

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**SCHOOL OF SCIENCE AND TECHNOLOGY**

**COURSEWORK FOR THE BIS, BCNS, BIT, BCS, BSDA, BSE, YEAR 1**

**ACADEMIC SESSION April 2023; SEMESTER 3**

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

**STUDENT NAME: Law Rou Rou, Lee Xing Le, Liew Jieh Cheng, Tee Yu Chen, Yen Ming Wey**

**NRIC/PASSPORT NO: 030804-08-0550, 031112-10-0834, 031201-10-2129,030123-01-0741, 030223-14-1255**

**Group no: 26**

**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 Law Rou Rou, Lee Xing Le, Liew Jieh Cheng, Tee Yu Chen, Yen Ming Wey (student name). 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 signature / Date)



….................................. (Student’s signature / Date)



A black background with a black square

Description automatically generated ….................................. (Student’s signature / Date)



….................................. (Student’s signature / Date)



….................................. (Student’s signature / Date)



1. **Campus network**

**1.1 Overview**

A diagram of a computer network

Description automatically generated

Diagram: Existing network topology of Computer Labs and Library

To find out the current existing network architecture of computer labs and library in Sunway University, our team first finds the ip address of the computers in the library and computer labs by typing in the command line “ipconfig /all” into the Command Prompt of those PCs. After knowing these, we need to ping the PCs from a library PC to a computer labs PC and from a computer labs PC to a library PC. We have confirmed that all the pinging procedures have been completed successfully, indicating that the connections between them have been established effectively. In order to find out how they are connected, we used the “tracert” command which shows that all of the computers only visit the default gateway router, meaning that the computers in computer labs and library are part of the same Local Area Network (LAN). However, this only finds the routing processes to and from the library PC and computer labs PC. Therefore, we also ping and trace the PCs within the library and each computer lab respectively. As a result, they can directly communicate with each other without the need to go through any default gateway router.

Furthermore, all devices in both the libraries and labs have unique IP and MAC addresses, ensuring proper identification and communication within the network. During a physical inspection, it was observed that the Ethernet cables are connected either in a bus configuration, where they connect to a main cable on the ground that leads to the switch, or in a star configuration, where the cables are directly connected to the switch.

**A computer screen with white text

Description automatically generatedLibrary Computers Pings**

A computer screen with white text

Description automatically generatedA computer screen with white text

Description automatically generated A computer screen with a black screen

Description automatically generatedA computer screen with white text

Description automatically generated A computer screen with white text

Description automatically generated

A computer screen with a black screen

Description automatically generated A computer screen with white text

Description automatically generatedA screen shot of a computer

Description automatically generated

In the library, the computers (B1, G) in the library have the same IP host portion (172.19.222), subnet mask (255.255.255.0), and default gateway (172.19.222.1), indicating that they are in the same subnet. This information was obtained using the command 'ipconfig /all'. The IP address range for the library is specified as 172.19.222.1 – 172.19.222.255, based on the subnet mask of 255.255.255.0. Additionally, the library printers reside in a separate subnet with an IP range of 172.18.230.0 and a subnet mask of 255.255.255.0.

**Labs Computers Pings**

A computer screen with white text

Description automatically generated A screenshot of a computer

Description automatically generatedA computer screen shot of a computer screen

Description automatically generated A computer screen with white text and black text

Description automatically generatedA computer screen with white text

Description automatically generated A computer screen with white text

Description automatically generatedA computer screen with white text

Description automatically generated A computer screen with white text

Description automatically generated A screen shot of a computer

Description automatically generated A computer screen with white text

Description automatically generated

In the computer labs, each lab has a different IP host portion (e.g., 172.19.217, 172.19.219, 172.19.210) while having the same subnet mask of 255.255.255.0 but different default gateways. This indicates that each lab is in a different subnet. The IP address range for Lab A is specified as 172.19.217.1 – 172.19.217.255 based on the subnet mask of 255.255.255.0. Similar IP ranges can be determined for the other labs.

