第 53 屆 全國技能競賽

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 **Skillsc0!**
。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

※ 本試題情境以 Gateway 執行 NAT 功能，供內部存取網際網路，請選手遵循此架構進行實作。於 ISP 上檢閱路由表時，RFC 1918 規範之網段應不可見，否則路由相關項次均不予評分

※ 當使用需要憑證進行加密的服務時，在客戶端不應顯示憑證錯誤。如果有任何憑證錯誤，則該服務將不予評分

第一站

General Setting

- 依據附錄 A 安裝虛擬機，並設定主機名稱、網卡名稱、IP 位址與預設閘道
- 為使評分方便，請於所有主機允許網際網路控制訊息協定

LOGIN

- 確認所有 server 及 client 擁有以下登入資訊

OS	Username	Password
Linux	root	Skillsc0!
	user	
Windows	Administrator	
	user	

System Configuration

- 確認所有 server 及 client 使用以下系統配置

Region/Timezone: Taipei (UTC+8)
Locale: English US (UTF-8)
Key Map: English US

windc

Active Directory

- 作為 wsc2024.tw 的 Domain controller 及 Global catalog
- 建立以下 OU:
  - DevOps
  - Networking
  - Managers
- 建立以下 global AD 群組:
  - TW_DevOps (位於 DevOps OU 底下)
  - TW_Networking (位於 Networking OU 底下)
  - TW_Managers (位於 Managers OU 底下)
- 使用會場提供的 ad-users.csv 建立使用者

DNS

- 將 **ISP** 設定為 forwarder
- 作為 **wsc2024.tw** 內部 DNS
  - 為 wsc2024.tw 當中的 server 建立相對應的 A 記錄
  - 為 wsc2024.tw 當中的 server 建立相對應的 PTR 記錄
  - 為所有 service 建立所需的 CNAME 記錄
  - 建立 MX 記錄
- 作為 **wsc2024.tw** 外部 DNS
  - 建立所需的 A 記錄
  - 為所有 service 建立所需的 CNAME 記錄
  - 建立 MX 記錄
- 若選手無法將內外部 DNS 實作於同一伺服器，請將外部相關記錄維護於 ISP 上

第二站

Group Policy

- Networking 群組無法關閉或重啟系統
- 僅允許 Networking 群組使用者安裝 FileZilla (將使用隨附的 FileZilla_3.64.0_win64-setup.exe 進行測試，請將此安裝檔置於 inpc 的 C 磁碟根目錄下，並於評分前確保 FileZilla 在所有電腦均未安裝)

Certificate Authority

- 組態為 ISP 下的 Enterprise Sub CA，Subject-Name 為 **“CN=WSC2024-CA”**
  - 其 CDP URL 為 **“http://windc.wsc2024.tw/certenroll/WSC2024-CA.crl"**
  - 其 AIA URL 為 **“http://windc.wsc2024.tw/certenroll/WSC2024-CA.crt"**

lnxdc

Domain member client

- 加入 wsc2024.tw 網域，確保網域使用者可以登入此 server

DHCP

- 作為 DHCP server，配發 172.16.10.0/24 網段 IP
  - 配發範圍為 172.16.10.100-172.16.10.199
  - 設定適當的 scope option
  - 必須自動更新 A 、PTR 記錄

Web

- 提供 Web ，URL 為 https://internal.wsc2024.tw
  - 內容顯示 “Internal page for wsc2024.tw”
  - 使用 **WSC2024-CA** 所發布的憑證

E-Mail

- 提供 Webmail，URL 為 https://webmail.wsc2024.tw
  - 設定 SMTPS 及 IMAPS 並作為 wsc2024.tw 的郵件伺服器
  - 所有 wsc2024.tw 當中的使用者都要可以正常寄送、接收郵件
  - 確保能與 worldskills.org 正常寄送、接收郵件
  - 使用 **WSC2024-CA** 所發布的憑證

第三站

Gateway

Routing

- 啟用 forwarding 並作為 router
  - 設定預設路由，供內部存取 internet
- 根據附錄 A 設定 VLAN，並正確設定相對應的 VM Interface
  - 若無法成功實作 ，請將 HQ-Trunk 更改為相對應 VLAN 的 VM Interface

NAT

- 使用 iptables 設定 NAT
  - 讓所有 wsc2024.tw 當中的 host 可以存取 Internet
  - 讓外部可以使用 public IP 1.1.1.2 存取內部服務
  - 內部服務包含: CDP、AIA 、Mail

DHCP Relay Agent

- 設定 DHCP Relay Agent 讓內部 client 可以自動取得 IP

Remote Access

- 設定 SSL VPN 可供 Client 使用 Anyconnect 連線
  - 以 **vpn.wsc2024.tw** 提供服務
  - 使用 192.168.39.0/24 作為 VPN 網段
  - 設定正確的 DNS Server IP
  - 使用 WSC2024-CA 所發布的憑證
  - 確認用戶端連線後仍可存取 Internet

inpc

- 加入 wsc2024.tw 網域，作為內部用戶端測試網路環境
- 信任 CA 憑證，確保評分時不會出現憑證錯誤

第四站

ISP

Routing

- 啟用 forwarding 並作為 router

DNS

- 作為 worldskills.org 的 name server
  - 為 internet network 的 host 建立相對應的 A 記錄
  - 為 service 建立所需的 CNAME 記錄
  - 建立 MX 記錄
- 為 wsc2024.tw 設定 Conditional forwarder

Certificate Authority

- 設定 Root CA，使用 **"/WSC/CA/"** 作為 CA 根目錄
  - Subject-Name 為 **"C=TW, O=WSI, CN=Root-CA"**
  - 其 CDP URL 為 **"http://www.worldskills.org/Root-CA.crl"**
  - 其 AIA URL 為 **"http://www.worldskills.org/Root-CA.crt"**

E-Mail

- 設定 SMTP 及 IMAP 並作為 **worldskills.org** 的郵件伺服器
  - 所有 worldskills.org 當中的使用者都要可以正常寄送、接收郵件
  - 確保能與 wsc2024.tw 正常寄送、接收郵件

Web

- 提供 **https://www.worldskills.org**，作為 Internet 頁面
  - 內容顯示 "Worldskills 2024 FR"
  - 使用 **Root-CA** 所發布的憑證

outpc

- 作為外部用戶端測試網路環境
- 信任 CA 憑證，確保評分時不會出現憑證錯誤
- 登入使用者 user，並使用系統內建 Mail Application 登入 user@worldskills.org 測試 Mail 功能，請勿將測試郵件刪除

