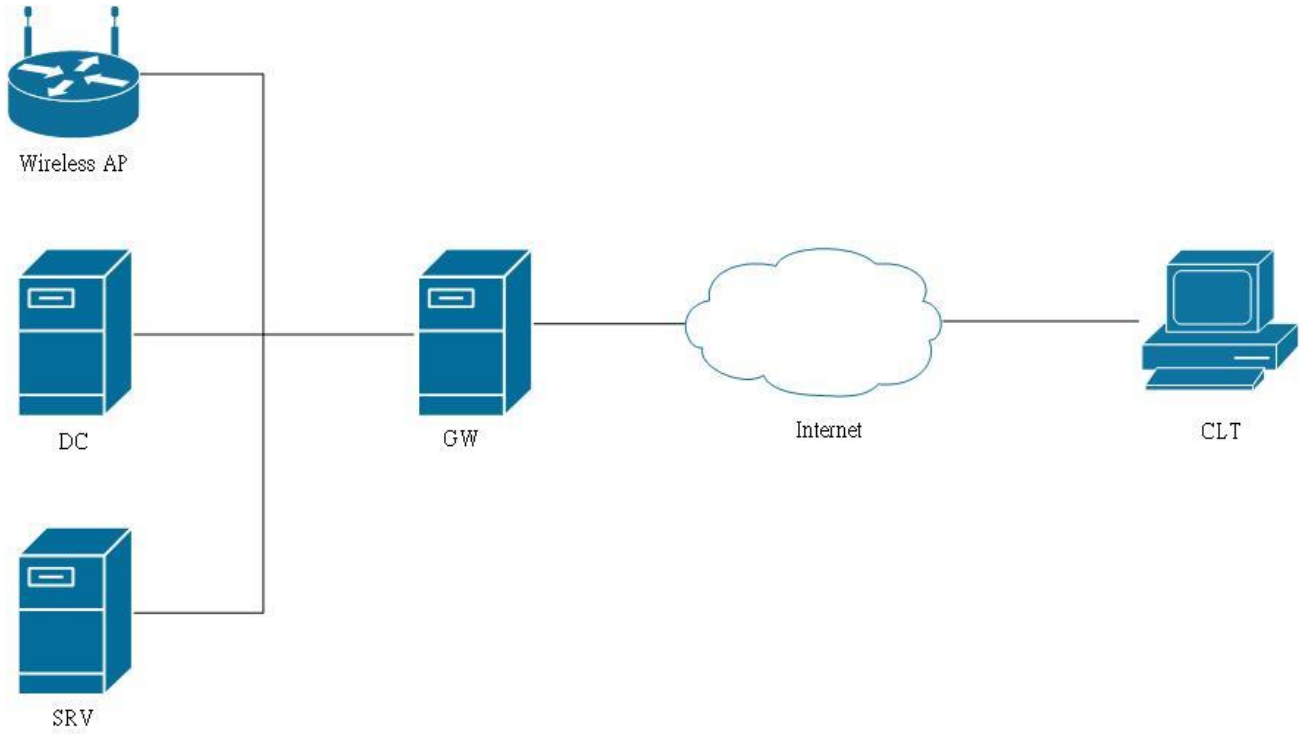
第四十五屆全國技能競賽分區初賽

資訊與網路技術



。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。

。評分前將對所有虛擬系統進行重新啟動的動作，建議選手於競賽結束前預留些許時間，自行關閉虛擬系統。

。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。

。PC1 與 PC2 會預先安裝 Windows Server 2012 R2，並安裝好 VMware Workstation 11 供選手使用。

DC :	Ethernet0	192.168.38.10/23
SRV:	Ethernet0	192.168.38.20/23
	Wlan0	DHCP
GW:	eth0	192.168.39.254/23
	eth1	45.39.105.1/29
CLT:	Ethernet0	45.39.105.2/29
AP:	Mgmt	192.168.38.30/23

- 請在安裝好所有虛擬機後，在 PC1 與 PC2 的桌面建立其所有虛擬機捷徑，並將捷徑名稱設定與主機名稱相同。

DC (Windows Server 2012 R2) :