**Tracert From Lab to Library**

**A computer screen with white text

Description automatically generated with low confidenceA picture containing text, screenshot, operating system, software

Description automatically generatedTracert From Lab A to Lab B**

**Tracert Within a Single Lab**

A computer screen with a black and white text

Description automatically generated**A computer screen shot of a computer

Description automatically generated with low confidence**

**Tracert From Library to Lab**

When tracing the route from the library to the labs, from one lab to the others, or from a lab to the library, only the default gateway router is visited. This indicates that they are connected through the same router. However, each lab and the library have different gateways, suggesting that the router connecting them utilizes multiple interfaces and sub interfaces to create multiple subnets. This can be achieved by implementing VLANs for each interface on a switch and connecting multiple VLANs to one router using a trunk port.

Tracing the route among devices within the same lab reveals that they can directly find each other without passing through the router, suggesting connectivity through switches or direct cable connections. However, when tracing the route between different labs, devices need to pass through their respective default gateways to reach the target device, indicating that they are in different subnets.

**Design for new network**

**A computer network diagram with many computers

Description automatically generated**

(Clearer image on the last page)

After having a thorough investigation of the existing campus network, we identified areas for improvement and gained valuable insights. Drawing from this knowledge, we designed a new network by incorporating things that we learned from our research. We have learnt about the strengths of utilizing technology such as segmenting LAN into VLANs, implementing a router-on-stick configuration and using access ports and trunk ports of a switch in our design.

In addition, we explored alternative approaches such as dividing a large LAN into smaller LANs using multiple routers. However, we discovered that routers are significantly more expensive than switches and that the routing capacity of a single router is not fully utilized. On the contrary, employing a router-on-stick configuration allows us to efficiently utilize the existing network architecture while achieving superior performance in segmenting department networks. Moreover, this configuration offers greater scalability for future network changes, as adjustments can be easily made.

Besides, we explored the possibility of using fiber optic instead of Ethernet for the switch, such as adding a fiber optics module in the switch-PT. However, we encountered a limitation with this approach as the maximum number of ports supported by fiber optic switches was only 9, which falls short of the minimum requirement of 10 workstations in a department. Consequently, the use of additional switches became necessary, resulting in higher costs and reduced scalability compared to the 2960 model which provides 20 ethernet ports.

As a result, we made the decision to employ the router-on-stick configuration as the backbone of the network. Each department is segmented into VLANs using the dedicated 2960 switch, which connects to separate sub interfaces on the central router serving as the default gateway. To gather all the VLANs, a trunk switch is implemented with a trunk port that enables connectivity to the central router. Additionally, we have incorporated a web server within one of the VLANs in the network.

**2.0 Router**

**2.1 Overview**

The design utilizes a central router to control LAN traffic and establish connectivity to the internet. The GigabitEthernet0/0 interface of the router is connected to the LAN of the departments while GigabitEthernet0/1 interface is connected to the ISP. The routing is achieved by connecting the GigabitEthernet0/0 interface (LAN) to the GigabitEthernet0/1 interface (internet) of the router. To serve as default gateways for each department's VLAN, four sub interfaces are configured on the GigabitEthernet0/0 interface. The respective default gateway IP addresses are as follows:

GigabitEthernet0/0.1 for the Finance department: 172.19.219.1

GigabitEthernet0/0.2 for the Registry department: 172.19.220.1

GigabitEthernet0/0.3 for the HR department: 172.19.221.1

GigabitEthernet0/0.4 for the IT department: 172.19.222.1

All these sub interfaces have a subnet mask of 255.255.255.0.

For GigabitEthernet0/1 that acts as the outer interface that connects to the internet, the public IP address is given as 113.23.128.82 with a subnet mask of 255.255.128.0.

**2.2 Design purpose**

The purpose of this design, from a technical and resource management perspective, is to establish an efficient and centralized network architecture that enables effective traffic control, resource allocation, and management within the LAN environment.

First, precise control and routing of LAN traffic can be achieved by only utilizing a central router. The router serves as a traffic controller, directing data packets between VLANs and managing the flow of information within the network. This facilitates optimized network performance and ensures efficient utilization of available bandwidth.

Besides, the central router enables connectivity between the LAN and the internet. By connecting the LAN to the GigabitEthernet0/1 interface of the router, the design establishes a gateway for accessing external networks and internet services. This ensures that users within the LAN can visit online webpages and communicate with other devices on the internet.