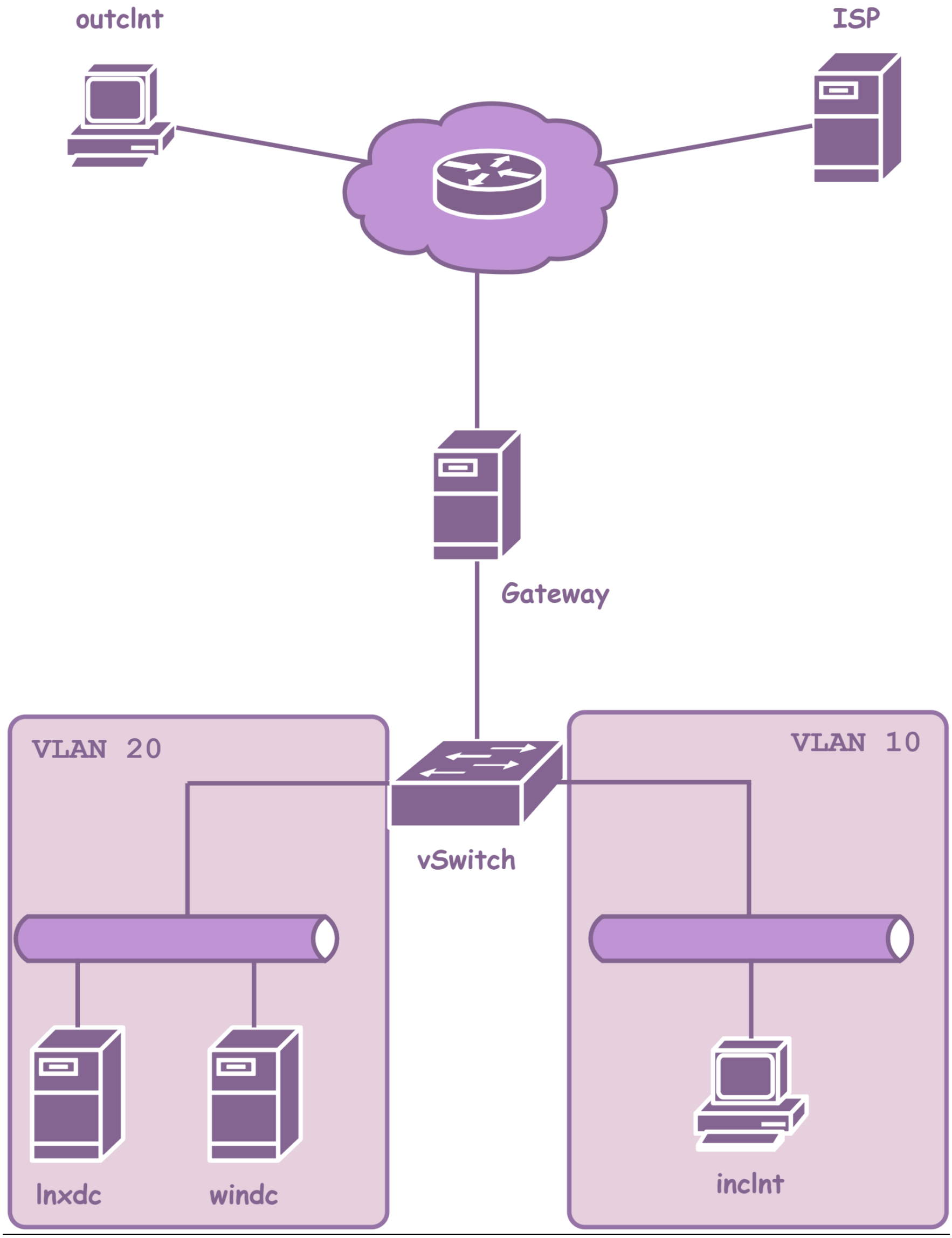
Appendix

IP Address Assignment

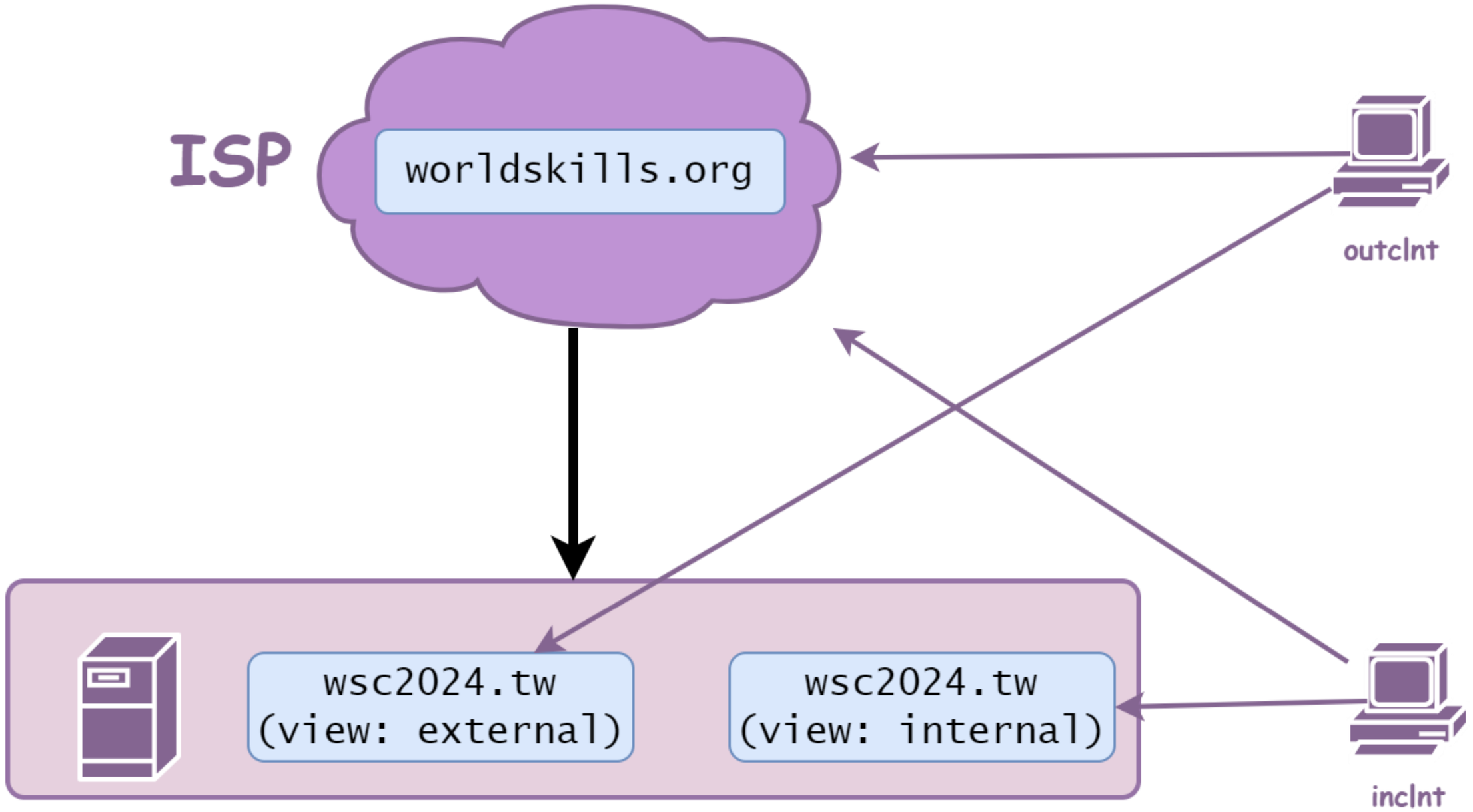
VM Hostname	OS	OS Interface	IP Address	Default Gateway	VM Interface
ISP	Debian 11	eth0	8.8.8.8/24	N/A	Internet
		eth1	1.1.1.1/24		ISP-HQ
outpc	Windows 11	Ethernet0	8.8.8.9/24	8.8.8.8	Internet
Gateway	Debian 11	eth0	1.1.1.2/24	N/A	ISP-HQ
		vlan10	172.16.10.254/24		HQ-Trunk
		vlan20	172.16.20.254/24		
windc	Windows Server 2022	Ethernet0	172.16.20.10/24	172.16.20.254	HQ-VLAN20
lnxdc	Debian 11	eth0	172.16.20.20/24	172.16.20.254	HQ-VLAN20
inpc	Windows 11	Ethernet0	DHCP		HQ-VLAN10

