

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

**SCHOOL OF SCIENCE AND TECHNOLOGY**

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

**ACADEMIC SESSION DEC 2018; SEMESTER 2**

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

**STUDENT NAME: THAM JIAN HAO, LIM XIWEI, LAI LI XUAN, NG JIA WEN,**

**THAM ROU YI**

**NRIC/PASSPORT NO: 030208140131, 030802140580, 020925120708, 020610101078, 030109100900**

**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.

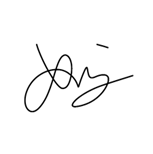
**IMPORTANT**

# 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 THAM JIAN HAO, THAM ROU YI, LIM XIWEI, LAI LI XUAN, NG JIA WEN (Name) 21042692, 21024161, 21045596, 22089148, 21057146 (std. ID) received the assignment and read the comments.



30/6/2023 30/6/2023 30/6/2023 30/6/2023 30/6/2023



(Signature/date)

**Academic Honesty Acknowledgement**

“I **THAM JIAN HAO, THAM ROU YI, LIM XIWEI, LAI LI XUAN, NG JIA WEN** (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.”



A black background with a black square

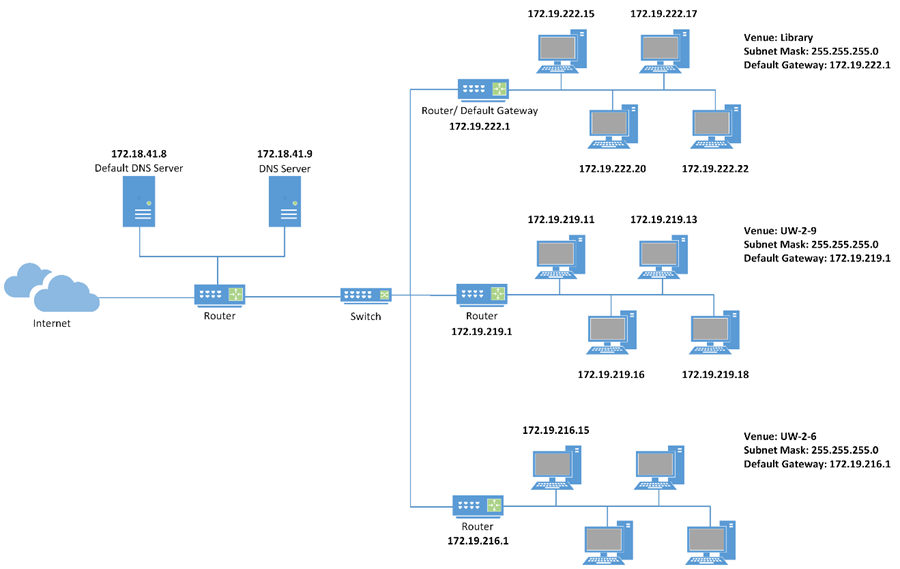
Description automatically generated 30/6/2023 A signature on a white background

Description automatically generated with medium confidence30/6/2023 30/6/2023 30/6/2023 30/6/2023



(Student’s signature / Date)

1. **Existing Campus Network**

****

**Figure 1.** Existing Network Architecture

Based on our findings, the main router connecting the Internet to our campus network serves as an intermediary gateway between the external and internal networks. The main router is assigned a public IP address by the Internet Service Provider (ISP) and has a private IP address that is used within the local network. Other devices within the network will only have a private IP address. Through network diagnostic commands like ping and tracert, we discovered that our campus network utilizes a Class B private IP address range, specifically ranging from 172.16.0.0 to 172.31.255.255. However, during our research, we encountered some inconsistencies regarding the default subnet mask for Class B addresses. According to standard classful addressing, the default subnet mask for Class B should be 255.255.0.0 instead of the 255.255.255.0 subnet mask displayed in Figure 3. Nevertheless, we concluded that the campus network’s IP addresses still fall within the Class B address range but are being utilized with a specific subnet configuration.

**A screenshot of a computer

Description automatically generated**

**Figure 2.** nslookup Result

During our preliminary investigations, we discovered the IP address (172.18.41.8) of the Domain Name System (DNS) server connected to our campus network. However, further investigations in Figure 3 revealed that every computer in the library and computer labs is linked to two different DNS servers. Interestingly, we noticed that one of the IP addresses coincided with the IP address obtained in Figure 2. As a result, we deduced that there are two DNS servers connected to the main router.

The main router is then connected to the switch before being connected to the LANs encompassing the computer labs and library. This configuration ensures proper network segmentation, centralizes the location of the DNS server, and makes it easily accessible to all devices within these LANs. Initially, we used bridges to connect the LANs. However, after conducting research, we discovered that switches provide the same functionality with greater efficiency. While bridges connect smaller network segments to form a more extensive network and relay frames from one LAN to another, switches can connect more network segments compared to bridges. Considering the number of computer labs on our campus, we decided to replace the bridges with switches to ensure optimal network performance.