To improve scalability of the network, sub interfaces are used instead of adding multiple physical interfaces on a router. Sub-interfaces allow for the virtual segmentation of a physical interface into multiple logical interfaces, each representing a separate VLAN or network. This approach simplifies network expansion as additional VLANs can be easily accommodated without the need for additional physical interfaces. By leveraging sub-interfaces, it minimizes the complexity of managing multiple physical interfaces on the router such as cabling and the limitations of space for ports to be installed. The implementation of sub interface optimizes the utilization of hardware resources. This is because it eliminates the need for dedicating separate physical interfaces for each VLAN. By efficiently allocating resources, university can maximize the utilization of their router hardware, reduce power consumption, and minimize the physical footprint of the network infrastructure. As a result, the cost for building and maintaining the network infrastructure is reduced.

In conclusion, this network design emphasizes efficiency and resource management by utilizing a centralized router, sub-interfaces, and VLANs. The design enables precise traffic control, optimized resource allocation, and simplified network scalability. Overall, this design promotes a robust and cost-effective network architecture that efficiently manages resources and ensures optimal performance within the LAN environment.

**2.3 Configuration details**

**A picture containing headphones, screenshot

Description automatically generated**

Establish a console connection between the switch and a PC using a serial cable. Proceed by accessing the switch's terminal. Gain privileged EXEC mode by executing the 'enable' command, followed by entering the configuration terminal using the 'configuration terminal' command.

A screenshot of a computer program

Description automatically generated

The router is configured with no ip domain lookup to tell the router not to search for any wrong words typed in the CLI. The password of “cisco” is set for the change from User EXEC mode to Privileged EXEC mode. Consequently, we set the configuration line and telnet access line with the password “cisco”. Then, the password is encrypted using the “service password-encryption” command line. A banner that warns of unauthorized access is prohibited is also configured. All this running configuration is set as the startup-configuration.

**2.3.1 Outer interface configuration**

A picture containing text, screenshot, font, line

Description automatically generated

A public IP address is configured to allow the devices in the LAN to communicate with external networks. The interface of GigabitEthernet0/1 is accessed with the command “interface G0/1”. Then, the command “ip address 113.23.128.82 255.255.128.0” is used to set the IP address and subnet mask for the interface. Then, the state of interface is changed to up to activate the interface. After these configurations, the devices in the LAN should be able to send data to any other LANs as long as they are connected to the internet.

**2.3.2 Sub interface configuration**

A screenshot of a computer code

Description automatically generated with low confidence

Diagram: Configuration for finance department

A picture containing text, screenshot, font, line

Description automatically generated

Diagram: Configuration for registry department

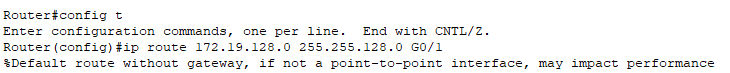
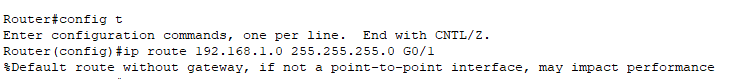
In the configuration terminal, command "interface G0/0.1" is used to access the sub interface of GigabitEthernet0/0. Dot1Q encapsulation is then applied to the incoming data from the finance department's access switch using the command "encapsulation dot1Q 1". The IP address of the sub interface is configured as 172.19.219.1 with a subnet of 255.255.255.0, and the sub interface is activated with the "no shutdown" command. Similarly, to configure a sub interface for registry, interface G0/0.2 is activated when accessing into the interface. Another encapsulation is enforced by using the same encapsulation method for VLAN 2 (encapsulation dot1Q 2). The default gateway Ip for this department is set as 172.19.220.1 with a subnet mask of 255.255.255.0. Finally, “no shutdown” command is used, ensuring that the sub interface is in the activated state.

Generally, the configuration can be applied to the HR and IT departments according to the following steps:

1. Access the configuration terminal and enter the router's interface configuration mode.
2. To configure a sub interface for the respective department, use the command "interface G0/0.X" where "X" represents the appropriate sub interface number.
3. Apply Dot1Q encapsulation to the incoming data from the department's access switch using the command "encapsulation dot1Q Y", where "Y" denotes the corresponding VLAN number for the department.
4. Configure the IP address for the sub interface using the command "ip address A.B.C.D subnet-mask", where A.B.C.D represents the desired IP address and subnet-mask is the appropriate subnet mask for the department.
5. Activate the sub interface using the "no shutdown" command to ensure it is in an operational state.
6. Verify the configuration by checking the IP addresses, encapsulation settings, and activation status of the sub interfaces.

