

國家高速網路與計算中心

TWAREN VPLS與SSL-VPN 架構說明

報告人: 莊博勝

TWAREN架構演進－第一代

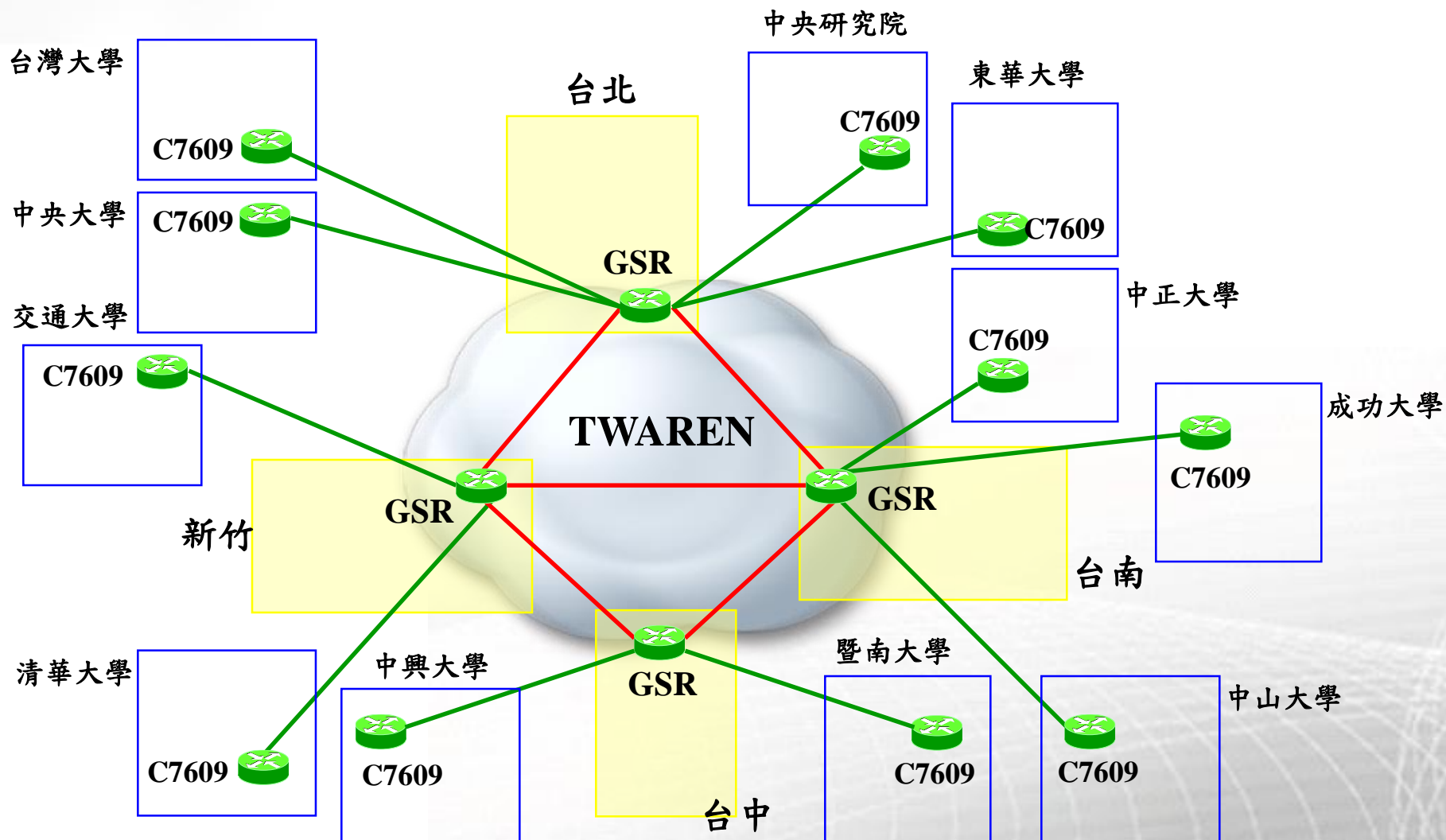
- Production Network
- Research Network
- Optical Network