Moving forward, based on our investigations and conversations with the IT staff, we determined that the topology for the computer labs and library is a bus topology. This choice was made considering factors such as cost, ease of maintenance, and the absence of hubs in the computer labs and library. Moreover, the absence of additional IP addresses representing central nodes like routers, hubs, or switches when using the tracert command between PCs within the same room suggests that a star topology can be ruled out (Figure 3). Thus, the bus topology aligns with the network configuration of the computer labs and library, offering an efficient and practical solution. We further ascertain that each computer lab and the library operate as an individual bus topology, as illustrated in Figure 1.

**A computer screen with white text

Description automatically generated**

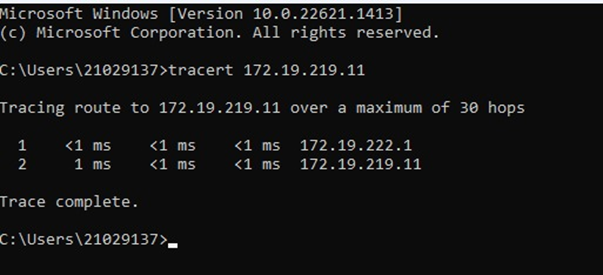
**Figure 3.** Library Sending Device ipconfig and tracert Result

A screenshot of a computer program

Description automatically generated

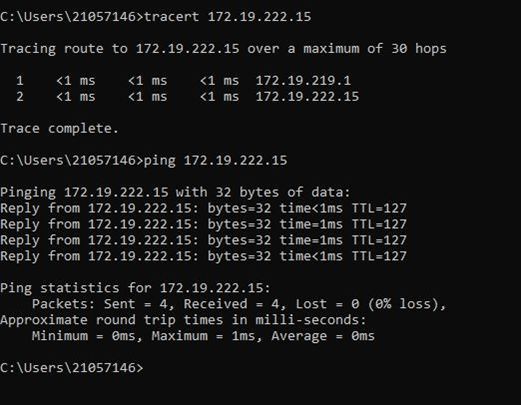
**Figure 4.** Library Sending Device ping Result

By utilizing the ipconfig /all command, we successfully obtained the subnet mask (255.255.255.0) and the IP address of the default gateway (172.19.222.1) for the library (Figure 3). Moreover, it is evident from Figure 3 that the sending device in the library possesses the IP address 172.19.222.15. Furthermore, we were able to determine the IP addresses of the other three computers through the ping results (Figure 4). Additionally, by employing the tracert command, we discovered that the route from the library computer (172.19.222.15) to a computer (172.19.219.11) located in the UW-2-9 computer lab traverses through a router, as shown in Figure 5.

****

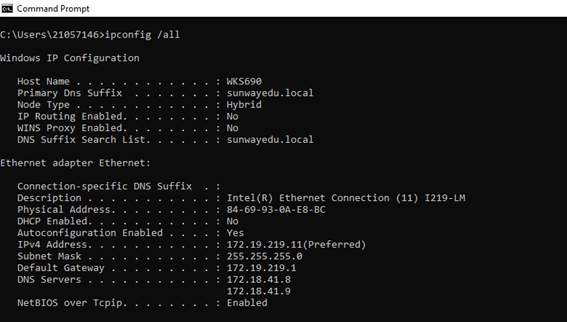
**Figure 5.** Library to UW-2-9 Computer Lab tracert Result

Interestingly, it is evident that the router address coincides with the default gateway address (172.19.222.1). This correlation is further substantiated when conducting a tracert from the UW-2-9 computer lab to the library (Figure 6).

****

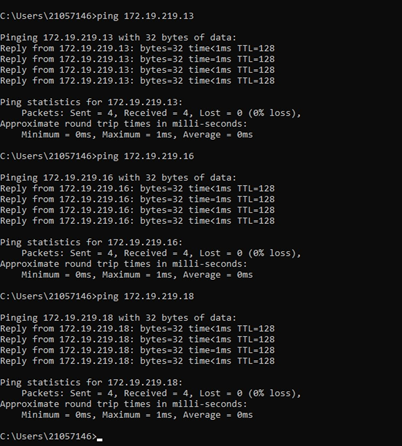
**Figure 6.** UW-2-9 to Library tracert and ping Result

Figure 6 shows that the route from the UW-2-9 computer lab to the library passes through the router located in UW-2-9 (172.19.219.1), which is the same IP address as the default gateway address of UW-2-9 (Figure 7).

****

**Figure 7.** UW-2-9 Lab Sending Device ipconfig Result

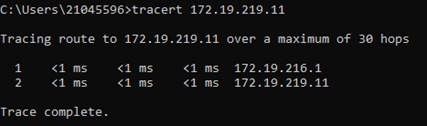
Furthermore, we obtained the IP addresses of the other three computers through the ping results, as illustrated in Figure 8.

