第51屆全國技能競賽

分區技能競賽

資訊與網路技術

術科試題

選手姓名		崗位編號	

開始比賽前請勿翻閱試題。

開始比賽後請先在試題封面及評分標準表寫上姓名及編號。

本試題不含封面共12頁。

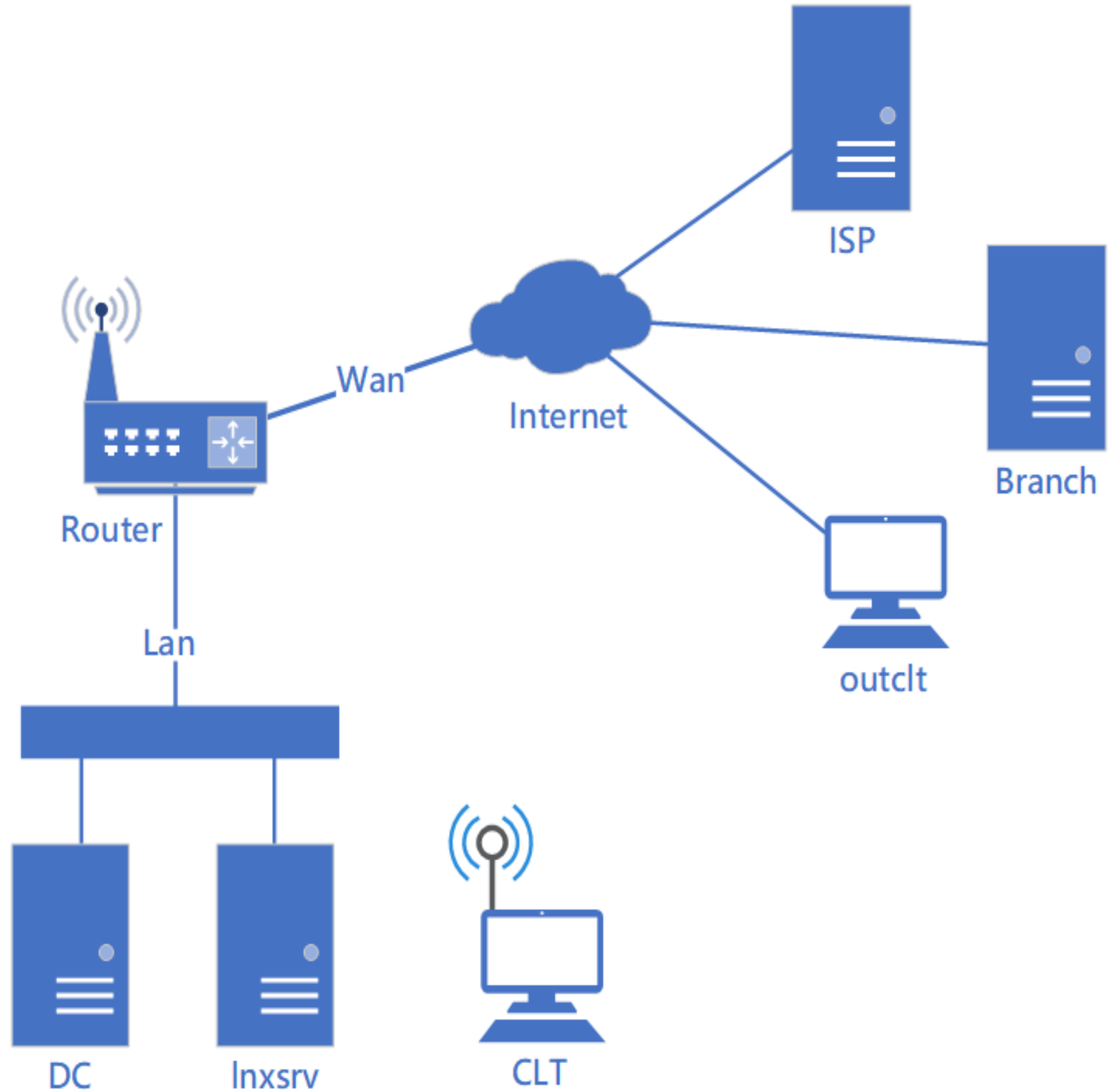
考試後**請繳回本試題**及**評分表**，不得攜出試場。

第51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，並依照試題敘述完成要求。
- 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