Production Network

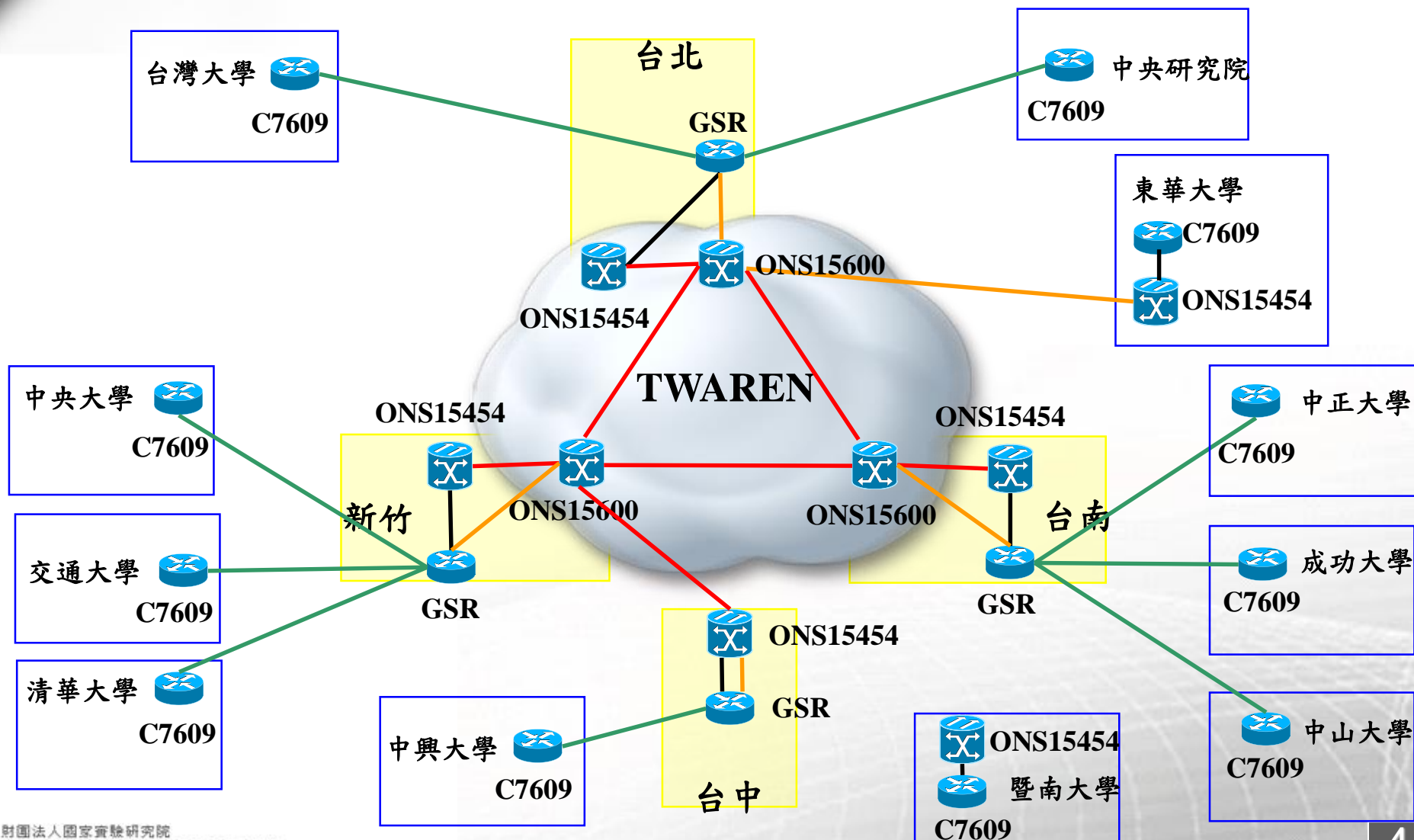


Optical
Production
Research

10GE
STM-64/OC-192
STM-16/OC-48
GE



Research Network

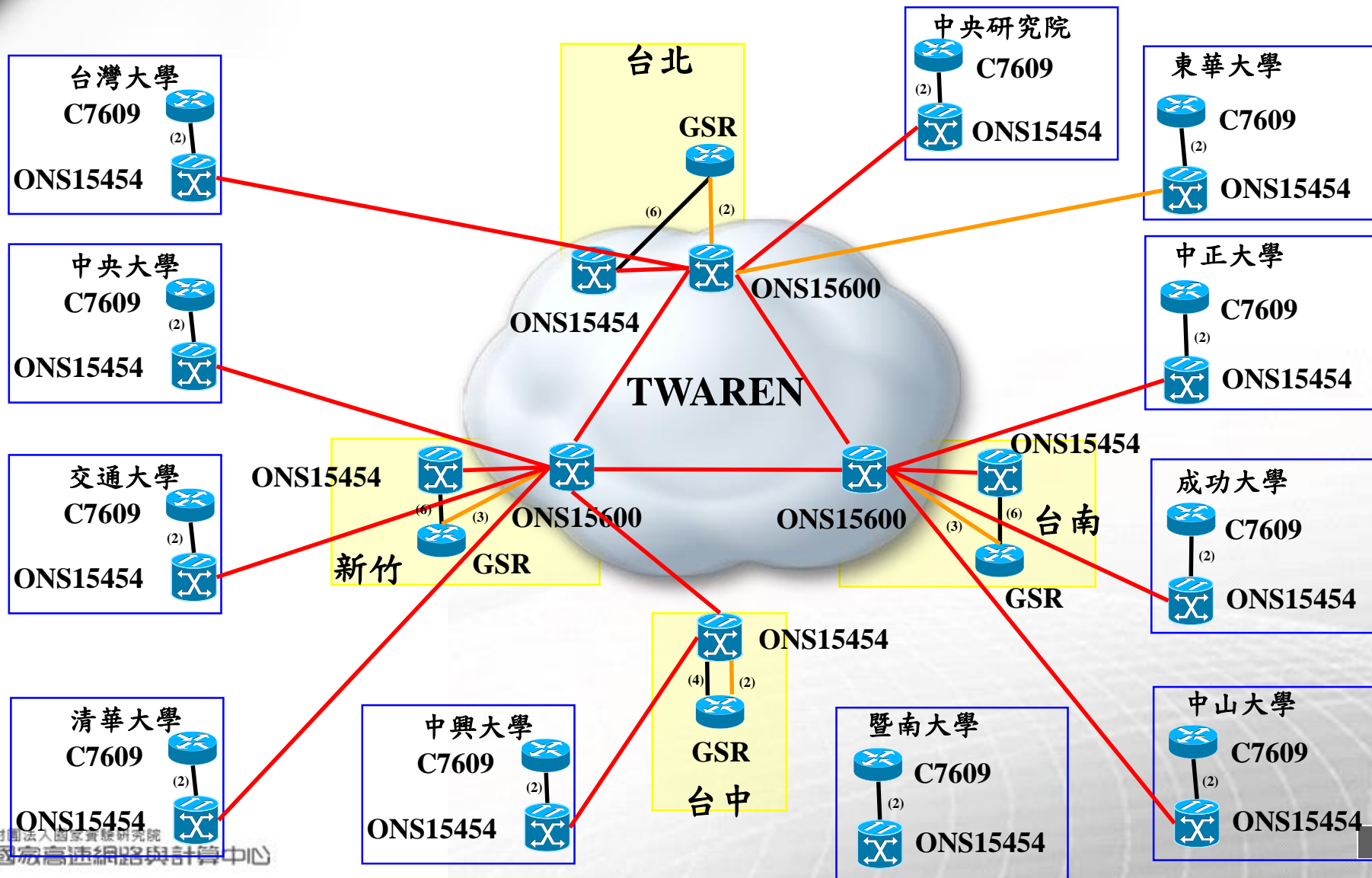


