第四十六屆國際技能競賽國手選拔賽

資訊與網路技術 Day 1 環境設計與規劃

第一站

請選手設計出一個公司內部環境，可以避免任何的單點故障（Single Point of Failure），並且需要在故障發生後盡快讓服務恢復正常運作。

故障發生點可能會是任意作業系統當機，任意服務突然停止，路由器 / 交換器故障等等。

環境提供的服務與功能：

- 基礎網路連通性（Network Connectivity）
- 網域服務（Active Directory）
- 名稱解析服務（DNS）
- 自動配發 IP 服務（DHCP）
- 郵件服務（Mail）
- 網頁服務（Web）
- 檔案分享服務（File Share）
- 各服務 SSL 加密（AD、Mail、Web、File Share）

環境規劃要求：

- 請將公司內網與 Internet 區隔開，僅將必要服務開放對外
- 開放 Internet 存取的服務請勿使用未加密的協定，例如 HTTP、SMTP 或是 Telnet 等
- 公司內部請客戶端規劃專用網段，隔離伺服器主機與客戶端主機
- 公司對外規畫兩條外線，請自行規畫 WAN 端的備援方案
- 可用的 Public IP 為 140.150.160.0/28，用戶端使用私有 IP 位址

第二站

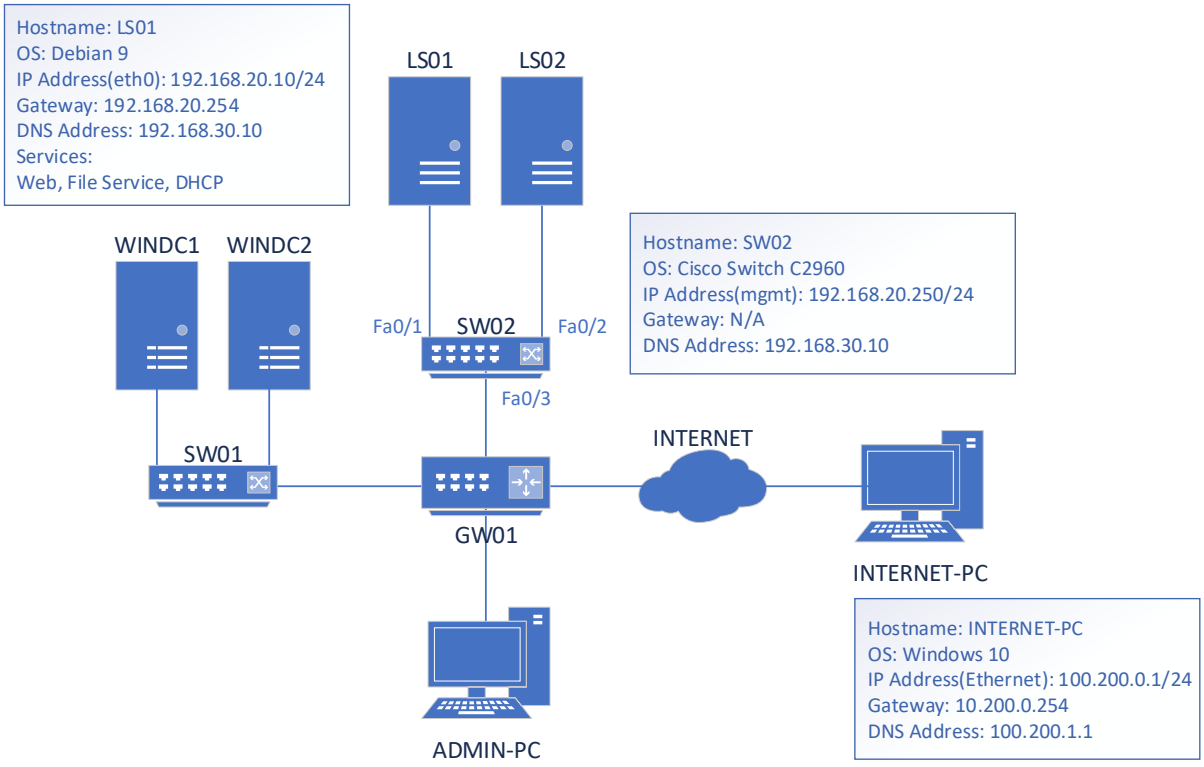
選手要做的事情 ：

- 畫出網路拓樸，並規劃合理的 IP 設定與實體接線
- 寫出各服務將使用的備援機制原理。請參考以下簡短範例：

  > Active Directory ：在網域中安裝兩台 AD，一台是 WINDC1，另一台是 WINDC2。DC 之間會頻繁的定時同步資源，且在特定事件發生時額外觸發同步。當一台 DC 無法提供服務時，網域內會自動偵測並改用其餘正常運作的 DC。

