SCHOOL OF SCIENCE AND TECHNOLOGY
COURSEWORK FOR THE BIS, BCNS, BIT, BCS, BSDA, BSE, YEAR 1

ACADEMIC SESSION: APR 2023; SEMESTER 2/3

NET1014: Networking Principles **DEADLINE: 16 JULY 2023 23:59**

Name	ID	PROGRAM	SIGNATURE
Yap Jay Ann			

INSTRUCTIONS TO CANDIDATES

- **This assignment will contribute Assignment 1 (20%) + Assignment 2 (10%) to your final grade.**
- This coursework is a group assignment (maximum of 5 students per group). You must come out with the report with not more than **23 pages.**
- The report should be printed out double sided and submitted before the deadline.
- It is strongly recommended you don't wait for last minute to submit the report.

IMPORTANT

The University requires students to adhere to submission deadlines for any form of assessment. Penalties are applied in relation to unauthorized late submission of work.

Courseworks must be submitted on their due dates. If a coursework is submitted after its due date, the following penalty will be imposed:

- ONE day late : 5 % deducted from the total marks awarded.
- TWO days late : 10 % deducted from the total marks awarded.
- THREE : 15% deducted from the total marks awarded.
- 1 week more days late : Assignment will not be marked and 0% will be awarded.

Lecturer's Remark (Use additional sheet if required)

I..... (Name) .....std. ID received the assignment and read the comments..... (Signature/date)

Academic Honesty Acknowledgement

"I, Yap Jay Ann, (groupmates), verify that this paper contains entirely my own work. I have not consulted with any outside person or materials other than what was specified (an interviewee, for example) in the assignment or the syllabus requirements. Further, I have not copied or inadvertently copied ideas, sentences, or paragraphs from another student. I realize the penalties *(refer to page 16, 5.5, Appendix 2, page 44 of the student handbook diploma and undergraduate programme)* for any kind of copying or collaboration on any assignment."

(Student's signatures / Date:) 15 July 2023

Table of Contents

1.0 Overview
- 1.1 Introduction
- 1.2 Objectives

2.0 Implementation Details
- 2.1 Sunway Network Architecture and Justification
- 2.2 New Network Design
- 2.3 IP Addressing and Justification Department 1 (Finance Department)
- 2.4 IP Addressing and Justification Department 2 (IT Department)
- 2.5 IP Addressing and Justification Department 3 (Collab Room)
- 2.6 IP Addressing and Justification Department 4 (Registry)

3.0 Router
- 3.1 Overview
- 3.2 Implementation details
- 3.2.1 Configuration
- 3.3 Configuration challenges and workarounds

4.0 Switch
- 4.1 Overview
- 4.2 Implementation detail
  - 4.2.1 Configuration Multilayer Switch
  - 4.2.2 Layer 2 Switch
- 4.3 Web Server Configuration
- 4.3 Configuration challenges and workarounds

5.0 Features

6.0 Conclusion

7.0 References

8.0 Lesson Learnt

1.0 Overview

1.1 Introduction

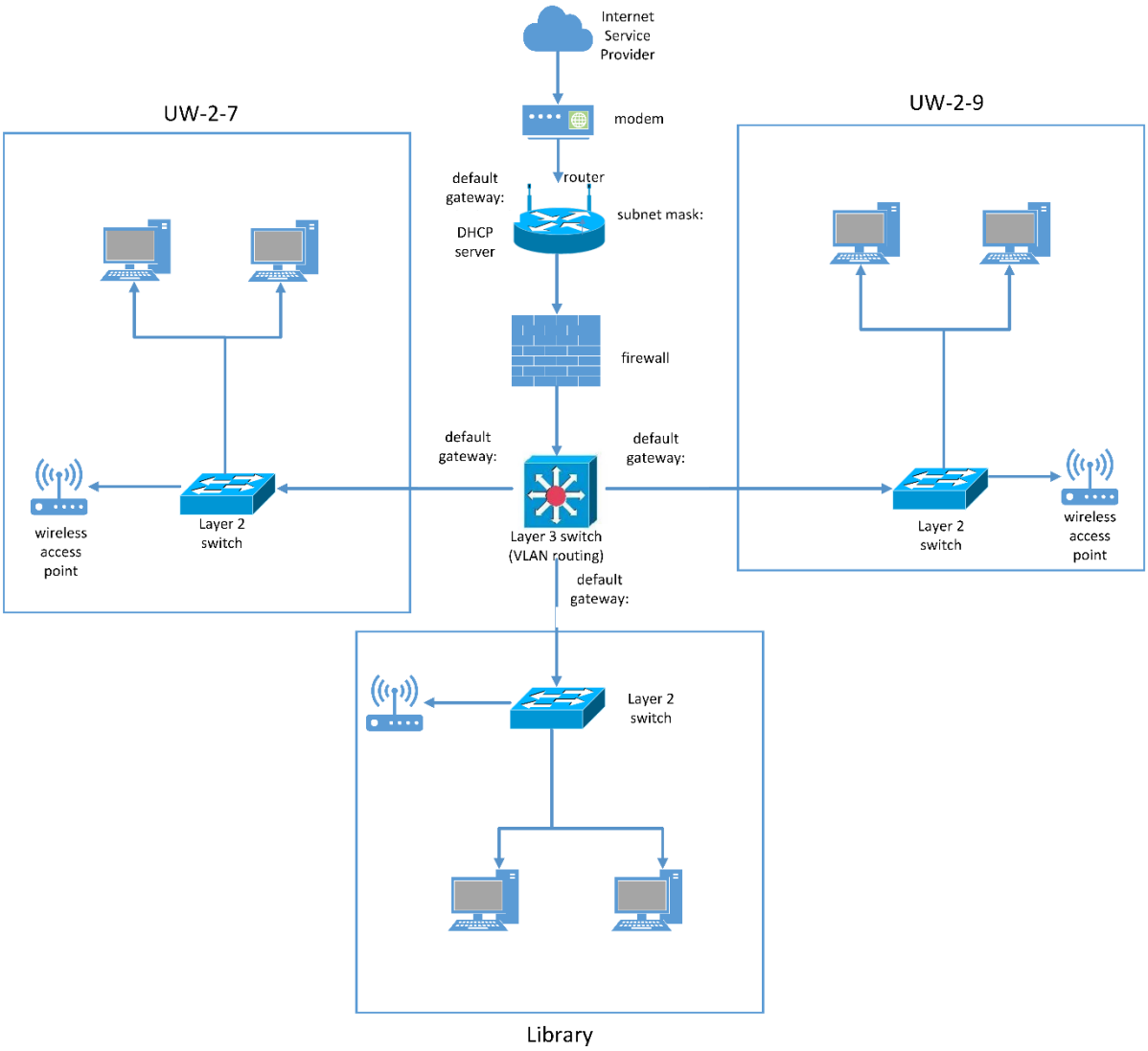
Our team of junior network engineers have been tasked to study, design and configure a Local Area Network (LAN) for Sunway Campus; using the school's current network architecture as a base to give us an idea on how we will design our LAN. Furthermore, we have also been given the opportunity to develop ideas that we could implement into the new network to keep it protected and monitored. Our team will then conduct a presentation on this new network.

1.2 Objectives

For this project, we first will first study and draw a topology of the campus' current network. Next, with the knowledge we gained from the current network, we will design a new LAN that can accommodate four of the university's departments that will be able to be connected to each other and can access simple websites on the Web Server. Finally, we will then come up with suggestions for any safety methods that can be used to protect this new network from attacks while allowing us to easily monitor the system itself to prevent any issues from occurring.

