

第 48 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 9 頁。

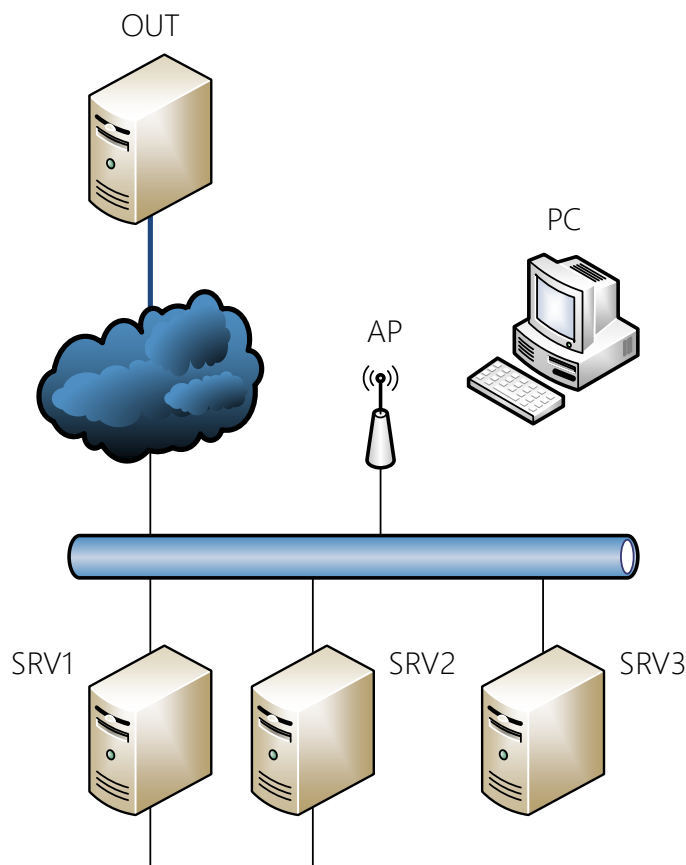
比賽後請將本試題及評分表留在崗位上，不得攜出賽場。





第四十八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



General Setting

- 請替所有虛擬機安裝 VMware Tools。
- 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。
- 關閉所有 Windows 作業系統初始登入動畫
- 所有作業系統皆須允許 ICMP 協定
- 評分時將會檢查崗位整潔度與線材製作品質

OUT

- 設定 NTP 服務，提供公司內部伺服器 SRV1 與 SRV2 校時
- 設定 DNS 服務，提供 outside.out 網域名稱解析，請依據題目需求建立相關正解與反解紀錄
- 設定 Web 服務，可透過 <http://www.outside.out/> 瀏覽公司外部網站，並在首頁顯示 "Public Site for National Skills Competition"

SRV1

- 根據附錄 C 設定使用者與密碼
- 設定 Web 服務
 - 提供 [http\[s\]://www.wsdomain.com.tw/](http[s]://www.wsdomain.com.tw/) 瀏覽公司內部網站，並在首頁顯示 "Internal Site for XXX Corporation"
 - 提供 HTTP 與 HTTPS 連線
 - 提供 <http://www.wsdomain.com.tw/outside> 連接至公司外部網站
 - 提供 <http://www.wsdomain.com.tw/file> 連接至 SRV2 的分享資料夾 /share/file，在網頁上顯示檔案清單
 - 設定基本驗證，登入使用者 nsc 後即可在網頁上下載檔案
- 設定 SSH 服務，僅允許本機使用者 nsc 登入
- 與 NTP 伺服器 OUT 進行校時
- 設定 IPTables，僅放行必要的流量進入，其餘一律拒絕



SRV2

- 根據附錄 C 設定使用者與密碼
- 設定 Samba 服務，服務僅聆聽於與 SRV1 對接的介面
 - 分享 /share/web 提供 SRV1 網頁服務掛載
 - 分享 /share/file 提供檔案分享
- 設定 SSH 服務，僅允許 SRV1 使用密碼登入，其餘連線皆須使用 SSH Key 做驗證
- 與 NTP 伺服器 OUT 進行校時

SRV3

- 架設網域 wsdomain.com.tw，並依據附錄 B 建立 130 個公司使用者帳號
- 設定 DNS 服務，提供 wsdomain.com.tw 網域名稱解析，請依據題目需求建立相關正解與反解紀錄
 - 將 outside.out 的 DNS 請求轉送給 OUT
- 設定 DHCP 服務，提供內網自動取得 IP
- Head Quarter 群組使用者登入網域後，桌面上會自動提供 Putty 連接
 - 自動設定 Default Profile，讓使用者開啟 Putty 後，不用任何設定就可以直接連線至 SRV1 (提示：設定會儲存在 HKCU\Software\SimonTatham 裡)
- 網域電腦需自動信任公司內部網站使用的 SSL 憑證