* 若預設閘道為 N/A，則請勿做任何設定，否則該台 VM 不予評分！

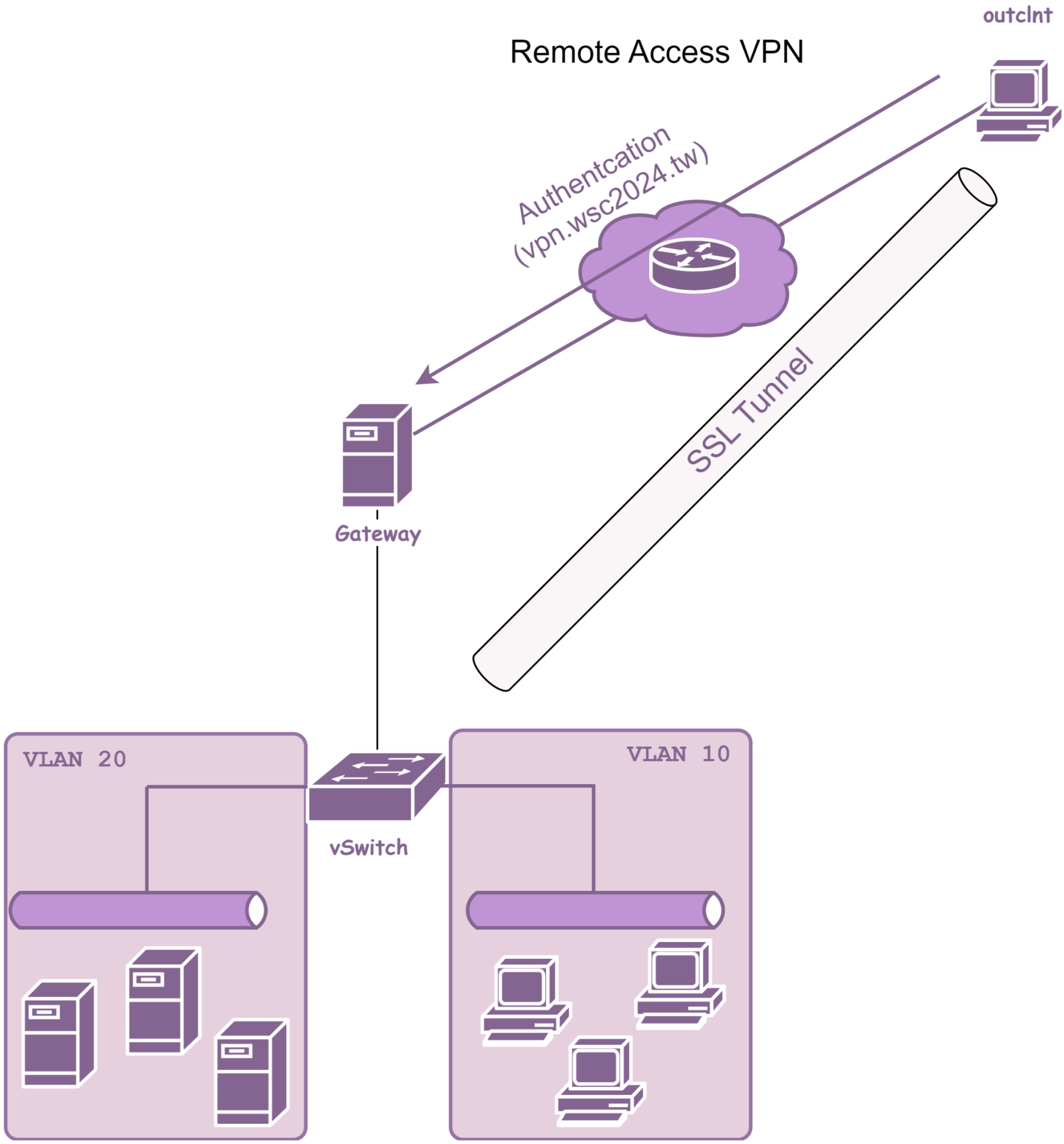
Logical topology 1



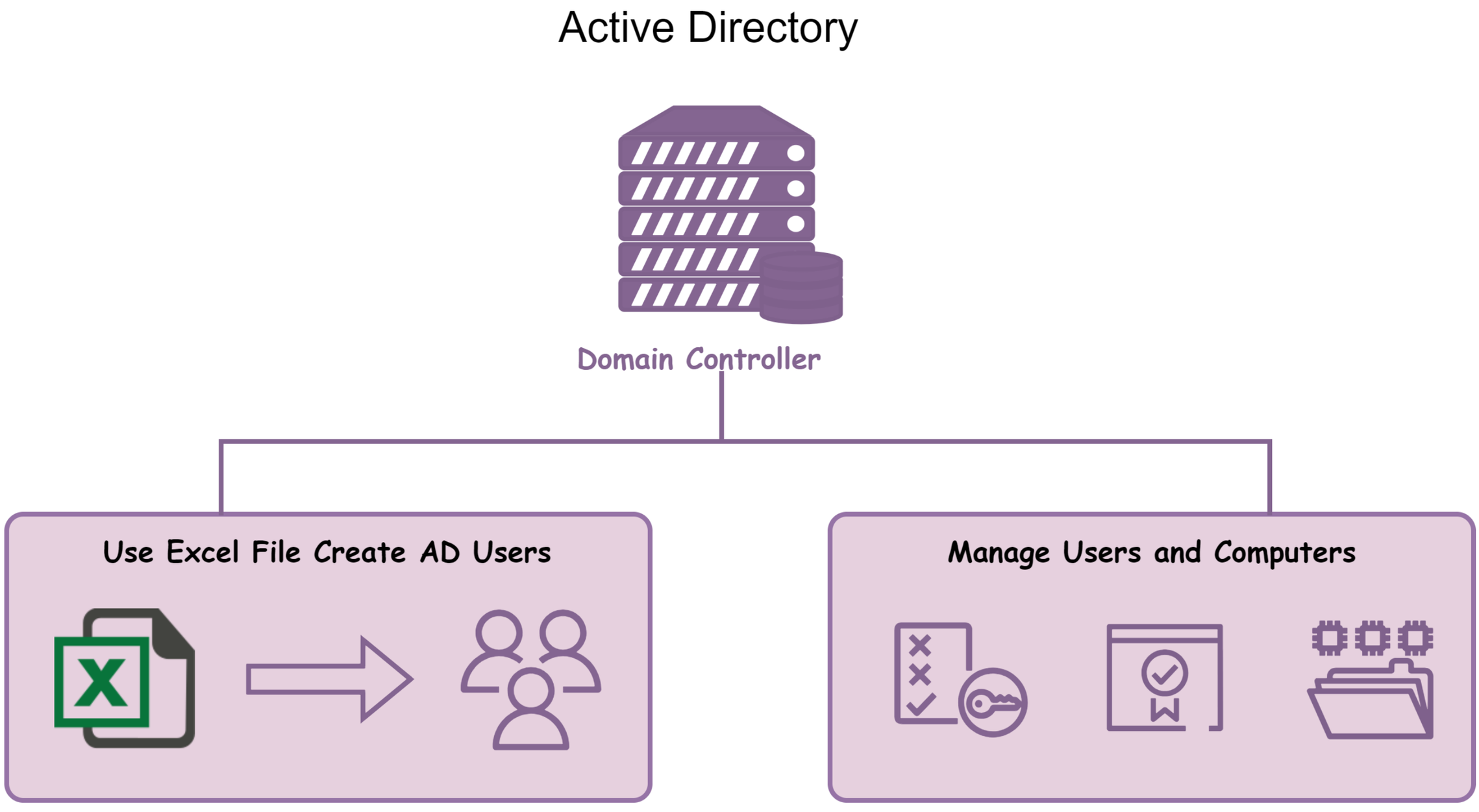
DNS 架構 1


ISP
worldskills.org
outclnt
wsc2024.tw
(view: external)
wsc2024.tw
(view: internal)
inclnt