- 在 PC1 新增虛擬機 DC，並安裝 Windows Server 2012 R2。

- Active Directory

  - 安裝 Active Directory Domain Service，並建立網域 itnsa.org.tw。

  - 根據附錄 A 建立相關使用者，密碼為(none)表示使用者預設無密碼，並且必須在第一次登入時更改密碼。(請保留各群組後三十個使用者用於評分)

  - 密碼須符合複雜性原則，最少 10 字元，且密碼可立即更改並無有效期限。

  - 依附表建立的使用者不能以任何方式或被任何人直接刪除(對使用者點選右鍵刪除)。

  - 啟用相關機制讓被刪除的 Active Directory 物件可以被復原。

  - 由於尚未規劃群組原則，請將所有電腦與使用者群組原則更新時間調整為三小時自動更新一次，並手動執行一次更新以便立即套用此原則。

- DNS

  - 安裝 DNS 服務，擔任 DNS Master 角色，根據需求新增適當的紀錄，並將記錄存放在 Active Directory 中。

  - 限制只允許網域中授權的 Name Server 進行同步。

  - 在 DC 更改區域紀錄後，第一時間通知 SRV 立即進行更新。

- DHCP

  - 安裝 DHCP 服務，配發 192.168.39.101-200 的網段，指定 DNS 為 SRV，GW 為預設閘道，網域名稱為 itnsa.org.tw。

SRV (Windows Server 2012 R2) :

- 在 PC1 新增虛擬機 SRV，安裝 Windows Server 2012 R2

- 加入 itnsa.org.tw 網域，同時擔任內部伺服端與客戶端進行功能測試。

- DNS

  - 安裝 DNS 服務，擔任 DNS Slave 角色，並且每半小時與 DC 同步網域中的 DNS 紀錄，若連續兩小時同步不成功，將會暫停回應 DNS 查詢直到下次成功同步。

- IPAM

  - 安裝 IPAM，監控 DC 的 DHCP 與 DNS 服務。

- Wireless

  - 安裝無線網路介面卡，並用以測試無線路由器功能與 DHCP 功能。

- MMC

  - 建立一個管理主控台，在選單中加入網域裡的服務以便統一管理，並將此主控台存在網域 Administrator 的桌面，命名為 Pre-NSC45-Services.msc (此主控台中會包含所有 DNS 服務，DHCP 服務，IIS 服務與 Active Directory 使用者與電腦)。

  - 在選單中加入一個連結，名為 SRV Web，並在其中顯示 SRV 的首頁

  - 建立並設定完主控台後，更改主控台模式以防止使用者新增或移除選單中的嵌入式管理單元。

- Share Folder

- 建立資料夾 C:\web\，僅允許 Web_Operator 與 Domain Admins 群組讀寫，以 web 名稱分享，分享權限與資料夾權限相同，將隨身碟中附的首頁檔案 Default.htm 放置於此資料夾內，並將首頁標題與內容修改為自己的區域、崗位號碼及姓名。

- IIS

- 安裝網頁伺服器，在預設站台將 C:\web\設置為根目錄，使用 http://www.itnsa.org.tw 瀏覽網頁，不需輸入驗證資訊即可瀏覽。

GW (Debian 7.8.0) :

- 在 PC2 新增虛擬機 GW，並安裝 Debian 7.8.0。

- User Account

- 根據附錄 B 建立相關使用者。

- 在一般使用者登入時，不顯示上次登入時間訊息。

- 在每次 Root 登入時，將訊息"Root Logged in"使用 syslog 功能記錄在/var/log/syslog 中。

- DNS

- 安裝 DNS 服務，替服務外部的網頁提供位址解析服務。

- Web

- 安裝網頁服務，提供外部使用者瀏覽，網址為 http://www.public.itnsa.org.tw/ 。

- 掛載//srv.itnsa.org.tw/web 到本機的/web，並將其設定為首頁根目錄；GW 和 SRV 的首頁會顯示相同的內容。

- 僅允許存取首頁檔案，禁止存取其他檔案 (例:http://www.public.itnsa.org.tw/otherfiles.html) 。

- Firewall

- 允許內部發起任何連線，並只允許外部對 GW 提供的服務(DNS,Web,SSH)主動發起連線，其餘一律丟棄。

- 提供 NAT 轉址服務，讓內部私有網段能夠上網。

- SSH

- 安裝 SSH 服務，提供遠端連線服務。

- 在輸入驗證資訊之前，顯示訊息" This is GW server, only authorized access is allowed !! "。

- 對內網允許使用 port 22 連接，但對外網只允許使用 port 22239 連接。

CLT (Windows 8.1)