PC

- 加入網域 wsdomain.com.tw
- 安裝無線網卡，利用無線 AP 連接至公司內部網路

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。



Appendix A - IP Address Assignment

VM Hostname	OS	Host PC	Interface	IP Address	Default Gateway
OUT	Windows Server 2016	PC1	Ethernet	12.34.56.78/28	N/A*
SRV1	Debian 9		eth0	192.168.100.201/24	192.168.100.1
			eth1	10.0.0.1/30	N/A*
SRV2	Debian 9		eth0	192.168.100.202/24	192.168.100.1
			eth1	10.0.0.2/30	N/A*
SRV3	Windows Server 2016	PC2	Ethernet	192.168.100.203/24	192.168.100.1
PC	Windows 10		Ethernet	DHCP	
AP			WAN	12.34.56.77/28	N/A*
			LAN	192.168.100.1/24	N/A*

* 若預設閘道為 N/A，則請勿做任何設定

Appendix B - Domain Users

Username	Group	Password
Administrator	Domain Admins	Skills39
HQ01-50	Head Quarter	
BRANCH01-30	Branch	
SALES01-50	Sales	

Appendix C - Linux Local Users

Username	Group	Password
root	root	Skills39
nsc	LSAdmin	



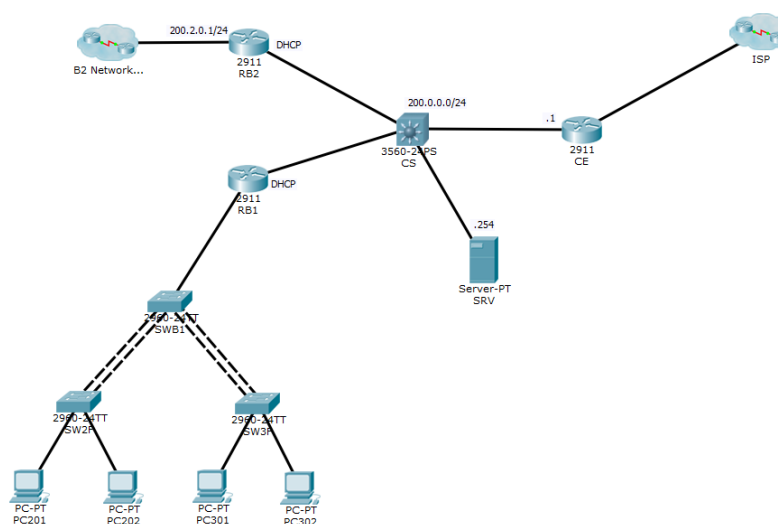
Packet Tracer 試題

作答說明

本題目的初始檔在崗位隨身碟裡，請複製至電腦桌面，並使用 Cisco Packet Tracer 開啟進行作答。

完成後，請存檔為 "崗位編號-姓名.pka"，並複製回崗位隨身碟，供裁判評分。

Network diagram





General settings for all routers

- 設定如圖所示的裝置名稱與介面 IP 位址
- 建立本機使用者 locadmin，密碼為 Skills39，並將密碼以 Type-7 密文形式儲存
- 設定進入 Privileged EXEC Mode 的密碼為 pa15，並以 MD5 Salt Hash 形式儲存
- 以 Console 接入設備進行管理時，需輸入密碼 Skills39，登入系統後，將直接進入特權模式 (Privileged EXEC Mode)
- 以 Telnet 連入設備進行遠端管理時，需以本機使用者帳號進行驗證
- 僅開放 2 組 VTY 管理通道，其餘通道以「不受理任何連入協定」的方式關閉
- (見附圖)若已有一組 VTY 通道正在使用中，將於第二筆連線建立後顯示：

Warning: Another user currently logged in!

```
PC>telnet 1.2.3.4
Trying 1.2.3.4 ...Open
User Access Verification

Username: admin
Password:
Sample>
Sample>telnet 1.2.3.4
Trying 1.2.3.4 ...Open
Warning: Another user currently logged in!

User Access Verification

Username: admin
Password:
Sample>
Sample>telnet 1.2.3.4
Trying 1.2.3.4 ...Open

[Connection to 1.2.3.4 closed by foreign host]
```



