

# 第 52 屆全國技能競賽

## 分區技能競賽

### 資訊與網路技術

#### 正式賽

#### 競賽試題

選手姓名		崗位編號	
------	--	------	--

開始比賽前請勿翻閱試題。

請先在試題封面及評分表寫上姓名及崗位編號。

本試題不含封面共 15 頁。

比賽後請將本試題及評分表留在崗位上，不得攜出賽場。

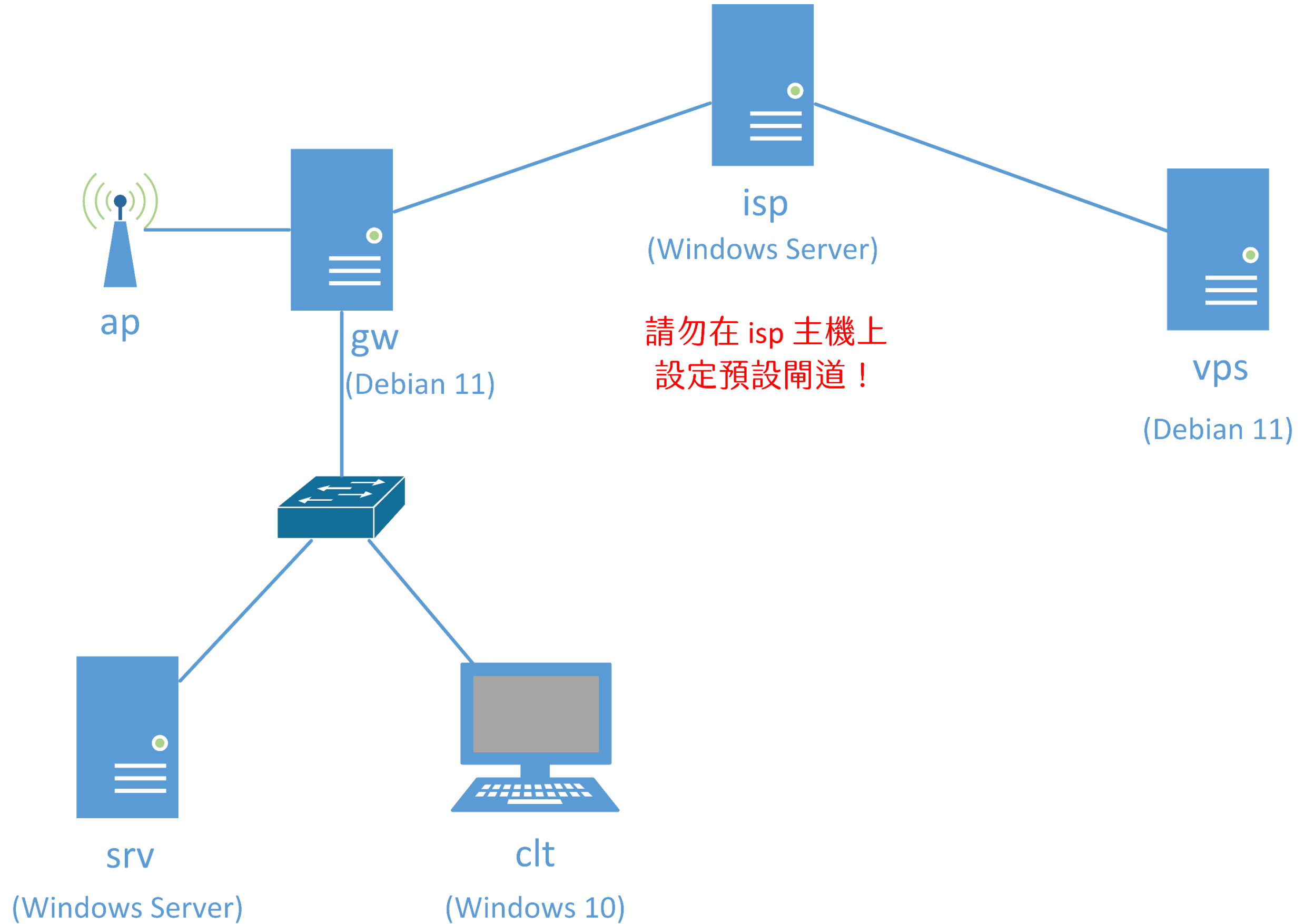




## 第 52 屆全國技能競賽 分區賽試題 – 資訊與網路技術

### 第一項

- 本競賽為固定式起訖時間，請選手自行掌握工作流程，並依據試題敘述完成要求。
- 如在比賽過程中有任何疑問，或題意描述不清楚，請立即向裁判反應。
- 評分時，將盡可能採用功能測試，項目之區隔以評分表所列為主，個別項目完全符合試題之敘述即得分，無部份給分。
- 工作項目中須設定密碼之處，若試題未明確指定，則一律使用 **Skills39**。
- 除了必須以檢視設定值的方式進行評分的項目外，所有面向用戶的服務一律由用戶端系統進行功能測試，否則該項目不予計分。
- 試題內所用到的作業系統皆為虛擬機，請勿將服務設定於 Host 作業系統上





## Scenario

你是某公司的小小 IT，因 Google 雲端空間政策改變，公司在雲上租了一台 VPS 虛擬機，請滿足老闆的一些需求：

- 將該 VPS 虛擬機用來備份公司內部系統資料，並提供公司備援用首頁
- 公司本來只有一個公司內網，但貴賓造訪時，常常抱怨沒有 Wi-Fi 可以上網，請你新增一個只能用來上網的 Wi-Fi 給客戶使用

※ 為正確模擬該情境，請幫忙設定 isp 虛擬機。

※ 以下公司內網即表示 192.168.1.0/24 網段，客戶網段即表示 192.168.99.0/24 網段

## General Setting

- 依據附錄 A 在 PC1 與 PC2 上安裝虛擬機，並設定主機名稱、網卡名稱、IP 位址與預設閘道
- 為使評分方便，請於所有主機允許網際網路控制訊息協定
- 瀏覽 HTTPS 網頁時，不可出現憑證錯誤訊息
- 評分時將會檢查崗位整潔度與線材製作品質

## Isp

- 模擬網際網路，將此虛擬機視為網際網路用戶端及網路路由器，請勿設定預設閘道！