Optical Network



Optical
Production
Research

10GE
STM-64/OC-192
STM-16/OC-48
GE



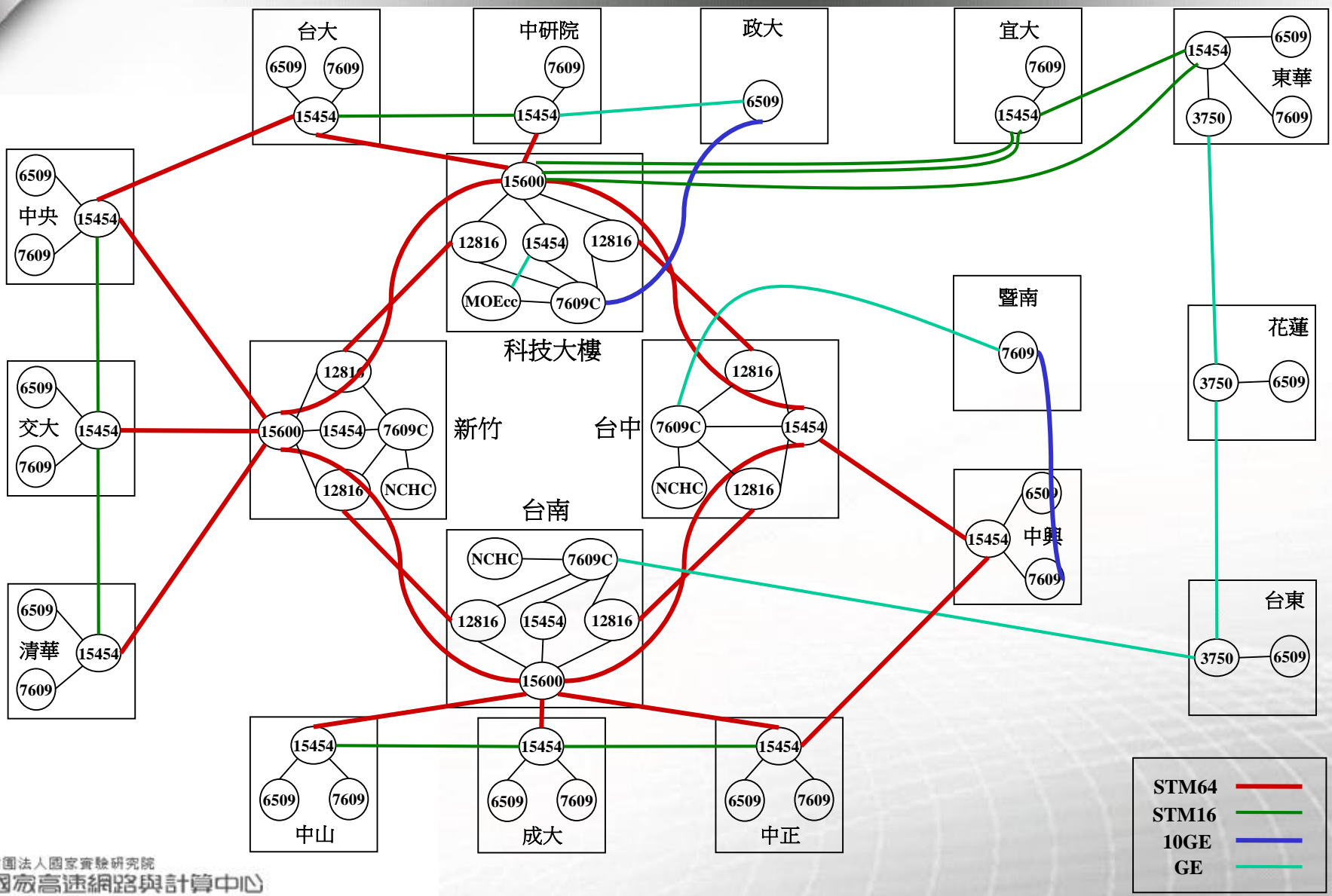
TWAREN架構演進 – 第二代

- Physical Topology
- Logical Topology