By following these configuration steps, sub interfaces can be configured for each department, applying Dot1Q encapsulation and assigning unique IP addresses to facilitate communication and routing between VLANs. The activation of the sub interfaces and configuration of default gateways ensure proper connectivity and access to external networks.

**2.4 Routing configuration**



To establish a connection between the campus router and the ISP network, it is necessary to configure the routing table of both routers using a static routing protocol. The initial step involves configuring the campus network router to incorporate the ISP network into its routing table. This can be achieved by accessing the configuration terminal. Assuming that the network address of the ISP router is 192.168.1.0, with a subnet mask of 255.255.255.0, the following command is used: "ip route 192.168.1.0 255.255.255.0 GigabitEthernet0/1". This command specifies the route to the ISP network.

Next, we need to configure the ISP router to facilitate routing to the campus network. Due to the presence of multiple VLANs within the campus network, it is not feasible to configure routing for a specific VLAN alone. As a solution, we assign the routing IP address as 172.19.128.0, with a subnet mask of 255.255.128.0. By doing this, any network falling within this range can be effectively routed.

To locate the ISP server from one of the workstations in the campus network, we can use the "tracert" command. This command will provide a result displaying both routers in the network path.

A screenshot of a computer

Description automatically generated

**2.5 Connectivity and inter-VLAN routing test**

As VLANs are implemented on all departments, each department will have its own default gateway even if they connect to the same router.

Finance Department PC to its default gateway

A screenshot of a computer

Description automatically generated with medium confidence

Ping is successful from Finance department PC to its default gateway. This proves that the router is connected to the devices in the finance VLAN.

Registry Department PC to its default gateway

A screenshot of a computer program

Description automatically generated with medium confidence

Ping is also successful from registry department PC to its default gateway. Thus, connection is successfully established between the PC and the router.

From 1 department to another

A screen shot of a computer

Description automatically generated with low confidence

To test the inter-VLAN routing capability of the router, the tracert command is performed from the finance department PC to the registry department PC. From the result, the first device is the router, and the second device is the targeted PC in the registry department. When the ICMP data is sent by the finance department PC, the switch cannot find the targeted device as they are not in the same subnet. Thus, it sends the data to the default gateway which is the first device shown in the list. Then the router routes the data to the VLAN of the targeted device as the VLAN is configured as one of the sub interfaces. Finally, the data successfully reaches the targeted device.

**3.0 Switch**

**3.1 Overview**

This network design incorporates inter-VLAN routing to facilitate communication between different departments within an organization. The design consists of four switches for each of the departments: Finance, Registry, HR, and IT, along with a trunk switch responsible for interconnecting the VLANs.

The switches for each department are configured with distinct IP addresses to enable communication within their respective VLANs. The IP addresses assigned to the switches are as follows:

Finance switch: 172.19.219.2

Registry switch: 172.19.220.2

HR switch: 172.19.221.2

IT switch: 172.19.222.2

To facilitate inter-VLAN routing, a dedicated trunk switch is employed. This switch acts as a central hub, connecting all VLANs within the network. The trunk switch is configured with multiple VLANs and their corresponding IP addresses:

VLAN1 for Finance department: 172.19.219.3

VLAN2 for Registry department: 172.19.220.3

VLAN3 for HR department: 172.19.221.3

VLAN4 for IT department: 172.19.222.3

All switches, including the trunk switch, use a subnet mask of 255.255.255.0.

**3.2 Design purpose**

The reason for using this design is to create logical separation and secure communication between different departments while allowing them to communicate when necessary. Each department is assigned a separate VLAN, which helps in enhancing network security by isolating traffic between departments. Inter-VLAN routing enables communication between VLANs, allowing the departments to share resources and collaborate effectively.

