第 50 屆全國技能競賽

資訊與網路技術

第一站試題

選手姓名		崗位編號	

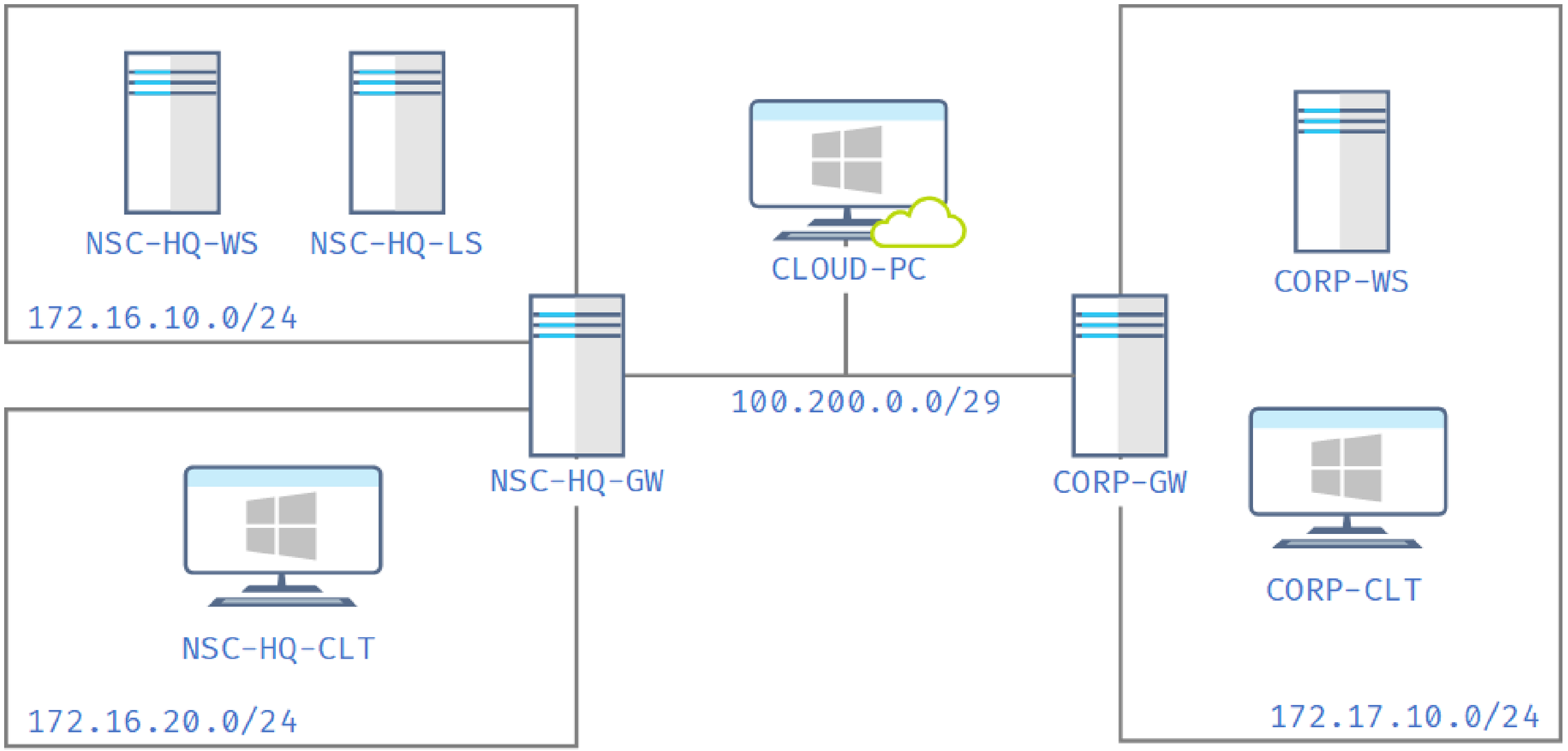
裁判長宣佈前請勿翻閱試題。

開始比賽後請先在試題封面及答案卷寫上姓名及編號。

考試後**請繳回本試題**及**評分表**，不得攜出試場。

- 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。
- 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
- 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。
- 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**。

整體架構 Overview Architecture



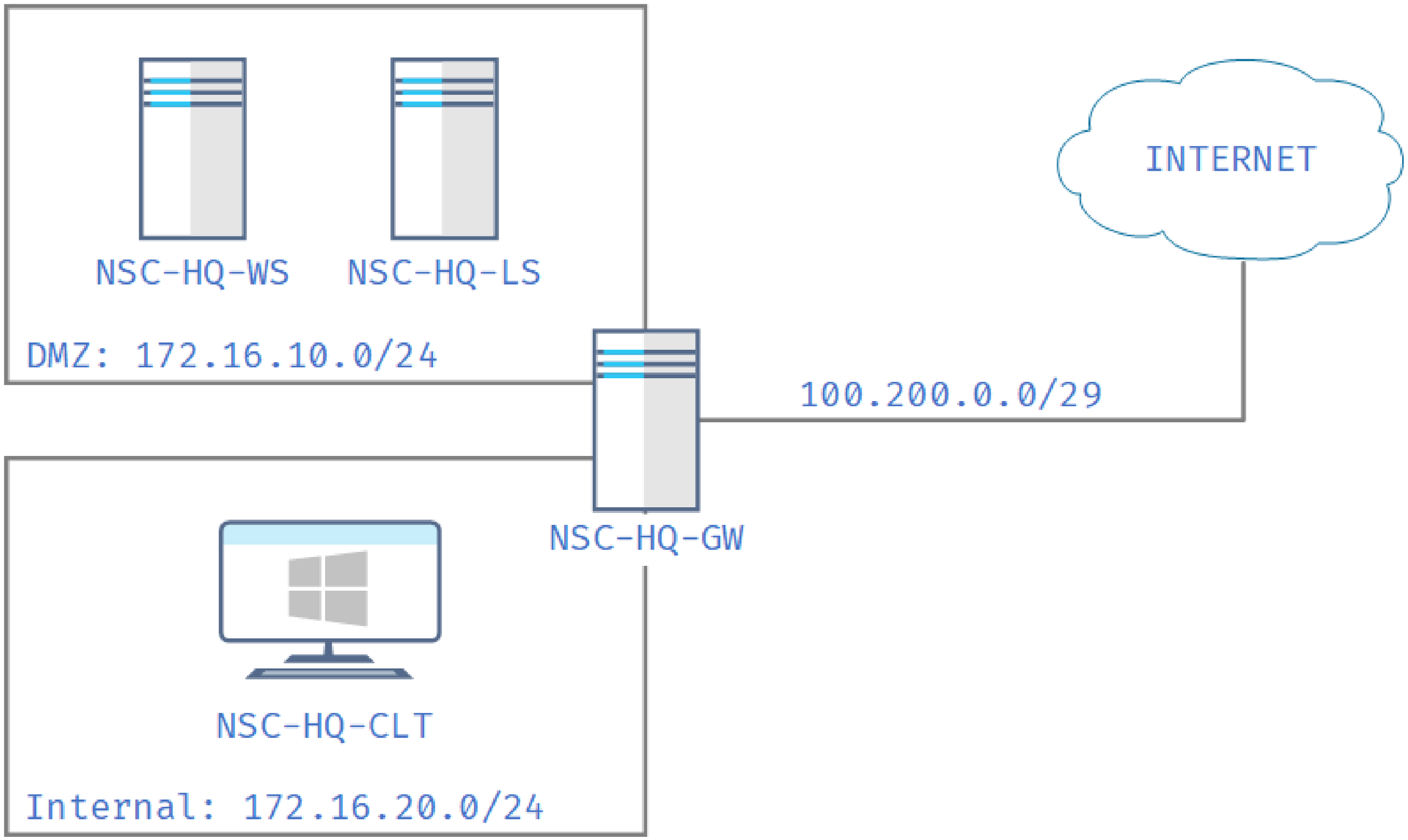
試題情境

你是一個自由接案的系統工程師，有兩家新公司（NSC 與 CORP）請你建置基礎架構
兩家公司的 IT 人員都已經將虛擬化環境準備完畢，並且製作好虛擬機範本（Template）。請依據兩家提供的環境建置需求書，設計並建置網路與服務。
請根據需求建立與設定相關服務；若無特別指定，可自行選擇使用 Windows Server 或 Debian 實作
契約中雙方有協議出幾項**基本設置規範**，請工程師務必遵照此基本設置規範；若有違反，該公司將會**羅列為驗收缺失**（**扣分項**）。

基本設置規範

Host 主機不參與整個網路環境，請將其所有網卡 **IPv4** 及 **IPv6** 功能**關閉**
試題中不指定 VM 所在的 Host 主機，兩部 Host 主機均須使用；請根據環境需求與硬體限制，自行分配系統資源
依照附件 A 與拓樸圖設定**主機名稱**、**介面卡名稱**與 **IP 參數**
請將所有 **VM 名稱**設定與其**主機名稱**相同
為方便做測試，允許所有作業系統的 **ICMP** 流量

