



---

# WEEKLY REPORT

---

Network Administration



MARCH 27, 2024

SWINBURNE UNIVERSITY OF TECHNOLOGY

# LAB REPORT 1

## (from week 1 to week 4)

### Table of Contents

#### ❖ Week 1

- Key concepts.....2
- Innovative ways to address business needs.....8
- Reflection and plan for further study.....8
- Key configurations and commands.....9

#### ❖ Week 2

- Key concepts.....11
- Innovative ways to address business needs.....15
- Reflection and plan for further study.....16
- Key configurations and commands.....17

#### ❖ Week 3

- Key concepts.....21
- Innovative ways to address business needs.....23
- Reflection and plan for further study.....24
- Key configurations and commands.....25

#### ❖ Week 4

- Key concepts.....30
- Innovative ways to address business needs.....33
- Reflection and plan for further study.....33
- Key configurations and commands.....34

#### ❖ References.....36

## Week 1

### ➤ Key concepts

A computer includes some **critical components**: **input**, **output**, **controller**, and **storage**.

*e.g. the input is the card reader, the output can be considered as the light bulbs.*

If there is only one component not contained, the computer could not work properly.

Refer to some key components that can be called **end-user devices** of the network

*e.g. personal computers, servers that provide services like e-mail, web, Telnet, FTP, etc., and Misc like VOIP phones, Printers, etc.*

Some **media types** are mainly used today:

**Copper** is one of the most common choices. There are 3 main types of copper such as **Unshielded Twisted Pair**, **Shielded Twisted Pair** and **Coaxial Cable**. The difference between the first two is that the Shielded Twisted Pair is covered in a sheathing that protects the part inside the cable from some harmful features of the environment and **major problems with the media** (which will be mentioned in the next section).

Glass such as **Fiber Optics** and some air options are also ubiquitous nowadays such as **Infrared**, **Wi-Fi**, **Bluetooth**, etc.

*Referring to the **scenario**, Thu is listening to music with her Bluetooth Air Pods and she is standing near the microwave, destructive interference might happen with the song she is listening to. So how can this strange phenomenon be explained?*

There are two **major problems with the media**: **Interference** and **Attenuation**.

**Interference** is the disruption of other signals into the network. In the example above, the waves from the microwave disrupt the Bluetooth signals so the song has interfered with the annoying noise.

**Attenuation** will occur when the distance of nodes gradually weakens the transmission rates of the data. for example, when Thu is standing too far away from her phone, she can not hear the sounds from her Air Pods clearly and some sounds can be lost.

In recent years, many modern **network devices** have appeared; however, in the basic network, some devices should be contained and these devices are usually categorised by their network layers (the concepts about network layers will be mentioned in the next section).

Layer 1 devices are **Repeater**, **Hub** (multiport Repeater), **Cable**, and **Modem**.

Layer 2 devices include **Bridge**, **Switch** (multiport Bridge), and **Network Interface Card** (NIC).

Layer 3 devices include **Router**, and **Brouter** (Bridge Router).

In this report, not all network devices are listed and just some devices used in layers 1, 2, and 3 are mentioned).

It is impossible that a network does not have the protocols. **Protocols** are the pre-set rules that network devices use when transferring data. For instance, the three-way handshake must be completed before transmitting TCP data.

In this report, two data communication models will be discussed to see the similarities and differences between them: **OSI model and TCP/IP model**.

**OSI model** stands for **Opening System Interconnection**. It has 7 separate layers and each of them performs its tasks independently. Note that the ordinal number of each layer is increased from Physical to Application layer. The functions corresponding to the layer name will be illustrated in the table below.

***Open System Interconnection (OSI)***

<b><i>Layer</i></b>	<b><i>Layer name</i></b>	<b><i>Functions</i></b>
<b><i>1</i></b>	<b><i>Physical</i></b>	<i>Transmitting raw data bits across the media</i>
<b><i>2</i></b>	<b><i>Data Link</i></b>	<i>Data is packaged into frames and transferred to the destination using physical address (MAC address)</i>
<b><i>3</i></b>	<b><i>Network</i></b>	<i>Receiving frames from the data link layer and transferring them to the destination by using a logical address (IP address)</i>
<b><i>4</i></b>	<b><i>Transport</i></b>	<i>Manage the delivery and do the error check of data packets</i>
<b><i>5</i></b>	<b><i>Session</i></b>	<i>Manage sessions between users</i>
<b><i>6</i></b>	<b><i>Presentation</i></b>	<i>Provides data format information to the application</i>
<b><i>7</i></b>	<b><i>Application</i></b>	<i>Performs services for the applications used by end users</i>

The **TCP/IP model** includes 4 layers: **Network Access, Internet, Transport** and **Application**. (Figure 1.1 below describes each layer of the TCP/IP model corresponding to the OSI model)

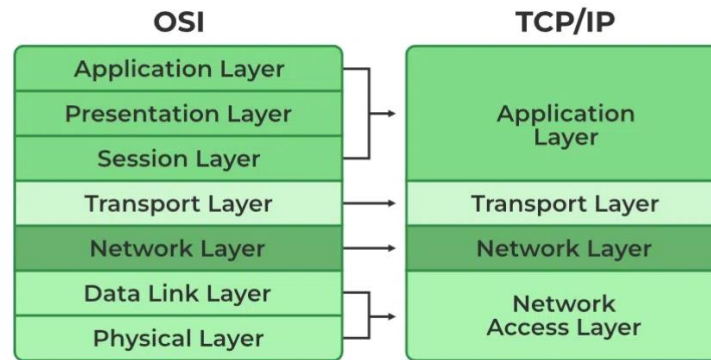


Figure 1.1

One of the most important basic networking concepts is **Encapsulation and Decapsulation**.

In the **Encapsulation** process, the application data is transmitted from the source node and passed through the application layer, presentation layer and session layer then the original data is packed into the data unit called segments in the transport layer. From the transport layer, data is sent to the network layer and the segment is transformed into the packet in this layer. When the packet comes to the Data Link layer, it is packed into the frame and the last step of the process is when data is processed in the first layer – The physical layer. The data now are all 0 and 1 bits and these bits will be transferred to the signals to move to the first layer of the destination node.

The data will go through the layers of the destination devices in the opposite way of the source device and that opposite process is the **Decapsulation**.

**PDU** stands for **Protocol Data Unit** is a single unit of information transmitted in different layers of the networking devices. Here are the PDUs corresponding to each OSI model's layer:

Layer 4: **Segment**

Layer 3: **Packet**

Layer 2: **Frame**

Layer 1: **Bits**

*(The process of **PDU**, **Encapsulation** and **Decapsulation** are shown in Figure 1.2).*

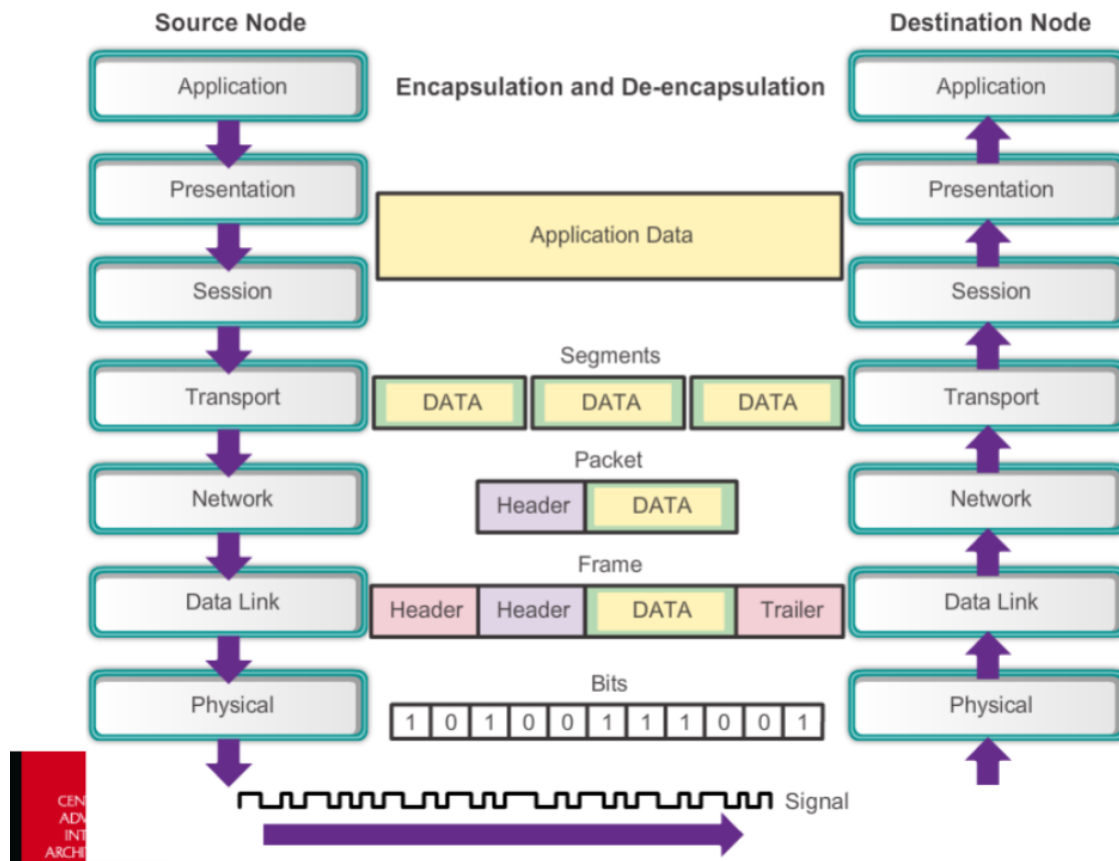


Figure 1.2

Throughout history, as we all know humans have used **Decimal System** with 10 digits. However, computers are not as intelligent as us so they have to transfer the input data into two digits (1 and 0) like ON and OFF only which is called **Binary System**.

e.g.      *Decimal number: 17; 100; 4.5*      *Binary number: 01110100*

To help the computer understand what data humans try to transmit, there is a mechanism that has the ability to convert the other types of number systems to binary.

