWin22SVR3, let's perform **revert** action on this VM.

l. Right- click the **Win** key on the tool bar at the bottom left of the window, click **Shutdown or Sign out**, then select **Shutdown.** Click **continue** to accept the default reason to shut down, and proceed to shut down the VM.

m. Back to **Hyper-V manager,** right click **sWin22SVR3**, and select **Revert.…**. In the **Revert Virtual Machine** pop up box, click **Revert** button to confirm that you want to revert the VM to its previous (the latest) checkpoint.

After reverting completes, verify that **sWin22SVR3** has its *original* settings, i.e.

- Network Adapter connection: Wantirna
- IP settings: IP=192.168.100.13 , SM=255.255.255.0

n. In **Hyper-V manager,** right-click **sWin22SVR3**, and select **Settings.** Is the Network Adapter connected to Wantirna? **ye**

Check with your lab supervisor if the result is different!

o. In **Hyper-V manager,** right-click **sWin22SVR3**, and select **Start**.

Again, right-click on **sWin22SVR3**, this time select **Connect.** Click **Connect** (or **Reconnect**).

Type in the password (**Pa55w.rd**) and press **Enter**.

Once the log in is complete, use Command Prompt to verify the IP settings. (Hints: Refer to steps **f-h** in the previous pages)

Are the IP settings the same as what are recorded in step **i**? **ye**

Check with your lab supervisor if the result is different!

Exercise 2. Using Hyper-V in ATC626 Computer Lab (If time permits)

1. Log in to a computer in ATC626 computer lab.
2. Re-do the **Exercise 1.**

Exercise 3. Documenting your digital Lab Journal

1. Read "Lab Class Journal Submission requirements" if you have not done so, in order to best prepare for your learning and assessment.

   The Lab Class Journal is one of the assessments in this unit. A draft is to be submitted in week 4, and the final version in week 12. The Lab Class Journal is where students can record the concepts, design strategies, techniques, configurations and commands that they learn in the laboratory classes. Students can use their Lab Class Journal as a reference during the Skills Assessment in the Final Assessment Period.

2. Record the concepts, design strategies, techniques, configurations and commands that you learn in this week laboratory class.

Do not leave the lab until the pack up stage is complete

Pack Up

1. Shut down all guest VMs.
2. From the **Virtual Switch Manager…,** click on **Croydon**, and then click on the **Remove** button.
3. **Sign out** from the Host virtual machine and make sure that it is **Stopped** otherwise it will run in the background and use up your quota.
4. If on campus, **log off from the ATC626 lab PC,** and push your chair in as you leave.

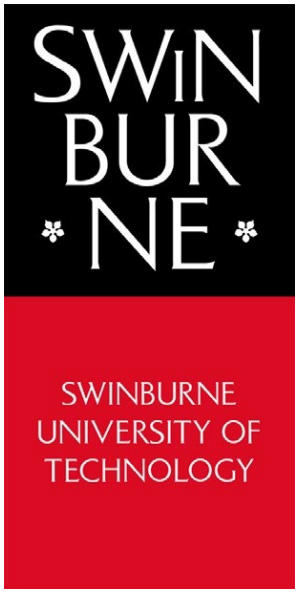
~~~~~ End of Lab ~~~~~

TNE10005/TNE60002

Network Administration

Lab 2

Getting familiar with Network Administration Labs



Aim:

- To obtain an understanding of the roles of virtual switches, software-based router and virtual machines in the Network Administration labs.
- To become familiar with the recommended good practice Network Administration labs.

Note: *For those of you who have studied networking before, this lab will appear deceptively simple. The focus of this lab for experienced students is to explain the observations.*

Lab/Virtual machines

- *NetAdLab* Azure lab
- *sWin22DC1*, sWin22SVR1, Swin10CL101, sWin22RTR and sWin22SVR2.

Preparation:

- View "*Lecture 01 Presentation – Topic 2: Network Devices*"
- Review "Lab Report 1 requirements"
- Complete Lab 1 – Exercise 1

Resources:

- Network Administration Lab - Network Topology
  https://swinburne.instructure.com/courses/57016/files/28232483?module_item_id=3845607
- Microsoft Unit: Using Virtual Machines – Recommended Best Practices (Video)
  https://swinburne.instructure.com/courses/57016/files/28232320?module_item_id=3845610
- How to Connect to Network Administration's Azure Labs
  https://swinburne.instructure.com/courses/57016/files/30187456?module_item_id=4131816

Introduction

Network Administration students, to practice weekly, can use a computer in ATC626 computer lab to connect to the virtual machine allocated to them in this unit's Azure lab. An allocated virtual machine in the unit Azure lab is called the ***Host Machine*** since it will host other virtual machines used for practice, as presented in *Fig.1 Network Administration Lab – Network Topology*.

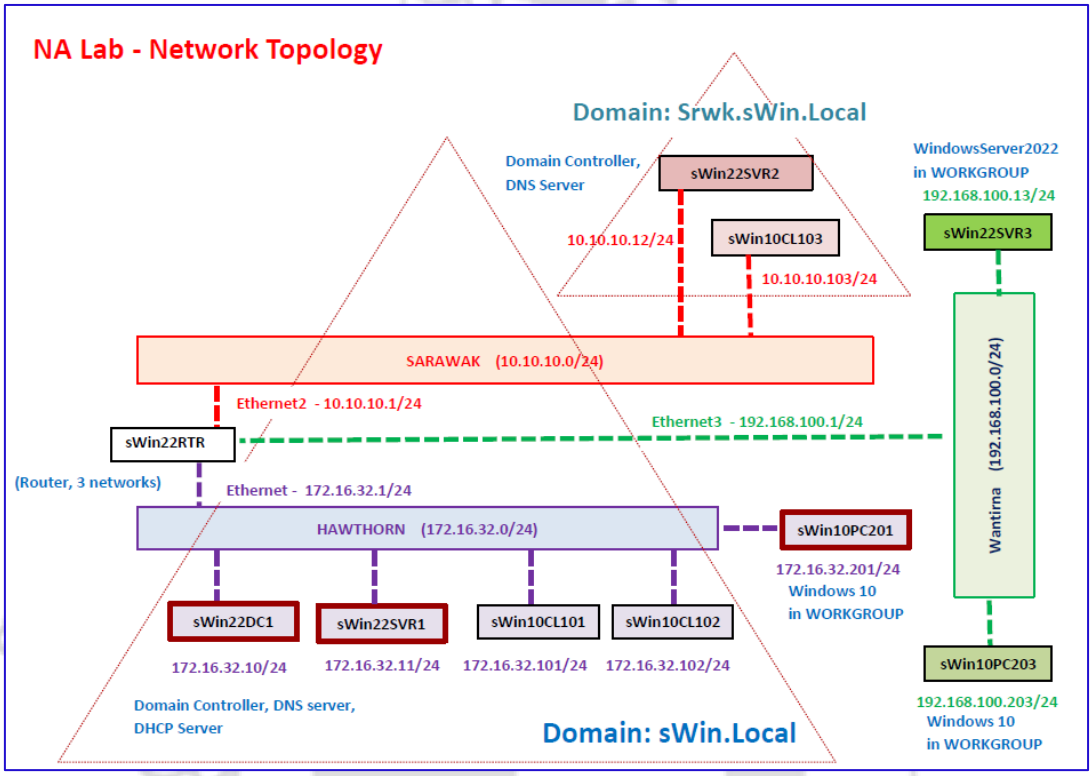


Figure 1: Network Administration Lab – Network Topology

It is essential to understand how end user devices (i.e. virtual machines) and network devices (i.e. virtual switches, software based router), presented in the topology, communicate and/or facilitate communication and services.

A virtual machine (VM) needs to firstly be connected to a virtual switch so that it can communicate with other VMs connected to that same virtual switch. For communication between 2 VMs that are connected 2 different virtual switches, then **a router** is needed. In addition to being connected to a virtual switch, in order to communicate with other VM, a VM must also be configured with correct **IP settings**.

Notes:

Prior to this week lab students should have viewed **Lecture 1 – Topic 2 – Network Devices** in order to easier understand concepts explained in this lab.

In this lab, we are going to **only explore through observing** the components that make up the lab network topology, based on the lab's original settings where all virtual machines are correctly pre-connected pre-configured with IP settings. In the following week labs, we will be learning how to configure virtual machines with correct IP settings, how to configure DHCP server, DNS server, etc.

Exercise 1.

Examine the existing virtual switches.

First, let's look at the existing virtual switches: *Hawthorn, Sarawak* and *Wantirna.*

1. Load the Hyper-V Manager.

   The Hyper-V Manager icon should appear on your desktop or toolbar.

Figure 2: Hyper-V Manager Icon

Double clicking the Hyper-V Manager icon will launch it. If the icon is missing on your computer press the **Win** key and then select **Hyper-V Manager…**

From the Actions pane of **Hyper-V Manager** select **Virtual Switch Manager…**

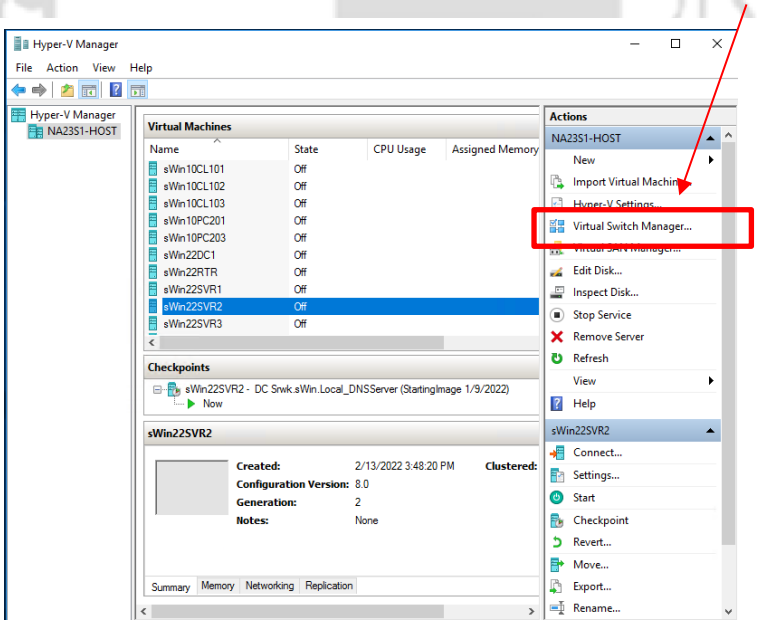


Figure 3: Hyper-V Manager Interface

2. At the top left, under **Virtual Switches**, you can see the 3 existing virtual switches: *Sarawak, Hawthorn* and *Wantirna*, created as parts of the unit's Network topology.

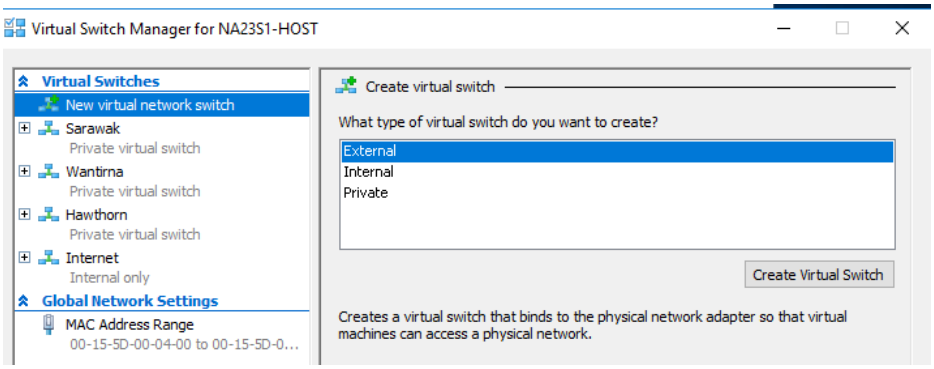


Figure 4: Virtual Switch Manager

At the top right, under **Create virtual switches**, it is listed the 3 types of virtual switch that we can create within Hyper-V: *Private, Internal* and *External.*

- **Private** switches allow **guest VMs to communicate to each other *ONLY when they are on the same host machine.***
- **Internal** switches function the same as the Private switches, and also have the added ability allow **guest VMs to communicate directly to the host machine**.
- **External** switches provide VMs located on them access to the physical network to which the Hyper-V host machine is connected.

In Figure 4. Virtual Switch Manager, what type of virtual switch are the *Sarawak, Hawthorn* and *Wantirna* switches? **private switches**

Can the guest VMs: sWin22DC1, sWin22SV1, sWinCL101, etc. communicate with the host machine? **Ye**?

If you are practicing in ATC626 lab, can the guest VMs (i.e. sWin22DC1, sWin22SV1, sWinCL101, etc.) hosted in the machine you are using communicate with any host machines that other students in the lab room are using? _____

Since the unit lab exercises do not require communication between guest VMs and host machine, neither require communication amongst students' guest VM and/or host machines, the 3 switches *Sarawak, Hawthorn* and *Wantirna* are created with the type of **private**.

Exercise 2.

Examine communication amongst VMs that connected to the same switch.

Refer to *Fig.1 Network Administration Lab – Network Topology*, and list VMs that are connected to the following switches:

- **Hawthorn**: _____
- **Sarawak**: _____
- **Wantirna**: _____

Now, let's observe the communication amongst VMs that are connected to the **Hawthorn** switch.

1. In **Hyper-V manager,** under **Virtual** machines, right click **sWin22DC1**, and select **Revert…**. In the **Revert Virtual Machine** pop up box, click **Revert** button to confirm that you want to revert the VM to its previous (*StartingImage*) checkpoint.

   To start the VM, right click on **sWin22DC1**, and select **Start**.
   Again, right click on **sWin22DC1**, and select **Connect**. Again, click on the **Connect** button to confirm proceeding to connect.

   In the password box for **sWin\Administrator** account, type in the password (**Pa55w.rd**) and click on the **Submit** icon (i.e. "→").

   After Windows completes loading, to check **IP settings of sWin22DC1**, right-click the **Win** key on the tool bar at the bottom left of the window, the **Start Menu** will pop up.

Figure 5: Windows Start Menu

Select **Run**. In the **Open** box, type **cmd** and click **OK**.

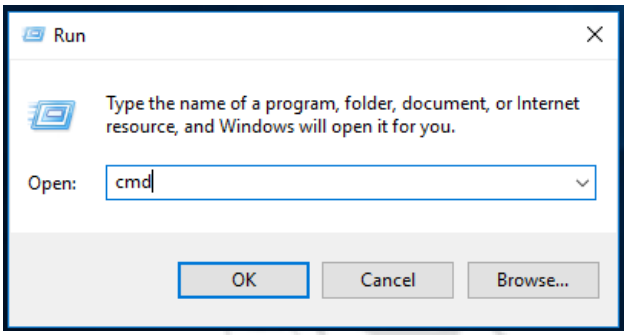


Figure 6: To Launch Command Prompt

In the **Command Prompt**, type **ipconfig** and press **Enter**.

Record the output for the **Ethernet Adapter's IP configuration.**

2. Repeat *Exercise 2 – Step 1* on **sWin22SVR1.**

3. Repeat *Exercise 2 – Step 1* on **sWin10CL101.**

4. To verify communication between sWin22DC1 and sWin22SVR1, back to **sWin22DC1,** in the **Command Prompt**, type **ping** <*IPv4 Address of sWin22SVR1's Ethernet Adapter previously recorded*>, and press **Enter**.

   The ping should be successful, and you should have received a message similar to this:

```
C:\Users\Administrator>ping 172.16.32.11

Pinging 172.16.32.11 with 32 bytes of data:
Reply from 172.16.32.11: bytes=32 time=1ms TTL=128
Reply from 172.16.32.11: bytes=32 time<1ms TTL=128
Reply from 172.16.32.11: bytes=32 time<1ms TTL=128
Reply from 172.16.32.11: bytes=32 time=1ms TTL=128
```

Figure 7: Successful Ping Replies

5. Repeat the previous step (*Exercise 2 – Step 4)* to verify communication between sWin22DC1 and **sWin10CL101**.

   Hints:
   In the **Command Prompt**, type **ping** <IPv4 Address of sWin10CL101 previously recorded>, and press **Enter**.

   Check with your lab supervisor if you did not receive successful ping replies in steps 4 and 5!.

6. Now, let's break the connection by changing the Network Adapter of **sWin10CL101** to connect to a different virtual switch, i.e. **Sarawak**.

   Back in **Hyper-V Manager**, right-click sWin10CL101 and click to select **Settings.** In Settings for sWin10CL101, under Hardware, click to select **Network Adapter.** In the **Network Adapter** window, pull down the **Virtual switch:** and select **Sarawak,** then click **OK.**

Back in **sWin22DC1**, **ping** <IPv4 Address of sWin10CL101 recorded in step no. 3> again.

Is the ping successful? _____

The ping should be unsuccessful and you should have received a message similar to this:

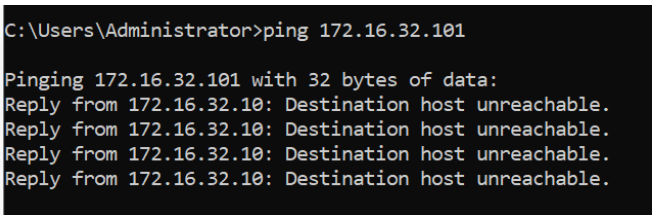


Figure 8: Unsuccessful Ping Replies

We have verified that the guest VMs (sWin22DC1, sWin22SVR1 and sWin10CL101) connected to the same virtual switch (Hawthorn) can communicate with each other. This is in accordance to the switch concepts introduced in Lecture 1 – Topic 2 – Network devices, that switches work in OSI layer 2 to connect devices together into networks, commonly referred as local area networks (LANs), allowing devices to share resources such as files, printers, etc. with each other.

If it is important to connect computer/devices to the correct switch so that the computers/devices can communicate correctly with other computers/devices in their networks; it is also important to ensure that guest VMs in the unit labs are connected to the correct switch so that students can successfully do their lab exercises. Hence, **it is recommended that you always revert a VM before using it**. The revert process for a VM in this unit brings the VM back to its pre-installed connections, settings and roles as described in the unit Lab – Network Topology.

Next, let's extend the network communication from sWin22DC1 to a VM connected to a different switch. Refer to Figure 1: Network Administration Lab – Network Topology, which VMs are connect to the **Sarawak** switch? _____

Exercise 3.

Examine communication between VMs that connected to different switches.

1. Revert, start, connect and log in to **sWin22SVR2.** After log-in process completes, find and record the VM's IPv4 Address here _____

   Hints: Refer to Exercise 2 – Step 1.

2. From **sWin22DC1,** attempt to communicate with **sWin22SVR2.**

   In **sWin22DC1**, **ping** <IPv4 Address of sWin22SVR2 previously recorded>

   Is the ping successful? _____

   If the ping is unsuccessful, what do you think the cause is? _____

   sWin22DC1 is connected to Hawthorn switch, whilst sWin22SVR2 is connected to Sarawak switch. Communication between 2 different network requires the aid of a layer-3 device, i.e. **router** (Refer to Lecture 1 – Topic 2 – Network devices). We need a router to aid communication between the 2 network Hawthorn and Sarawak.

   The sWin22RTR is a software-based router deployed in the unit lab to aid the communication of all VMs connected to the 3 networks (3 switches) – Hawthorn, Sarawak and Wantirna.

3. Revert, start, connect and log in to the software-based router **sWin22RTR.**

4. After log-in process completes, since sWin22RTR is a software-based router, wait for a few minutes for the VM to prepare itself to function as router, before try again to communicate from sWin22DC1 to sWin22SRV2.

   Back to **sWin22DC1**, **ping** <IPv4 Address of sWin22SVR2> again.

   The ping should be successful this time. If it did not, please check with your lab supervisor.

   The existence of sWin22RTR is crucial for successful communication amongst VMs connected to the different switches. Hence, in any lab exercises that require to use VMs connected to different switches (networks), make sure that you bring the sWin22RTR router up long enough for it to connect these networks together.

In addition to being correctly connected to the network switches and the existence of routers, devices/computers in the networks, there are other settings and services that MUST be correctly configured, such as

- Configuring IP settings manually
- Configuring DHCP servers to automatically assigning IP settings to devices/computers
- Configuring DNS servers for IP-Name resolution
- etc.

These functions and roles will be introduced and discussed in more details in the later weeks (refer to the Unit Outline – Weekly Schedule), i.e.

- Week 5: DHCP
- Week 6: DNS
- Week 7: Domain and Domain Controller

Then after each week lectures, during lab sessions, we will gradually learn how to configure DHCP server, DNS server, Domain Controller, etc.

In real-world practice, the company's network administrators commonly automate as much administration tasks as possible for time efficiency, configuration consistency and diminishing human errors. For examples, instead of manually configure IP settings for devices/computers, DHCP server(s) are planned and deployed to automatically assign IP settings to devices/computers in the company networks.

Exercise 4.
Observe the IP Address Assignment by a DHCP Server

All guest VMs in the unit labs are pre-configured with correct IP settings, as detailed in Figure 1: Network Administration Lab – Network Topology. Hence, unless instructed in the lab to change any VM's IP settings, you should always revert a VM before using and **do not attempt to change its IP** settings.

The sWin22DC1 virtual machine, as described in Figure 1: Network Administration Lab – Network Topology, is deployed as a Domain Controller, a DHCP server and a DNS server. Hence, if you are unsure on what IP settings you should configure for a VM, automatically obtain an IP address and related settings from the DHCP server **sWin22DC1.**

As explained earlier, we will learn more about DHCP and DHCP server configurations in the later weeks. In this lab we will only configure a VM to obtain IP settings from one of the already deployed DHCP servers in the unit labs.

1. Back to **sWin10CL101**, in the **Command Prompt** window, type **ipconfig /all,** then press **Enter**.

   Notice that the VM's IPv4 Address is currently **manually** configured.

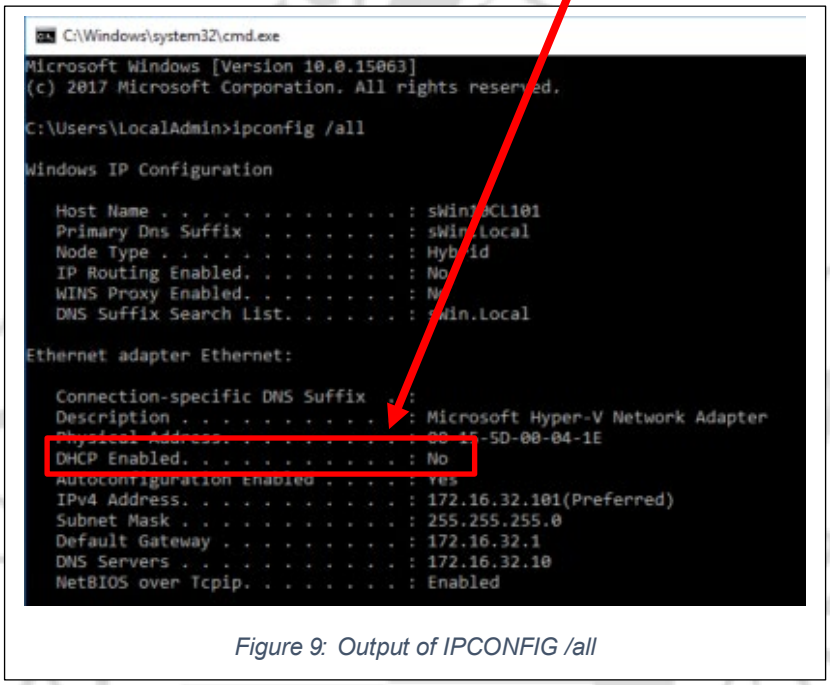


Figure 9: Output of IPCONFIG /all

   In Exercise 2, step no.6, we changed the Network Adapter of **sWin10CL101** to connect to a different virtual switch, i.e. **Sarawak**. Ensure that you change it back to connect to the virtual switch **Hawrthorn** before proceeding to the next step.

2. Now, we are going to configure sWin10CL101 to obtain IP settings from a DHCP server.

   Changing IP configuration of a device requires the administrative rights. Hence, we need to use a tool that has the administrative rights. In **sWin10CL101,** right-click the **Win** key, then click to select **Windows PowerShell (Admin).** Click **Yes** to confirm to proceed as an Administrator.

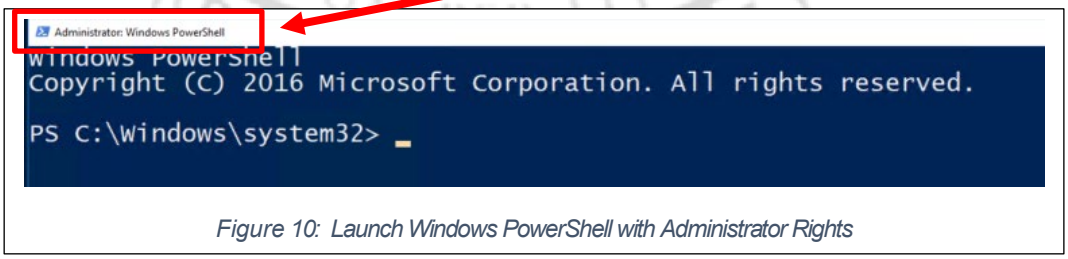


Figure 10: Launch Windows PowerShell with Administrator Rights

In the **Windows PowerShell** window, type

netsh interface ip set address Ethernet dhcp

and press **Enter**.

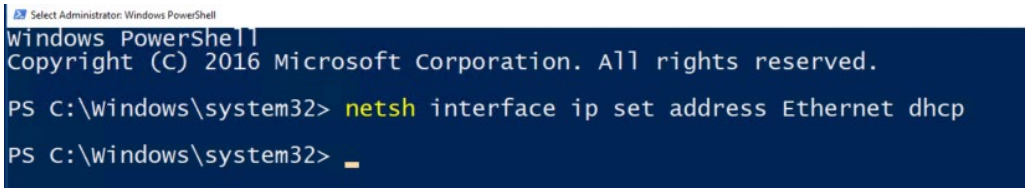


*Figure 11: Configure the network adapter **Ethernet** to obtain IP settings automatically*

3. In **Windows PowerShell**, type **ipconfig /all**, and press **Enter**.

   Observe the changes as the result of configuration made in the previous step:

   a. IP Configuration is set to obtain IP automatically from a DHCP server

   b. sWin22DC1 is the DHCP server that assigns the IP Settings to the network adapter Ethernet of sWin10CL101

   c. IP Settings assigned to sWin10CL101

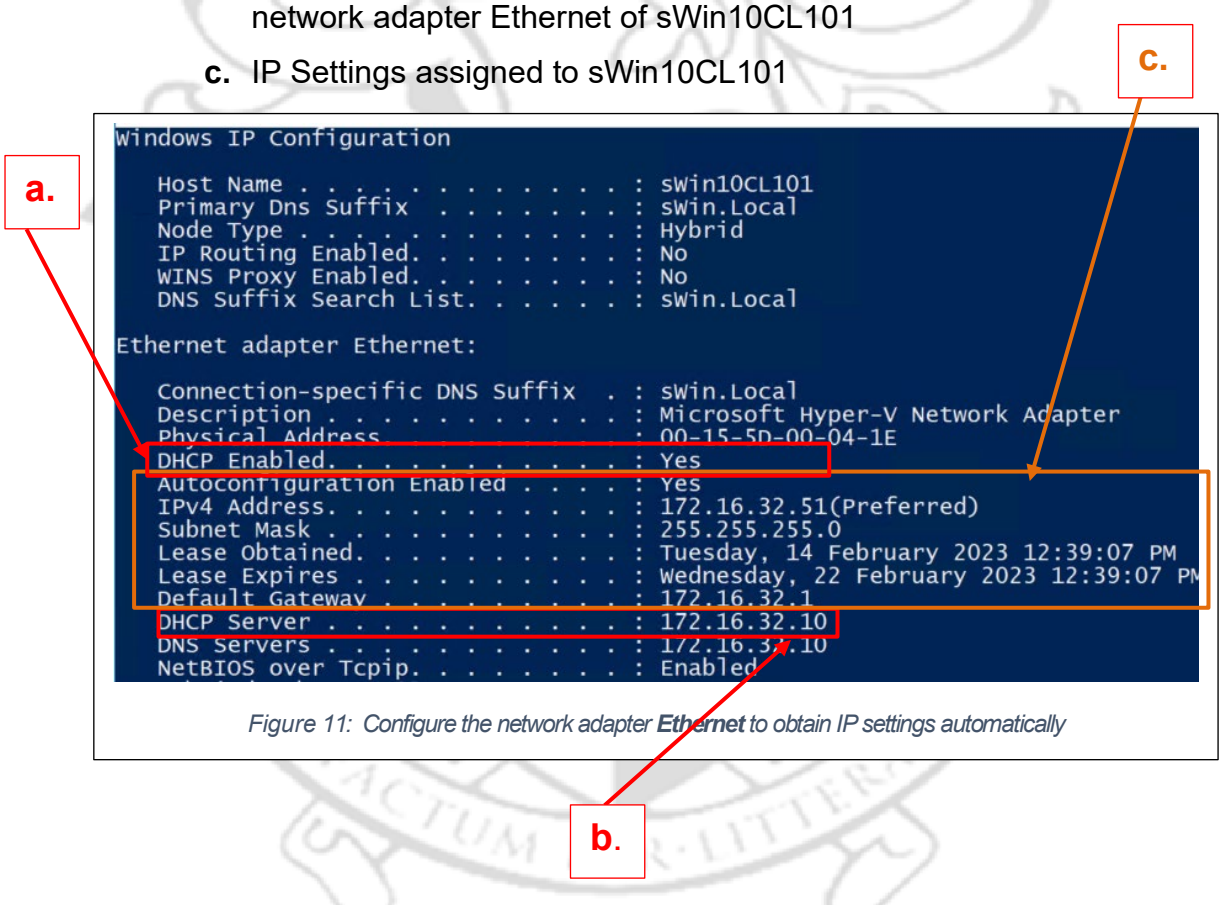


*Figure 11: Configure the network adapter **Ethernet** to obtain IP settings automatically*

4. Verify that communication between sWin22DC1 and sWin10CL101 remains successful after sWin10CL101 is assigned with the new IP settings.

   Back to **sWin22DC1**, in the **Command Prompt** window, type

   ping 172.16.32.51 (Notes: 172.16.32.51 is the newly assigned IP address)

   then press **Enter.**

   The ping should be successful and you should have received successful ping replies from sWin10CL101 (172.16.32.51)

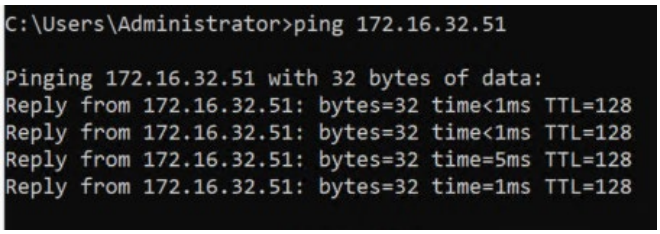


Figure 12: Successful Ping Replies from sWin10CL101 with newly assigned IP address

Exercise 5.
Continue to document your digital Lab Journal

1. Read "Lab Class Journal Submission requirements" if you have not done so, in order to best prepare for your learning and assessment.

   The Lab Class Journal is one of the assessments in this unit. A draft is to be submitted in week 4, and the final version in week 12. The Lab Class Journal is where students can record the concepts, design strategies, techniques, configurations and commands that they learn in the laboratory classes. Students can use their Lab Class Journal as a reference during the Skills Assessment in the Final Assessment Period.

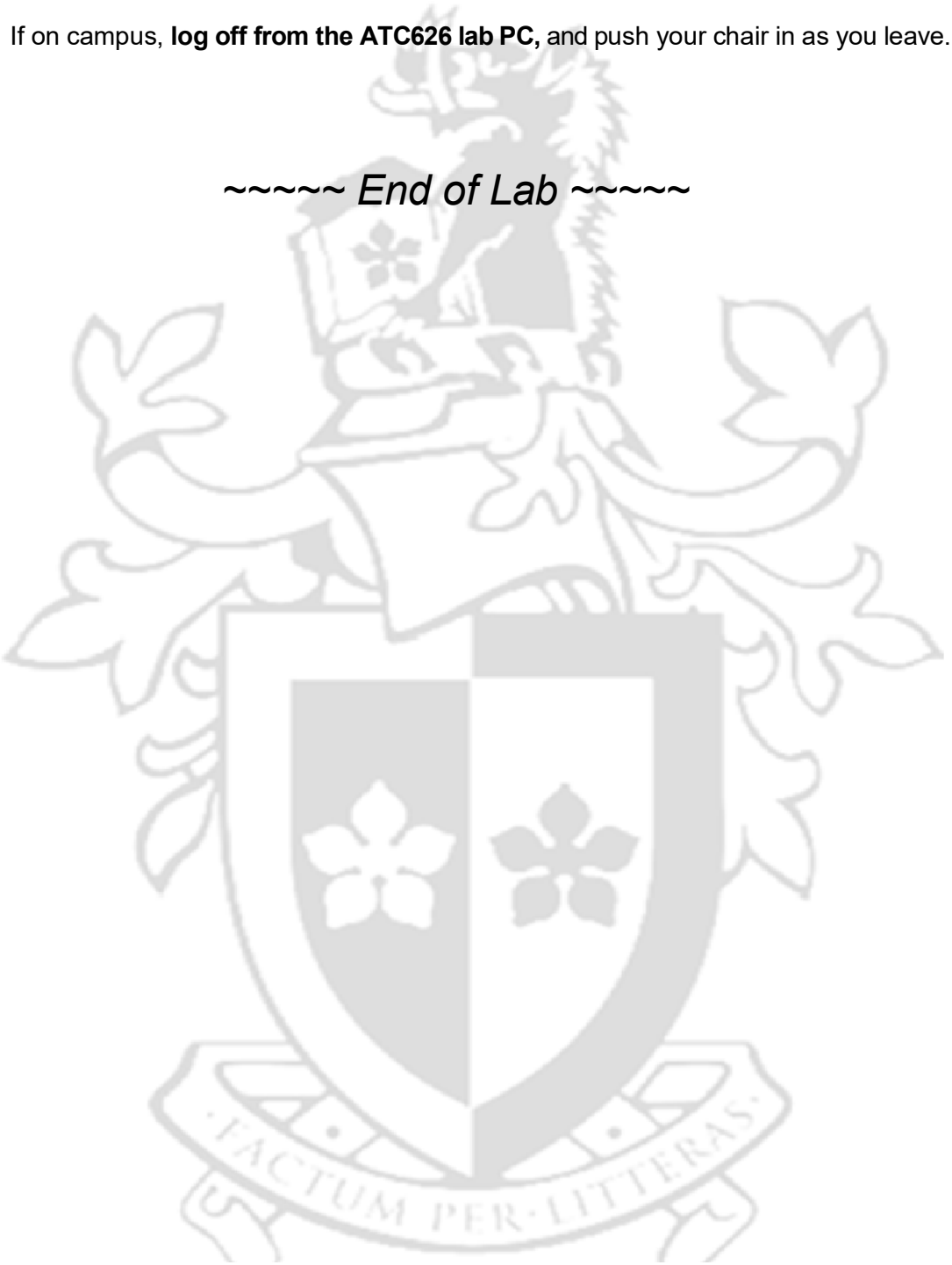
2. Record the concepts, design strategies, techniques, configurations and commands that you learn in this week laboratory class.

Do not leave the lab until the pack up stage is complete

Pack Up

1. Shut down all guest VMs.
2. **Sign out** from the Host machine and if you are using Azure lab, make sure that it is **Stopped** otherwise it will run in the background and use up your quota.
3. If on campus, **log off from the ATC626 lab PC,** and push your chair in as you leave.