第一站 - NSC 公司


INTERNET
NSC-HQ-WS
NSC-HQ-LS
DMZ: 172.16.10.0/24
100.200.0.0/29
NSC-HQ-GW
NSC-HQ-CLT
Internal: 172.16.20.0/24

基礎架構建置

- 伺服器 VM 請建置於 DMZ 區域，客戶端機器請建置於 Internal 區域
- 確認使用者可正常連線至 Internet
- 確認公司內可直接使用主機名稱來互相連線
- 確認新電腦在連接至 Internal 區域後，可自動取得 IP 與相關 DNS 設定

使用者帳號

- Linux 主機將使用 admin/Skills39L 登入，且該帳號擁有 sudo 權限
- Windows Server 主機將使用 admin/Skills39W 登入，且該帳號擁有最高管理員權限
- Internal 區域內的 Windows 10 主機將使用 admin/Skills39 登入，且該帳號擁有最高管理員權限
- 請撰寫 script，admin 帳號可登入該主機並執行指令建立 **VPN** 使用者

主機	（必填）
指令	usercreate *使用者名稱 密碼*

憑證建置

- 建置 CA 伺服器，簽署與配發 nsc.com 網域的憑證
  - 可透過 https://www.nsc.com/ca.crt 網址下載 nsc.com 網域根憑證
  - 請於下方寫下 nsc.com 網域根憑證 Thumbprint 末五碼

公司首頁

- 請建置公司首頁 https://www.nsc.com
  - 首頁標題請顯示 `"NSC"`
  - 首頁內容請以 h1 顯示 `"Welcome to NSC homepage"`
  - 網路中任意位置均可瀏覽公司首頁，並且不可出現憑證錯誤訊息

客戶端電腦

- 在公司內網可使用 \\file.nsc.com\public 連接至公司內部分享資料夾
  - 禁止存放執行檔與壓縮檔（`.exe .sh .bat .zip .tar .tar.gz`）
  - 總容量限制為 1G

資安相關設定

- 請在 GW 上設定防火牆規則

來源 / 目的	Internal	DMZ	Internet
Internal	O	O	X
DMZ	Linux 主機可 SSH Windows 主機可遠端桌面 對內與對外提供的服務	O	對內與對外提供的服務
Internet	SNAT	O	O

  - 允許規則上開放之流量的回應封包（Stateful）
  - 上列表格未提及之流量一律丟棄（DROP）

VPN 建置

- 使用者可以從 Internet 透過 VPN，連接至 **NSC 公司內的分享資料夾**
  - VPN 網址：vpn.nsc.com
  - 測試時將會使用 **CLOUD-PC** 的 **admin** 使用者進行做連線，並預先建立以下兩個 VPN Profile
    - VPN Profile 名稱為 **NSC VPN Admin**，帳號 **admin**，不需輸入密碼即可登入
    - VPN Profile 名稱為 **NSC VPN User**，連線時須輸入帳號密碼

第 50 屆全國技能競賽

資訊與網路技術

第二站試題

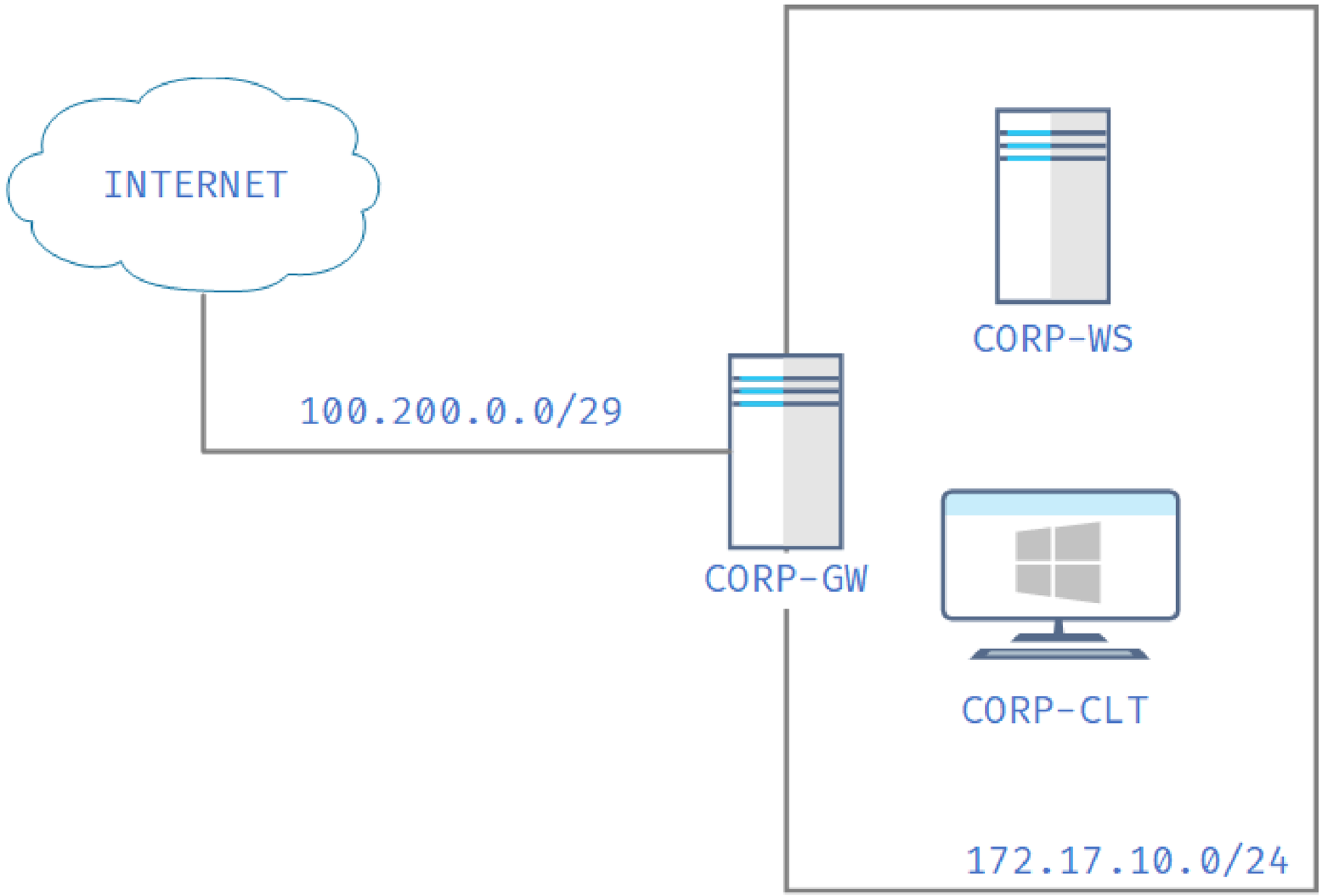
選手姓名		崗位編號	

裁判長宣佈前請勿翻閱試題。

開始比賽後請先在試題封面及答案卷寫上姓名及編號。

考試後**請繳回本試題**及**評分表**，不得攜出試場。

第二站 - CORP 公司



基礎架構建置

- 確認使用者可正常連線至 Internet
- 確認公司內可直接使用主機名稱來互相連線
- 確認新電腦在連線至內網後，可自動取得 IP 與相關 DNS 設定

使用者帳號

- Linux 主機將使用 admin/Skills39L 登入，且該帳號擁有 sudo 權限
- Windows Server 主機將使用 admin/Skills39W 登入，且該帳號擁有最高管理員權限
- Windows 10 主機將使用 admin/Skills39 登入，且該帳號擁有最高管理員權限

憑證建置

- 建置 CA 伺服器，簽署與配發 corp.com 網域的憑證
  - 可透過 https://www.corp.com/ca.crt 網址下載 corp.com 網域根憑證
  - 請於下方寫下 corp.com 網域根憑證 Thumbprint 末五碼

公司首頁

- 請建置公司首頁 https://www.corp.com
  - 首頁標題請顯示 "CORP"
  - 首頁內容請以 h1 大小顯示 "Welcome to CORP homepage"
  - 網路中任意位置均可瀏覽公司首頁，並且不可出現憑證錯誤訊息