- To convert **Decimal to Binary**, these steps need to be followed:

e.g. Convert 160 to binary:

**Step 1:** Write down the  $2^n$  from right to left. Note that n is from 0 to 7 and is increased by one.

$2^7$      $2^6$      $2^5$      $2^4$      $2^3$      $2^2$      $2^1$      $2^0$

**Step 2:** Starting from left to right, find and write down the values of  $2^n$  under each  $2^n$  and make sure that **value+previous values** is less than the decimal number. **DO NOT** write down the value that **value+previous values** is greater than the decimal number. **IF** that **value+previous values** is greater than the decimal number, skip that one and change to the next  $2^n$  and stop when the **value+previous values** is equal to the decimal number.

$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
128	64	32					
<160	64+128>160	32+128=160					
128	SKIP	160	STOP				

**Step 3:** Convey every **SKIP** and every digit after **STOP** to 0. Convert the **remainder digit** to 1.

$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
128	64	32					
<160	64+128>160	32+128=160					
128	SKIP	160	STOP				
1	0	1	0	0	0	0	0

→ 160 = 10100000

- To convert **Binary to Decimal** these steps need to be followed:

e.g. Covert 10101010 to decimal:

**Step 1:** Write down the  $2^n$  under each binary digit and from right to left. Note that n is from 0 and increased by 1 whenever comes to the next digit.

1	0	1	0	1	0	1	0
$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$

**Step 2:** Find the values of  $2^n$  and write down them under each binary digit.

1	0	1	0	1	0	1	0
$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
128	64	32	16	8	4	2	1

**Step 3:** Add all the values under digit 1. **DO NOT** add the values under digit 0.

1	0	1	0	1	0	1	0
$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
128		32		8		2	

→ 128 + 32 + 8 + 2 = 170

→ 10101010 = 170

- To convert **Binary to Hexadecimal** these steps need to be followed:

e.g. Convert 10101011 to Hexadecimal:

**Step 1:** Divide the Binary number into 2 equal parts.

1010 and 1011

**Step 2:** Convert each of these parts into Decimals

1010 = 10 and 1011 = 11

**Step 3:** Convert these Decimals into Hexadecimal as the table below:

Binary	Decimal	Hex
0000	0	0
0001	1	1
0010	2	2
0011	3	3
0100	4	4
0101	5	5
0110	6	6
0111	7	7
1000	8	8
1001	9	9
1010	10	A
1011	11	B
1100	12	C
1101	13	D
1110	14	E
1111	15	F

10 = A and 11 = B

➔ 10101011 = AB

**ASCII** (American Standard Code for Information Interchange) is a standard that assigns letters, numbers, and other characters in the 8-bit binary numbers (*shown in Figure 1.3*).



Chr	Binary ASCII	Decimal ASCII	Chr	Binary ASCII	Decimal ASCII	Chr	Binary ASCII	Decimal ASCII
<b>A</b>	01000001	65	<b>N</b>	01001110	78	<b>1</b>	00110001	49
<b>B</b>	01000010	66	<b>O</b>	01001111	79	<b>2</b>	00110010	50
<b>C</b>	01000011	67	<b>P</b>	01010000	80	<b>3</b>	00110011	51
<b>D</b>	01000100	68	<b>Q</b>	01010001	81	<b>4</b>	00110100	52
<b>E</b>	01000101	69	<b>R</b>	01010010	82	<b>5</b>	00110101	53
<b>F</b>	01000110	70	<b>S</b>	01010011	83	<b>6</b>	00110110	54
<b>G</b>	01000111	71	<b>T</b>	01010100	84	<b>~</b>	01111110	126
<b>H</b>	01001000	72	<b>U</b>	01010101	85	<b>!</b>	00100001	33
<b>I</b>	01001001	73	<b>V</b>	01010110	86	<b>@</b>	01000000	64
<b>H</b>	01001000	72	<b>W</b>	01010111	87	<b>#</b>	00100011	35
<b>K</b>	01001011	75	<b>X</b>	01011000	88	<b>\$</b>	00100100	36
<b>L</b>	01001100	76	<b>Y</b>	01011001	89	<b>%</b>	00100101	37
<b>M</b>	01001101	77	<b>Z</b>	01011010	90	<b>^</b>	01011110	94

Figure 1.3

### ➤ Innovative ways to address business needs

In the real world of business, there can be interference from your own network or neighbour's, non-wifi wireless devices, microwaves or radar systems since Wi-Fi transmits over the airwaves. The symptoms of interference issues are lagging and slow transmission. To mitigate this problem, some solutions can be adopted:

Ensure the proper design and configuration of access points (APs) to minimize interference because the AP signals might be interfering with each other. If there is too much overlap between APs, it can cause co-channel interference. "About a 15% to 20% coverage overlap between is an ideal number for business." – cited from: <https://www.networkworld.com/article/734150/coping-with-wi-fi-s-biggest-problem-interference-2.html>

Using the 2.4 GHz band generally has more interference and congestion, so using the 5 GHz band can help clients avoid interference.

Increasing Wi-fi transmission can indirectly help minimize network interference.

### ➤ Reflection and plan for further study

In the first week, converting between the number systems takes me a lot of time to complete, especially from **Decimal to Hexadecimal** and from Hexadecimal back to Decimal.

To address this problem, after doing the **pre-recorded lecture** on number systems on Canvas, I practice these conversions by doing the *optional further conversion questions* file in the post-viewing questions section on Canvas and having a look at some Samples of conversions on Google.

## ➤ Key configurations and commands

There is no lab in the first week. However, some shortcuts and networking symbols should be known before doing the following week's labs.

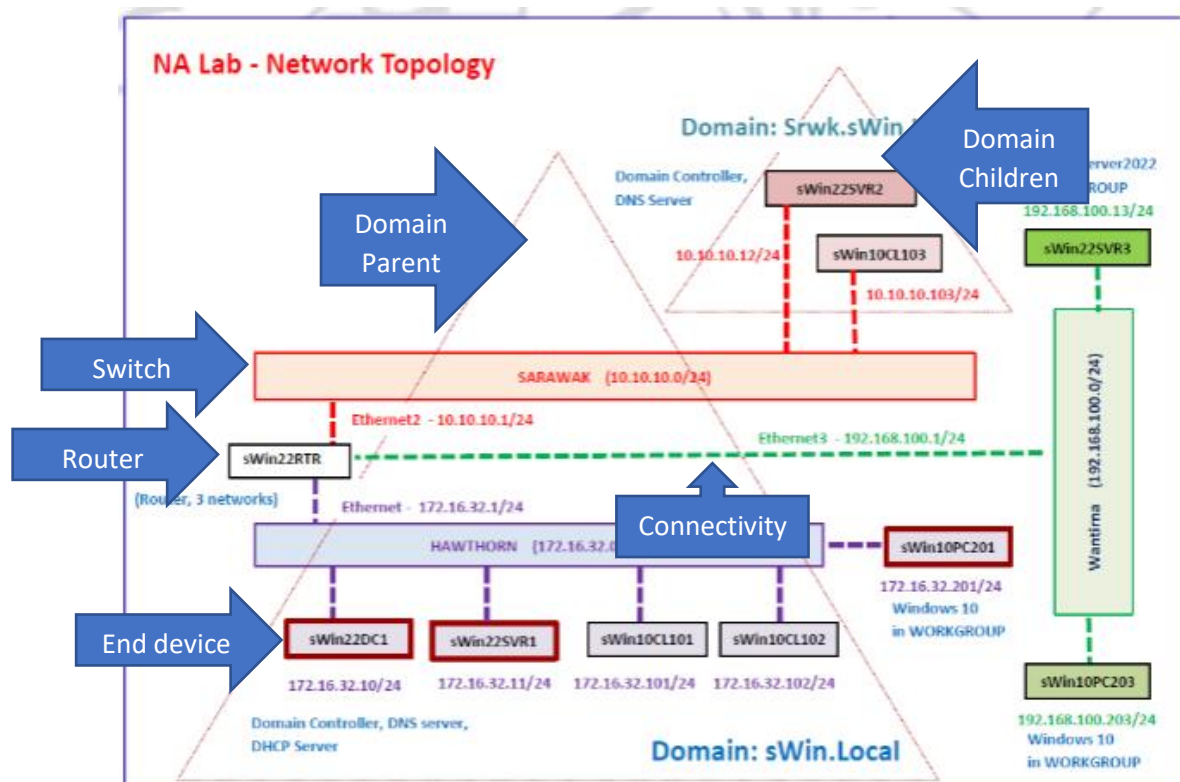


Figure 1.4

**Connectivity:** has a specific colour for a specific subnet  
*e.g. purple for Hawthorn, red for Sarawak, etc.*  
Connectivity is related to media types section on page 2.