2.0 Implementation Details

2.1 Sunway Network Architecture (IP addresses and subnet masks hidden for privacy purposes)



Explanation

The diagram above illustrates the (simplified) existing architecture of Sunway campus network. The campus network connects to the Internet via a modem, which converts the analog signals from the Internet Service Provider to digital signals for the computers and other devices within the network to understand and receive data from the internet (demodulation). It also converts digital signals to analog signals so end devices can send data to the internet. The modem connects to a router, which forwards data packets between the Sunway campus Local Area Network (LAN) and the Internet. In this case, it functions as a central hub that directs network traffic, facilitating communication between network devices and providing internet access. It is then connected to a firewall, which monitors network traffic that are incoming and outgoing to make decisions on whether to permit or restrict the traffic for security purposes. Next is the multilayer switch, which is essentially a switch with routing capabilities. This means it can make routing decisions based on IP addresses, rather than just forwarding packets based on Layer 2 information such as MAC addresses. In Sunway campus network, the multilayer switch is used for inter-VLAN routing – a process of forwarding networking traffic between different Virtual Local Area Networks. A VLAN is a logical overlay network that isolates the traffic for each set of devices that share a physical

LAN. In Sunway network, we found that the computer labs and library are segmented into different VLANs as the 3 sets of PCs in the three different locations in the diagram have different default gateways (which are configured on the multilayer switch). Without the multilayer switch, the hosts in the many VLANs in Sunway campus would only be able to communicate within their respective networks. Therefore, implementing a multilayer switch connects all VLANs like a central hub to enable sharing data across an expansive campus network. By segmenting smaller networks into VLANs, Sunway network achieves better traffic control, improved performance, subnet separation, and enhanced security. The multilayer switch is then connected to many Layer 2 switches that are located in every floor. Unlike the multilayer switch, the layer 2 switches solely operate on Data Link layer and use MAC addresses to make data forwarding decisions. The layer 2 switches are then connected to the PCs in the computer labs and library. In addition, they are connected to wireless access points which allow Wi-Fi devices such as students' laptops to connect to Sunway campus network. Lastly, all the devices in Sunway campus (except for devices that connect via Wi-Fi) are connected by Ethernet as it is considered faster than wireless connection. Direct wired connections have higher bandwidth capacity, lower latency, and immunity to signal loss than wireless.

Network design

The design of the Sunway Library and Computer Labs network is hierarchal and a combination of both star and bus topology, which consists of the internet service, modem, firewall and layer 3 switches which is the main reason for the star topology. A bus topology is known as a backbone which make devices to connect cables up and down to reach the main cable. The bus topology transport data across the cable and when data arrives at the node, it examines the destination address (MAC/IP address) to see whether it matches their address (GeeksforGeeks, 2020).

The advantage of using a bus topology is because its simplicity. Bus topologies are easy to implement and require less cabling compared to other networking topologies. es. It is simple to add or remove devices from a network without impacting other devices. Most importantly, it is cost-effective, as a backbone is a shared medium, and it is less expensive to set up and maintain. However, the disadvantage of using a bus topology is that he if the backbone is damaged, the whole network is affected. This is why bus topologies are not commonly utilised in modern networking because they are unsuitable for dealing with massive volumes of data (GeeksforGeeks, 2020).

For the multilayer switch in the diagram, it is a star topology. A star topology is linked to a central network device such as a hub, switch, or computer and all the communication between the devices is routed through the hub. The advantage of using a star topology is that it provides higher reliability compared to the bus topology. It only impacted device is affected if a connection breaks, while the remainder of the network remains operational. This fault separation helps to improve the network dependability. Besides, it is also easy to troubleshoot because it only affects specific connections. However, the disadvantage of star topology is that it has a complex installation, when compared to simpler topologies, establishing a star topology may need more planning and installation efforts (GeeksforGeeks, 2020). Additionally, it has a single point of failure where if the central hub goes down, none of the devices in network can forward data packets to each other.

Justification

Library Network (private IP addresses hidden)

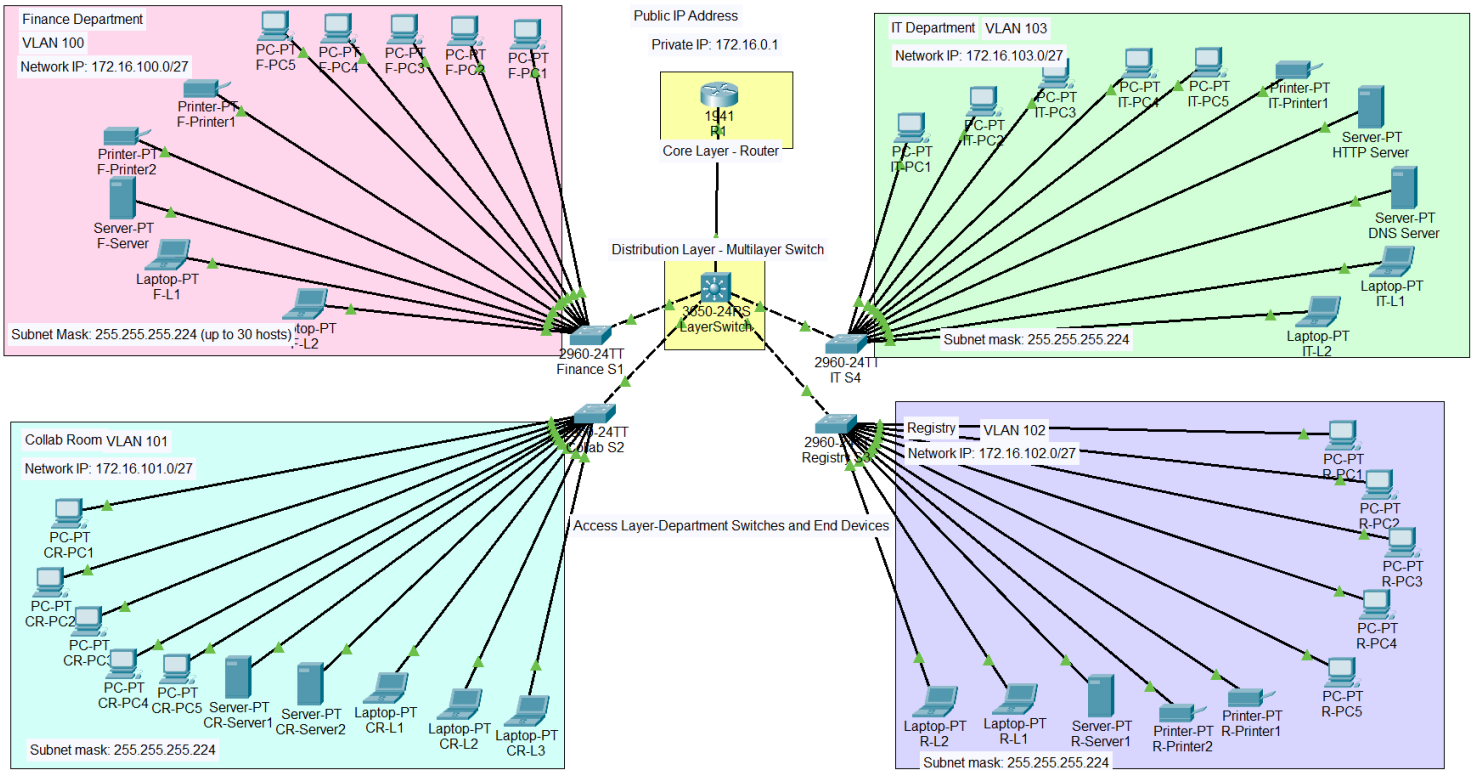
IPv4 Addresses: xxx.xx.xxx.x, xxx.xx.xxx.x
Subnet Mask: xxx.xxx.xxx.x
Default Gateway: xxx.xx.xxx.x