資安相關設定

- 請在 GW 上設定防火牆規則

來源 / 目的	Inside	Internet
Inside	O	對內與對外提供的服務
Internet	SNAT	O

  - 允許規則上開放之流量的回應封包（Stateful）
  - 上列表格未提及之流量一律丟棄（DROP）

附件 A：主機名稱與 IP 位址

主機名稱	作業系統	介面名稱	IP 位址	預設閘道
NSC-HQ-WS	WS 2019	Ethernet0	172.16.10.10/24	172.16.10.254
NSC-HQ-LS	Debian 10	eth0	172.16.10.20/24	172.16.10.254
NSC-HQ-CLT	Windows 10	Ethernet0	via DHCP	
NSC-HQ-GW	Debian 10	eth0	172.16.10.254/24	
		eth1	172.16.20.254/24	
		eth2	100.200.0.1/29	
CORP-WS	WS 2019	Ethernet0	172.17.10.10/24	172.17.10.254
CORP-CLT	Windows 10	Ethernet0	via DHCP	
CORP-GW	Debian 10	eth0	172.17.10.254/24	
		eth1	100.200.0.2/29	
CLOUD-PC	Windows 10	Ethernet0	100.200.0.3/29	

* 若預設閘道為空白，則請勿做任何設定

第 50 屆全國技能競賽

資訊與網路技術

第三站試題

選手姓名		崗位編號	

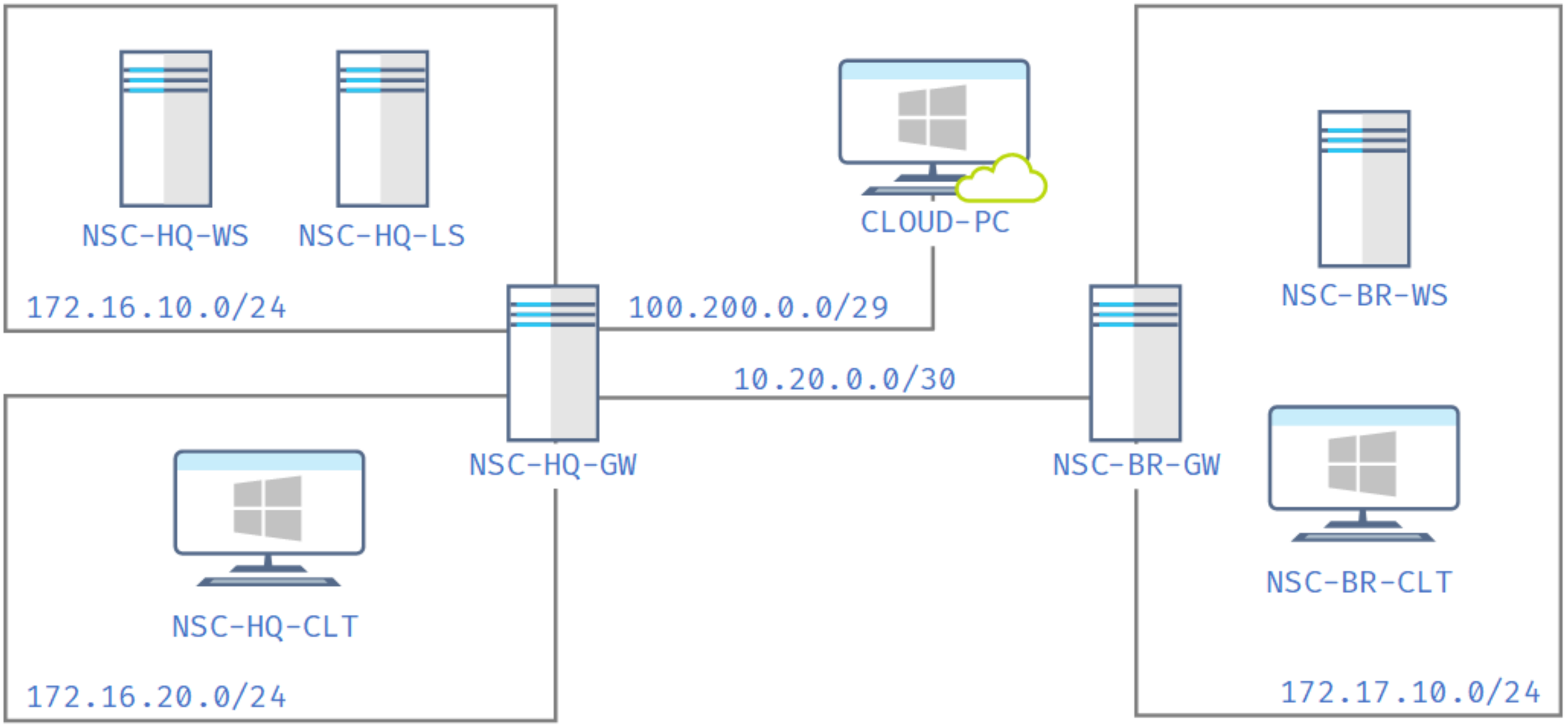
裁判長宣佈前請勿翻閱試題。

開始比賽後請先在試題封面及答案卷寫上姓名及編號。

考試後**請繳回本試題**及**評分表**，不得攜出試場。

- 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。
- 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
- 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。
- 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**。

整體架構 Overview Architecture



試題情境

- 月黑風高的一天過去了，CORP 公司股票大跌，NSC 公司一夜之間惡意併購了 CORP 公司，CORP 公司內的所有 IT 人員都已資遣完畢；為了管理方便與資安考量，兩家公司之間牽了一條專線，所有 CORP 對外開放的服務與上網的流量皆須經過 NSC 的 GW
- 請盡可能保留 CORP 與 NSC 兩家公司內的所有主機，並將主機名稱依照拓樸圖與附件 A 進行更名
- 請根據需求建立與設定相關服務；若無特別指定，可自行選擇使用 Windows Server 或 Debian 實作
- 契約中雙方有協議出幾項**基本設置規範**，請工程師務必遵照此基本設置規範；若有違反，該公司將會**羅列為驗收缺失（扣分項）**。

基本設置規範

- Host 主機不參與整個網路環境，請將其所有網卡 **IPv4** 及 **IPv6** 功能**關閉**
- 試題中不指定 VM 所在的 Host 主機，兩部 Host 主機均須使用；請根據環境需求與硬體限制，自行分配系統資源
- 依照附件 A 與拓樸圖設定**主機名稱**、**介面卡名稱**與 **IP 參數**
- 請將所有 **VM 名稱**設定與其**主機名稱**相同
- 為方便做測試，允許所有作業系統的 **ICMP** 流量

第三站 - NSC & CORP 公司

基礎架構建置

- 確認所有使用者可正常連線至 Internet
- 確認兩家公司內可直接使用主機名稱來互相連線
- 確認新電腦在連接至內網後，可自動取得 IP 與相關 DNS 設定

使用者帳號

- 公司遭併購後為精簡管理成本，決定導入 Active Directory 進行帳號控管
  - 請依據附件 B 預先建立使用者
  - 為避免 CORP 公司使用者登入延遲，請在 CORP 內網設置 RODC 主機，並確認使用者在 CORP 內網登入時會使用該 RODC 主機進行驗證
    - 僅允許 CORP 公司的使用者在 RODC 主機上做密碼快取
- 將所有 Linux 主機加入網域，但保留原本的本機 **admin** 帳號作為備用
- 將所有 Windows Server 主機加入網域，但保留原本的本機 **admin** 帳號作為備用
- 將所有 Windows 10 主機加入網域
- 請更新昨日撰寫的 script，**admin** 帳號可登入該主機並執行指令建立 VPN 與 AD 使用者

主機	（必填）
指令	usercreate *使用者名稱* *密碼*

  - 若此 script 執行成功，評分時不需管理員權限的評分項，將會使用此指令建立的新使用者進行評分，例如測試主機是否加入網域時，會使用這個新使用者進行登入；若此 script 執行失敗，將會在 AD 上直接建立一個使用者進行測試
  - 昨日透過 script 所建立的使用者仍可登入 VPN

既有架構沿用

- 保留原先 NSC 與 CORP 內的 CA 服務與配發的憑證
- 保留原先 NSC 與 CORP 內的首頁站台

公司內部管理頁面

- 在 **NSC-HQ-LS** 主機上提供 https://internal.nsc.com:8080
  - 網頁根目錄在 /var/www/internal
  - 首頁標題請顯示 `"NSC Internal"`
  - 首頁內容請以 h1 顯示 `"DP Russian"`
- 網路中任意位置均可瀏覽公司首頁，並且不可出現憑證錯誤訊息
- 該站台須符合 RFC6797 規範
- 若瀏覽器使用 HTTP 連接，將會自動跳轉成 HTTPS

第 50 屆全國技能競賽

資訊與網路技術

第四站試題

選手姓名		崗位編號	

裁判長宣佈前請勿翻閱試題。

開始比賽後請先在試題封面及答案卷寫上姓名及編號。

考試後**請繳回本試題**及**評分表**，不得攜出試場。

Part 2 - NSC & CORP 公司

網域客戶端電腦

- 所有客戶端電腦物件將放置於組織單位（OU）ClientPC 底下
- 客戶端登入時會將 \\file.nsc.com\public 自動掛載為 S 槽
- 客戶端電腦會自動安裝 Microsoft Edge for Business
  - 開啟 Microsoft Edge for Business 時，將會顯示首頁 https://www.nsc.com
- 客戶端電腦可透過控制台中的 Get Program 按鈕，從網路上下載並安裝 WSL2 更新
  （若選手在競賽期間已執行過 WSL2 更新，再次點選按鈕會直接跳到 Finish 畫面）

