第 49 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	

裁判長宣佈前請勿翻閱試題或進行任何操作。

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 8 頁。

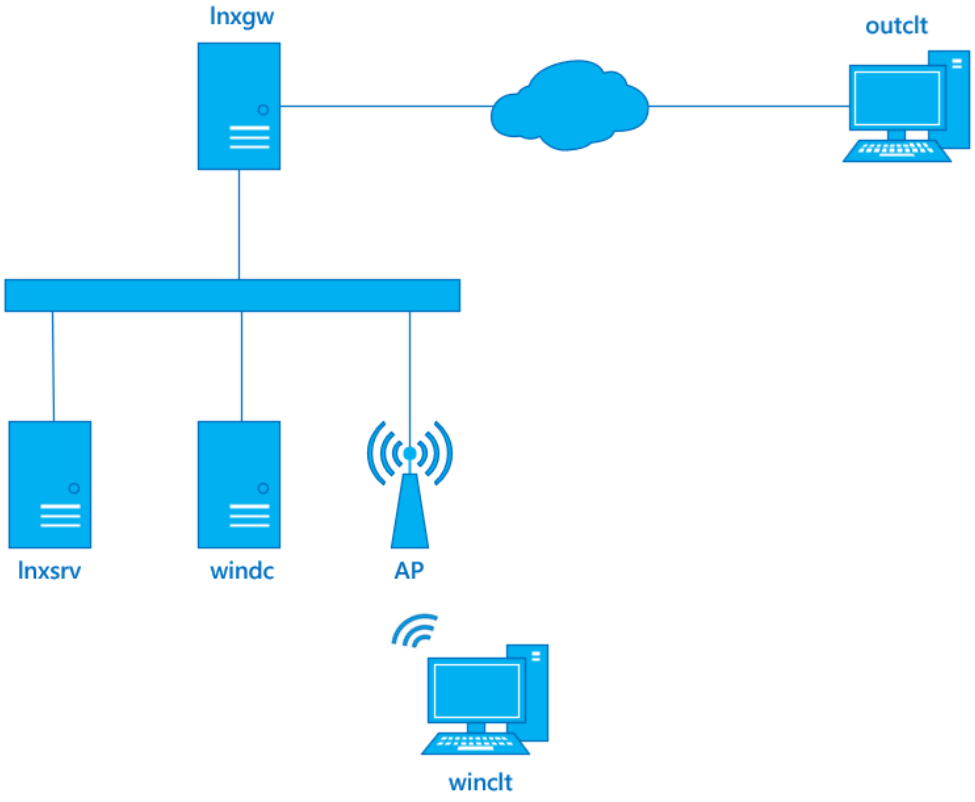
比賽後**請將本試題**及**評分表留在崗位上**，不得攜出賽場。

49th 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

請替所有虛擬機安裝 VMware Tools
請替所有 Debian 系統安裝 CURL Tool，便於測試功能



windc

- 安裝 Windows Server 2019 於 PC1，模擬內部伺服器，並依照附錄 A 設定 IP 位址與主機名稱。
- 安裝 Active Directory 服務，並建立 nsc49.skills.tw 網域，並依照附錄 B 建立使用者。
- 請建立三個 OU，命名為 ADDCs、SRVs、CLTs，分別放置組織內所有的網域控制站、成員伺服器、用戶端系統。
- 建立網域時，套用至網域控制站的預設設定組，在進行今日工作項目時，應予以保留並維持套用
- 安裝 DNS 服務，並依照題目需求建立相關的資源紀錄。
- 安裝 DHCP 服務，範圍設定為 192.168.1.100 至 200，並設定 192.168.1.150 供 winclt 固定取得。
- 設定 GPO，並以下列所需設定: (此項將只需套用至組織內的用戶端系統)
  - 關閉電腦初始登入動畫。
  - 在登入時，登入清單上將不會顯示上一個登入的使用者。
  - 無法存取控制台。
- 設定 Share Folder，並以下列所需設定:
  - 依附錄 D 設定分享 \\windc.nsc49.skills.tw\web 給 webManager 使用者管理公司網頁。
  - \\windc.nsc49.skills.tw\web 將在 webManager 登入時自動掛載至 W:。
  - (繼上) 僅允許存放 *.jpg、*.php、*.css、*.html 四種檔案，並限制只能使用 1G 的容量。
  - 提供給 lnxsrv 掛載。
- 安裝 CA 服務，配發憑證供網域內及外部網頁伺服器使用
  - CA 名稱為 NSC49 CA
  - 當 outclt 及 winclt 瀏覽 HTTPS 網頁時，不可出現憑證錯誤訊息。