Lab UW-2-7
IPv4 Address: xxx.xx.xxx.xx, xxx.xx.xxx.xx
Subnet Mask: xxx.xxx.xxx.x
Default Gateway: xxx.xx.xxx.x

Lab UW-2-9
IPV4 Addresses: xxx.xx.xxx.xx, xxx.xx.xxx.xx
Subnet Mask: xxx.xxx.xxx.x
Default Gateway: xxx.xx.xxx.x

Screenshots
Library
(screenshots of ipconfig/all, ping, tracert, nslookup for all computers and DHCP server hidden for privacy purposes)

2.2 New Network Design



The new design of the network topology for Sunway Campus is a hierarchal topology. The network is set up in multiple layers (Core, Distribution, Access layer) with each layer serving a specific purpose. The design structures with a router, one layer 3 switch, four layer 2 switches and ten workstations connected to each layer 2 switch, making up a total of 40 workstations in this topology. The core layer includes the router, the distribution layer includes the multilayer switch, and the access layer consists of the department (layer 2) switches and workstations. The above campus network was designed to connect 4 departments: Finance department, Collab Room, Registry, and IT department. All devices are connected by FastEthernet.

The functions of each device is similar to what is already explained for Sunway's campus network. Generally, the router's function is to forward data packets to the intended IP addresses and facilitate communication between networks. The router in this design is to connect the multilayer switch to a device such as a modem to allow access to the Internet. The multilayer switch functions similarly to Sunway's layer 3 switch, which is to perform inter-VLAN routing to allow all the departments that are assigned separate VLANs to share data with each other via routing. The default gateways assigned for each VLAN are also configured in the multilayer switch. The multilayer switch connects to 4 Layer 2 switches dedicated for each department. They operate at Data Link Layer and therefore forward packets to each department based on the end devices MAC addresses and facilitate communication within each separate department.

Additionally, we followed Sunway campus network design by keeping each department in a separate Virtual Local Area Network. There are many benefits to doing this, mainly it allows for logical segmentation of the network, grouping the workstations by functions rather than locations. This provides flexibility in the design of the physical network as it is possible to access the same VLAN from a different floor or building. Another reason

is VLANs isolate network traffic, limiting unauthorized access, makes the management more organized and enhances the security (Williams, 2023). This also allows faster network performance due to reduction in broadcast traffic and optimized bandwidth usage.

Similar to the current network architecture at Sunway Campus, we have chosen to continue using the hierarchical topology approach for our new network design. In this topology, devices are organized in layers, with a core node (typically a router) at the top. This connects to Layer 3 and Layer 2 switches in the distribution and access layers, respectively, which ultimately connect to end devices (such as workstations). This layered structure allows for efficient management, better traffic control, and straightforward scalability.

The hierarchical topology is ideal for a campus network because it supports scalability as you can easily expand the network by adding more switches as new departments are introduced. Each department operates within its own VLAN, ensuring isolation and efficient traffic handling while still being part of the larger network through centralized management. This design allows for better traffic flow and segmentation, making it easier to troubleshoot and maintain.

Lastly, we are using classless IP addressing instead of classful IP addressing, this is to avoid inefficient allocation of IP addresses. For example, class B IP address can handle up to 65,534 hosts with the default subnet mask of /16, but it is far more than enough for our network design since it only consists of four departments with about 10 hosts each. Classless IP solves most of this wastage problem. Finally, we have come up with the subnet mask of /27 which can handle up to 30 usable hosts out of 32 hosts for each department, where the other two hosts are reserved for Network ID and Broadcast ID. This subnet mask provides a more appropriate and efficient allocation of IP addresses for each department within the Sunway campus network.

2.3 Department 1 (Finance Department)

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	172.16.0.1	255.255.255.224	N/A
LayerSwitch	F0/2	172.16.100.1	255.255.255.224	172.16.0.1
Finance-S1	VLAN 100	172.16.100.2	255.255.255.224	172.16.100.1
F-PC1	F0/0	172.16.100.3	255.255.255.224	172.16.100.1
F-PC2	F0/0	172.16.100.4	255.255.255.224	172.16.100.1
F-PC3	F0/0	172.16.100.5	255.255.255.224	172.16.100.1
F-PC4	F0/0	172.16.100.6	255.255.255.224	172.16.100.1
F-PC5	F0/0	172.16.100.7	255.255.255.224	172.16.100.1
F-Printer1	F0/0	172.16.100.8	255.255.255.224	172.16.100.1
F-Printer2	F0/0	172.16.100.9	255.255.255.224	172.16.100.1
F-Server	F0/0	172.16.100.10	255.255.255.224	172.16.100.1
F-Laptop1	F0/0	172.16.100.11	255.255.255.224	172.16.100.1
F-Laptop2	F0/0	172.16.100.12	255.255.255.224	172.16.100.1

Justification

Network Address used: 172.16.100.0/27
Subnets Used: 1
Subnet Mask: 255.255.255.224

The first usable IP is addressed to the LayerSwitch (172.16.100.1).
The second usable IP is addressed to the Finance-S1 (172.16.100.2).
The subsequent IPs are addressed to the workstations connected to the Switch LAN (172.16.100.3 – 172.16.100.12).
This subnet allows for up to 30 usable hosts

Router: xxx.xx.xxx.xx (Public IP Address), 172.16.0.1 (Private IP Address)

2.4 Department 2 (Collab Room)

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	172.16.0.1	255.255.255.224	N/A
LayerSwitch	F0/3	172.16.101.1	255.255.255.224	172.16.0.1
Collab-S2	VLAN 101	172.16.101.2	255.255.255.224	172.16.101.1
CR-PC1	F0/0	172.16.101.3	255.255.255.224	172.16.101.1
CR-PC2	F0/0	172.16.101.4	255.255.255.224	172.16.101.1
CR-PC3	F0/0	172.16.101.5	255.255.255.224	172.16.101.1
CR-PC4	F0/0	172.16.101.6	255.255.255.224	172.16.101.1
CR-PC5	F0/0	172.16.101.7	255.255.255.224	172.16.101.1
CR-Server1	F0/0	172.16.101.8	255.255.255.224	172.16.101.1
CR-Server2	F0/0	172.16.101.9	255.255.255.224	172.16.101.1
CR-Laptop1	F0/0	172.16.101.10	255.255.255.224	172.16.101.1
CR-Laptop2	F0/0	172.16.101.11	255.255.255.224	172.16.101.1
CR-Laptop3	F0/0	172.16.101.12	255.255.255.224	172.16.101.1

Justification

Network Address used: 172.16.101.0/27
Subnets Used: 1
Subnet Mask: 255.255.255.224

The first usable IP is addressed to the LayerSwitch (172.16.101.1).
The second usable IP is addressed to the Finance-S1 (172.16.101.2).
The subsequent IPs are addressed to the workstations connected to the Switch LAN (172.16.101.3 – 172.16.101.12).
This subnet allows for up to 30 usable hosts

Router: xxx.xx.xxx.xx (Public IP Address), 172.16.0.1 (Private IP Address)