資安相關設定

- 請在 NSC-HQ-GW 上設定防火牆規則；由於 CORP 站台不直接對外，不須在 NSC-BR-GW 做防火牆設定
  （區域定義請參考 Day 1 的圖示說明；CORP 公司內網視為 Internal）

來源 / 目的	Internal	DMZ	Internet
Internal	O	X	X
DMZ	Linux 主機可 SSH Windows 主機可遠端桌面 對內與對外提供的服務	O	對外提供的服務
Internet	O (SNAT)	O (SNAT)	O

  - 允許規則上開放之流量的回應封包（Stateful）
  - 上列表格未提及之流量一律丟棄（DROP）
  - 註：DMZ 區域內的 Linux 主機需安裝 SSH 服務，Windows 主機需啟用遠端桌面服務；且皆可使用 admin 帳號進行登入
- 禁止網域內主機暫停/延後 Windows Update
- 禁止網域內主機啟用 Windows Insider Program

VPN 建置

- 使用者可以從 Internet 透過 VPN，連接至**公司內網進行所有伺服器主機的管理**
  - VPN 網址：vpn.nsc.com
  - 測試時將會使用 **CLOUD-PC** 的 **admin** 使用者進行做連線，並預先建立以下兩個 VPN Profile
    - VPN Profile 名稱為 **NSC VPN Admin**，帳號 **admin**，不需輸入密碼即可登入
    - VPN Profile 名稱為 **NSC VPN User**，連線時須輸入帳號密碼
  - 使用者開啟 Microsoft Edge for Business 瀏覽器時，會自動連線至 VPN `

公司內部管理系統 CI/CD 流程

- 使用者 **nsc001** 在 **NSC-HQ-CLT** 上登入時，在桌面上提供以下兩個腳本：
  - 將內部管理頁面的根目錄內容作差異同步（Differential Synchronization），將最新的內容同步於桌面上的 internal-www 資料夾中
  - 將內部管理頁面的根目錄內容作差異同步（Differential Synchronization），將目前 internal-www 資料夾內的檔案同步到內部管理頁面的根目錄中

附件 A：主機名稱與 IP 位址

主機名稱	作業系統	介面名稱	IP 位址	預設閘道
NSC-HQ-WS	WS 2019	Ethernet0	172.16.10.10/24	172.16.10.254
NSC-HQ-LS	Debian 10	eth0	172.16.10.20/24	172.16.10.254
NSC-HQ-CLT	Windows 10	Ethernet0	via DHCP	
NSC-HQ-GW	Debian 10	eth0	172.16.10.254/24	
		eth1	172.16.20.254/24	
		eth2	100.200.0.1/29	
		eth3	10.20.0.1/30	
NSC-BR-WS	WS 2019	Ethernet0	172.17.10.10/24	172.17.10.254
NSC-BR-CLT	Windows 10	Ethernet0	via DHCP	
NSC-BR-GW	Debian 10	eth0	172.17.10.254/24	
		eth1	10.20.0.2/30	
CLOUD-PC	Windows 10	Ethernet0	100.200.0.3/29	

* 若預設閘道為空白，則請勿做任何設定

* 若主機名稱為粗斜體字，表示該主機是更名過後的主機名稱

附件 B：使用者帳號

網域	所屬公司	帳號名稱	群組	密碼
nsc.com	NSC	nsc001	nsc-group	Skills39001
		nsc002		Skills39002
		...		...
		nsc999		Skills39999
	CORP	corp001	corp-group	Skills39001
		corp002		Skills39002
		...		...
		corp999		Skills39999