- 設定網域名稱解析服務，提供 worldskills.tw 網域名稱解析，並依試題需求建立相關正解紀錄
- 設定憑證服務，為 https://www.worldskills.tw 站台提供憑證
- 設定網頁服務，可透過 https://www.worldskills.tw 瀏覽該網站，並在首頁顯示：  
worldskills TW No.1

## gw

- 啟用 IP 封包轉送服務，並提供公司內網及客戶網段可以上網
- 設定動態主機設定協定服務，提供 Wi-Fi 接入使用
- 設定 Secure Shell 服務，公司使用者 user88 在 clt 上連線時，不須輸入密碼即可連線
- 新增兩個 20GB 硬碟，一個掛載至/disk1 並提供給 srv 使用，另一個掛載至/disk2
- 設定 Samba 檔案共享服務，僅供公司內網存取
  - 分享 /disk2/share 目錄，啟用使用者驗證，僅允許使用者 user01-90 存取



- 設定 iptables，請依試題需求設定網路位址轉譯，供客戶上網與外部存取公司服務
  - 客戶網段僅能用來上網，不可存取公司內網
  - 禁止跨越介面存取 gw 上的任何服務 (e.g. 在 clt 上 SSH 連線至 52.52.52.52)

## srv

- 架設網域控制站，網域名稱為 lemon.com，並依據附錄 B 建立 100 個使用者帳號
- Windows 的功能更新將在評估過後再統一開放升級，請讓網域內的 PC 維持於本次競賽所使用的 Windows 10 主版本下
- 設定網域名稱解析服務，提供 lemon.com 網域名稱解析，請依據題目需求建立相關正解紀錄
  - 將 DNS Server 指向 srv 的用戶，也應可順利解析 worldskills.tw 域名下的記錄
- 設定憑證服務，為 lemon.com 網域提供憑證服務
- 設定動態主機設定協定服務，提供公司內網接入使用
- 設定網頁服務，提供 <https://www.lemon.com> 作為公司首頁
  - 使用 gw 提供的 20GB 硬碟，作為網頁根目錄
  - 若使用明文協定連線，請自動導向加密協定連線
  - 網際網路上的使用者應能正常存取公司首頁