2.5 Department 3 (Registry)

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	172.16.0.1	255.255.255.224	N/A
LayerSwitch	F0/4	172.16.102.1	255.255.255.224	172.16.0.1
Registry-S3	VLAN 102	172.16.102.2	255.255.255.224	172.16.102.1
R-PC1	F0/0	172.16.102.3	255.255.255.224	172.16.102.1
R-PC2	F0/0	172.16.102.4	255.255.255.224	172.16.102.1
R-PC3	F0/0	172.16.102.5	255.255.255.224	172.16.102.1
R-PC4	F0/0	172.16.102.6	255.255.255.224	172.16.102.1
R-PC5	F0/0	172.16.102.7	255.255.255.224	172.16.102.1
R-Printer1	F0/0	172.16.102.8	255.255.255.224	172.16.102.1
R-Printer2	F0/0	172.16.102.9	255.255.255.224	172.16.102.1
R-Server1	F0/0	172.16.102.10	255.255.255.224	172.16.102.1
R-Laptop1	F0/0	172.16.102.11	255.255.255.224	172.16.102.1
R-Laptop2	F0/0	172.16.102.12	255.255.255.224	172.16.102.1

Justification

Network Address used: 172.16.102.0/27
Subnets Used: 1
Subnet Mask: 255.255.255.224

The first usable IP is addressed to the LayerSwitch (172.16.102.1).
The second usable IP is addressed to the Finance-S1 (172.16.102.2).
The subsequent IPs are addressed to the workstations connected to the Switch LAN (172.16.102.3 – 172.16.102.12).
This subnet allows for up to 30 usable hosts

Router: xxx.xx.xxx.xx (Public IP Address), 172.16.0.1 (Private IP Address)

2.6 Department 4 (IT Department)

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	172.16.0.1	255.255.255.224	N/A
LayerSwitch	F0/5	172.16.103.1	255.255.255.224	172.16.0.1
IT-S4	VLAN 103	172.16.103.2	255.255.255.224	172.16.103.1
IT-PC1	F0/0	172.16.103.3	255.255.255.224	172.16.103.1
IT-PC2	F0/0	172.16.103.4	255.255.255.224	172.16.103.1
IT-PC3	F0/0	172.16.103.5	255.255.255.224	172.16.103.1
IT-PC4	F0/0	172.16.103.6	255.255.255.224	172.16.103.1
IT-PC5	F0/0	172.16.103.7	255.255.255.224	172.16.103.1
IT-Printer1	F0/0	172.16.103.8	255.255.255.224	172.16.103.1
IT-Server1	F0/0	172.16.103.9	255.255.255.224	172.16.103.1
IT-Server2	F0/0	172.16.103.10	255.255.255.224	172.16.103.1
IT-Laptop1	F0/0	172.16.103.11	255.255.255.224	172.16.103.1
IT-Laptop2	F0/0	172.16.103.12	255.255.255.224	172.16.103.1

Justification

Network Address used: 172.16.103.0/27
Subnets Used: 1
Subnet Mask: 255.255.255.224

The first usable IP is addressed to the LayerSwitch (172.16.103.1).
The second usable IP is addressed to the Finance-S1 (172.16.103.2).
The subsequent IPs are addressed to the workstations connected to the Switch LAN (172.16.103.3 – 172.16.103.12).
This subnet allows for up to 30 usable hosts

Router: xxx.xx.xxx.xx (Public IP Address), 172.16.0.1 (Private IP Address)

3.0 Router

3.1 Overview

Router is a networking device that connects two or more packet-switched networks or subnetworks. A router helps direct data packets to their intended IP address while it can also scan the header of a packet to establish its own destination, then consults the routing table to find the most efficient way to that destination. The packet then subsequently sent to the next network along the route. Our network contains one router.

3.2 Implementation details

3.2.1 Configuration

Step 1 – enable router, configure terminal and host name

```
router>enable
router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#hostname R1
R1(config)#exit
R1#
%SYS-5-CONFIG I: Configured from console by console
```

Step 2 – configure router password

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#no ip domain lookup
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#service password encryption
                ^
% Invalid input detected at '^' marker.

R1(config-line)#service password-encryption
R1(config)#banner motd $ Authorized Users Only!!! $
R1(config)#ex
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

Step 3 – configure router interface and IP addresses

```
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#hostname R1
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#ip add 172.16.0.1 255.255.255.224
R1(config-if)#no sh

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

R1(config-if)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
R1#wr
Building configuration...
[OK]
R1#ping 172.16.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms

R1#
```

3.3 Configuration challenges and workarounds (if any)

There were not much challenges in figuring out how the router is going to access. The process was straightforward.

4.0 Switch

4.1 Overview

Switch is a networking device that joins devices on a network and forward data packets devices such as LAN (Local Area Network). A switch only distributes data to the one destinated device which it is designed and not to networks of numerous devices. Our network design contains 1 multilayer switch and 4 layer 2 switches for each department.

4.2 Implementation details

4.2.1 Configuration Multilayer Switch

Step 1: configure host name

```
switch>enable
switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)#hostname LayerSwitch
LayerSwitch(config)#exit
LayerSwitch#
%SYS-5-CONFIG_I: Configured from console by console
```

Step 2: Configure default gateway to connect to router

```
LayerSwitch>enable
LayerSwitch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
LayerSwitch(config)#ip default-gateway 172.16.0.1
LayerSwitch(config)#exit
LayerSwitch#
%SYS-5-CONFIG_I: Configured from console by console
```

Step 3: Configure IP address and subnet mask for VLAN 1

```
LayerSwitch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
LayerSwitch(config)#int vlan 1
LayerSwitch(config-if)#ip address 172.16.0.1 255.255.255.224
LayerSwitch(config-if)#no shutdown
LayerSwitch(config-if)#exit
LayerSwitch(config)#exit
LayerSwitch#
%SYS-5-CONFIG_I: Configured from console by console
```

Step 4: configure four VLANs hostname and IP addresses

```
LayerSwitch>enable
LayerSwitch#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
LayerSwitch(config)#hostname LayerSwitch
LayerSwitch(config)#vlan 100
LayerSwitch(config-vlan)#name finance
LayerSwitch(config-vlan)#
LayerSwitch(config-vlan)#exit
LayerSwitch(config)#vlan 101
LayerSwitch(config-vlan)#name collab-room
LayerSwitch(config-vlan)#
LayerSwitch(config-vlan)#exit
LayerSwitch(config)#vlan 102
LayerSwitch(config-vlan)#name registry
LayerSwitch(config-vlan)#
LayerSwitch(config-vlan)#exit
LayerSwitch(config)#vlan 103
LayerSwitch(config-vlan)#name IT
LayerSwitch(config-vlan)#
LayerSwitch(config-vlan)#exit
```