****

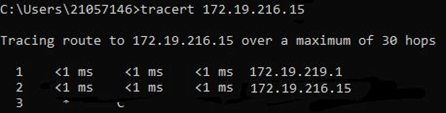
**Figure 8.** Computers within UW-2-9 Lab ping Result

Throughout our investigations, we were dumbfounded by the absence of the main router and receiving lab’s router IP addresses when using the tracert command. Our research indicated that tracert relies on Internet Control Message Protocol (ICMP) Time Exceeded messages for tracing routes. With that said, some routers are specifically configured not to disclose their IP addresses in the ICMP Time Exceeded messages. Such measures are implemented for security purposes to prevent potential attackers from obtaining excess information on the network topology. As a result, when using the tracert command, only the IP addresses of sending routers will be displayed, which indicates that the packets have successfully reached the receiving router and are being forwarded towards their destination.

Building upon our observations, we formulated a hypothesis suggesting that each lab possesses its own router. To validate this hypothesis, we analysed the evidence presented in Figure 9 and Figure 10, and our hypothesis was confirmed to be true.

****

**Figure 9.** UW-2-6 to UW-2-9

****

**Figure 10.** UW-2-9 to UW-2-6

1. **Campus Network Design**

**A diagram of a computer network

Description automatically generated**

**Figure 11.** New Campus Network Overview

* 1. **Overview**

**Router-on-a-Stick Technique**

Our network architecture encompasses three buildings: Sunway University, Sunway College, and Sunway International School. These buildings house four departments: Human Resources, Finance, Registry, and Marketing. To achieve logical segmentation, we have implemented VLANs, enabling us to isolate network traffic and categorize devices into distinct virtual networks based on their department or purpose. Each department is assigned its respective VLAN: Finance (VLAN 11), Human Resources (VLAN 12), Registry (VLAN 13), and Marketing (VLAN 14).

To address the communication needs between VLANs, we employ a technique called Router-on-a-Stick. This technique allows VLANs to communicate using a single physical interface on the main router. Sub-interfaces are configured on the main router's interface, with each sub-interface corresponding to a specific VLAN. Unique VLAN IDs are assigned to these sub-interfaces to differentiate traffic from different VLANs. By implementing this method, we achieve efficient traffic routing between VLANs without requiring separate physical interfaces for each VLAN on the router. This approach optimizes resource utilization and simplifies network management.

In our network setup, devices within each department of a building are connected to department switches. These department switches are then connected to a distribution switch, which serves as the central point of connectivity. The distribution switch is further connected to the main router, which is responsible for routing traffic between the department VLANs and other networks or to the internet. This arrangement creates a hierarchical network architecture. In addition, the distribution switch is connected to a syslog server, which acts as a centralized repository for collecting log messages from various devices and systems. The syslog server plays a crucial role in the Intrusion Prevention System (IPS) by providing network administrators with a centralized location for monitoring and analysing network logs.

The devices in each department, like printers and computers, form the access layer. They are connected to switches, which act as the distribution layer. These switches are then connected to the central distribution switch, which acts as the central point of connectivity within the distribution layer. At the core layer, we have the main router, which serves as the backbone of the network and houses the Internet gateway. This architecture enables inter-VLAN communication and ensures connectivity between VLANs belonging to various departments across the three buildings.

**Internet Connectivity**

The main router connects to the ISP using a Digital Subscriber Line (DSL) connection to establish Internet connectivity. The DSL modem converts digital signals between our network and the DSL line. It is connected to a cloud-based service that symbolizes the Internet in this context, providing access to various resources hosted online. Outside our local network, we have a border or ISP router that handles traffic routing between our network and the ISP network, enabling us to connect to the Internet.

An aggregation switch connects the Internet router to two servers. One of these servers hosts the website www.sunway.com with the IP address 10.10.10.10, where user requests from our network will be routed to this web server to retrieve content from this website. Additionally, we have a DNS server responsible for translating human-readable domain names into IP addresses that computers can understand. We have opted to utilize Google's DNS service for resolving domain names. To achieve this, we have assigned the IP address 8.8.8.8 as our DNS server, as it specifically belongs to Google's public DNS service.

**Limitations and Viewpoints**

However, a significant drawback of our network design is its reliance on the main router. In the event of a main router failure or unavailability, the entire network would experience a severe impact. Communication between devices within VLANs and between VLANs would become impossible, disrupting network connectivity. The main router's crucial role in routing packets between networks and providing access to external networks, such as the Internet, amplifies the consequences of its failure.

Despite this significant flaw in our network design, other factors such as cost-effectiveness, scalability and flexibility are prioritised, leading us to decide on this network design. Since the Router-on-a-Stick design allows a single physical router interface to handle multiple VLANs, this will reduce the need for additional hardware, hence lowering the cost of implementing this design. On a more realistic note, a campus network design should be flexible and versatile as it accommodates many individuals for their network and connectivity needs. And for that, our design allows the segregation of VLANs and efficient use of network resources because multiple sub-virtual interfaces can be created on a single physical interface. Lastly, we believe it is common for universities to scale up and expand their campus over the years of operation, which is why scalability is also one of the dominant factors in deciding our network design. By configuring just the main router, modifying and adding VLANs can be accomplished, making it a scalable solution as the network requirements evolve.