lnxsrv

- 安裝 Debian 9.8 CLI 於 PC1，模擬內部伺服器，並依照附錄 A 設定 IP 位址與主機名稱。
- 以附錄 C 新增使用者。
- Users 群組的使用者不可變更自己的密碼，其餘使用者皆可。
- 當一般使用者登出 (root 不需) 時，紀錄至 /var/log/logout/<username>_logout.log，格式為 "<date> - <username> Logout"。
- 安裝 WEB 服務，並依下述需求設定:
  - 提供 http://www.nsc49.skills.tw/ 及 https://www.nsc49.skills.tw/ 站台。
  - 掛載 \\windc.nsc49.skills.tw\web 至 /web 作為此站台的根目錄。
  - 網頁首頁請使用隨身碟裡的檔案。(請記得放至\\windc.nsc49.skills.tw\web)
  - 當 Client 使用未加密協定瀏覽此站台時，自動轉向至加密協定。
  - (繼上) 請使用不會改變 HTTP Method 的方式完成自動轉向。

- 安裝 SSH 服務，並以下列所需設定:
  - 允許 root 登入
  - 請限制 SSH 服務使用一般化的方式進行驗證 (使用者嘗試登入時，由後端的驗證模組直接認證登入資訊，而非透過 SSH Server)

lnxgw

- 安裝 Debian 9.8 CLI 於 PC2，模擬內部 Gateway 及 Firewall，並依照附錄 A 設定 IP 位址與主機名稱。
- 安裝 DNS 服務，並以下列所需設定:
  - 管理 public.nsc49.skills.tw 網域，供外部 Client 使用。
- 設定 Firewall 服務，並以下列所需設定:
  - 讓外部使用者可由 https://www.public.nsc49.skills.tw/ 瀏覽內部網頁

  註: 內容會與 https://www.nsc49.skills.tw/ 一致。
  - 讓內部網路可以使用外部網卡的 IP 上網。
  - 對外僅開放所需之流量，請以最嚴謹的方式實施。

winclt

- 安裝 Windows 10 於 PC2，模擬內部 Client 進行測試，並依照附錄 A 設定 IP 位址及主機名稱。
- 安裝 Wireless 網卡，測試 Wireless 功能
- 加入 nsc49.skills.tw 網域

outclt

- 安裝 Windows 10 於 PC2，模擬外部 Client 進行測試，並依照附錄 A 設定 IP 位址及主機名稱。
- 簡單建立一個使用者 (名稱不限)，進行測試。
- 允許 ICMP 協定，讓內部網路可以測試上網
- 在瀏覽器上輸入 myfirewall 時，可以檢視本機 Windows 防火牆的日誌紀錄

AP

- 模擬內部 Wireless Router，並依照附錄 A 設定 IP 位址。
- 設定 SSID 為 NSCXX (XX 為崗位號碼，若您的崗位號碼為 01 則設定為 NSC01，以此類推)。
- 設定驗證方式為 WPA2-PSK，並使用 AES 作為加密機制。
- 請將設定之密碼寫於下方，評分時將會根據此密碼進行評分:

_____

- 關閉內建 DHCP 功能。

Appendix A

VM HostName	OS	Host PC	Interface	IP Address /Submask	Default Gateway	DNS
windc	Windows Server 2019	PC1	Ethernet	192.168.1.10/24	192.168.1.1	127.0.0.1
lnxsrv	Debian 9.8		eth0	192.168.1.20/24	192.168.1.1	192.168.1.10
lnxgw	Debian 9.8	PC2	eth0	192.168.1.1/24		192.168.1.10
			eth1	100.100.1.1/30		
winclt	Windows 10		Wi-Fi	Via DHCP		
outclt	Windows 10		Ethernet	100.100.1.2/30		100.100.1.1
AP			LAN	192.168.1.30/24		