Remote VPN 架構



Active Directory



第五站

※ 所有 Ansible playbooks 都應放在 Host 的 /data/ansible 目錄底下，可以根據自身需求建立運行 playbooks 相關的資料夾/檔案。

General Setting

- 依據附錄 A 安裝虛擬機，並設定主機名稱、網卡名稱、IP 位址與預設閘道
- 為使評分方便，請於所有主機允許網際網路控制訊息協定

Ansible

General

- 所有 tasks 在執行第二次時都應該只會有 “ok” 或是 “skipped” state
- SSH 連線時應使用 dev 使用者進行連線

Basic config

- 建立 1-basic.yml 以進行系統基本設定
  - 根據 /etc/ansible/hosts 檔內的 “hostname” 變數設定主機名稱
  - 根據環境需求調整 /etc/resolv.conf 並設定正確的 DNS Server
  - 根據需求調整正確 /etc/hosts
  - 將時區調整為 Taipei (UTC+8)

Users

- 建立 2-users.yml 以新增使用者
  - 根據 /etc/ansible/users.csv import 使用者
  - 確保 uid, user, password, home, shell 屬性正確
  - 確保當使用者的 UID 及名稱相同時，password 並不會 change

SSH

- 建立 3-ssh-server.yml 以設定 SSH
  - /etc/ansible/users.csv 使用者進行 SSH 連線時，僅允許透過 “sshport” 欄位中指定的 port 登入

DNS

- 建立 4-dns-server.yml 以設定 DNS
  - 安裝 DNS，並掌管“portal.wsc2024.tw”
  - 根據環境需求新增相關紀錄

Web

- 建立 5-web-server.yml 以設定 Web
  - 安裝 Web service
  - 根據 "/etc/ansible/users.csv" url 欄位建立 http 個人網頁
  - 網頁內容顯示 "Homepage for <user>!”
  - 連線時於瀏覽器輸入 http://[**url**] ，將顯示位於 /home/[**user**]/[**DocumentIndex**]欄位，例如 http://richard.portal.wsc2024.tw/ 將開啟位於 /home/richard/hit.html 頁面

第六站

Site-to-Site VPN

GRE over IPsec

- 於 Gateway 與 R1 之間建立 GRE over IPsec VPN
  - IPsec 加密演算法可自行決定
  - 透過動態路由協定交換路由，確保兩邊內部網路可以互相存取
  - 確保 Ansible Zone 可以存取 Internet

windc

DNS

- 將 portal.wsc2024.tw 子網域授權給 LIN1

Monitoring

Grafana & Prometheus

- 在 lnxdc 使用提供的 tar.gz 檔安裝 Grafana 與 Prometheus
    - Grafana URL 為 https://monitor.wsc2024.tw
- 在 Grafana 使用提供的 JSON 檔，建立一個名為 Node Exporter 的 Dashboard
    - 在 Dashboard 中可以監控 HQ Site 中的所有 Linux 主機基本數據，例如 CPU、記憶體、硬碟與網路的使用狀況
- 在 Grafana 新增一個名為 Web Monitor 的 Dashboard
    - 每 15 秒會連線至 https://www.worldskills.org，檢查是否正常回應 HTTP 200
    - 呈現方式不限，但是需在網頁狀態異動時，在畫面上明顯發現有異常
    - 請在評分前確認該網頁狀態為正常；評分時會執行指令將網頁服務暫停，並觀察 Grafana Dashboard 的畫面；請選手在下方寫下將網頁服務暫停的指令：
        - _____

Appendix

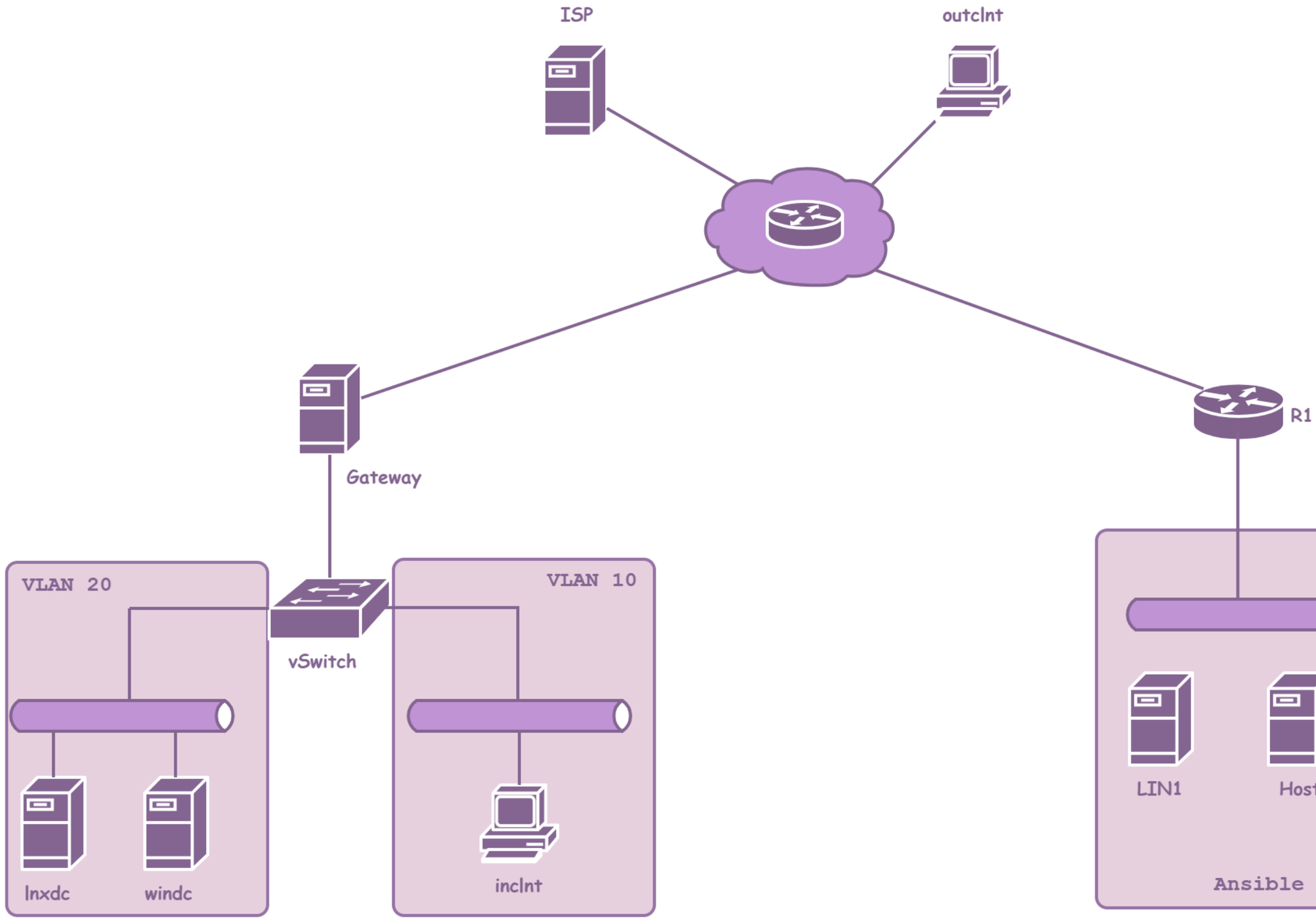
IP Address Assignment

VM Hostname	OS	Interface	IP Address	Default Gateway	VM Interface
ISP	Debian 11	eth0	8.8.8.8/24	N/A	Internet
		eth1	1.1.1.1/24		ISP-HQ
		eth2	2.2.2.1/24		ISP-BR
outpc	Windows 11	Ethernet0	8.8.8.9/24	8.8.8.8	Internet

