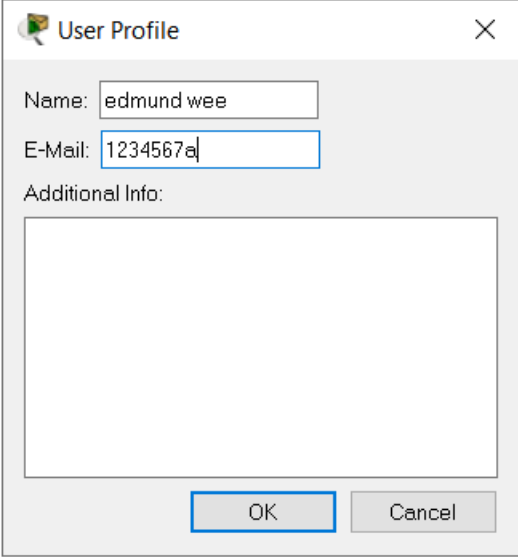


**TEMASEK POLYTECHNIC
SCHOOL OF INFORMATICS & IT
DIPLOMA IN INFOCOMM AND DIGITAL MEDIA
PROJECT SPECIFICATION
AY2024/2025 OCTOBER SEMESTER**

INTERNETWORKING TECHNOLOGIES (CIML011)

INSTRUCTIONS TO CANDIDATES

1. This project specification consists of 11 pages (including cover page).
2. This project consists of 2 main deliverables.
 - IP address planning and designing
 - Implementation of Project Requirements in Packet Tracer Files
3. This project is to be completed and submitted by the deadline stated in the Teaching Plan using the submission link in POLITEMall.
4. This project carries a weightage of 50% where 10% is for group work and 40% is for individual
5. For individual packet tracer files (i.e. INWT-C-Project Site-X.pka), please enter your name and admin number (e.g. see screenshot below) and click OK before attempting the project.



The screenshot shows a 'User Profile' dialog box. It has a title bar with a close button (X). The dialog contains the following fields and controls:

- Name:** A text input field containing the text 'edmund wee'.
- E-Mail:** A text input field containing the text '1234567a'.
- Additional Info:** A label followed by a large, empty text area for additional information.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

Project Background and Requirements

Global Enterprises is setting up offices in 4 branch offices around Singapore. As the company's network administrator, you are tasked to deploy the network infrastructure for these sites.

In groups of 4 people, you are to accomplish the following:

1. IP addressing planning and designing for
 - WAN connectivity
 - LANs
2. Packet Tracer configuration
 - Configure LACP EtherChannel
 - Configure Switch Security
 - Configure HSRP
 - Configure ACL
 - Configure Network Management
 - Configure multi-area OSPF
 - Configure site to site VPN

Scenario

Global Enterprise has 4 sites and has subscribed for Internet connectivity for each site via an Internet Service Provider (ISP). Based on your group number, you are to use the IP address range provided in Appendix A. The WAN network topology is as shown in Figure 1.