~~~~~ End of Lab ~~~~~



TNE10005/TNE60002

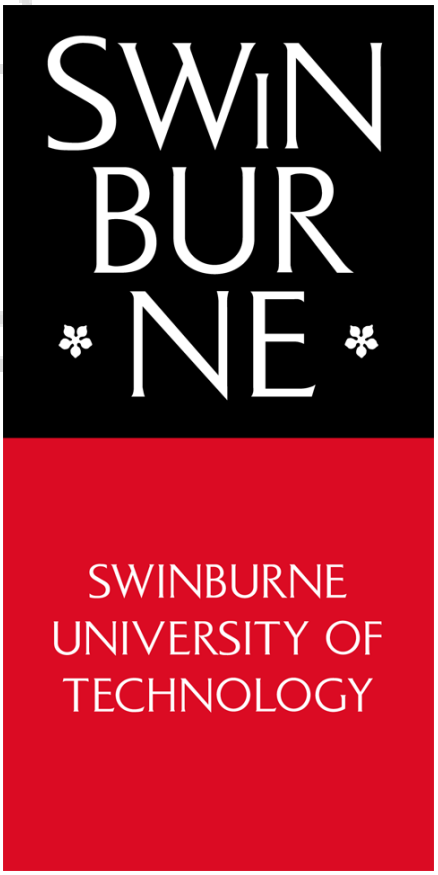
Network Administration

Lab 3

Introduction

to

IPv4 Addressing



Aims:

- Configure IPv4 Addresses
- Observe the purpose of the default gateway
- Observe the purpose of the subnet mask

Note: *For those of you who have studied networking before, this lab will appear deceptively simple. The focus of this lab for experienced students is to explain the observations.*

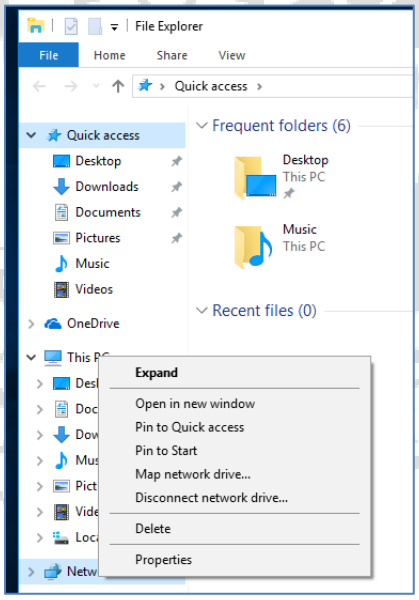
Preliminary settings

Note: *How to do these preliminary steps have been covered in past labs. If you cannot remember how to do these steps refer to Lab 01 and make sure you record how to do it in your journal for future labs.*

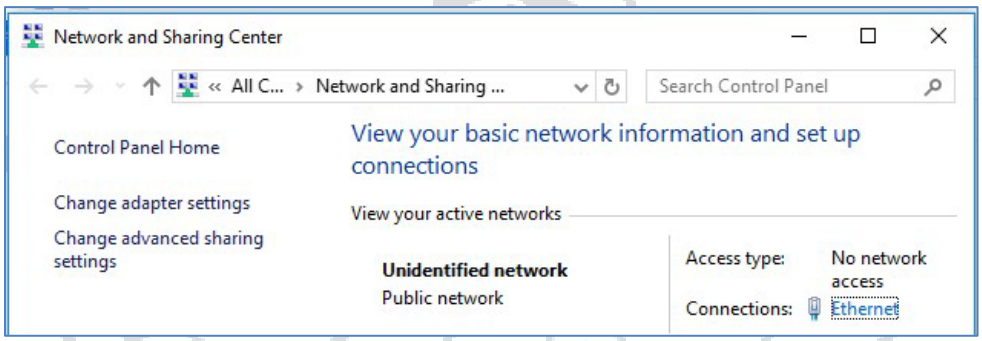
1. Revert and launch sWin22RTR, sWin22SVR1, sWin10PC201and sWin22SVR3
2. Check the virtual PC network configuration and ensure that virtual PCs have connected to the correct networks, as given in the topology diagram.
3. Ensure that the virtual PCs sWin22SVR1, sWin10PC201 and sWin22SVR3 have IP addresses configured as outlined in the topology diagram before proceeding. Note:

   To get to the adapter configuration:

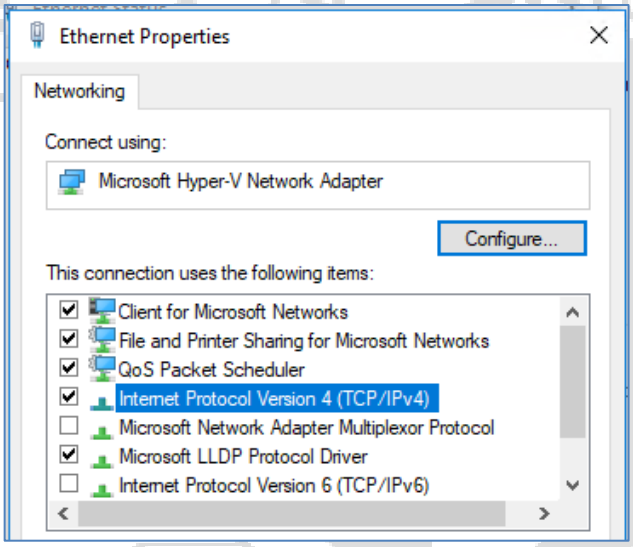
   i Launch **File Explorer**  . Within the *File Explorer* window, *Right-click* on **Network,** then click to select **Properties.**



ii Within the *Network and Sharing Centre* window, *click* on the **Ethernet** link**,** then double-click to select **Properties.**



iii Within the *Ethernet Properties* window, *double-click* on **Internet Protocol Version 4 (TCP/IPv4),** then configure the virtual PC's IP settings as required**.**



Topology

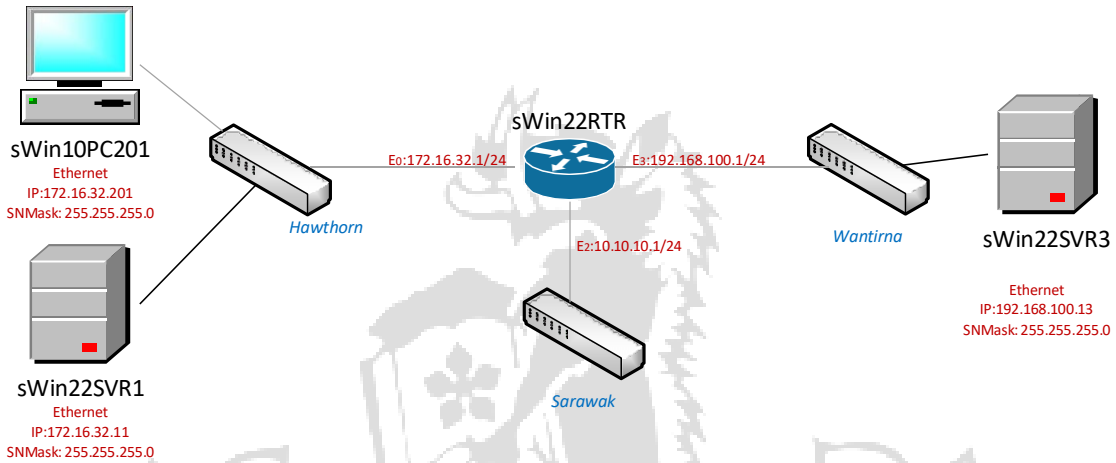


Figure 1 – Network Topology diagram for Lab 3

Gateway Addresses

In order to understand what a gateway address does, lets' do some preliminary tests:

4. On **sWin10PC201** right-click **Start** and select **Powershell**.

5. At the PowerShell prompt, type **`ipconfig`** and press **Enter**.

6. Record the output here:

```
Connection-Specific DNS Suffix: _____
IPv4 Address:                   172.16.32.201
Subnet Mask:                    255.255.255.0
Default Gateway:                _____
```

7. We will now use the **ping** command to see which devices we can communicate with, with our current IP configuration.

   Ping stands for **P**acket **In**ternet **G**roper. It uses the ICMP protocol to request a reply packet to be sent back. If we can successfully ping a device it means that our ICMP *Echo-request* packet arrived and the *Echo-reply* has also been returned. Thus confirming that our devices have two way communication.

8. Still on sWin10PC201 we will ping the IP address of sWin22SVR1. At the PowerShell prompt type:

```
Ping 172.16.32.11
```

   Was the ping successful? _____
   If it wasn't get a fellow student to check for errors. If neither of you can find an error in your typing, call your supervisor over to help.

   If the ping was successful you should have received a message similar to this:

```
Reply from 172.16.32.11: bytes=32 time=1ms TTL=128
```

9. We will now ping the IP address of our router. At the PowerShell prompt type:

```
Ping 172.16.32.1
```

   Your ping should have been successful *(if not have a fellow student try and troubleshoot, if neither of you can find the error, call your supervisor over*).

10. Now ping the IP address of our **sWin22SVR3**. At the PowerShell prompt type:

```
Ping 192.168.100.13
```

Was this successful?

_____

11. Pinging sWin22SVR3 should **not** have been successful.

Reviewing the theory covered in the lecture:

> *In order to communicate on any IPv4 network a device needs an **IP address** and a **Subnet mask**.*
>
> *Without an IP address and Subnet mask the device cannot communicate on the network. With **only** an IP address and Subnet mask, the device can communicate with other devices that are:*
>
> *a) Connected to the same network segment, and...*
> *b) Configured with an IP address in the **same subnet.***
>
> *If a device needs to communicate with a device in another network segment and subnet, then the network needs a router. The IP address of the local port of the router (i.e. the port on the device's subnet) must be configured as the **Default gateway.***

Because 192.168.100.13 is in a different subnet we expect the ping to fail when no default gateway address is configured.

Let's see if configuring the default gateway fixes this problem.

12. Review the topology diagram on page 3.

    a. Which address do you think should be used as sWin10PC201's gateway address?

    _____

b. On **sWin10PC201** go back to the **Ethernet** adaptor properties (Hint: check step 3 on page 2, if you cannot remember how to do this). In the ***Internet Protocol Version 4*** settings type the IP address: **172.16.32.1** as the ***Default gateway***.

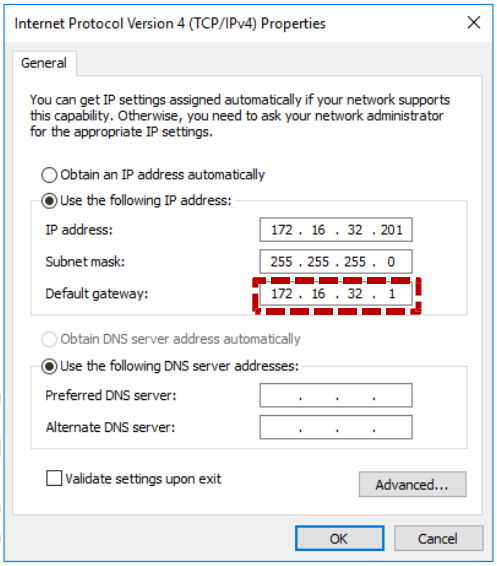


Figure 2 -Configuring the Default gateway address

13. Click **OK**, and close the Ethernet properties dialog box.

14. Back in **Powershell** see if you can ping 192.168.100.13 successfully.

    You should observe output similar to the following:

```
Pinging 192.168.100.13 with 32 bytes of data:
Reply from 192.168.100.13: bytes=32 time<1ms TTL=127
Reply from 192.168.100.13: bytes=32 time<1ms TTL=127
Reply from 192.168.100.13: bytes=32 time<1ms TTL=127
Reply from 192.168.100.13: bytes=32 time<1ms TTL=127
```

    (If not have a fellow student try and troubleshoot, if neither of you can find the error, call your supervisor over).

> *A gateway address is required if you need to communicate with a device in another subnet. The IP address of the local router interface, (i.e. the router interface that is connected to your network) should be configured as your gateway address.*

We have now observed the importance of the Default gateway address.

Subnet Mask

We will now explore the function of the subnet mask.

*A networked device uses the **subnet mask** to determine which MAC address needs to be entered into the Data-link layer's **Destination Address**. There are only two options, the MAC address of the destination device or the MAC address of the Default gateway.*

*If the network portion of the destination device's address **matches** the network portion of the source device's address then the MAC address of the **destination device** will be entered.*

*If the network portion of the destination device's address **does not match** the network portion of the source device's address then the MAC address of the **default gateway** will be entered.*

Figure 3 illustrates how the destination MAC address is selected and used.

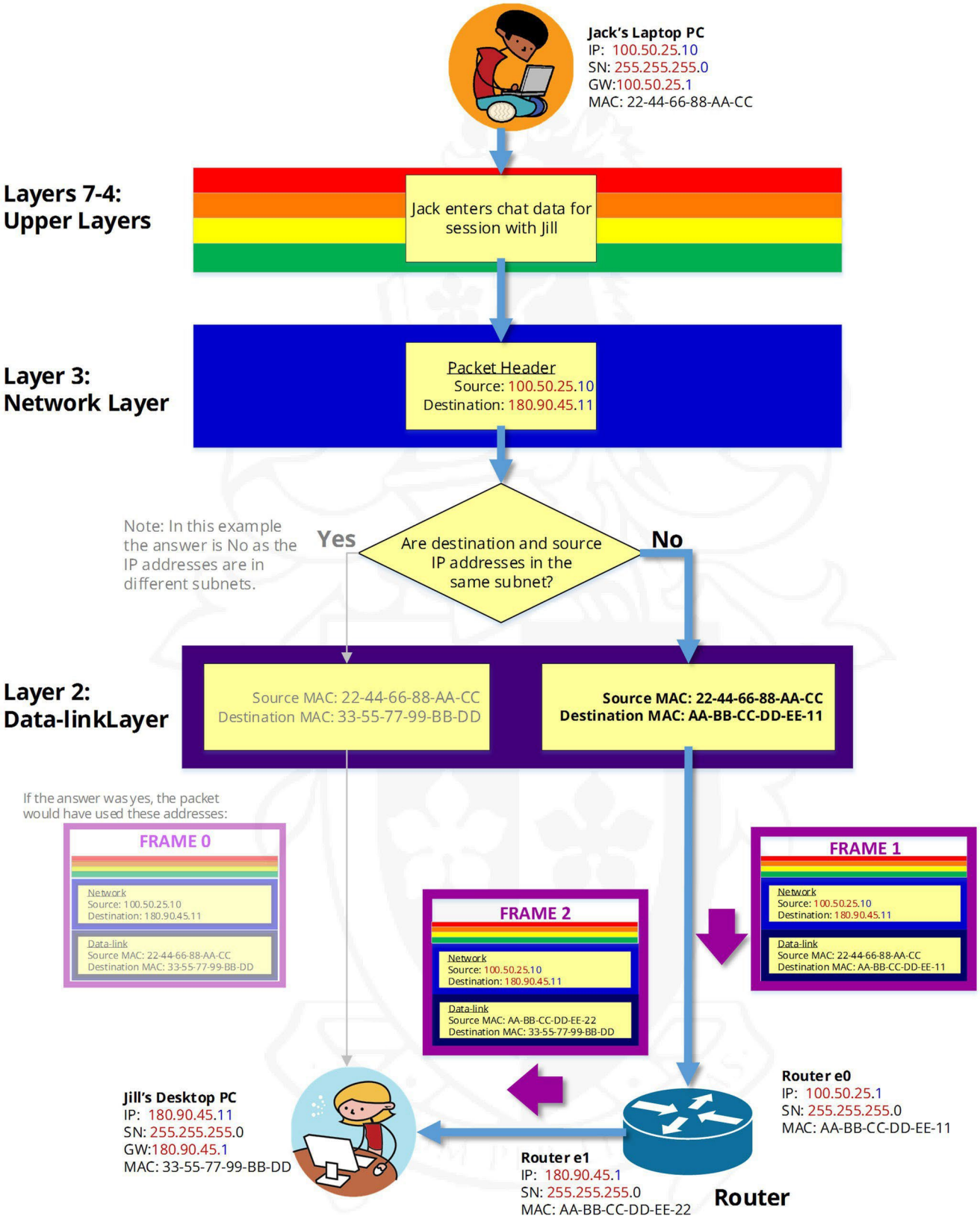


Figure 3 - How Subnet masks determine destination MAC addresses

15. Question: Look at the source and destination addresses of Frame 1 and Frame 2.

    a. Which addresses change? _____

    b. Which addresses stay the same? _____

    c. Try to explain why some change and others don't:

    _____

ANDing

16. Subnet masks work by:

    a. ANDing the binary Source IP address with the local subnet mask.
    (Remember when both bits are 1 the result is 1, if either bit is 0 the result is 0)

    b. ANDing the binary Destination IP address with the local subnet mask.

    c. Comparing the resultant network addresses to see if they are identical.

        i If identical they use the destination's MAC address as the layer 2 destination address.

        ii If different they use the default gateway's MAC address as the layer 2 destination address. (Note: In this situation, if no gateway address is configured the packet will be dropped)

17. ***Example***

    a. PCa has the IP4 configuration of:

        IP: 10.10.10.100

        SN: 255.255.255.0

        GW: 10.10.10.1

    PCa wants to communicate with PCb.

    PCb has the IP address of IP: 10.10.10.102

i To calculate its own **network address** PCa uses its IP address and Subnet mask.
It performs an AND operation:

PCa IP	00001010	.	00001010	.	00001010	.	01100100
PCa SN	11111111	.	11111111	.	11111111	.	00000000
PCa Network Address	00001010	.	00001010	.	00001010	.	00000000

ii To calculate PCb's **network address** PCa uses its own subnet mask and ANDs it with PCb's IP address

PCb IP	00001010	.	00001010	.	00001010	.	01100110
PCa SN	11111111	.	11111111	.	11111111	.	00000000
PCb Network Address	00001010	.	00001010	.	00001010	.	00000000

iii If we convert both PCa's and PCb's network addresses back to decimal we get:

PCa	10	.	10	.	10	.	0
PCb	10	.	10	.	10	.	0

We can see that both network addresses are identical. So at the Data-link layer PCb's MAC address will be inserted as the destination address.

18. Question: Do PCc and PCd have the same network address?

PCc IP:192.168.100.103

PCc SN: 255.255.255.0

PCd IP: 192.168.111.104

We will now look at this from a practical perspective.

19. On **sWin10PC201** ping **172.16.32.1** (the local router interface).

    Make sure the ping is successful.

20. On **sWin10PC201** change the subnet mask to **255.255.255.192**, and **delete** the Default gateway address (the Default gateway should be " . . . ").
    (Hint: check step 3 on page 2, if you have forgotten where to configure this)

    a. Make sure that you click **OK** on the **Ethernet Properties** dialogue box.

    b. Now try to **ping 172.16.32.1**

       Were you successful? _____

21. On **sWin22Svr1** make the same IP configuration changes. Change the subnet mask to **255.255.255.192**, and **delete** the Default gateway address.

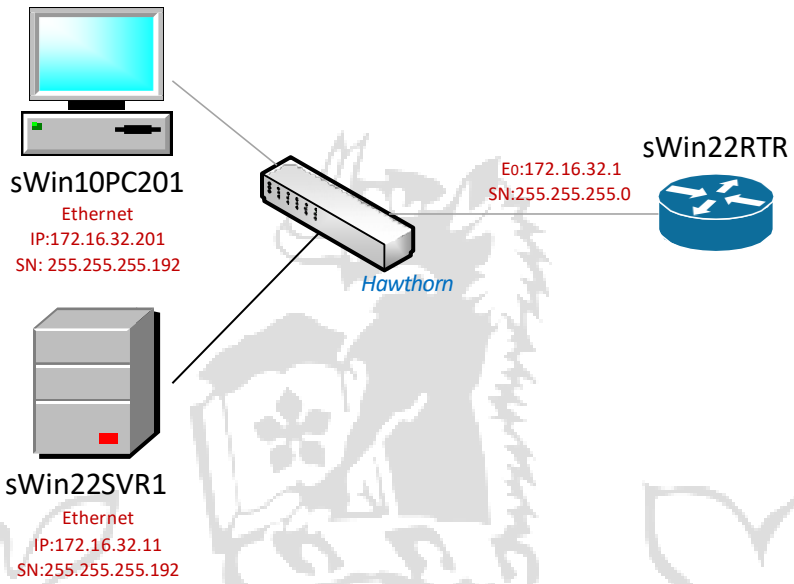
    a. Now try to **ping 172.16.32.1**

       Were you successful? _____

    b. Now try to **ping sWin10PC201**

       Were you successful? _____

22. Review the addressing of our current network segment.



a. Why could **sWin22SVR1** successfully ping **sWin22RTR(E_0)** but not **sWin10PC201**?

b. **sWin22SVR1** and **sWin22RTR(E_0)** could successfully ping, but they have different subnet masks. Explain how this could be? *(**Note:** If you are new to networking, do not stress if you cannot answer this question… you will be able to by the end of the semester).*

Extension – Investigating ARP

Note: This is an optional component of the lab. Only students who have finished early should consider doing the practical exercises in this extension.

