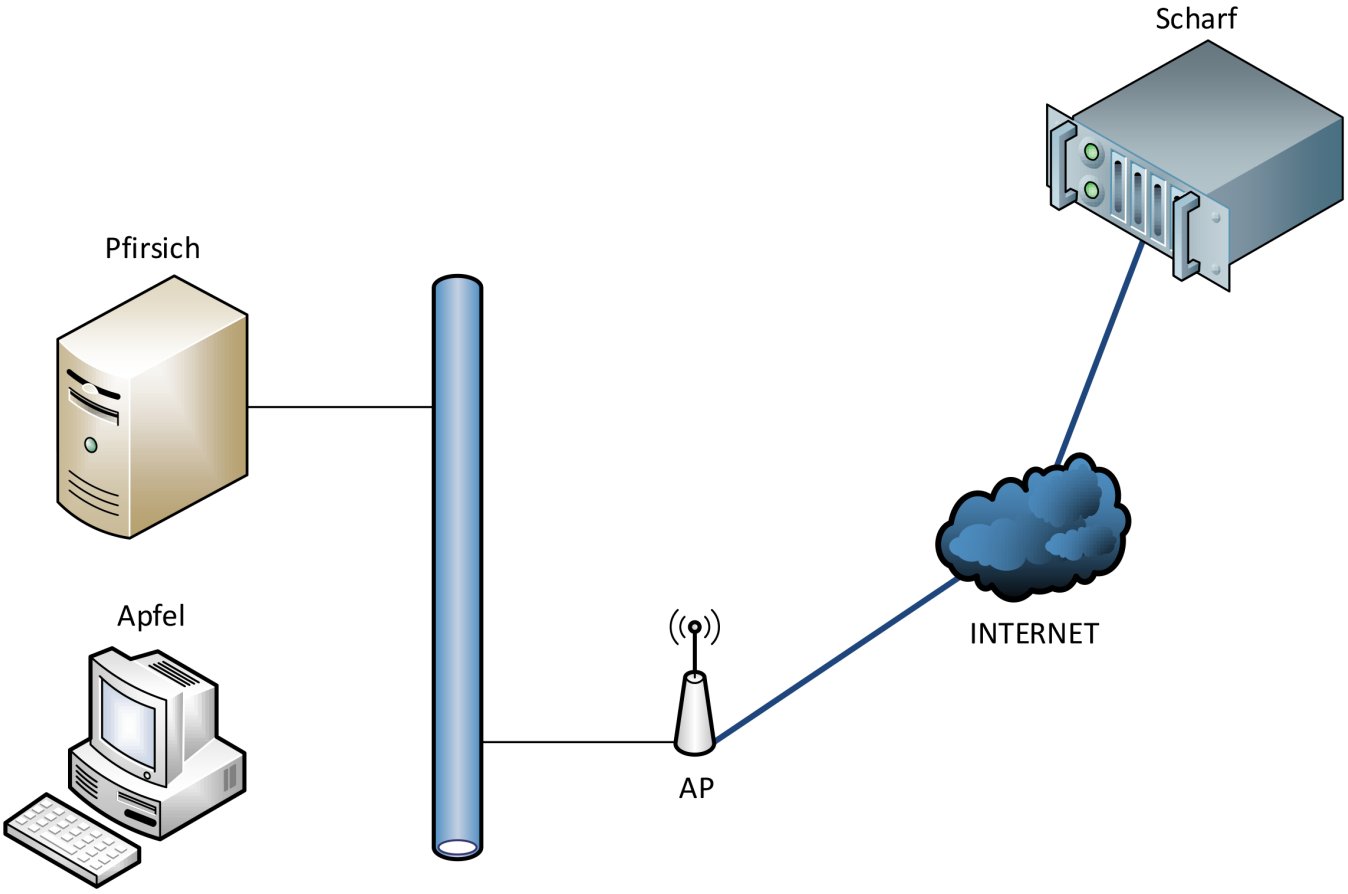
46th TWSkills
Preliminary

39 | IT Network Systems Administration

System Administration



- 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。

Scenario

你受雇於一間新加盟的糖果公司，今天是你的第一天上班。老闆要求你在時間內部署完成公司內部網域並完成員工電腦相關設定；公司已經向電信業者申請一台無線路由器，並要求你重新設定。另外公司在外部租了一台伺服器，提供公司網頁服務與其他相關功能。