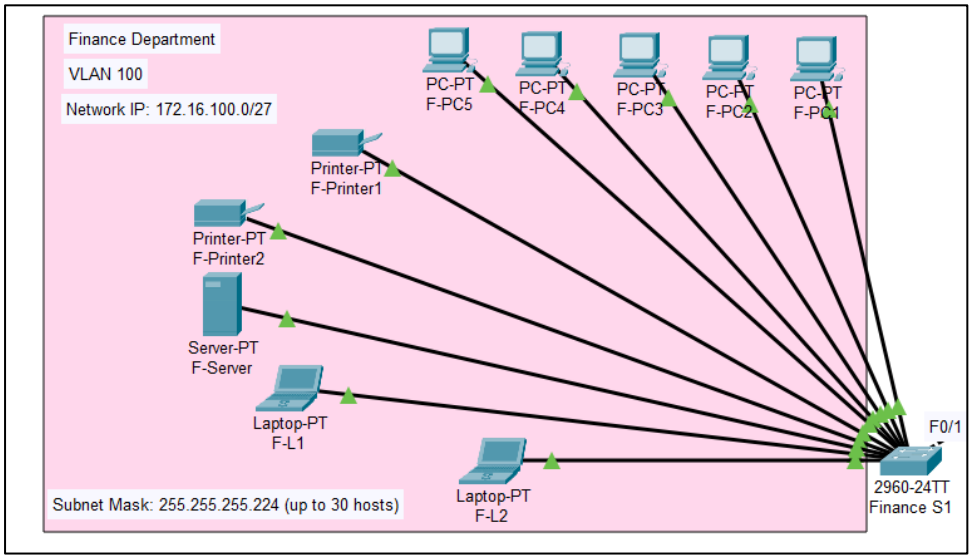
```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 100
Switch(config-vlan)#int vlan 100
Switch(config-if)#ip add 172.16.100.1 255.255.255.224
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#
Switch(config)#vlan 101
Switch(config-vlan)#int vlan 101
Switch(config-if)#ip add 172.16.101.1 255.255.255.224
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#
Switch(config)#vlan 102
Switch(config-vlan)#int vlan 102
Switch(config-if)#ip add 172.16.102.1 255.255.255.224
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#
Switch(config)#vlan 103
Switch(config-vlan)#int vlan 103
Switch(config-if)#ip add 172.16.103.1 255.255.255.224
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

```
Switch#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gig1/0/1, Gig1/0/6, Gig1/0/7, Gig1/0/8
                                                 Gig1/0/9, Gig1/0/10, Gig1/0/11, Gig1/0/12
                                                 Gig1/0/13, Gig1/0/14, Gig1/0/15, Gig1/0/16
                                                 Gig1/0/17, Gig1/0/18, Gig1/0/19, Gig1/0/20
                                                 Gig1/0/21, Gig1/0/22, Gig1/0/23, Gig1/0/24
                                                 Gig1/1/1, Gig1/1/2, Gig1/1/3, Gig1/1/4
100  finance                           active    Gig1/0/2
101  collab-room                       active    Gig1/0/3
102  registry                          active    Gig1/0/4
103  IT                                active    Gig1/0/5
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
100  enet  100100     1500  -      -      -        -    -        0      0
101  enet  100101     1500  -      -      -        -    -        0      0
102  enet  100102     1500  -      -      -        -    -        0      0
103  enet  100103     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

```
Switch>enable
Switch#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1/0/1   unassigned      YES NVRAM  up                    up
GigabitEthernet1/0/2   unassigned      YES NVRAM  up                    up
GigabitEthernet1/0/3   unassigned      YES NVRAM  up                    up
GigabitEthernet1/0/4   unassigned      YES NVRAM  up                    up
GigabitEthernet1/0/5   unassigned      YES NVRAM  up                    up
GigabitEthernet1/0/6   unassigned      YES NVRAM  down                  down
GigabitEthernet1/0/7   unassigned      YES NVRAM  down                  down
GigabitEthernet1/0/8   unassigned      YES NVRAM  down                  down
GigabitEthernet1/0/9   unassigned      YES NVRAM  down                  down
GigabitEthernet1/0/10  unassigned      YES NVRAM  down                  down
GigabitEthernet1/0/11  unassigned      YES NVRAM  down                  down
GigabitEthernet1/0/12  unassigned      YES NVRAM  down                  down
GigabitEthernet1/0/13  unassigned      YES NVRAM  down                  down
GigabitEthernet1/0/14  unassigned      YES NVRAM  down                  down
GigabitEthernet1/0/15  unassigned      YES NVRAM  down                  down
GigabitEthernet1/0/16  unassigned      YES NVRAM  down                  down
GigabitEthernet1/0/17  unassigned      YES NVRAM  down                  down
GigabitEthernet1/0/18  unassigned      YES NVRAM  down                  down
GigabitEthernet1/0/19  unassigned      YES NVRAM  down                  down
GigabitEthernet1/0/20  unassigned      YES NVRAM  down                  down
GigabitEthernet1/0/21  unassigned      YES NVRAM  down                  down
GigabitEthernet1/0/22  unassigned      YES NVRAM  down                  down
GigabitEthernet1/0/23  unassigned      YES NVRAM  down                  down
GigabitEthernet1/0/24  unassigned      YES NVRAM  down                  down
GigabitEthernet1/1/1   unassigned      YES NVRAM  down                  down
GigabitEthernet1/1/2   unassigned      YES NVRAM  down                  down
GigabitEthernet1/1/3   unassigned      YES NVRAM  down                  down
GigabitEthernet1/1/4   unassigned      YES NVRAM  down                  down
Vlan1                  172.16.0.1      YES manual up                    up
Vlan100                172.16.100.1    YES manual up                    up
Vlan101                172.16.101.1    YES manual up                    up
Vlan102                172.16.102.1    YES manual up                    up
Vlan103                172.16.103.1    YES manual up                    up
```