The Address Resolution Protocol is how the Network Layer and the Data-link layer are able to link IPv4 addresses with MAC addresses.

It achieves this by keeping a table of IP and MAC addresses. Every time a device tries to communicate with another device it uses the IP address (and subnet mask) that has come from the Network Layer and tries to locate the appropriate MAC address in the ARP table. If there is no match, ARP will then send out a broadcast to try and locate the device with that IP address. If that device replies to the broadcast, the reply will have the MAC address in the source field of the frame, which can then be inserted as a new entry in the ARP table.

In this exercise we will observe how an ARP table is constructed, and how addresses within the same subnet and addresses in another subnet are treated differently.

23. Configure the IP address settings of sWin10PC201 and sWin22SVR1 as given in Figure 4.

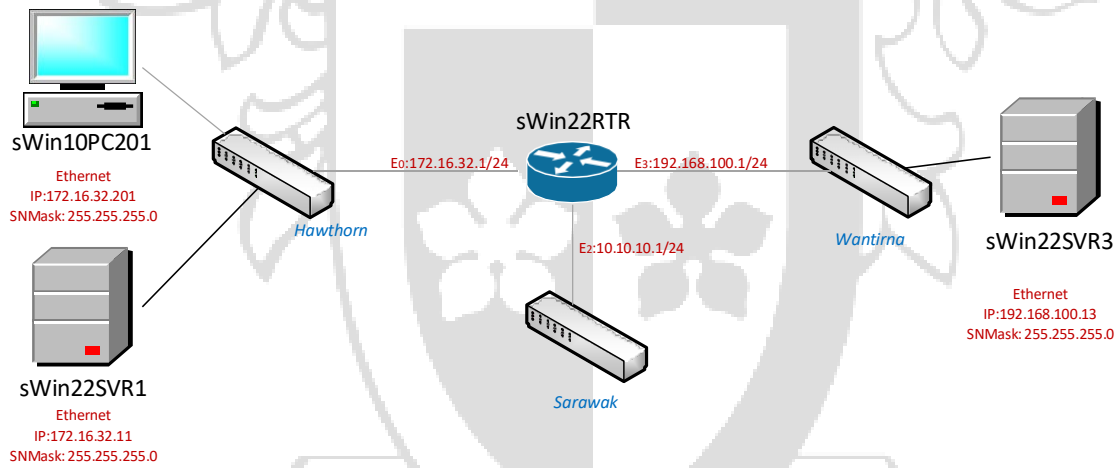


Figure 4 - Extension Network Topology

24. Start up the virtual machines sWin22DC1 and sWin22SVR2

25. On sWin10PC201, load up **Windows PowerShell (Admin)**, and type:

```
arp –d
```

26. Now display the ARP table by typing:

```
arp - a
```

Ideally (if you were fast enough) there will be no entries in your ARP table, however you may observe one or two 224.0.0.x addresses (.22 is used by IGMP, and .252 is used by LLMNR – both are beyond the scope of this course). If you were slow the Default gateway may have an entry appear.

27. Now ping sWin22SVR1, and display your ARP table (i.e. arp –a). You should now see an entry for it.

28. Now ping sWin22DC1 (172.16.32.10) and display your ARP table. There should now be an entry for this.

29. If your default gateway is not appearing in your ARP table ping it (172.16.32.1) and make sure that there is an entry in the ARP table.

    a. What happened every time you pinged a new address?

    the arp table is updated

    b. How many entries do you now have in your ARP table? _____

30. Now ping sWin22SVR3 and check your ARP table. Are there any new entries? _____

31. Now ping sWin22SVR2 (10.10.10.12) and check your ARP table. Are there new entries now? _____

32. Explain your observations:

33. Get your supervisor to check your explanation.

Pack Up

1. Shut down all guest VMs.
2. **Sign out** from the Host virtual machine and make sure that it is **Stopped** otherwise it will run in the background and use up your quota.
3. If on campus, **log off from the ATC626 lab PC,** and push your chair in as you leave.

End of Lab

TNE10005/TNE60002

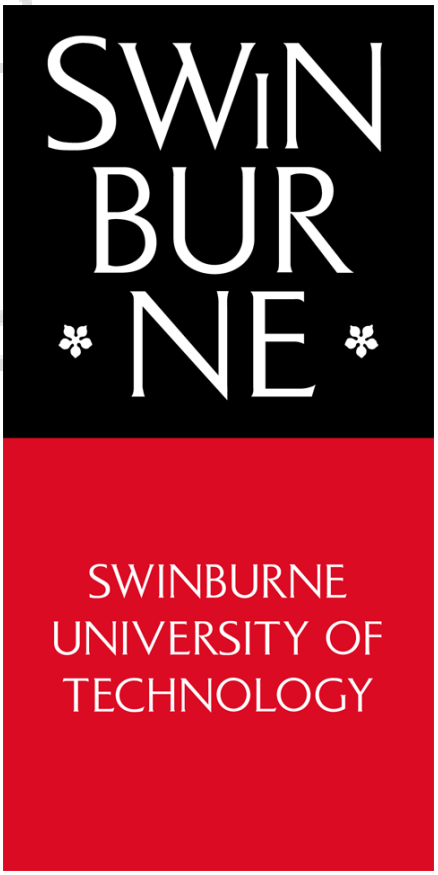
Network Administration

Lab 4

DHCP

in a

Windows Server 2022 Domain



Aims:

To install and configure DHCP

- Scopes
- Exclusions
- Reservations
- Options
- (High Availability)

Virtual Machines

sWin22DC1, sWin22SVR1, and sWin10CL101

Preliminary Settings

1. Ensure all guest VMs are reverted prior to starting.
2. Launch **sWin22DC1**. Log on as **sWin\Administrator** with the password **Pa55w.rd** *(the "sWin\" part is important!)*.
3. Repeat step 2 for **sWin22SVR1** and **sWin10CL101**.
4. On **sWin10CL101** right click on the **Start** button and run **Windows Powershell (Admin)**.
5. At the prompt type:

```
Set-NetIPInterface –InterfaceAlias Ethernet –dhcp enabled
```

Wait about 20 seconds, then type **`ipconfig /all`** and press **Enter**.

Record your IPv4 Address, Subnet Mask and Default Gateway here: **IPv4**

Address: **172.16.32.53**

Subnet Mask:

255.255.255.0

Default Gateway:

172.16.32.1

What type of address is this? **IPv4?**

Installing DHCP

6. On **sWin22SVR1**, in Server Manager, from the **Manage** menu select **Add Roles and Features.**
7. As we will be installing to the local server (i.e. the server we are currently logged on to) we can accept the defaults for the next three screens. So click **Next** three times and stop on the **Select server roles** page.
8. Click in the check box next to **DHCP Server.** You will be prompted to add features that are required. Click the **Add Features** button, and **Next,** three times.
9. On the **Confirm installation selections**, verify that you are adding the DHCP server tools and click the **Install** button.
10. When the text under the blue line reads **Configuration required. Installation succeeded on sWin22SVR1**, click the **Close** button.

Post-deployment configuration

Even though we have installed the DHCP server role, we need to now configure the role.

Server manager tells us this.

11. In **Server Manager**, notice that there is now a yellow triangle alert that appears.

Figure 1 - DHCP Post-deployment flag

12. Click on the alert, then click on **Complete DHCP configuration**.

    What you do next depends on your network environment. Since sWin22SVR1 is a Windows Domain sWin.Local, then you must **Authorize** your new DHCP server with the **Domain Controller** before any computer in the domain will accept a lease from it. To do this you would need to provide the account details of a user that has the rights to make this change, such as the domain Administrator.

    On the **DHCP Post-install configuration wizard**, click the **Next** button.

    On the Authorization page, accept the default section, and then click the **Commit** button. *(Note: If you have logged in with the wrong account [see step 2], you will need to select "Alternate Credentials" and enter the login name provided in step 2).*

    On the Summary page, click **Close.**

    We have now completed the post-deployment configuration, but our server is still not configured to offer IP addresses.

Creating a Scope

Remember, IPv4 addresses are **logical** addresses. Other than APIPA, administrators must configure them. Even though we use DHCP to automate the allocation of IP addresses, we still need to configure those addresses.

The first step is to configure a **Scope**.

13. In **Server Manager**, click the **Tools** menu, then select **DHCP**

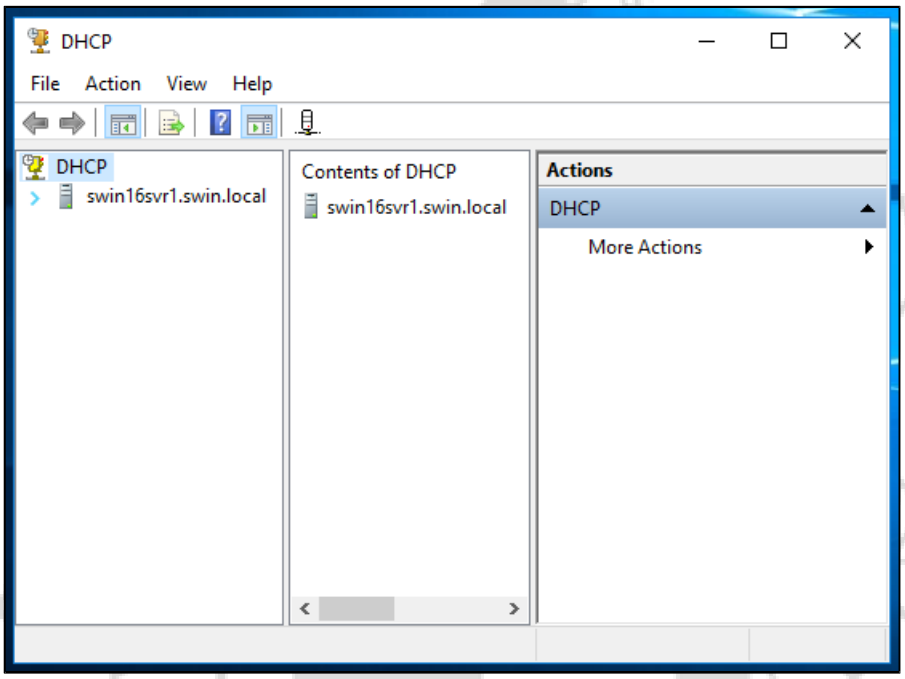


Figure 2 - A new installation of DHCP Server

Notes:

*The figures in this lab document are captured for DHCP Management console on **sWin-Server that running Windows Server 2016.** Hence, the server's name is sWin16SVR1. Students should check on sWin22SVR1 when practicing using the unit Azure lab VMs.*

14. If you have not configured step 12 correctly then a red arrow will appear on you server. If this has happened to you, consult with a fellow student, and if neither of you can resolve the problem call your supervisor over.
15. To create a **Scope**, click on the server name (sWin22SVR1) to expand the sub-containers **IPv4** and **IPv6**. We want **IPv4**.

    Now this is one of the peculiarities with Windows, you do not get a right click menu until you have clicked on an object.

    Click on **IPv4**, then right click on **IPv4** and select **New Scope...**

    This brings up the new scope wizard.

16. Click **Next** on the first page of the wizard, and enter the name **Hawthorn**. In the description you would normally briefly record the purpose and in a large organisation the job number so that who authorised it and who configured it can be retrieved. This can be vital for the security of your network as you need to shut down services that are no longer required. A good description allows you to do this.

    Click **Next**.

17. On the **IP Address Range** page of the wizard, enter the values as provided in Figure 3.

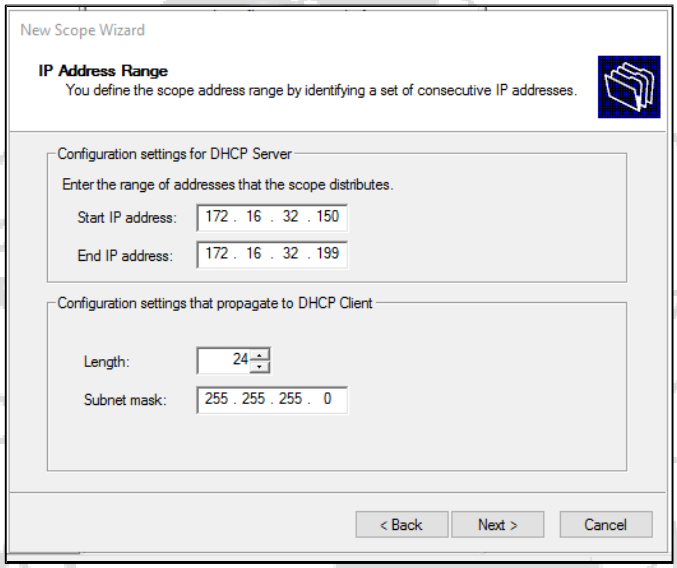


Figure 3 - DHCP New Scope IP Address Range

    Then click **Next**.

18. On the **Add Exclusions and Delay** page we will not configure Exclusions yet. But notice the **Subnet delay in milli second:** field. This allows you to delay how long the server waits before it sends out a **DHCP** offer packet. This is very useful when you want to have a backup DHCP server and you only want it to kick in when the primary DHCP server is down. The delay allows this to happen.

    Click **Next.**

19. You should now be on the **Lease Duration** page. Normally we would leave this at 8 days. But sometimes you may be running a conference or exhibition where many users will not be returning the next day. You do not want the DHCP server holding that IP address back and not offering it to any new devices for 8 days. In situations like this we would set the lease time to 8 hours.

    The rule of thumb is for devices on a cable you lease for 8 days, for devices on WiFi 8 hours.

    Choose a lease period between 8 hours and 8 days and click **Next**.

20. On the **Configure DHCP Options** page we will select **No**, and click **Next**.

    We will cover DHCP Options later in this laboratory.

21. Click **Finish**

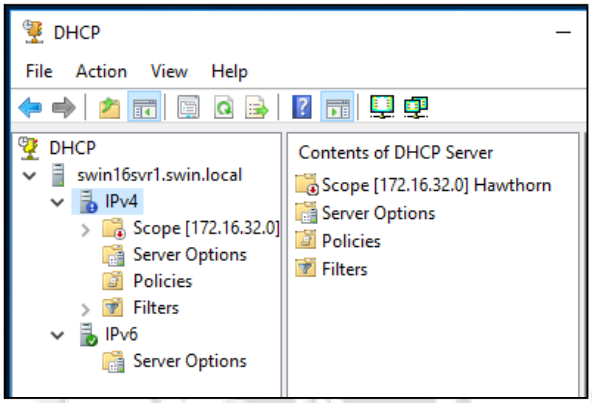


Figure 4 - An Inactive DHCP Scope

22. In the DHCP Management console you will notice that there is a red down arrow in the icon of the new scope we have just created (and a resultant blue exclamation mark with the IPv4 container).

    This means that the Scope has not been activated. Remembering that Windows has a frustrating quirk, **click** on the **Scope** icon, then **right click** the **Scope** icon and select **Activate** from the context menu. The red down arrow and blue exclamation mark should have now disappeared, and you DHCP server is now ready to send out offers.

23. Since sWin22DC1 is also a DHCP server, to ensure that this server will not lease out any IP addresses, we now need to stop its service

    On **sWin22DC1**, in Server Manager, click **Tools**, and then click **DHCP.**

    In the DHCP console, click on **sWin22dc1.swin.local.** Right click on **sWin22dc1.swin.local**, select **All Tasks**, and then click **Stop**.

    Now sWin22SVR1 is the only DHCP server.

24. To test if our DHCP server is now working change to **sWin10CL101** and go to **Powershell**.

    First, release the existing leased IP address
    Type:
    ```
    ipconfig /release
    ```
    and press **Enter.**

    Then, attempt to obtain a new IP address
    Type:
    ```
    ipconfig /renew
    ```
    and press **Enter.**

This triggers the computer to send out a **DHCP discover** packet.

Record your IPv4 Address, Subnet Mask and Default Gateway here:

IPv4 Address: 172.16.32.150

Subnet Mask: 255.255.255.0

Default Gateway: _____

This address should be from the scope you have just configured.

Configuring Exclusions

There are times when we need to remove addresses from a Scope's pool. A legacy application running on a computer might need a specific address, or you can't risk a device being given any other address and must be configured manually (Note: there is a better way to meet this requirement, we learn about it below with Reservations). In this situation you might want to **exclude** addresses from your pool. We will configure exclusions in this section and reservations in the next section.

25. On **sWin22SVR1** in the **DHCP management** console, make sure that the **Hawthorn** scope is expanded. **Right click** on the **Address Pool** container and select **New Exclusion Range…**
26. Enter the **Start IP address** as 172.16.32.150, and the **End IP address** as 172.16.32.159, and click the **Add** button.

We will now test to see if our exclusion range is being applied.

On sWin10CL101, type **`ipconfig /release`** press enter and type **`ipconfig /renew`**, (hint: you can press the up arrow to recall past commands) and press enter. Record the output here:

IPv4 Address: 172.16.32.160

Subnet Mask: 255.255.255.0

Default Gateway: _____

What has changed? _____

Configuring a Reservation

When the lease time expires, eventually the DHCP server will offer that IP address to another device. This can be a problem when need to host a resource that everyone needs access to. In those situations the device needs to only be given one address. If it has one address in one month and a different address in another month, then all the links to the resource may stop working. You could use a manually configured IP address (i.e. where you have to log on to the device and manually set the IP address), but if you need to change your addressing scheme, you will need to manually change the address of all of these devices.

In the section above, I stated there is a 'better' way to ensure that a device only ever has one address. You can use a **Reservation**. A reservation gives a device the same IP address, again and again. A reservation also has the advantage of keeping the configuration central, so if you need to change your addressing scheme you can do it all in the DHCP server.

Let's work through how to configure a Reservation

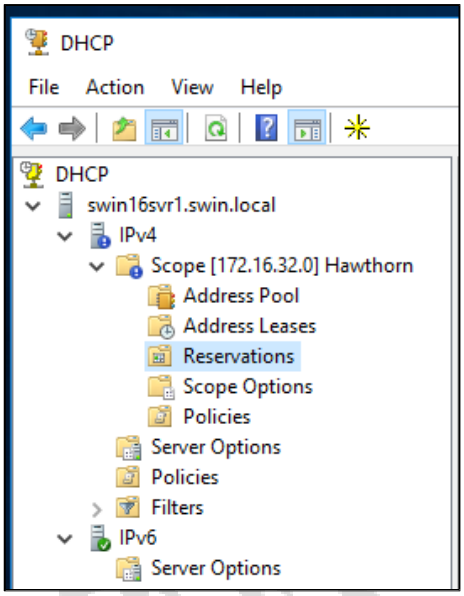


Figure 5 - DHCP Reservation Container

27. In DHCP Management, ensure that the IPv4 and Scope containers are expanded. **Right click** on **Reservations**, and choose **New Reservation...**

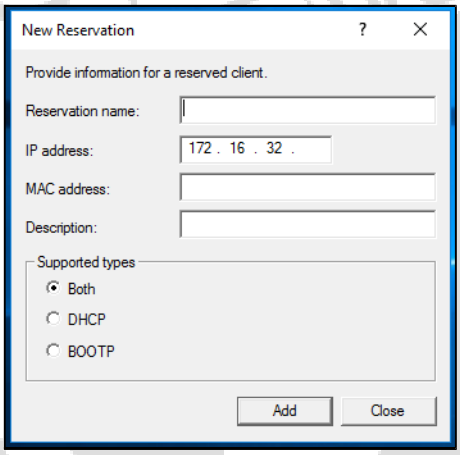


Figure 6 - Configuring a Reservation

28. In the **Reservation name** field enter the name **sWin10CL101** and the **IP address `172.16.32.199`.**

    We will now find the MAC address sWin10CL101 so we can complete configuring the reservation.

29. Change back to **sWin10CL101**, and in **Windows PowerShell (Admin)** type **`ipconfig /all`** and press **Enter.**

    You should see output similar to the following

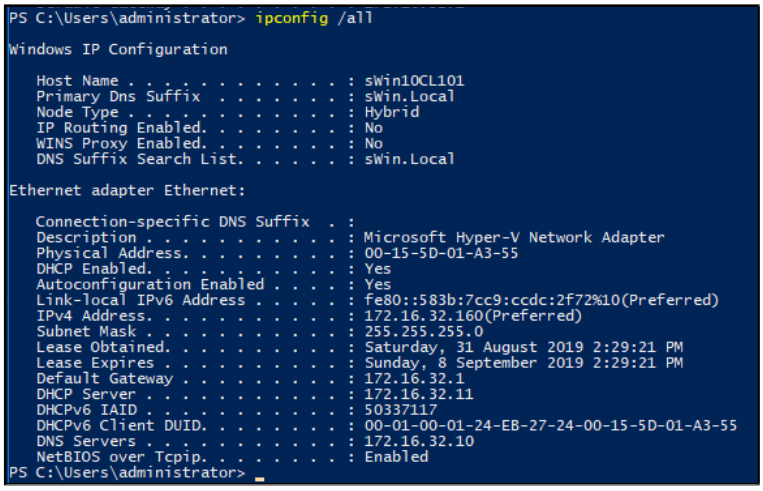


Figure 7 - Finding a MAC Address

30. Locate the line **Physical Address** and record it here:
    00-15-5D-00-04-1E

31. Change back to **sWin22SVR1** and in the **MAC address** field, without the hyphens (i.e. '-') enter the Physical Address in step 0.

    For example, in Figure 7 the address is presented as **00-15-5D-01-A3-55.** I would enter this as **00155D01A355**

32. Switch back to **sWin10CL101** and do an ipconfig /release followed by and ipconfig /renew

33. Record your address here:

    IPv4 Address: ~~172.16.32.199~~

    Subnet Mask: 255.255.255.0

    Default Gateway: _____

    What has changed? _____

DHCP Options

So far we have learned how to use automatic IP configuration via DHCP to configure Windows computers to receive an IP address and a subnet mask. But these settings only allow our devices to communicate with other devices that are in both the same subnet and same LAN.

A device needs a **Default gateway** address to be able to communicate outside its own subnet. A device needs a **DNS Server** to be a part of an Active Directory Domain, or browse the internet using URLs.

We can use DHCP to deploy these settings using **DHCP Options**.

Options can be applied at a number of levels: Server, Scope, Reservation and with policies. Policies will not be assessed in the skills exam, so we will not attempt them in this lab.

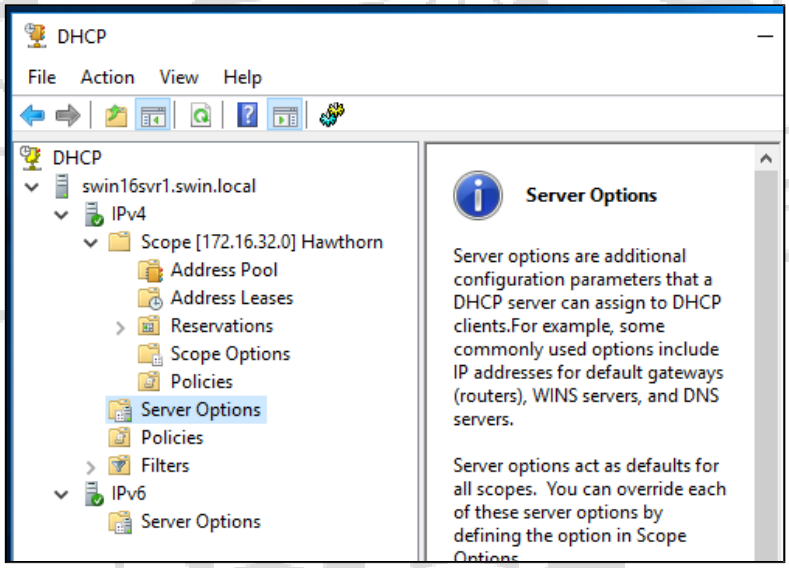


Figure 8 - Levels of DHCP Options

34. On **sWin22SVR1**, in **DHCP Management console**, expand the scope created in the section **IPv4** above.
    Click on the **Server Options** container, then **right click** to bring the **context menu**.

35. Select **Configure Options…**

    This brings up the **Options** dialog box

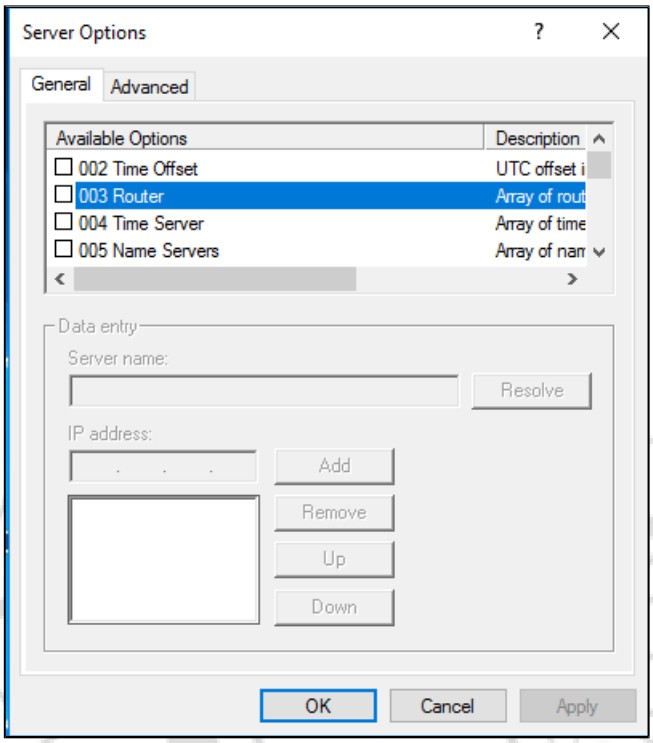


Figure 9 - Configuring Server Options

There are other options we can configure:

Option code	Name
003	Router
004	Time Server
005	Name Servers
006	DNS Servers
12	Hostname
015	DNS Domain Name
031	Perform Router Discovery

Server Options

Sometimes we want a setting to be the same for all devices from all scopes on the DHCP server. For example, a DNS server can be used by all subnets. As our network does not currently have a DNS server, we will configure some other options.

36. In the **Server Options** dialog configure:
    a. **003 Router** IP address setting to be `172.16.32.2`, and click **Add**.
    b. **015 DNS Domain Name** to be *NetAdmin.edu* and click **OK**.

37. Back on **sWin10CL101** release and renew your IP address.

    Verify that your new settings have been applied and record your new IP configuration here:

    DNS suffix: **sWin.Local**
    NetAdmin.edu

    IPv4 Address: **172.16.32.199**

    Subnet Mask: **255.255.255.0**

    Default Gateway: _____

Scope Options

Scope options are identical to Server option, except for how widely they apply. While Server options apply to all scopes on a DHCP server, Scope options only apply to the pools in each scope.

Usually Scopes are associated with subnets. So it makes sense to configure default gateways using scope options, but use **Server Options** to configure those settings that need to apply to all scopes.

38. Back on **sWin22SVR1**, expand the Hawthorn scope, click on **Scope Options**, then, right click to bring up the context menu.

    Select **Configure Options…**, configure **003 Router** IP address setting to be 172.16.32.1, and **015 DNS Domain Name** to be *ScopeSetDNS.com* and click **Add**.

39. Back on **sWin10CL101** release and renew your IP address.

    Verify that your new settings have been applied.

    What has changed? What has remained the same?

    DNS Suffix changed to ScopeSetDNS.com

Reservation Options

We have already learned how to configure a **Reservation**. Once the initial configuration is completed you can go back in and set the options for that Reservation.

40. Back on **sWin22SVR1**, expand the Hawthorn scope, expand the Reservations container and click on the **172.16.32.199**, then, right click to bring up the context menu.