- VLAN Topology

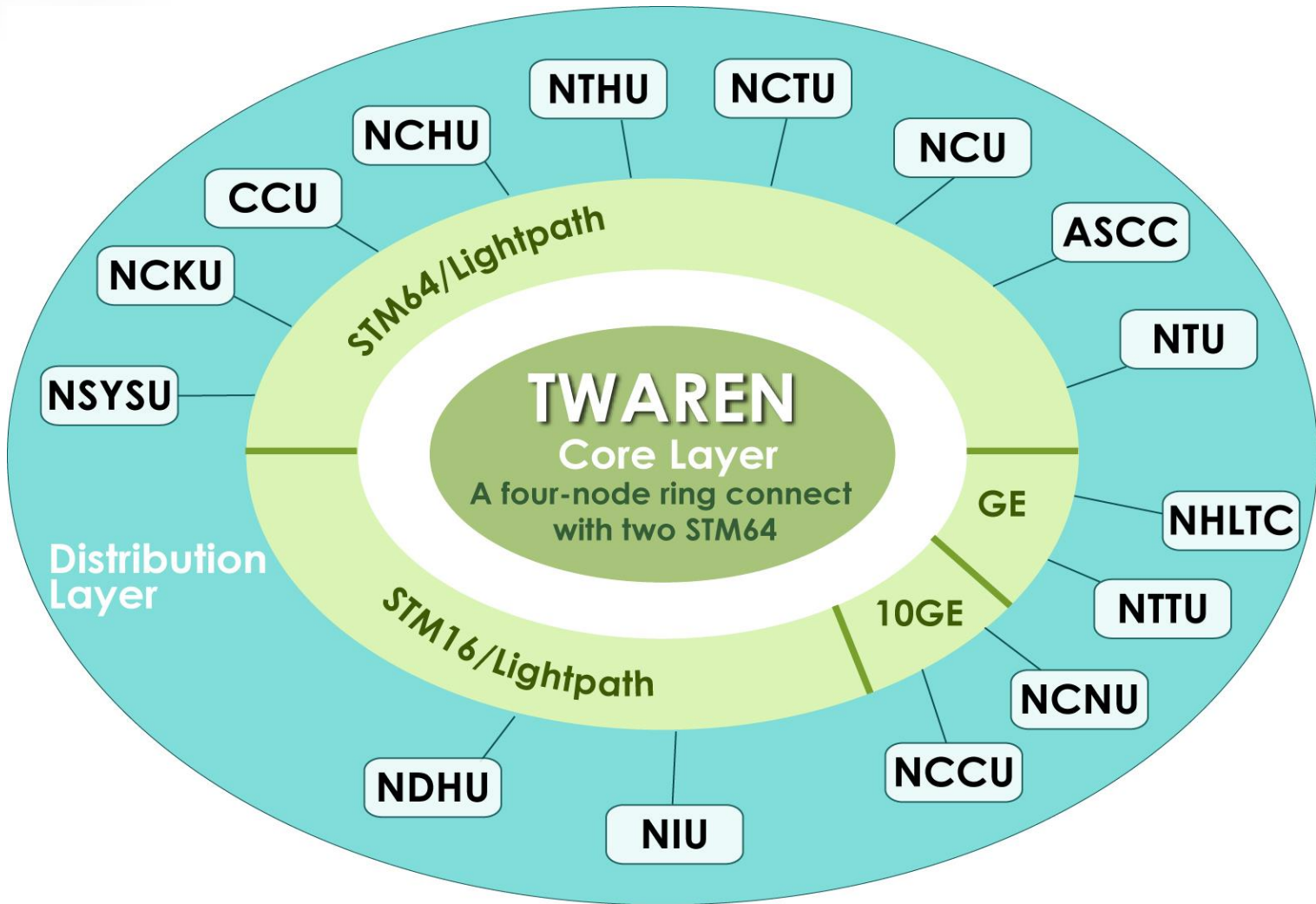
Physical Topology 1/2



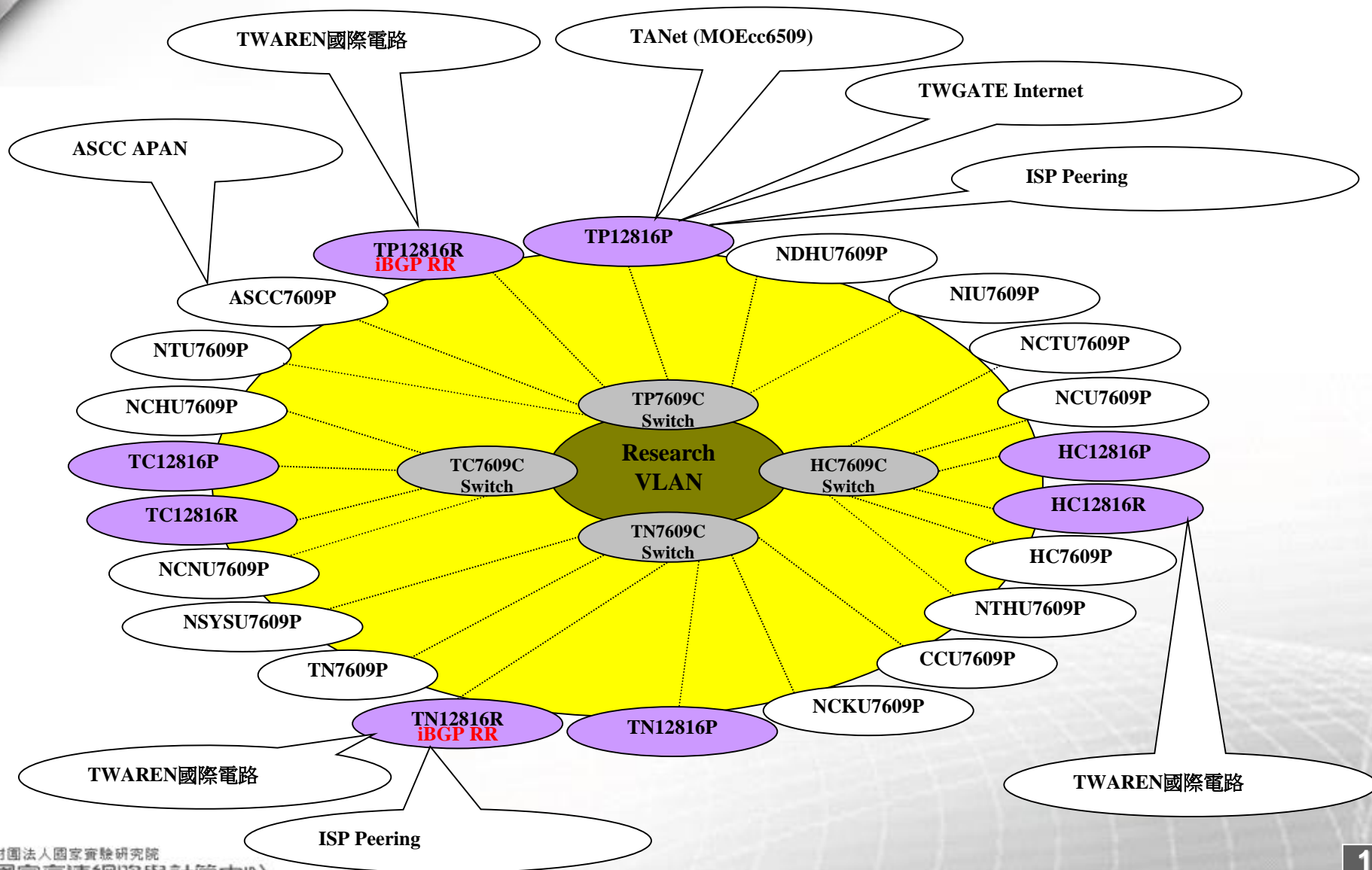
Physical Topology 2/2



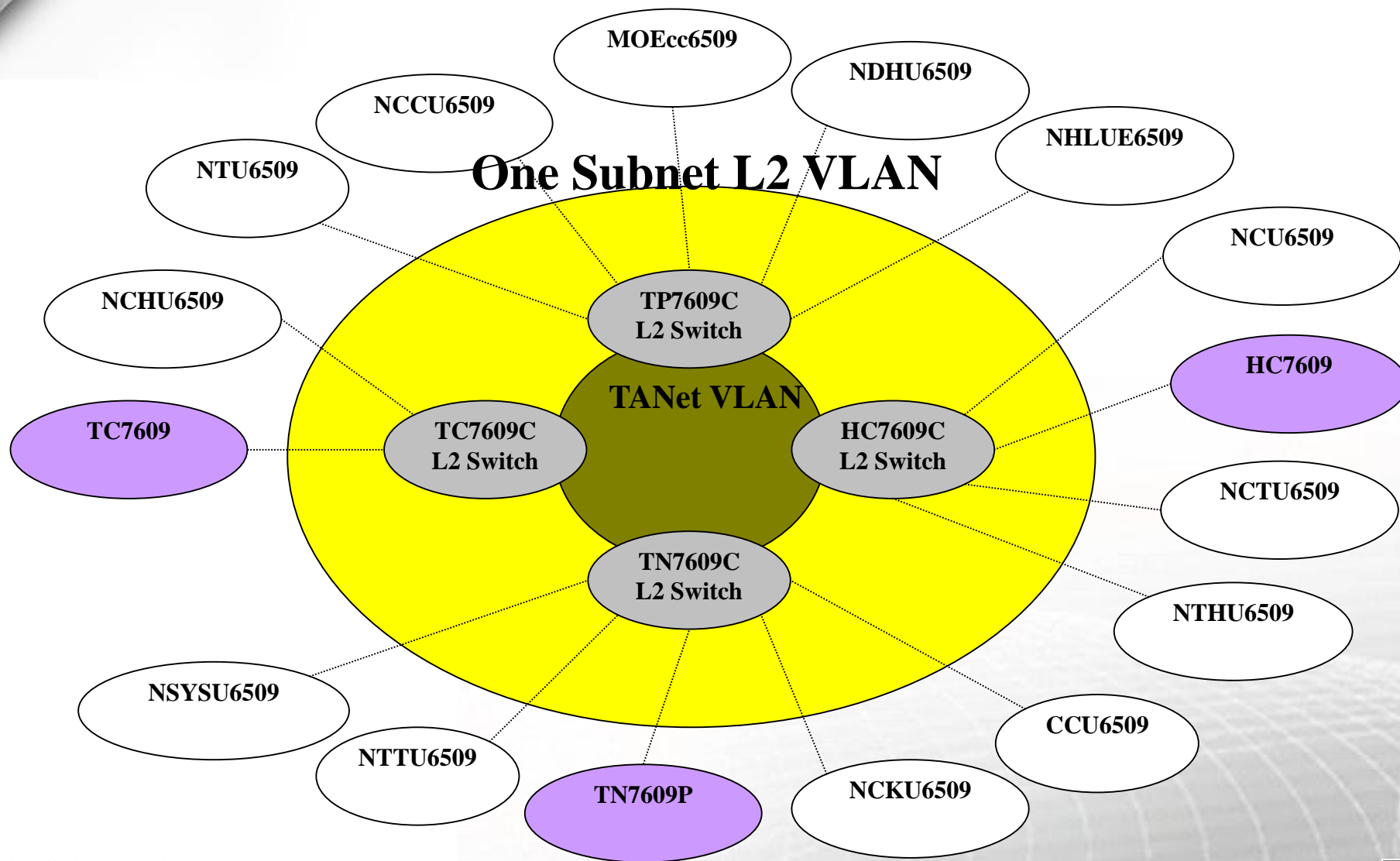