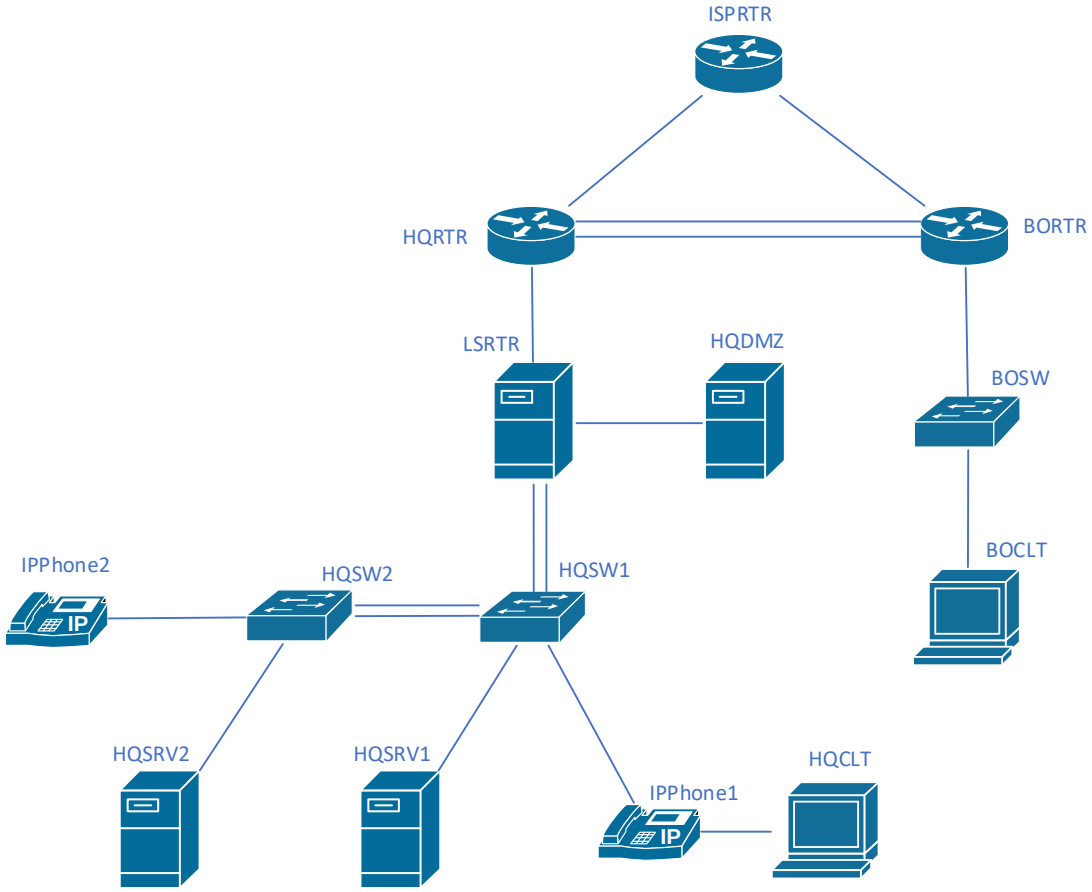
- 請務必詳細寫出所有主機名稱，備援機制與原理，測試用的方法或是 URL，與預計復原時間與根據

範例網路拓樸：


Hostname: LS01
OS: Debian 9
IP Address(eth0): 192.168.20.10/24
Gateway: 192.168.20.254
DNS Address: 192.168.30.10
Services:
Web, File Service, DHCP
LS01
LS02
WINDC1
WINDC2
Fa0/1
SW02
Fa0/2
Hostname: SW02
OS: Cisco Switch C2960
IP Address(mgmt): 192.168.20.250/24
Gateway: N/A
DNS Address: 192.168.30.10
Fa0/3
SW01
INTERNET
GW01
INTERNET-PC
ADMIN-PC
Hostname: INTERNET-PC
OS: Windows 10
IP Address(Ethernet): 100.200.0.1/24
Gateway: 10.200.0.254
DNS Address: 100.200.1.1