4.2.2 Layer 2 Switches

1. Finance department switch



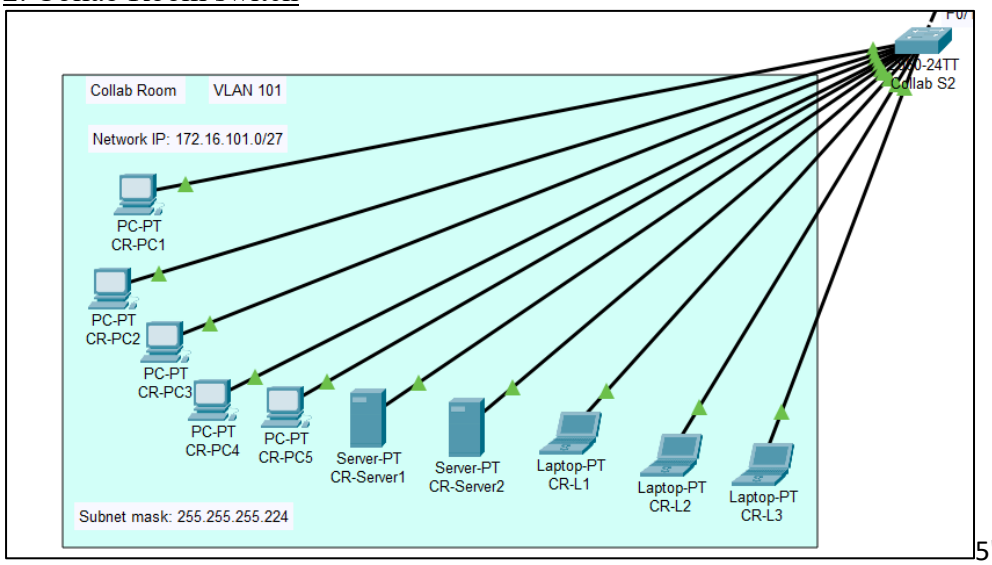
Configuration - Finance Switch

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Finance-S1
Finance-S1(config)#exit
Finance-S1#
%SYS-5-CONFIG_I: Configured from console by console
```

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int range f0/2-11
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 100
% Access VLAN does not exist. Creating vlan 100
Switch(config-if-range)#do wr
Building configuration...
[OK]
```

```
Switch(config)#int f0/1
Switch(config-if)#switchport mode access
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (1), with Switch
GigabitEthernet1/0/2 (100).

Switch(config-if)#switchport access vlan 100
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

2. Collab Room switch



5"

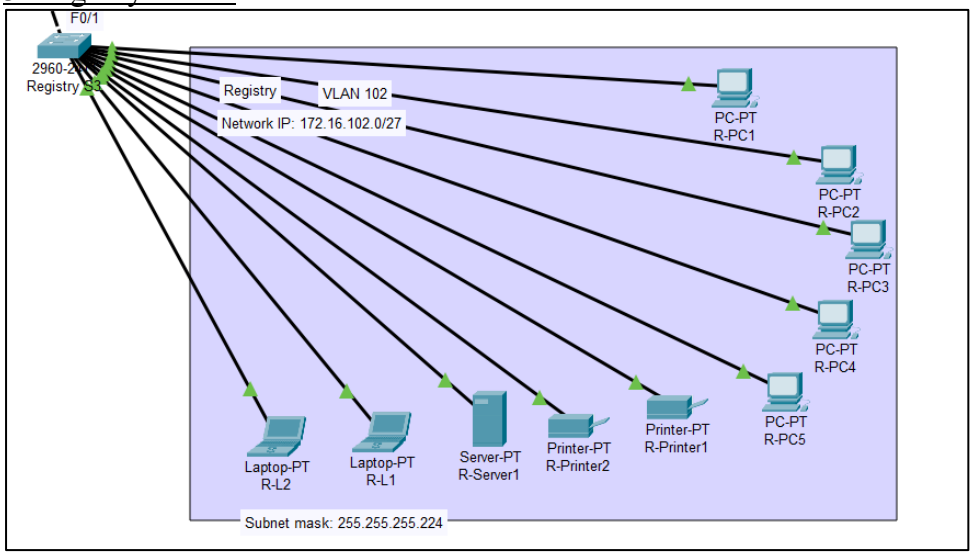
Configuration – Collab Room Switch

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Collab-S2
Collab-S2(config)#
Collab-S2(config)#exit
Collab-S2#
%SYS-5-CONFIG_I: Configured from console by console
```

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int range f0/2-11
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 101
% Access VLAN does not exist. Creating vlan 101
Switch(config-if-range)#do wr
Building configuration...
```

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int f0/1
Switch(config-if)#switchport mode access
Switch(config-if)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (1), with Switch
GigabitEthernet1/0/3 (101).

Switch(config-if)#switchport access vlan 101
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

3. Registry switch



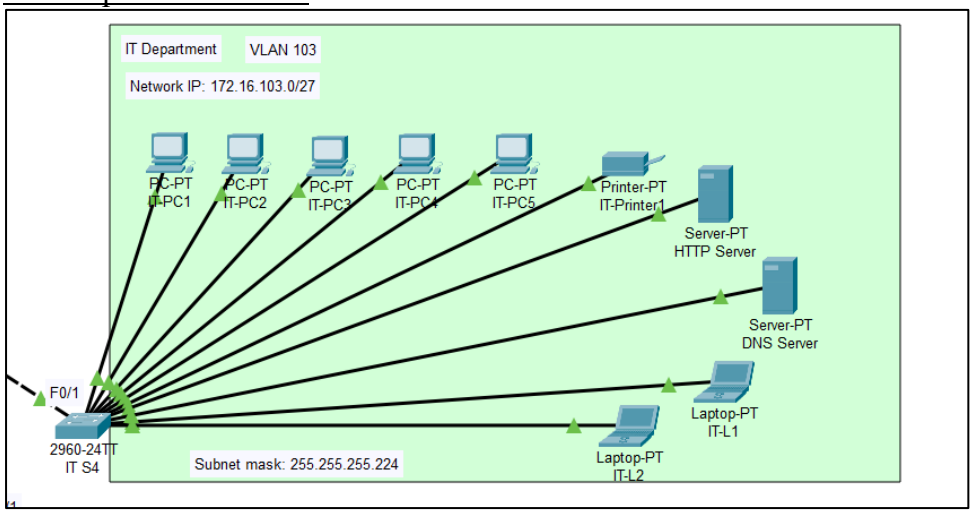
Configuration – Registry Switch

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Registry-S3
Registry-S3(config)#exit
Registry-S3#
%SYS-5-CONFIG_I: Configured from console by console
```

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int range f0/2-11
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 102
% Access VLAN does not exist. Creating vlan 102
Switch(config-if-range)#do wr
Building configuration...
[OK]
```

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int f0/1
Switch(config-if)#switchprt
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (1), with Switch
GigabitEthernet1/0/4 (102).

                          ^
% Invalid input detected at '^' marker.

Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 102
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

4. IT department switch



Configuration – Registry Switch

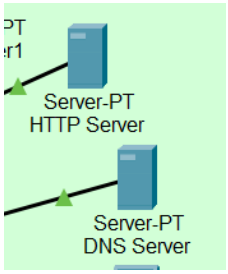
```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname IT-S4
IT-S4(config)#exit
IT-S4#
%SYS-5-CONFIG_I: Configured from console by console
```

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int range f0/2-11
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 103
% Access VLAN does not exist. Creating vlan 103
Switch(config-if-range)#do wr
Building configuration...
[OK]
```