Topology



第二項

Scenarios

你是 Dora 公司裡的 IT Expert，日前收到Dora的委託架設內部 dora.local 網路，最近 Dora 公司業績長紅，Dora 的合作夥伴 Diego 想要拓展分公司，但是搗蛋鬼不相信你的技術所以想要說服 Dora 換一位 IT 人員，你為了不讓搗蛋鬼繼續搗蛋決定親自展現自己在資網所學到的技術，請於時間內完成指定要求。

General Settings

- 依據**附錄 D** 設定主機名稱與 IP 位址。
- 所有作業系統皆須允許 ICMP 協定。
- Host 主機請關閉 IPv4 與 IPv6 功能。
- 登入 Windows 虛擬機任何使用者不得有登入動畫。
- 憑證請統一使用 CA 發放之憑證，評測時請勿出現憑證錯誤畫面。

DC - Windows Server 2019

- 建立 dora.local 網域，依**附錄 A** 建立使用者
- dora.local域名僅用於企業內部系統環境使用，請設定 DNS 服務管理相關資源紀錄
    - 其餘請求請轉送至 ISP（51.51.51.1）
- 提供名稱為 DORA-ROOTCA 的 CA，並簽發相關服務憑證
- 提供 VPN 讓使用者可以遠端存取服務，僅允許 user39~user46 撥入
- 設定 GPO，並依下列所需設定：
    - 允許使用者 user50 可以本機登入 DC
    - 禁止使用者 user50 開啟小畫家及 msinfo32.exe

lnxsrv - Debian 10

- 依**附錄 A** 建立使用者
- 設定 DHCP 服務，範圍設定為 192.168.10.100 ~ 200，並將192.168.10.51 保留給 CLT 自動取得
    - DNS 伺服器請指定為 192.168.10.10
- 設定 DNS管理diego.com相關紀錄，將branch.diego.com授權給Branch進行管理
    - 請為 dns.diego.com (Resource Record) 進行適當設定以便完成 DNS 授權
- 提供 https://erp.dora.local，內容<h1>Dora We did it!</h1>
    - 外部網路可透過 https://erp-dora.diego.com:4443 瀏覽網頁
- 設定 sudo，僅限 webadmin 可以使用，且只能執行**附錄 C** 上的指令

第三項

CLT - Windows 10

- 加入 dora.local 網域，模擬內部 Client 進行測試
- 撰寫 script 執行後顯示數值，為 AD 網域所有使用者之數目（若不能一鍵執行請寫出腳本路徑）

使用者	
執行方法	

Branch - Debian 10

- 設定 DNS 服務，管理 branch.diego.com
- 提供 https://www.branch.diego.com，內容顯示 "Go Diego Go!"

ISP - Preconfigured

- 已模擬 ISP 伺服器，管理 .com 的 DNS 相關紀錄
- 已將 diego.com 網域授權至 dns.diego.com (51.51.51.2)
- 已提供 http://www.isp.com 網頁內容顯示 "Swiper - no swiping!"