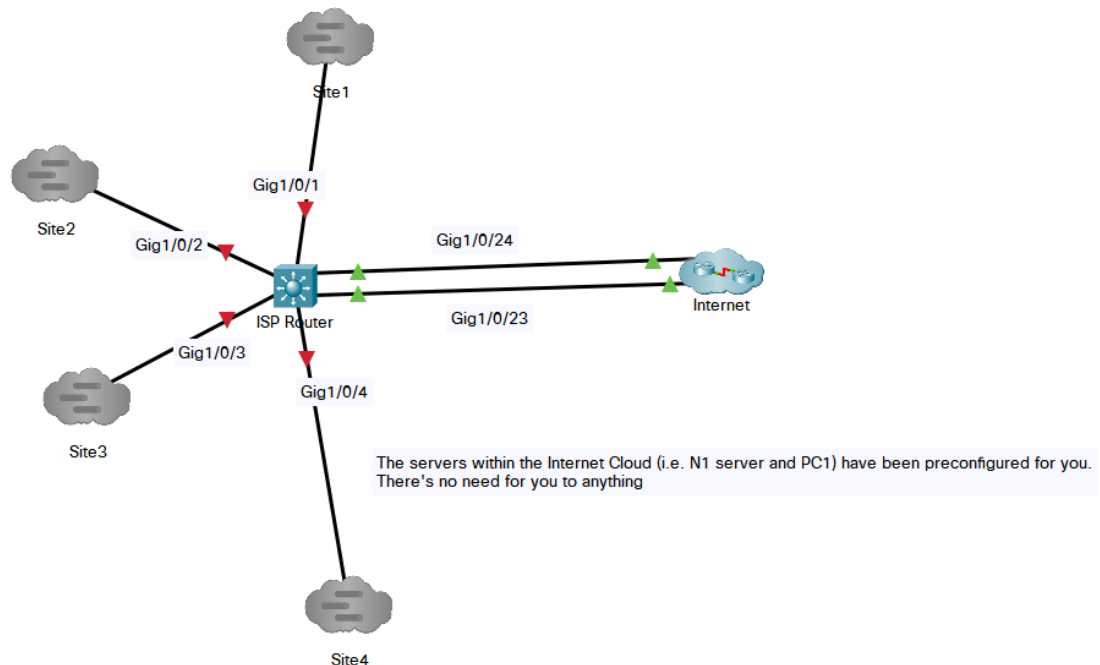


Figure 1: WAN Topology

The following five packet tracer files will be provided and you are to configure these files based on the tasks described in this project specification: -

1. INWT-C-Project Internet Cloud
2. INWT-C-Project Site-1
3. INWT-C-Project Site-2
4. INWT-C-Project Site-3
5. INWT-C-Project Site-4

Each team member is to choose one of the four INWT-C-Project Site-X packet tracer sites files and configure it individually. **Task No. 2 to 9 is to be configured in this packet tracer file. You are to configure the INWT-C-Project Site-X packet tracer sites file individually.**

The INWT-C-Project Internet Cloud will be used for providing network connectivity between the four packet tracer sites files. **Task No. 10 is to be configured in this packet tracer file. You are to configure the INWT-C-Project Internet Cloud packet tracer file as a group.** Do note that the end devices within the INWT-C-Project Internet Cloud packet tracer file has been preconfigured for you. You do not need to make any configuration changes on these devices. However, you do need to configure the ISP router in order for the network connectivity to work.

Task 1 – Network addresses (1% Group Work)

- 1.1 Using the provided IP address range in Appendix A, you are to work as a group to subnet the assigned Internet address range into 4 equal subnetworks such that the four branch offices can connect to the ISP. This calculated Network Addresses block will be used for your WAN and LAN. Provide your calculated 4 Network Addresses block into Table 1 and include this table as part of your project report.

Table 1: Network addresses

Branch office name	Network Address
Site-1	e.g. x.x.x.x/xx
Site-2	
Site-3	
Site-4	

Task 2 – Router interfaces and LAN addresses (2.5% Individual Work)

- 2.1 Based on the LAN topology provided in Figure 2, you are to configure the environment based on the tasks specified in this project specification.