The trunk switch acts as a central point for the VLANs, allowing traffic to flow between them. By configuring the trunk port between the trunk switch and the router, the network enables communication between the VLANs and the external network, ensuring connectivity to the internet and other external resources.

In terms of scalability, if there are additional devices within the same department that need to join the network, they can easily join by connecting to the department's switch. If the available switch ports are fully utilized, the network can be expanded by adding additional switches, which can be connected to the trunk switch and configured with the appropriate VLAN settings. Similarly, when a new department is established, a dedicated switch can be installed for that department. By connecting the new switch to the trunk switch and configuring a new VLAN specifically for the department, connectivity can be established seamlessly.

Overall, this design ensures efficient and controlled network communication by utilizing VLANs and inter-VLAN routing. It provides flexibility and scalability in network management, enhances security by isolating traffic, and enables efficient utilization of network resources.

**3.3 Configuration details**

**3.3.1 Trunk switch configuration**

A screenshot of a computer

Description automatically generated with low confidence

To begin, establish a console connection between the switch and a PC by utilizing a serial cable connected to the RS232 port. Privileged EXEC mode is entered by executing the 'enable' command, followed by entering the configuration terminal using the 'configuration terminal' command. The interface vlan 1 is accessed by the command 'interface vlan 1'. The IP address of vlan 1 is set to 172.19.219.3 with a subnet mask of 255.255.255.0 using the command 'ip address 172.19.219.3 255.255.255.0'. The vlan 1 is turned on by utilizing the 'no shutdown' command. Similarly, for vlan 2, the configuration for the IP address 172.19.220.3 is done.

A number on a white background

Description automatically generated

Now, the trunk switch has two VLANs set. By default, VLAN 1 is assigned to all interfaces on the switch. Therefore, the interface connecting to the finance department does not require configuration since the finance department utilizes VLAN 1. However, it is necessary to switch the registry department's interface to VLAN 2.

To accomplish the VLAN switch for interface F0/2, which is connected to the registry department’s switch, the interface is accessed and the command "switchport mode access" is utilized to ensure the port operates in access mode rather than trunk mode. Subsequently, the command "switchport access vlan 2" is used to change the F0/2 interface to VLAN 2.

A white background with black text

Description automatically generated

Finally, the interface that is connected to the router(G0/1) should be configured. In order for the router to be reached by all VLANs, the mode of this port needs to be set to trunk mode. The command "switchport mode trunk" can be used to accomplish this.

**3.3.2 Finance Department switch configuration**



Establish a console connection between the switch and a PC using the serial cable. The switch has been assigned the hostname 'finance'. Proceed by accessing the switch's terminal. Gain privileged EXEC mode by executing the 'enable' command, followed by entering the configuration terminal using the 'configuration terminal' command. The switch's hostname is set as 'finance'.

A screen shot of a computer

Description automatically generatedA black screen with white text

Description automatically generatedA screenshot of a computer screen

Description automatically generated A computer screen shot of white text

Description automatically generated

Subsequently, we configure the terminal password as “cisco” and disable domain-lookup to prevent unwanted DNS lookup. A MOTD banner is also configured to warn about unauthorized access. To restrict the console port access and enable Telnet access, a password is configured to both. We then save the running-config as the startup-config.

A screen shot of a computer

Description automatically generated with medium confidence



The interface of VLAN 1 is accessed at the configuration terminal. This is achieved by executing the command "interface vlan 1". Subsequently, the switch's IP address is set as 172.19.212.2 with a subnet mask of 255.255.255.0 using the command "ip address 172.19.219.2 255.255.255.0". The "no shutdown" command is used to ensure that VLAN 1 transitions to an active state. The default gateway of the switch is also set as the ip address of the router by the command “ip default-gateway 172.19.219.1”.

**3.3.3 Registry Department switch configuration**

A black text on a white background

Description automatically generated with low confidence A number on a white background

Description automatically generated

The switch of the registry department is also consoled in the same manner as the previous configuration. The hostname is configured as 'registry'. Access is made to the interface of VLAN 2, and the IP address is set as 172.19.220.2 with a subnet mask of 255.255.255.0. The state of the interface is enabled by utilizing the 'no shutdown' command. The default gateway IP is configured as 172.19.220.1.