第 50 屆全國技能競賽

資訊與網路技術

第五站試題

選手姓名		崗位編號	

裁判長宣佈前請勿翻閱試題。

開始比賽後請先在試題封面及答案卷寫上姓名及編號。

考試後**請繳回本試題**及**評分表**，不得攜出試場。

注意事項

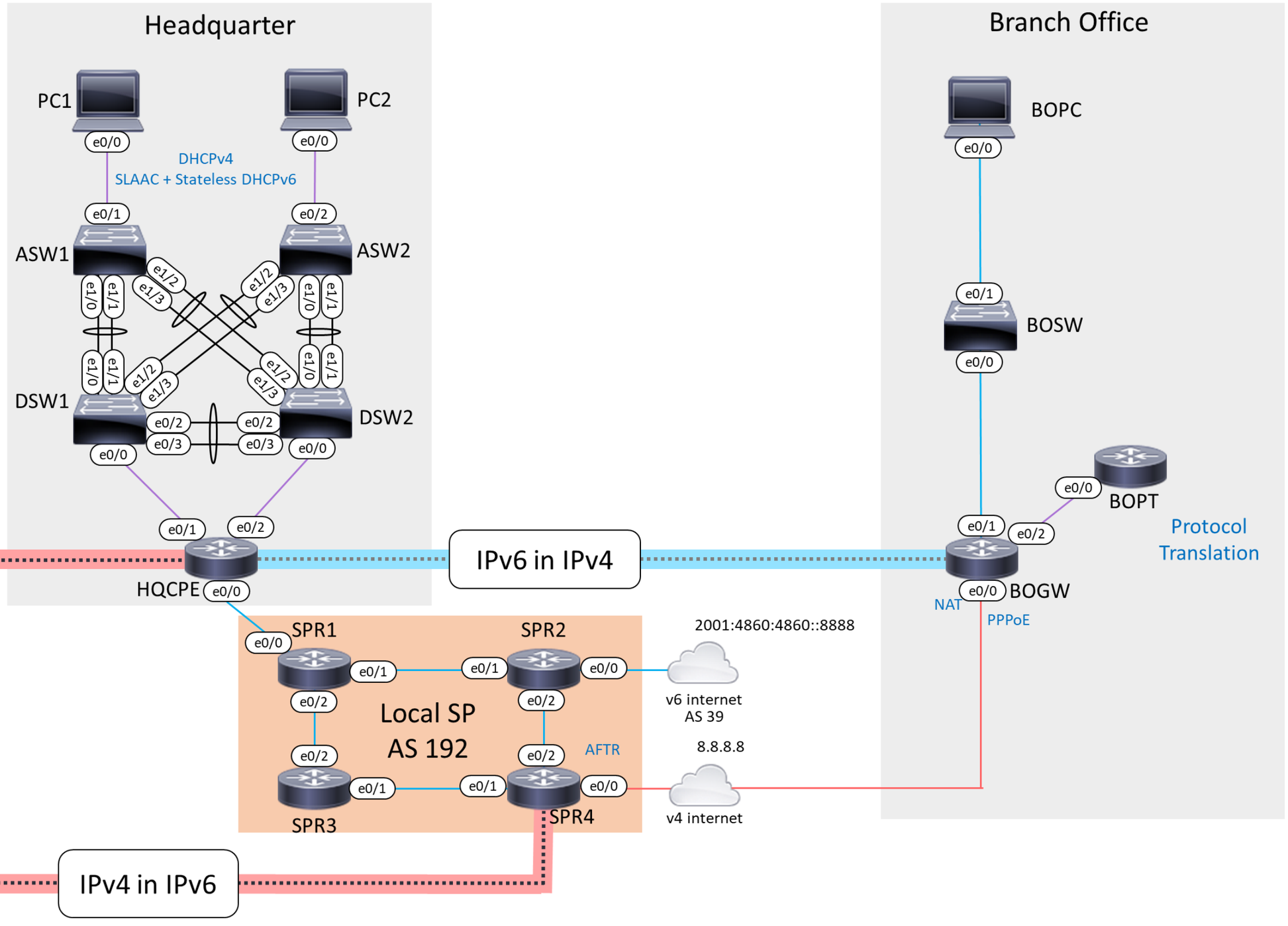
。設備已預先進行若干設定，請依試題敘述完成工作項目

。評分前將重啟所有設備，請選手務必儲存工作進度

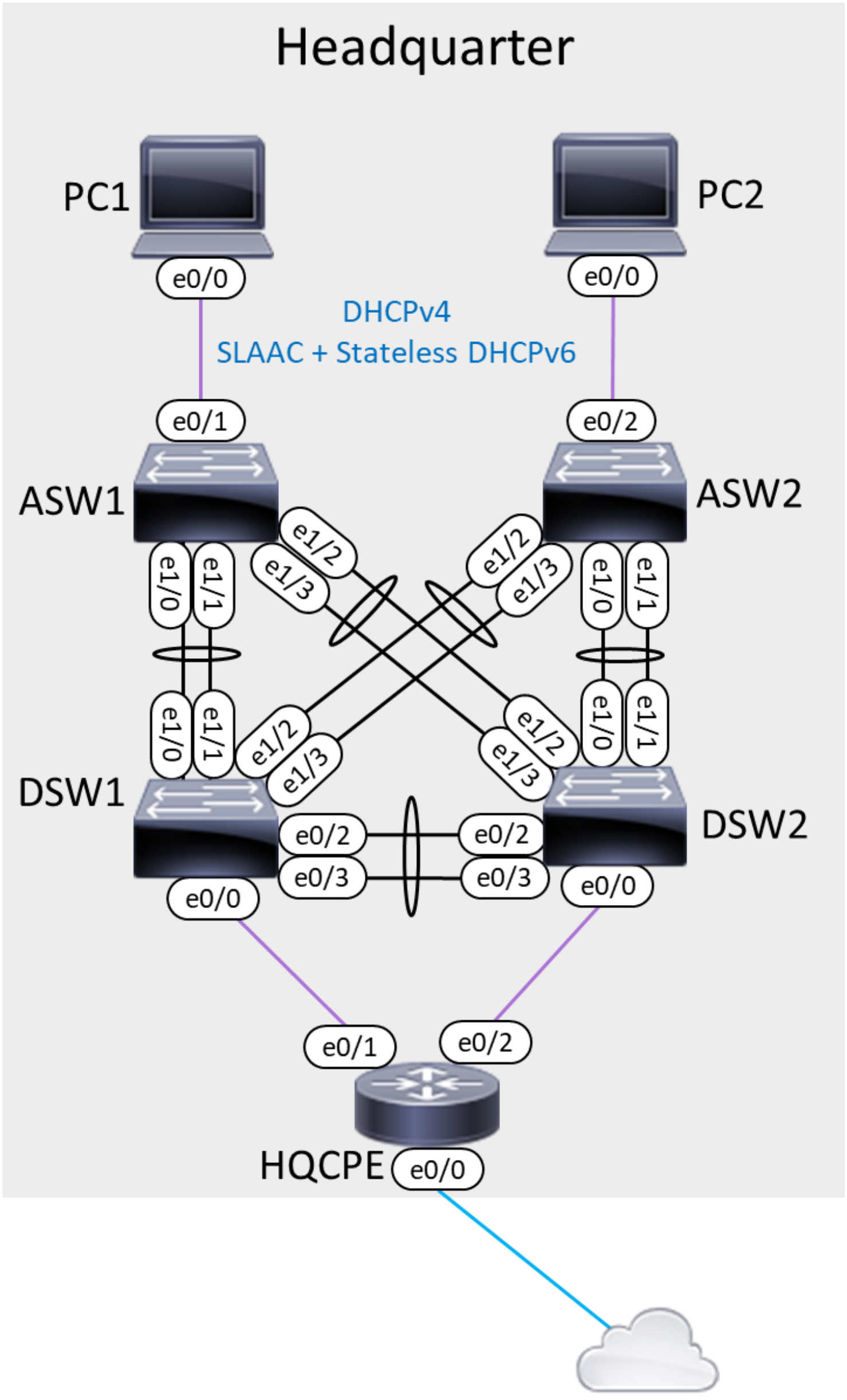
。除題目有明確指定施作方式的項目之外，其餘工作均可由任何形式完成，以成功實作題目情境架構與網路連通性為先

。若實作特定項目時，需額外新增過渡網段，可自行規劃與配置

Overview Topology Layout



Headquarter Site



Headquarter

HQ VLAN Table

ID	Interface Assignment (ASW1 & ASW2)	Network
110	E0/1	192.168.110.0 /24 2001:192:168:110::/64
120	E0/2	192.168.120.0 /24 2001:192:168:120::/64

。HQ 內所有 Switch 的 VTP Domain 均應設定為 NSC50，密碼為 VTPPASSWD，並將 VLAN 相關設定儲存於 NVRAM

。於 Switch 之間的介面設定 Link Aggregation

。所有使用者的流量於 Switch 之間轉遞時應帶有 802.1Q Tag

。DSW1 與 DSW2 為所有 HQ VLAN 的 Gateway，並共同以該網段第 1 個可用 IP 提供服務，在網路連通性完全正常的情況下，由 DSW1 優先擔任 VLAN 110、DSW2 優先擔任 VLAN 120 的 Gateway，若失去外聯能力，則將 Gateway 角色 failover 至另一台上

。最佳化 Switch 轉送訊框的路徑，在網路連通性完全正常的情況下，DSW1 與 DSW2 之間的線路不應承載 User Traffic

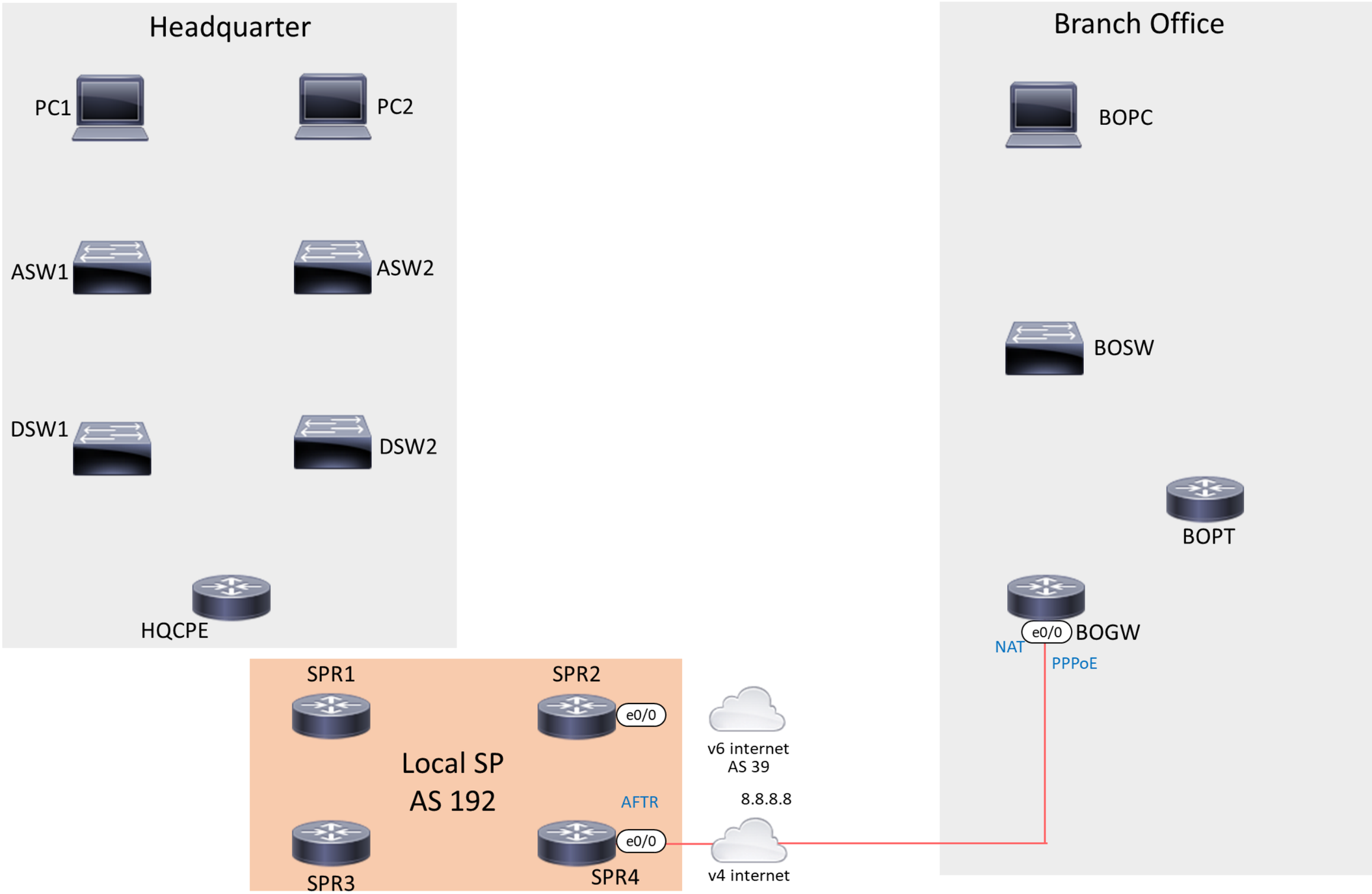
。於 DSW1 & DSW2 對接 HQCPE 的介面上設定 IP 位址，並最佳化轉送封包的路徑，依 Gateway 角色狀態，外連時將去/回同路