    Select **Configure Options…**, configure **015 DNS Domain Name** as *ResSetDNS.com*, and click **OK**.

Option Precedence

If the same configuration setting is set in Server, Scope, and Reservation options, which is the option to '*rule them all*'? This is what we will investigate in this section.

41. Using the steps outlined above, use DHCP management console on **sWin22SVR1** to ensure the option **015 DNS Domain Name** is configured according to the following table:

Option	**DNS Domain Name**
Server option:	*NetAdmin.edu*
Scope option:	*ScopeSetDNS.com*
Reservation:	*ResSetDNS.com*

42. On **sWin10CL101**, at a command prompt, release and renew your IP address.

    Type **`ipconfig /all`**, what is the **Hostname** that appears?
    sWin10CL101

    Which option rules them all? **ResSetDNS.com**

*If you finish your lab early, you can attempt the extension questions, otherwise please skip forward to **Pack up.***

Extension (Optional)

i. What are the risks of only using one DHCP server in an organisation?

ii. What are the issues of using two DHCP servers on a network offering the same scopes? How can these issues be addressed?

iii. When configuring DHCP we did not bind a scope to an interface. When a DHCP server has multiple interfaces, how does it know which interface to send offers on.
Install DHCP on sWin22RTR, create some pools that offer addresses in the same subnets as are currently configured on each Router interface.

Connect a PC to the different virtual switches and see what leases they give.

Pack up

1. Shut down all guest VMs.
2. **Sign out** from the Host virtual machine and make sure that it is **Stopped** otherwise it will run in the background and use up your quota.
3. If on campus, **log off from the ATC626 lab PC,** and push your chair in as you leave.

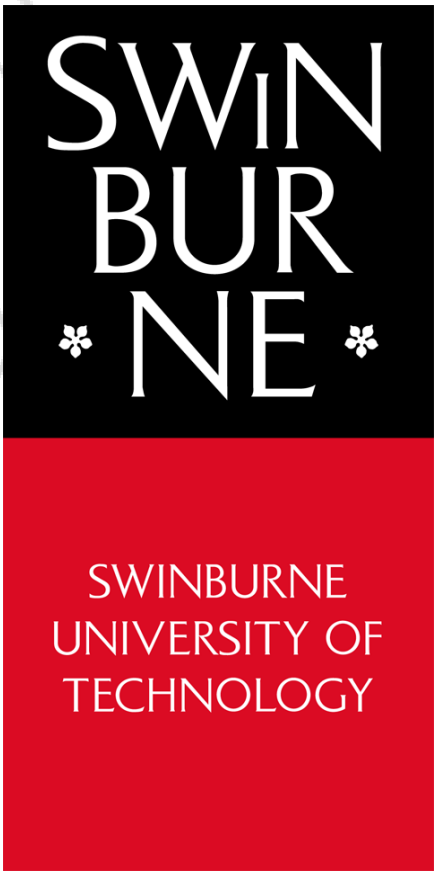
End of Lab

TNE10005/TNE60002

Network Administration

Lab 5

Introduction to DNS



Aims:

To

- Understand the purpose of DNS.
- Install DNS
- Configure zones, records, and zone transfers

Virtual Machines

sWin22DC1, sWin22SVR1, sWin22SVR3, sWin10PC203

Preliminary Settings

1. Change sWin22SVR3's switch to the Hawthorn network. Configure sWin22SVR3's IP configuration to:
    - IP: **172.16.32.13**/24
    - GW: **172.16.32.1**
    - Preferred DNS Server: **172.16.32.10**
2. Change sWin10PC203's switch to the Hawthorn network. Configure sWin10PC203's IP configuration to:
    - IP: **172.16.32.203**/24
    - GW: **172.16.32.1**
3. Ensure all VMs are on the Hawthorn network and have IP addresses in the same subnet.

Laboratory

Installation

1. Log into **sWin22DC1.**
2. Log into **sWin22SVR1** and from **Server Manager > Manage > Add Roles and Features** install the **DNS Server** role, with all default settings.

When the installation is complete, **close** the **Add Roles and Features Wizard**. Go back to **Server Manager**, and from the **Tools** menu, select **DNS**.
This should bring up the **DNS Manager** console.

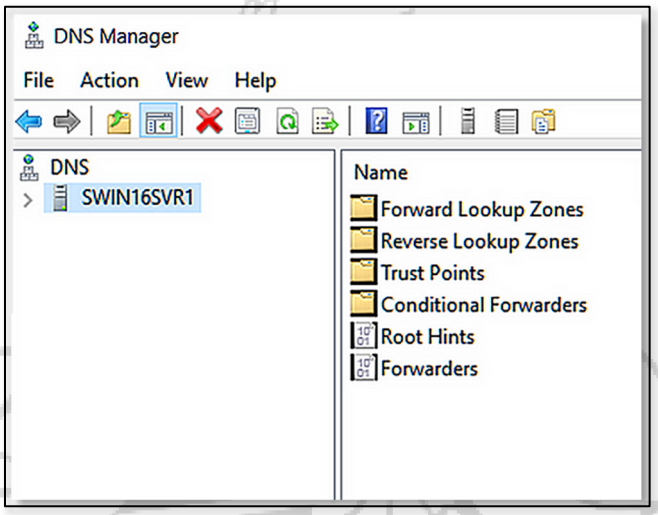


Figure 1 - DNS Manager Console

Notes:

*The figures in this lab document are captured for DHCP Management console on **sWin-Server that running Windows Server 2016.** Hence, the server's name is sWin16SVR1. Students should check on sWin22SVR1 when practicing using the unit Azure lab VMs.*

Creating a Primary Forward Lookup Zone

3. In **DNS Manager**, expand **SWIN22SVR1** and click on **Forward Lookup Zones**.
4. Right click **Forward Lookup Zones** to bring up the context menu, and select **New Zone…**
5. On the Welcome screen, click **Next**. On the **Zone Type** page, select **Primary zone** and click **Next**. Enter the Zone name ***burne.edu***, and click **Next**.

   Accept the default Zone file name and location, and click **Next**.
6. Dynamic updates are important for networks that have a lot of mobile users (e.g. a large corporation with a number of buildings in a city and meetings being scheduled across different buildings). When a computer leases a new IP address (e.g. when it connects in a different building) then its DNS record will be dynamically updated with the new IP address.

   If we were installing within an Active Directory Domain we could choose *Allow only secure updates*. Be we are installing in a Workgroup on a Stand-alone server. Allowing non-secure updates means a hacker could spoof one of our servers and update the

record for that server so that all traffic will be directed to an IP address of the hacker's choice.

7. So we will keep the default **Do not allow dynamic updates**, and click **Next,** then **Finish**.

   DNS Manager should look like Figure 2 - New Primary Zone

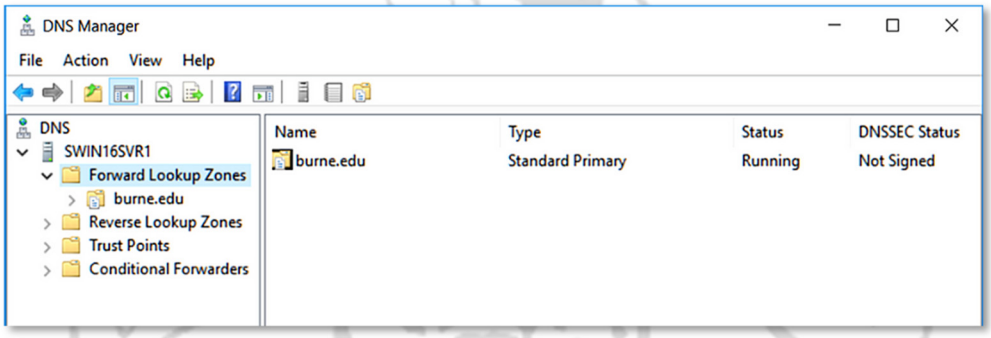


Figure 2 - New Primary Zone

Creating Network Resources

File Server

In Windows Server 2022, the **File Server** role is installed by default, so all we need to do now is make resources available on the network.

8. On **sWin22SVR3**, launch the **File Explorer** ( ) and navigate to **This PC**. Under **This PC**, create a Folder by right clicking **Local Disk (C:)**, choosing **New** from the context menu, and **Folder**.
9. Name the new folder **Data**.

   In the Data folder create a New text document called **TopSecret.txt**, add some text to the document and save it.

   We now need to **Share** the folder so users can access it over the network.
10. To share the **Data** folder, right click on the Data folder and select **Properties** from the context menu. Then select the **Sharing** tab, and click **Advanced Sharing...**
11. Check **Share this folder**. Limit the number of simultaneous users to **10.** Click the **Permissions** button and make sure that **Read** permissions are configured for **Everyone**. Click **OK**, twice, then **Close** to return to File Explorer.

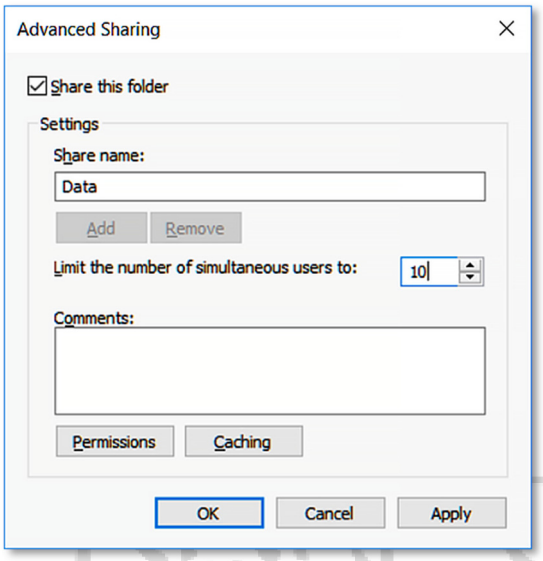


Figure 3 - Advanced Sharing

Web Server

In Windows Server, Internet Information Services (IIS) provides the Web Server role. We will now install IIS and create a default web page, so we can investigate how DNS supports web browsing.

12. On **sWin22SVR3**, in **Server Manager**, start the **Add Roles and Features** wizard, and accept the default options until you get to the **Select server roles** page.
13. Add the **Web Server (IIS)** role, accepting the default options for the remainder of the wizard. Close the wizard when installation has completed.

    Note: If the installation takes a while, move onto steps 14-15, and ensure that installation is complete before attempting step 16.
14. Click **Start**, and resisting the urge to press the enter key afterwards, type **notepad.** The **notepad** icon will appear in the programs list.

    Right click this icon and **Run as administrator**.
15. In the notepad type something similar to the following *(do better if you can)*:

```
<html>
<body>
<h1>Welcome to Kim's Web Site</h1>
<p align="center">This site is under construction </p>
</body>
</html>
```

16. Save this text file as **index.htm** in the **C:\inetpub\wwwroot** folder.
    Note: If we had not run notepad as an administrator, Windows would not have allowed us to save here.

Creating DNS records

Without DNS users from around the internet would need to use the server's IP address to access the resources on the server. So we need to create records so when a user types in *www.burne.edu* into their browser it takes them to the web server.

17. On **sWin22SVR1**, in DNS Management and in the **Forward Lookup Zones** > **burne.edu** primary zone, create records for www by:
    a. Right click the burne.edu zone and select **New Host**.
    b. In the **Name** field enter ***www***. Make sure that the FQDN is *www.burne.edu*.
    c. In the **IP address** field enter ***172.16.32.13***, then click the **Add Host** button.

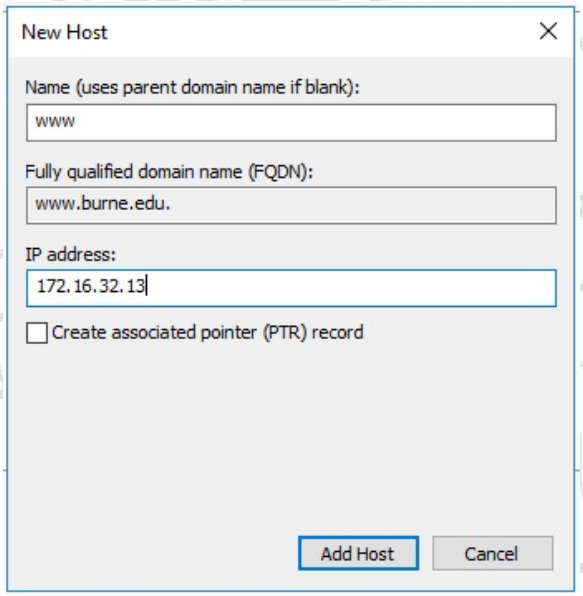


Figure 4 - Creating a New DNS A Record

    d. You will get a pop-up to tell you that the record has been created. Click **OK**.

18. We will now create a record for our **File server**. But the File Server role is being hosted on sWin22SVR3, and we have already created a record for it in step 17.

    It also makes no sense to tell users to enter *www.burne.edu* when they want to access a file server!

    So rather than creating a new record for a server that already has a record. This redundancy would cause real problems if you ever had to change the IP address of a server, you would then have to change every record for that server.

    So we will create an **alias** by creating a **CNAME** record. A CNAME record points to an existing record and allows an alias name to be attached to it.

    a. Right click on the **burne.edu** zone and select **New Alias (CNAME)**.
    b. Enter the name ***FileSvr*** in the **Alias name** field and make sure that the FQDN is *FileSvr.burne.edu*.

c. To set the **target host** click on the **Browse** button. Double click **sWin22SVR1** in the **Records** pane, then double click the **Forward Lookup Zones** container, double click the **burne.edu** zone and select the **www Host (A)** record. Click **OK** twice to return to DNS Management.

We have now created DNS records for our network resources.

If you discover that you have made a mistake with your DNS record, remember that you may need to type ***ipconfig /flushdns*** on **sWin10PC203** in order to clear the DNS cache.

Testing DNS

19. Log onto **sWin10PC203** as **Admin**:
    a. In the Ethernet adapter settings add **sWin22SVR1**'s IP address as sWin10PC203's preferred DNS server.
    b. Open the **Microsoft Edge** browser and type in ***www.burne.edu*** in the address bar. You should be directed to the web page you created in step 15.
    (If you get an error here, try to troubleshoot it with a fellow student and if that is unsuccessful, call the tutor over)
    c. Open File Explorer and type \\FileSvr.burne.edu
        - When prompted enter ***Administrator*** as the username and ***Pa55w.rd*** as the password.
        - You should now be able to see the **Data** folder created in step 9. Double clicking **Data** will allow you to see the contents of the shared folder.

    (If you get an error here, try to troubleshoot it with a fellow student and if that is unsuccessful, call the tutor over)

Zone Transfers

20. Create a secondary zone called ***burne.edu*** on **sWin22DC1** by loading **DNS Management**, right clicking on **Forward Lookup Zones**, and choosing **New Zone…** Work through the wizard to configure a **secondary** zone
21. On the **Zone name** dialog enter ***burne.edu*** and click **Next**.
22. On the Master DNS server dialog, enter **sWin22SVR1**'s IP address and click next, etc, then Finish.
23. Double-click on the new **burne.edu** zone and notice that the zone has not been loaded. This is a security measure. The DNS server on sWin22SVR1 does not hand over information just because another DNS server asks politely. Secondary Zones must have zone transfers approved and configured before data is transferred.
24. On **sWin22SVR1** in **DNS management**, right click on **burne.edu** and select **Properties**.

25. Click on the **Zone Transfers** tab.
    Now we have two choices, we can either keep a list of all DNS servers in the domain in the Name Servers tab, or we can authorise each DNS server individually. We will do the former.

    a. Click on the **Name Servers** tab and **Add… *sWin22DC1.swin.local***, and click **Resolve**. Notice that we have an error. This error is because we do not have a reverse lookup zone configure. This error will not prevent DNS from working. So click **OK**.

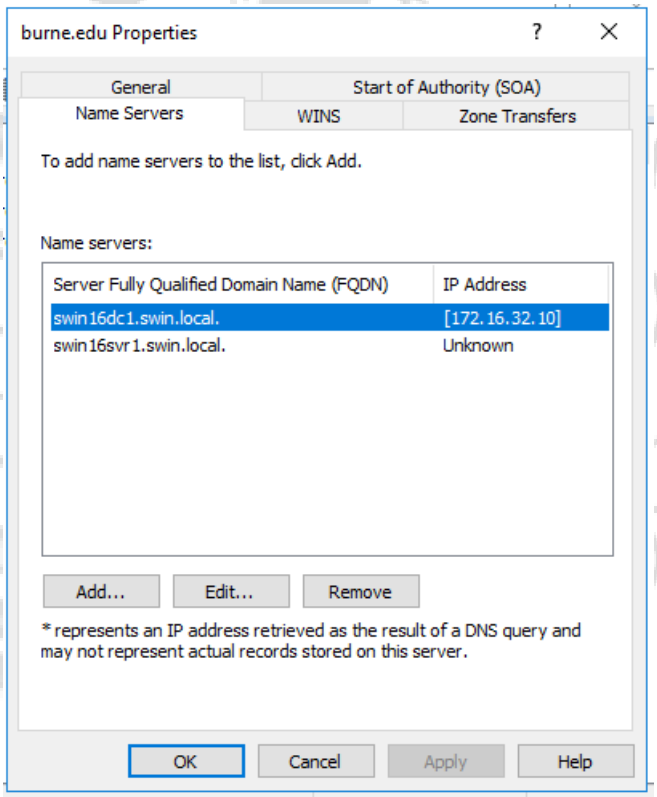


Figure 5 - Zone Transfers Name Servers Tab

    b. Now click on the **Zone Transfers** tab again, and **Allow zone transfers, Only to servers listed on the name servers tab**. Then click **OK**.

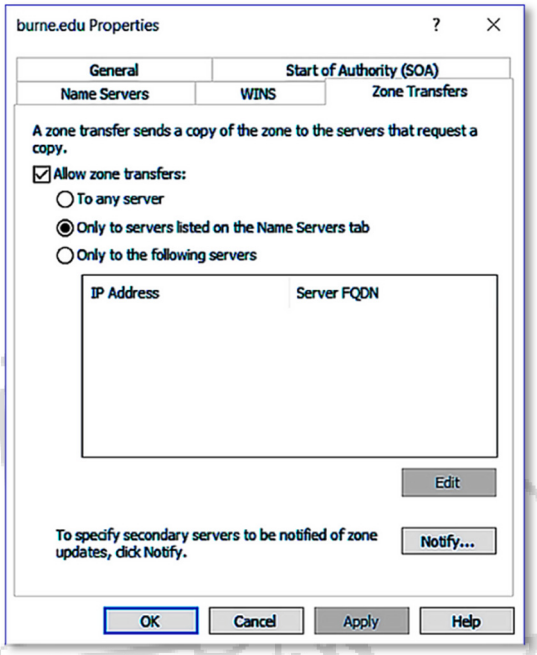


Figure 6 - Allow Zone Transfers

26. Go back to **sWin22DC1**and refresh the new sWin.local secondary zone. Does the data appear? Probably not – it takes time for the transfers to occur. If not, wait a couple of minutes then, right click the **burne.edu** zone and select ***Transfer from Master***. It should load this time.
27. Try creating some more records in the **burne.edu** Primary zone and see it they transfer to your secondary zone.

yep

Extension

(Extension exercises are optional for students who finish the lab early – the subsequent Pack Up section is not optional)

28. Create an alias for your **www** record in the **burne.edu** zone. Use your first name as the record name
29. On **sWin22SVR1** create a **Stub zone** for **sWin.local**, whose primary zone is hosted on **sWin22DC1.**

    Which records were not transferred?

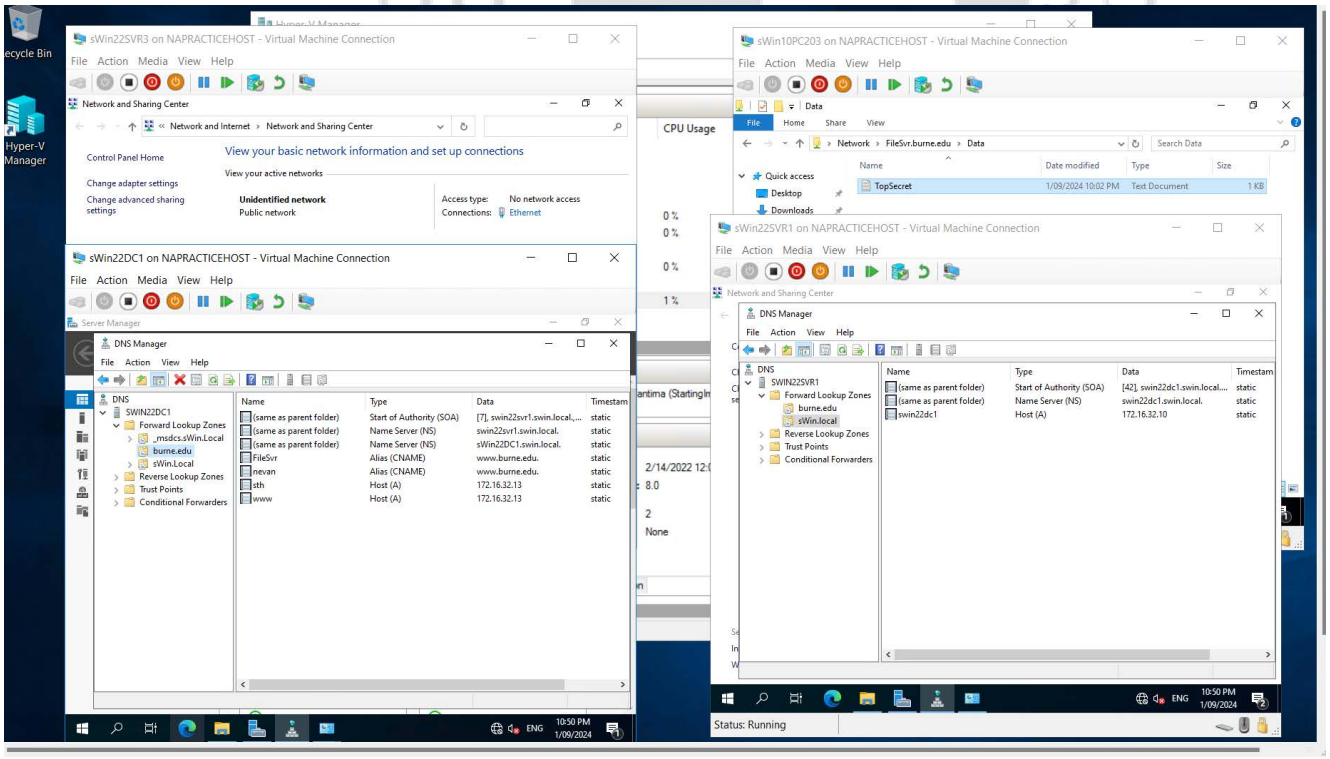
    Which records have been transferred? What do the records in a stub zone have in common?

Records in a Stub Zone

- **Transferred Records**: The stub zone will contain NS (Name Server) records that point to the authoritative DNS servers for the `sWin.local` zone. It may also include A (Address) records for those name servers.
- **Records Not Transferred**: The stub zone does not contain all the records from the primary zone; it only contains the records necessary to identify the authoritative servers. Therefore, any other records (like A records for hosts within the `sWin.local` zone) will not be transferred.

Pack

1. S
2. **S** **pped**
   o
3. If as you
   le



TNE10005/TNE60002

Network Administration

Lab 6

Configuring a Windows Server 2022 Domain

SWINBURNE UNIVERSITY OF TECHNOLOGY

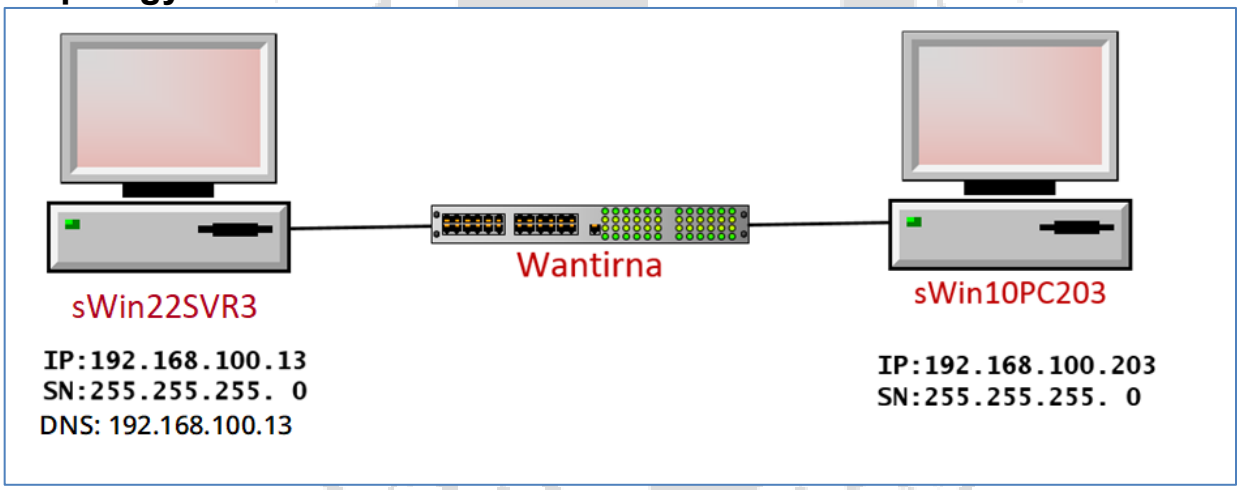
Aims:

- Install AD DS role to Windows Server 2022
- Join Windows 10 computers to a domain
- Create Domain User Accounts
- Create Domain Computer Accounts
- Create Domain Group Accounts
- Secure resources on Domain

Preliminary settings

1. Download and launch **sWin22SVR3** and **sWin10PC203**
2. **Connect** the Network Adapter of sWin22SVR3 and sWin10PC203 to the Virtual switch "**Wantirna**".
3. Ensure that both virtual machines have IP addresses in the subnet **192.168.100.0/24** before proceeding. Test by pinging from **sWin10PC203** to **sWin22SVR3** (remember default firewall settings block ping, you can allow pinging by creating a firewall rule or by sharing a folder – if you don't know how to do that, but you are confident that both Virtual machines are on the same subnet, proceed).

Topology

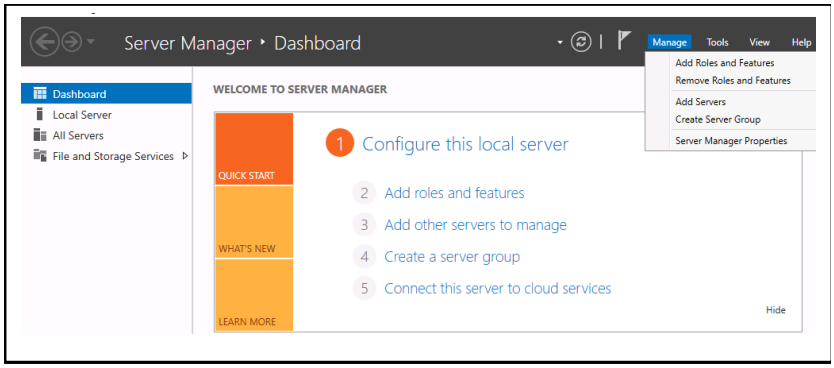


Creating a Domain

Configuring a Domain Controller

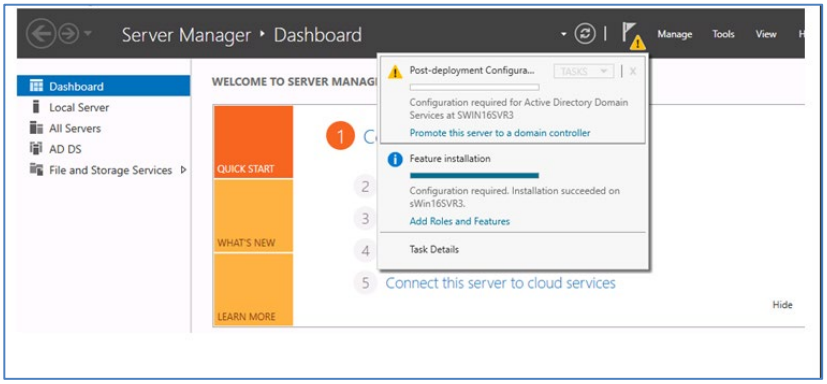
4. Log into **sWin22SVR3** as the Administrator with ***Pa55w.rd***. Configure its DNS address to be **192.168.100.13.**

5. From **Server Manager,** in the ***Manage*** tools, use ***Add Roles and Features*** to add the role of ***Active Directory Domain Services***, accepting the **default** settings.