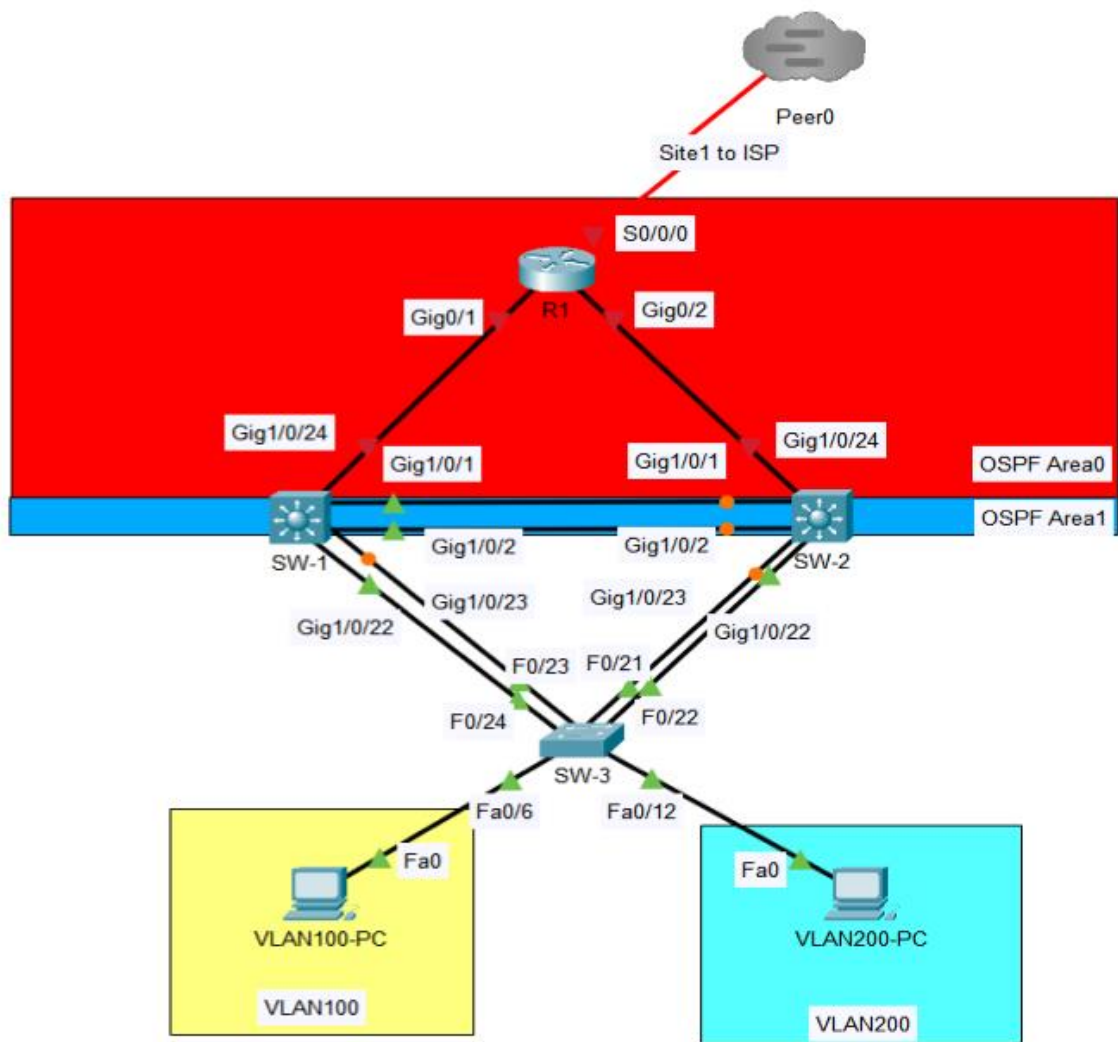


Figure 2: LAN Topology

2.2 As an individual, you are to further divide the IP subnets for WAN and LAN requirement. You are to fill up the empty fields in Tables 2 and 3.

Table 2: Interfaces used and IP addresses

Router	Interface	Description	Network Address (CIDR Format)	IP address
R1	Serial 0/0/0	Site-to-site connection with ISP router	e.g. x.x.x.x/xx	e.g. x.x.x.x
	Gigabit Ethernet 0/1	R1 connection with SW-1		
	Gigabit Ethernet 0/2	R1 connection with SW-2		
	Router ID / Loopback 0	For OSPF		

SW-1	Gigabit Ethernet 1/0/24	SW1 connection with R1		
	Etherchannel 1	Etherchannel between SW-1 and SW-2		
	Etherchannel 2	Etherchannel between SW-1 and SW-3		
	Router ID / Loopback 0	For OSPF		
	VLAN100			
	VLAN100	VLAN100 HSRP Virtual Gateway		
	VLAN200			
SW-2	Gigabit Ethernet 1/0/24	SW2 connection with R1		
	Etherchannel 1	Etherchannel between SW-2 and SW-1		
	Etherchannel 3	Etherchannel between SW-2 and SW-3		
	Router ID / Loopback 0	For OSPF		
	VLAN100			
	VLAN200			
	VLAN200	VLAN200 HSRP Virtual Gateway		
SW-3	Fast Ethernet 0/6			
	Fast Ethernet 0/12			
	Etherchannel 2			
	Etherchannel 3			
LAN1-PC	Fast Ethernet 0			
LAN2-PC	Fast Ethernet 0			

Table 3: LAN IP Address Ranges

LAN Name	VLAN ID	Required Hosts	Network Address CIDR /	Start of IP address range	End of IP address range
VLAN100	VLAN100	14	e.g. x.x.x.x/xx	e.g. x.x.x.x	e.g. x.x.x.x

VLAN200	VLAN200	30			
---------	---------	----	--	--	--

Task 3 – End devices and VLAN allocation configuration (2.5% Individual Work)

- 3.1 In the Project Site.pkt file, you are to configure your site's end devices using the LAN IP subnets calculated in Table 3.
- 3.2 You are to assign on SW-3's switchports 0/1 to 0/10 to VLAN100 and switchports 0/11 to 0/20 to VLAN200.

