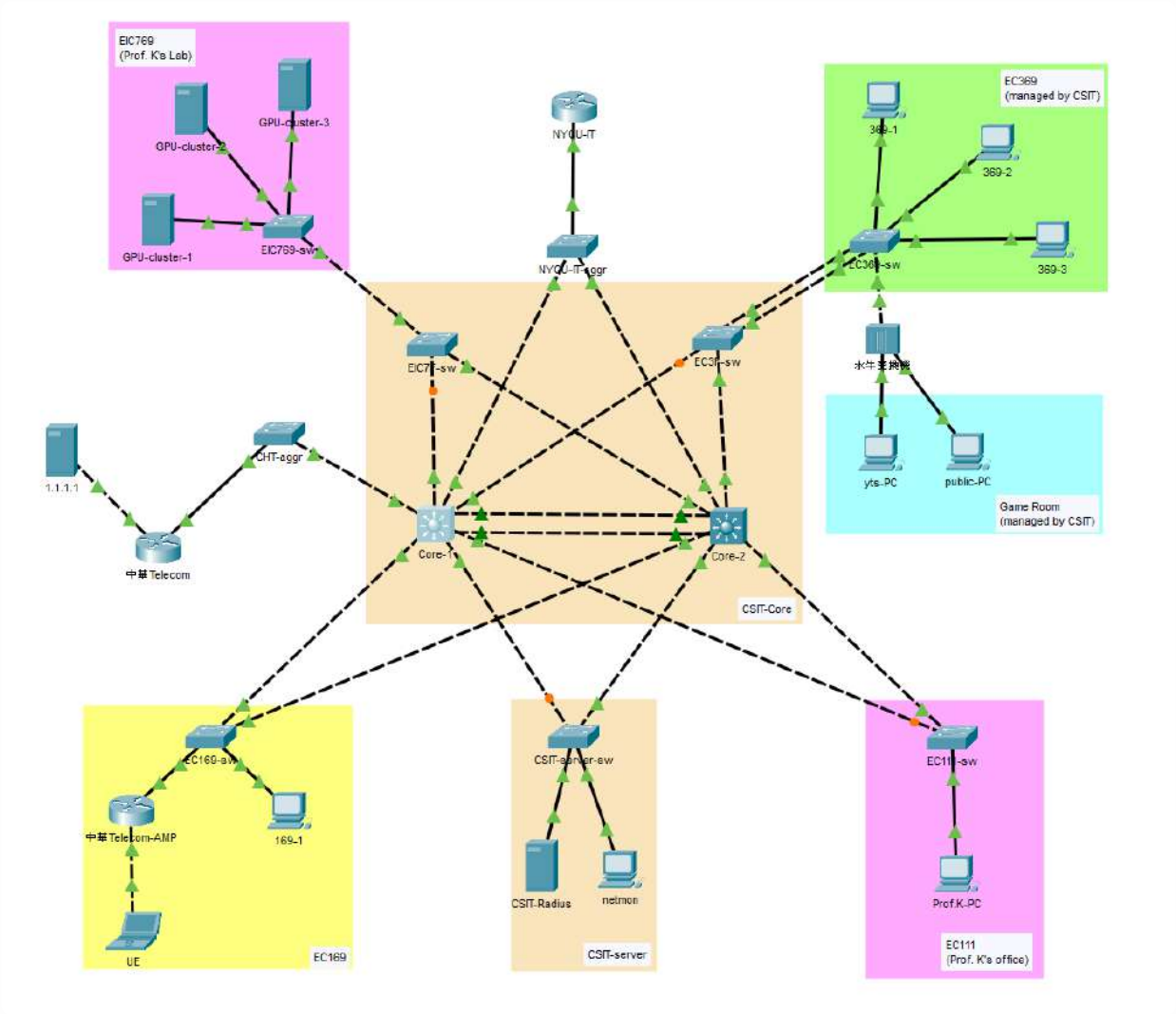
CCNA Lab4 (Release)

