

第四十七屆國際技能競賽 國手選拔

資訊與網路技術

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）
- 監控服務（Monitoring）
- 自動化（Automation）

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

在架構中進行安全強化（Security Hardening）提出相對應的解決方案

包含但不限於：

- 作業系統強化
- 網頁服務強化
- 加密演算法強化
- 安全監控和告警機制
- 系統監控和健康檢查
- 各服務 SSL 加密（AD、Mail、Web、File Share）

第二站

Project Description

位於亞美尼亞的 dnsdhcp 公司，地地道道的端遊魔法師，明年將主辦第 47 屆電競技能競賽。為此，他們急建新 dnsdhcp 遊戲公司（前 ANC 主公司更替），更併購光子工作室，助力開發。緊急需一 IT 高手，搭起網路橋樑，順暢連上 Google 雲端，確保比賽及業務運作安全無虞。

光子工作室為客戶端開發者，測試雲功能。Google 資料中心是重要後盾，提供完美支援。

dnsdhcp 公司用極少成本搭建遊戲維度，聯結光子工作室，共舞成功序曲。

另外近期 IT 團隊發現總部使用的路由器每過幾天就會當機，需要進行更換。但由於短期內無法取得新機或是備品，團隊決定使用一台 Linux 主機作暫時的替代品。在進行路由器切換的過程中須確保所有既有機制皆不中斷且正常運作。

General Settings

- 請安裝作業系統，並自行規劃網段與 IP
 - 總部請將主機配置於相對應的 VLAN
 - 評分時皆會以 DNS 名稱 <hostname>.<domain> 進行連線
 - 總部：dnsdhcp.tw
 - 分部：5k6jo3.tw
 - Internet：gmail.com
- Linux 作業系統預設關閉 Terminal Bell
- 為了紀念已故的 vim 作者 Bram Moolenaar，所有 Linux 預設編輯器為 vim
- 所有系統透過 OUT 進行 NTP 校時
- 使用所有與憑證相關服務時，請勿出現憑證錯誤等資訊
- 預設密碼若未指定，請使用 Skills39

Security Requirements

- 所有可以登入的作業系統、網路設備與網頁服務

Single Sign-On

- 總部 (Head Quarter) 會使用 HQTWDC (Active Directory) 進行單一登入
 - 只有總部的人可以登入總部的系統
- 分部 (Branch Office) 會使用 BRSRV (OpenLDAP) 進行單一登入
 - 分部的人可以登入分部的系統，但是總部也可以用自己的帳號登入分部的系統
- 所有系統皆須經過驗證才可以存取，除非已經透過 SSO 進行驗證
- 評分前請各位選手分別在總部的 AD 與分部的 OpenLDAP 建立新的帳號，後續評分皆會使用該帳號進行登入操作

Login Restrictions

- 所有總部的網路設備都只有總部管理網段 Management VLAN 才能登入
- 所有分部的網路設備都只有 BRPC 才能登入
- 所有外網的網路設備都只有 OUT 才能登入

第三站

Networking

- 請設定總部的 VLAN
- 於 HQGW、BRGW 設定 NAT，使內部主機可以存取 Internet
 - 外部主機可以存取內部服務
- 於 HQGW、BRGW 設定 GRE Tunnel 使兩邊內部主機互相存取
 - 使用 IPSec 加密此 Tunnel
- 於 OUT 新增 Loopback 網卡
 - OUT 上所有服務皆須 Listen 於此網卡
- 除了與 BRPC 和 BRSRV 的連線以外，只要其餘的外部設備連接 BRSW 便會直接封鎖連線
 - 若原本連接 BRPC 和 BRSRV 的介面連接非上述設備，也會直接封鎖連線
- 請在外網使用 BGP 交換路由，內網使用 OSPF 交換路由
 - 評分前會請選手自行說明設計

DNS

- 總部網域為 dnsdhcp.tw
- 分部網域為 5k6jo3.tw
- 於 IX 上提供 DNS 服務，網域為 gmail.com，並為 Google 上的 mail 服務設定適當的紀錄