Lab 06 – Figure 1

6. From ***Server Manager***, you should notice an alert symbol (a yellow triangle with a '!') to the left of the **Manage** tools. Click on this and select ***Promote this server to be a domain controller***.



Lab 06 – Figure 2

7. **Add a new forest** and call the domain **sWin.Local** (**.Local** is added so we don't interfere with any other domains if our server is connected accidentally to others).

8. For both the **Domain Functional Level** and **Forest Functional Level**, choose the **Windows Server 2016** level (Note: if there were older DCs already in the domain we would need to choose a domain functional level that would equal the oldest DC, as we are creating a new forest with only one DC we can set the domain functional level at the highest).

9. Accept the default options for installing a **DNS server** and a **Global catalog** (a GC is required as it is this will be the only DC in this forest). For the DSRM password type ***Pa55w.rd***. Keep in mind that if you are doing this for real, this password needs to be recorded and stored in a safe place where replacement administrators can find it (e.g. in a document called 'emergency passwords' stored in the company safe).

10. Accept the defaults for the remainder of the wizard. Note that errors may be displayed when the wizard completes the tests. This is mainly due to the virtual machine not being connected to the internet.

11. At the end of the installation, **restart** the computer and log in again as the **administrator** (*Sign in to: Swi*n = This is the administrator account in the domain Swin.Local)

Creating resources

12. Create a folders at **C:** called **sWinData** and **Home**

13. In the **sWinData** folder create 3 text documents named **General.txt**, **Restricted.txt** and **TopSecret.txt**

14. Share the **Home** folder so that the **Everyone** group has **Full Control** (i.e. right click the folder, select **Properties**, select the **Sharing** tab, click **Advanced Sharing**..., click **Share this folder**, click the **Permissions** button, tick **Full Control** in the **Allow** column).

Joining a Domain

15. From **sWin10PC203**, log in as **Local Administrator** (This is the administrator account of sWin10PC203). Ensure that the DNS address is configured with the IP address **of sWin22SVR3**'s address.

    You can use **ping** to confirm, **ping sWin.Local**. If an IP address is returned in the ping attempt, then you know DNS is working.

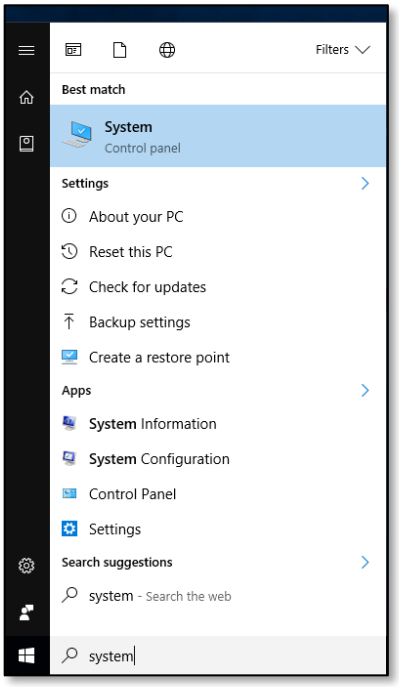
    Optional

    An alternative is to use nslookup is a command line utility that allows us to trouble shoot DNS problems. In this situation we can run a cmd console and type **nslookup** <enter>. You will be presented with the prompt **>**. At this prompt type the name of the domain, URL or machine name you want to resolve and press enter. If DNS is working it should return the IP address of that name.

    In this situation we want to resolve our domain name. So type **sWin.Local** <enter>. If it returns the IP address of the domain controller, it is working (hint: type ***exit*** to leave NSLookup)

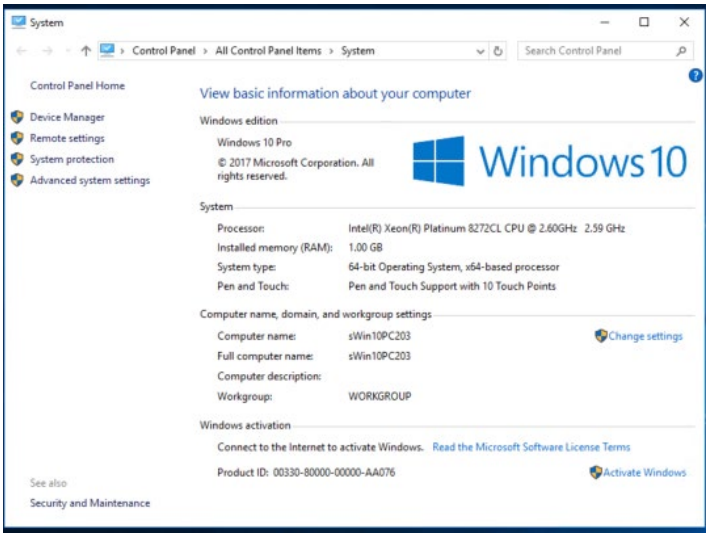
16. At the Start screen, start typing **System**.

    Note that when you start typing, a search bar appears and lists the applications and files that match you typing. Click **System** (Control Panel) to launch it.



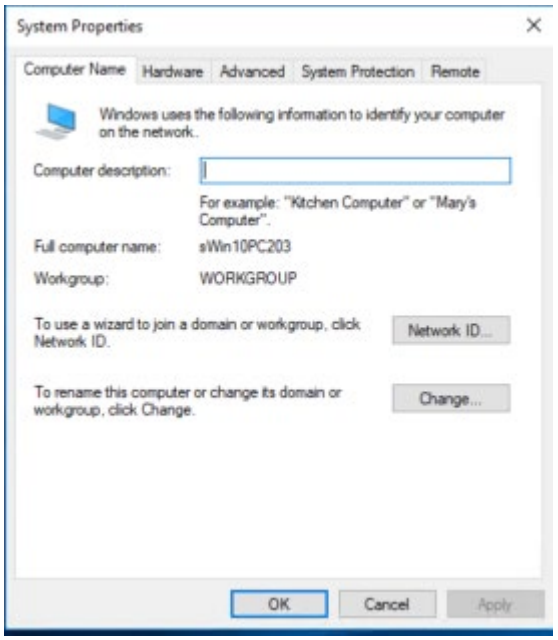
Lab 06 – Figure 3

In the **System** window, select **Change Settings**.



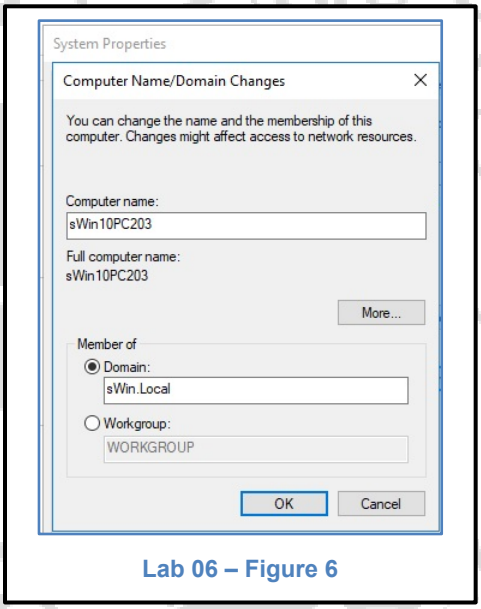
Lab 06 – Figure 4

In the **System Properties** dialog box, select **Change**.



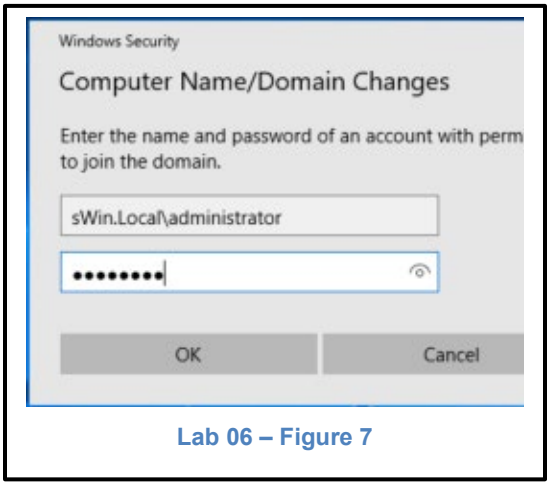
Lab 06 – Figure 5

17. In the **Computer Name/Domain Changes** dialog box, select **Domain,** and in the **Member of Domain** field type **sWin.Local** and press **OK**.



Lab 06 – Figure 6

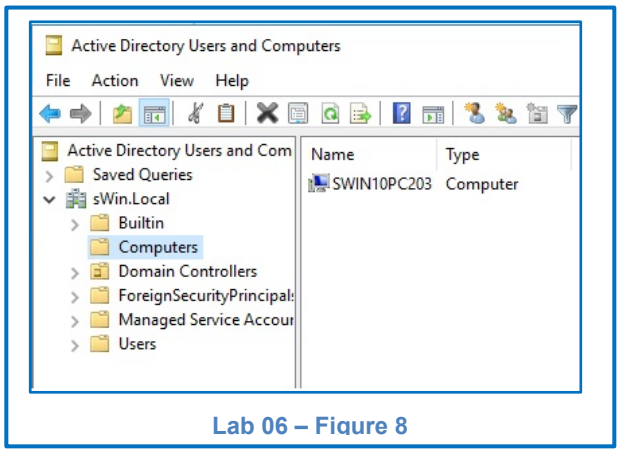
18. When prompted, enter the username and password of an account that has the permissions to create computer accounts in the domain. In this situation we will use the **administrator**'s account, but normal we would use another account.



Lab 06 – Figure 7

Click **OK** to confirm and finish the joining process. Reboot the virtual machine when prompted.

19. You will notice that a computer account has been created in the **Computers** container in **Active Directory Users and Computers** (which can be accessed from **Server Manager, Tools**).



Lab 06 – Figure 8

Creating Accounts

Logging on With an Existing User Account

Logging on with existing accounts is a bit tricky with Windows 10.

Now that we have joined the domain, we can now log on with a local user account (e.g. **sWin10PC203\Jill**) or we can log on with a domain user account (e.g **sWin\Jill**).

If we log on with a local user account, we will be authenticated by the SAM, but consequently we can only have authorisation to resources on the local PC.
If we log on with a domain user account we will be authenticated by Active Directory and can have authorisation to any resource on the domain.
The question is how to determine whether we are logging in to the domain or the local machine.

20. Notice that when the **sWin10PC203** machine has rebooted, it now asks us to press **"CTRL + ALT + DELETE"** to log on. But when we do press CTRL+ALT+DELETE it is still defaulting to the local Jill's login. Click on **Other User**. Notice how it now states under the password field "Log on to: **sWin**". This means that the log on expected is from a sWin domain account. The problem is, we have not created any domain user accounts.

Creating User Accounts

We will now create a domain user account for the user Jill St John.

21. On **sWin22SVR3, in Active Directory Users and Computers** (This Tools can be launched from **Server Manager – Tools,** or by running the command **dsa.msc**).

22. Right click on the **Users** container and select **New…**, **User**.

23. Type **Jill** for the first name, **St John** for the last name and **Jill** for the user logon name, then click **Next**.

24. Enter the standard lab password for the password and confirm password.

    Normally we would keep the default setting of **User must change password at next logon** so that the user's password is known only by them. If creating a batch of user accounts we would also disable the account so it could not be used until we could confirm that the new user had started. For service accounts we would want the password to never expire.

    Clear the checkbox next to **User must change password at next logon**, so that we don't have to change the password when Jill logs on.

25. Go back to **sWin10PC203** and log on as **sWin\Jill**.

26. On **sWin22SVR3**, repeat the steps above to create a new user account called **Jack.**

Creating Computer Accounts with DSA.msc

27. In **Active Directory Users and Computers** right click on the **Computers** container and select **New…, Computer**

28. The computer name you type must exactly match the computer name of the PC you are creating an account for. In this case we are going to create an account for our second Windows 10 PC.

    In the **Computer name:** field, type **sWin10PC201.**

    Click on the **Change…** button and type in **Jill** then click the **Check Names** button. This gives Jill permission to join her computer to the domain, otherwise we would need to enter in the administrator details as we did in step 18. Click **OK.**

    Jill can now follow steps similar to steps 15 to 19 to join her computer to the domain.

    Don't try this now, as our host lab machines don't have in sufficient RAM, but at the end of the lab, after you have shut down sWin10PC203, start up sWin10PC201 and join it to the sWin.Local domain with Jill's username and password.

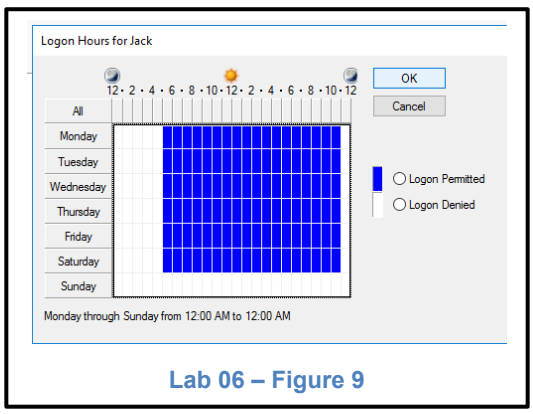
Configuring Account Properties

Setting User Account Properties

29. In **Active Directory Users and Computers**, in the **Users** container, right click on **Jack**'s user account and select **Properties**.

30. Configure the following settings for the following tabs:

General:	Display name = Jack Nguyen Description = Company Accountant Office = 477B-101A E-mail = Jack@sWin.Local
Address:	Street = 477B Burwood Rd City = Hawthorn State = Vic. Post Code = 3122 Country = Australia
Account:	Logon Hours = 5AM-11PM, Monday to Saturday Logon To = sWin10PC203, sWin10PC201



Lab 06 – Figure 9

Note: There are other important properties in the Account tab, such as **Unlock account, User must change password at next logon**, etc. We saw many of these in the new user wizard, but here is where we change these properties once the account has been created.

Profile: Home folder, Connect = Z: **\\sWin22SVR3\Home\%username%**

Note: The **%username%** is a system variable that will be replaced by the user's name (in this case Jack). The benefit of using this variable is that if you ever want to copy this user account, this property will then point to the new user's home folder. See Creating Account Templates, later in the lab.

Memberof: Remote Desktop Users

Note: We will add more memberof groups when we have created more groups later in the lab.

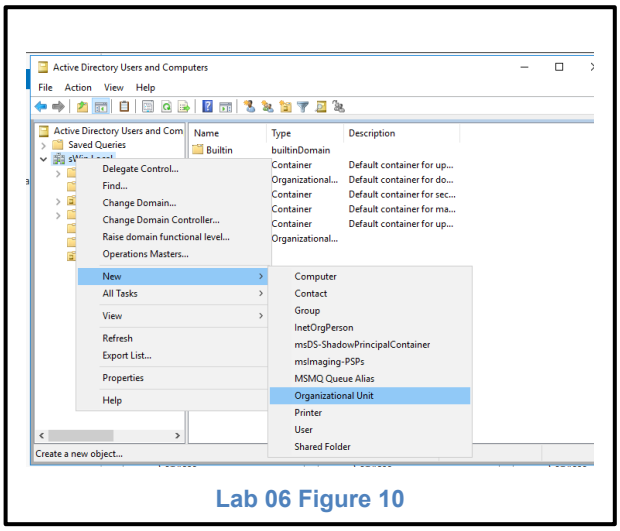
Setting Computer Account Properties

31. In **Active Directory Users and Computers**, in the **Computers** container right click on click on **sWin10PC203** and select **Properties**.
32. On the **General** tab, in the **Descriptio**n field enter a description of **sWin10PC203** e.g. **Jill's Virtual machine**. On the **Location** tab click and in the field enter **477B-101**.

Creating an Organisational Unit

An Organisational Unit is an administrator created container for accounts and groups. The administration of OU's can be delegated to other users so that the main administrator can organise the work load amongst the administration team.

33. In **Active Directory Users and Computers** right click on the **sWin.Local** domain root and choose **New…**, **Organizational Unit**. Name the OU **AccountDept**. If the OU is a temporary OU, remove the tick from the **Protect container from accidental deletion**. This OU is not going to be used in a live organisation so we'll remove the tick.



Lab 06 Figure 10

Creating Group Accounts

Creating Resource Groups

Resource groups are also called ACL groups. Their purpose is to streamline the way administrators control access to resources and to minimise the size of DACLs in order to keep servers functioning efficiently. The group scope Domain Local groups are best suited as ACL groups. They can only be given permissions to local resources yet they can have accounts from any trusted domain as members. Thus we can use domain local groups to control access from anywhere in the forest.

34. Right click on the new OU we created in step 33 and select **New…**, **Group**.

35. Ensure that you click the **Domain local** control button, so that the new group is of the right scope.

    The names of ACL groups should adhere to the following conventions. They should begin with ACL to reflect their purpose or DL to reflect their scope. The next part of the name should reflect the resource or resources they are controlling access to.

    The name should not reflect the users that are accessing the resource.

ACL groups can only give one set of permissions. In other words you cannot use and ACL group to give Read permissions to one user and Full Control to another user. ACL groups can only give the same set of permissions, all read, or all read write or all full control. Consequently we reflect the level of permissions being given in the name.

We will be creating DL groups to grant access to the sWinData folder created in step 12.

Examples of group names that comply with the convention are DL_sWinData_RW, ACL_sWinData_RO.

36. Devise a naming scheme that meets the conventions above and create **two** DL groups for the sWinData folder. One DL group should give members **Read Only** access, the other group should give members **Read Write** access.

Assigning Permissions for Resources

Assigning NTFS Permissions

37. Right click on the folder **C:\sWinData** and select **Properties** and click on the **Security** tab.

38. This properties tab allows us to view the NTFS permissions currently allocated to the sWinData folder, but unlike Windows Server 2003, we cannot edit the NTFS permissions. Click the **Edit** button.

39. Here we can edit the currently assigned permissions. We want to add the resource groups we create in the Creating Resource Groups section of the lab.

    Click the **Add** button, and in the **Enter the object names…** field type the first two or three letters of the resource group names, e.g. **DL**. Then click **Check Names** to list the matching groups.

40. Click on the **Read Write** version of your resource group and click **OK**.

41. Make sure there are ticks in the allow column for the permissions:
    i. Read & Execute
    ii. List Folder Contents
    iii. Read
    iv. Write

    The first three permissions are default, but the write permission will need to be set. You may need to scroll the permissions down in order to see the write permission.

42. Now add the **Read Only** version of your resource group.

43. Make sure there are ticks in the allow column for the permissions:

    i. Read & Execute

    ii. List Folder Contents

    iii. Read

Then click **OK** and verify that the correct permissions have been set.

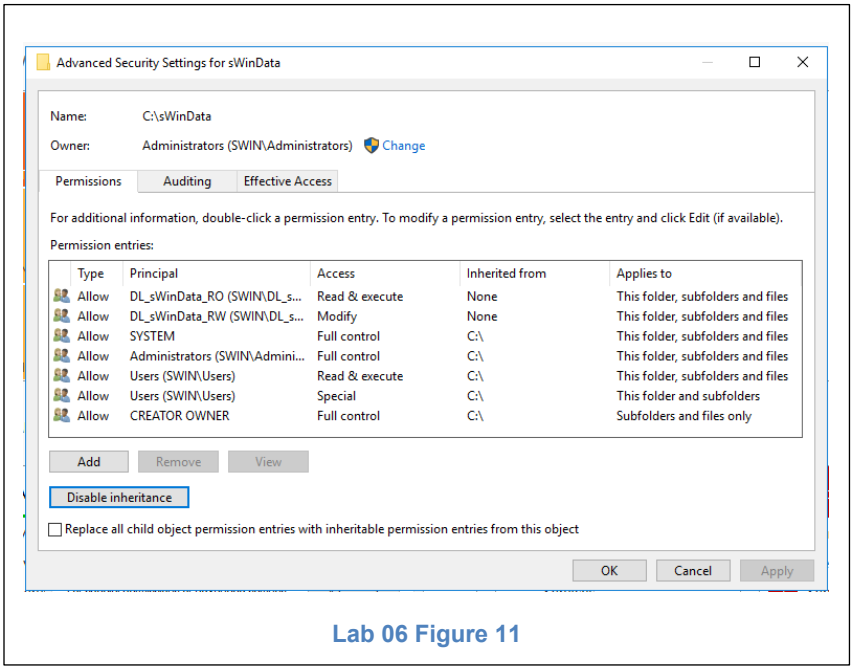
Notice that at the bottom of the list of groups with permissions to sWinData is the **Users** group.

What sort of permissions do they have?_____.

Removing Inherited Permissions

We will need to remove the permissions assigned to the **Users** group if we don't want everyone to have access to the files in this folder.

44. In the **Security** tab of the SWinData folder **Properties**, click on the **Advanced** button.



Lab 06 Figure 11

45. Click the **Disable inheritance** button, and select **Convert inherited permissions into explicit permissions on this object** option.

If we had selected the **Remove all inherited permissions for this object** option we would have deleted all of the inherited permissions, even the Administrator permissions, thus potentially cutting our own access to the folder.

For documents that need to be very secure we would remove the inherited permissions and then add the accounts that we want to provide access to.

In this situation, there is only **one group** we want to remove from the list, so we choose **Convert...**.

46. In the list of **Permission entries:** click on every entry for the **User** group (and no other group!, then click **Remove**. Then click **OK** for the next two dialogs until you are back at the **sWinData Properties** dialog.

Assigning Share Permissions

NTFS permissions should always form the foundation of our access control, as they are applied in all circumstances. But if we want accounts to be able to access the data in a folder via the network, we must create a share. Thus we must also allocate share permissions.

47. Click on the **Sharing** tab and then the **Advanced Sharing…** button

48. By placing a tick in the **Share this folder** checkbox we activate the other controls on this dialog.

    We will accept the default share name. By default it is the same as the folder name, but they can be different. This allows us to create a number of shares for any particular folder. We can create one share that will only allow read only access to a folder. We can then create another share for that folder that will allow full control access.

    When we create a share, by default the share is advertised to all computers that have Network Discovery enabled. However if we have a share that provides full control access to a folder, we may not want it to be advertised. Consequently we are able to hide a share by adding a **$** to the end of the share name. For example, in this situation we would name the share **sWinData$** and it would no longer be advertised and hence users could not browse to the share. A user would have to know the full UNC path (i.e. \\server\sharename, e.g. **\\sWin22SVR3\sWinData$**) in order to access the share.

    Note that we have not changed the name of the folder, it is still called sWinData, but by adding a **$** to the end of the share name, it becomes a hidden share.

49. Click on the **Permissions** button, and assign the **Everyone** group **Full Control**.

    Some may ask “isn’t Full Control a security risk?” The answer is yes, if you don’t have a good NTFS permission scheme in place.

    In this circumstance we intend for at least one group to have write access to the files in the folder. If we left the share permissions as the default read only, then no user would be able to write to the files in the folder while accessing them through the share. Not even the administrators! Not very functional! So knowing that we have a sound permission scheme in place (e.g. we removed the users group inheritance), I can safely set the share permission to full control. This way I have flexibility with future resource groups I create to give them whatever permission I feel the resource group needs.

    Click **OK** for the next three dialogs, until you are back to the **Local Disk (C:)** window.

Creating Account Groups

Account groups enable an administrator to streamline the allocation of permissions to a number of user or computer accounts. Account groups are created to group user and computer accounts that have similar requirements.

The Global group scope is typically used for creating account groups.

Requirements may be based on function within the organisation, or geography in an organisation that is spread over a wide area. For example we may be an administrator for a large company based in a tall building. We may want to prevent users from accidentally printing to printers on different floors. So we create account groups that will group the user accounts of users who are based in each floor. More typically, we create account groups based on function.

For example, in most medium to large organisations, people are employed in departments
e.g. Sales, Production, Research, Support, Accounts, Maintenance, etc. Typically the users in each department perform a similar function, thus they tend to need access to the same resources. So we create an account group based on function in the organisation and give the group a name that reflects both the scope of the group and the functional area of the organisation. For example G_Accounts.

In distributed organisations (i.e. over a number of sites) our naming convention may need to be a hybrid of function and geography. This is certainly the case in a multi-domain forest.

For example, using the SWin campuses as a framework, for the Accounts department we may use group names such as: G_Accounts_Hwn, G_Accounts_Swk, G_Accounts_Lil, etc.

50. In **Active Directory Users and Computers** right click on the **AccountsDept** OU, and select **New…, Group**.

    Ensure that the group scope is **Global** and name the group **G_Acc_Mgrs**. Then click **OK**.

    Right click on our new group and choose **Properties,** then the **Members** tab. Add **Jill** as a member of the **G_Acc_Mgrs** group.

51. Repeat step 50, but this time name the group **G_Acc_Pay** and make **Jack** a member of this group.

Nesting Groups

We now need to link all of the groups together, so that our user accounts have the intended access to the SWinData folder. When we make one group a member of another group we call it group **nesting**.

52. For the **DL_SWinData_RW** group, using the same method in step 50, add the **G_Acc_Mgrs** group as a member.
53. For the next nesting we will use a slightly different approach. Right click on the **G_Acc_Pay** group, select **Properties**, but this time click the **Memberof** tab. Add the **DL_SWinData_RO** group as a member of group.
54. Ensure that you click **OK** to apply the configuration changes.

Testing the configuration

55. On **sWin10PC203**, log on as **Jill** and check to ensure that she has read and write access to the folder (remember the UNC path, step 48, will take us to the share directly if network browsing is too slow).

    Remember access tokens are created when a user account logs in. If Jill is already logged on to sWin10PC203 then none of the SIDs of the new group memberships will be present in her access token.

    Whenever group membership changes, *the user needs to log off and log back on* in order to create a new access token with the SIDs of the new groups.

56. Log on as **Jack** and ensure that he only has read access to the folder.

Extension

- Create some appropriate resource groups for the files TopSecret and Restricted. Also create some more user accounts making them members of the account groups we have created. Play around with different permission to the different groups and different group membership for the user accounts. See if you can predict the effective permissions for each group. Test your predictions by logging in as a user and try to access the different objects.
- Close down **sWin10PC203** and start **sWin10PC201.** See if you can add **sWin10PC201** to the domain using **Jill**'s domain credentials.

Pack up

1. Shut down all guest VMs.
2. **Sign out** from the Host virtual machine and make sure that it is **Stopped** otherwise it will run in the background and use up your quota.
3. If on campus, **log off from the ATC626 lab PC,** and push your chair in as you leave.

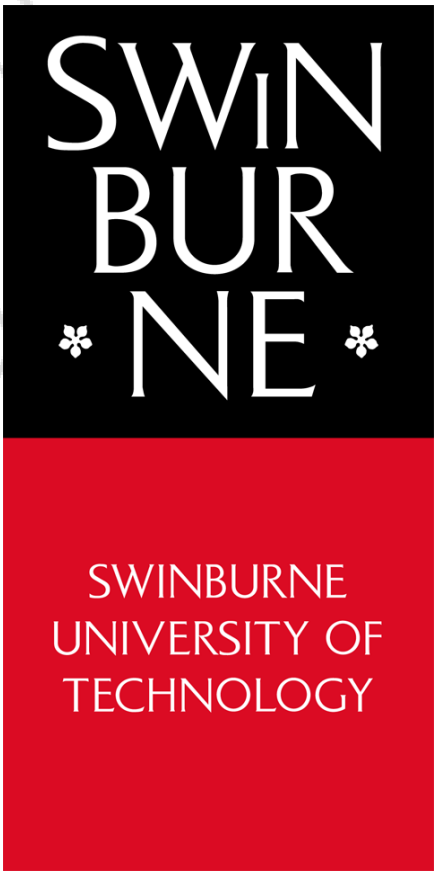
End of Lab

TNE10005/TNE60002

Network Administration

Lab 7

Increasing Object Security Using AD Groups



Aims:

- Install a child domain
- Create resources to share throughout the forest
- Deploy a secure and scalable group strategy.