第四十六屆國際技能競賽國手選拔賽

資訊與網路技術 Day 2 環境整合



。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

第三站

網路架構

- 在 LSRTR 與 HQSW1 之間的兩條線路設定 LACP
- 在 HQRTR 與 BORTR 之間的專線設定 MLPPP，使其同時運作，加大頻寬；
  並使用 MPPE 加密此專線上的流量
- 設定 HQ 的兩台交換器
  - 根據附錄 B 設定交換器 VLAN
  - 設定交換器使其支援 Extended VLAN，並且請勿啟用 VTPv3
  - 兩台交換機之間請用 LACP 協定做 Link Aggregation
    - 設定為 802.1q Trunk，並且只允許必要的 VLAN 通過
  - 設定 spanning tree
    - HQSW1 為 VLAN10 的 Root Bridge
    - HQSW2 為 VLAN20 的 Root Bridge
  - 所有的 Access Mode 介面在接到終端設備時須直接進入到 Forwarding State
  - 若在 Access Mode 介面收到 BPDU，則鎖定介面 10 分鐘
  - 阻擋所有在 Access Mode 介面收到 DHCPOFFER 與 DHCPACK 封包
  - 其餘沒使用的介面請全部關閉
- 公司內部跑 RIPv2（HQRTR，BORTR 與 LSRTR）
  - HQRTR 與 BORTR 之間路由交換於 GRE Tunnel
  - 僅在必要的介面啟用路由協定
- Internet 跑 OSPFv3（HQRTR，ISPRTR 與 BORTR）
  - 僅在必要的介面啟用路由協定
  - ISP 負責發佈 OSPF Network-LSA 資訊給連結上所有的 OSPF 鄰居
  - ISP 負責發佈 Default Route 給 HQRTR 與 BORTR，不允許使用 always 關鍵字
- 於 HQRTR 和 BORTR 之間建立 VTI，加密雙方 Internet(經 ISP)路徑的流量
  - 啟用 PFS，Hash 使用 SHA512，加密模式為 AES256，DH Group 為 ECP521
- 將 HQRTR 跟 LSRTR 之間的流量加密，使用非對稱的 Pre-shared key

第四站

系統服務

HQDMZ（Windows Server 2016）

- 安裝 Active Directory，根據附錄 C 建立使用者與群組
  - 啟用 LDAPS
  - 使用者登入網域後，自動掛載資料夾
    - 群組資料夾（G）：\\share.kazan.ru\groupshare\%groupname%
    - 個人資料夾（S）：\\share.kazan.ru\share\%username%
    - 使用者只能看到各自群組或是自己的資料夾
    - 各群組資料夾可使用的最高容量為 2GB
    - 禁止存放執行檔（.exe，.bat，.ps1）
- 安裝 CA
  - 根憑證命名為 WSC2019-CA
  - 設定 CRL 位址為 http://cert.kazan.ru/CertEnroll/WSC2019-CA.crl，並且確認 CRL 正常運作
  - 自動發放使用者憑證，使用者登入網域中的任何一台電腦都使用同一張使用者憑證，不會再重新產生新的使用者憑證
- 安裝 IIS
  - 提供公司內外部網站 www.kazan.ru/，並設定備援與同步
    - HQDMZ 與 HQSRV1 之間，HQDMZ 為主要主機，HQSRV1 為備援主機，不進行負載平衡。
      - 當 HQDMZ 無法連接時，HQSRV1 自動切換為主要主機
      - 當 HQDMZ 恢復正常提供服務時，HQDMZ 則自動切換回主要主機
    - 即時同步 HQDMZ 與 HQSRV1 的根目錄內容與站台設定
    - 在早上 6 點到午夜 12 點(UTC+8)的時候同步限速 512Kbps，其餘時間不限速
    - 自動將 HTTP 導向至 HTTPS
    - 自動將 http(s)://kazan.ru 導向至 https://www.kazan.ru
  - 提供公司內部頁面 https://sso.kazan.ru/
    - 使用 Active Directory 作為驗證資訊，並實作 SSO，讓網域內使用者不用輸入驗證資訊即可瀏覽
    - 於此頁面中顯示目前正在瀏覽的使用者名稱

HQSRV1（Windows Server 2016）

- 設定分享資料夾，使用 iSCSI 掛載的硬碟
- 安裝 IIS，並依據 HQDMZ 的需求做相對應的設定
- （或是 HQSRV2）安裝 Radius 服務，並依據 Cisco 設備驗證需求做相對應的設定