**Switch:** connecting devices within the same subnet

**Router:** connecting devices in different subnets

Before doing the labs, **Azure Lab** need to be registered. To sign in every **Virtual Machine (VM)**, the password is: **Pa55w.rd**

Some interesting **shortcuts**:

Type: Window icon + R → **Run**

In **Run**, type: **cmd** → Open **Command Prompt**

**Powershell** → Open **Powershell Window**

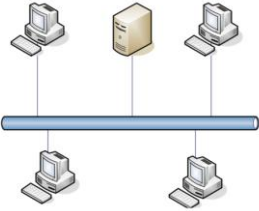
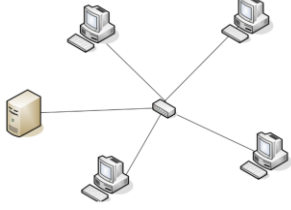
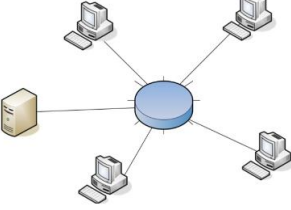
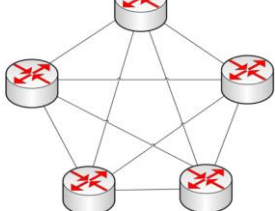
**ncpa.cpl** → change **network configurations**

*Completed on 8<sup>th</sup> March, 2024.*

## Week 2

### ➤ Key Concepts

**Network Topology** is the arrangement of a network that comprises nodes and connecting lines via source devices and destination devices. Some network topologies are listed in the table below:

Topology name	Definition and Feature	Illustration
<b>Bus Topology</b>	All devices are connected to the backbone.	
<b>Star Topology</b>	All devices are connected to a central concentrator.	
<b>Ring Topology</b>	All devices are connected in a circular manner, forming a closed loop or connected to a central MAU.	
<b>Fully Meshed Topology</b>	Every device is connected to each other.	

All network topologies have their **advantages and disadvantages**. Take **Fully Meshed Topology** as an example, it is the safest topology and has the greatest redundancy because every device is connected to each other but it is very difficult and expensive to administer and maintain.

Data transmission is just like the way a letter is sent. On the envelope, it must have the addresses of the sender and the receiver. Similar to networking, the devices must know if data is sent for them or not, know which port to send data out, etc.

Here is how **Network Addressing** is established. At the Physical layer, data is in the form of 0 and 1 bits. When these bits are passed to Data Link layer, they are broken down into bytes

(1 byte = 8 bits). After that, the **frame** is assigned meaning based on location. Various fields in the frame are **Pre-amble**, **Destination Address**, **Source Address**, **Type/Length**, **Frame Check** and **Encapsulated data from upper layers**.

There are 2 types of address in networking: **Physical address** and **Logical address**. To understand the difference between them, the example and table below are referred to:

A laptop has its address and this address will never change despite a person taking the laptop to other places → **Physical Address** or **MAC address**.

*When using the terminal to show the physical address of the device, it should be shown in Figure 2.1 below:*

```
Ethernet adapter Local Area Connection:
Physical Address. . . . . : 00-03-FF-AF-CA-87
```

*figure 2.1*

Every time the laptop is moved to a new place, its address will be changed to the new one → **Logical Address** or **IP address**.

*When using the terminal to show the logical address of the device, it should be shown in Figure 2.2 below:*

```
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::3075:a3fd:85b7:40f8%10
    IPv4 Address. . . . . : 10.10.0.50
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 10.10.0.1
```

*figure 2.2*

Physical Address	Logical Address
created when the device is manufactured	configured by the Network Administrator
operated at Data Link layer	operated at Network Layer
Cannot be divided into separate sub-network	Is used to group devices into sub-networks

The **Address Resolution Protocol (ARP)** enables layers 2 and 3 to resolve each other. The commands to work with the ARP table will be mentioned in the Key Configurations and Commands section on page 12.

IP address is a logical and hierarchical address, comprising 32 bits and to make it easier to read, the IP address is broken into 4 octets and separated by the dot signs.

*e.g. 10001101.11110000.10101010.00111100 or 141.240.170.60*

The example below indicates **the hierarchy of IP address**:

*123.24.243.12 = store.parks.ca.gov*

If the order of octets in the IP address is changed, the address will lose its hierarchy.

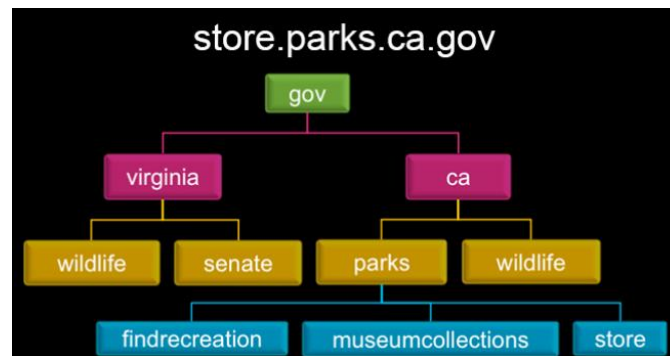


Figure 2.3

The hierarchy of IP addresses is also implied by **subnetting** and the administrators use **Subnet Masks** to configure devices to a specific place in the hierarchy.

The subnet mask is 32 bits in length and comprises all “1” bits on the left and all “0” bits on the right.

*e.g. 11111111.11111111.11111111.00000000 in binary*

*255.255.255.0 in decimal*

**CIDR** is the number of “1” bits: /24 (must have the slash before the CIDR value).

**Host portion** is all “0” bits part.

**Network portion** is all “1” bits part.

*Because the bits always begin at the significant end of the byte, decimal subnet masks can only contain the numbers: 0, 128, 192, 224, 240, 248, 252, 254 and 255.*

It is necessary to understand how to find the **Network Address** or **Subnet ID** If we already know the **Host Address** and the **Subnet Mask**. So what is Network Address or Subnet ID and how to find them?

**Network Address** is the first address of the subnet and all bits in host portion are set to 0.

*e.g. 172.16.0.0/16*

**Broadcast address** is the last address of the subnet and all bits in host portion are set to 1.

*e.g. 172.16.255.255/16*

**Host Address** is a unique address of a device in the subnet (unique host portion).

*e.g. 172.16.0.1/16*

The network address can be identified if there are a host address and a subnet mask. To identify it, the **AND operator** can be applied:

Data Set A	0	1	1	0
Data Set B	0	1	0	1
Result	0	1	0	0

e.g. The host address is 172.16.240.1 and subnet mask is 255.255.0.0. The network address and broadcast address can be identified by following these steps:

**Step 1:** Convert the decimal values to binary values:

172 . 16 . 240 . 1  
10101100 . 00010000 . 11110000 . 00000001

255 . 255 . 0 . 0  
11111111 . 11111111 . 00000000 . 00000000

**Step 2:** Do the **ANDING**

10101100 . 00010000 . 11110000 . 00000001  
11111111 . 11111111 . 00000000 . 00000000

Result: 10101100 . 00010000 . 00000000 . 00000000

**Step 3:** Convert the result back to decimal

10101100 . 00010000 . 00000000 . 00000000 = 172.16.0.0

The subnet mask can determine the level of the network (figure 2.4 below)

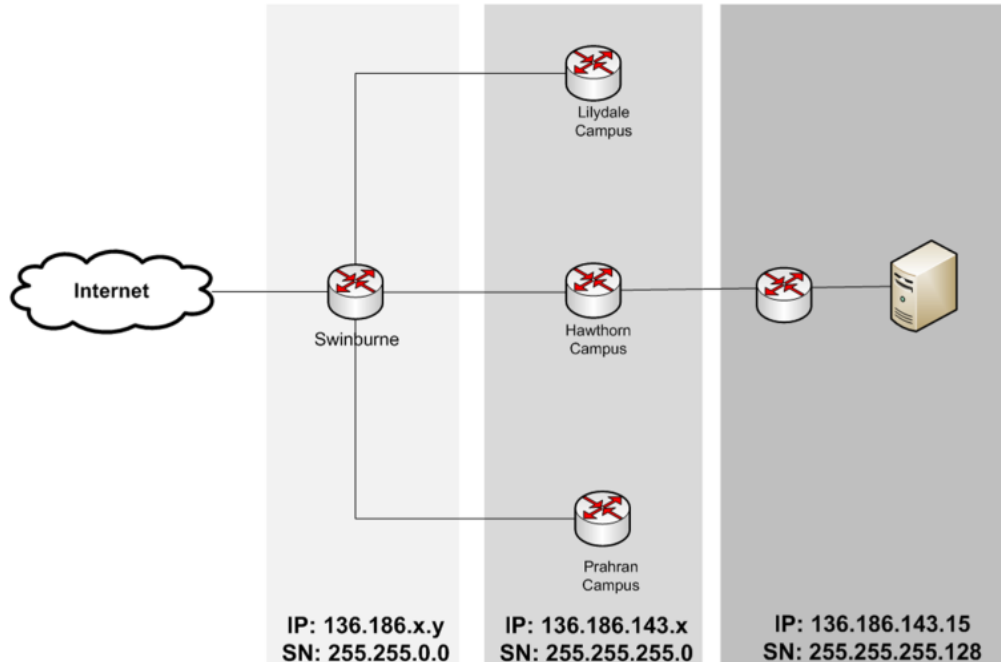


Figure 2.4

There are some **Logical Address Rules** which are:

Addresses in the **same subnet** must be connected to the same LAN (same hub or switch). Therefore, devices must be in the same subnet to communicate in the same LAN. Thus an **IP address** and a **Subnet Mask** must be configured at a minimum.