**3.3.4 Other Departments switch configuration.**

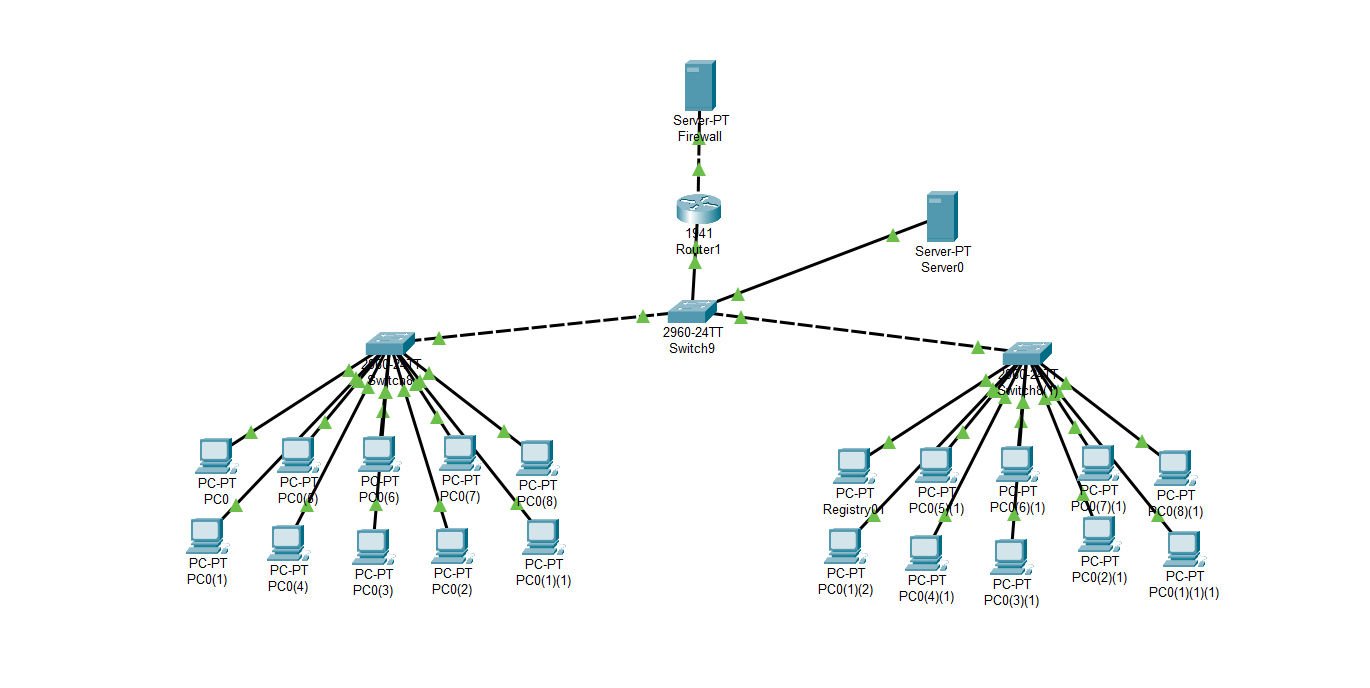


Diagram: Topology of two departments configured

Similar to the Finance and Registry departments, the other departments (HR and IT) in the organization follow a similar configuration approach to enable inter-VLAN routing and establish communication within their respective VLANs.

General switch configuration steps:

1. Establish a console connection between the switch and a PC using a serial cable.
2. Set the hostname of the switch to a descriptive name.
3. Enter privileged EXEC mode by executing the 'enable' command.
4. Enter the configuration terminal using the 'configuration terminal' command.
5. Access the interface of VLAN X by executing the command "interface vlan X”.
6. Set the IP address of the switch to a unique address within the corresponding department's subnet, along with the appropriate subnet mask.
7. Enable the interface by using the 'no shutdown' command.
8. Configure the default gateway IP as the IP address of the router to enable connectivity to external networks.
9. Repeat the above steps for each department's switch, assigning unique IP addresses within their respective VLANs.
10. Configure the trunk switch by assigning IP addresses to each VLAN used in the network.
11. Configure the interfaces connecting to other switches as access ports using the "switchport mode access" command and assign a respective VLAN for the access port.