TWAREN Logical Topology



Research VLAN Topology



TANet VLAN Topology



TWAREN架構演進－第三代

- VPLS Physical Topology
- VPLS Logical Topology



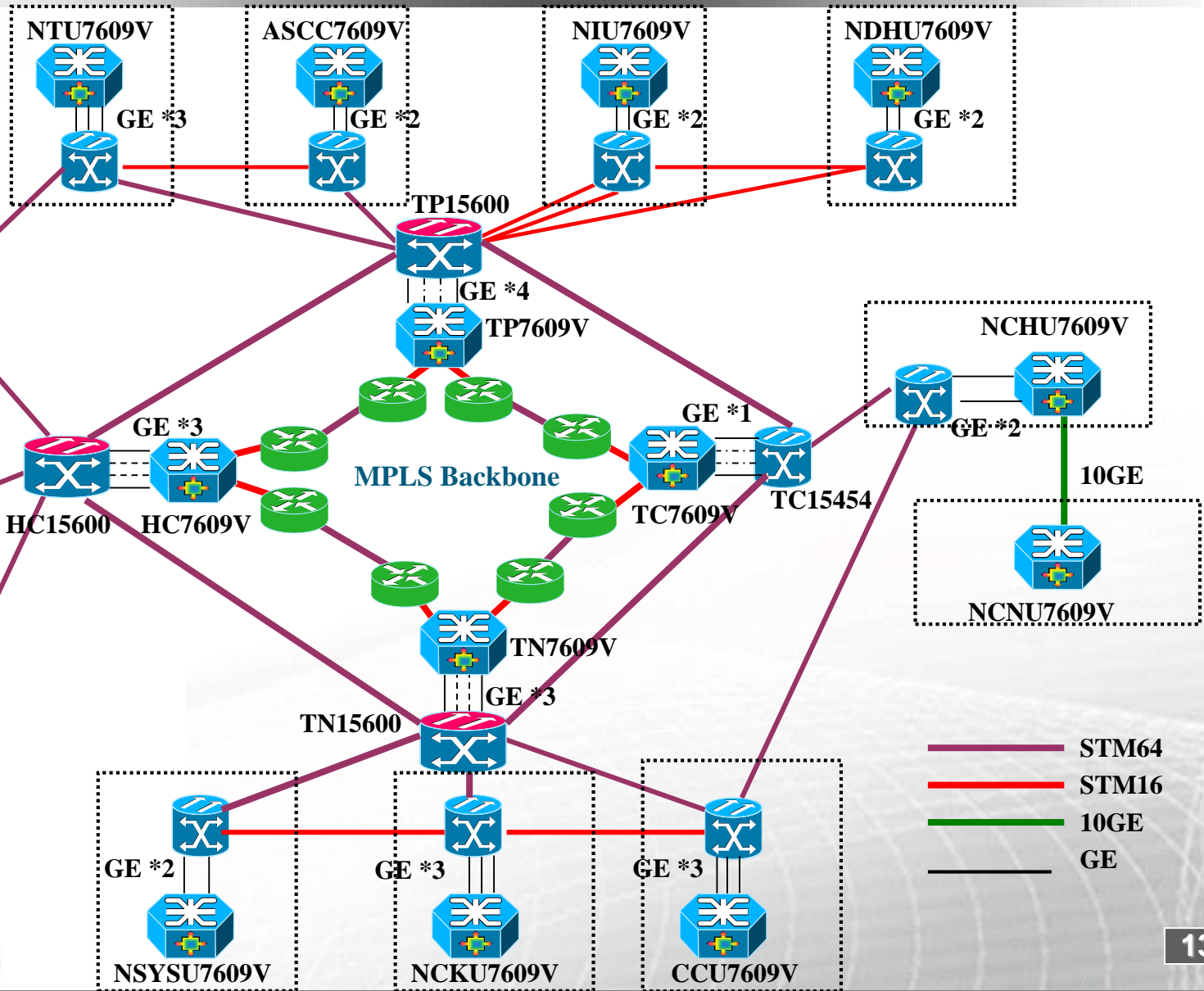
VPLS Physical Topology