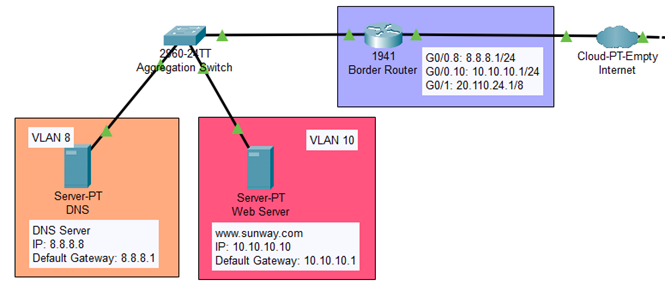
* 1. **Implementation Details**
     1. **Addressing Table**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** | **Default Gateway** |
| DNS | NIC | 8.8.8.8 | 255.255.255.0 | 8.8.8.1 |
| Web Server | NIC | 10.10.10.10 | 255.255.255.0 | 10.10.10.1 |
| Border Router | G0/0 | 20.110.24.1 | 255.0.0.0 | N/A |
| G0/1.8 | 8.8.8.1 | 255.255.255.0 | N/A |
| G0/1.10 | 10.10.10.1 | 255.255.255.0 | N/A |
| Aggregation Switch | VLAN 1 | N/A | N/A | N/A |
| Main Router | G0/0 | 20.110.24.2 | 255.0.0.0 | N/A |
| G0/1 | 192.168.15.1 | 255.255.255.0 | N/A |
| G0/1.11 | 192.168.11.1 | 255.255.255.0 | N/A |
| G0/1.12 | 192.168.12.1 | 255.255.255.0 | N/A |
| G0/1.13 | 192.168.13.1 | 255.255.255.0 | N/A |
| SYSLOG | NIC | 192.168.15.23 | 255.255.255.0 | 192.168.15.1 |
| Distribution Switch | VLAN 1 | N/A | N/A | N/A |
| Sunway University Switch | VLAN 1 | N/A | N/A | N/A |
| Sunway College Switch | VLAN 1 | N/A | N/A | N/A |
| Sunway International School Switch | VLAN 1 | N/A | N/A | N/A |

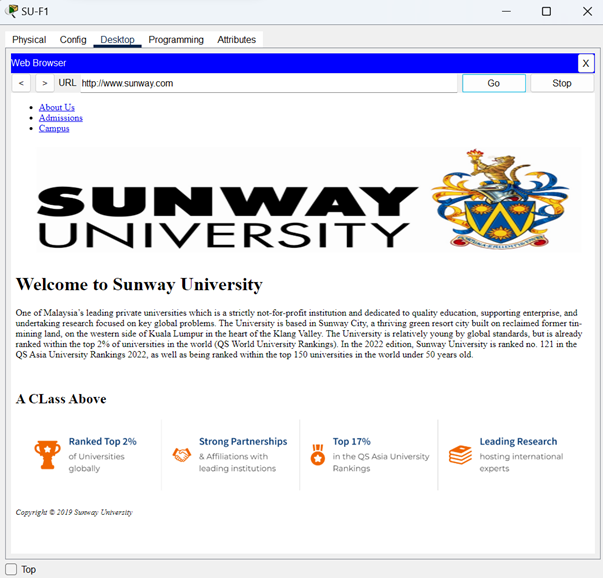
* + 1. **Switch Port Assignment Specifications**

|  |  |  |  |
| --- | --- | --- | --- |
| **Device** | **Ports** | **Assignment** | **Network** |
| Aggregation Switch | F0/1 | VLAN 8 – DNS | 8.0.0.0/24 |
| F0/2 | VLAN 10 – Sunway | 10.0.0.0/24 |
| G0/1 | 802.1Q Trunk | N/A |
| Distribution Switch | F0/1 | 802.1Q Trunk | N/A |
| F0/2 | 802.1Q Trunk | N/A |
| F0/3 | 802.1Q Trunk | N/A |
| F0/4 | 802.1Q Trunk | N/A |
| G0/1 | 802.1Q Trunk | N/A |
| Sunway University Switch | F0/1 – F0/6 | VLAN 11 – Finance | 192.168.11.0/24 |
| F0/7 – F0/8 | VLAN 12 – HR | 192.168.12.0/24 |
| F0/9 – F0/10 | VLAN 13 – Registry | 192.168.13.0/24 |
| F0/11 – F0/13 | VLAN 14 – Marketing | 192.168.14.0/24 |
| G0/1 | 802.1Q Trunk | N/A |
| Sunway College Switch | F0/1 – F0/4 | VLAN 12 – HR | 192.168.12.0/24 |
| F0/5 – F0/10 | VLAN 13 – Registry | 192.168.13.0/24 |
| F0/11 – F0/13 | VLAN 14 – Marketing | 192.168.14.0/24 |
| G0/1 | 802.1Q Trunk | N/A |
| Sunway International School Switch | F0/1 – F0/4 | VLAN 14 – Marketing | 192.168.14.0/24 |
| F0/5 – F0/6 | VLAN 13 – Registry | 192.168.13.0/24 |
| F0/7 – F0/10 | VLAN 12 – HR | 192.168.12.0/24 |
| F0/11 – F0/14 | VLAN 11 – Finance | 192.168.11.0/24 |
| G0/1 | 802.1Q Trunk | N/A |