## 第二項

### vps

- 新增 60GB 硬碟，掛載至 /backups 作為公司內部備援用的硬碟空間
  - /backups/disk1、/backups/disk2 將分別用來存放 gw 上 /disk1、/disk2 的資料
- 設定網頁服務，提供 <https://www.lemon.com> 作為公司備援用首頁
  - 使用 /backups/disk1 作為網頁根目錄
  - 若使用明文協定連線，請自動導向加密協定連線
  - 以 IP 連線網頁服務時，須顯示網頁服務預設頁面
- 設定 Secure Shell 服務，允許 root 使用密碼登入
- 提供一腳本或自動化服務，執行後，自動將 gw 的 /disk1、/disk2 資料同步至 vps 的 /backups，並寫入系統日誌，日誌內容至少須包含：“Sync file: <file name>”
- 設定 iptables，僅允許從公司內部對其進行遠端管理

### clt

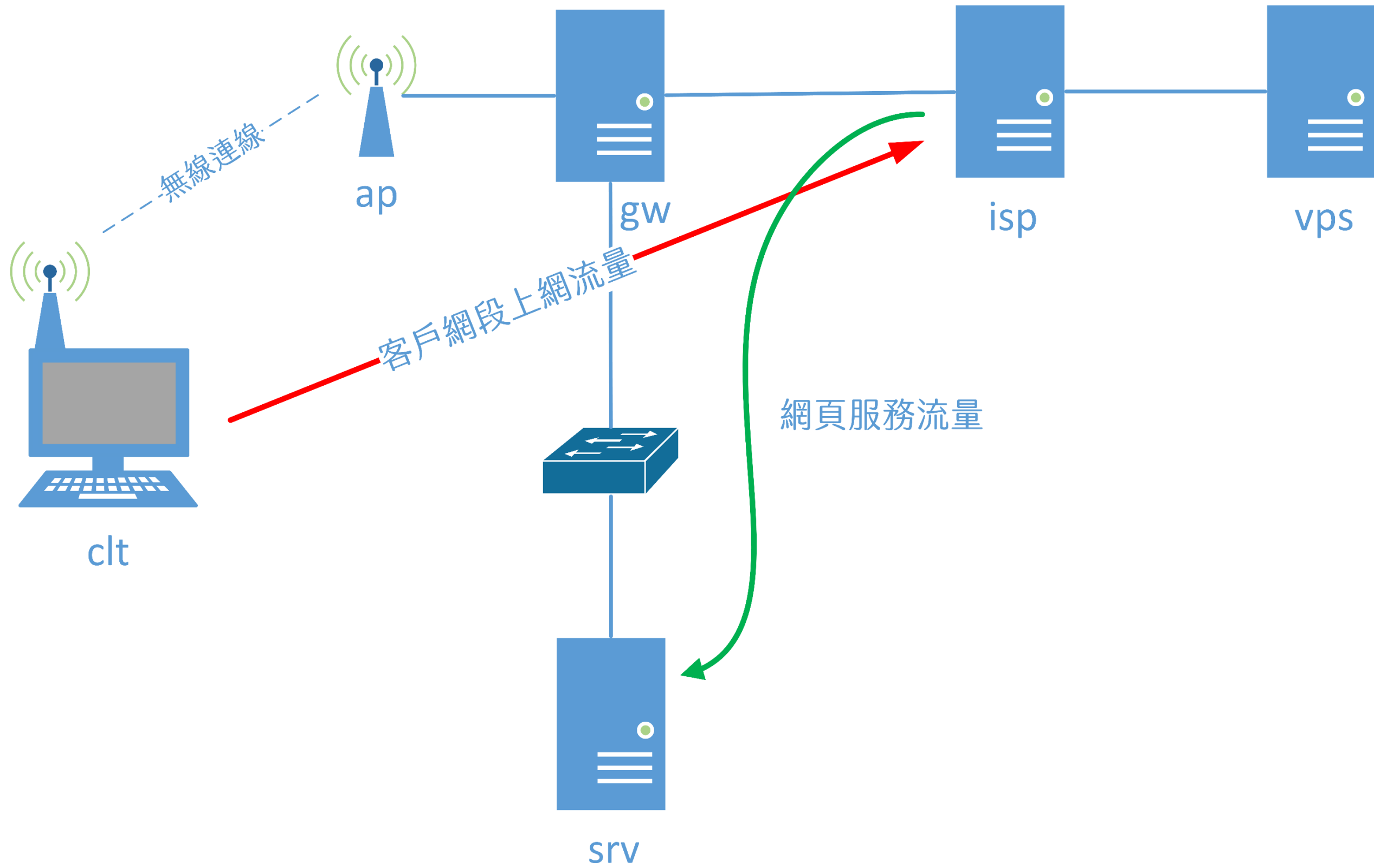
- 加入網域 lemon.com
- 禁止網域名稱快取
- 使用者 user88 桌面上請提供快速切換網站的腳本，瀏覽 <https://www.lemon.com> 時，將顯示 vps 上的網頁，以利測試備援站台是否正常
- 安裝無線網卡
  - 將於評分最後模擬公司客戶，連接無線網路，可連線 <https://www.worldskills.tw>