Task 4 – Configure LACP EtherChannel (2.5% Individual Work)

- 4.1 Configure LACP EtherChannel on the interconnection links between SW-1, SW-2 and SW-3.
- 4.2 The interconnection link between SW-1 and SW-2 is to be configured as Layer 3 and the rest of the interconnection links are to be configured as Layer 2.

Task 5 – Configure Network Devices Security (5% Individual Work)

- 5.1 Configure enable secret password for all Cisco network devices to Ciscoenpass.
- 5.2 Configure console password for all Cisco network devices to Ciscoconpass.
- 5.3 Configure vty password for all Cisco network devices to Ciscovtypass.
- 5.4 All passwords are to be encrypted.
- 5.5 Configure hostname for all Cisco network devices.
- 5.6 Configure VLAN100 and VLAN200 on the switches. Ensure that interface VLAN1 is shutdown on all switches. Secure unused switchports on all switches by shutting them down as well.
- 5.7 Move all unused access switch ports to VLAN999 (BlackHole).
- 5.8 Configure secure trunk between SW-1, SW-2 and SW-3. Configure VLAN99 (i.e. MGMT) as native VLAN for these links.
- 5.9 On SW-3, implement port security on all active switchports. Allow a maximum of 4 MAC addresses to be learned on the ports. Ensure that all learned MAC addresses on the port will be added to the running configuration. Configure the port security violation mode to drop packets from MAC addresses that exceed the maximum and generate a Syslog entry. However do not disable these ports.

- 5.10 Configure all trunk ports on all switches as DHCP snooping trusted ports.
- 5.11 Configure on all PortFast and BPDU guard on all access points on SW-3. Also on SW-3, limit untrusted ports on all access ports to 10 DHCP packets per second. Enable DHCP snooping for all VLANs.

Task 6 – Configure HSRP (5% Individual Work)

- 6.1 Configure HSRP on both SW-1 and SW-2 for both VLAN100 and VLAN200. SW-1 will be active gateway for VLAN100 and SW-2 will be active gateway for VLAN200 with their counterpart MultiLayer switches configured as standby. In the event of active switch failure, the standby switch will take over as active. Ensure that the active switch will resume the active role when it becomes available again.

Task 7 – Configure ACL (5% Individual Work)

- 7.1 Configure extended named ACL on your site routers such that all your site's PCs are allowed to view the HTTPS webpage hosted on N1 server (located within the Internet cloud) and not the HTTP webpage. All other traffic are allowed and should not be affected by this ACL.

Task 8 – Configure Network Management (2.5% Individual Work)

- 8.1 Enable LLDP on all Cisco network devices.

Task 9 – Multi-area OSPF (5% Individual Work)

- 9.1 Configure multi-area OSPFv2 between the multilayer switches and R1.

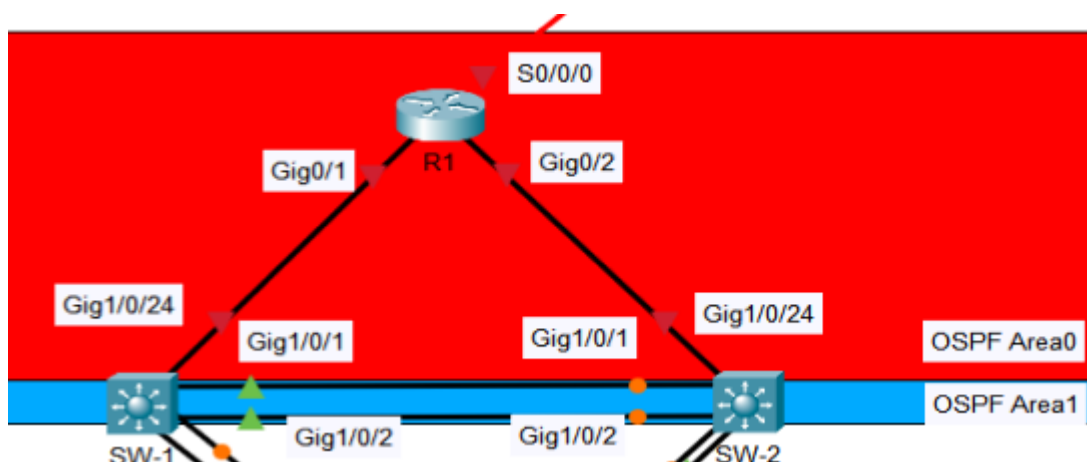


Figure 3: OSPF Areas

- 9.2 Configure OSPFv2 on R1 with a process ID of 1 and a router ID of 1.1.1.1, OSPFv2 on SW-1 with a process ID of 1 and a router ID of 2.2.2.2 and OSPFv2 on SW-2 with a process ID of 1 and a router ID of 3.3.3.3.