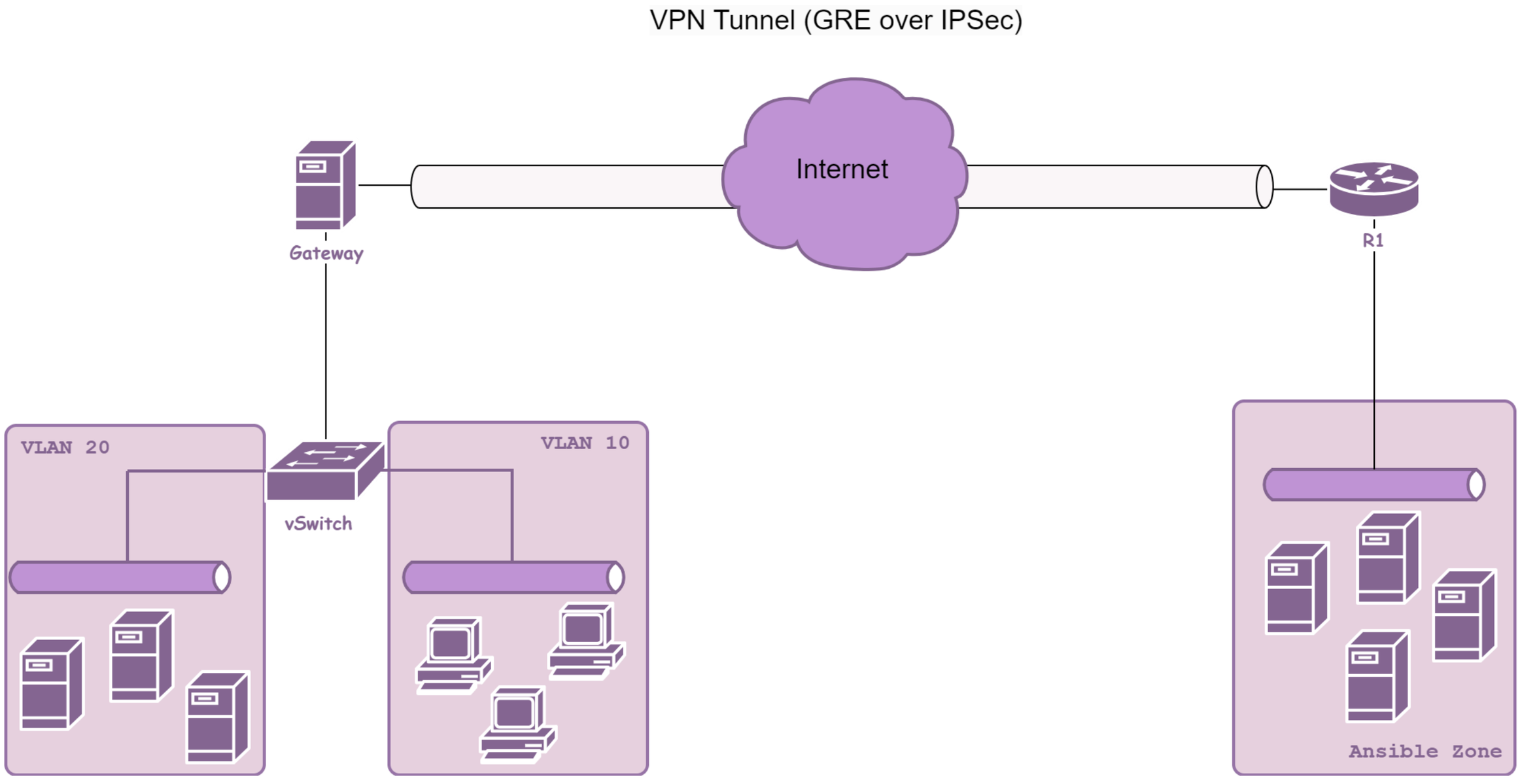
Gateway	Debian 11	eth0	1.1.1.2/24	N/A	ISP-HQ
		Tun0	10.10.10.1/30		N/A
		vlan10	172.16.10.254/24		HQ-Trunk
		vlan20	172.16.20.254/24		
windc	Windows Server 2022	Ethernet0	172.16.20.10/24	172.16.20.254	HQ-VLAN20
lnxdc	Debian 11	eth0	172.16.20.20/24	172.16.20.254	HQ- VLAN20
inpc	Windows 11	Ethernet0	DHCP		HQ- VLAN10
R1	Cisco IOS-XE	GigabitEthernet1	2.2.2.2/24	N/A	ISP-BR
		GigabitEthernet2	10.1.1.254/24		BR-LAN
		Tun0	10.10.10.2/30		N/A
Host	Debian 11	eth0	10.1.1.10/24	10.1.1.254	BR-LAN
LIN1	Debian 11	eth0	10.1.1.20/24	10.1.1.254	BR-LAN