outclt - Windows 10

- 作為外部 Client 進行測試
- 依照**附錄 B** 預先設定好 VPN 設定檔

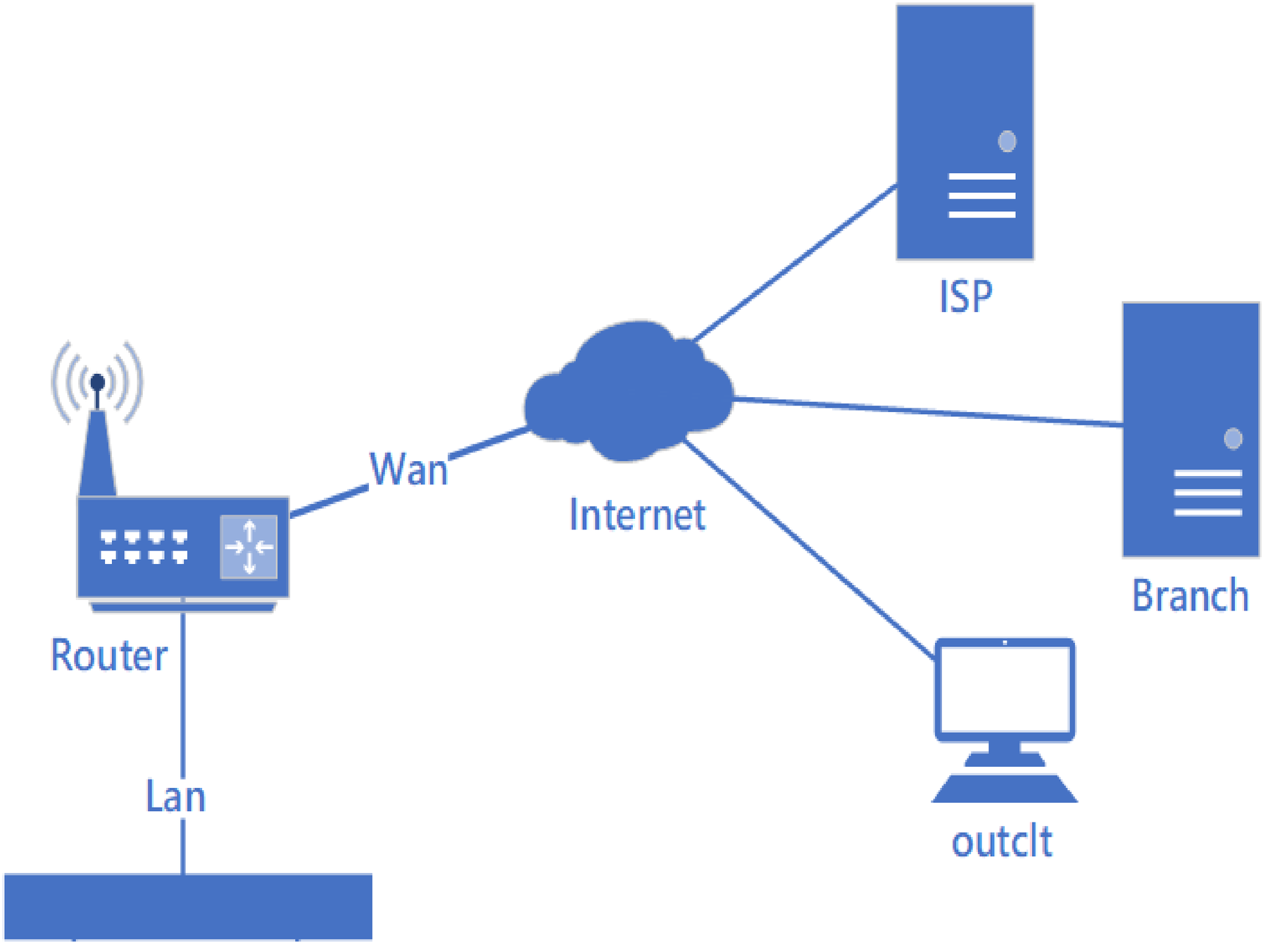
AP - Wireless Router

- 設定無線路由器供內部連線
- 設定相關設定讓內部可以存取外部網路
- 為方便使用者於公司不同地區環境時存取網路，公司計劃整併所有內部SSID的連線體驗，請將所有屬於公司的SSID，於用戶端操作介面統一顯示為NSC-XX並自動連線

- 於本次競賽僅以一組SSID進行概念測試，請將AP之SSID設定為RealAP-XX，並納入前述之整合設定組中，於用戶端顯示為NSC-XX　　※以上 XX 均為崗位號碼