Work Project

General Settings

- 在PC1安裝虛擬系統pfirsich
- 在PC2安裝虛擬系統apfel與scharf，並替apfel安裝無線網卡
- 根據附錄A設定主機名稱與IP位址
- 請在競賽PC開機並登入後，於背景自動啟動題目中的三台虛擬系統（不顯示VMware Workstation視窗）
- 防止使用者意外刪除VM與快照(snapshot)

Pfirsich (Windows Server 2012 R2)

Active Directory

- 建立goldbaran.jelly網域
- 根據附錄B新增使用者與群組
- 為避免Brute-force Attack，所有使用者需在6個月後強制變更密碼、在網域中任何電腦登入失敗達三次，將鎖定該帳戶；為方便未來管理，請將存放以上設定之群組原則物件名稱設定為ACCT-SEC-POLICY
- 若嘗試登入已被鎖定的帳戶，則在該主機產生事件紀錄
- 登入網域使用者時，需顯示訊息Welcome to Goldbaren Corporation !!

DNS

- 安裝DNS服務，設定適當紀錄供網域內的使用者與網路服務進行URL解析
- 將與haribo.gummy相關的DNS請求轉送到scharf

DHCP

- 安裝DHCP服務，自動配發IP給網域內電腦
- 將apfel配發到的IP固定為172.30.30.101

Certificate Authority

- 安裝CA服務，配發憑證供網域內與外部網頁伺服器使用
- 由於SHA1演算法已被認為是不安全的，請將根憑證之雜湊演算法設定為SHA2，並將其使用期限設定為三年

Firewall

- 網域內，僅允許pfirsich發起遠端連線(SSH/Telnet)

Scharf (Debian 8)

- 除了Root使用者之外，在scharf上不需新增其他使用者，評分時使用的使用者將會在評分時現場新增（指令為useradd username或adduser username，選手可自行選擇，但不可在其後使用其他參數）

VIM

- 請將vim設定為系統預設文字編輯器
- 使用vim時預設顯示行號

DNS

- 安裝DNS服務，為haribo.gummy設定適當的記錄

Web

- 安裝網頁服務，提供http://www.haribo.gummy作為首頁，且限制網頁服務的頻寬使用量為1MB/s
- 提供個人頁面https://private.haribo.gummy/~username，首頁預設顯示 ” This is the homepage for username !!”
- SSL使用由pfirsich簽署之憑證，apfel瀏覽網頁時，不可出現憑證錯誤訊息
- 個人頁面需登入方可瀏覽，以本機使用者帳戶進行驗證，且無流量限制
- 為方便評分，請在首頁根目錄中製作一個20M的檔案，並命名為20M.rar

SSH

- 安裝SSH服務，允許Root與一般使用者使用帳號密碼登入
- 連續三次登入失敗將會鎖定此來源IP位址
- 一般使用者（Root不需）登入時須將時間與使用者名稱紀錄於 /var/log/ssh_log/username.log

Firewall

- 設定防火牆，請使用最嚴謹之防護，阻擋外部任何非服務相關的流量

Apfel (Windows 8.1)

- 加入網域goldbaran.jelly
- 讓所有使用者可在CMD下以指令putty.exe呼叫PuTTY程式

AP (Wireless Access Point)