* 若預設閘道為 N/A，則請勿做任何設定，否則該台 VM 不予評分

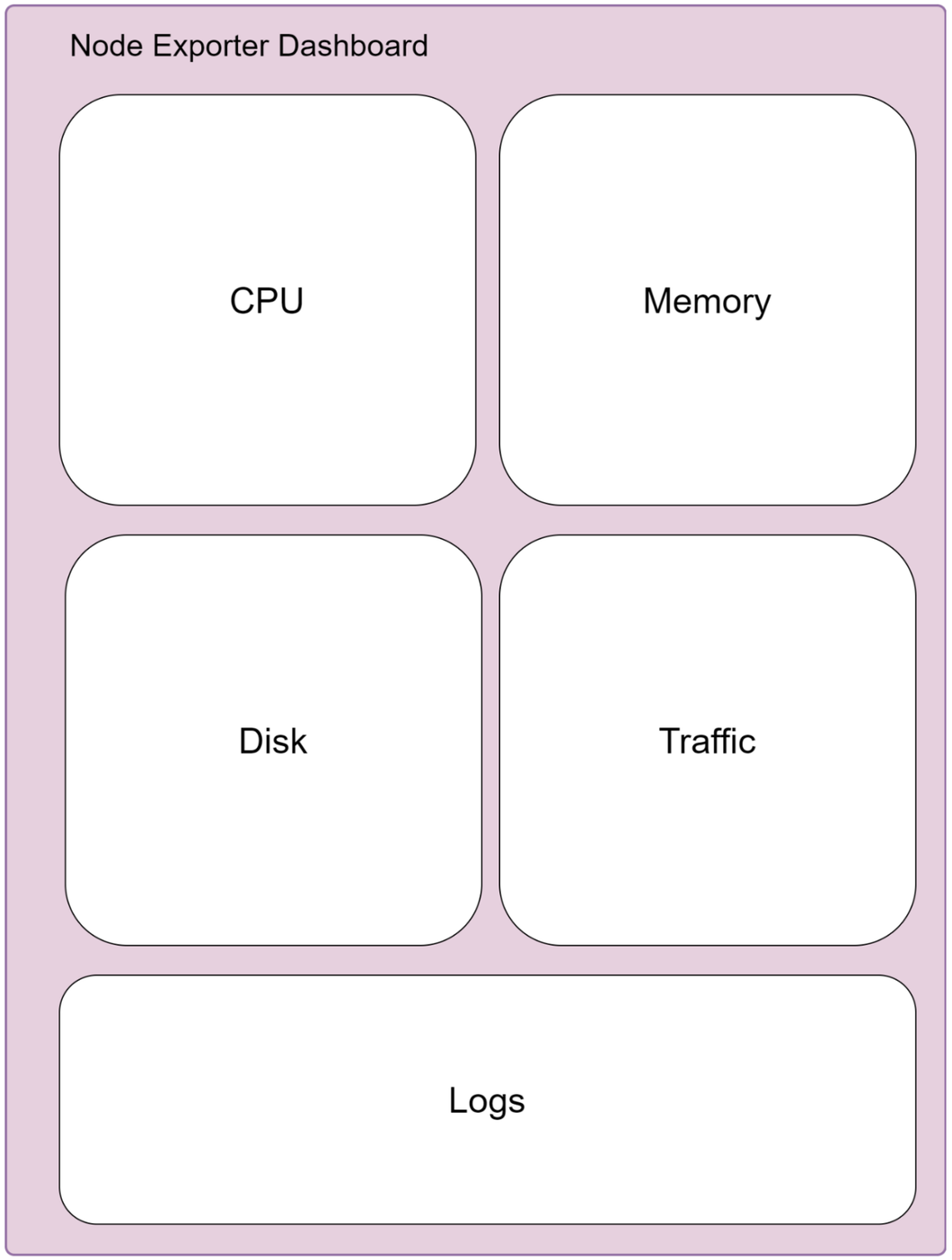
Logical topology 2



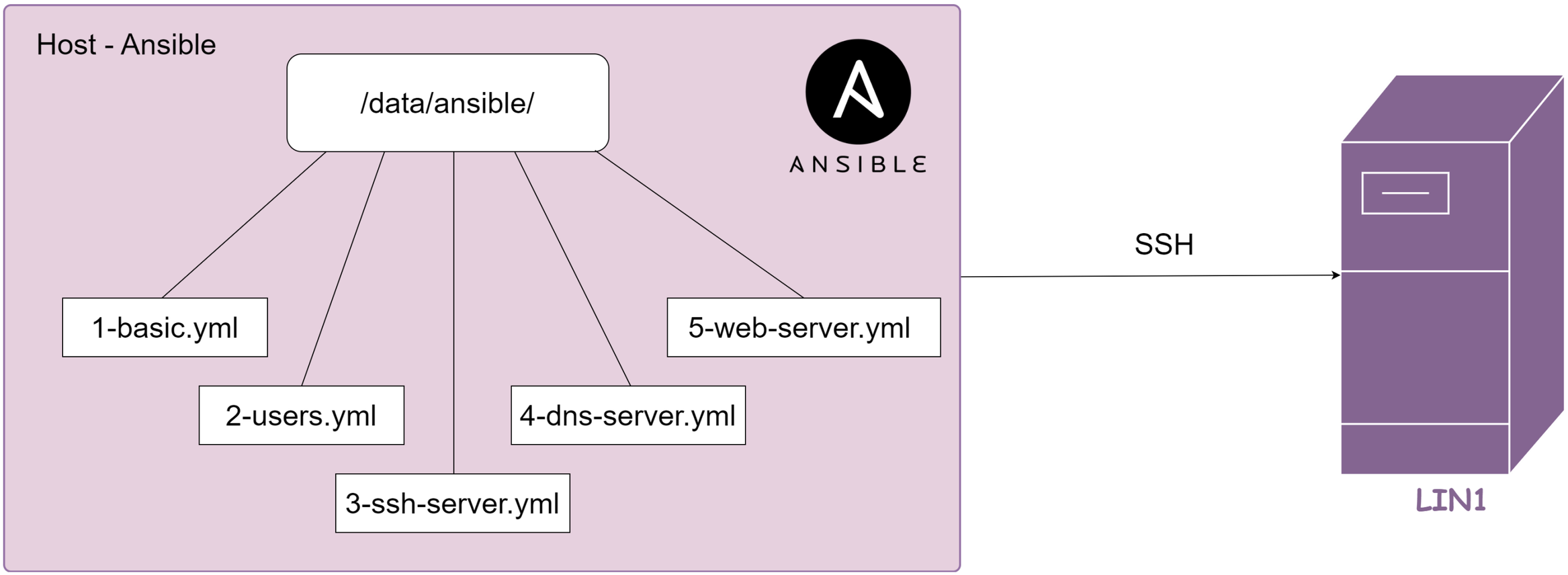
VPN 運作方式


VPN Tunnel (GRE over IPSec)
Internet
Gateway
R1
VLAN 20
VLAN 10
vSwitch
Ansible Zone