* + 1. **Network Access**



**Figure 12.**  External Network Infrastructure



**Figure 13.**  Personalized Website Hosted on Web Server

We have implemented the necessary components in our network setup to enable access from workstations to a website hosted on the web server (Figure 12). The web server, with the IP address 10.10.10.10, serves as the host for the website www.sunway.com. This website contains content which we personalized that can be accessed by the workstations (Figure 13). Moreover, we have integrated a DNS server into our network configuration. With this configuration, the DNS server, powered by Google's DNS service, resolves the domain name www.sunway.com to the IP address 10.10.10.10. By combining these elements, workstations in our network can seamlessly access the website hosted on the web server. As a result, users can easily retrieve the website's content and actively engage with the provided services.

* + 1. **IP Address Usage: Public and Private**

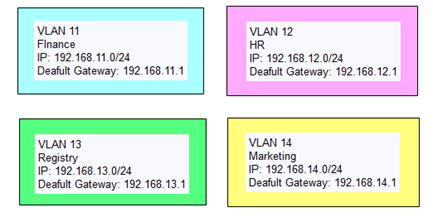
A close-up of a router

Description automatically generated

**Figure 14.** Main Router Interface Details

We use private addresses (such as 192.168.11.1/24) within our network design (Figure 14). Private IP addresses are reserved for internal use within private networks and are not globally routable. However, we need a public IP address to connect to the internet. In this case, we assign the public IP address 20.110.24.2 to the G0/0 interface of our main router (Figure 14). This address serves as the gateway connecting our internal network to the ISP and allows communication with external networks and Internet resources.

* + 1. **Classless IP Address**



**Figure 15.** VLAN Configuration Details

Each building is divided into four departments, and each department is assigned a specific subnet (Figure 15). For example, the Registry department implements the subnet 192.168.13.0/24. This implementation reflects the utilization of classless addressing, enabling greater flexibility in IP allocation and maximizing the efficient utilization of available address space. By adopting classless IP addressing, our network design aligns with modern standards and provides enhanced scalability and network management capabilities. This approach allows for optimized address allocation within each department while accommodating future growth and network expansion requirements.

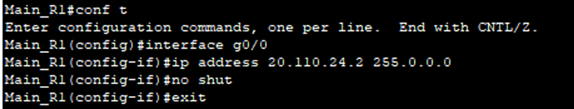
1. **Router** 
   1. **Overview**

Our network design includes 2 routers, the main router and the border router. Both routers work together to establish and maintain network connectivity but serve different purposes in the network design. The border router connects the internal and external networks and manages the traffic flow between them, whereas the main router focuses more on connecting the internal network components, such as the workstations and the switches.

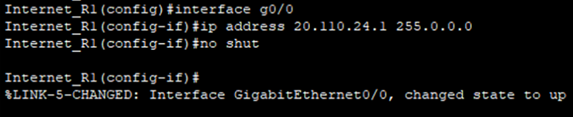
The border router links the DNS server and web server to the Internet, enabling communication between the internal networks and both servers. The border router also manages the network’s firewall and implements security measures. It protects the internal network from unauthorized access or threats from the Internet.

The main router serves as the central point of connection for the network. It is connected to the DSL modem on one end and to all the workstations across different departments in various buildings on the other end. The main router acts as the internal gateway, which allows communication between workstations and provides Internet access. The IP addresses and subnets of the workstations can also be set through the main router. This is done by configuring Dynamic Host Configuration Protocol (DHCP) to assign IP addresses to all end stations automatically.

* 1. **Implementation details**
     1. **Setting Up Default Gateway**



**Figure 16.** Setting up Default Gateway on Main Router



**Figure 17.** Setting up Default Gateway on Border Router

We set up the default gateway on the routers by configuring the IP address of the DSL modem as the main router’s IP address and the Internet IP address as the border router’s IP address. Setting up a default gateway enables communication between the local network and external networks. It acts as the entry and exit point for network traffic, allowing data transmission between local network devices and external networks. Without a properly configured default gateway, local network workstations would be unable to communicate with workstations of different networks.