HQSRV2（Debian 9）

- 新增兩個 10G 硬碟，使用 LVM 分割硬碟，以利未來增加空間
  - 分配各 5G 空間給 FTP 與 iSCSI
- 安裝 FTP 服務
  - 僅提供 SSL 加密，且將根目錄限制於/ftp
  - 僅允許使用者 ftpuser 存取
- 安裝 iSCSI 服務，使用 LVM 切出的 5G 硬碟空間
- 安裝 LDAP 服務，提供獨立目錄空間做其他驗證服務
  - 建立目錄 internal.kazan.ru
  - LDAP 需啟用 LDAPS，使用 HQDMZ 所簽發的憑證
  - 根據附錄 D 建立使用者與群組
  - 目錄內的使用者可以登入本機
- 安裝 Cacti
  - 監控 HQRTR 與 BORTR 的所有啟用介面流量，網址為 https://cacti.kazan.ru
  - 登入 Cacti 時請使用 HQSRV 上的 LDAPS 做驗證
- 安裝 FTP 服務
  - 僅提供 SSL 加密，且將根目錄限制於/ftp
  - 僅允許使用者 ftpuser 存取
- （或是 HQSRV1）安裝 Radius 服務，並依據 Cisco 設備驗證需求做相對應的設定
- 設定 SNMP 服務
  - 當網域 kazan.ru 使用者登入網域失敗或是帳號被鎖定時，HQDMZ 會主動以 SNMP 知會 HQSRV2，並將這些紀錄顯示於 https://audit.kazan.ru

設備存取限制

- 在所有 Cisco 設備設定 SSH，並完成以下功能
  - 新增一個 admin 的特權使用者，避免 AAA 無法連線時使用
  - 新增 enable 密碼為 Skills39，避免 AAA 無法連線時使用
  - 向 HQSRV1 或 HQSRV2 上的 Radius 進行身分驗證，包含 enable 密碼驗證
    - 使用者 user01 登入後即有 privilege level 15 權限
    - 使用者 user02 登入後僅有 privilege level 1 權限
- 在 HQSRV2 安裝 SSH 服務
  - 除了 HQDMZ 可以使用密碼登入 root 之外，其餘的電腦要登入 root 必須同時使用兩個不同的私鑰才能登入
  - 兩個私鑰需先被 AES 演算法進行加密，再被 Key Derivation Function 迭代（Iteration）100 次，key 為 Skills39
  - 預先在 HQCLT 登入 IT01 使用者，並在桌面上設定好 Putty Profile 供評分使用
- 於 ISPRTR 設定 Telnet，並完成以下功能：
  - Telnet 連線僅允許由連接 HQRTR 的介面進入
  - SSH 連線僅允許由連接 BORTR 的介面進入
  - 為確保 ISPRTR 上的介面 IP (包括 Loopback)不論在未來如何異動，此限制原則將維持運作，不須再進行任何調整，上述設定必須僅以「連線進入的介面」為判定放行與否的依據，禁止以基於 ACL 比對的方式完成此需求

語音通訊

在 HQDMZ 上設定 CME 服務，提供公司內部語音通話

- CIPC 請安裝於 HQCLT
- 以附件提供的 MOH.au 作為話機等待對方時的音樂
  - 告知話機已 UDP Port 4000 來接收 MOH（Music On Hold）的訊號
  - CIPC 將無法聽到 MOH
- 將話機與 CIPC 註冊於 CME 中
  - （User01）IP Phone 1 使用號碼 1011
  - （User02）CIPC 使用號碼 1021
  - （User03）IP Phone 2 使用號碼 1031
- 所有話機中設定電話目錄，可以在目錄中找到三個使用者的名稱與電話
- 所有話機中自己的號碼與撥出的號碼皆須以使用者名稱來顯示
- 所有話機中的 Button 2 與 3 可以用來打給另外兩支電話
- 所有話機中的 Button 4 可以用來代接他人的來電
- 所有話機中顯示訊息 " HQ Office IP Phone "
- 所有話機中可通話的時間為 08:00 到 17:00，撥打 1234 來解除限制
- 撥打 1999 時所有話機皆會同時響起，直到有人接聽時停止
- IP Phone 1 與 IP Phone 2 之間設定 Intercom 按鈕，不用取聽筒就可以直接對話

附錄 A-1

主機名稱	介面名稱	IP 位址	對接設備
HQRTR	S0/0/0	200.0.0.1/30	BORTR
	S0/0/1		
	G0/0	10.0.0.1/30	LSRTR
	G0/1	100.0.0.1/24	ISPRTR
	Lo0	1.1.1.1/32	
BORTR	S0/0/0	200.0.0.1/30	HQRTR
	S0/0/1		
	G0/0	192.168.30.254/24	BOSW
	G0/1	100.0.1.1/24	ISPRTR
	Lo0	1.1.1.2/32	
ISPRTR	G0/0	100.0.0.2/24	HQRTR
	G0/1	100.0.1.2/24	BORTR
	Lo0	8.8.8.8/32	
HQSW1	F0/21		LSRTR
	F0/22		
	F0/23		HQSW2
	F0/24		
	F0/1		HQSRV1
	F0/6		IP Phone 1
	VLAN10	192.168.10.251	
HQSW2	F0/23		HWSW1
	F0/24		
	F0/1		HQSRV2
	F0/6		IP Phone 2
	VLAN10	192.168.10.252	
BOSW	F0/1		BORTR
	F0/2		BOCLT
	VLAN30	192.168.30.251	