情境



在經過課程的磨練後你成為了 cc 助教與中華電信的實習生，你將靠著前幾次 Lab 的知識完成資工系網路拓譜的建置。身為資工系的助教，你有義務盡可能的滿足資工系內教授與學生的要求(best effort)。

施工範圍

所有機器前綴為 `CSIT`, `EC`, `EIC` and `Core` (屬於CSIT) 還有中華電信相關的機器 (屬於 CHT) 都是你的操作範圍(aggr除外)。
為了減少溝通流程， `NYCU-IT` 授權你設定他們的機器以快速完成拓譜需求。

⚠️ 注意事項 ⚠️

- 寫作業的過程中建議定時存檔，以免 Packet Tracer 突然 crash
  - 特別是在 Simulation 模式下如果紀錄太多封包可能會因為記憶體用量過大而 crash，請多加注意
  - 定時存檔包括保存 pka 以及 switch 的設定
- 在 Packet Tracer 底下測試網路時，時常有「前幾次測試沒通，後來就通了」的情況
  - 如果網路不通時可以多測 1、2 次以確保不是 Packet Tracer 在雷你
- 請勿增加任何不必要的設定以免影響自動評分腳本

Spec

Basic

- Hostname: 每台 switch & router 的 hostname 為 label 上的名字 (中華Telecom = CHT)
- 記得 shutdown 所有沒有使用的 interfaces
- STP mode: rapid-pvst
- 設定 AAA，RADIUS Server 資訊如下
  - host: 140.113.100.175
  - port: 1812
  - name: radius (必要時才需設定)
  - Preshared-Key: 1l0v3T4
  - 帳號: `ccna`, 密碼: `ddob` (共用)
  - 所有 CSIT 的機器都能透過上述帳號密碼登錄 (名稱皆設為與 hostname 相同)
- 新增一條 authentication list 叫 ssh_login
  - 僅看 RADIUS server 和 local user
  - RADIUS server 優先於 local user
  - 請將它套用到所有 vtys
- SSH
  - domain-name: cs.nctu.edu.tw
  - version 2
  - key length: 2048

VLANs

- Game Room 使用 VLAN 38
- EC169 使用 VLAN 169
- EC369 使用 VLAN 369

- Prof. K 使用 VLAN 111
- MGMT 使用 VLAN 100
- CHT 使用 VLAN 209

請依據網段自行判斷 IP 設定位置

- Vlan 100 /27
  - Core-1 140.113.100.165
  - Core-2 140.113.100.166
  - CSIT-server-sw 140.113.100.167
  - EC169-sw 140.113.100.169
  - EC111-sw 140.113.100.170
  - EC3F-sw 140.113.100.171
  - EC369-sw 140.113.100.172
  - EIC7F-sw 140.113.100.173
  - EIC769-sw 140.113.100.174
- Vlan 111 /27
  - gateway: 此網段最後一個可用 IP
  - Core-1 140.113.111.180
  - Core-2 140.113.111.182
- Vlan 169 /25
  - gateway: 此網段最後一個可用 IP
  - Core-1 140.113.169.110
  - Core-2 140.113.169.112
  - CHT-AMP 140.113.169.100
- Vlan 369 /24
  - gateway: 此網段最後一個可用 IP
  - Core-1 140.113.69.250
  - Core-2 140.113.69.252
- Vlan 38 /28
  - gateway: 此網段最後一個可用 IP
  - Core-1 140.113.38.10
  - Core-2 140.113.38.12
- Vlan 209 /29
  - Core-1

        - SVI: 172.168.10.1
        - gig1/0/10: 172.168.10.11
    - Core-2
        - SVI: 172.168.10.2
        - gig1/0/10: 172.168.10.12
    - NYCU-IT
        - 172.168.10.3
    - CHT
        - 172.168.10.13