* + 1. **Auto-start & Configuration Saving**

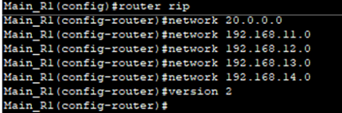
**A screen shot of a computer screen

Description automatically generated**

**Figure 18.** Saving The Running Configuration to the Startup File

To make our routers start automatically after rebooting, we used the copy running-config startup-config command to save the running configuration to the startup file on the non-volatile random-access memory (NVRAM) after finishing all configurations. After this procedure, the routers would maintain their configuration settings even after a restart or power cut.

* + 1. **Dynamic Routing**



**Figure 19.** Enabling Routing Information Protocol (RIP)

In our network design, we implemented dynamic routing on routers by enabling the Routing Information Protocol (RIP) in the network. Then, we configured the main router to advertise the IP addresses of all the departments. Dynamic routing protocols are implemented to handle large networks and to allow efficient network operation. It also allows routers to exchange routing information, adapt to network changes and dynamically update routing tables for optimal routing decisions.

1. **Switch**
   1. **Overview**

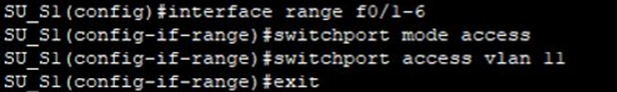
We have incorporated five switches in our network design to ensure smooth and efficient data transmission. One of these switches acts as an aggregation switch, strategically positioned between a DNS Server, Web Server, and a router. By implementing VLANs, we can exercise precise control over device connectivity and efficiently isolate network traffic as needed, thus enhancing security.

To optimize network configuration, we have assigned VLAN 8 to the DNS Server (F0/1), VLAN 10 to the Web Server (F0/2) and set G0/1 as a trunk port for data exchange between VLANs. This ensures efficient and secure communication within the network. We have also designated one switch as the main switch, serving as the central control point for managing data transmission to various departments in different buildings.

For instance, if data needs to be transmitted from Sunway University to Sunway College, it will pass through the main switch before reaching the College switch, guaranteeing reliable delivery. The main switch is also crucial in maintaining connectivity and data transmission, even if the router experiences issues. This ensures uninterrupted operation and facilitates communication between buildings.

With three switches strategically placed in separate buildings, our network design enables seamless connectivity and efficient data transmission across departments and workspaces. The switch located in Sunway University serves as a key hub for transmitting data to different departments in various buildings. This interconnected network of switches ensures smooth data exchange and accessibility throughout the entire network infrastructure.

* 1. **Implementation Details**
     1. **Setting Up Access Ports**

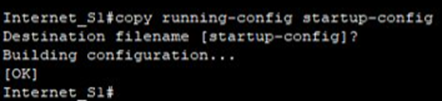
****

**Figure 20.** Setting Up Access Ports on a Switch

Network administrators leverage VLANs to exert precise control over device connectivity and effectively segregate network traffic. By assigning appropriate VLAN designations to access ports, administrators can establish distinct network segments within a single switch, thereby enhancing security and optimizing traffic management. This level of control empowers administrators to restrict unauthorized access and mitigate the risk of security breaches.

In the specific context of Sunway University, College, and International School, we have configured switches accordingly. At Sunway University, we have implemented distinct VLAN assignments for various departments, including Finance, HR, Registry, and Marketing. To ensure strict access control, we employed the switchport mode access command, which designates the port as an access port. This configuration ensures that any device connected to the port can only communicate with other devices in the same VLAN. Furthermore, the switchport access vlan command is utilized to assign a Layer 2 interface to the specified VLAN.

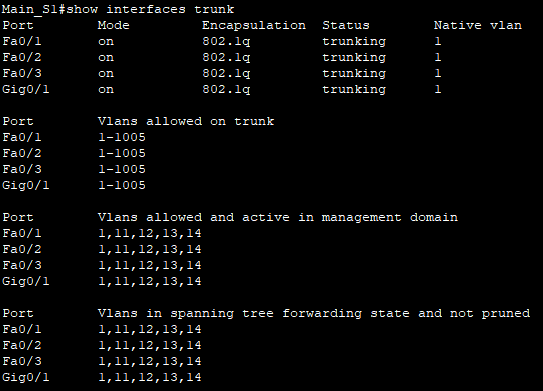
* + 1. **Auto-start & Configuration Saving**

****

**Figure 21.** Saving the Running Configuration to the Startup File

Switch deployment across multiple locations and departments is streamlined using the auto-start and configuration saving features. By employing the copy running-config startup-config command, administrators can efficiently duplicate settings, VLAN assignments, security rules, and other network parameters from one switch to another using the stored configuration. This standardized approach ensures a consistent network environment throughout the organization and significantly reduces the time and effort required to set up each switch.