Virtual Machines

sWin22DC1, sWin22RTR, sWin22SVR2, sWin22SVR3, sWin10CL101, sWin10PC203.

First, launch and log on to sWin22DC1. Then launch sWin22RTR. When sWin22RTR is loaded, launch and login to the following virtual machines in this order: sWin22SVR2, sWin22SVR3.

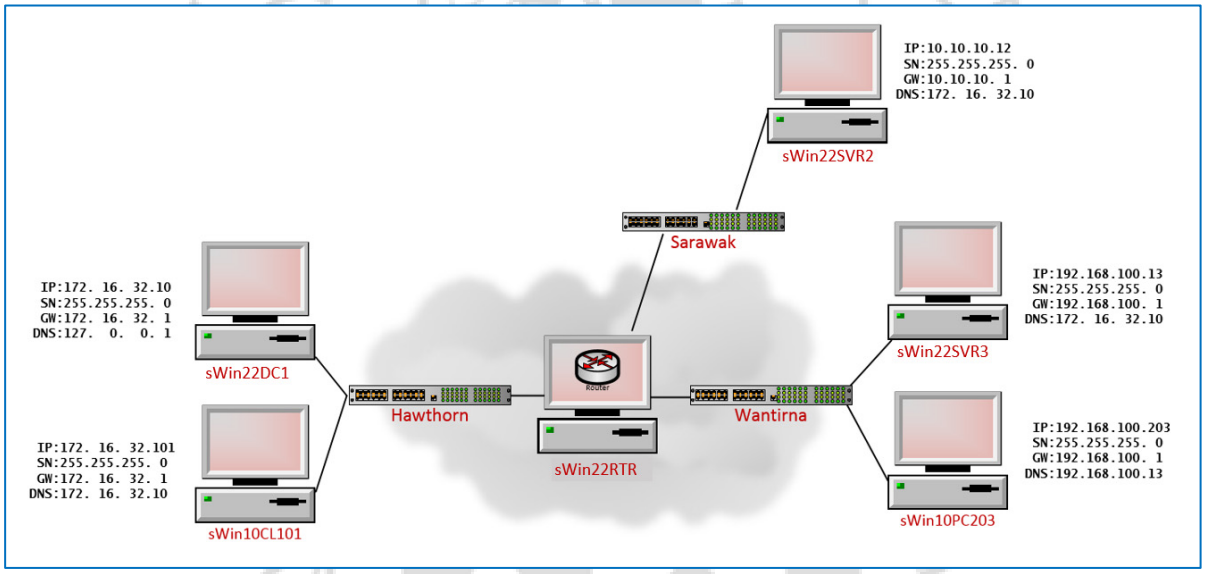


Figure 1 - Lab 07 Topology

Preliminary settings:

> ***Note:***
> *This lab assumes that you have taken adequate notes and mastered key steps from past labs. If you find that your notes are missing key steps, make sure you update them before you leave.*

Check to see if sWin22SVR3, sWin10CL101 and sWin10PC203 are connected to the correct virtual switches and have the IP configuration that matches Figure 1 - Lab 07 Topology.

This should not take longer than 10 minutes.

Lab Exercises

Create a Child Domain

1. Verify that the DNS server address is properly configured on **sWin22SVR3** by ensuring you can successfully ping ***sWin.local***. If you cannot successfully ping, see if you and a fellow student can troubleshoot the error. Call for assistance from the tutor if you have not resolved the problem in five minutes.
2. Add the **Active Directory Domain Services** role to **sWin22SVR3** (refer to Lab 06 if you cannot remember how to do this).
3. Once the installation is complete, on **sWin22SVR3**, in **Server Manager**, click on the alert and select **Promote this server to be a domain controller**.

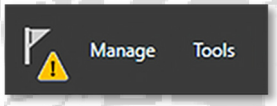


Figure 2 - Promote Server

4. On the wizard page **Deployment Configuration**:
    a. Select the deployment operation **Add a new domain to an existing forest**,
    b. Click the **Select...** button to provide the Enterprise Administrator's credentials and enter:
        i. ***sWin.local\Administrator*** as the User name, and
        ii. ***Pa55w.rd*** as the password.
    c. Fill out the rest of the page as given in Figure 3 - Child Domain Creation, and click **Next**.

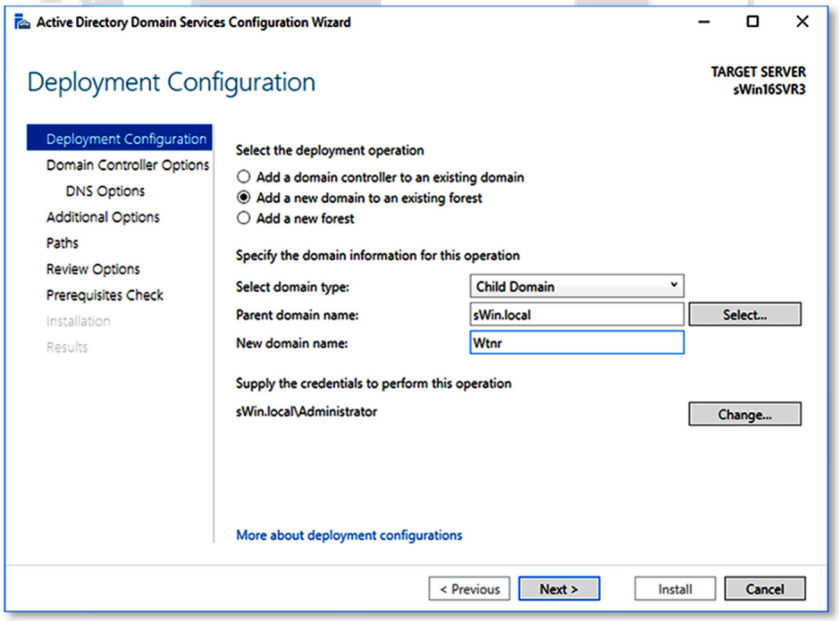


Figure 3 - Child Domain Creation

5. On the **Domain Controller Options** page of the wizard, ensure that the options selected match those given in Figure 4 - Domain Controller Options

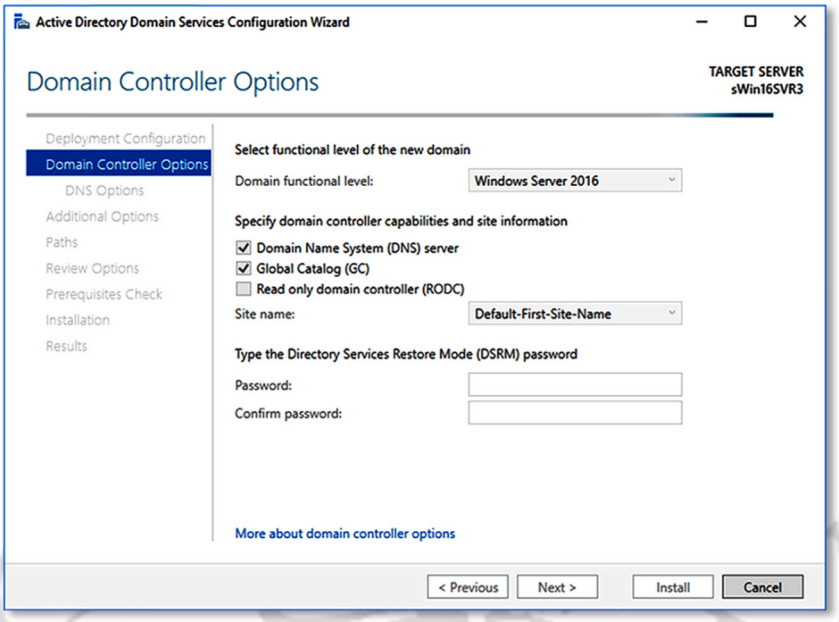


Figure 4 - Domain Controller Options

6. Enter the standard lab password as the **DSRM** password and click **Next.**
7. On the **DNS Options** wizard page, ensure **Create DNS delegation** is ticked and that the Credentials for delegation creation is **sWin.local\Administrator**, and click **Next**.

   Click **Next** for the next three pages of the Wizard.

   On the **Prerequisites Check** page, ignore the alert about *cryptography algorithms*, this is beyond the scope of this course, and does not create a serious threat, and click **Install**.

   sWin22SVR3 will now be promoted as the primary DC in a new child domain. In order to do this a DNS server for the child domain needs to be installed and all of the relevant forest information must be copied across from sWin22DC1.

   This all takes some time, so we will use this time to create some user accounts and network resources.

Only if you receive an error message of failing to promote sWin22VR3, perform the following steps on both sWIn22DC1 and sWinSVR2:

- *Launch Windows PowerShell*
- *Within the Windows PowerShell, type **repadmin /syncall** and press **<Enter>***

Group Strategy

We will now try to create the following objects and resources:

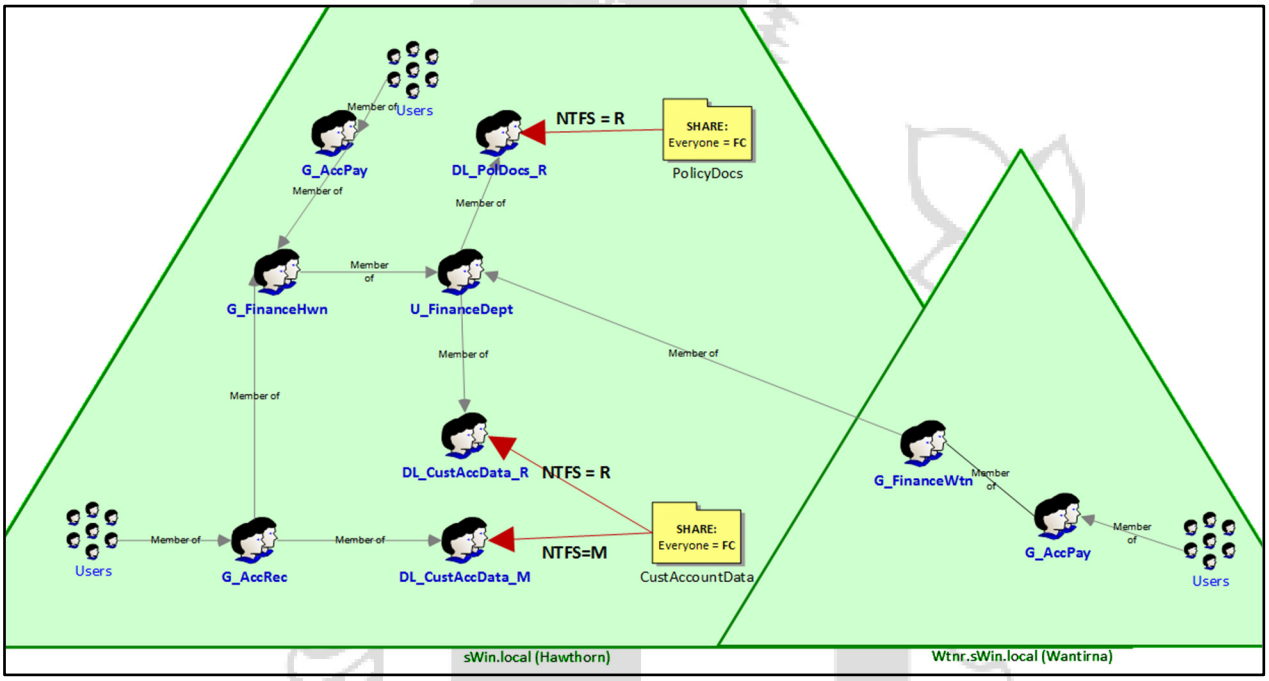


Figure 5 - Group Strategy for Lab 07

Creating Network Resources

8. On **sWin22DC1:**
   a. Create the folders:
      i. **C:\Policy_Docs**
      ii. **C:\CustAccountData**
      iii. **C:\Home**
   b. Share these folders with the **share** permissions **Everyone = Full Control**.
   c. Create some sample files in both the **Policy_Docs** and **CustAccountData** folders
   d. On the folders Policy_Docs and CustAccountData, following the steps from the ***Removing Inherited Permissions*** from last week's lab, remove all permissions for the **Users** group (and no other group).

Create an OU

9. On **sWin22DC1** launch **Active Directory Users and Computers**, right click on **sWin.local** and select **New** > **Organizational Unit**. Name the new OU **Finance**.

Create sWin.local Groups

10. Right click on the new OU **Finance**, and select **New** > **Group**.
    a. Name the group **G_FinanceHwn**.
    b. Ensure that the Group scope **Global** is selected and that the Group type is **Security**.

> ***NOTE:*** *We will only be using the **Security** Group type in Network Admin. You cannot allocate permissions with Distribution groups. Distribution groups are effectively e-mail lists.*

> ***NOTE:*** Second Level Account Groups
>
> Occasionally we face the need to group account groups. For example, a department may have a number of teams within the department such as Accounts Receivable and Accounts Payable or Maintenance Electrical, Maintenance Building and Maintenance Plumbing. In some circumstances the administrator needs to give one team access to a resource, but not the other teams. Then in different circumstances the administrator may need to give the whole department access to a resource.
>
> The most efficient, flexible and scalable way of doing this is to create a second level account group where we make the first level account group a member of the second level account group.
>
> For example in the Accounts department we may want to create the first level account groups G_Acc_Rec and G_Acc_Pay. We would make the user accounts members of the appropriate group according to which team they are allocated to. We then create a second level account group call G_Acc_Dept and add the G_Acc_Rec and G_Acc_Pay group's members. This way we only need to give the G_Acc_Dept access to a resource and the member groups also get access. This approach is sometimes called the I G G DL A group strategy.
>
> In a multi-domain forest, we cannot use Global groups as second level account groups if we want to provide access to resources in different domains. This is due to the fact that the Global group scope can only have accounts from its local domain as members. Thus in situations where we need to create a second level account group in a multi-domain forest we need to use the Universal group scope.
>
> Taking the Swinburne campuses as an example. Assuming that we have domains at each campus and together they form a forest. We would create global groups at each campus e.g. G_Accounts_Hwn, G_Accounts_Swk, etc. For our second level account group we would create the Universal group U_Acc_Dept, and make each of the G_Acc... groups from each domain members. This approach is called the I G U DL A group strategy.

11. Repeat the process to create the following groups:

Name	Scope
G_AccPay	Global
G_AccRec	Global
U_FinanceDept	Universal
DL_CustAccData_R	Domain Local
DL_CustAccData_M	Domain Local
DL_PolicyDocs_R	Domain Local

NOTE: *When creating groups the default scope is* ***Global****. This can be a potential problem if you are creating many groups in a rush and forget to change the default group to Domain Local. If you do make this mistake you cannot directly change a Domain Local group into a Global group. However you can change either type to a Universal group, and from a universal group you can change to either Global or Domain Local. So if you accidentally create the wrong scope, don't panic, just change to a Universal group, make sure that you click OK, then you can change back to the correct scope.*

We will nest the groups later on.

Creating sWin.local User Accounts and Templates

In last week's lab we used **Active Directory Users and Computers** to create user accounts. In this section we are going to create a user account template.

Users in the same team generally need to access the same resources. They generally need to use the same computers, same printers and same data, hence need to be members of the same groups. Now you could configure all of these attributes every time you create a new user... or you can create a **User account template**. A user account template is just a user account that we copy every time we need to create a new user account for that team.

NOTE: When you copy a user account template the following attributes are copied to the new user account:

- *Group Memberships*
- *Home Directories*
- *Profile Settings*
- *Logon Scripts*
- *Logon Hours*
- *Password Settings*
- *Department Name*
- *Manager*

12. On **sWin22DC1** launch **Active Directory Users and Computers**. Right click on the OU **Finance** and select **New** > **User**

    a. Enter ***_UsrTmpAccPay*** as both the **First name**, and **User logon name**, and click **Next**.

    b. As this account will not be used by any user we do not need to add a password, but we need to ensure that **User must change password at next logon**, and **Account is disabled**. Ensure both are ticked then click **Next**, then **Finish**.

13. We now need to configure the attributes that we want copied to each new user account for this team:

    Right click on **_UsrTmpAccPay** and select **Properties**
    *(Note: If you are behind schedule only configure **a** & **b**)*

    a. On the **Profile** tab:

        i. **Home folder** to **Connect**, **H:**,
        To: **\\sWin22DC1\Home\%username%**

    b. On the **Member Of** tab:

        i. **Add**, **G_AccPay**

    c. On the **Account** tab, set:

        i. **Logon Hours…** to Monday to Friday

        ii. **Log On To…** to **sWin10CL101**

        iii. **Account expires** = the last day of the current year.

    Then click **OK**

14. To copy this template, right click the **_UsrTmpAccPay** account and select **Copy…**

    a. Enter the First name ***Doug***, the Last name ***Pirahna*** and the User logon name ***dpirahna***, and click **Next**.

    b. Enter the Password ***Pa55w.rd*** and remove the ticks **User must change password**, and **Account is disabled**.
    (Note: In the real world we not do this, this is to speed up the lab)

    c. Duplicate this template again for another new user **Luigi Vercotti**.
    After duplicating, on the user's Member Of tab, remove the current group, and make Luigi a member of the G_AccRec group.

    Note: You should now be able to observe new user folders in the C:\Home\ folder.

We will now change back to the Wantirna domain to finalise its configuration.

Verifying Successful Child Domain Creation

15. On **sWin22SVR3**, type Pa55w.rd to log on as WTNR\Administrator. In Server Manager, from Tools select **Active Directory Domains and Trusts**. Expand **sWin.local** and verify that **Wtnr.sWin.local** has been added as a child domain. It should appear similar to Figure 6 - Active Directory Domains and Trusts.

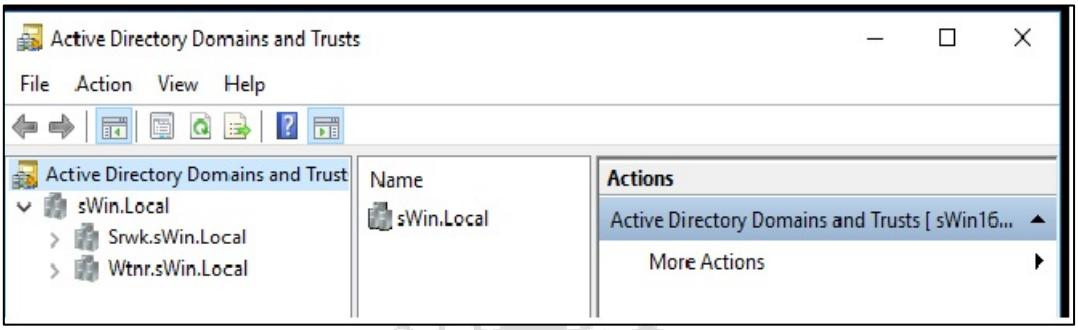


Figure 6 - Active Directory Domains and Trusts

Create Wtnr.sWin.local Objects

Create an OU in PowerShell

16. On **sWin22SVR3**, load **PowerShell** and type:

    new-ADOrganizationalUnit -name Finance -path "
    dc=Wtnr,*dc=sWin,dc=local"*

    and press **Enter**

Create a New User Account Using PowerShell

17. Enter the following to create a new user account for Kim:

    ```
    New-AdUser -name "Kim" -Path "ou=Finance,dc=Wtnr,dc=sWin,dc=local" -
    accountPassword (ConvertTo-SecureString -AsPlainText "Pa55w.rd" -
    Force) -enable $True
    ```

Create Groups Using PowerShell

18. Enter the following to create the groups for the Wantirna domain.

    a. **New-ADGroup -name G_FinanceWtn -GroupCategory Security -GroupScope Global -path "ou=Finance,dc=Wtnr,dc=sWin,dc=local"**

    b. **New-ADGroup -name G_AccPay -GroupCategory Security -GroupScope Global -path "ou=Finance,dc=Wtnr,dc=sWin,dc=local"**

19. Use the following to set the membership and nesting of the Wantirna groups:

    a. **Add-ADGroupMember G_AccPay Kim**

    b. **Add-ADGroupMember G_FinanceWtn G_AccPay**

Join sWin10PC203 to the New Domain

By default, new computer accounts are created in the Computer container in AD. If we want a Computer Account to be created in a specific OU we can just right click on that OU and select New, Computer…

But this does not help when an Administrator joins from a computer without an account to the domain. To change the default location for Computer Accounts we need to use **redircmp**.

20. On **sWin22SVR3**, in **PowerShell** type the following:

    redircmp "ou=Finance,dc=Wtnr,dc=sWin,dc=local"

We will now join **sWin10PC203** to the Wantrina domain.

21. On **sWin10PC203**, test whether DNS is working by successfully pinging the new child domain **Wtnr.sWin.local**

    If successful, join **sWin10PC203** to the **Wtnr.sWin.local** domain, as covered in Lab 6, section "Joining a Domain" (i.e. System Info > Change settings).

    a. Use the credentials **Wtnr\Administrator** and the password **Pa55w.rd**. (Skip the *Add an account* prompt)

    b. After **sWin10PC203** has rebooted, verify that its Computer account is appearing in the **Finance** OU in the Wantirna domain.

Nesting the Groups in the Forest

Note: *We have already completed the nesting for the Wantirna domain using PowerShell.*

Nesting Within the Hawthorn Domain

22. On **sWin22DC1**, in **Active Directory Users and Computers**, in the **Finance** OU, nest the groups according to the Group Strategy in Figure 5.
    Hint: *You can double-click a group name from within the member/member-of properties will load the properties of the next group.*

    In summary:

    a. **Doug Pirahna** is a member of **G_AccPay**.
    G_AccPay is a member of **G_FinanceHwn**.
    G_FinanceHwn is a member of **U_FinanceDept**.
    U_FinanceDept is a member of **DL_CustAccData_R**.
    Assign **DL_CustAccData_R** the permissions,
    Read and **List folder contents** to the **CustAccountData** folder.

    b. **Luigi Vercotti** is a member of **G_AccRec**.
    G_AccRec is a member of **G_FinanceHwn**.
    G_FinanceHwn is a member of **U_FinanceDept**.
    G_AccRec is a member of **DL_CustAccData_M**.
    Assign **DL_CustAccData_M** the permissions,
    Modify to the **CustAccountData** folder.

    c. **U_FinanceDept** is a member of **DL_PolicyDocs_R**
    DL_PolicyDocs_R the permissions,
    Read and **List folder contents** to the **PolicyDocs** folder.

Nesting Groups between Domains

23. Staying on **sWin22DC1** in **Active Directory Users and Computers**, double-click on **U_FinanceDept**, and click on the **Members** tab. Then click the **Add...** button.

24. On the **Select Users, Contacts...** dialog box, click the **Locations...** button.
    Expand the **sWin.local** domain, and scroll down and select the **Wtnr.sWin.local**, and click **OK**.

25. In the **Enter the object names…** field type ***G_***, and then click the **Check Names** button. Notice that all of the Wantirna groups are listed. Select the **G_FinanceWtn**, and click **OK**.

Testing the Access Permissions

> *Work around – If you get an error stating Kim cannot log in remotely do one of the followings:*
> 1. *Log on to sWin10PC203 as Wtnr\Administrator, or*
> 2. *On sWin22SVR3 make the Everyone group a member of the Remote Desktop Users group.*

26. On **sWin10PC203** log on as **Kim**. From Windows File Explorer (), enter the UNC for **sWin22DC1** and press enter, i.e.

    `\\sWin22DC1.sWin.local\CustAccountData`

27. Kim is a member of the G_AccPay team. She should only have read access. Verify that this is the case.
28. On **sWin10CL101**, log on as **Luigi Vercotti**. Connect over the network to the **CustAccountData** folder. Verify that you can save changes and create new files.

> *Before you change the memberships of any groups, remember that a Group's SID must appear in the Access token of the user. If you change group membership after a user has logged on, the new group's SID will not yet appear in the users Access token. In other words you must log the user off, then log back on in order to generate a new Access token.*

Extension *(Optional)*

Create two more DL groups for CustAccountData. One to have Full Control permissions and the other to have Deny Write permission.

Add the U_FinanceDept as a member of the new Full Control DL.
What are the differences? *(once you have generated a new Access token :)*
Add the U_FinanceDept as a member of the new Deny Write DL.

What are the differences?

See if you can explain your observations using the theory covered in the lecture (i.e. cumulate NTFS..., cumulate Share..., most restrictive applies)

Pack up

1. Shut down all guest VMs.
2. **Sign out** from the Host virtual machine and make sure that it is **Stopped** otherwise it will run in the background and use up your quota.
3. If on campus, **log off from the ATC626 lab PC,** and push your chair in as you leave.

End of Lab

TNE10005/TNE60002

Network Administration

Lab 8

Configuring

Group Policies

in a

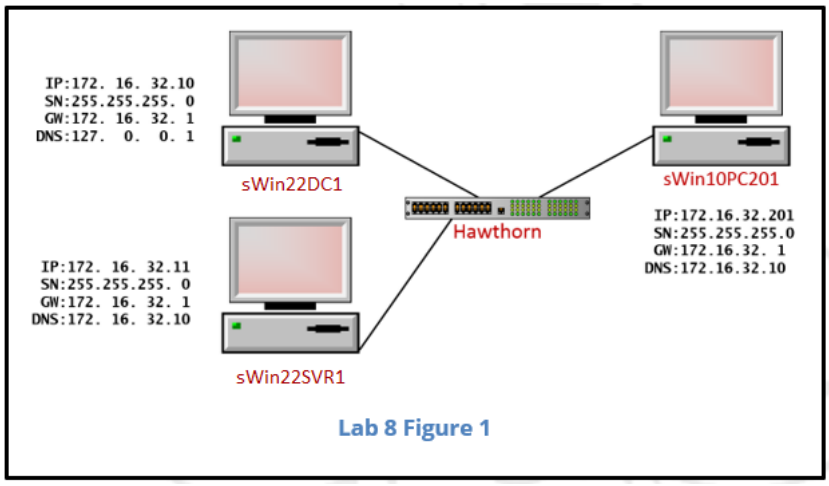
Windows Server 2022 Domain

SWINBURNE UNIVERSITY OF TECHNOLOGY

Aim

The aim of this lab is to understand how to configure and deploy Group Policies

Topology



Lab 8 Figure 1

Preliminary settings

1. Revert the virtual machines (VMs) **sWin22DC1**, **sWin22SVR1** and **sWin10PC201.** Check the Hyper-V settings and ensure the three VMs have their **Network Adapter** configured for the **Hawthorn** virtual switch.
2. Launch **sWin22DC1**, when it displays the logon screen, launch **sWin22SVR1** and **sWin10PC201**.
3. Log on to **sWin22DC1** as **Administrator.** Ensure that **sWin22DC1** configured with the IPv4 address **172.16.32.10/24**.
4. Ensure that the **DNS address for sWin10PC201** contain the sWin22DC1's IPv4 address.
5. Join **sWin10PC201** to the **sWin.Local** domain.

6. At **sWin22DC1**, create at least three user accounts and at least two global groups: **G_ICTProcurement** and **G_ICTSupport** (create more if you want).

   Of the three users, assign one user account to be a member of both global groups. Assign the remaining user accounts so that they are members of only one group and that both groups has more than one member.

Local Policies

Hardening a desktop

7. Log on to **sWin10PC201** as **Administrator**.
8. Click the **Win** key to bring up the **Start screen.** At the **Start screen**, start typing **gpedit.msc,** then select the **gpedit.msc (Microsoft Common Console Document)** to load the **Local Group Policy**.
9. First we will **turn off autoplay** so that when a user inserts a CD or USB device, it will not automatically load the autorun script.

   In the **Computer Configuration** section, expand the **Administrative Templates** container, then expand the **Windows Components** container.

10. Double-click the **Autoplay Policies** container, and double-click the **Turn off Autoplay** policy. Click on the **Enabled** option button and enter a comment along the line of "Policy set by <name> to prevent malware being copied by autorun scripts".

    Set the **Turn of Autoplay on:** setting to **All drives**. Click **OK.**

11. Double-click on **Set the default behavior for Autorun**, click the **Enabled** option button, enter a relevant comment and set the **Default Autorun Behavior** option to **Do not execute any autorun commands.** Click **OK**.