### ap

- 設定無線路由器，SSID 為 NSCXX (XX 為崗位編號，若崗位編號 01 則 SSID 將使用 NSC01，以此類推)，驗證方式為 WPA2-PSK，並使用 AES 做加密機制。
  - 無線網路登入密碼請使用 10 個英文字母，包含大小寫，並將你要使用的密碼寫於下方，評分時將會根據下方密碼進行登入評分。
-



# Flow Diagram





## Appendix A - IP Address Assignment

VM Hostname	OS	Host PC	Interface	IP Address	Default Gateway
isp	Windows Server 2022	PC1	Ethernet0	52.52.52.254/24	N/A*
			Ethernet1	46.46.46.254/24	
vps	Debian 11		eth0	46.46.46.46/24	46.46.46.254
gw	Debian 11	PC2	eth0	52.52.52.52/24	52.52.52.254
			eth1	192.168.1.254/24	
			eth2	192.168.99.254/24	
srv	Windows Server 2022		Ethernet	192.168.1.10/24	192.168.1.254
clt	Windows 10		Ethernet	DHCP	
			Wi-Fi	DHCP	
ap			LAN	192.168.99.253/24	

\* 若預設閘道為 N/A，則請勿做任何設定，否則該台 VM 不予評分！

## Appendix B - Domain Users

Username	Group