General settings for all switches

- 設定如圖所示的裝置名稱
- 設定進入 Privileged EXEC Mode 的密碼為 pa15，並以明文形式儲存
- 以 Console 接入設備進行管理時，需輸入密碼 Skills39
- 停用 VTP，並依下表建立 VLAN 並指派至正確的介面

Name	Interface Assignment	Network
ROOM1	SWB1: Fa0/21 – Fa0/24, Gi0/1 SW2F: Fa0/1 – Fa0/6, Fa0/21 – Fa0/22 SW3F: Fa0/1 – Fa0/6, Fa0/21 – Fa0/22	200.1.1.0/24
ROOM2	SWB1: Fa0/21 – Fa0/24, Gi0/1 SW2F: Fa0/7 – Fa0/12, Fa0/21 – Fa0/22 SW3F: Fa0/7 – Fa0/12, Fa0/21 – Fa0/22	200.1.2.0/24

Sector B1 inter-VLAN routing

- 在 RB1 連接用戶的介面上設定 Router-on-a-stick，子介面編號與 VLAN ID 一致
- 分別以第一個可用位址，設定為所有 VLAN 網段的 Gateway
- 設定 DHCP Relay Agent，讓所有 VLAN 的用戶端可經由 SRV 取得 IP 位址



Core networking

進行本階段的設定時，不可使用下列指令：

1. (config)#ip route
 2. (config-router)#router-id
 3. (config-router)#log-adjacency-changes
 4. (config-router)#default-information originate
 5. (config-if)#ip ospf dead-interval
- 設定 RB1 與 RB2 經由 DHCP 取得 Gi0/1 介面的 IP 位址
 - CE 上已預先進行了 DHCP Server 的部分設定，選手僅需修正既有的問題，並依試題需求完成設定
 - 於所有路由器上啟動 OSPF Process 1, 交換路由資訊
 - 將 RB1 連接用戶的內部網段宣告為 Area 1
 - 將 RB2 連接用戶的內部網段宣告為 Area 2
 - 若超過 1 分鐘仍未收到鄰居發送的 OSPF 相關封包，則判定對方已下線並中斷鄰居關係
 - 於 RB1 上進行設定，將內部所有 VLAN 網段合併為一筆/16 的摘要路由
 - 為避免 OSPF 將 GigabitEthernet 高速介面與 FastEthernet 介面的傳輸效能誤判為相同，請進行相關的調整，使其能分辨最高達 10 Gigabits 的介面頻寬差異
 - RB1 與 RB2 的路由表上須有一筆指向 CE 的 Default Route
 - 在 RB1 上觀察 OSPF 鄰居狀態時，須包含與下圖一致的資訊：

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.255.255.0	10	FULL/DR	00:00:31	200.0.0.1	GigabitEthernet0/1
10.255.255.2	0	2WAY/DROTHER	00:00:30	200.0.0.3	GigabitEthernet0/1



Sector B1 switching

進行本階段的設定時，除 SWB1 的 Gi0/1 介面之外，所有交換器的介面上不得存有任何

Spanning Tree 相關設定

- 於所有交換器上進行設定，在連接其他交換器的介面上停用 DTP，並將連接非交換器設備的介面設定為 802.1w Edge Port
- VLAN ROOM1 的 Root Bridge Priority 為 13159，VLAN ROOM2 則為 21352
- 在 SWB1 上觀察 VLAN ROOM1 與 ROOM2 的 Spanning Tree 運行狀態時，須包含與下圖一致的資訊：

Interface	Role	Sts	Cost	Prio.	Nbr	Type
Fa0/21	Desg	FWD	100	128	.21	P2p
Fa0/22	Desg	FWD	19	128	.22	Shr
Fa0/23	Desg	FWD	100	128	.23	P2p
Fa0/24	Desg	FWD	19	128	.24	Shr
Gi0/1	Desg	FWD	19	32	.25	P2p

- SW2F 與 SW3F 的 Fa0/1 – Fa0/12 介面僅用於連接終端設備，完成相關設定，若單一介面同時有兩部以上的裝置接入，將於 SRV 上產生 Syslog 事件記錄，並僅允許第一個接入的裝置上網

CE 的對外連線已預先做好設定，完成上述試題後，PC 應能成功以 DHCP 取得 IP 位址，可用以驗證網路的連通性以及瀏覽位於 test.yisp.net 的測試網頁