Prohibiting access to the Control Panel

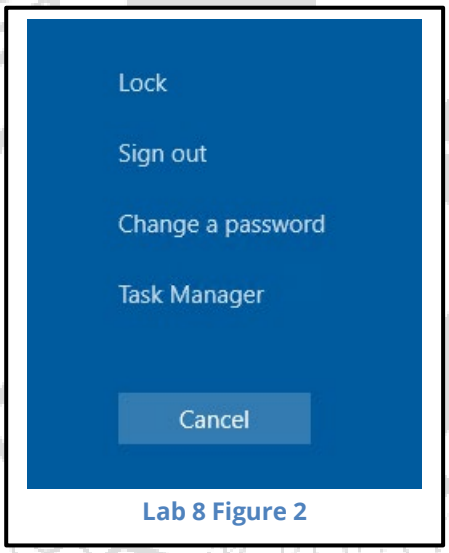
If the workstation we are configuring is planned to be used for a single purpose (e.g. library catalogue), then it is desirable to restrict users from having access to the control panel.

12. Verify that you can access the control panel. To do so, at the **Start screen**, type **Control panel,** then select it to run. Once verified, close the Control panel.
13. Back in gpedit, in the **User Configuration,** expand the **Administrative templates**, then click on the **Control Panel** container.
14. Double-click on **Prohibit access to the Control Panel and PC settings**, and entering in a descriptive comment, click the **Enabled** option button, then **OK**.
15. At the **Start screen,** start typing **Control Panel** and observe whether it still appears in the **Best match** list.

    If it does, launch it. Were you successful? _____

Ctrl+Alt+Del Options

When we press the Ctrl+Alt+Del (or **Ctrl+Alt+End** in the guest machine) options we are given the following options:



Lab 8 Figure 2

If the workstation we are configuring is to be used for a single purpose by many people you may want to remove some of these options. For example, the **Lock this computer** option is frustrating for other users as they are unable to use the PC while locked.

We will now remove this option:

16. Verify that you have this option by pressing Ctrl+Alt+Del (Ctrl+Alt+End in a guest machine). Once you have verified the option, press **Cancel**.
17. In the **Local Group Policy Editor** console, find in the **User Configuration, Administrative Templates, System, Ctrl+Alt+Del options** container, the **Remove Lock Computer** option.

    Double-click on the option, and **Enable** this setting, entering a descriptive comment. Click **OK.**

    Test to see if your settings have been applied by pressing Ctrl+Alt+Del (Ctrl+Alt+End in a guest machine).
18. Repeat the steps for the **Remove Task Manager** option. Verify that it is working.

Creating an Organisational Unit Structure

19. Switch back to **sWin22DC1**, in **Active Directory Users and Computers**, create an OU called **ICT**.
    (see Lab6, p.9, step 34 if you cannot remember how to create an OU).
20. Within the **ICT** OU create two child OUs **ICTSupport** and **ICTProcurement**.
21. Move one of the user accounts created in step 6 into the **ICTSupport** OU, move another into the **ICTProcurement** OU. Move any remaining user accounts along with the groups created in step 6 into the **ICT** OU. This can be achieved by clicking on the account and dragging it to the OU.

Delegating Control of an OU

We want a user from the ICT Support team to take over the management of the user account passwords and groups in the ICTSupport OU.

22. Right click on the **ICTSupport** OU.
23. Select **Delegate Control…** to start the wizard. Add the user account that you copied into the **ICTSupport** child OU.
24. Delegate the following tasks:
    a. Reset user passwords and force password change and next logon
    b. Create, delete and manage groups
    c. Modify the membership of a group
    d. Finish the wizard.

We have now given this user the rights required to do much of the day-to-day management of the user accounts in this OU. Consequently, we have delegated some of the urgent, but relatively unimportant tasks that can distract us from some of the longer term, but important tasks.

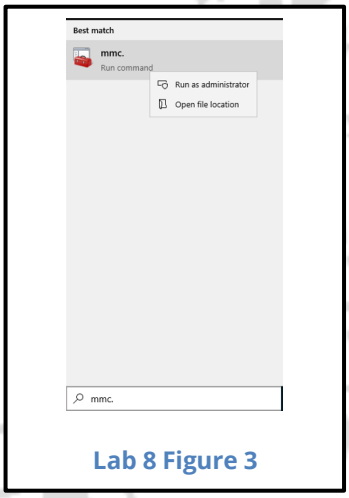
Creating a Custom Console

Now that we have delegated some of the day-to-day responsibilities, we also need to provide the users we have delegated access to the **Active Directory Users and Computers** console. The problem with this is it provides information to these users on the structure of our network. Information that may be useful to potential hackers.
It is safer to create a new console for these users with delegated permissions so that they only see the objects (OUs, accounts, etc).

We can do this by creating a **Custom Console.**

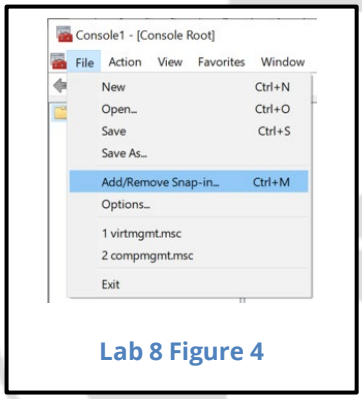
25. On the tool bar at the bottom left of the window, next to the the **Win** key , in the ***Type here to search*** box, type **mmc.**

    Click **Run as administrator** to launch the **MMC** (Microsoft Management Console) with the administrative privilege.



Lab 8 Figure 3

In the **Console1 – [Console Root]** window, click **File** then select **Add/Remove Snap-in….**



Lab 8 Figure 4

Select **Active Directory Users and Computers** snap-in, then click **Add>** and click **OK.**

26. Expand the sWin.local domain and get to the **ICTSupport** OU.

27. Right click on the **ICTSupport** OU and select **New Window from Here**.

    We have now created a custom console for this OU. We have one more thing to do though. We still have the initial console window that has the domain root, and all of the details we wanted to hide from our delegated user.

28. Click on the **Window** menu and select the **Console Root\ …** window. Now, without closing the whole console, close this window (i.e. click on the inner/lower window. Now, without closing window).

29. We should now only have the ICTSupport OU window in the console.
    Save the console as **ICTSupportConsole**.

Creating a Group Policy Objects

Order of application

Before we start creating different GPOs, let's undertake an exercise that will demonstrate the order in which GPOs are applied.

Many GPO settings are like light switches, if configured they can only be on or off. Like a light switch, if a person walks into a room and turns the light on, then the next person comes in and turns the light off, and the next person turns it on when they come in, it is always the last person that flicked the switch that determines whether the light is off or on.

The same is true with GPOs. While an administrator has some tricks up their sleeve to override this, the general rule is that when GPOs conflict over a setting, the last GPO applied will determine the setting.

Let's see this in action.

Remember we configured the Local Group Policy on sWin10PC201 so that the Remove Lock Computer option was enabled. We will now create a GPO that will conflict with this Local Group Policy setting.On **sWin10PC201**, sign out. Then log on as a domain user whose user account is located in the **ICTProcurement** OU.Notes: Ensure to put **sWin** in front of the logon name to tell the computer that the account is from the swin domain. This is useful to know when you have a local account and a domain account with the same logon name**).**

> If you could not log on and receive a message "*To sign in remotely, you need the right to sign in through Remote Desktop Services……*", on the VM (i.e. sWin10PC201), click on the **View** menu, then deselect **Enhanced session**.

Verify that the **Task Manager** option does not appear when we press **Ctrl+Alt+Del** key combination.

30. On **sWin22DC1** run **gpmc.msc** (or select **Group Policy Management** from the **Tools** menu in **Server Manager**).

    Expand the **Domains** container and expand **sWin.local** until you see **Group Policy Objects.**

31. Right click on **Group Policy Objects** and select **New**.

    Enter the name **Enable Task Manager** as the name of the new GPO.

32. Right click on this new GPO and select **Edit…** This will launch the GPO in gpedit.

33. Expand User Configuration > Policies > Administrative Templates > System, down to the **Ctrl+Alt+Del options** and in the **Remove Task Manager** properties, click on the **Disabled** option button.

    Notice that we now have a double negative. We have disabled the removing of the task manager. This means that the task manager should be available.
    Predict what the result of this GPO will now be:

    _____

    On sWin10PC201 verify if your prediction was correct. Was it? _____

    We have three points that need to be considered here:

    - GPO's must be linked to a container before they will be applied
    - Objects must reside in that container if the GPO is going to apply to them.
    - GPOs must propagate to other PCs before they can come into effect.

By default GPOs are reapplied every 5 minutes in a domain controller, and 90 ± 30 minutes to other computers in the domain. So a change in a GPO may take up to 120 minutes (i.e. 2 hours) before we will see it in effect on some workstations.

GPUpdate

Every time a computer reboots the computer configuration settings of all of the GPOs that are linked to container that the computer's account resides in are applied. Similarly when a user logs on to the domain the user configuration settings of all the GPOs that are linked…etc, are applied.

Another tool that allows an administrator to reapply GPOs is **GPUpdate.**

Typed in at the start menu or command line **gpupdate** will refresh all of the settings that have changed since the last application of GPOs.

We can modify **gpupdate** by using the following switches:

`gpupdate /force` - Will apply all GPO settings both user and computer configurations whether they have changed or not.

`gpupdate /target:user` - Will apply all of the user configuration settings, the word user can be substituted with computer to apply all ofthe computer configuration settings.

`gpupdate /boot` – Will cause the PC to reboot after the GPO has been applied

Every time you change a GPO setting, you should type **gpupdate** on both the domain controller and the workstation you are testing on.

Linking GPOs to Containers

Link the new GPO to the domain, type gpupdate on both **sWin22DC1** and **sWin10PC201**.

34. In the **Group Policy Management** windows right click on the **sWin.local** domain and select **Link an Existing GPO…** Select the **Enable Task Manager** GPO and click **OK**.
35. Run **gpupdate /force** on both **sWin22DC1** and **sWin10PC201**.

36. View your Ctrl+Alt+Del options on **sWin10PC201**

    What is the setting? _____

    Which GPO is applied? _____

37. Back on **sWin22DC1**, create a GPO called **Remove Task Manager** and link it to the **ICTSupport** OU. This time, remembering the double negative, set the **Remove Task Manager** setting to **Enabled**.

    Run **gpupdate /force** on both guest machines.

    Record the result of this change to sWin10PC201:

    _____

38. Now log on to **sWin10PC201** as the user account from **ICTSupport**. Explain any differences:

    _____

    _____

    _____

This exercise illustrates the following points.

- GPOs only apply to objects in the containers to which the GPOs are linked
- GPOs are applied in an order. When settings conflict, if the administrator has not overridden then, the setting in the last GPO applied will be configured.

Remember that the order in which GPOs are applied are:

a. Local Computer Policy
b. Site
c. Domain
d. OU
e. Child OUs (recursively

More GPO Settings

We will now learn about some other GPO settings. In each instance we will be creating a new GPO and linking it to the **ICT** OU.

Preventing Software Running Policies

There are a number of ways we can restrict users from running specific software. In this lab we will use the **Don't run specified Windows Applications** policy, but there are also Software Restriction Policies and AppLocker.

39. On **sWin22SVR1**, log in as one of the user account created in step 6, and run **calc.exe** (**Desktop app)** to ensure that you can run it.
40. On **sWin22DC1** in **GPMC** create and link a GPO called **RestrictRunningOfCalc** to **sWin.Local** domain.
41. Edit the GPO and browse to
    User Configuration\Policies\Administrative Templates\System.
42. Prevent users from running **calc.exe** by configuring the **Don't run specified Windows** applications policy setting.

> ***Note:***
> This policy setting only prevents users from running programs that are started by the **File Explorer process**. It does not prevent users from running programs, such as Task Manager, which are started by the system process or by other processes. Also, if users have access to the command prompt (Cmd.exe), this policy setting does not prevent them from starting programs in the command window even though they would be prevented from doing so using File Explorer.

43. Attempt to run **calc.exe** again (i.e. browse to C:\Windows\System32\calc.exe in File Explorer), it should not run.

> **Note:**
> The following settings can also be used to restrict the running of software:
>
> - **Software Restriction Policies** (*User configuration, Policies, Windows Settings, Security Settings.* Right-click *Software Restriction Policies* and choose *New Software Restriction Policies*).
> - **AppLocker** (*Computer Configuration\Policies\Windows Settings\Security Settings\Application Control Policies\AppLocker*). Applocker has three major steps to be configured. Advantages of Applocker is that you can easily restrict all versions of a piece of software, or all software from a specific company. You can also run Applocker in Audit mode, which will let you track who is using the software.

Linking Multiple GPOs

We have seen throughout this lab that we can link multiple GPOs to the one container. The question that now arises is 'what if two GPOs linked to the same container conflict in a setting?'
Let's see if we can observe what happens.

Changing Priority of GPOs

44. Using GPMC, link to the **ICTProcurement** OU, first the **Remove Task Manager** GPO created in step 37 and then the **Enable Task Manager** GPO created in step 31.
45. On **sWin10PC201**, log in as the user account located in the **ICTProcurement** OU

    Which GPO is being applied? _____

46. Back in **GPMC** at the **ICTProcurement** OU, observe the link order of the **Remove Task Manager** and **Enable Task Manger** GPOs.

    Change the order of the GPOs so that **Enable Task Manager** is at position **1**.

    Do this by selecting the **Enable Task Manager** GPO and clicking on the parrow.

47. Test **sWin10PC201**, which GPO setting has been applied? _____

Filtering GPOs

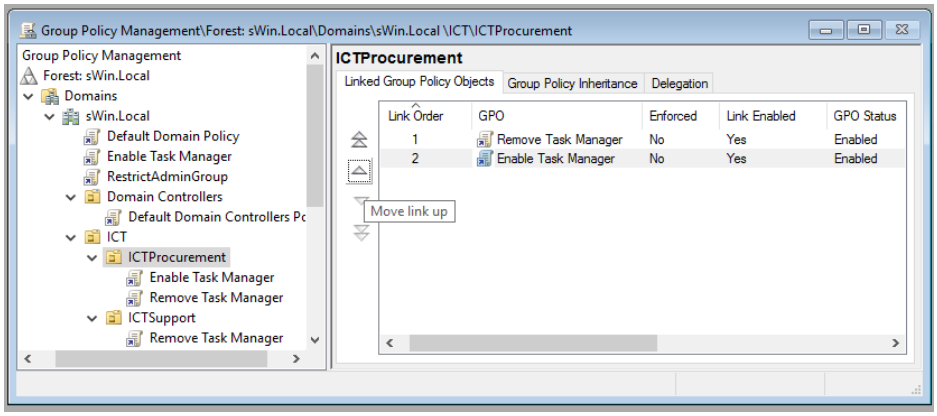
The term Group Policy Object refers to the fact that each is a collection or group of policies that can be linked to a container. The computer and user objects in those containers are configured with the settings in the respective computer configuration and user configuration policy settings.

You cannot link a GPO to a group, only to a Local Computer Policy, Site, Domain and OU.

Consequently students beginning in network administration can be confused.

While we cannot link a GPO to a group, we can change the permission of a GPO so that it is only applied to targeted groups. This is called Filtering.

There are three approaches to filtering: GPMC, GPO Security and WMI filtering.



Lab 8 Figure 5

WMI filtering is the most powerful and most complex. For example we can write a script that will check to see how much disk space is free before proceeding with software deployment, or it can check to see if a patch was previously installed prior to applying a policy. How to configure WMI filtering is beyond the scope of this unit. Students only need to know what WMI filtering is.

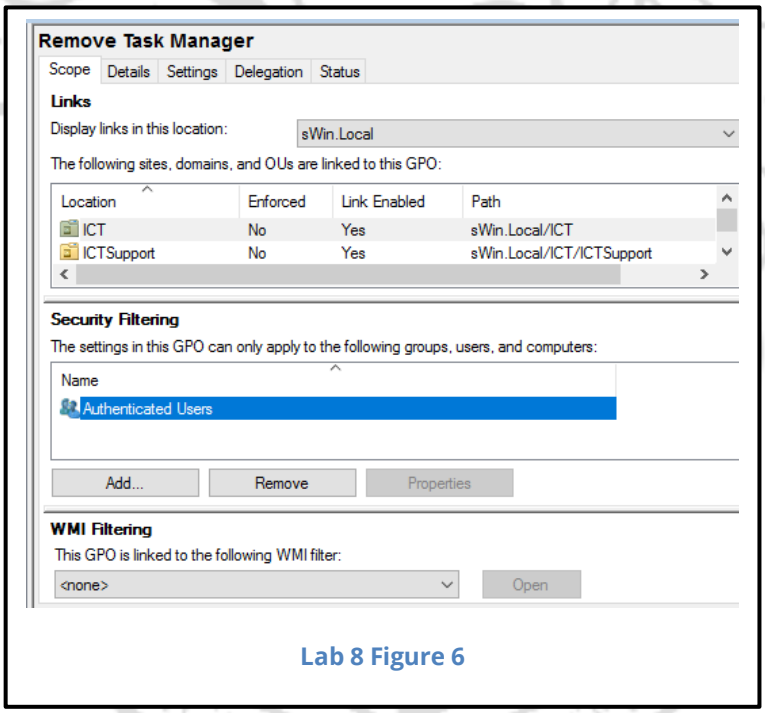
GPMC Filtering

48. In *GPMC delete* the link between the **ICTProcurement** OU and the **Enable Task Manager** GPO.

    Link the **Remove Task Manager** GPO to the **ICT** OU

49. In the **Group Policy Objects** container, click on the **Remove Task Manager** GPO.

    In the **Security Filtering** settings, notice that it currently has the **Authenticated Users** group configured.



Lab 8 Figure 6

Click **Remove**, then **Add...** the **G_ICTProcurement** group.

When filtering a GPO, you must ensure that the targeted accounts have read permissions.

Ensure that your GPO has **Allow Read** permissions assigned.

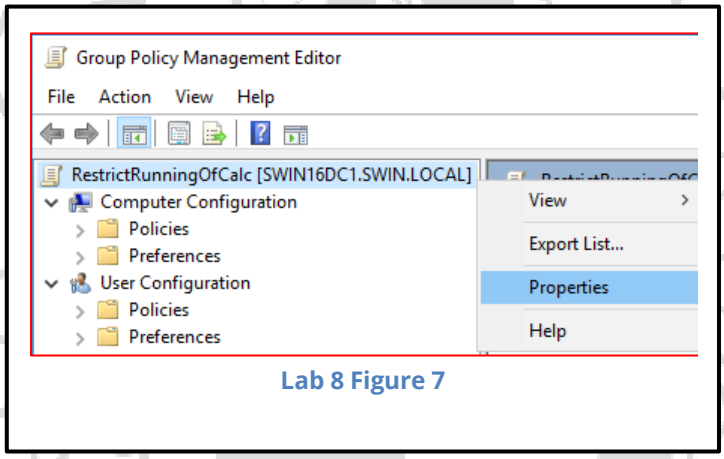
Now the **Remove Task Manager** GPO will only be applied to members of the **G_ICTProcurement** group.

You will also need to modify the read permissions of the GPO, which we will do in the next step.

Filtering with GPO Security

50. In GPMC right click on the **Restrict Running of Calc** GPO and select **Edit…**

At the top left of the GPO right click on the GPO name and select **Properties.**

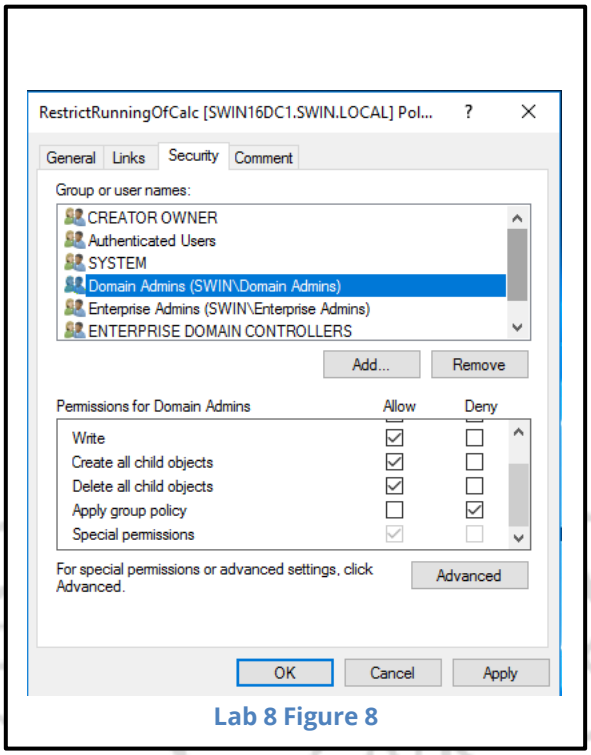


Lab 8 Figure 7

51. A familiar properties dialog will appear. Click on the **Security** tab and then click on the **Domain Admins** group.

In the Permissions for **Domain Admins**, scroll down until you can see the permission **Apply group policy**.

Place a tick in the **Deny** column for the **Apply group policy** permission.



Lab 8 Figure 8

This will mean that this GPO will apply to everyone except those in the Administrators group.

Please keep in mind that we sparingly use deny permissions.

52. On **sWin22SVR1**, log off and log on again as the **Administrator** and see if you can now run the calculator.

Modelling GPOs

Modelling is a fantastic tool for troubleshooting GPOs. In the lecture I spoke about how with Windows 2000 we used to have to unlink, update, and then test to see which GPO was causing problems for a PC or user. It took such a long time.

Group Policy Modelling is a wizard that will allow you to select a container, a user or a computer. It will then apply all of the group policies that apply and generate a report that tells you which GPO is causing what setting.

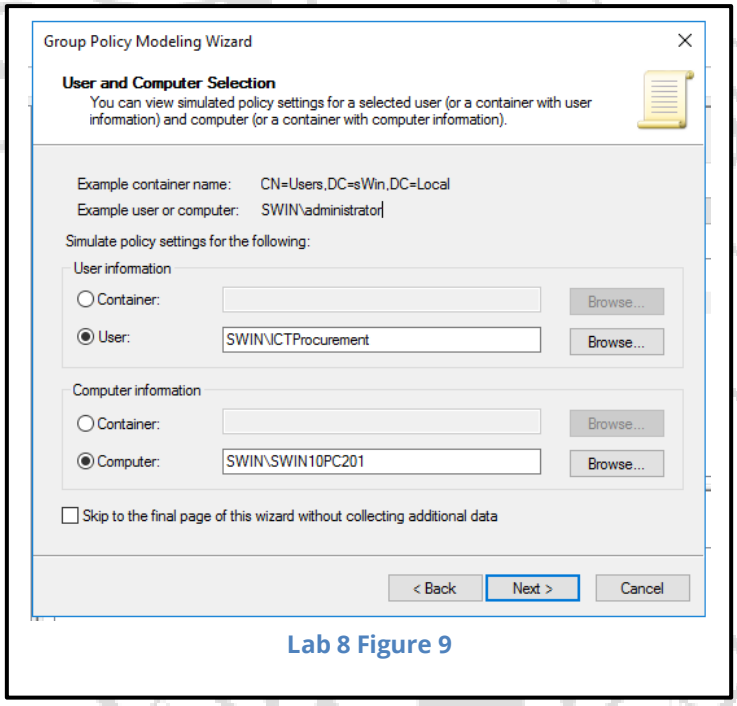
For example, you are an administrator and you need access to the task manager, but the

computer you are on won't run the task manager. You can run the modelling with your account and the computer you were working on and drill through the report to find what GPO is causing it to be hidden.

This makes it much easier to correct errors in our GPOs.

You can also use **rsop.msc** and **gpresults** to troubleshoot GPOs. Like WMI filters, we don't need to know how to use rsop.msc in this unit, we only need to know that it can be used for troubleshooting GPOs.

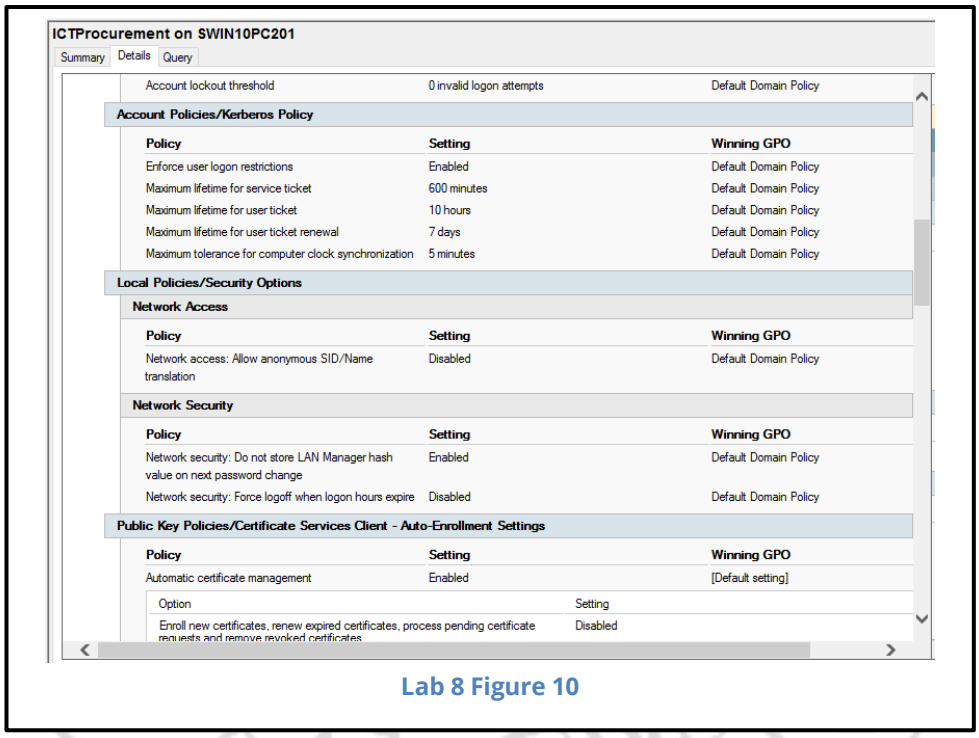
53. In GPMC near the bottom of the left hand pane, right click on Group Policy Modeling and start the Wizard.
54. As we are modelling GPOs applied to this domain, select the defaults for the Domain Controller Selection.
55. In the User and Computer Selection step, enter the **ICTProcurement** user and the **sWin10PC201** computer.



Lab 8 Figure 9

Tick the **Skip to the final page...** check box and click **Next**.

56. Ignore any warnings about not trusting this page (after all Microsoft generated it). On the report, click on the **Details** tab to see what GPOs are being applied.



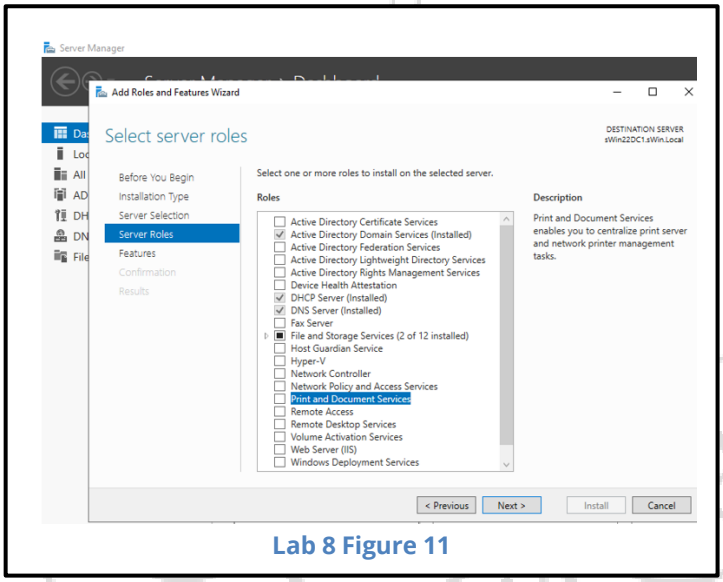
Lab 8 Figure 10

Deploying Printers with GPOs

57. In GPMC Create a new GPO called **IctPrinterDeploy** and link it to the **ICT** OU.

Create a new Printer

58. First, let add the Print Services by adding the **Print and Document Services** Server Roles.



Lab 8 Figure 11

After Server Roles is added. In **Server Manager**, under the **Tools** menu, click to launch the **Printer Management** console.