By following this configuration approach, the HR and IT departments are now equipped with their respective VLANs, IP addresses, and default gateways. These configurations allow for secure communication within their departments and inter-VLAN routing through the trunk switch.

**3.4 Connectivity test for switch**

A picture containing text, screenshot, font

Description automatically generated

Ping is successful from Finance department PC to finance department switch.

A picture containing text, screenshot, font

Description automatically generated

Ping is successful from Finance department PC to trunk switch. This shows that the PC in the VLAN can connect to the trunk switch.

A screenshot of a computer program

Description automatically generated with low confidenceA screenshot of a computer

Description automatically generated with medium confidence

Ping is successful from Finance department PC to Registry department switch. This shows that the PC is able to connect to the switch in a different VLAN. However, the PC cannot directly connect to the switch without passing through the router (172.19.219.1) as shown in the diagram above. Hence, the traffic between VLAN is separated logically but connection can still be established.

**4.0 Features**

**Workstations**

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

The workstations in each department are connected to the switch in a star topology. Each department has 10 workstations. The workstations in the departments are configured as follows:

Finance department workstations IP range: 172.19.219.11 - 172.19.219.20, default gateway IP: 172.19.219.1

Registry department workstations IP range: 172.19.220.11 - 172.19.220.20, default gateway IP: 172.19.220.1

HR department workstations IP range: 172.19.221.11 - 172.19.221.20, default gateway IP: 172.19.221.1

IT department workstations IP range: 172.19.222.11 - 172.19.222.20, default gateway IP: 172.19.222.1

All of them have a subnet mask of 255.255.255.0.

The workstations in one department can directly find each other. However, they cannot directly communicate with the workstations in another department as they are logically separated by VLANs. A router is needed to direct the traffic for the communication between VLANs.

A screen shot of a computer

Description automatically generated with low confidence

Diagram: Tracert result from finance department workstation to registry department workstation

**Servers**

A server is installed in the network to accommodate HTTP, DNS and FTP service. The IP address is configured as 172.19.198.11 with a subnet mask of 255.255.255.0 using the same method as the configuration of workstations. A new VLAN is also configured on the switch for this network and sub interface of GigabitEthernet0/0.5 is added in the router.

**Web server**

A web server for the campus is set up for both the LAN and the users from the external network to access.

A screenshot of a computer

Description automatically generated

To enable the web service on the server, the ‘services’ panel is accessed. Then, the HTTP and HTTPS services are switched to ‘On’ state. Now, all the workstations in the network are able to access the website hosted on this server by typing in the IP address of the web server in the web browser.A screenshot of a computer

Description automatically generated

**DNS server**

In order to enable convenient access for users to the web server, a DNS server is implemented on the same server device. To configure the DNS server, the service is enabled in the services panel. The IP address of the server is entered, and the domain name is set as ‘campus’.

A screenshot of a computer

Description automatically generated

Now, by adding the ip address of the DNS server in the workstations, it allows the workstations to visit the web page by simply typing <http://campus> in their web browser as the DNS server will resolve the domain name to the IP address of the web server.

A screenshot of a computer

Description automatically generated

**FTP server**

FTP service is also provided by the server device to facilitate file transferring between departments. A username and password are set, and the permission can also be specified based on the requirements and restrictions of the departments. To access the FTP file storage, the command “ftp campus” is used. After the login credentials are entered, the user will be able to log in. Several commands such as uploading files – “put” and downloading files – “get” can be utilized to enhance the efficiency of file transferring process between departments.

A screenshot of a computer

Description automatically generated A screenshot of a computer

Description automatically generated

**Security mechanism**

In order to monitor networks and systems for malicious activities, we will implement an Intrusion Detection System and Prevention System (IDPS), which is a combination of Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) in our network topology. The main objective of IDPS, alongside additional security software or systems, is to protect the computer networks. IDPS security functions as a supplementary line of defense against attack when implemented with authorization and verification restriction strategies. For each individual device in a network, firewalls and antivirus or malware software are normally deployed, but as the network expand, more unidentified devices, such as wireless devices and USB storage devices that enter the system may cause an issue to the security of the network. An entire network cannot be completely safeguarded from assault by firewalls and anti-malware software on its own because they play a little role in the overall security mechanism. Therefore, an intrusion detection system is intended to apply to our newly created network system to alert the security team for investigation if it detects any suspicious activities. IDPS can obtain the activities of the system and use the information collected through previously established trends to identify when an attack occurs or offer descriptions and evaluation of how an attack occurred, such as by observing network connections while tracking activities for malicious behavior or violations of policies. This can be extremely helpful to determine what intrusions have already occurred or were treated as attempted in the past to prevent attacks in the future.