Communication with other subnets (different LANs or **different networks**) must be sent to a **router** or **gateway**. Thus a **default gateway address** must be configured in order to communicate outside the local LAN .

*And how to know whether the addresses are in the same subnet or not is discussed in the previous section by finding the Network Address of each subnet and then comparing them.*

Here are some **Logical Address Constraints** that are not allowed to be assigned to hosts:

- **224.0.0.0 – 239.255.255.255** : are reserved for **multicast** purposes.
- **224.0.0.0 – 255.255.255.254** : are reserved for IETF **research** purposes.
- **127.0.0.1 – 127.255.255.255** : is reserved for **this device** (loopback address)
- **255.255.255.255** : is reserved for **all devices** (universal broadcast address)
- **First address** (Network Address) and **last address** (Broadcast Address)

Here are the **Private IP Addresses** which are only reserved for private networks, and cannot be used for Internet traffic:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

**Automatic Private IP Addressing (APIPA)** enables a DHCP client to automatically assign an IP address to itself when there is no DHCP server available to perform that function:

169.254.0.0 – 169.254.255.255.

*DHCP will be discovered in the later section of this report.*

To host a resource from anywhere on the Internet, the server must be allocated a **Public IP Address** which is not a Private IP Address or IP Address Constraints listed above.

## ➤ Innovative ways to address business needs

In a business, it is important to determine an appropriate network topology depending on the requirements and goals of the business.

While creating a topology for a large network, administrators should use different topologies for different network points, especially between LAN and WAN and consider some future features such as expansion, network security, transmission speed and accessibility.



Some departments in a business that do not need a high rate of availability can be designed with partially meshed topology. The departments need a high rate of availability such as the department taking responsibility for banking and transferring money must be attached with a fully meshed topology because this type of topology makes sure all the devices can communicate with each other and the redundancy.

### ➤ Reflection and plan for further study

As there are too many IP address constraints, I could not remember all these constraints. In the lecture revision quiz 2, I made mistakes with a question relating to finding a valid IP address that can not be in the range of IP address constraints and private address.

**Incorrect**

**Question 3** 0 / 1 pts

Which of the following is a valid IP address to configure a computer with?

- ☒ 238.1.2.3 /24
- ☐ 172.16.10.0 /16
- ☐ 172.16.256.1 /24
- ☐ 172.16.10.0 255.255.255.0

Incorrect

### Question 8

0 / 1 pts

Which of the following IP addresses would be appropriate for a Web server that is required to have worldwide availability?

- ☒ 10.168.255.9 255.255.0.0
- ☐ 172.38.0.1 255.255.0.0
- ☐ 192.168.10.5
- ☐ 172.16.18.10 255.255.255.0

To solve this problem, I revise all these constraints and do more practice in identifying the valid IP address and correcting all the questions I answered incorrectly.

### ➤ Key configurations and commands

The explanation for the names of the VMs in detail (refer to Fig.2.6):

**sWin22:** Window server and 2022 is the year version

**RTR:** functions as a router

**DC:** functions as a DHCP server, a DNS server and a Domain Controller.

**PC:** a machine in a workgroup

**CL:** a machine in the domain

And the last number is just a particular machine, i.e. **sWin10Cl101**.

It is important to understand the functions of each device in the topology in Fig. 2.6 below. For example, sWin22RTR functions as a Router and Hawthorn switch connects all the devices in Hawthorn network, etc.

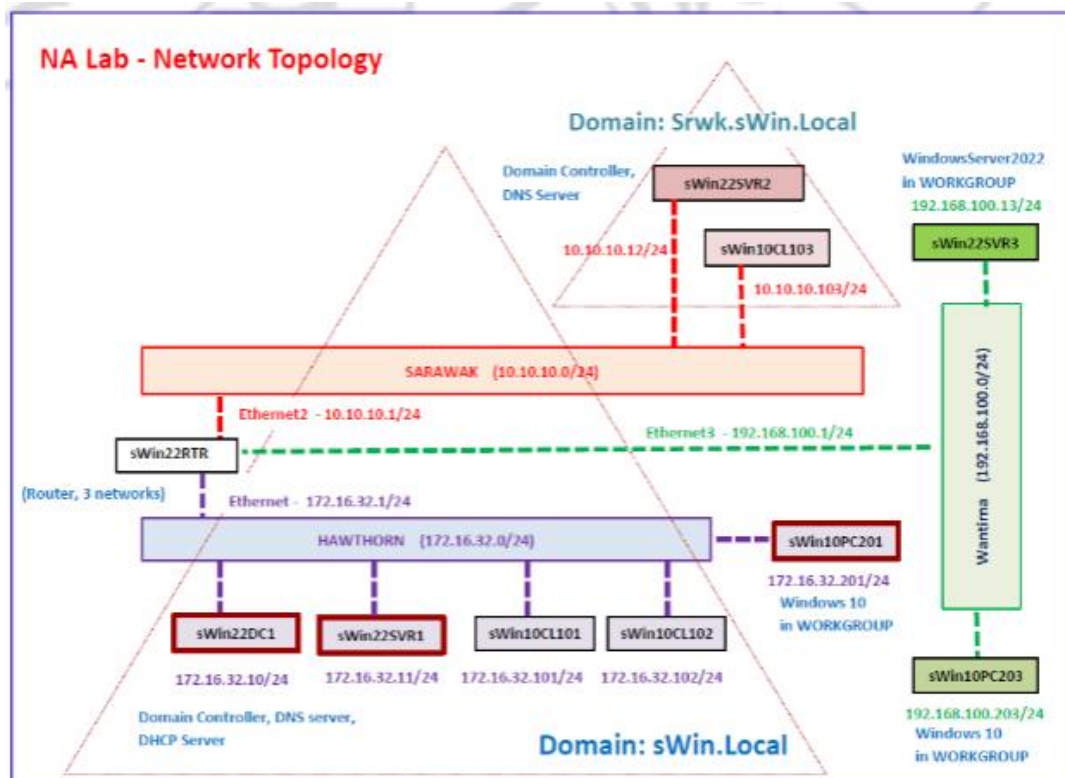
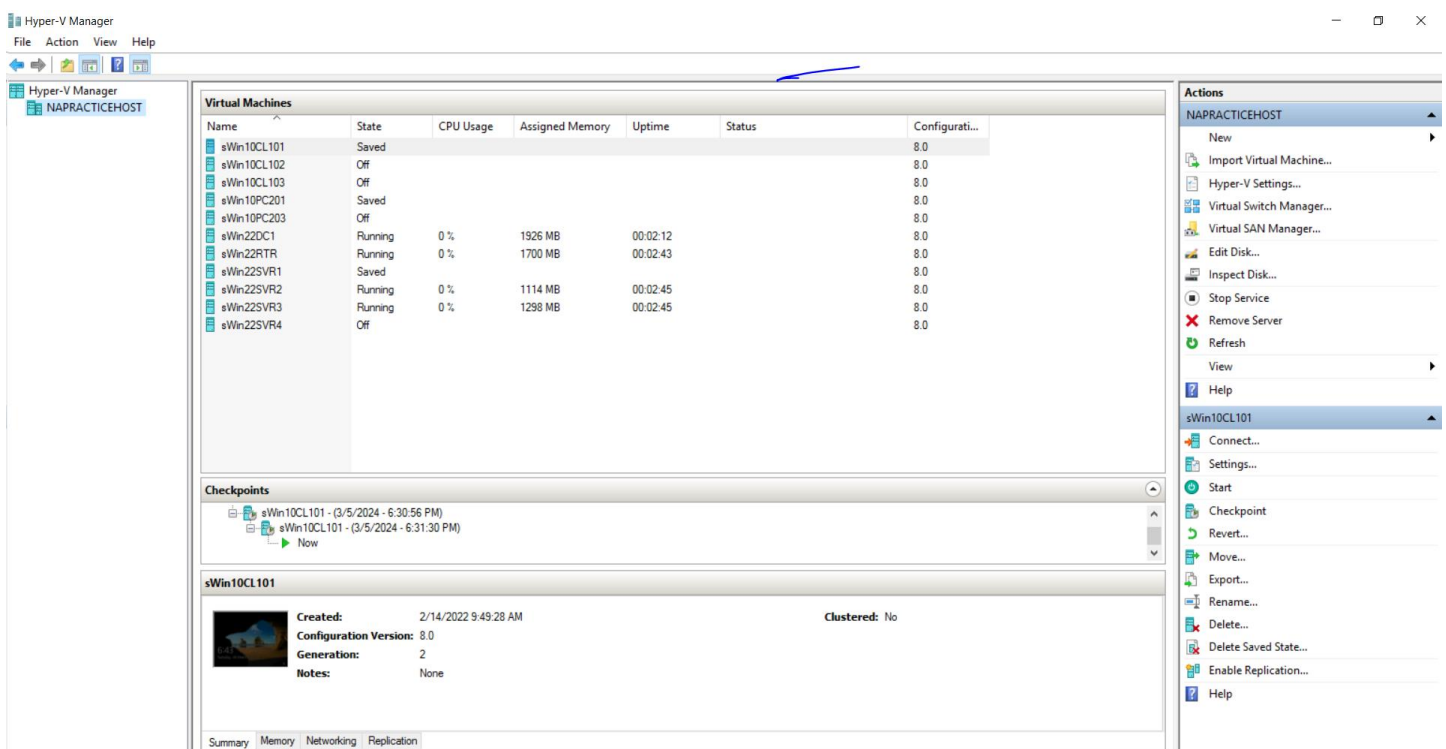