PC & Servers

因為研究生忙於產出論文，請幫助他們設定終端設備以確保他們能夠正常上網。
請依據網段自行判斷 Default gateway

- CSIT-server
    - CSIT-Radius 140.113.100.175
    - netmon 140.113.100.176
- EC169
    - UE: 210.211.99.1/24
    - 169-1: 140.113.169.1/25
- EC111
    - Prof.K-PC: 140.113.111.165/27
- EC369
    - 369-1: 140.113.69.1/24
    - 369-2: 140.113.69.2/24
    - 369-3: 140.113.69.3/24
- Game room
    - yts-PC: 140.113.38.1/28
    - public-PC: 140.113.38.2/28
- EIC769
    - GPU-cluster-1: 140.113.111.166/27
    - GPU-cluster-2: 140.113.111.167/27
    - GPU-cluster-3: 140.113.111.168/27

Redundancy

Core-1 與 Core-2 是為了 HA 而設計的冗餘架構，請依據此理念為核心配合 VLAN 設定表來決定所有線路的模式 (acess or trunk)。

- Core-1 <-> CHT-aggr: access
- EC169-sw <-> CHT-AMP: access
- Core-1 <-> Core-2: trunk all available VLANs

LAG

設定後所有 LAG 都應該為 up

- Core-1 <-> Core-2
  - static group 1
- EC3F-sw <-> EC369-sw
  - LACP group 2
  - EC369-sw: passive

OSPF

- Core-1、Core-2 的 OSPF 請不要宣告在 interface 上
- NYCU-IT、CHT 的 OSPF 請宣告在 interface 上
- Single area 0, process-id 42

> 請記得將除了 MGMT 以外的內部網路宣告出去，否則外面的世界碰不到這

RIP (外網模擬)

CHT 要用 RIP 把 1.1.1.1 宣告出去
version 2
network 1.0.0.0

> Hint: 可以去 1.1.1.1 裡面翻一下，找到你需要的資訊

FHRP

- 請使用 HSRPv2
- group id = VLAN id
- VLAN 369
  - 將 Core-{1,2} 的 priority 設為 {100, 200}，使得無論任何開機順序 Core-1 為 active 且 Core-2 為 standby
- 請自行判斷剩下的哪些網段需要使用。

> Hint: 哪些 VLAN 需要 gateway 但前面沒有設定到?

GRE tunnel

NYCU-IT 作為學校的網路管理中心，流量理應以 NYCU-IT 的路由器作為 AS 對外的 gateway，但因為某些因素 CHT 並沒有實體線接入 NYCU-IT，而是接入 CSIT 的 Core-1。請利用 GRE tunnel 實現旁路由，讓資工系內所有流出的封包還是經由 NYCU-IT 轉送。

- CHT <-> NYCU-IT (Interface number 69)
  - NYCU-IT: 69.69.69.1/30
  - CHT: 69.69.69.2/30

> Hint: 在 OSPF 要如何將 default route 告訴其他人?

有教授反應在實驗室內 4G 訊號很差，因此中華電信決定在 EC169 內加裝一台訊號放大器。你必在 CHT 與 CHT-AMP 之間設定 tunnel 使得 UE 可以碰到外網。 UE 網段只存在於 UE 與 CHT-AMP 之間，且 UE 只能通到外網而不能碰到資工系內的其他機器 (see ACLs)。

- CHT <-> CHT-AMP (Interface number 0)
  - CHT: 10.0.0.2/30
  - CHT-AMP: 10.0.0.1/30
  - CHT-AMP gi0/0/0: 140.113.169.2/25
  - CHT-AMP gi0/0/1: 210.211.99.2/24

> Hint: 記得設定返回路徑的 static route(只宣告必要路由)