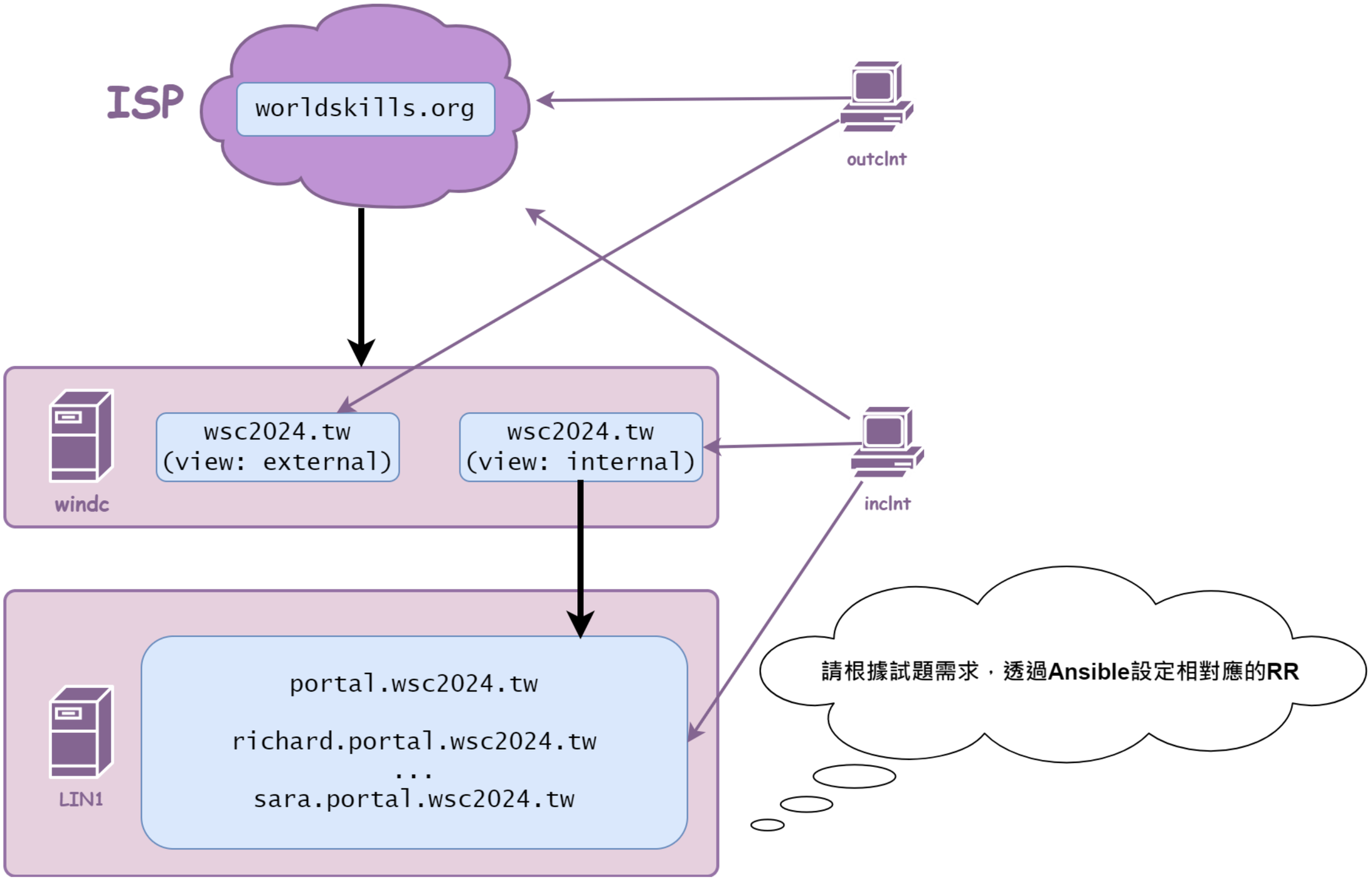
Monitoring 架構



Ansible 運作機制



DNS 架構 2


ISP
worldskills.org
outclnt
wsc2024.tw
(view: external)
wsc2024.tw
(view: internal)
windc
inclnt
portal.wsc2024.tw
richard.portal.wsc2024.tw
...
sara.portal.wsc2024.tw
LIN1
請根據試題需求，透過Ansible設定相對應的RR

第七站

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

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

。所有 Switch 的 E3/0-E3/3 介面，僅用於臨時相互連接使用，不開放跨網路設備傳輸或存取網際網路

。於 Switch 之間的介面設定 Link Aggregation，請以建立鏈結需時較短的方式完成，並以外部通訊對象為分配流量的依據（所有用戶端存取同一個 Internet 上的伺服器時，來回的訊務均將使用同一條 實體接線進行傳輸）

。所有使用者的流量於 Switch 之間轉遞時應帶有 802.1Q Tag

。所有 Switch 於接線狀態改變時，應使用 Proposal / Agreement
機制進行協商，並避免 ASW2 的 E0/2 介面在此期間遭遇瞬斷

。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

。額外設定相關機制，供相容的用戶端以 SLAAC 取得 IPv6 DNS Server 資訊

。於 HQCPE 上設定對外的預設路由

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

第八站

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)
。為避免 Headquarter 與 Branch Office 失聯，造成 Branch OfficePC 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 NATOverload，直接存取 Internet