7609V

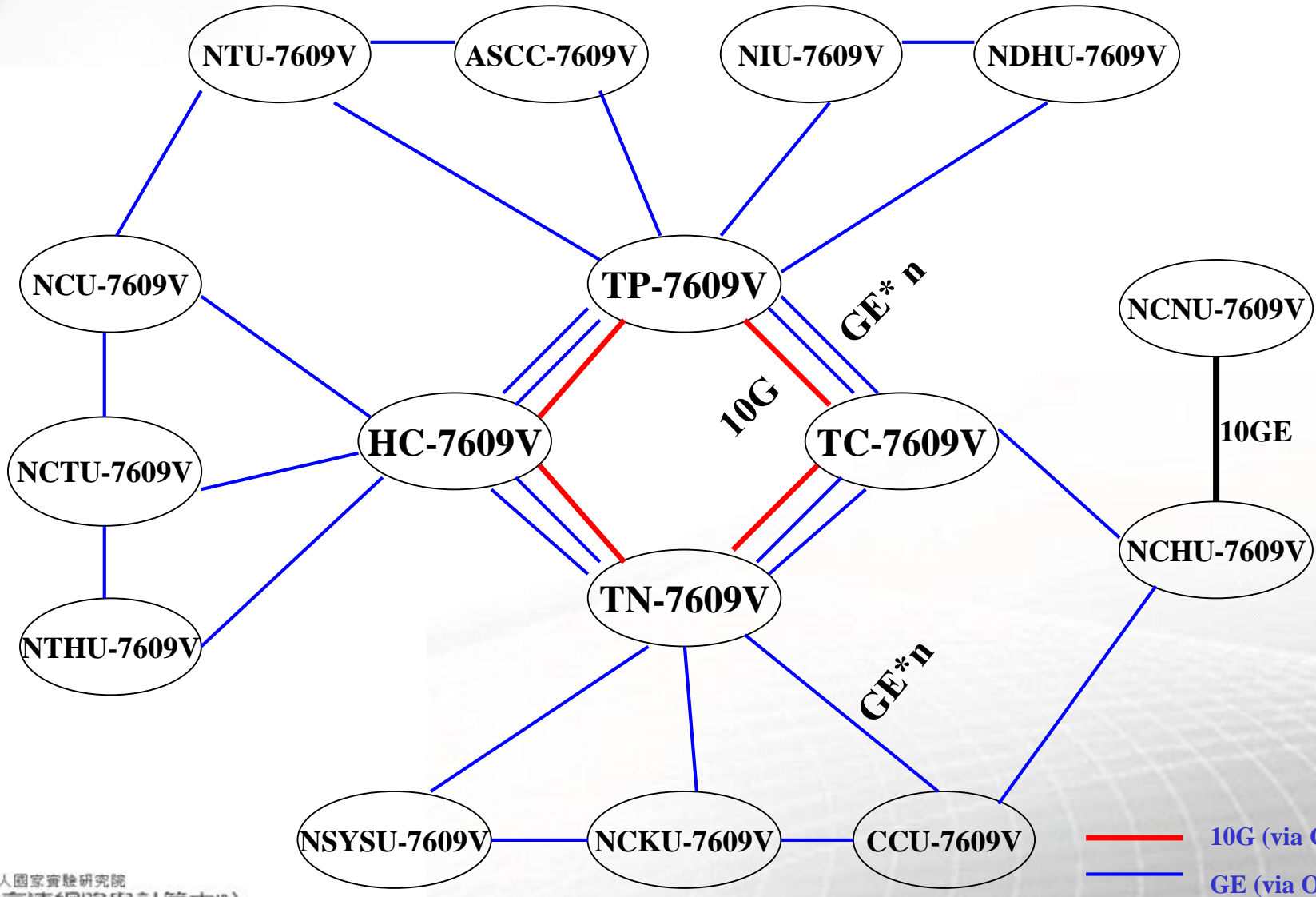
ONS15454

ONS15600

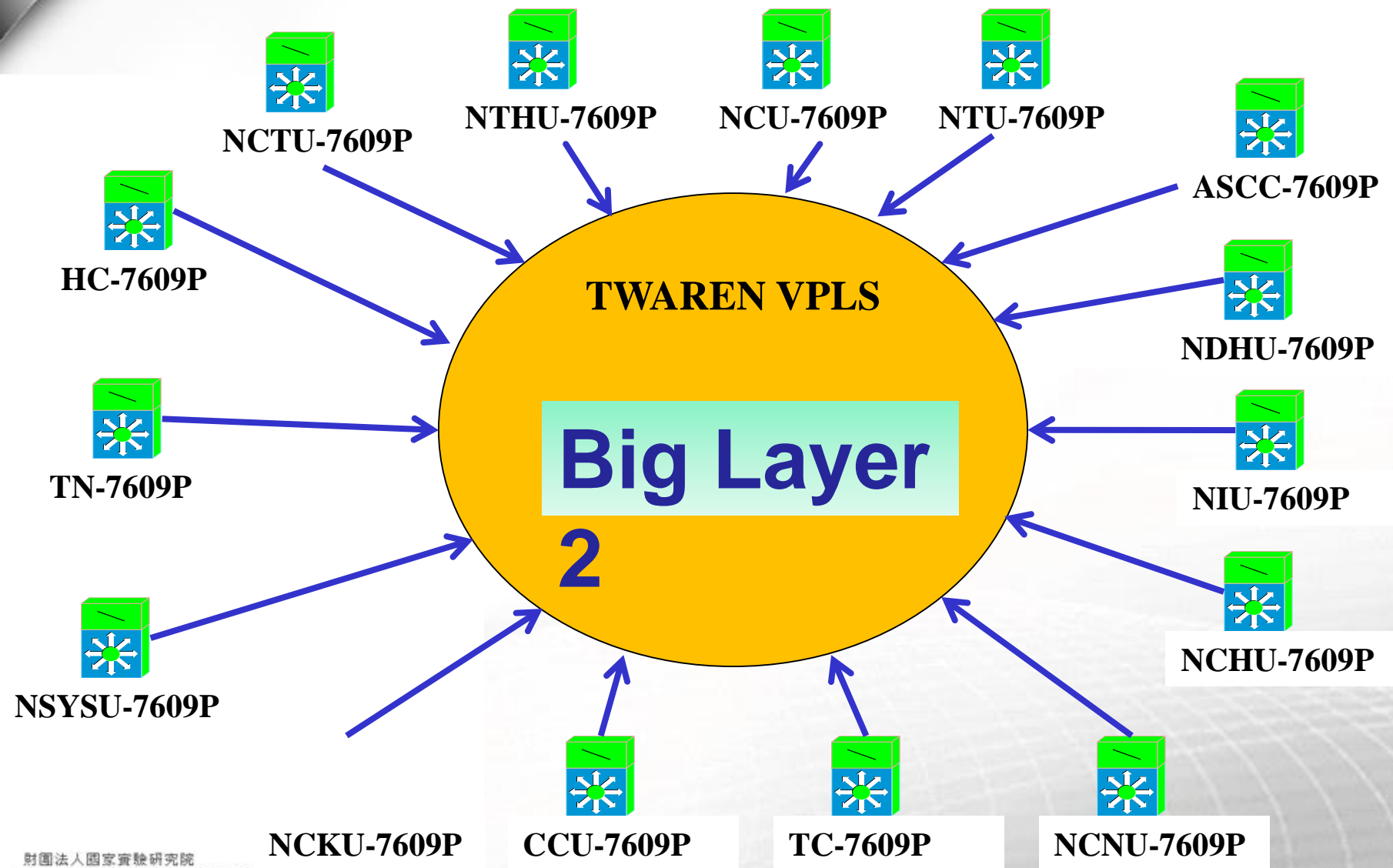
GSR12816



VPLS Logical Topology



TWAREN IP Layer Topology(2008.Q2)