Tunnel network should not be declared in OSPF

ACLs

在設定 ACL 之前要確定所有參與 routing 的機器都能互相 ping 通

> ChatGPT(看看就好):
> 當我踏進資工系機房的那一刻，腦中浮現的是整張拓樸圖與那數十條 VLAN 線路的邏輯。我們身為 CC 助教，被賦予一個任務：不只是讓網路能通，而是「讓誰該通就通、誰不該通就永遠封鎖在外」。
> 第一個設下規則的是管理 VLAN，這是學校網管的禁地，我們不允許它越過 Core 路由器對外連線，於是我寫下 Outgoing ACL；同時，我們也必須守好從外部進入的邊界，擋下所有 10.x 和 192.168.x 的非法來源。
> 面對 Game room，我們給予了它們連線自由，但前提是不能碰資工系內網——不管是 Vlan209 還是其他教室的 IP。
> 而在夜深人靜的時候，總有那麼一個人——我們的網路管理者 ｙｍｌａｉ，只從他那一台主機進行遠端管理。於是我們只留下那唯一的 IP 通過 ACL 30，其餘一律拒絕。在完成所有基本拓樸連線後，我們開始強化網路邊界的管控。資工系核心區 EC369 是我們重點監控的對象之一。那裡

> 除了學生使用，也常有伺服器測試部署。我們不希望有人直接從外部透過 HTTP 或 HTTPS 嘗試掃描或攻擊 EC369 的設備，因此我們設定 ACL 110，精準封鎖所有目的埠為 80 與 443 的 TCP 流量。
> 這些 ACL，不只是設定，它們像是一道道看不見的防線，靜靜守護著資工系網路的秩序。

- named `Outgoing` standard ACL，請使用恰好 2 條 entries，對於從 Core-{1,2} 往 NYCU-IT
  - 禁止來自 Management 網段流量出去
  - 允許其他所有流量出去
- named `Incoming` standard ACL，請使用恰好 3 條 entries，對於從 NYCU-IT 往 Core-{1,2}
  - 禁止所有來自 192.168.0.0/16 或是 10.0.0.0/8 的流量進入
  - 允許其他所有流量進入
- named `UE-OUTBOUND` extended ACL，請使用恰好 3 條 entries，上對於 CHT-AMP
  - 禁止 UE 訪問資工系內部網路(包含 Vlan209)
  - 允許其他流量進入
- named `GAMEROOM-OUTBOUND` extended ACL，請用恰好 2 條 entry，對於 Gameroom
  - 禁止 Gameroom 主機訪問資工系內部網路
  - 允許其他流量
- numbered 30 standard ACL，請用恰好 1 條 entry，對於 Core-{1,2}
  - 僅允許來自 140.113.100.176/32 的 SSH 上來，否則直接拒絕 SSH 流量
  - 不能設定在 interface 上
- numbered 110 extended ACL，請使用恰好 3 條 entries，對於 EC369
  - 禁止 dst port 是 80、443 的 TCP 流量進入
  - 允許其他所有流量進入

若有兩種設定位置的可能，請優先設定在 VLAN SVI 上，並且思考其中的差異

Q&A 與 Tips

AAA 有設好但是就是沒辦法 SSH 進去，換了一隻帳號就可以了，這是爲什麼？

可以藉由 `show aaa local user lockout` 檢查是否因爲該帳號登入次數過多而被鎖登入。

Core-{1,2} 有那麼多個 IP，RADIUS Server 要怎麼設定 Client IP？

可以在 Core-{1,2} 上面下 `show ip route` 來看他的 route table，看 RADIUS Server 的 IP 會從哪個 interface 出去，就填該 interface 的 IP。

作業繳交

- 如果有任何對 Spec 有不清楚的地方需要請助教解釋或是需要助教幫忙，請寄信到 npta@cs.nctu.edu.tw **如果你寄信到助教的私人信箱，那麼有可能會被忽略！**
- 將 pka 上傳至 E3 作業繳交區（檔名請命名為 HW4_<學號>.pka）
  - e.g. HW4_123456789.pka
  - 命名錯誤扣 project 總分 10 分
- 請確定你有保存 switch 的 config，到時候評分時我們將重啓交換機。
- 最後分數將以評分腳本爲主，完成度僅供參考。
- **Deadline: 2025/5/23 19:00。**