※ 請勿建立與比賽無關的網卡及設定

Appendix B

UserName	Group	Password
IT01 – IT50	Information Technology	Skills39
RD01 – RD40	Research and Development	
SRV01 – SRV10	Service Management	
webManager	WebManagers	

Appendix C

UserName	Group	Password
admin01 – admin10	Admins	Skills39
user001 – user100	Users	

Appendix D

Local Path	Share Path	Permission	Mount at
C:\web	\\windc.nsc49.skills.tw\web	webManager	W:

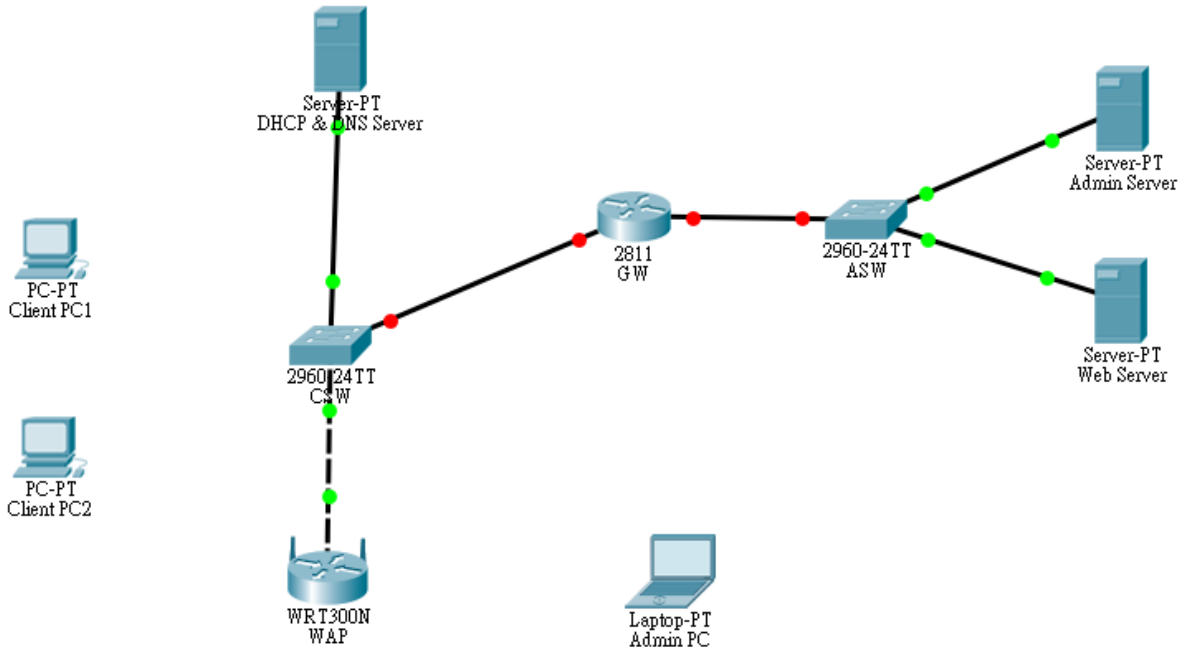
Cisco Packet Tracer Activity

請用 Cisco PacketTracer 開啟隨身碟裡的 PKA 檔完成下列任務，並注意存檔。在比賽終了前，請將存檔更名為 崗位號.PKA，存入隨身碟以便評分。

介面位址設定

Device	Interface	IP Address
GW	Fa0/0	IPv4: 1st usable host address IPv6: 2001:db8::1
	Fa0/1	IPv4: 1st usable host address IPv6: c:1:5:c:0:ffff::1
CSW	Management SVI	IPv4: 2nd usable host address
ASW	Management SVI	IPv4: 2nd usable host address
WAP	LAN	IPv4: 3rd usable host address
DHCP & DNS Server		IPv4: 192.168.0.5 IPv6: 2001:db8::5
Admin Server		IPv4: 192.168.0.140 IPv6: c:1:5:c:0:ffff::140
Web Server		IPv4: 192.168.0.135 IPv6: c:1:5:c:0:ffff::135
Admin PC		IPv4: via DHCP IPv6: via SLAAC
Client PC1		IPv4: via DHCP IPv6: via SLAAC
Client PC2		IPv4: via DHCP IPv6: via SLAAC