Security

。於 HQ 的 Access Layer Switch 防堵 ARP 攻擊，允許的 ARP 內容基於其是否吻合用戶端以 DHCP 請求位址的當下所記錄的資訊

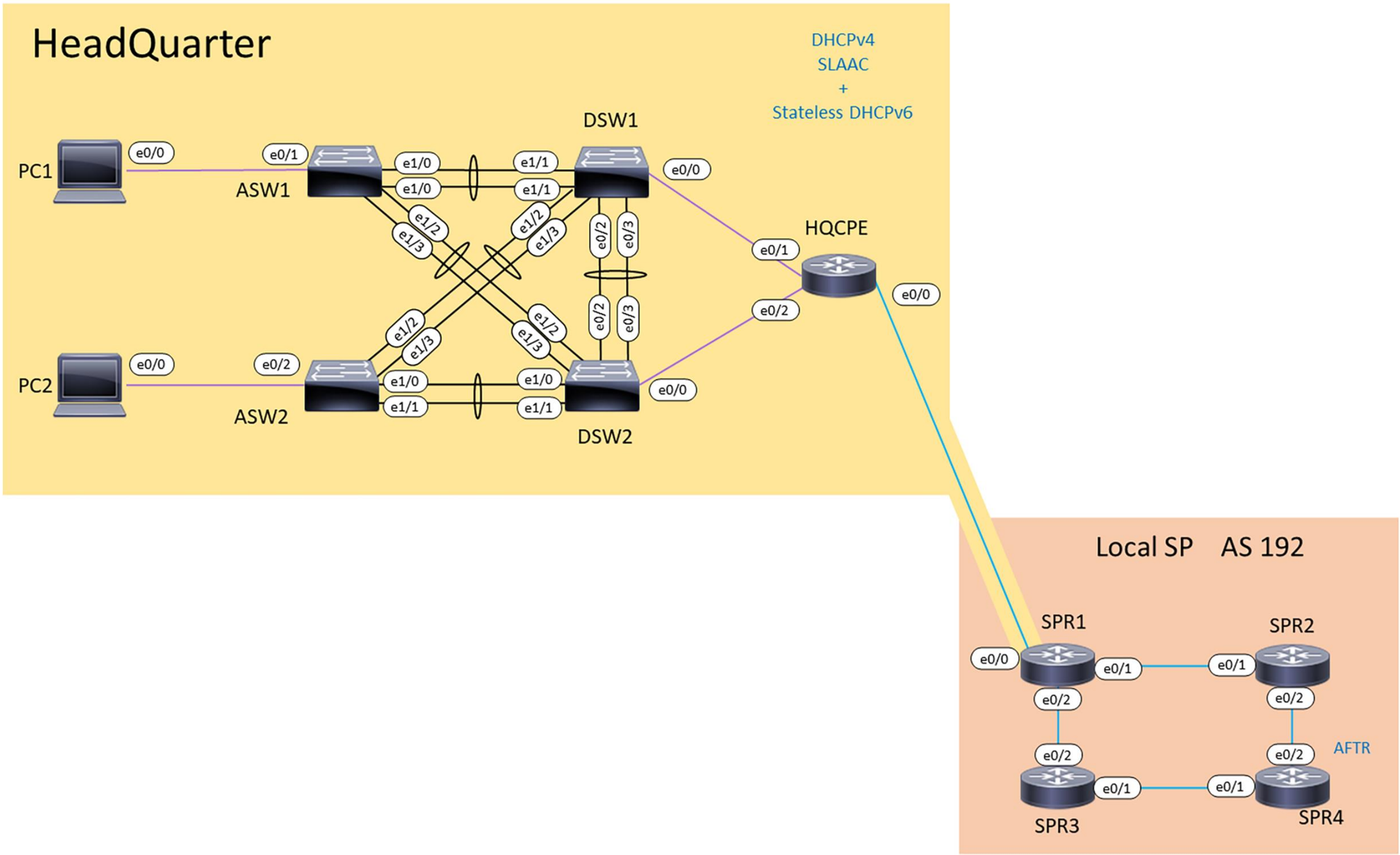
。將 HQCPE 與 BOGW 之間的 Tunnel 以 IPsec 加密

。將 HQCPE 與 SPR4 之間的 Tunnel 以 IPsec 加密

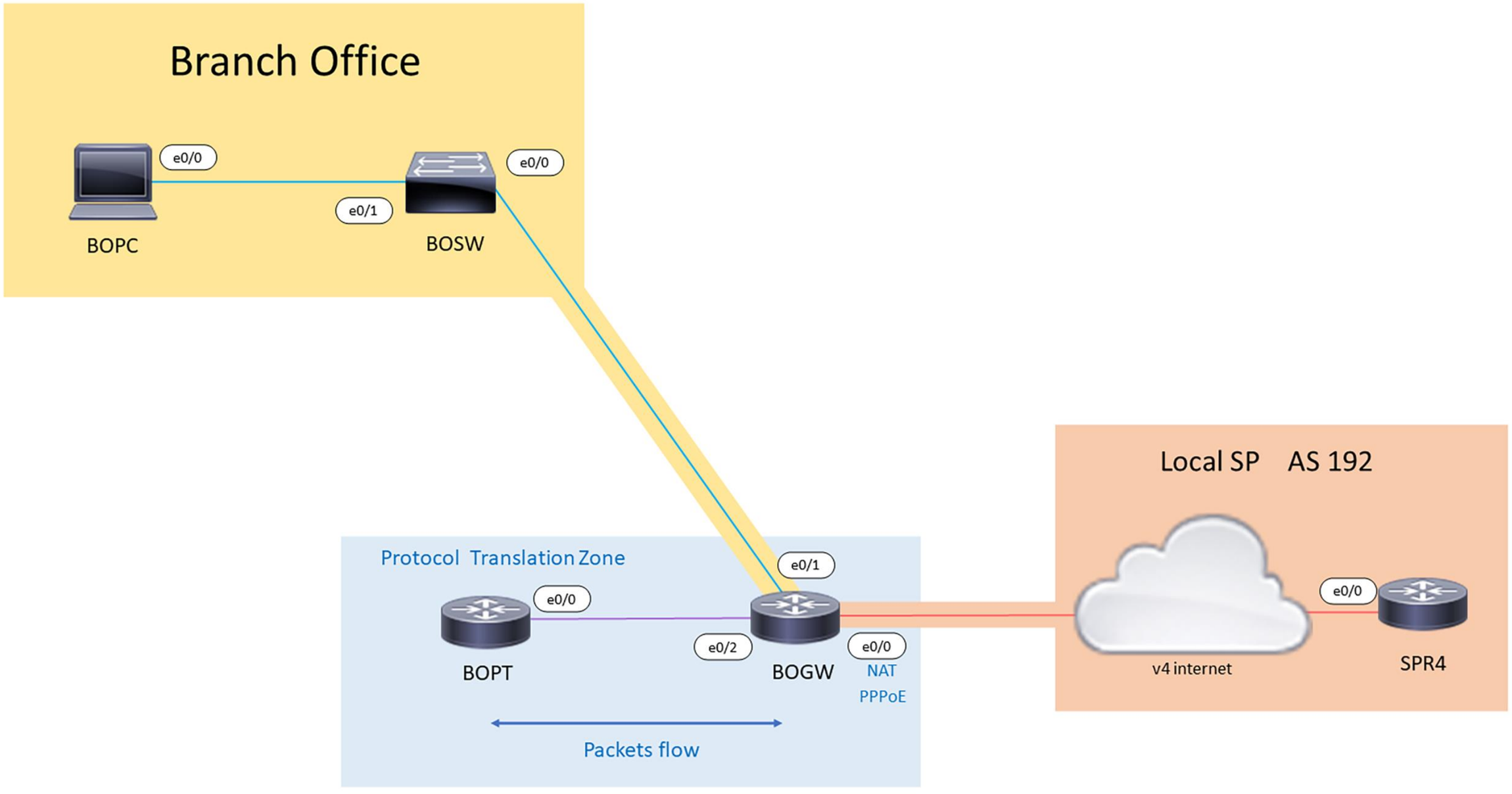
。由於 IPv6 並無 NAT 提供簡易的防護，請於 HQCPE 上針對 IPv6 設定 Stateful Access Control，避免來自 Internet 的主動連線

※完成後，Headquarter 與 Branch Office 的 PC 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

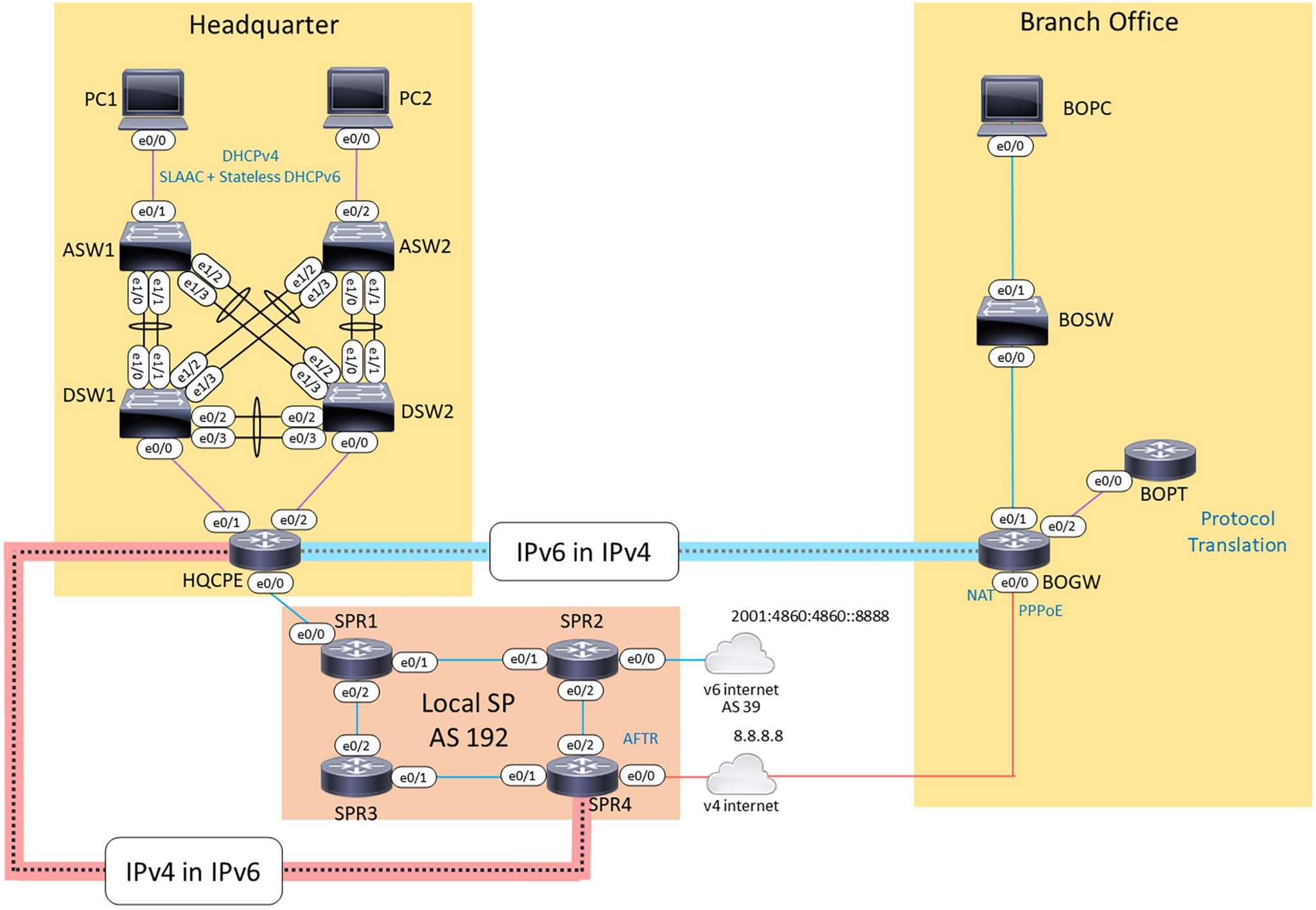
HeadQuarter 架構



Branch Office 架構



Overview


Headquarter
PC1
PC2
e0/0
e0/0
DHCPv4
SLAAC + Stateless DHCPv6
e0/1
e0/2
ASW1
ASW2
e1/2
e1/3
e1/0
e1/1
DSW1
DSW2
e0/2
e0/3
e0/0
e0/1
e0/2
HQCPE
IPv6 in IPv4
Branch Office
BOPC
BOSW
BOPT
Protocol
Translation
BOGW
NAT
PPPoE
SPR1
SPR2
SPR3
SPR4
Local SP
AS 192
AFTR
2001:4860:4860::8888
v6 internet
AS 39
8.8.8.8
v4 internet
IPv4 in IPv6