Figure 2.6

After accessing the Host Virtual Machine in Azure Lab, **Hyper-V manager** should be clicked to launch. The interface of Hyper-V manager and all the VMs are shown in fig.2.5 below:

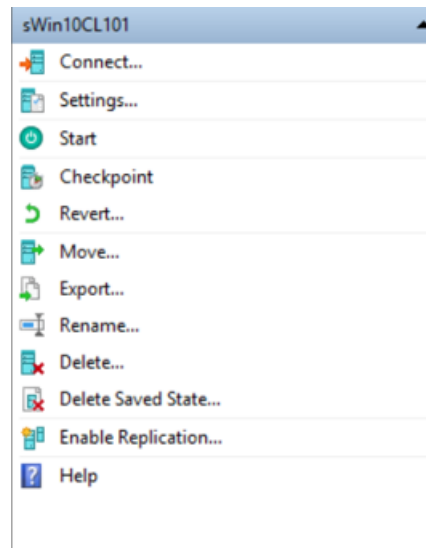


*figure 2.5*

In Hyper-V manager, some actions are done in the lab:

**Create virtual switch in Virtual Switch Manager** and enter information in some fields in new virtual switch. Configure **Connection Type** to be a **Private network**.

Examine the properties of a VM: When clicking on the VM name, i.e. sWin10CL101, some options are shown in *Fig.2.6*:



*Figure 2.6*

In **Settings**, some properties of the VM can be viewed such as the amount of RAM allocated to the VM, the controller the VM's hard disk attached and which network the VM is attached to.

It is important to check if the network is attached to the VM correctly.

**Checkpoints** (StartingImage – cannot be deleted) will save the state of a VM at a particular time hence it enables **reverting** the VM to that time configuration.

**Good Practice:** always revert the VM before starting and connecting to the VM.

To view the **IP configurations**, in the **Command Prompt**, type **ipconfig** and press Enter. The output, i.e. IPv4 Address and Subnet Mask will come up in **Ethernet Adapter** part (*Fig.2.7*).

```
Microsoft Windows [Version 10.0.20348.169]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::1521:47f7:a133:b357%6
    IPv4 Address. . . . . : 192.168.100.13
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
```

Figure 2.7

To configure the IP address and subnet mask, these steps must be followed:  
VM's name → in **Server Manager Window** → click **Local Server** → In **Properties** section  
→ click the link next to **Ethernet** → in the **Network Connections** → right click **Ethernet**  
→ select **Properties** → click on **Internet Protocol Version 4 (TCP/IPv4)** → select  
**Properties** button → enter the required IP address and subnet mask → click **OK** twice.

*Completed on 15<sup>th</sup> March, 2024.*

## Week 3

### ➤ Key Concepts

Here are some **TCP/IP Protocol Suites** corresponding to each layer of the TCP/IP model:

TCP/IP layer	TCP/IP Protocol Suites
Application	HTTP, FTP, SMTP, DNS, RIP, SNMP
Transport	TCP, UDP
Internet	IPv4, IPv6
Network Interface	Ethernet, 802.11 wireless LAN, Frame Relay, ATM

A **Socket** is a combination of an IP address, a transport protocol, and a port number.

It is important to remember the port number of each port:

**HTTP** – TCP PORT 80

**FTP** –TCP PORT 21

**SMTP** – TCP PORT 25

**DNS** – UDP PORT 53

**RIP** – UDP PORT 520

**SNMP** – UDP PORT 161

IPv4 address space is divided into 5 classes: A, B, C, D and E. Each class has a specific range of IP addresses but classes A, B and C are now used by most devices on the Internet. Class D and E are used for special purposes (*shown in figure 3.1 below*).

**Five Different Classes of IPv4 Addresses**

Class	First Octet decimal (range)	First Octet binary (range)	IP range	Subnet Mask	Hosts per Network ID	# of networks
Class A	0 – 127	0XXXXXXXX	0.0.0.0-127.255.255.255	255.0.0.0	$2^{24}-2$	$2^7$
Class B	128 – 191	10XXXXXXXX	128.0.0.0-191.255.255.255	255.255.0.0	$2^{16}-2$	$2^{14}$
Class C	192 – 223	110XXXXXX	192.0.0.0-223.255.255.255	255.255.255.0	$2^8-2$	$2^{21}$
Class D (Multicast)	224 – 239	1110XXXX	224.0.0.0-239.255.255.255			
Class E (Experimental)	240 – 255	1111XXXX	240.0.0.0-255.255.255.255			

Figure 3.1

*Note that **Classful Addressing** is no longer used nowadays which is replaced by **CIDR**.*

It is important to understand **What is Subnetting? How to create subnets?** and the **Benefits of subnetting**.

**Subnetting** is the process of creating a subnetwork within a network. Devices in the same subnet can communicate with each other but they can not communicate when they are in different subnets (must have the router and Default Gateway must be configured).

To **create subnets**, the administrator must know the demands for each subnet (the number of hosts in each subnet or subnet size) and how many subnets they should create.

To create a subnet, bits in the host portion are borrowed and moved to the network portion. If **n** is the number of borrowed bits and **m** is the remaining host bits after borrowing:

*The number of subnets < or =  $2^n$*

*The number of valid hosts in each subnet =  $2^m - 2$*

*The reason why minus 2 is to minus the first address and last address which are used to assign to network address and broadcast address.*

e.g. Refer to the network with subnet ID is **192.168.1.0/24** We need to divide this subnet into 4 smaller subnets.

We have to borrow 2 host bits because:  $4 = 2^2 \rightarrow /26$

Number of hosts in each subnet =  $2^6 - 2 = 62$  hosts  $\rightarrow$  gap size = 64 (Whenever go to the next subnet, add 64).

The address will be cut at the fourth octet  $\rightarrow$  add 64 at the fourth octet of the address whenever go to the next subnet.

To find the **broadcast address**, change all the host bits of **subnet address** to 1 and then convert back to decimal after calculating.

e.g. 192.168.1.00000000  $\rightarrow$  192.168.1.00111111 = 192.168.1.63

The other way to find **broadcast address** is minus 1 from the fourth octet of the **next subnet's address**.

To find the **first address**, add 1 to the fourth octet of **subnet address**.

To find the **last address**, minus 1 from the fourth octet of **broadcast address**.

All the subnets with all addresses are listed in the table below:

Subnet Address	First Address	Last Address	Broadcast Address
192.168.1. <b>0</b> /26	192.168.1.1/26	192.168.1.62	192.168.1.63/26
192.168.1. <b>64</b> /26	192.168.1.65/26	192.168.1.126	192.168.1.127
192.168.1. <b>128</b> /26	192.168.1.129	192.168.1.190	192.168.1.191
192.168.1. <b>192</b> /26	192.168.1.193	192.168.1.254	192.168.1.255

Using subnetting provides a wide range of **benefits**. The first benefit is that it **reduces network congestion** by segmenting traffic. The second benefit is the **ability to use a single network address across multiple locations**. *For example, Class B Network Address can be divided so that each branch can have its own subnet.* The third benefit is **increasing security** by using firewalls to separate subnets.

There is another way to do subnetting called **Subnetting in a Flash** (named by Swinburne lecturer). **Subnetting in a Flash** is applied through the following rules:

*Example: 192.168.10.0*

*255.255.255.224*

**Step 1:** Subtract the **non-.255 number** from 256 to find the **gap**.

$256 - 224 = 32$

**Step 2:** Start at zero and count by the result until gets to 256 ( but **DO NOT** include 256, just before 256), adding the **gap** every time moving to the next subnet.