※本試題中所有 IPv4 網段均由 192.168.0.0/16 依序切割劃分



GW, ASW, CSW

。設定如拓樸圖所示的裝置名稱
。建立使用者 admin，密碼為 Skills39
。以 Console 接入裝置進行管理時，需輸入密碼 Skills39
。遠端連線至裝置進行管理時，需經使用者驗證方可登入
。登入管理介面後，若要切換為 Privileged EXEC Mode，應輸入密碼 Skills39
。將 Console 密碼以可逆密文形式儲存，使用者密碼與 Privileged EXEC Mode 的驗證密碼則以不可逆密文形式儲存
。僅允許以 SSH 方式進行遠端管理

GW

。請自行排除相關問題以順利存取該設備的指令介面
。依附表所示設定介面的 IP 位址
。Fa0/0 介接的 IPv4 網段應為 100 人使用的網路進行最佳化，請依此資訊計算出適宜的子網路遮罩
。Fa0/1 介接的 IPv4 網段將在未來擴展至最多 5 台伺服器，請計算出適宜的最佳化子網路遮罩
。Fa0/1 的 IPv6 位址，Interface ID 長度需與「IPv4 位址的總長度」相同
。未來於該裝置上設定的所有密碼，長度至少須為 7 碼
。為避免 SSH 管理遭暴力破解，若每分鐘內登入失敗次數達 3 次，則禁止登入 5 分鐘

DHCP & DNS Server

。依附表所示設定介面的 IP 位址
。啟用 DHCP 服務，可配發的位址範圍為 192.168.0.21 – 192.168.0.99
。設定 DNS，將 www.nsc49.tw 與 ftp.nsc49.tw 均對應至 192.168.0.135
。為便於未來的管理，若伺服器的 IP 位址在未來需要更動，僅需重新設定 www.nsc49.tw 的記錄，ftp.nsc49.tw 的記錄即可自動對應

Admin Server

。該伺服器暫不提供網路服務，目前僅規劃用以遠端管理網路設備，請依附表所示設定介面的 IP 位址

Web Server

。該伺服器的網路服務已預先設定完成，請依附表所示設定介面的 IP 位址

WAP

。該裝置僅作為無線網路存取點使用，不須設定為整合路由器
。依附表所示設定管理介面的 IP 位址
。提供 802.11n 無線網路服務，SSID 為 Skills39
。啟用 WPA2 保護，連線至無線網路時，需輸入密碼 Skills39
。關閉 Beacon 訊息的發送

Admin PC, Client PC1, Client PC2

。完成無線存取點設定後，Admin PC 即會自動連線至無線網路
。將 Client PC1 與 Client PC2 接入網路
。該環境目前僅剩下接頭兩端採用不同 EIA/TIA 568 標準的網路線材，請在 Packet Tracer 上選用該線材，將 PC 連線至 CSW
。CSW 上的 Fa0/13 – Fa0/24 規劃給用戶端使用，請依介面編號的順序接線
。請確保 Client PC1 使用網路時，將會啟用 CSMA/CD 機制
。請確保 Client PC2 使用網路時，將會啟用 CSMA/CA 機制
。由「DHCP & DNS Server」取得 IPv4 位址等資訊
。由 GW 取得 IPv6 預設閘道資訊，並使用無狀態自動設定產生 IPv6 位址

ASW

。依附表所示設定管理介面的 IP 位址

CSW

。依附表所示設定管理介面的 IP 位址
。若於用戶端介面偵測到訊框偽造 GW 的 BIA，則丟棄該訊務，並於 RAM 中留存事件紀錄備查
。試題中要求將 PC 連接至 CSW，而線材的選擇其實並不正確，但網路卻能夠正常連通，此現象歸功於 Cisco 交換器所支援的某種功能，試問若要關閉該功能，應如何進行設定？請將指令未經縮寫的完整內容，設定為 CSW 的每日訊息 (Message Of The Day)

※完成後，網路應可正常通訊，並能夠以 http://www.nsc49.tw 瀏覽 Web Server 上的網頁