TWAREN 新服務

- Multipoint to Multipoint Layer 2 VPN
 - 在一個網路平台上提供多個虛擬私有網路，
 - 讓跨地區的校園或辦公室網路連結模擬成在同一區域網路
 - 針對跨地區的合作計畫或測試平台可提供彈性VPN網路服務
- User-Based SSL VPN接取服務
 - 針對不同的帳號認證，提供不同的VPN 網路連結
 - 提供學研界使用者可於不在單位時，仍可透過VPN接取服務連回校園網路或工作單位使用內部資源。

多點Laye2 VPN與SSL-VPN使用時機

- 校本部與分校的校園網路連接
- 組織本部與分部的網路連接
- 醫院與醫院連結
- 建構測試網路平台
- 專屬網路建置(ex：防災網路、Native IPv6 網路)
- 出差時，連回校內讀取圖書資源(ex：電子期刊)
- 校園IP 不足時利用SSL-VPN 做IP 動態的分配
- ...

已申請服務之學校及研究單位

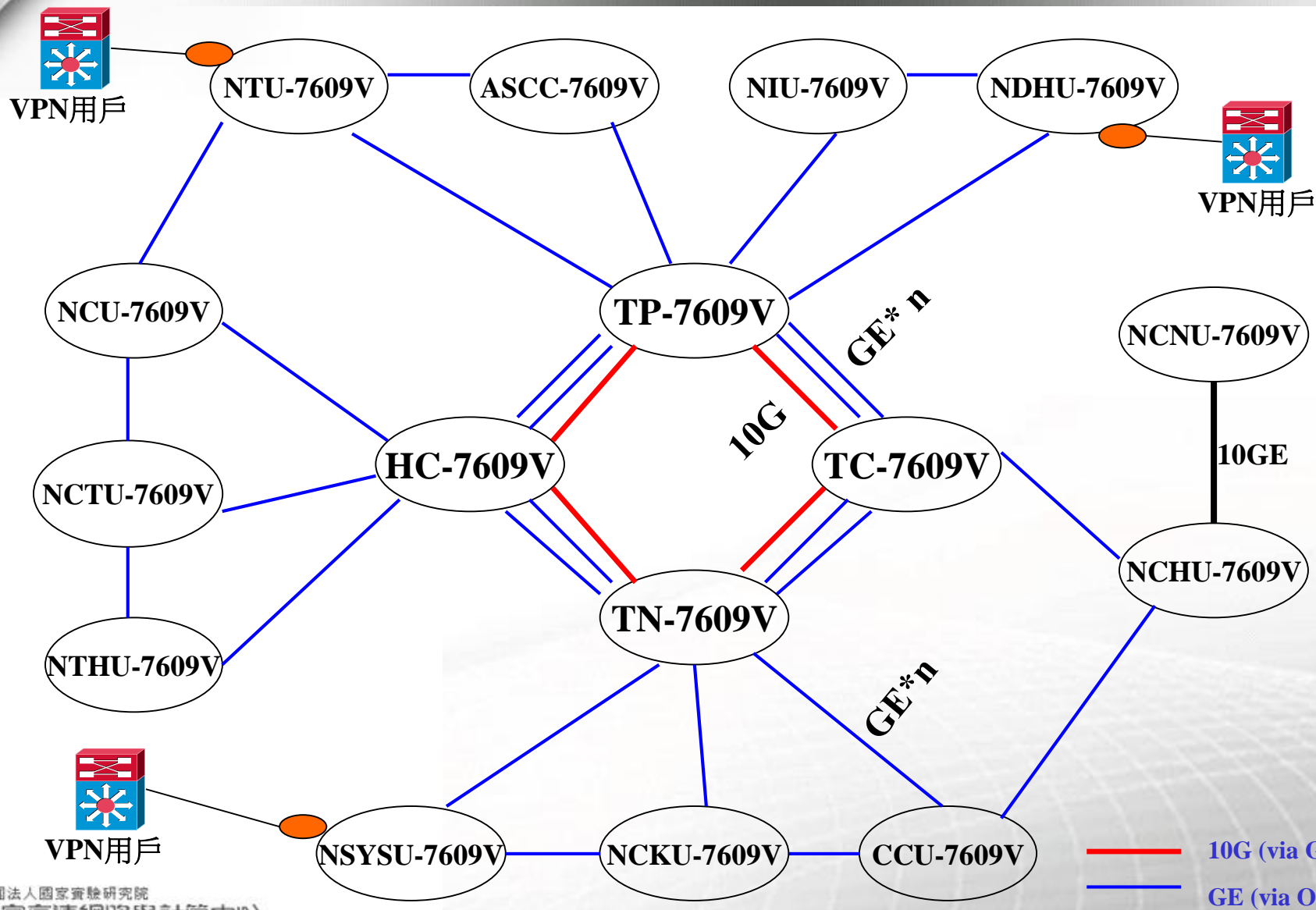
■ VPLS

- 國家衛生研究院內網連接
- 水利署災防網路建置
- 中山大學與中央研究院網路Peering
- 台大醫院與雲林分院網路介接
- 成大醫院與斗六分院網路介接
- 國網中心內網連線