。HQ 所有 PC 以 DHCP 設定 IPv4 位址，DHCP Server 為 HQCPE

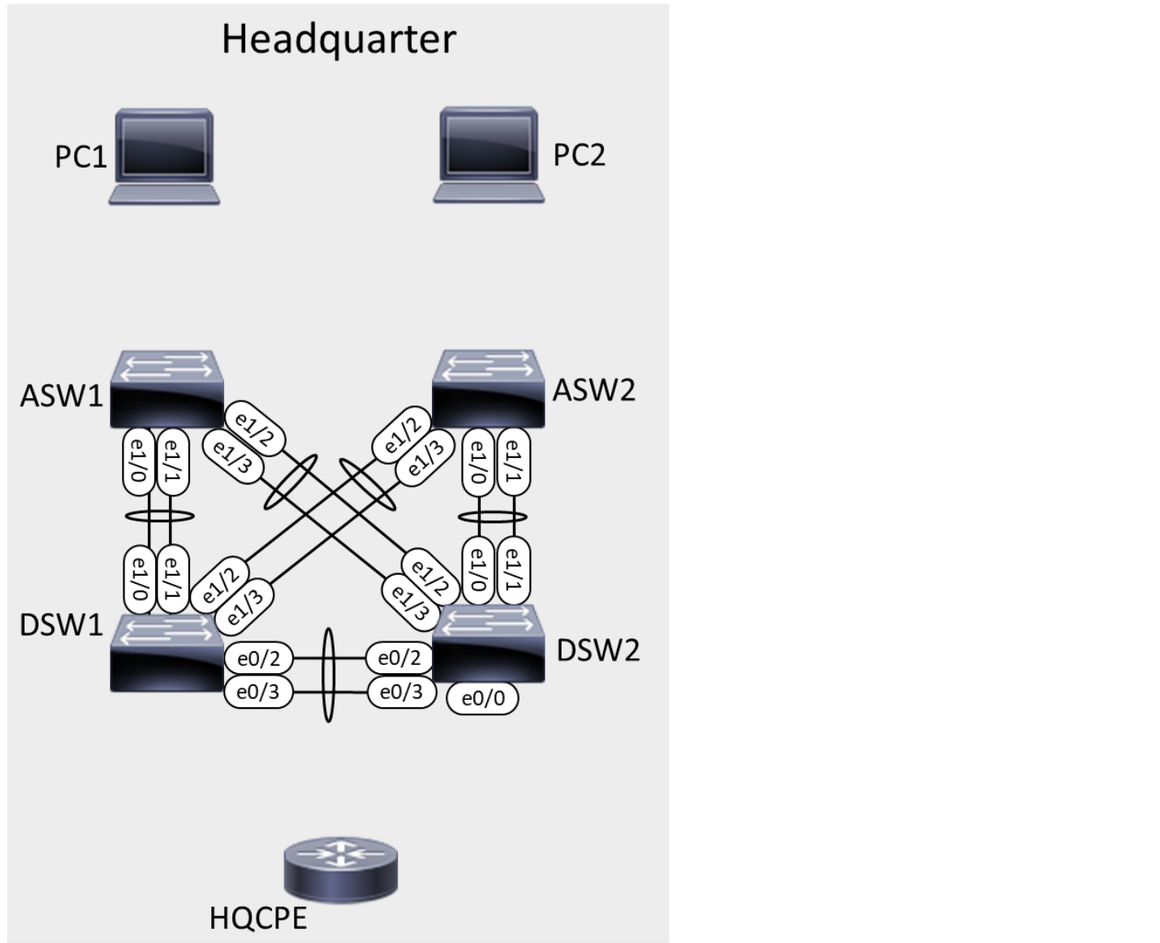
。HQ 所有 PC 以 Stateless Autoconfiguration 設定 IPv6 位址，並由 DHCP 取得 DNS Server 資訊