9.3 Configure each network in OSPFv2 assigning areas according to the below table

Table 4: OSPF areas assignment

Device Name	Interface	OSPFv2 Area
R1	Gig0/1	0
	Gig0/2	0
	S0/0/0	0
SW-1	Gig1/0/24	0
	Etherchannel 1	1
SW-2	Gig1/0/24	0
	Etherchannel 1	1

Task 10 – Inter-routing between all the sites and Site to Site VPN (9% Group Work)

10.1 Working as a group and using the multiuser cloud functionality of the packet tracer, you are to configure OSPF routing on the ISP router (found in the Internet Cloud.pkt file) and all site routers (found in the respective Project Site.pkt file), such that all the sites can be reached each other via the ISP router. **You can refer to the Packet Tracer Multiuser Cloud Setup Guide on how to get multiple packet tracer files can communicate with each other.**

10.2 In addition, configure site to site VPN based on the below tables.

Table 5: ISAKMP Phase 1 Policy Parameters

Parameter	Site-X WAN Router	ISP Router
Key Distribution Method	ISAKMP	ISAKMP
Encryption Algorithm	AES 256	AES 256
Hash Algorithm	SHA-1	SHA-1
Authentication Method	Pre-share	Pre-share
Key Exchange	DH 5	DH 5
IKE SA Lifetime	86400	86400
ISAKMP Key	Cisco123	Cisco123

Table 5: IPSec Phase 2 Policy Parameters

Parameter	Site-X WAN Router	ISP Router
Transform Set Name	VPN-SET	VPN-SET
ESP Transform Encryption	ESP-AES	ESP-AES
ESP Transform Authentication	ESP-SHA-HMAC	ESP-SHA-HMAC
Peer IP Address	<To be assigned by you>	<To be assigned by you>
Traffic to be Encrypted	Inter-branch traffic (Exclude traffic to and from Internet)	Inter-branch traffic (Exclude traffic to and from Internet)
Crypto Map Name	VPN-MAP	VPN-MAP
SA Establishment	IPSEC-ISAKMP	IPSEC-ISAKMP

10.3 Ensure that your respective site's PC can reach N1 server.

Project Presentation

1. During the presentation, the project group will be ask to demonstrate the completeness of your project.
2. All routers / switches / hosts / laptops in the packet tracer will be assessed by the tutor during the project presentation.

Q&A (10% Individual Work)

1. Each student should be well prepared to answer all questions to show understanding of the whole project.
2. Theory questions may also be asked to ascertain your basic understanding of Networking

Project Reports Deliverables

1. Submit updated Tables 1, 2 and 3 in separate word documents for each group member.
 - <1st group member name>-<1st group member admission number>.docx
 - <2nd group member name>-<2nd group member admission number>.docx
 - <3rd group member name>-<3rd group member admission number>.docx
 - <4th group member name>-<4th group member admission number>.docx
2. Submit the 5 packet tracer files
 - <1st group member name>-<1st group member admission number>.pkt
 - <2nd group member name>-<2nd group member admission number>.pkt
 - <3rd group member name>-<3rd group member admission number>.pkt
 - <4th group member name>-<4th group member admission number>.pkt
 - Group-<group number>-Internet Cloud.pkt

The group leader shall submit the above 9 documents in 1 single submission by compressing these documents into a single zip file. The actual number of documents to be submitted will varies according to your actual project group size.

3. Refer to Teaching Plan for Project submission deadline.
4. Word documents and packet tracer files are to be submitted in submission link found in POLITEMall.
5. The group shall conduct a 30-minute presentation for the project. The presentation will comprise of a hands-on demonstration by individual members (15 mins) and question & answer session (15 mins).

----- End of Project -----

Appendix A

Group No.	Assigned IP Address Range
1	21.21.21.0/24
2	22.22.22.0/24
3	23.23.23.0/24
4	24.24.24.0/24
5	25.25.25.0/24
6	26.26.26.0/24
7	27.27.27.0/24
8	28.28.28.0/24