AD

- 在 HQTWDC 設定 ADDC，並建立相關測試使用者與群組
- 提供 LDAPS

LDAP

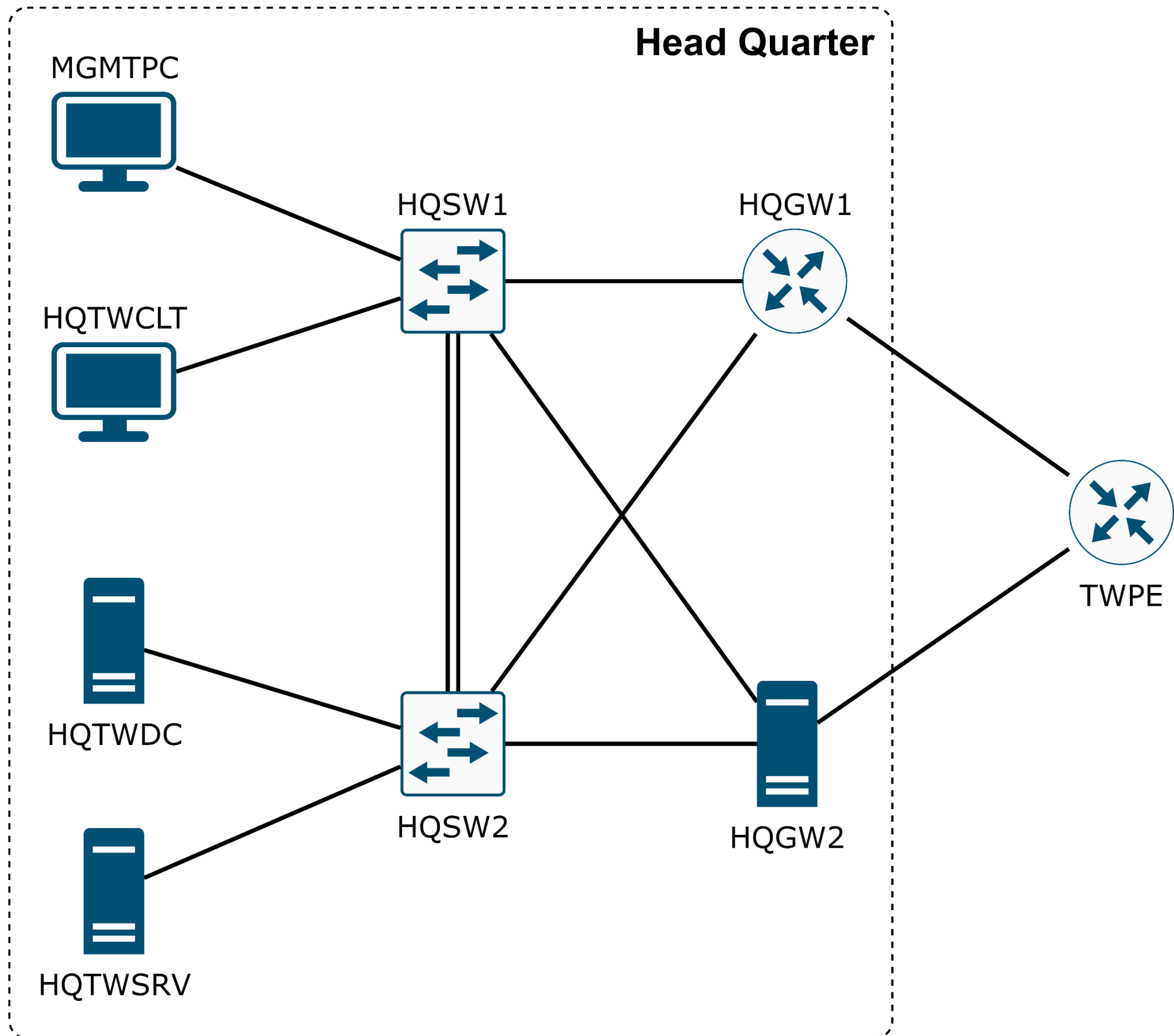
- 在 BRSRV 設定 OpenLDAP，並建立相關測試使用者與群組
- 僅提供 LDAPS
- 輸入 add-ldapuser <username> <password> 後可新增指定的使用者