user01 ~ user90	Lemon Users
apple01 ~ apple10	Apple Users





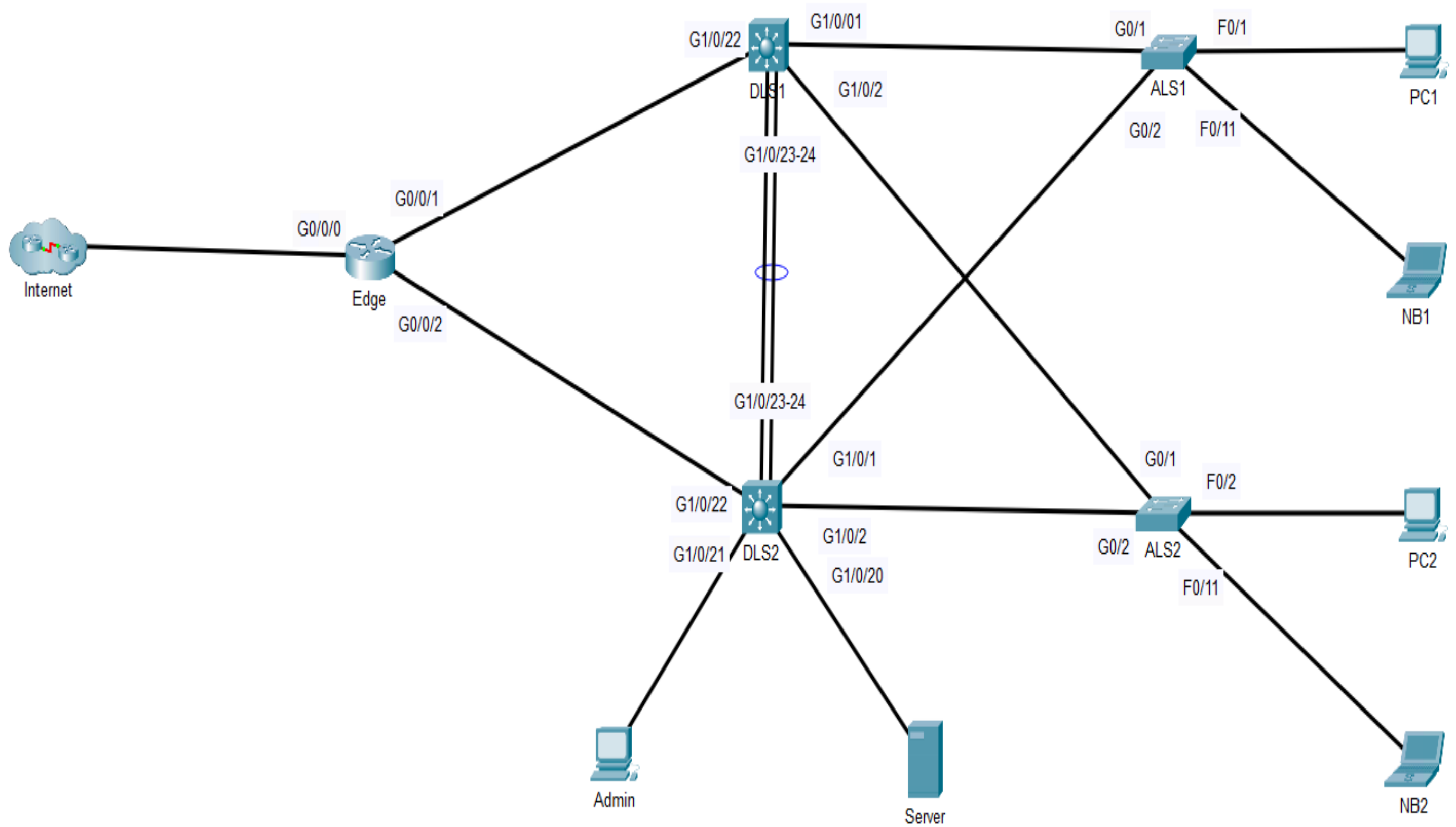
## 第三項

### Packet Tracer

- 本競賽為固定式起訖時間（時間 1.5 小時，確切時間由分區裁判長當場公佈），請選手自行掌握工作流程，並依照試題敘述完成要求。
- 題目的敘述順序不一定是解題的最佳順序，選手可自由決定先後順序。
- 如在比賽過程中有任何疑問，或題意描述不清楚，請**立即**向裁判反應。但裁判將**不會**為個別選手解釋非題目錯誤的疑問。
- 評分時，將以 Cisco Packet Tracer 內建的評分引擎比對選手操作結果及預建的標準答案，因此選手要依題目指示做答，不是功能對了就會得分。
- 工作項目中須設定密碼或金鑰之處，若試題未明確指定，則一律使用 **Skills39**。
- Packet Tracer 的 PKA 檔案在崗位隨身碟內，請先更改檔名為 **NSC3922-崗位號.pka** (例如 5 號崗位選手就改為 NSC3922-05.pka)。完成更改檔名請直接在隨身碟的 PKA 檔案點兩下開啟做答。（**不可把 PKA 檔案複製至崗位電腦**）
- **建議適時存檔**，以免萬一應用程式異常中止，導致選手做答遺失。比賽中因此狀況造成的時間浪費將不給予增加比賽時間。如因賽場設備問題需要處理，裁判長將就處理設備問題時間，給予增加比賽時間。
- 比賽結束前，請記得存檔，並確定崗位隨身碟裡只有一個合乎正確檔名的最終做答 PKA 檔案，否則導致無法評分，將無法補救。
- 比賽結束後，要繳回崗位隨身碟及本試題題本後離場！裁判會集中隨身碟進行評分作業。