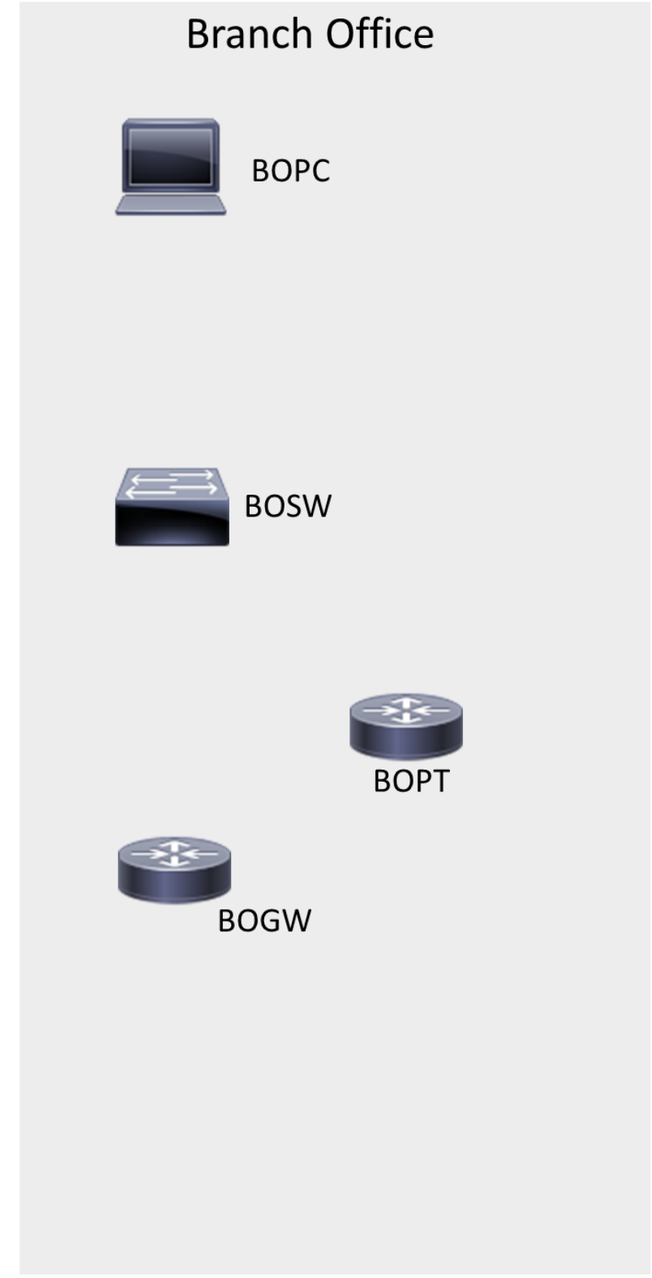
。於 HQCPE 上設定對外的預設路由

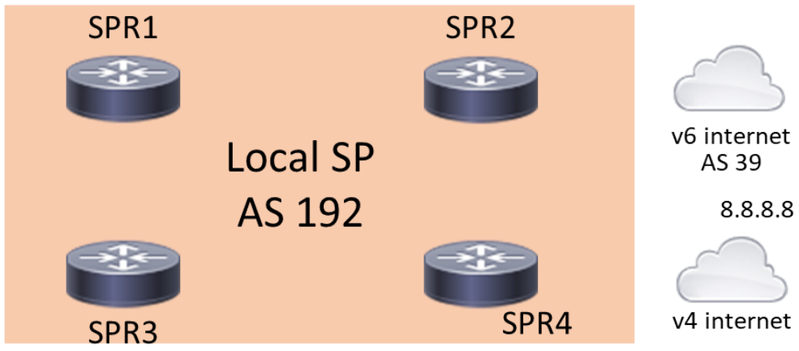
IPv4 Topology



Headquarter L2 LAN Topology





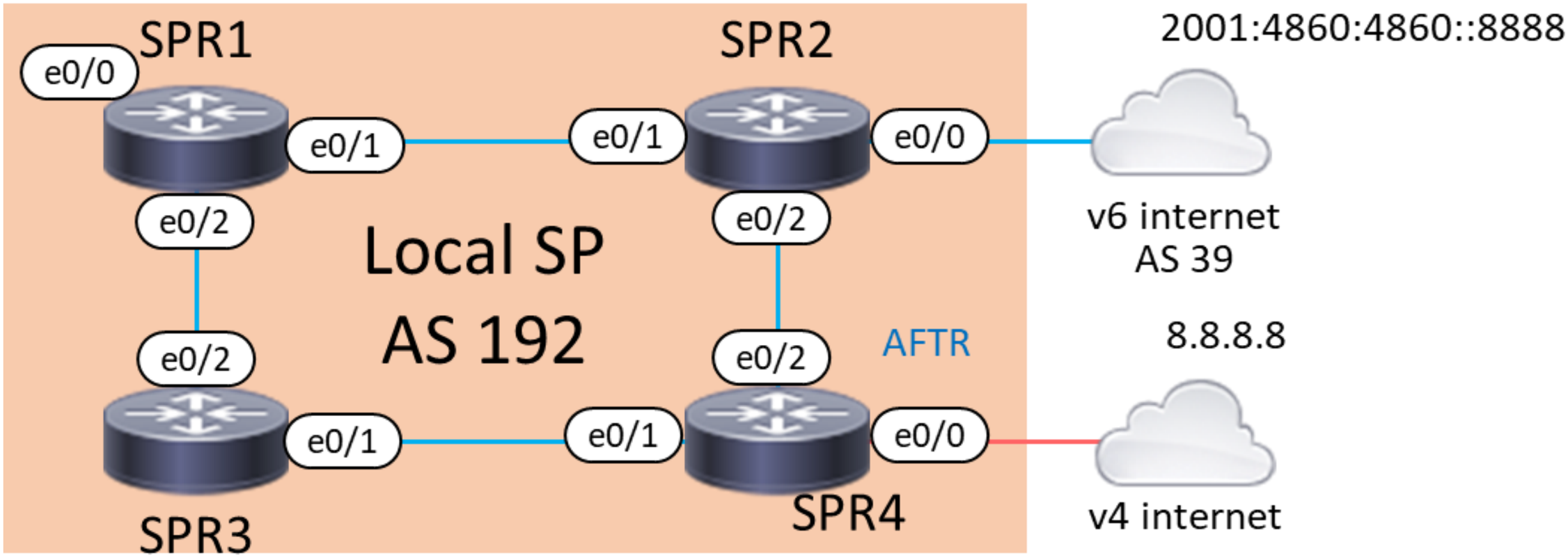


Local SP

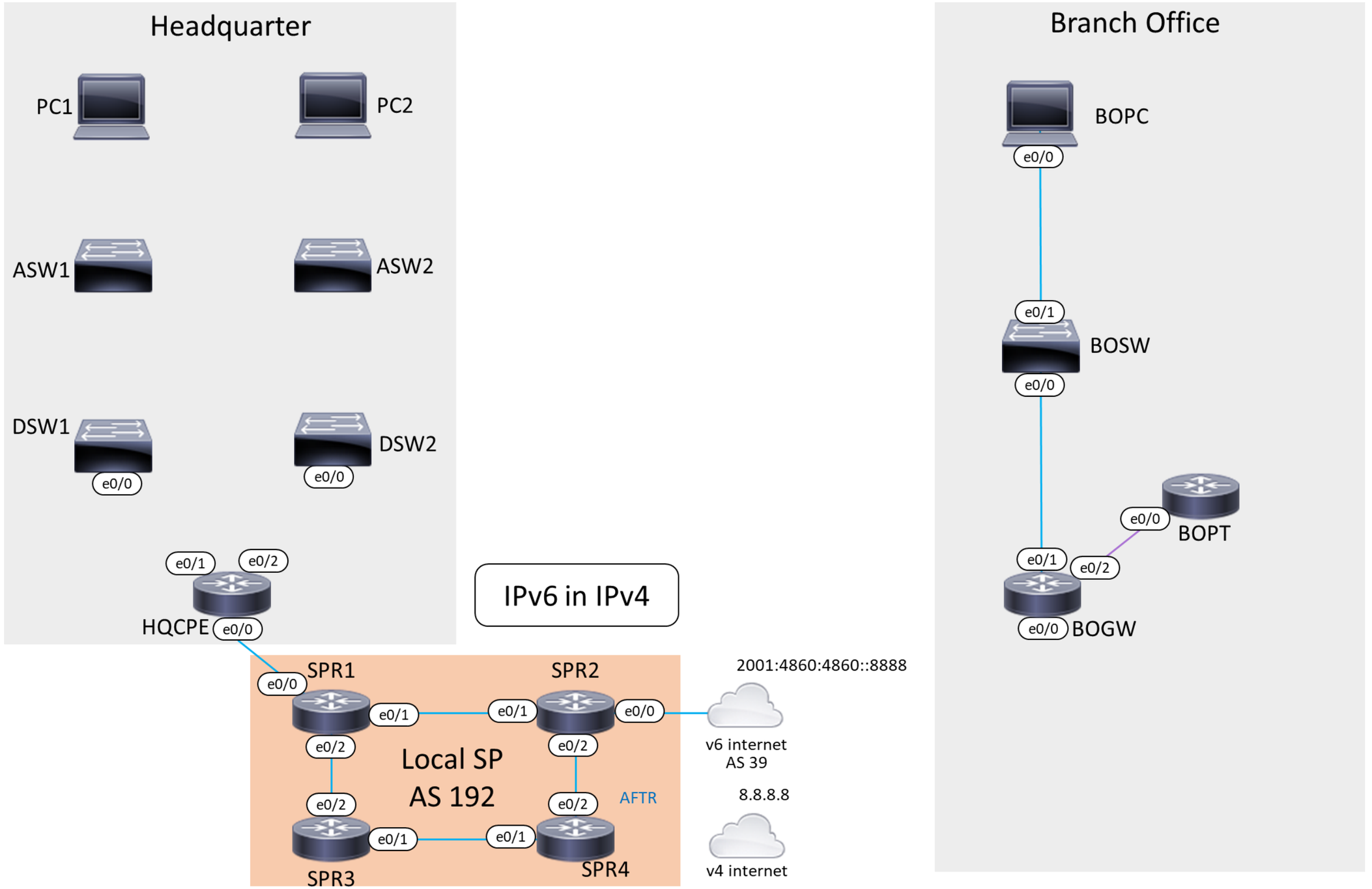
※Local SP 採 DS-Lite 架構，即用戶的 IPv6 為原生，IPv4 配發私有網段給用戶，客戶將 IPv4 封裝於 IPv6 封包中，並轉送至 IPv4 的 Internet 出口 (SPR4)，由 SPR4 進行 NAT 以存取 Internet

。於 SPR1-SPR4 之間啟用動態路由協定，並交換包括 Loopback 在內的 IPv6 網段資訊與預設路由資訊
。SPR1 作為收容客戶的 Edge Router，將從 2001:192::/32 中分配網段予用戶，於本次試題中，配發了 2001:192:168::/48 給 Headquarter，請設定靜態路由指向用戶
。於 SPR4 與 HQCPE 之間建立 Tunnel，傳輸 IPv4 封包，並設定靜態路由指向用戶 (於本次試題中，配發了 192.168.0.0/16 給 Headquarter)，請以 tunnel header overhead 最小的方式完成
。於 SPR4 設定 NAT，以利用戶存取 IPv4 Internet，以 39.39.39.1 作為用戶 PC 轉換後的 Public IP，並將 39.39.39.2 固定對應至 HQCPE
。於 SPR2 設定 BGP AS 192，上級 ISP 的對接介面 IP 為 2001:39:39:39::39，ASN 為 39，請將 2001:192::/32 通告給上級 ISP，並應由上級 ISP 取得預設路由資訊
。於 SPR4 設定靜態預設路由以存取 IPv4 Internet，上級 ISP 的對接介面 IP 為 39.39.39.39
。用戶 (Headquarter)以 IPv6 存取 Internet 時，雙向訊務優先以 SPR1-SPR2 路徑轉送；以 IPv4 存取 Internet 時，雙向訊務則優先以 SPR1-SPR3-SPR4 路徑轉送