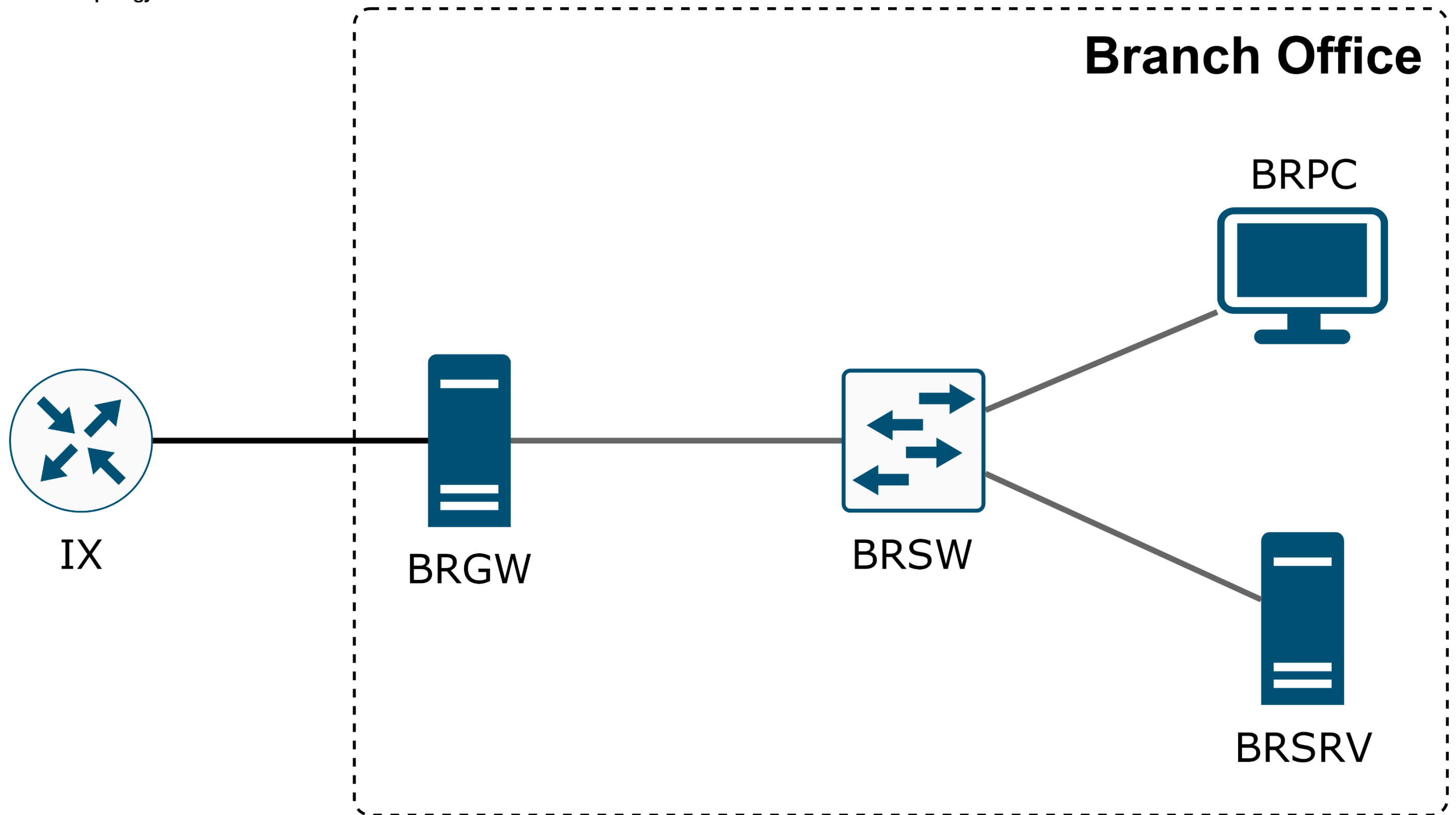
第四站

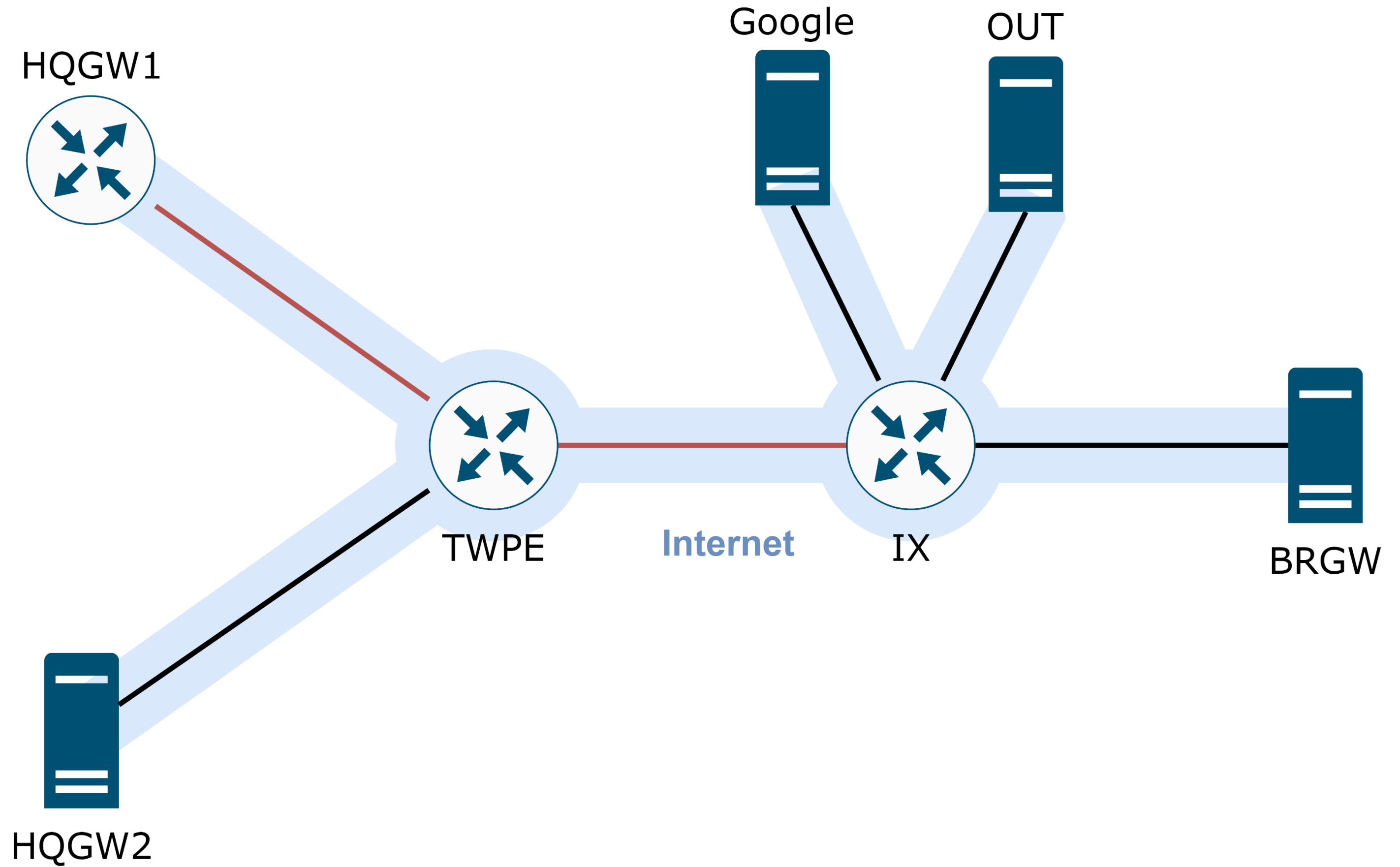
附錄中五個不同的題組，請各別改善每一個網路結構和服務層面，並列出所有存在的問題以及列出相應的解決辦法。