## Topology





位址表

裝置	介面	IP 位址/前置碼長度	預設閘道	DNS
Internet	F0/1	209.165.200.254/27	N/A	N/A
www.isp.tw	Fa0	1.1.1.1/24	1.1.1.254	1.1.1.1
Edge	G0/0/0	209.165.200.225/27	209.165.200.254	N/A
	G0/0/1	192.168.254.1/30	N/A	N/A
	G0/0/2	192.168.254.5/30	N/A	N/A
DLS1	G1/0/22	192.168.254.2/30	N/A	N/A
	VLAN 10	第一個主機位址	N/A	N/A
	VLAN 20	第一個主機位址	N/A	N/A
	VLAN 30	第一個主機位址	N/A	N/A
	VLAN 40	第一個主機位址	N/A	N/A
	VLAN 239	第一個主機位址	N/A	N/A
DLS2	G1/0/22	192.168.254.6/30	N/A	N/A
	VLAN 10	第二個主機位址	N/A	N/A
	VLAN 20	第二個主機位址	N/A	N/A
	VLAN 30	第二個主機位址	N/A	N/A
	VLAN 40	第二個主機位址	N/A	N/A
	VLAN 239	第二個主機位址	N/A	N/A
ALS1	VLAN 239	第三個主機位址	最後一個主機位址	N/A
ALS2	VLAN 239	第四個主機位址	最後一個主機位址	N/A
Server (www.nsc52.tw)	Fa0	192.168.239.5/28	最後一個主機位址	192.168.239.5
Admin	Fa0	192.168.239.11/28	最後一個主機位址	192.168.239.5
PC1 (VLAN10)	Fa0	DHCP	最後一個主機位址	192.168.239.5
PC2 (VLAN20)	Fa0	DHCP	最後一個主機位址	192.168.239.5
NB1 (VLAN30)	G0	DHCP	最後一個主機位址	192.168.239.5
NB2 (VLAN40)	G0	DHCP	最後一個主機位址	192.168.239.5



## VLAN 表

VLAN	名稱	IP 位址	預設閘道	註解
VLAN 10	HR	192.168.10.0/24	最後一個主機位址	
VLAN 20	Finance	192.168.20.0/24	最後一個主機位址	
VLAN 30	Guest	192.168.30.0/24	最後一個主機位址	
VLAN 40	Staff	192.168.40.0/24	最後一個主機位址	
VLAN 239	Management	192.168.239.0/24	最後一個主機位址	原生 VLAN
VLAN 1999	Parking		N/A	所有未使用連接埠

## OSPF 路由器 ID

裝置	路由器 ID
Edge	1.1.1.1
DLS1	2.2.2.2
DLS2	3.3.3.3



## 第四項

### Part 1: 裝置設定

- 為 Edge, DLS1, DLS2, ALS1, ALS2 設定主機名稱。
- 為 Edge, DLS1, DLS2, ALS1, ALS2 設定雜湊加密的啟用密碼。
- 為 Edge, DLS1, DLS2, ALS1, ALS2 設定加密的主控制台密碼。
- 為 DLS1, DLS2, ALS1, ALS2 設定加密的 VTY 密碼。
- 在 Edge 建立使用者 **admin** 並設定雜湊加密密碼。
- 在 Edge 為 VTY 啟用 SSHv2 連線並設定成唯一接受的連線協定
  - 網域名稱：**nsc52.tw**
  - RSA 金鑰模數：**2048** 位元
  - 建立本機帳號 **admin**，及雜湊加密密碼
- 為 Edge, DLS1, DLS2, ALS1, ALS2 設定在執行模式輸入不存在的命令時，不會被當成主機名稱進行 IP 解析。
- 為 Edge, DLS1, DLS2, ALS1, ALS2 設定主控台和 VTY 在輸入命令或設定時，不被輸出的日誌訊息截斷輸入內容。

### Part 2: VLAN

- 為交換器 DLS1, DLS2, ALS1, ALS2 依 VLAN 表設定 VLAN。
- 設定主幹
  - 設定交換器間的連接埠為主幹
  - 使用靜態主幹模式並停用 DTP 協商
  - 依 VLAN 表設定原生 VLAN
- 依表格資訊設定靜態存取埠並指派 VLAN。
- 設定交換器 DLS1, DLS2, ALS1, ALS2 連接 PC 或伺服器的連接埠啟用，防止 CAM Table 泛洪攻擊的安全機制，要自動保留合法 MAC 位址於執行設定檔，在偵測到違規使用時，確保合法的流量不受影響，但要留下日誌供事件調查用。
- 停用 Parking VLAN 的連接埠。