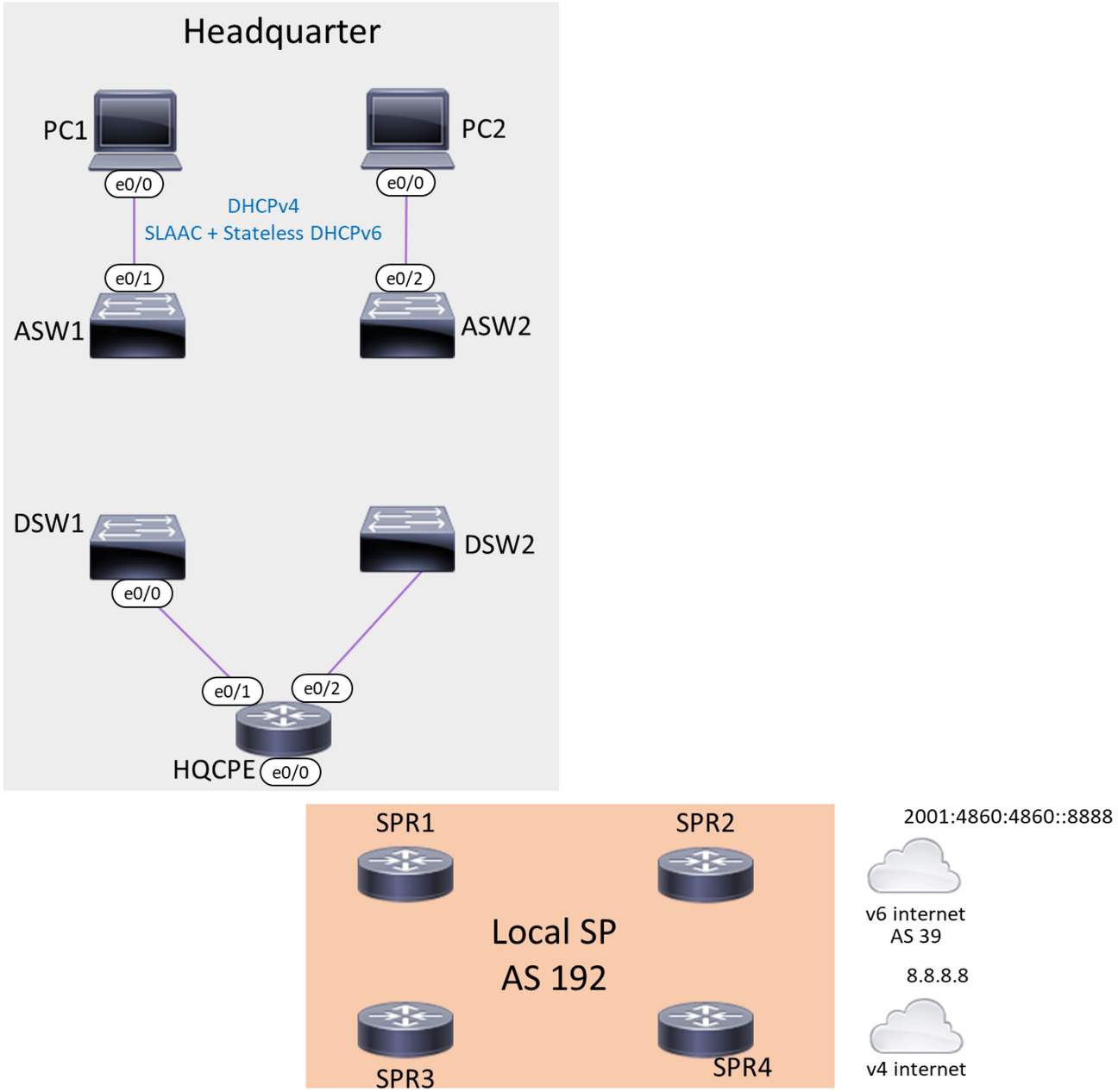
Local SP


SPR1
e0/0
e0/1
e0/2
SPR2
e0/1
e0/2
e0/0
2001:4860:4860::8888
v6 internet
AS 39
8.8.8.8
Local SP
AS 192
e0/2
e0/1
SPR3
e0/2
AFTR
e0/1
e0/0
SPR4
v4 internet

IPv6 Topology



DualStack (DS Lite) Topology



第 50 屆全國技能競賽

資訊與網路技術

第六站試題

選手姓名		崗位編號	

裁判長宣佈前請勿翻閱試題。

開始比賽後請先在試題封面及答案卷寫上姓名及編號。

考試後**請繳回本試題**及**評分表**，不得攜出試場。

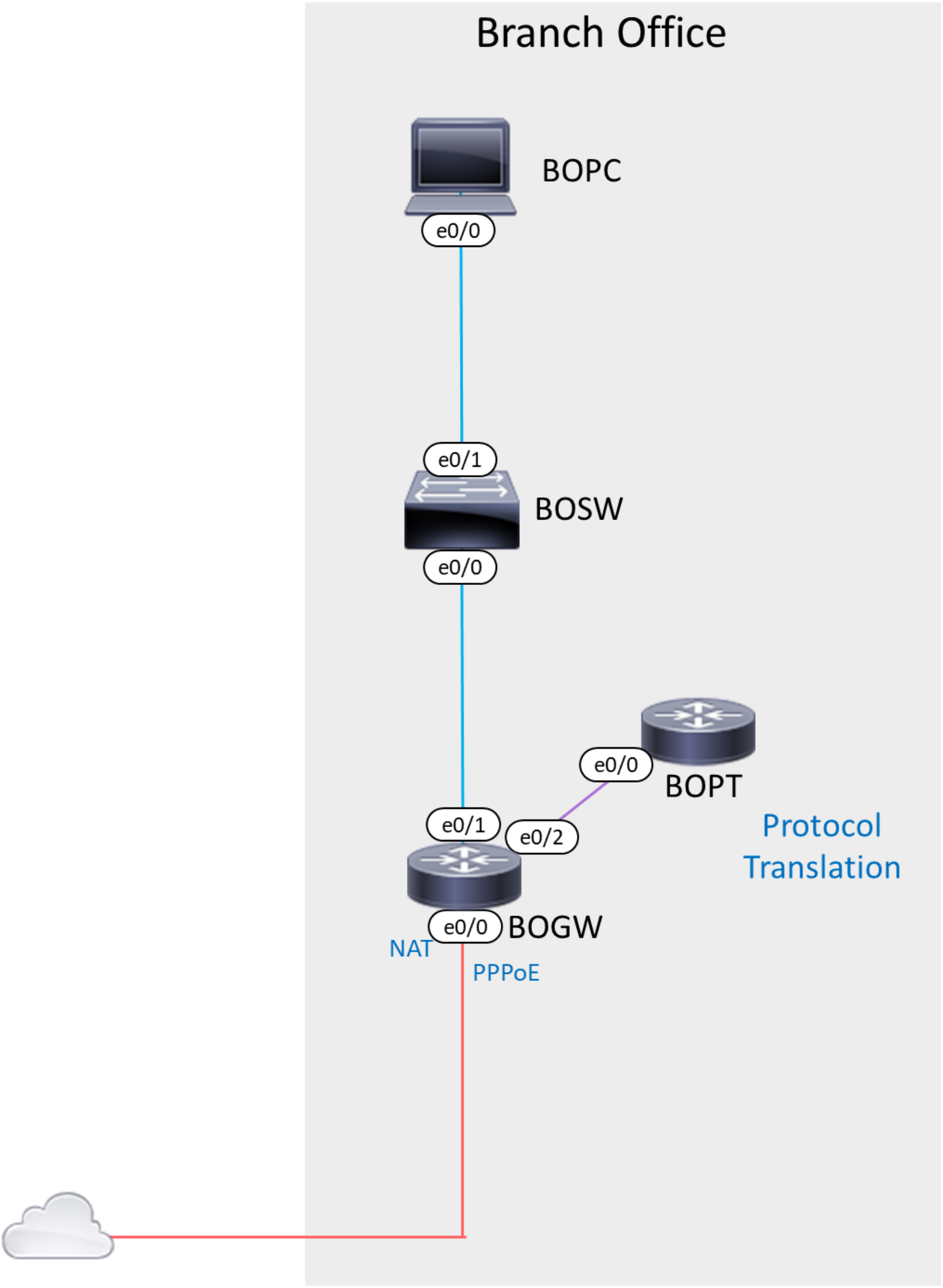
Branch Office

。於 BOGW 上設定 PPPoE，由 ISP 取得固定 Public IP (93.93.93.6)
撥接帳號為 20200920@isp.worldskills.tw，密碼為 Skills39
※若選手無法完成此項目，請改為直接將對外的 Ethernet 介面設定為 93.93.93.6/24，如此即便 PPPoE 項目失分，仍可繼續維持整體連通性
。於 BOGW 設定對外的預設路由
。於 HQCPE 與 BOGW 之間建立 Tunnel，傳輸 IPv6 封包 (除雙方內部網路使用此 Tunnel 相互存取之外，Branch Office 用戶存取 IPv6 Internet 時，也需將封包經此 Tunnel 轉至 HQCPE 後，由 Headquarter 轉送至網際網路)，請以不須設定 tunnel destination 的方式完成
。為避免 Headquarter 與 Branch Office 失聯，造成 Branch Office PC 完全無法存取網際網路，請將目的地為 64:FF9B::/96 的封包，送至 BOPT，並進行 Protocol Translation 轉換為 IPv4 封包 (IPv4 目的地位址由 IPv6 的最後 32 位元析出，例如 64:ff9b::808:808 將會被轉換為存取 8.8.8.8 的 IPv4 封包)後，再由 BOGW 進行 NAT Overload，直接存取 Internet

Security

。將 HQCPE 與 BOGW 之間的 Tunnel 以 IPsec 加密
。由於 IPv6 並無 NAT 提供簡易的防護，請於 HQCPE 上針對 IPv6 設定 Stateful Access Control，避免來自 Internet 的主動連線

Branch Site


Branch Office
BOPC
e0/0
e0/1
BOSW
e0/0
e0/0
BOPT
e0/1
e0/2
Protocol
Translation
e0/0
BOGW
NAT
PPPoE

※完成後，Headquarter 與 Branch Office 應可相互存取，並可使用 8.8.8.8 與 2001:4860:4860::8888 測試 Internet 存取；
如選手有需要執行來自外部的測試，可 telnet 至上述的 Internet 測試 IP，登入帳戶與密碼均為 test

Tunnel Layout