第五站

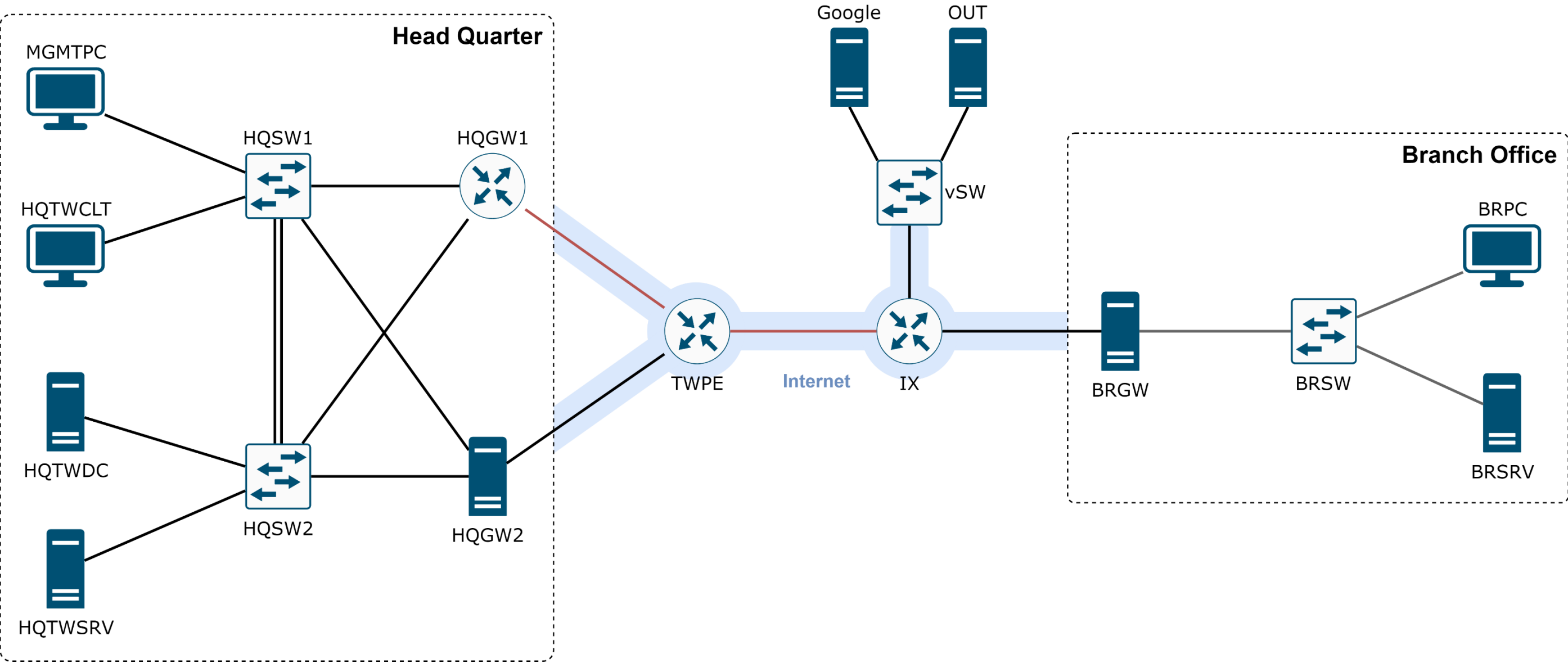
根據第一站的設計，進行系統與網路設備安裝，並規劃實體接線，以及根據需求設定環境、服務和硬體設備。