Intrusion detection software (IDS) consists of two major types, which are the Network Intrusion Detection System (NIDS), and Host Intrusion Detection System (HIDS). In order to secure environments where traffic is probably to be vulnerable to attack, a Network Intrusion Detection System (NIDS) is often spread across a network or installed at critical nodes. It actively monitors network traffic moving across the network nodes where it is placed. They can be reasonably simple to safeguard and hard for intruders to find. Therefore, a potential attacker might not be aware that the NIDS has picked up on their possible attack. The advantages are that they can analyze all inbound and outbound traffic, detect events in real-time that allow for quick response times and are more challenging for an intruder to detect. On the other hand, A Host Intrusion Detection System (HIDS) focuses on the protection of an individual host or device such as a server. HIDS works by comparing snapshots of the current state of system files and compare it with its previous state to detect any changes made to it. When it detects any suspicious activities or instructions, it will send an alert to the administrator while providing information about the affected files to carry out a thorough investigation on the issue.

Consequently, we will also implement an Intrusion prevention system (IPS) into our network topology that works alongside the IDS. Since IDS can only detect malicious activity in the network, IPS plays the role of actively preventing and blocking these intrusions in the network. The immediate action taken by an IPS when discovering possible threat includes discarding of malicious packet and termination of connection to prevent threat from reaching its intended target.

There are two types of detection methodology used for detection, which are Signature-based detection and Anomaly-Based detection. Signature-based detection deals with known types of attack or malicious activities by comparing it with the database system. If the attack pattern matches with the database, it will generate an alert that indicates security threat. However, since it relies heavily on known attacks in the database, it will not be able to identify new threats since they do not have known signature. Thus, the Anomaly-Based detection system comes in place. An Anomaly-Based detection uses machine learning to create a model for a “normal” behavior. Any deviation from the norm is identified as an anomaly and flagged for immediate alerting. Although anomaly-Based detection works well on zero-day attacks, it is more prone to generate a false positive alert. Thus, the IDPS uses both Signature-Based detection and Anomaly-based detection to strengthen the protection.

In short, the Intrusion Detection System and Prevention System (IDPS) can act as a security mechanism that protects our newly designed network from the attack.

**5.0 Lesson Learnt**

After completing this assignment, we as a group understand the importance of having a well-designed network topology that can aid in sending information across the internet. A good network design should consider various factors including optimal performance, cost-effectiveness, complexity, scalability, security, and data protection. In most cases, designing an ideal network topology will greatly depend on the requirements and demand of each customer. A balance between needs analysis, technology design and cost assessment are needed to design an ideal network for each situation.

Consequently, through the usage of cisco packet tracer, we learnt the importance of having a well-defined plan and documentation before starting the configuration process. The importance of understanding the connectivity requirements of each device plays a crucial part in connecting the correct devices together. Moreover, we learnt that the process of segmenting LAN into multiple VLAN is essential in designing our network because it helps in improving the performance of the network as it can reduce the broadcasting traffic and improves the network efficiency. In addition, VLAN also helps enhance the security mechanism of the network as sensitive data can be isolated to prevent unauthorized access from the data. The logical groupings of VLAN also provides scalability to the network design as new devices can be added into the network by just configuring a new VLAN, which eases the process of network expansion in the future.

Working in a group, we understand the importance of having effective communication between every group member to facilitate a smooth completion on the assignment given. We should always harness various opinions from each member to gain valuable insights to generate innovative ideas and solutions for the project. Furthermore, distributing responsibility among group members is crucial to ensure the participation of every member in this collective learning process throughout the assignment.

A computer network diagram with a few computers connected to each other

Description automatically generatedA diagram of a computer network

Description automatically generatedA diagram of a router

Description automatically generated