- **請寫下自訂的Wi-Fi連線密碼**

Internet Diagram



附錄 A

User	Group	Password
user01~user50	Users	Skills39
webadmin	Web	

附錄 B

連線名稱	VPN類型	驗證方式
nsc51	不限	使用者驗證

附錄 C

指令
ls
cat
mv

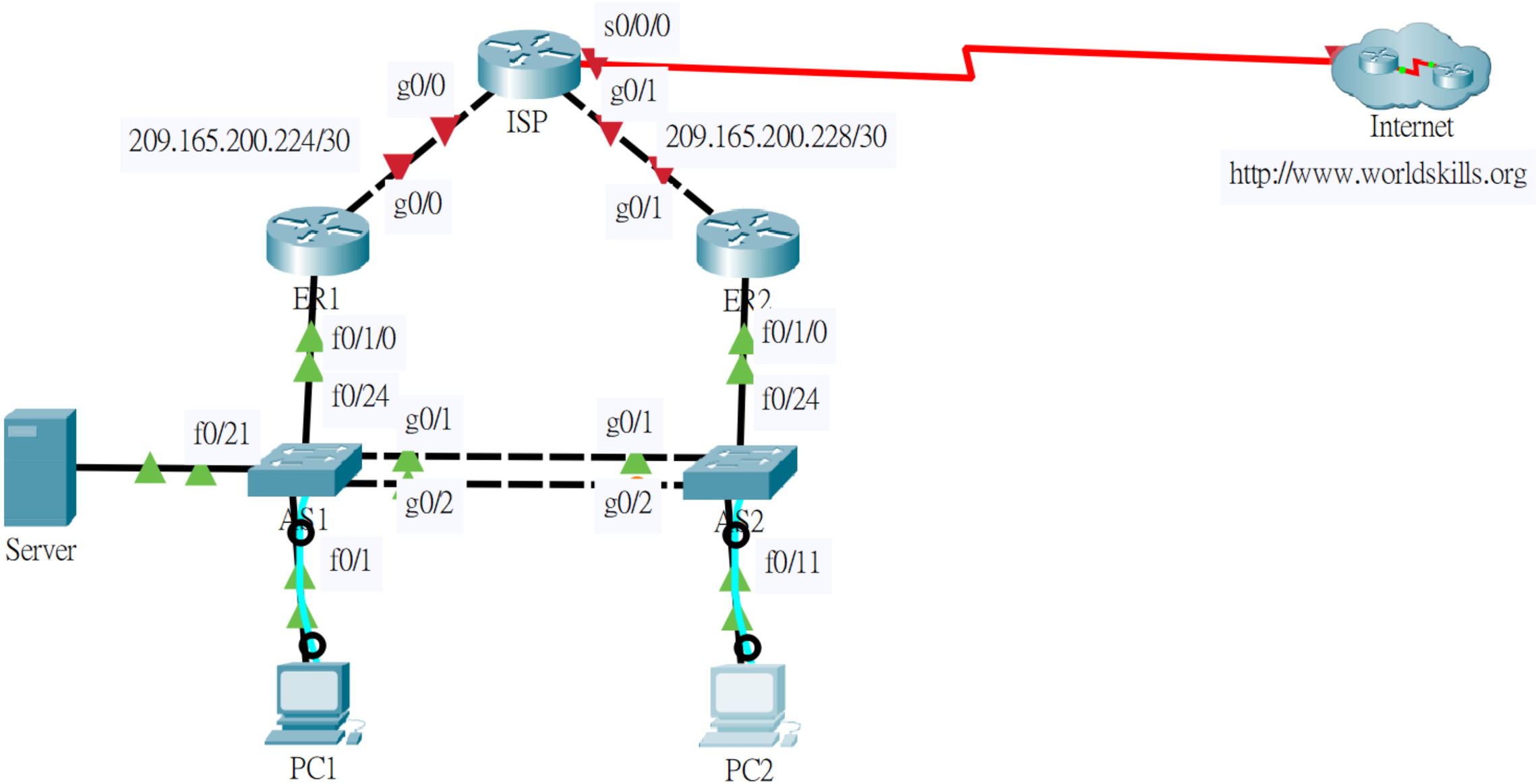
附錄 D:主機名稱與 IP 位址

Hostname	Interface	IP Address	Gateway	DNS Server
DC	Ethernet	192.168.10.10/24	192.168.10.254	192.168.10.10
lnxsrv	eth0	192.168.10.20/24		
CLT	WiFi	DHCP		
AP	Wan	51.51.51.2/28	51.51.51.1	51.51.51.1
	Lan	192.168.10.254/24	N/A	
ISP		51.51.51.1/28		
Branch	eth0	51.51.51.3/28		
outclt	Ethernet	51.51.51.10/28		

第四項

Packet Tracer

Topology



VLAN

ID	Name	Interfaces	Network
10	Student	Fa0/1-5, fa0/24, g0/1-2, Po1	192.168.10.0/24
20	Staff	Fa0/11-15, fa0/24, g0/1-2, Po1	192.168.20.0/24
30	Server	Fa0/21-23, fa0/24, g0/1-2, Po1	192.168.30.0/24
98	Parking	(Unused Ports)	N/A
99	Native	fa0/24, g0/1-2, Po1	N/A
100	Management	fa0/24, g0/1-2, Po1	192.168.100.0/24

管理設定 - ER1, ER2, AS1, AS2

• 設定如圖所示的裝置名稱，網域名稱尾碼為 skills39.tw

• 建立管理帳號 admin，密文密碼為 Skills39

• 建立特權密文密碼 Skills39

• 設定主控台以管理帳號登入

• 設定文字模式網路管理功能，只接受來自 Management VLAN 的主機，以 IETF 標準的加密協定進行登入，請建立一筆名為 ADMIN 的 ACL 協助完成此項目，並應統計不被允許的封包數