* + 1. **Trunking and Encapsulation**

****

**Figure 22.** show interface trunk Result

Trunking allows for the transmission of multiple VLANs over a single connection, providing scalability and simplifying network management as the number of VLANs and devices grows. Configuring trunking is done using the switchport mode trunk command, while the show interface trunk command provides valuable information about the trunk configuration. By running the show interface trunk command, we may discover the native VLAN, the precise trunk encapsulation protocol (such as 802.1Q), and if an interface functions in trunk mode. It also gives us details on the VLANs authorized on this trunk, showing that VLANs 1 - 1005 are allowed to communicate across this trunk. Overall, the show interface trunk command provides thorough information that facilitates comprehending and effectively managing the trunking setup.

1. **Security Mechanisms**

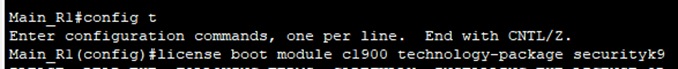
This is a simulation of a real-life scenario where our newly designed network is under attack, or a security violation is detected. The following are some practical implementations for our network design to overcome this threat.

* 1. **Overview and Justification**

In addition to the core network setup, we have implemented several additional features to enhance network security and scalability. This is essential when it comes to monitoring malicious activities and securing our network from policy and security violations. These features include implementing an Intrusion Prevention System (IPS), a firewall, and measures to ensure network scalability. These additional components safeguard the network from potential threats, enforce access control policies, and accommodate future growth.

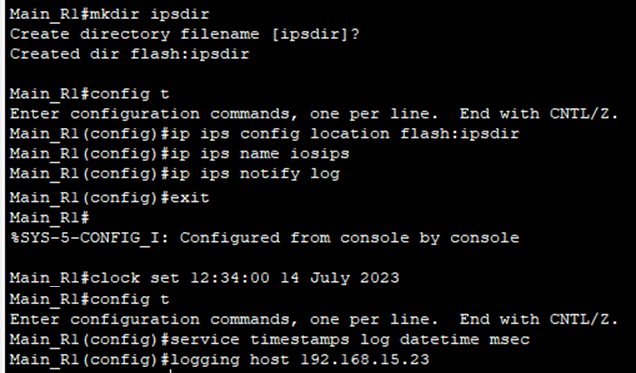
* 1. **Implementation details**
     1. **Intrusion Prevention System (IPS)**

Monitoring network and system activities for malicious activities or policy violations can be achieved through an IPS. This system actively analyses network traffic and system logs to identify real-time unauthorized access, potential threats, or policy violations. It goes beyond merely detecting suspicious activity and takes immediate action by automatically responding to and mitigating threats.



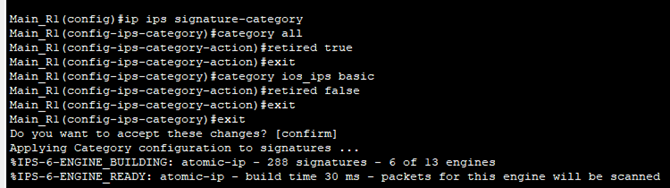
**Figure 23.** Enable Security Technology Package

Initially, we enabled the Security Technology package on our main router since it is not enabled by default. This involves manually entering a command (Figure 23), saving the running config file, and rebooting the router.



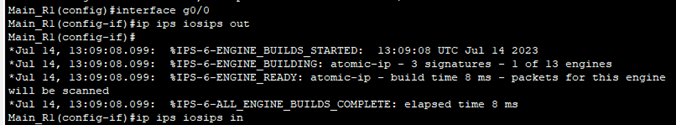
**Figure 24.** Setting Up IPS

On Main\_R1, we created a directory named “ipsdir” in the flash memory using the mkdir command. We then set the IPS signature storage location as the “ipsdir” directory. An IPS rule named “iosips” is created. To facilitate event notification and IPS syslog messages display, we enable syslog notification, configuring the main router to send log messages to the IP address 192.168.15.23 (Syslog Server).



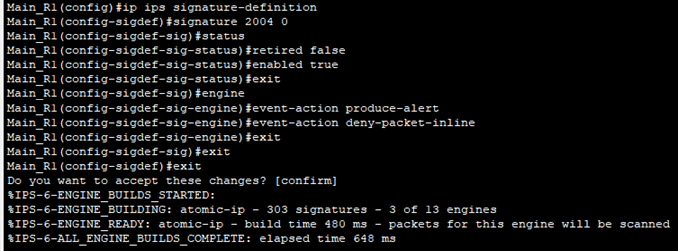
**Figure 25.** Configuring Signature Categories

Next, we retired all signature categories except the “IOS\_IPS Basic” category. This decision is made as we are still beginners and want to focus on understanding the essential signatures related to common security threats for Cisco IOS devices. Signature categories refer to groups or classifications of signatures based on the type of network threats they detect.



**Figure 26.** Applying to G0/0 Interface

We applied the IPS rule to the main router's G0/0 interface in both directions: “in” and “out.” The direction “in” means that IPS inspects only traffic going into the interface, while “out” means that IPS inspects only traffic going out of the interface. Inbound monitoring helps detect and block external threats, while outbound monitoring focuses on data protection and compliance enforcement. By implementing IPS on the Internet-facing interface (G0/0), we enhanced security as this interface is directly connected to external networks and potential threats, which is typically exposed to a higher level of risk.