*0, 32, 64, 96, 128, 160, 192, 224*

**Step 3:** These numbers become **the octet of the non-.255 number position**.

*192.168.10.0*

*192.168.10.32*

*192.168.10.64*

*192.168.10.96*

*.....*

## ➤ Innovative ways to address business needs

*Referring to the scenario, the company has multiple departments: Sales (160 hosts), Marketing (125 hosts), IT (45 hosts) and Finance (80 hosts), each requiring its own subnet for better organization and security.*



If using the traditional subnetting method as discussed above, these departments are divided into subnets that have the same size. Therefore, it leads to the waste of IP addresses.

To solve this problem, a better subnetting method can be applied which is called VLSM. **VLSM** stands for **Variable Length Subnet Mask**. This subnetting technique allows network administrators to create subnets of varying sizes based on the specific number of hosts needed in each subnet (Fig.3.2).

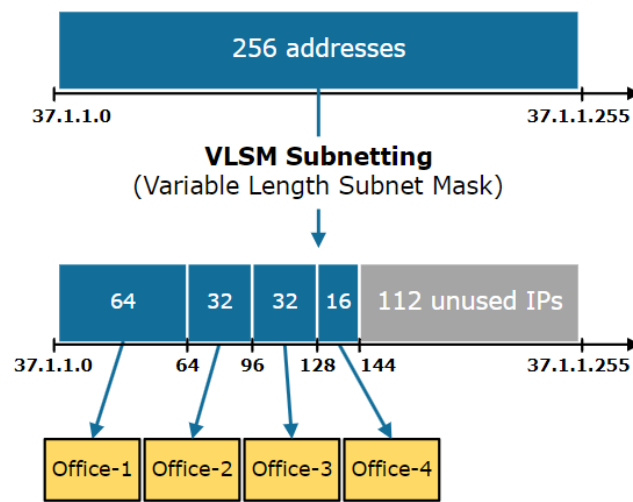


Figure 3.2

### ➤ Reflection and plan for further study

I get used to doing **subnetting in the traditional way**; however, I realize that this way takes me a longer time to do, compared to **Subnetting in a Flash**. I decided to step out of my comfort zone and start practising subnetting using the method **Subnetting in a Flash**.

Additionally, I practice the questions related to finding the first addresses, last addresses, subnet ID and broadcast address.

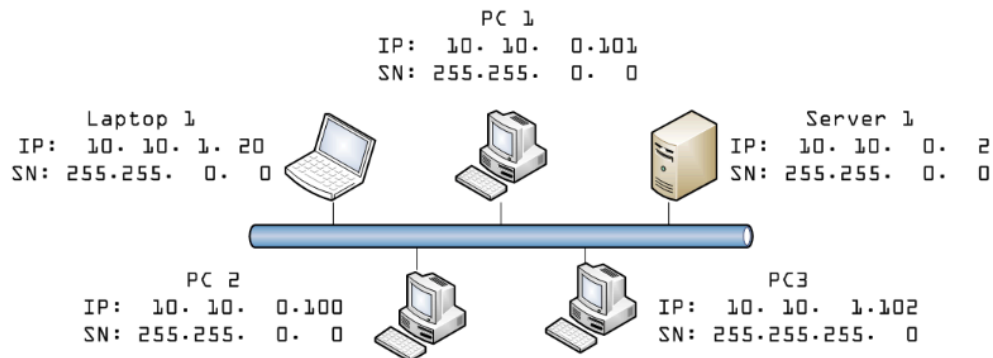
I also feel a little bit tricky when answering the questions about finding which devices can communicate or not and finding the devices configured incorrectly. In the revision quiz 3, I answered this kind of question incorrectly:

Incorrect

### Question 11

0 / 1 pts

Which of the following two devices can communicate



- ☐ PC1 to PC3
- ☐ Server 1 to PC3
- ☐ Laptop 1 to PC3
- ☒ PC3 cannot communicate with any other device

To work with these types of questions more easily, I revise all the concepts of the criteria for the ability to communicate between devices and read the answers of my unit convenor in **Ed discussion**.

Additionally, remembering all **PowerShell syntax** is a bit tricky for me as they are too complicated. I decided to practice more in typing these syntaxes more frequently at the weekly labs and also at home.

### ➤ Key configurations and commands

Some simple commands on Window PowerShell:

**cls:** clear the screen

**ipconfig:** list some configuration details (IPv4, IPv6, subnet mask, default gateway)

**ipconfig /all:** list all configuration details.

To Configure IPv4 and subnet mask by using **PowerShell**:

Type the following command:

## New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 172.16.16.10 -PrefixLength 20

Or Configure **Manually**: view *this configuration in week 2 Key Configurations and Commands*

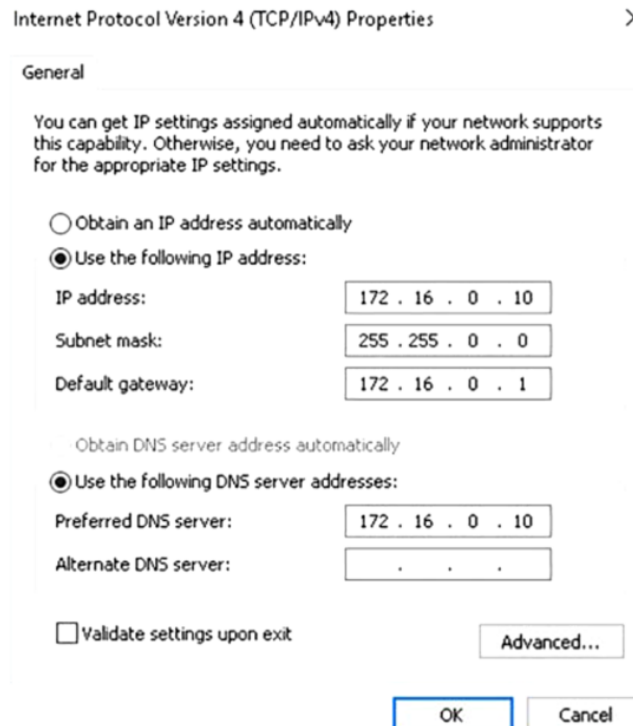


Figure 3.2

There are some **IPv4 Troubleshooting Tools** listed below:

**Arp**: view and edit arp cache mapping IPv4 address to MAC address.

**Hostname**: Displays the host name of the PC.

**Ipconfig**: displays current TCP/IP configuration values for IPv4, IPv6, DHCP configurations and DNS client resolver cache.

Type **ipconfig /all** to view all the IP settings. Notice the **DHCP Enabled** is no.

To configure the PC to obtain IP settings from a DHCP server: in the guest VM  
→ right-click **Win** key → select **Windows PowerShell (Admin)** → **Yes**

In **Windows PowerShell (Admin)** window, type:

**Netsh interface ip set address Ethernet dhcp** → enter

To verify the **DHCP enabled** to **Yes**: **ipconfig /all**

**Netstat**: displays statistics and other information about IPv4 and IPv4 connections.

**Netsh:** displays and allows administrator to administer settings for IPv4, and IPv6 on either local PC or remote PC.

**Nslookup:** queries a DNS server.

**Ping:** test IPv4 and IPv6 connectivity to other PC

**PC1:** 172.16.32.11

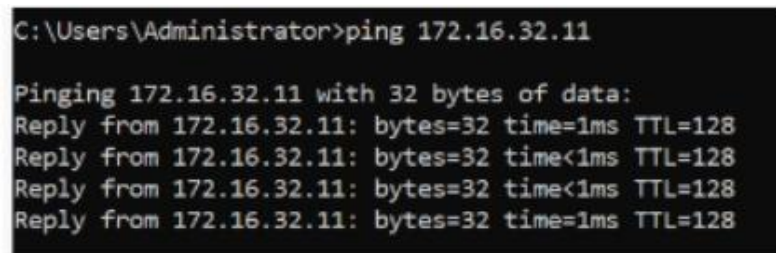
**PC2:** 172.16.32.12

To verify communication between 2 devices, in the **Command Prompt:**

on PC1 type: **ping 172.16.32.12** → enter

on PC2 type: **ping 172.16.32.11** → enter

If the ping is successful, the output should be as follows:



```
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 3.3

**Route:** view the local IPv4 and IPv6 routing tables and modify the local IPv4 routing table.

**tracert:** a sequence of increasing pings that helps to map out the path the data travels in. It helps the administrator to identify where along that path the connection may be down. *The output after doing tracert should come up as figure 3.3.*

```

C:\WINDOWS\system32\cmd.exe

Tracing route to www.swin.edu.au [136.186.1.10]
over a maximum of 30 hops:

  0  <1 ms    <1 ms    <1 ms    192.168.0.1
  1  3 ms      2 ms      2 ms      192.168.100.193
  2  66 ms     31 ms     48 ms     172.18.112.109
  3  34 ms     29 ms     32 ms     172.18.67.58
  4  37 ms     20 ms     32 ms     CPE-61-9-133-136.vic.bigpond.net.au [61.9.133.136]
  5  32 ms     27 ms     33 ms     TenGigabitEthernet4-1.lon55.Melbourne.telstra.net [165.228.103.225]
  6  *         37 ms     16 ms     TenGigE0-12-0-2.win-core1.Melbourne.telstra.net [203.50.79.129]
  7  43 ms     41 ms     46 ms     Pos0-0-0-0.fli-core1.Adelaide.telstra.net [203.50.6.186]
  8  48 ms     44 ms     43 ms     GigabitEthernet0-2.way27.adelaide.telstra.net [203.50.119.37]
  9  52 ms     18 ms     34 ms     optus3.lnk.telstra.net [139.130.237.10]
 10  39 ms     35 ms     33 ms     ge-wan4-1.55drc76fg.optus.net.au [61.88.179.14]
 11  38 ms     38 ms     44 ms     59.154.0.6
 12  50 ms     46 ms     48 ms     ge-1-0-4.bb1.a.adl.aarnet.net.au [202.158.199.9]
 13  37 ms     69 ms     51 ms     so-0-1-0.bb1.a.mel.aarnet.net.au [202.158.194.18]
 14  55 ms     53 ms     86 ms     gigabitethernet0.er1.swinburne.cpe.aarnet.net.au [202.158.200.130]
 15  67 ms     46 ms     49 ms     gw1.er1.swinburne.cpe.aarnet.net.au [202.158.200.142]
 16  *         *         *         Request timed out.
 17  57 ms     52 ms     60 ms     www.swin.edu.au [136.186.1.10]

Trace complete.

```

figure 3.3.

**pathping:** like **tracert** and also display information on packet loss for each router and subnet in the path.

Completed on 21st March, 2024.



## Week 4

### ➤ Key Concepts

One of the most critical concepts in **Networking Designs** is **Calculating Subnet Addresses and Host Addresses**.

*This part is related to the subnetting part in week 3 so it is necessary to revise this previous part before diving into this Design Concept.*

When determining subnetting, the administrator should:

- Choose the number of subnet bits based on the number of subnets required.
- Use  $2^n$  to determine the number of subnets available from n bits.  
*e.g. For 5 branches, the 3 subnet bits are required:  
cannot 2 bits because  $2^2 = 4 < 5$  (not enough)  
so must be 3 bits because  $2^3 = 8 \geq 5$*
- Choose the number of host bits based on the number of hosts that are required on each subnet.
- Use  $2^n - 2$  to determine the number of hosts that are available on each subnet.  
*e.g. For subnets with 100 hosts, 7 host bits are required:  
cannot 6 host bits because  $2^6 - 2 = 62 < 100$  (not enough)  
so must be 7 host bits because  $2^7 - 2 = 126 \geq 100$*

To calculate the number of bits (n) required where x = the number of subnets required.  
Here is the formula to do the calculation:

$$n = \text{roundup} \left\lceil \frac{\ln(x)}{\ln(2)} \right\rceil$$

Or look up the table below:

Subnets	Bits
2	1
4	2
8	3
16	4
32	5
64	6
128	7
256	8
512	9
1024	10
	etc.

When there are multiple smaller networks, **Supernetting** is used to combine them into a single larger network.

***Tips:** The **/slash notation increases** after **Subnetting** and **decreases** after **Supernetting**.*

Subnets chosen for **Supernetting** must be adjacent and must consolidate within upper boundary.

*e.g. 192.168.1.112/28 and 192.168.1.96/28 consolidate to 192.168.1.96/27*

*192.168.1.112/28 and 192.168.1.128/28 do not consolidate into anything*

**Dynamic Host Configuration Protocol (DHCP)** is a client/server protocol that automatically provides a host with its IP address and other related configuration information such as the subnet mask or default gateway.

DHCP is used for many **reasons** such as centralizing IP configuration settings, allowing flexibility in IP address management and catering for users who need to work at different places.

The process for **configuring a client for DHCP** will be discussed in the **Key Configuration and Commands** section below.

During the **DHCP connection**, the steps below are involved:

**Step 1:** DHCP **client** *broadcasts* a DHCP **DISCOVER** packet.

**Step 2:** DHCP **servers** *broadcast* a DHCP **OFFER** packet.

**Step 3:** DHCP **client** *broadcasts* a DHCP **REQUEST** packet.

**Step 4:** DHCP **Server1** *broadcasts* a DHCP **ACK** packet.

*The term **DORA** is to be easier to remember.*

**DHCP Renewal** will occur when **50%** of the **lease** has expired. A **lease** is defined as the time for which a DHCP server allocates an IP address to a client. When the expiration happens:

**Step 1:** DHCP **client** *sends a unicast* **DHCP REQUEST** packet.

**Step 2:** DHCP **Server1** *sends a unicast* **DHCP ACK** packet.

The client continues to try and renew using a unicast DHCP REQUEST every time it starts up. If the client fails to renew its lease after **87.5%** of the lease has expired, the full steps of DORA will be generated again.

**DHCP can be installed** in 2 ways:

Add the DHCP role using **Server Manager**

*Or:* Authorize the DHCP server with a privileged account if in a **Domain Environment**.



*These 2 ways will be covered in more detail in the **Key Configuration and Commands** section below.*

DHCP options can be applied at various levels: **Server**, **Scope**, and **Reservation**.

To be more specific:

**DHCP Scopes** is a container for administrating a pool of address and IP configurations. All addresses in a pool must come from the same subnet and a server can have many scopes.

**DHCP Reservation** ensures a device is allocated the same IP address. *For instance, when the PC has not been used for a long time, its IP address which is used to be assigned is allocated to the other device.* To ensure that the address is not used by others, DHCP Reservation should be applied.

Some devices need to have their IP settings manually configured and these addresses can not be offered to other devices. That is when **DHCP Exclusions** should be applied.

If the same setting is configured differently, the last applied wins. *For example, when the DHCP Reservation is configured after DHCP Scope, the DHCP Reservation configurations will remain and no settings for the Scopes exist.*

*The configurations for the options above will be covered in more detail in the **Key Configuration and Commands** section below.*

It is important to remember the **essential configurations** for different specific cases.

- If the devices are on the **same LAN**, **IP addresses** and **Subnet Masks** must be configured at a minimum.
- If they are in **different networks** or on the Internet, **IP addresses**, **Subnet Masks** and **Default Gateway** must be configured at a minimum.
- If they need to use **URLs**, all the elements above must be configured with a **DNS server**.

The lists below are key **DHCP options** which are frequently used:

**Default Gateway = 003 Router**

**DNS Server = 006 DNS Server**

**Time Server = 004**

**Name Server = 005**

**Hostname = 12**

**DNS Domain Name = 015**

A **DHCP Relay Agent** captures the DHCP Discover broadcasts and then unicasts them to a DHCP server on another network. It acts as a “man in the middle” and will broadcast all packets from the DHCP server and unicast all packets from the DHCP client.

*Just imagine DHCP Relay Agent as a Flight ticket agent. It will need to contact the clients first and then contact the flight centre to buy the tickets and lastly be paid by the clients when passing the tickets to them.*

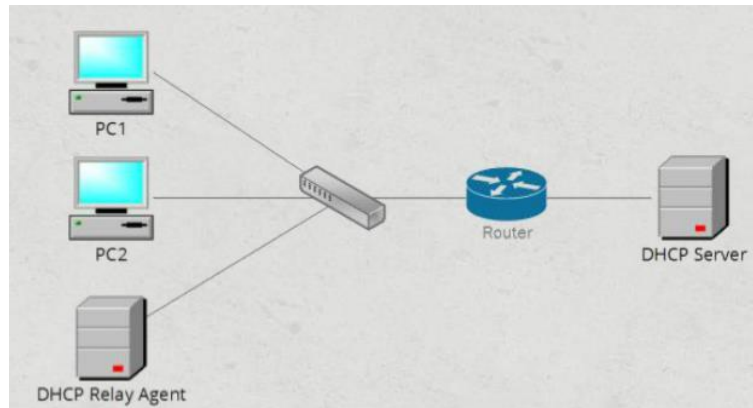


Figure 4.1

**DHCP redundancy** allows multiple DHCP servers to share the load and responsibility of serving IP addresses to clients. It provides backup and recovery options in case any server fails. This is a good practice to configure more than 1 DHCP server. However, *what happens if two DHCP servers offer the same addresses and how to solve it?*

That situation can lead to potential IP address conflicts and network connectivity issues. Some solutions can be adopted:

If there are two DHCP servers in a network, half of the address pool is used for one DHCP server and half of the pool is used for the other (50/50 rule)

Use DHCP Relay Agent with an 80/20 rule for the second server.

### ➤ Innovative ways to address business needs

One of the most serious security risks associated with DHCP that every administrator should know to tackle is **DHCP Starvation Attack**.

**“DHCP Starvation Attack** occurs when an attacker sends more requests for new IP addresses than the DHCP server can handle. The consequence is the legitimate client can not be assigned with IP address because of the overload caused by malicious requests.” – cited from: <https://menitasa.medium.com/common-dhcp-attacks-prevention-1f91b1defeb>

To reduce this attack on business, some steps can be taken:

Secure the devices and make sure that they are not reachable from the Internet or unauthorized person.

Assigned static IP address for all important devices instead of using dynamic IP address (DHCP).

Use firewalls configured with access rules on interfaces based on source/destination IP addresses.

### ➤ Reflection and plan for further study

I sometimes make mistakes when identifying the number of hosts each subnet support as I forgot to take out the first and last addresses. Therefore, before answering these types of questions, I have to think more carefully.

In this week's lecture, I understood all the concepts of DHCP, however, I have difficulty when working with real-life scenarios. To solve this problem, I revise the scenario questions in revision quiz 4 and read more scenarios on different materials.

### ➤ Key configurations and commands

Refer to Fig.4.2 below, sWin10PC201 can communicate with sWin22SVR1 because they are in the same network (Hawthorn). If sWin22SVR1 wants to communicate to sWin22SVR3, sWin22SVR1 need to be configured the default gateway which is the interface of the router that switch Hawthorn facing.

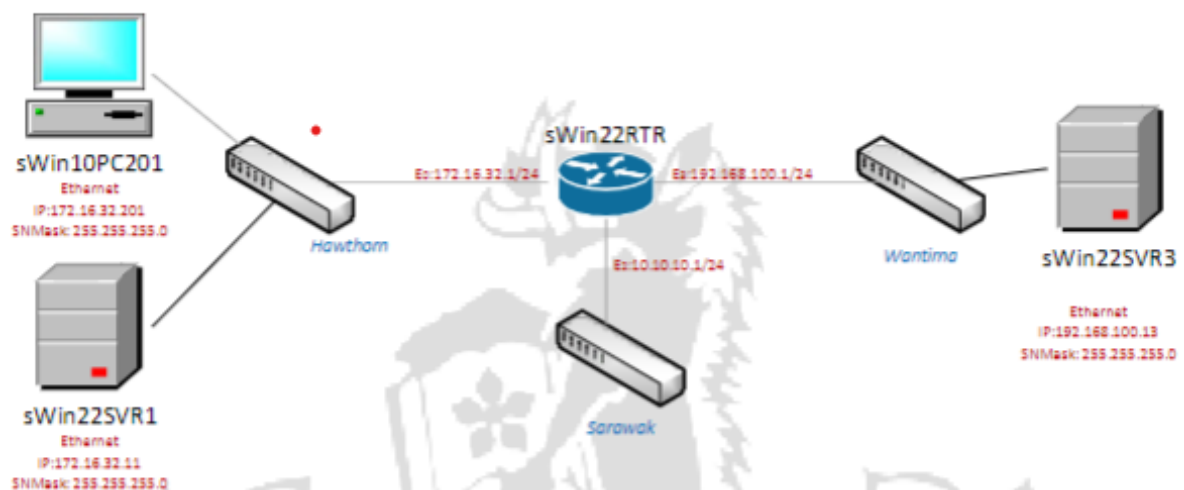


Figure 4.2

The device can communicate with the one that is in a different network if Default Gateway address is configured. To configure **Default Gateway** do all the steps for IPv4 manual configurations (*viewed in week 2 Key Configurations and Commands*) and do the additional step: In the **Internet Protocol Version 4 settings** type the IP address as the Default Gateway → OK (Fig.

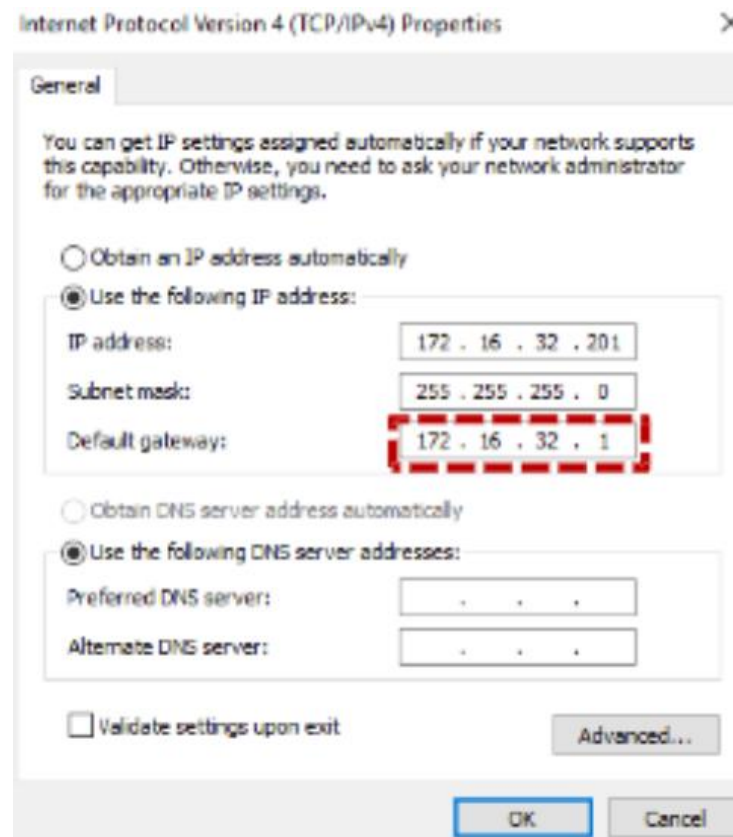


Figure 4.2

When using **PowerShell**: Type the command:

```
New -NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 172.16.32.201 -PrefixLength 20 -DefaultGateway 172.16.32.1
```

The **Address Resolution Protocol (ARP)** enables the two layers to resolve each other

In **Windows PowerShell (Admin)**:

To **display the arp table**, at a Windows command line type: **arp -a**

To clear the table, type: **arp -d**

*Completed on 29<sup>th</sup> March, 2024.*

## References

1. *Redirecting.* (n.d.). Login.microsoftonline.com. Retrieved April 4, 2024, from <https://swinburne.instructure.com/courses/57016/modules/items/3845558>
2. *Redirecting.* (n.d.). Login.microsoftonline.com. Retrieved April 4, 2024, from <https://swinburne.instructure.com/courses/57016/modules/items/3845560>
3. *Redirecting.* (n.d.). Login.microsoftonline.com. Retrieved April 4, 2024, from <https://swinburne.instructure.com/courses/57016/modules/items/3845562>
4. *Redirecting.* (n.d.). Login.microsoftonline.com. Retrieved April 4, 2024, from <https://swinburne.instructure.com/courses/57016/modules/items/3845564>
5. *Redirecting.* (n.d.). Login.microsoftonline.com.  
<https://swinburne.instructure.com/courses/57016/pages/lab-01-an-introduction-to-network-administration-labs>
6. *Redirecting.* (n.d.). Login.microsoftonline.com. Retrieved April 4, 2024, from <https://swinburne.instructure.com/courses/57016/files/30246162?wrap=1>
7. *Redirecting.* (n.d.). Login.microsoftonline.com.  
<https://swinburne.instructure.com/courses/57016/pages/lab-03-ipv4-and-subnetting>
8. *Redirecting.* (n.d.). Login.microsoftonline.com.  
<https://swinburne.instructure.com/courses/57016/quizzes/327198>
9. *Redirecting.* (n.d.). Login.microsoftonline.com.  
<https://swinburne.instructure.com/courses/57016/quizzes/327197>
10. *Redirecting.* (n.d.). Login.microsoftonline.com.  
<https://swinburne.instructure.com/courses/57016/quizzes/327195>
11. Tasa, M. (2022, June 6). *Common DHCP Attacks & Prevention - Meni Tasa - Medium.* Medium; Medium. <https://menitasa.medium.com/common-dhcp-attacks-prevention-1f91b1defeb>

12. What is VLSM? (n.d.). NetworkAcademy.io.  
<https://www.networkacademy.io/ccna/ip-subnetting/what-is-vlsm#:~:text=VLSM%20is%20a%20subnetting%20technique>
13. Identiv. (n.d.). *Designing Your Business Network Topology: Why Is It Important Today*.  
Www.identiv.com. <https://www.identiv.com/resources/blog/designing-your-business-network-topology-why-is-it-important-today>
14. How to fix Wi-Fi interference. (n.d.). Network World.  
<https://www.networkworld.com/article/734150/coping-with-wi-fi-s-biggest-problem-interference-2.html>
15. *What is DHCP and How It Works? A Complete Walkthrough | Simplilearn*. (n.d.).  
Simplilearn.com. <https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-dhcp-server-and-how-it-works>
16. What is Automatic Private IP Addressing (APIPA)? (n.d.). WhatIs.com.  
<https://www.techtarget.com/whatis/definition/Automatic-Private-IP-Addressing-APIPA>
17. GeeksforGeeks. (2017, March 7). Types of Network Topology - GeeksforGeeks.  
GeeksforGeeks. <https://www.geeksforgeeks.org/types-of-network-topology/>
18. Meridian Outpost. (2023). 5 Classes of IPv4 Addresses [Class A, B, C, D and E].  
Www.meridianoutpost.com.  
<https://www.meridianoutpost.com/resources/articles/IP-classes.php>