• 管理線路，登入閒置 200 秒自動登出。路由器登入後會直接進入特權模式，

ISP

▪ 對 ER1，ER2 介面使用子網路的第一個可用 IP 位址。

▪ 與 Internet 連接的序列介面，以能同時支持 IPv4 及 IPv6 的第二層協定，並加上能防止重播攻擊 (Replay Attack) 的認證協定來設定。連接的裝置為 PR1，金鑰為 PPPchapkey。

▪ 與 Internet 連接序列介面的 IPv4 位址設定遺失了，印象中只記得網路位址分割成點對點網路的最佳化大小。請在網路第二層連通後，嘗試用系統內建功能查出，並完成設定。為防止資訊外流，請在對外介面停用此功能。

▪ 與 PR1 之間，以鏈路狀態路由協定交換路由資訊。

- ■ 程序識別碼 15，路由器識別碼 2.2.2.2。
- ■ 利用介面位址，啟動介面參與路由協定。
- ■ 對 PR1 的區域是骨幹，對 ER1 及 ER2 介面區域是 15。
- ■ 用金鑰識別碼 39 之金鑰 ospfkey，在鄰接路由器介面上，為 OSPF 啟用加密認證。
- ■ 停止非必要介面發送路由協定封包。
- ■ 按比例調整參數，把路由協定收斂時間縮短為預設值的 1/4，如不能整除一律進位。

PC1，PC2

■ 網路介面以自動取得 IPv4 位址的協定運作，應能自 Server 取得位址，並用瀏覽器連接 http://www.worldskills.org 網站。

交換網路 - AS1, AS2

• 如附表建立 VLAN 並分配其介面

• 交換器及連接埠儘量停用相關專屬 (Proprietary) 協定，以保有多廠牌設備的互通性。

• 未使用連接埠放入 Parking VLAN，禁止來自 Parking VLAN 連接埠的流量被轉送至其它網路裝置。所有連接埠依最佳安全實作設定。

IP 網路 – ER1, ER2

• 以 SVI 為附表分配有網路位址的 VLAN 設定 IP 位址，主機位址為路由器名稱尾碼。

• 與交換器連接介面配合交換網路架構設定。

• 未使用交換連接埠放入 Parking VLAN，並依最佳安全實作設定。

• 對 ISP 介面使用子網路的最後一個可用 IP 位址。

高可用度 - ER1, ER2, AS1, AS2

• 兩台交換器之間的接線，請啟用基於 IEEE 協定技術的機制，合併為群組 1 進行備援及負載平衡。

• 啟用各項設定，讓交換網路能在拓樸異動時儘快收斂，並能有自動防止因接線錯誤，導致網路崩潰的功能。

• 使用由 Cisco 提出的 RFC 標準協定，設定 ER1 及 ER2，為 Student，Staff，Server 及 Management VLAN，以各網路的最後一個可用位址，提供網路閘道備援服務。請使用 VLAN 識別碼設定閘道備援群組編號。

• 為進一步平衡負載，調升優先權 5，使 Student 及 Server VLAN 以 ER1 為主要鏈路；Staff 及 Management VLAN，以 ER2 為主要鏈路。主要鏈路路由器要能以預設的優先權參數增減值，設定在 LAN 或 WAN 鏈路故障時進行故障移轉，並在故障鏈路恢復後，回到原本分流模式。

• 交換網路配合 ER1 及 ER2 的分流模式，用最小優先權值，把對應 VLAN 的流量在 AS1 或 AS2 上分流。

第五項

IP 服務

• 在 Server 設定服務，自動配發各所屬網路的第 100 – 199 個可用 IP 位址給 Student 及 Staff VLAN 的用戶端裝置。位址儲存區名稱請用 VLANnn，nn 為 VLAN 識別碼。網域名稱解析交由 IP 位址 8.8.8.8 主機處理。

• 手動設定 Server IP 位址為該 VLAN 的第 10 個可用 IP位址，其它參數比照 DHCP VLAN。

• 手動設定交換器管理介面，使用 Management VLAN 第 N+10 個可用 IP位址，N 為交換器名稱尾碼。

• 設定 ER1，ER2 系統時間自動與 Server 同步，AS1，AS2 手動調整時間。

• ER1，ER2，AS1，AS2 日誌訊息傳送至 Server 儲存。Server 上啟用必要服務以達成本項要求。

• 建立 ACL NAT_ACL 定義組織安全政策允許使用 Internet 的流量：

內部私有網路位址範圍 – 192.168.0.0 – 192.168.255.255

允許流量 – HTTP，HTTPS，DNS，PING。

• 設定使用連接 Internet 介面位址，將符合組織安全政策使用 Internet 的流量進行轉址及轉送。