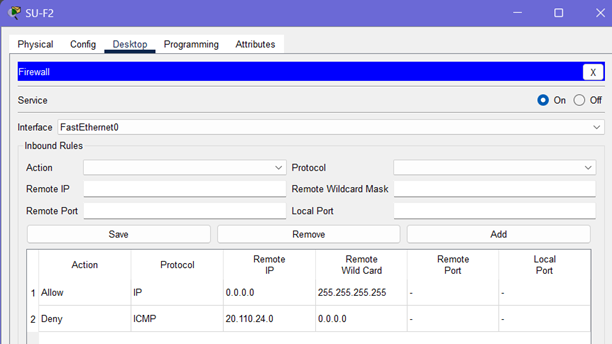


**Figure 27.** Modifying Signature Event-Action

Furthermore, we un-retire a specific signature known as the echo request signature and modify its action to “alert and drop.” The signature ID for this signature is “2004,” and the tuning option is represented by “0.” By implementing this configuration, we effectively prevent devices outside the network from pinging devices within the private network and vice versa. Both incoming and outgoing ping requests are blocked, triggering an alert for each denied ping attempt. These alerts are then directed to the syslog server for in-depth analysis and ongoing monitoring. It is important to note that this configuration does not interfere with the ping functionality between devices within the private network or their ability to access the web server. The focus is solely on restricting ping communication between devices inside and outside the network, enhancing security measures while maintaining seamless internal connectivity and access to web resources.

* + 1. **Implementation of Firewall**

While an IPS can actively prevent or block malicious activities, a firewall is a crucial security mechanism that complements the IPS. Firewalls help control and filter incoming and outgoing network traffic based on predefined rules, providing an additional layer of protection by blocking unauthorized access attempts and potentially malicious traffic. Since we are beginners who are unfamiliar with configuring an ASA firewall, we have opted to implement a firewall solely on computer devices instead of extending it to other devices, such as printers.





**Figure 28.** Firewall Settings

In Figure 28, our firewall rules are configured to deny ICMP protocol from the public network (20.110.24.0) and allow IP protocol from all possible IP addresses. By denying ICMP traffic, we blocked specific types of ICMP messages like ping requests, reducing the risk of information leakage and potential ICMP-based attacks. On the other hand, allowing IP traffic permits the forwarding of packets encapsulated with the IP protocol, enabling essential network communication such as web browsing, email, and file transfers. This ensures that necessary network operations can take place while maintaining security measures.

1. **Lessons Learnt**
   1. **Familiarizing with ping command in Command Prompt**

We are amazed by the simplicity yet profound usefulness of the ping command, where we can ping between devices using a command prompt on our computers or desktops. This tool grants us the ability to establish a direct connection with another device and observe how responsive the network is. In addition to the ping command, we frequently utilize other commands like tracert, pathping, and ipconfig /all to discover network connections and topologies. Moreover, exploring the campus network topology allowed us to expand our knowledge of different topologies and their respective features. Our lab tutorials have played a significant role in helping us learn the appropriate configuration commands. Overall, mastering the use of ping and other commands has dramatically enhanced our understanding and practical application of networking fundamentals. It is a crucial skill and understanding to have before moving on to designing a functional network simulation on platforms like Cisco Packet Tracer.

* 1. **Designing A New Network Topology using Cisco Packet Tracer**

Throughout this assignment, we got exposure to the practical implementation of network architectures through Cisco Packet Tracer, a powerful network simulation tool. The ability of this simulator to configure and customize network devices, assign IP addresses, and establish secure connections truly amazed us and provided a deeper understanding of network architecture and design principles. We particularly focused on the concept of Router-on-a-Stick for our network design, it is essentially a router with a single physical or logical connection to a network, and this method allows us to perform inter-VLAN routing in our design. Various aspects such as practicality, feasibility and scalability are taken into account when building our network in Cisco Packet Tracer to simulate real-world scenarios. Not only that, the considerations on cost, security measures and accessibility of our network topology are vital to ensure efficient data flow and network performance. Hence, it is safe to say that we are becoming more proficient and skilful in using Cisco Packet Tracer as a networking simulator.

* 1. **Further Exploration on Networking Fundamentals**

Besides discovering and designing a network topology, we managed to delve deeper into the topic of Cybersecurity to enhance our design and understanding. After a good amount of research and trial runs, we implemented multiple security mechanisms, such as Intrusion Prevention Systems (IPS) and firewalls, into our network. They play critical roles in securing networks against potential threats, which is an effort to make our network realistic and versatile. Exploring these topics beyond the syllabus made us realize the vast spectrum of different aspects in the field of networking. As a result, it reinforced our determination and commitment to enhance our knowledge of Networking Principles and upskill along the way.