59. Expand **Print Servers**, then expand **sWin22DC1 (local)**. Right click **Printers** and select **Add Printer…** The Network Printer Installation Wizard will then start:

a. On the **Printer Installation** page, select **Add a new printer using an existing port:** For this lab we will use the port **LPT1**, but normally the printer will have a network card installed and have its own IP address. Click **Next**.

b. On the **Printer Driver** page, select **Install a new driver**, and click **Next**.

c. On the **Printer Installation** page, select the **MS Publisher Color Printer**, and click **Next**.

d. On the **Printer Name and Sharing Settings** page, name the printer **ICT_Printer**, and share it as **ICT_Printer**. Click next, and on the **Printer Found** page, click **Next** again.

e. When the driver and printer have successfully installed, click **Finish.**

Set Permissions on the Printer

This step is not essential for deploying a printer, but if you don't want to have to be the person looking after all printer problems, you will need to ensure that someone has sufficient permissions to manage the printer.

60. Right click the printer **ICT_Printer** and select **Properties**, then the **Security** tab. In the same way as you would allocate NTFS permissions, give the group **G_ICTSupport** both the **Manage this printer** and **Manage documents** permissions. Click **OK** until you are back at **Print Management**.

Deploying the Printer Using GPOs

61. Back in **Print Management** right click **ICT_Printer** and select **Deploy with Group Policy…**

62. Next to the field **GPO name:** click the **Browse** button. Find the **IctPrinterDeploy** GPO, and click **OK**.

63. We will deploy this printers to the Users in the ICT OU, but if this GPO was linked to an OU that had computer accounts in it we would want to deploy the printer to computers

    a. Select the Checkbox **The users that this GPO applies to (per user)**, and click **Add**.

    b. Verify that the UNC for the printer appears in the **Printer Name** column, and click **OK**.

    c. You will get a message telling the operation succeeded. Click **OK**.

Test Deployment

64. Log on to **sWin22SVR1** as one of the users created above (if you are already logged in, execute a **gpupdate /force**) and verify that the printer has been deployed (Settings, Devices, Printers & Scanners)

Extension

Managing GPOs

Explore how you can use GPMC to backup and restore your GPOs

Find out how to use rsop.msc or the command line tool gpresult to troubleshoot GPOs.

Reminder

Record the concepts, design strategies, techniques, configurations and commands that you learn in this week laboratory class.

Pack up

1. Shut down all guest VMs.
2. **Sign out** from the Host virtual machine and make sure that it is **Stopped** otherwise it will run in the background and use up your quota.
3. If on campus, **log off from the ATC626 lab PC,** and push your chair in as you leave.

End of Lab

TNE10005/TNE60002

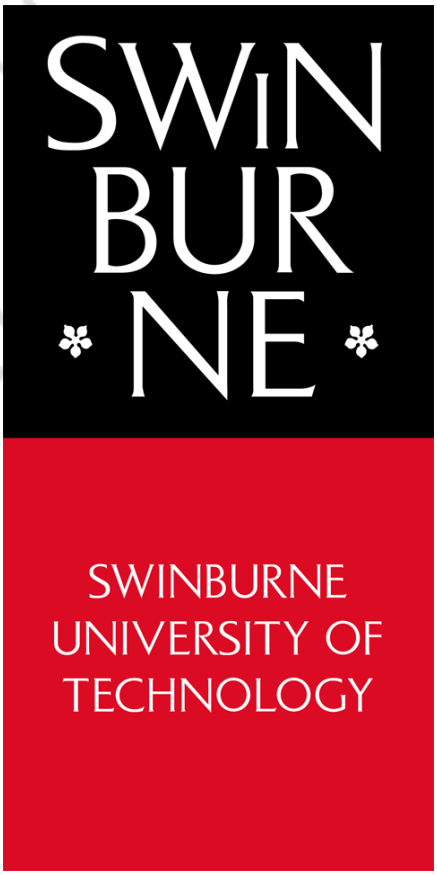
Network Administration

Lab 9

Managing Security

in

Active Directory



Aims:

To improve the baseline security of a Windows Server 2022 Domain.

Virtual Machines

sWin22DC1, sWin10CL101

Preliminary settings

1. Check the Hyper-V **settings** for **sWin10CL101**. Ensure the **Network Adapter** is configured for the **Hawthorn** virtual switch.
2. Launch **sWin22DC1**, and log on to **sWin22DC1** as **Administrator.**
3. Do not launch **sWin10CL101** until being instructed.
4. On **sWin22DC1** create an OU called **ICT**.
5. On **sWin22DC1**, in the **ICT** OU create:
    A. Two user accounts **IPuser**, **ISuser**.
    B. Two global groups: **G_ICTProcurement** and **G_ICTSupport.**
    C. Two **Domain Local** groups **DL_Data_FC** and **DL_Data_R**.
    D. Nest :

    Add remote desktop user for users as well

    - IPuser > G_ICTProcurement > DL_Data_R
    - ISuser > G_ICTSupport > DL_Data_FC
6. On **sWin22DC1** create a shared folder called **Data**. Allocate the **Share** permissions to **Everyone = Full Control.** Give the DL groups the NTFS permissions as described by their names.
7. Create a File called **TopSecret.txt** and add some data into it.

Security settings

8. On sWin22DC1, use **Group Policy Management** to edit the **Default Domain Controllers Policy.**

9. Configure the following settings in **Computer Configuration, Policies, Windows Settings, Security Settings**:

    A. **Account Policies, Password Policy**:

    - **Enforce password history** to **12** passwords remembered
    - **Minimum password age** to **1** day. When prompted accept the default for the Maximum password age (30 days).
    - **Minimum password length** to **8** characters
    - **Password must meet complexity requirements** to **enabled**

    B. **Account Policies, Account Lockout Policy**:

    - **Account lockout threshold** to **3** invalid logon attempts
      (Accept the default 30 minutes for other policies)

10. Create a GPO called **Lab9SecSettings** and link it to the **ICT** OU.

    A. **Local Policies, User Rights Assignment:**

    - **Allow log on locally**, add the **G_ICTSupport** and **Administrators** groups
    - **Deny log on locally**, add the **G_ICTProcurement** groups

11. Test some of these settings on **sWin10CL101**.

    A. Use **gpupdate /force** on the domain controller.

    B. Launch **sWin10CL101** virtual machine. Sign in as **swin\administrator**, then sign out.

    Predict whether the user can successfully log on **sWin10CL101** as **swin\IPuser**?

    _____

    C. Log on as **swin\IPuser**

    Is your prediction correct? _____

    If your prediction was not correct discuss it with a fellow student.

We will now try to understand the observation by seeing which settings have applied to sWin10CL101 by using **gpresult**.

> ***Note:***
> *You may remember from the lecture we learned about having at least two user accounts for every administrator. An unprivileged account for logging on, and a privileged account that administrators use when they need to run an application with elevated privileges. We will be using **Run as** in the next section. This is how you run an app with elevated privileges.*

12. On **sWin10CL101**, launch an elevated command line console, by clicking **Start**, type ***cmd***, but do **not** press enter!

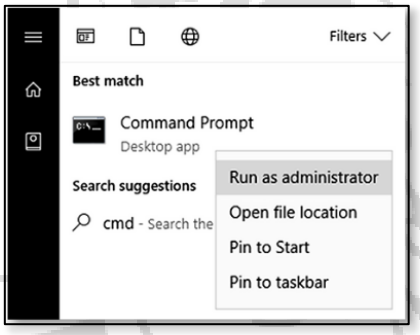


Figure 1 - Run as

- Right click the **Command Prompt** desktop app, and select **Run as administrator**.
- Enter the credentials **sWin\Administrator** with the default password.

13. At the command prompt, change to the IPuser's home folder by typing:
    cd c:\users\IPuser.
    At the command prompt type the following to generate a report on which GPO settings have been applied:
    ***gpresult /user* IPuser *\h* CL101GpoSettings.htm**, and press **Enter**.

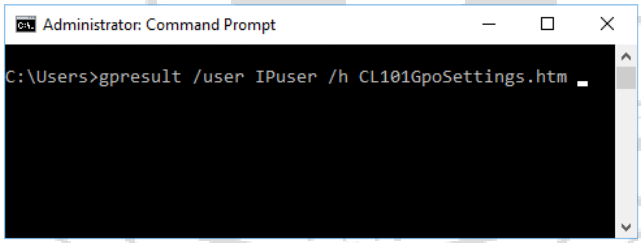


Figure 2 - GPresult

14. Using **File Explorer** browse to **C:\Users\IPuser** and double-click **CL101GpoSettings.htm**

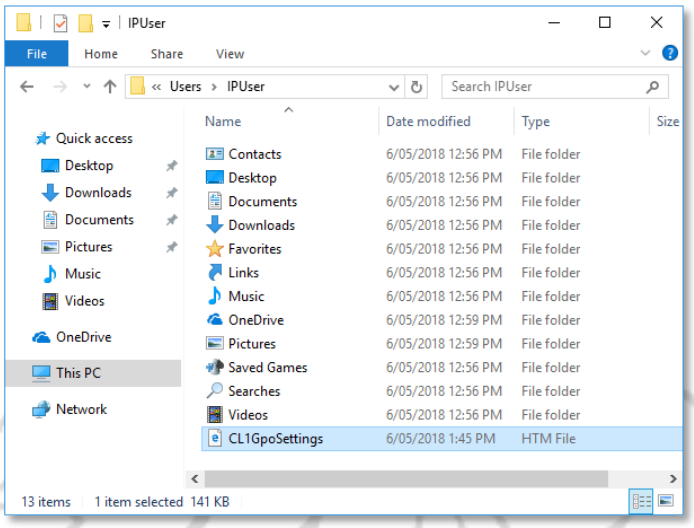


Figure 3 - GPresult Report Location

15. When the report loads, scroll down until you find the **Applied GPOs** section. Was the **Lab9SecSettings** GPO applied?

    Explain your observations:

    _____

    _____

16. In **Active Directory Users and Computers**, move the **sWin10CL101** from the **Computers** container to the **ICT** OU.

    Restart **sWin10CL101**, and log in as **IPuser**

    Were you successful?

    _____

    Explain your observation:

    _____

    _____

    Predict whether **ISuser** can log on, then log on to **sWin10CL101** as **ISuser**

    _____

17. From a command line run ***gpresult /h*** **CL101GpoSettings2.htm**

    Which of the following settings have changed? **Account Policies/Password Policy:** _____

    Local Policies/User Rights Assignment _____

    Try to explain your observation:

    _____

    _____

    _____

    _____

Restricting Groups

Restricting Groups is a very useful policy that allows the administrator to restrict membership of privileged groups such as the Administrators group.

If a hacker or a junior administrator adds a non-authorised user account to a privileged group, the next time the group policy is applied it all non-authorised accounts are removed.

18. At the **sWin.local** domain level, create and link a GPO called **RestrictAdminGroup**. When created, **Edit** the **Computer Configuration, Policies, Windows Settings, Security Settings, Restricted Groups** policy.
19. Right-click on the **Restricted Groups** container and select **Add Group...** Browse to **Administrators** group.
20. In the Administrators **Properties**, click the **Members of this group: Add** button and add the user account **ISuser**.
    Click **OK** until you are back at the Group Policy Management Editor.

21. In **Active Directory Users and Computers**, in the **Builtin** container, right-click on the **Administrators** group, click **Properties** and select the **Members** tab.

    Click on the **Add…** button and add the user account from the **G ICTProcurement** Group. Click **OK**.

    Click on the **Add…** button and add the user account from the **G ICTSupport** Group. Click **OK**.

22. Run **gpupdate /force**

    Go back to the **Members** tab of the **Administrators** group and verify that the user **ISuser** remains a member of the Administrators group, but the newly added user account **IPuser** has been removed.

Auditing

Auditing enables an administrator to keep a record of events such as: Who logs on to the network; who accesses important files. These records can be retrieved using the **event viewer** console.

23. On **sWin22DC1** in **GPMC** edit the **Default Domain Policy**.

    In **Computer Configuration**, **Policies**, **Windows Settings**, **Security Settings**, **Local Policies**, **Audit Policy**, configure the following settings:

    A. **Audit Account Logon Events** = Define these policy settings: Success & Failure
    B. **Audit Object Access** = Define these policy settings: Success & Failure

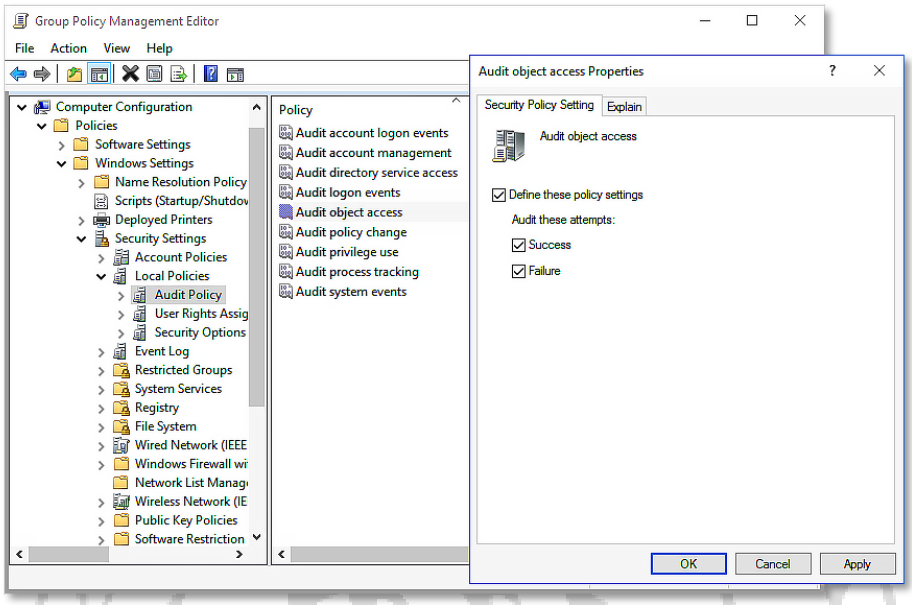


Figure 4 - Audit Object Access

24. Go to **C:\Data** and for **TopSecret.txt** go to the **advanced security security** settings and click on the **Auditing** tab.

25. Click **Add**, then click **Select a principal**, then enter **Authenticated Users**. In the **Type:** field select **All** (i.e. both success and failure). The click **OK** to close the Advanced Security settings, then **OK** again to close the **TopSecret** properties.

26. Restart **sWin10CL101**. Log in as **ISuser** and browse to **\\sWin22DC1\Data** and open up the **TopSecret** file, make some changes, and then save it.

> **Note**: *If you fail to log in as ISUser and get an error, first sign in as swin\Administrator and sign out, then sign in again as ISUser.*

27. On **sWin22DC1**, launch the **Event Viewer** app, expand **Windows Logs** and click on the **Security** log.

28. Look for the following event IDs:

    A. 4656 for object access events,

    B. 4624 for account logon events,

    C. 4634 for account logoff

    If you are struggling to locate the events you can **Filter Current Log...** for these event IDs, and/or you can **Find...** and enter in the user's logon name **ISuser**.

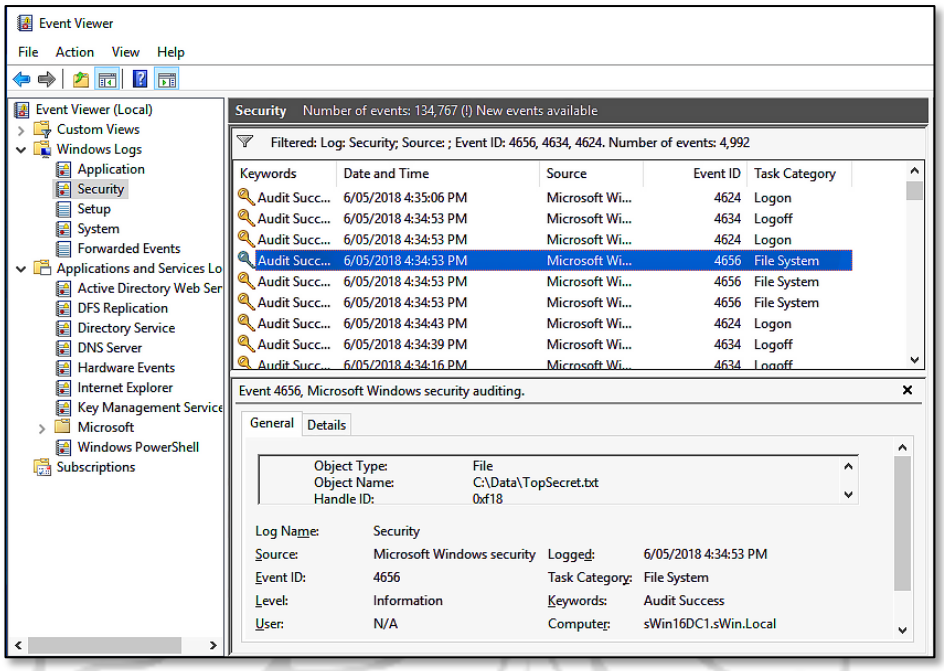


Figure 5 - Event Viewer: Audit Object Access

Using the Encrypted File System

EFS encrypts a file or a folder with a symmetric key, and then encrypts the symmetric key with an asymmetric key stored in a Windows certificate. This means that everyone's copy of the encryption key is both different and secure.

29. On **sWin10CL101**, ensure that the file **TopSecret.txt** is closed.

    A. Right click the file and select **Properties**.

    B. In the default **General** tab, click on the **Advanced...** button.

    C. In the **Advanced Attributes** dialog, check **Encrypt contents to secure data** and click **OK**.

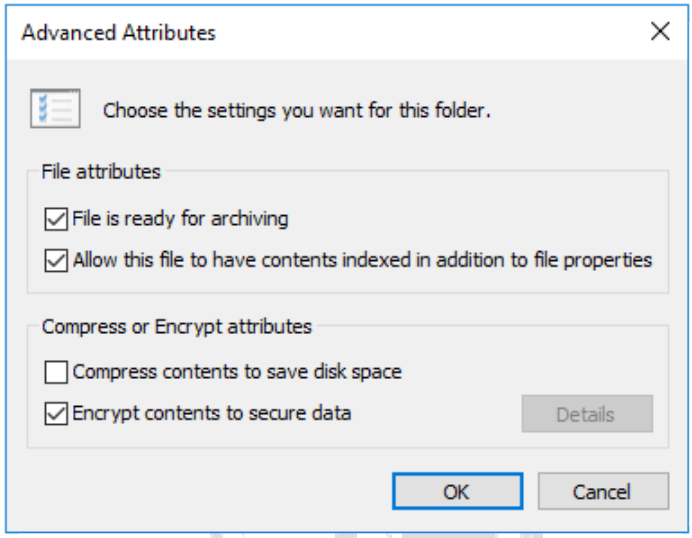


Figure 6 - Enable EFS

D. On the **TopSecret Properties** dialog, click **Apply**.

Now if you were to go back to Advanced… you would notice that the Details button is now active. If you wanted to add other user certificates, so they can access the encrypted file, you would do it here.

If you have time, log on to sWin10CL101 as IPuser, and see if you can open the encrypted file.

Hints:

You need to move the **sWIn10CL101** computer account back to the **Computers** container, so that the IPUser is not denied log in locally.

You also need to restart the sWin10CL101 o that GP settings can be reapplied to the computer.

*The remainder of this lab is **NOT** dependent on the preliminary OUs, User Accounts and Groups. If you run out of time you can practice these later. They can also be assessed in Part C of the Skills Exam.*

WSUS settings with GPO

Windows Server Update Services allow administrators to both streamline and control the updates that operating systems and applications require to remain secure.

A computer needs to be configured to download the updates from the WSUS server, and this can be done by using GPOs.

30. On **sWin22DC1** edit the **Default Domain Policy**.

    In **Computer Configuration, Policies, Administrative Templates, Windows Components, Windows Update** make the following changes:

    A. In **Specify intranet Microsoft update service location:**

    - **Enabled**
    - **Set the intranet update service…** = **http://172.16.32.1**
    - **Set the intranet statistics server** = **http://172.16.32.1**

    B. In **Configure Automatic Updates:**

    - **Enabled**
    - **Config. auto. updating:** = **4 – Auto download and schedule install**
    - **Scheduled install day:** = **Every day**
    - **Scheduled install time:** = **04:00**

    C. In **Enable client-side targeting:**

    - **Enabled**
    - **Target group name for this computer**: = **TestPCs**

GPO with Firewall

31. Create a new GPO called **Firewall-AllowPing** and link it to the domain.
32. Edit the GPO by going to and expanding **Computer Configuration, Policies, Windows Settings, Security Settings, Windows Defender Firewall with Advanced Security**

33. Keep expanding until you see **Inbound Rules**. Right click **Inbound Rules** and select **New Rule…** and configure the following as you work through the wizard:

    A. Rule Type = Custom

    B. Program = All programs

    C. Protocol and Ports = Protocol type: ICMPv4

    D. Scope = Any IP address

    E. Action = Allow the connection

    F. Profile = Domain, and Private (i.e. untick Public)

    G. Name

    - Name: = AllowPing
    - Description: = *Rule to temporarily allow pinging in the domain when troubleshooting. Technician: Kim. Job#1532*

Once this GPO has replicated to all computers in the domain you should be able to ping them all. However, once troubleshooting has completed, you should unlink this GPO to prevent ping scans being used in preparation for hacking.

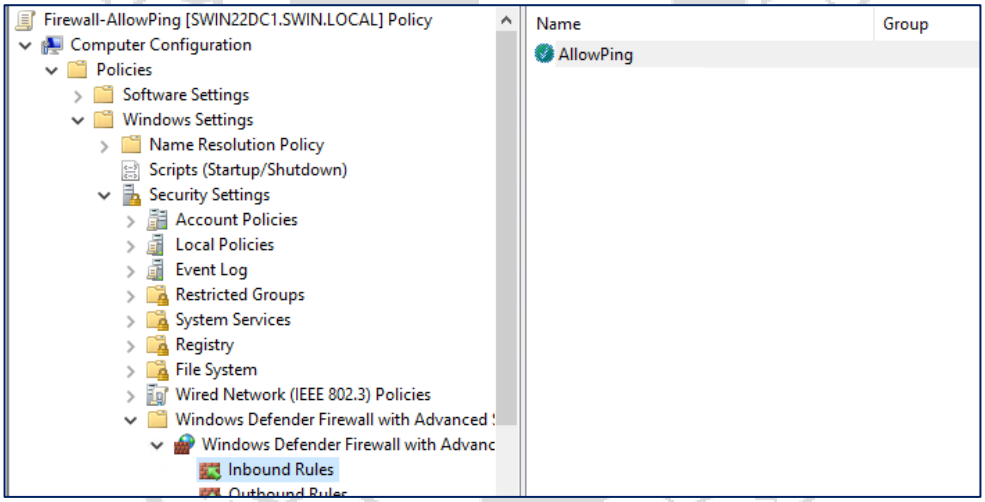


Figure 7 - Windows Firewall via GPO

Best Practices Analyzer or Security Compliance Manager

The Best Practices Analyzer (BPA) is built into Server Manager. It is a tool that scans the server for security hols, and performance improvements. It is similar to the Security

Compliance Manager (SCM), which also runs as a wizard and identifies potential security holes. The report provides a list of suggested improvements, with links that either fix the issue for you or take you to a Microsoft web page that provides instructions on how to rectify the issue. For a new network administrator it is a valuable security blanket.

As the focus of this lab is security, ideally we would prefer to use SCM, but as we would need to download it and install it we will proceed with the BPA.

34. In **Server Manager**, click on **All Servers**, and make sure that **SWIN22DC1** is selected. Then scroll down until you see **Best Practices Analyzer**.

35. Click on the drop down arrow next to **TASKS**, select **Start BPA Scan**, then click the **Start Scan** button.

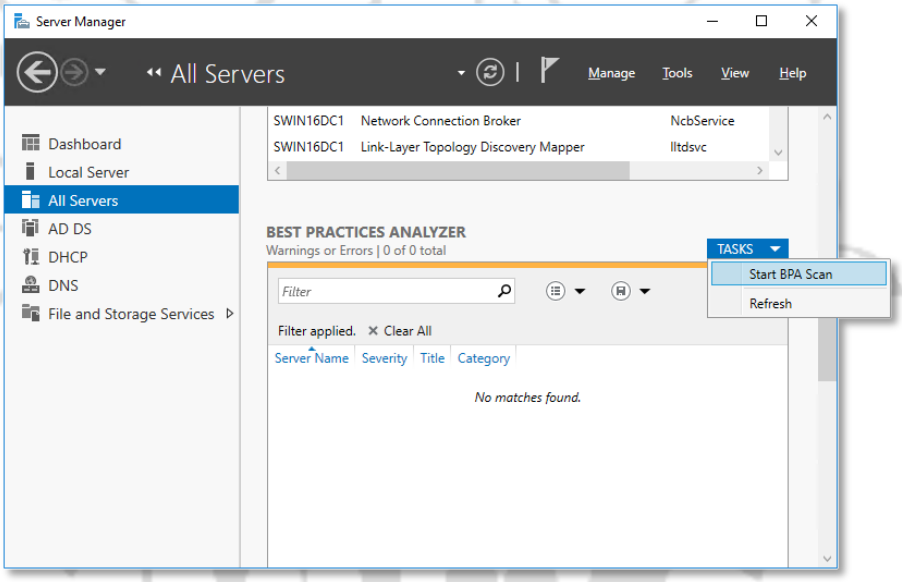


Figure 8 - Start BPA Scan

It takes a while, so be patient.

36. When the wizard completes you will be provided with a list of warnings.

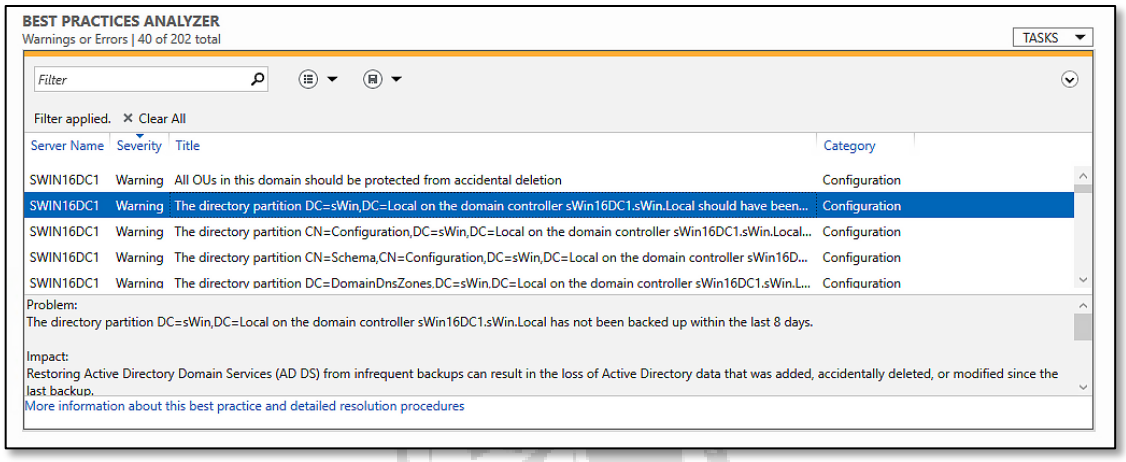


Figure 9 - BPA Report

Clicking on one of the items will provide you with details of the problem, the impact if the problem was to eventuate and a link to where you can get instructions on how to fix the problem... but the links won't work when you are not connected to the internet. So we will leave it here for this exercise.

Reminder

Record the concepts, design strategies, techniques, configurations and commands that you learn in this week laboratory class.

Pack up

1. Shut down all guest VMs.
2. **Sign out** from the Host virtual machine and make sure that it is **Stopped** otherwise it will run in the background and use up your quota.
3. If on campus, **log off from the ATC626 lab PC,** and push your chair in as you leave.

End of Lab