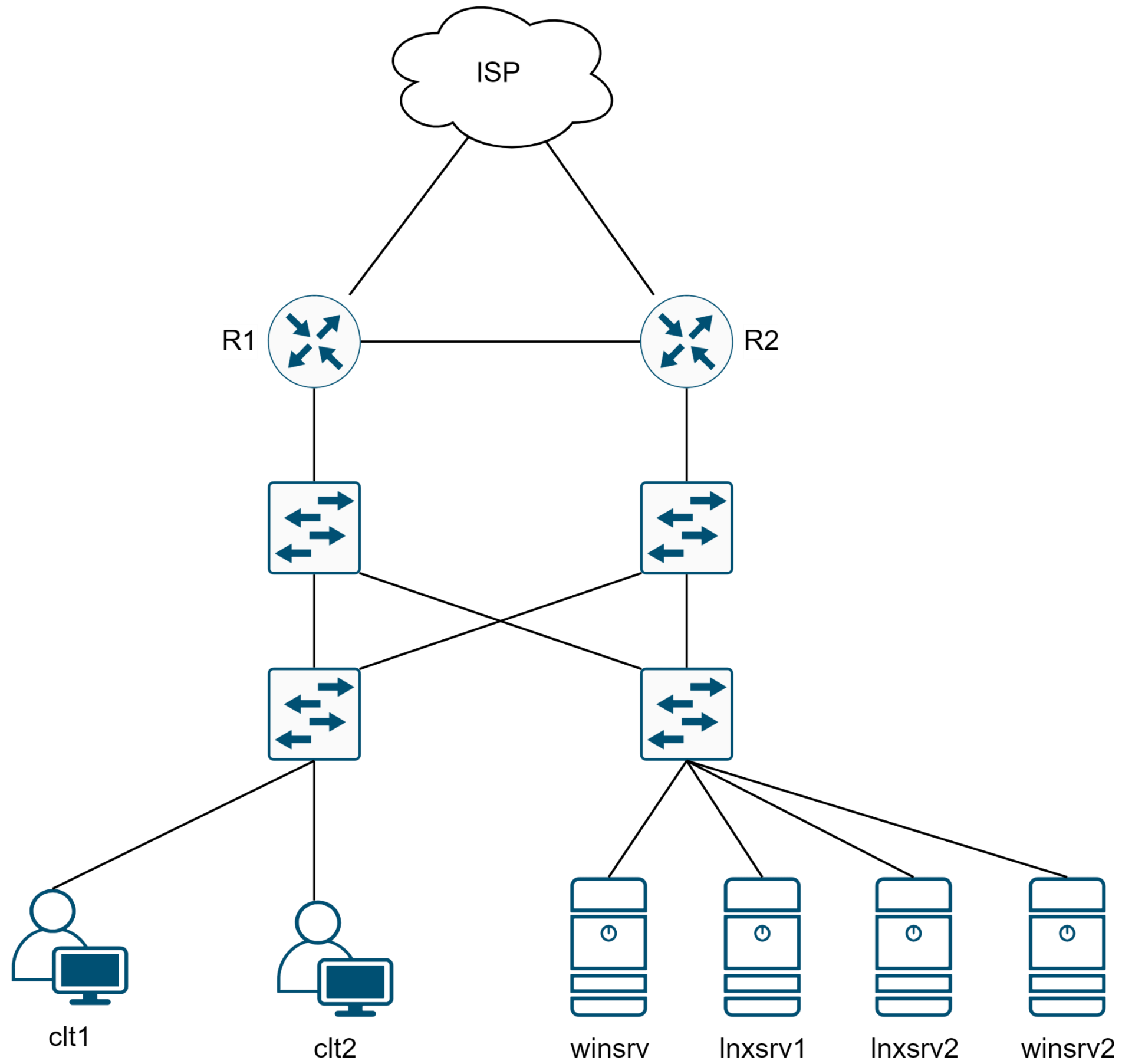




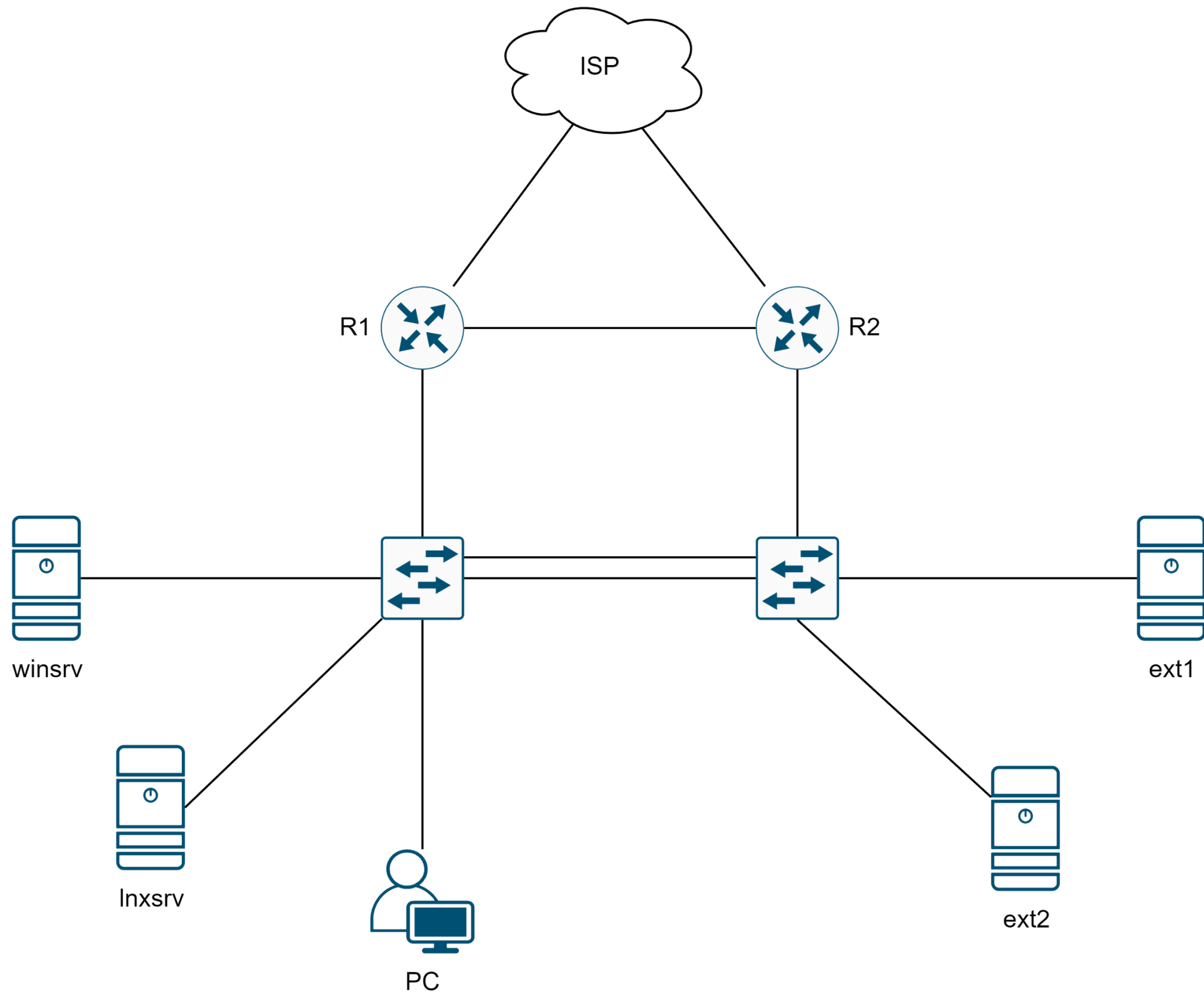
第二站 Topology – Overview



第四站 第一題



第四站 第二題



第四站 第三題