附錄 A-2

主機名稱	介面名稱	IP 位址	對接設備

LSRTR	eth0	10.0.0.2/30	HQRTR
	eth1	10.0.1.2/30	HQDMZ
	eth2.10	192.168.10.254/24	HQSW1
	eth2.20	192.168.20.254/24	
HQDMZ	Ethernet	10.0.1.1/30	LSRTR
HQSRV1	Ethernet	192.168.10.10/24	HQSW1
HQSRV2	Ethernet	192.168.10.20/24	HQSW2
HQCLT	Ethernet	DHCP	IP Phone 1
IP Phone 1		DHCP	HQSW1
IP Phone 2		DHCP	HQSW2
BOCLT	Ethernet	DHCP	BOSW

附錄 B

VLAN ID	VLAN Name
10	HQ-Server
20	HQ-Client
30	BO

附錄 C

使用者名稱	群組名稱	使用者密碼
IT0001-1000	Information Technology	Skills39
Sales0001-1000	Sales	
Mkt0001-1000	Marketing	

附錄 D

使用者名稱	群組名稱	使用者密碼
mon01-05	Monitoring	Skills39

第四十六屆國際技能競賽國手選拔賽

資訊與網路技術 Day 3 環境建置

- 請選手實作出 Day 1 設計的環境，並依照此題目後續敘述作相對應的設定

請選手設計出一個公司內部環境，可以避免任何的單點故障（Single Point of Failure），並且需要在故障發生後盡快讓服務恢復正常運作，並且在故障發生與復原時讓系統管理者知道（以發送 Email 為主）；信件中須提到事件發生時間、發生狀況與故障主機名稱。

故障發生點可能會是任意作業系統當機，任意服務突然停止，路由器 / 交換器故障等等。

環境提供的服務與功能：

- 基礎網路連通性（Network Connectivity）
- 網域服務（Active Directory）
- 名稱解析服務（DNS）
- 自動配發 IP 服務（DHCP）
- 郵件服務（Mail）
- 網頁服務（Web）
- 檔案分享服務（File Share）
- 各服務 SSL 加密（AD，Mail，Web，File Share）

環境規劃要求：

- 請將公司內網與 Internet 區隔開，僅將必要服務開放對外
- 在 Internet 上跑的服務請勿使用未加密的協定，例如 HTTP、SMTP 或是 Telnet 等
- 公司內部請規劃一個客戶端專用網段，隔離伺服器主機與客戶端主機
- 環境硬體設備規模請以場地設備清單提供的數量為限制；VM 規劃請自行做最佳化分配
- 所有設定請在伺服器端實作，請避免在客戶端電腦做太多設定；假設有一台剛安裝好的 Windows 10，加入網域後便可以使用所有備援機制
- 所有密碼請使用 Skills39，Windows 系統使用帳號 Administrator，Linux 系統使用帳號 root，Cisco 設備使用帳號 admin

選手要做的事情 ：

第五站

- 依照 Day 1 所做的設計，安裝所需的作業系統，規劃實體接線，並依需求設定環境、服務與硬體設備

第六站

- 在公司內網安裝一台專屬系統管理者的 Windows 電腦，此電腦將可以透過遠端桌面到所有 Windows Servers 與 SSH 連接到所有 Linux Servers 和 Cisco Devices
  - 此電腦將會用於測試服務與收發信件，請務必準備好測試用的客戶端環境；若該測試項無法在客戶端做測試才會直接連進管理介面檢查
  - 主機名稱請使用 ADMIN-PC，將電腦加入網域後使用網域管理員帳號登入，在桌面上製作連接至各主機與設備的超連接（RDP，Putty 或是 MMC），將檔案名稱設為主機名稱（例如 WINDC.rdp，LINRTR.lnk，WINDC-DHCP.mmc 等等）
- 在公司外網安裝一台測試公開服務的電腦，此電腦將可以測試提供給 Internet 的服務（DNS，Mail，Web）
  - 主機名稱請使用 INTERNET-PC