- 請依試題需求，自行設定無線路由器之密碼與相關設定

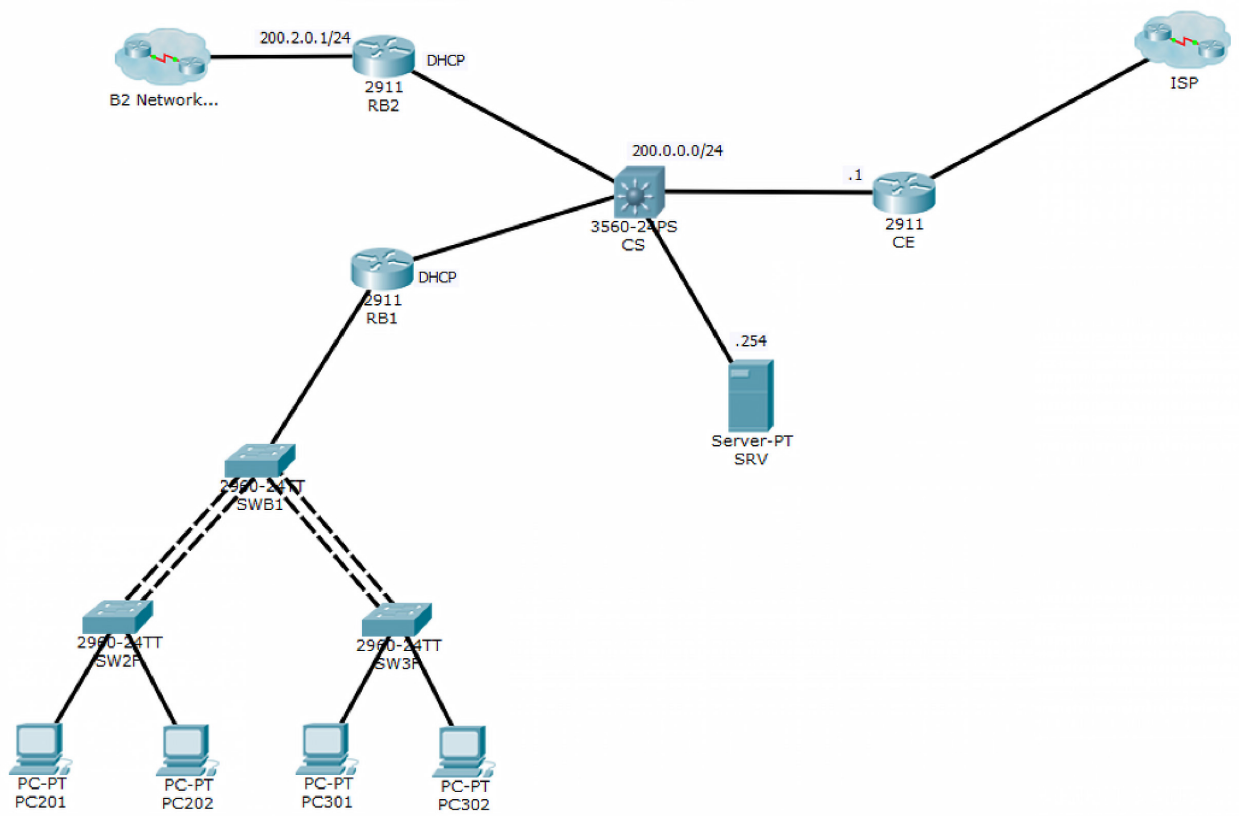
APPENDIX A

Device Name	Host Name	Operating System	Interface	IP Address
PC1	pfirsich	Windows Server	Ethernet	172.30.30.10/24
PC2	scharf	Linux Server	eth0	46.43.63.5/29
PC2	apfel	Windows Client	Ethernet	DHCP
AP			WAN	46.43.63.1/29
			LAN	172.30.30.254/24

APPENDIX B

Username	Password	Group
Administrator	Skills39	Domain Admins
RD01-50		Research and Development Department
MKT01-50		Marketing Department
ADV01-50		Advertising Department
SRV01-50		Service Department

Packet Tracer



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

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