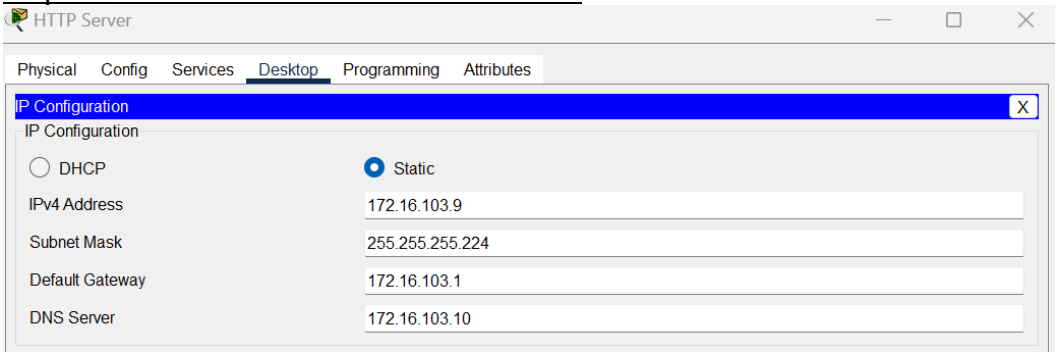
```
Switch>enable
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (1), with Switch
GigabitEthernet1/0/5 (103).

Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int f0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 103
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

4.3 Web server configuration

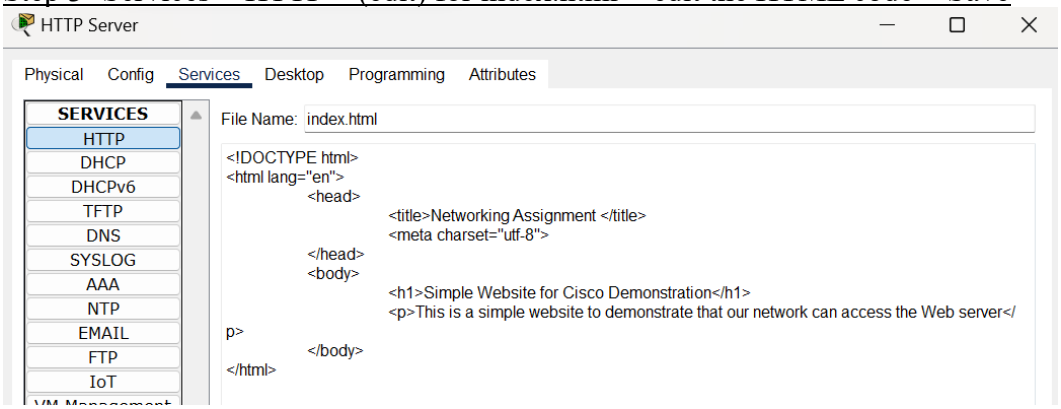
Step 1 - To configure web server, we use the two servers (HTTP and DNS) in the IT department.



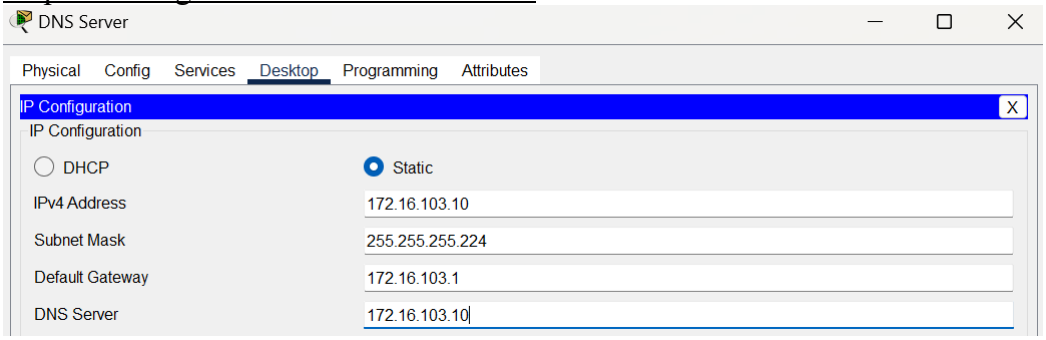
Step 2 – Put DNS IP address in HTTP Server



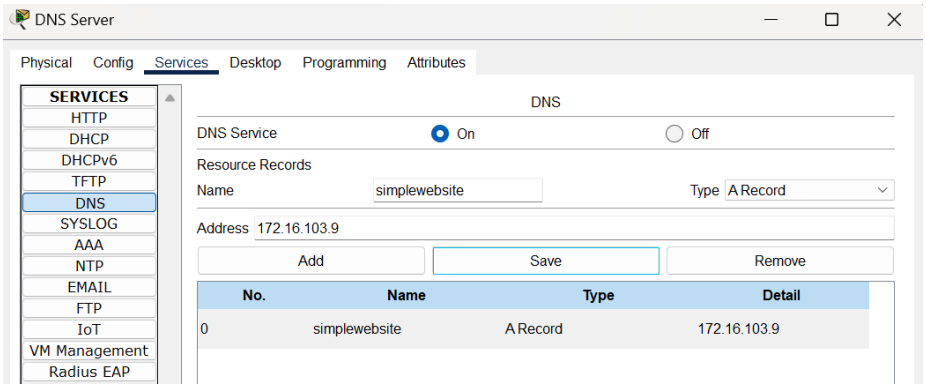
Step 3- Services > HTTP > (edit) for index.html > edit the HTML code > Save



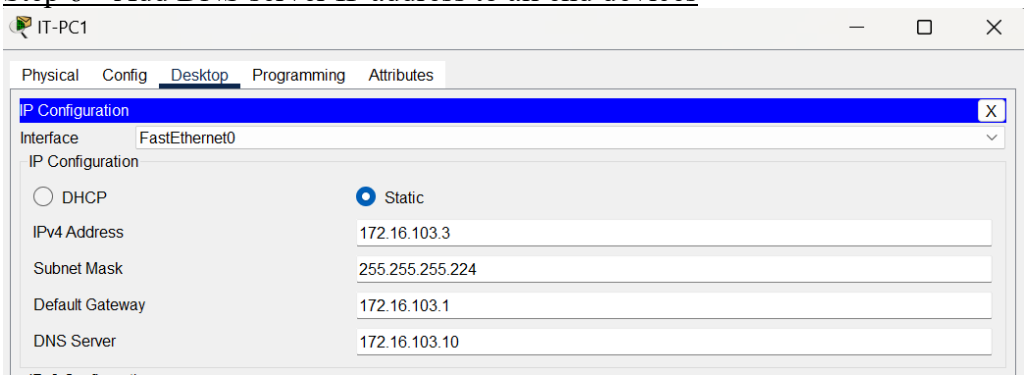
Step 4- Configure DNS Server IP address



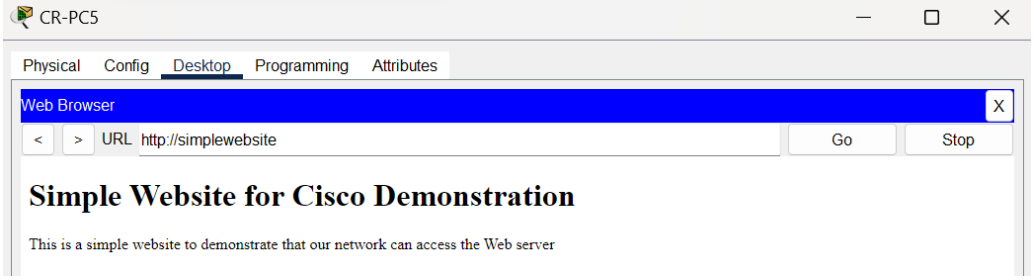
Step 5- Go to Services > DNS > turn on DNS Service > enter domain name and IP address of HTTP Server > Add



Step 6 – Add DNS server IP address to all end devices



Step 7-Enter domain name or web server IP address into URL search bar in PC desktop



4.4 Configuration challenges and workarounds (if any)

We found that configuring the multilayer switch was the most complex and tedious process. This is because in addition to connecting it to the router, we had to configure 4 VLAN interfaces together with their corresponding IP addresses. In our design, the multilayer switch was the most important it is used as a central hub for inter-VLAN routing to allow the different departments to share data with one another. Without it, each department can only communicate within itself and cannot access the web server hosted within the IT department. To solve this issue, we heavily referred on the IP addressing table that we constructed to ensure we have configured the setup correctly and used ping commands to check if PCs from one department can send packets to all the different departments.

Another challenge was configuring the Web server, as it required additional but crucial understanding of the protocols used for surfing the web. In our case, two notable ones were HTTP and DNS. It took some research to figure out how to host a web server in Cisco and the implementation of it required a bit of basic HTML to code a simple website.

5.0 Features

We can use a variety of security mechanisms to monitor network and system activity for malicious activities, policy violations or security breachers. These are some methods can guard our network and identify prospective assaults. Antivirus XDR (Extended Detection and Response), MDR (Managed Detection and Response), packet sniffing, anti-DDoS (Distributed Denial of Service), Intrusion Detection System (IDS), and Intrusion Prevention System (IPS).

Antivirus XDR solutions offer a secure environment. When potential dangers or malicious acts are recognised, Antivirus XDR gives real-time alerts and notifications. These notifications, which provide rapid visibility into suspicious activities, security administrators can respond fast and limit risk. The system may also respond to recognised hazards automatically, such as isolating affected endpoints or terminating malicious processes. A centralised console or dashboard that provides security administrators with a complete picture of the network and system environment. Because of this centralised visibility, security events, threats, and activities can be monitored and managed from a single interface.

Antivirus MDR solutions provide round-the-clock network and system security monitoring. Highly qualified security analysts actively monitor the environment for potential threats and security issues, frequently working for a Managed Security Service Provider (MSSP). This ongoing observation ensures rapid identification and reaction to security events. Antivirus MDR combines powerful threat detection technology and continuous monitoring. It gives business advantages of specialised security support and enhanced defences against sophisticated and developing cyberthreats.

Moreover, packet sniffing also known as network sniffing or packet analysis is a method for identifying and observing packet data as it travels through a network. It entails catching and looking at data packets that are being sent between network devices. Unauthorised access attempts like brute-force attacks, password sniffing, or unauthorised login attempts, can be detected by packet sniffing. Security administrators can identify and address any authorised access occurrences by looking at packet headers and recording login or authentication attempts.

Furthermore, a physical barrier between potential attackers and your network is created by anti-DDoS. DDoS attack mitigation is a feature of anti-DDoS solutions. In order to stop malicious traffic from reaching its intended target, they use a variety of techniques, including traffic redirection, rate restriction, traffic shaping, and the application of access control policies. They safeguard network and system resources by actively blocking or rerouting attack traffic, ensuring that genuine traffic can continue without interruption.

In addition, IDS is a hardware or software that monitors a network for malicious activity or policy violations. When suspicious activity is found, IDS delivers immediate alerts and notifications. Security administrators or a Security Operations Centre (SOC) receive these notifications which allowing them to react quickly to possible security incidents. IDS notifications contain details about the activity that was discovered, the affected hosts and the threat's severity. IDS is a passive security tool that scans packet headers, payloads, and other network data for indications of potential security breaches or malicious activity. IDS detects suspicious activity and issues alerts, but it does not actively work to thwart or lessen risks. Its

primary objective is detection, producing alerts that security officers can utilise to investigate further and take action.

On the other hand, IPS goes a step further by actively blocking or mitigating detected threats in real time. Firewalls with IDS/IPS capabilities provide an additional layer of security monitoring, helping detect and prevent network-based attacks. In order to identify and stop potential security risks, IPS continuously monitors network traffic and analyses it in real time. It examines packets, protocols, and application specific information to spot well-known attack signatures, malicious activity, or unusual behaviour. The IPS immediately acts to block or neutralise threats when they are identified, preventing them from reaching their target. IPS is a system that combines intrusion detection and prevention capabilities. It not only fins and warns of prospective security incidents, but also actively prevents or lessens them. This proactive response reduces the impact on network and system security by assisting in the prevention of successful assaults.