### Part 3: IP 設定

- 為 Edge, DLS1, DLS2, ALS1, ALS2 設定 IP 位址。
- 為 Server, Admin 設定 IP 位址。



## Part 4: 擴充樹協定

- 設定交換器 DLS1, DLS2, ALS1, ALS2 使用 Cisco 專屬版本的快速生成樹協定。
- 設定交換器 DLS1, DLS2, ALS1, ALS2 連接 PC 或伺服器的連接埠為 Edge Port，並啟用防誤接其它交換器的保護機制。
- 設定交換器 DLS1, DLS2 的擴充樹協定進行分流，盡最大可能讓 VLAN 10 和 VLAN 20 以 DLS1 為根交換器，VLAN 30, VLAN 40 和 VLAN 239 的以 DLS2 為根交換器，同時讓 DLS1, DLS2 互相備援。

## Part 5: 鏈路聚合

- 將交換器 DLS1, DLS2 間互連的多條實體鏈路聚合成一條邏輯鏈路以提昇頻寬。
  - 聚合成的邏輯鏈路介面編號為 1
  - 使用 IEEE 802.3ad 做為鏈路聚合協定，並設定為主動模式
  - 以封包的來源及目的 IP 做負載平衡

## Part 6: 閘道備援

- 在交換器 DLS1, DLS2 為 VLAN 10, VLAN 20, VLAN 30, VLAN 40 及 VLAN 239 設定 Cisco 專屬的不具負載平衡功能的閘道備援協定。
  - 使用的閘道備援協定版本，未來要能部署 IPv6
  - 各 VLAN 使用的群組編號為其 VLAN ID
  - 各 VLAN 的閘道都使用最後一個主機位址
  - VLAN 10 及 VLAN 20 以 DLS1 為主要閘道（優先權+10）
  - VLAN 30, VLAN 40 及 VLAN 239 以 DLS2 為主要閘道（優先權+10）
  - 在主要閘道恢復正常時，要立即進行角色移轉以保持負載均衡



## 第五項

### Part 1: 路由

- 為 Edge, DLS, DLS2 以程序 ID : **100** 啟用 OSPFv2
  - 依 OSPF 路由器 ID 表設定路由器 ID
  - 使用 **network** 敘述，依各子網路位址設定單區域 OSPF
  - 使用介面最高頻寬設定 OSPF 自動成本計算的參考頻寬
  - 停用不需要介面上的 hello 封包發送
  - 為點對點鏈路停用 DR 選舉
  - 把鄰居訊息發送頻率提升為每分鐘 20 次以加快收斂
  - 把鄰居訊息逾時閾值依與發送頻率的預設比例調整
- 設定預設路由
  - 在 Edge 設定指向 ISP 的靜態預設路由
  - 藉由 OSPF 散佈預設路由

### Part 2: DHCP

- 在 Edge 設定 VLAN 30 及 VLAN 40 的 DHCP 位址集區：

集區名稱	第一個 IP	最後一個 IP	遮罩，閘道，DNS
VLAN30	第三個主機位址	倒數第三個主機位址	依位址表
VLAN40	第三個主機位址	倒數第三個主機位址	依位址表

- 在 DLS1 及 DLS2 設定將 VLAN 10 及 VLAN 20 的 DHCP 請求轉送至 Server (DHCP 集區已設定)。
- 在 DLS1 及 DLS2 設定將 VLAN 30 及 VLAN 40 的 DHCP 請求轉送至 Edge。

### Part 3: NAT

- 在 Edge 設定 NAT
  - 設定名為 **NAT\_POOL** 的 NAT 集區，使用 Edge 連接 ISP 介面 IP 位址的下兩個 IP
  - 設定名為 **NAT\_ACL** 的 IP 延伸命名 ACL 來納入所有使用中的內部網段 (不要做網路摘要)
  - 為內部來源設定動態 PAT，讓 **NAT\_ACL** 允許的位址使用 **NAT\_POOL** 的公用位址上 Internet
  - 為 Server 設定靜態 NAT，使用 **NAT\_POOL** 的下一個公用位址



## Part 4: 存取控制

- 為 Edge, DLS1, DLS2, ALS1, ALS2 設定及套用編號 **10** ACL 以允許只有 VLAN 239 及 Edge 的內部 IP 位址網路可以存取 VTY (ACL 10 必須只用兩行敘述完成)。