- 在 PC2 新增虛擬機 CLT，安裝 Windows 8.1，並關閉初次登入動畫。

- 模擬外部客戶端，配合試題環境模擬，請不要設定 Default Gateway，並將 DNS 指向 GW 主機。

- 根據附錄 C 建立相關使用者。

- 為取得即時 DNS 資訊，請關閉 DNS 正確與錯誤紀錄快取功能。

- 由於 CLT 位於公共位址環境，請在防火牆阻擋所有 RFC1918 所規範的私有位址。

- 將 Putty 複製到使用者 UserXX (XX 為選手崗位號碼) 的桌面，並預先建立一筆利用 SSH 連接到 GW 的設定檔。

AP (Access Point) :

- 設定無線網路 SSID 為 WRLSXX，XX 為選手崗位號碼 (例：1 號崗位應設為 WRLS01)，加密方式為 WPA2 PSK，並將自訂的密碼寫於下方：

  _____

- 關閉內建 DHCP 功能。

Appendix A (Active Directory) :

Username	Group	Password	Office	Telephone
Administrator	Domain Admins	Skills39	F101	0800-453999
IT01-50	IT	(None)	F101	0800-453901
ACCT01-50	Accounting		F102	0800-453902
DEV01-50	Development		F103	0800-453903
Web_Operator	Domain Users	Skills39	F104	0800-453904

Appendix B (GW Local Users) :

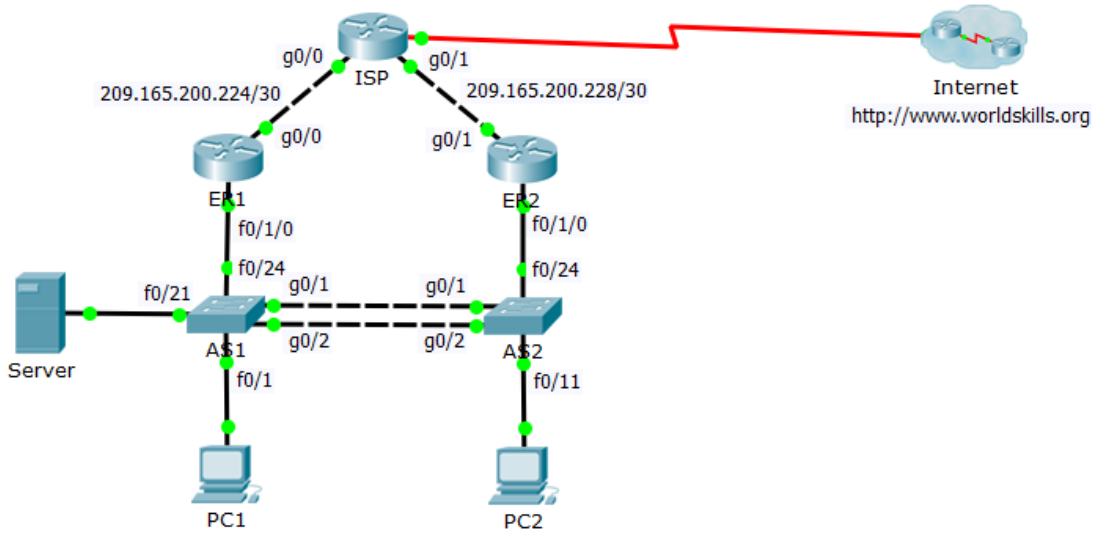
Username	Group	Password
Kevin	Officials	Skills39
Jerry		
Kobe		
Liang		

Appendix C (CLT Local Users) :

Username	Group	Password
Administrator	Administrators	Skills39
UserXX		

XX 為選手崗位號碼 (例：1 號崗位使用者名稱應為 User01)

PACKET TRACER DESCRIPTION



VLAN Table & Interface Assignment Information:

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，

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。

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。

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**，在鄰接路由器的介面上，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。