While IPS combines detection with prevention capabilities, actively blocking or reducing identified threats, IDS focuses on detection and alerting, providing insights into possible security issues. IDS and IPS both play significant roles in network security monitoring, although they differ on their response strategies. To achieve thorough threat detection and prevention, organisations frequently use both IDS and IPS as complimentary elements of their entire network security strategy.

6.0 Conclusion

In conclusion, our group has successfully designed a network from our analysis of Sunway's existing network architecture. With extensive research and team cooperation, we were able to design a simple LAN that is scalable and effective and can serve as a foundation in real world network design. Besides the physical connection of network devices, it is important to consider factors such as security, flexibility and performance when designing a network solution. By implementing VLANs and adopting classless IP addressing, we achieved better security, optimized network traffic control, and efficient allocation of IP addresses.

7.0 References

Aarness, A. (2023, February 6). *What is Endpoint Detection & Response? | EDR Security Definition*. Crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/#:~:text=Endpoint%20Detection%20and%20Response%20(EDR)%2C%20also%20referred%20to%20as

Alto, P. (n.d.). *What Is XDR?* Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-xdr

Check Point. (n.d.). *What is an Intrusion Detection System (IDS)?* Check Point Software. https://www.checkpoint.com/cyber-hub/network-security/what-is-an-intrusion-detection-system-ids/#:~:text=An%20Intrusion%20Detection%20System%20(IDS)%20is%20a%20monitoring%20system%20that

Cisco. (n.d.). *What Is XDR? - Extended Detection and Response*. Cisco. https://www.cisco.com/c/en/us/products/security/what-is-xdr.html#:~:text=Extended%20detection%20and%20response%20(XDR)%20delivers%20visibility%20into%20data%20across

ComputerNetworkingNotes. (2019, August 29). *Network Topologies Explained with Examples*. ComputerNetworkingNotes; ComputerNetworkingNotes. https://www.computernetworkingnotes.com/networking-tutorials/network-topologies-explained-with-examples.html

GeeksForGeeks. (2020, November 20). *Advantages and Disadvantages of Star Topology*. GeeksforGeeks.

https://www.geeksforgeeks.org/advantages-and-disadvantages-of-star-topology/

GeeksforGeeks. (2020, November 1). *Advantages and Disadvantages of Bus Topology*. GeeksforGeeks.

https://www.geeksforgeeks.org/advantages-and-disadvantages-of-bus-topology/

Graham-Smith, D. (2023b, February 7). Five reasons why Ethernet is better than Wi-Fi. ITPro. Retrieved July 15, 2023, from https://www.itpro.com/infrastructure/network-internet/369978/ethernet-vs-wifi-why-ethernet-is-better

Imperva. (n.d.). *Anti-DDoS Services | Instant Protection, Free Trial | Imperva*. Learning Center.

https://www.imperva.com/learn/ddos/anti-ddos-protection/

NETSCOUT. (n.d.). *What is packet sniffing?* NETSCOUT.

https://www.netscout.com/what-is/sniffer

Networks, A. (2021, July 27). *Classful and Classless Addressing Explained | Auvik*. Auvik Networks Inc. https://www.auvik.com/franklyit/blog/classful-classless-addressing/#:~:text=At%20a%20high%20level%2C%20classless

Slattery, T., & Burke, J. (2022, June 3). VLAN (virtual LAN). Networking. Retrieved July 15, 2023, from https://www.techtarget.com/searchnetworking/definition/virtual-LAN

VMWare. (2021, December 22). *What is Intrusion Prevention System? | VMware Glossary*. VMware.

https://www.vmware.com/topics/glossary/content/intrusion-prevention-system.html

Williams, L. (2023). What is VLAN? Types, Advantages, Example. *Guru99*.

https://www.guru99.com/vlan-definition-types-advantages.html

8.0 Lesson Learnt

Yap Jay Ann 21024765

As someone who majorly contributed to this assignment as the group leader, I can confidently say that this assignment has significantly enhanced my understanding of networking from a practical standpoint. Firstly, I learned how to obtain information about an existing network through the command line. Before this, I had never contemplated the inner workings of our campus network. Exploring Sunway's network using commands like "ipconfig," "ping," and "tracert" allowed me to visualize the network topology and obtain a clearer comprehension of the design choices behind a large-scale Local Area Network. Furthermore, I took on the responsibility of designing the proposed network for this assignment. I realized that designing a network is much more complex than simply connecting devices with the correct cables, in the correct ports. I have done weeks of research on concepts such as IP Addressing, VLANs, subnets, and protocols to ensure that we were able to implement an effective network that suits the case scenario given. Additionally, I learned how to implement the network I designed in Cisco Packet Tracer by cabling the devices in the correct interfaces and configuring the components. I believe this

was the hardest part of the assignment as I, together with 2 group members, had spent countless hours and stayed up for several nights going through many trials and errors trying to configure the devices, particularly the multilayer and layer 2 switches. Despite the major challenges we faced, we managed to connect all the devices and access a simple website hosted on a web server. Lastly, this challenging assignment has made me step up my leadership skills. I tried my best to be responsible by planning meetings in advance, doing extensive research before our meetings so I could explain to my fellow group members, planning the parts of the report and distributing the work to ensure the project gets done on time. Despite starting fairly early and finishing on time, I believe we would have less unnecessary stress if every member were equally proactive and put in similar amounts of effort, instead of leaving the heavy lifting to a few and only asking about the assignment when nearing the deadline.