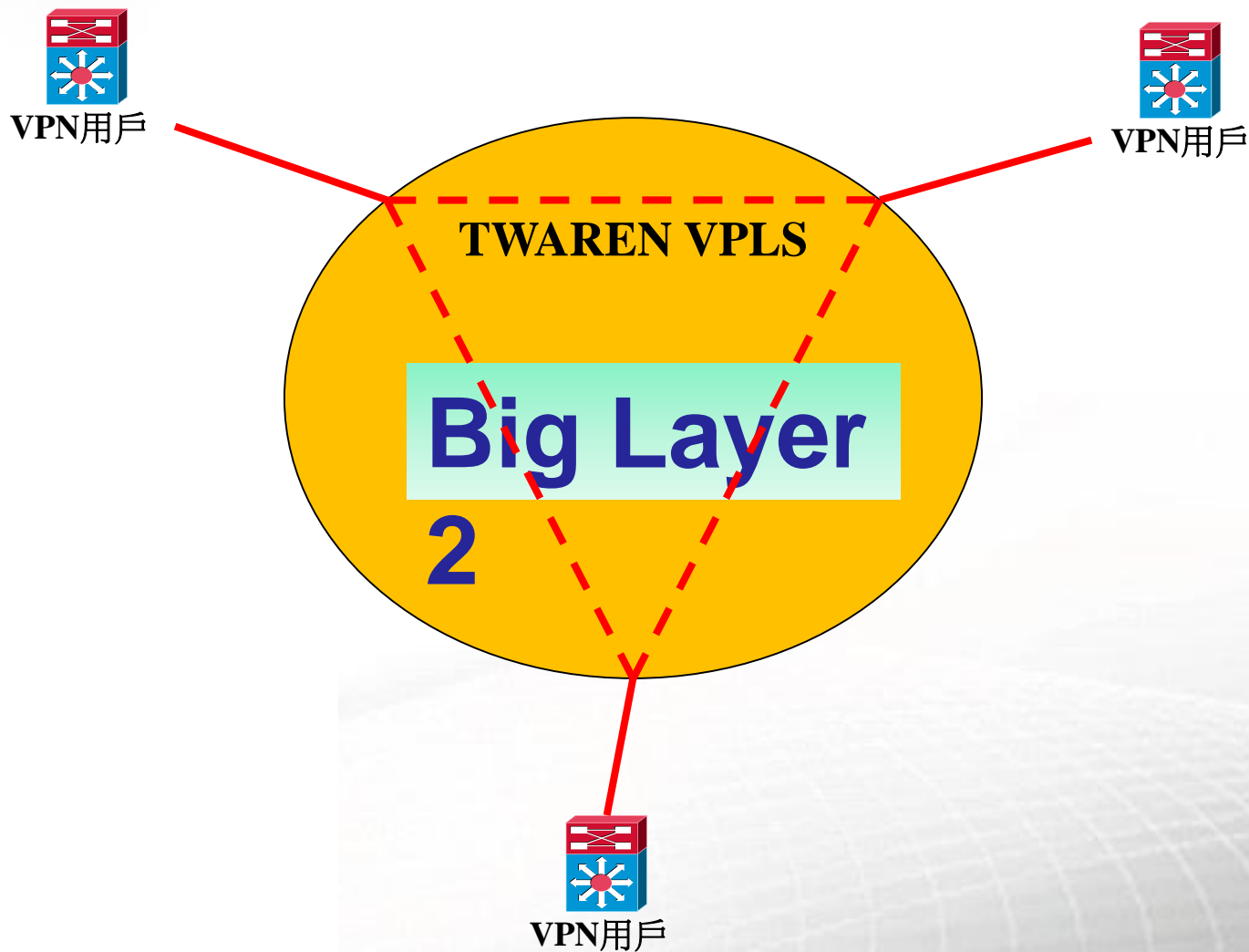
■ SSL-VPN

- 清華大學
- 東華大學
- 靜宜大學
- 國網中心
- 國家衛生研究院

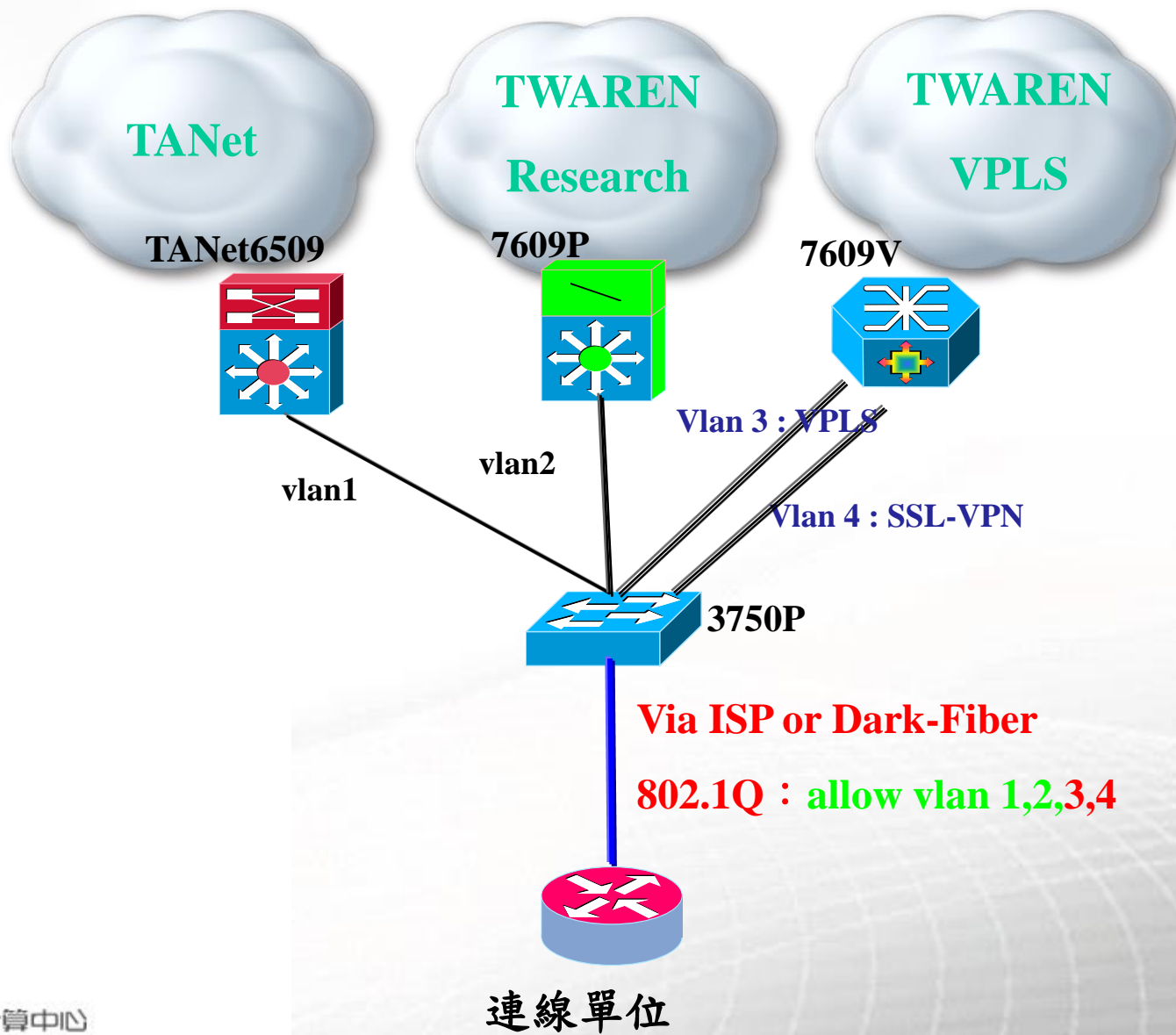
Gigapop使用VPLS服務 連線架構(實體架構)



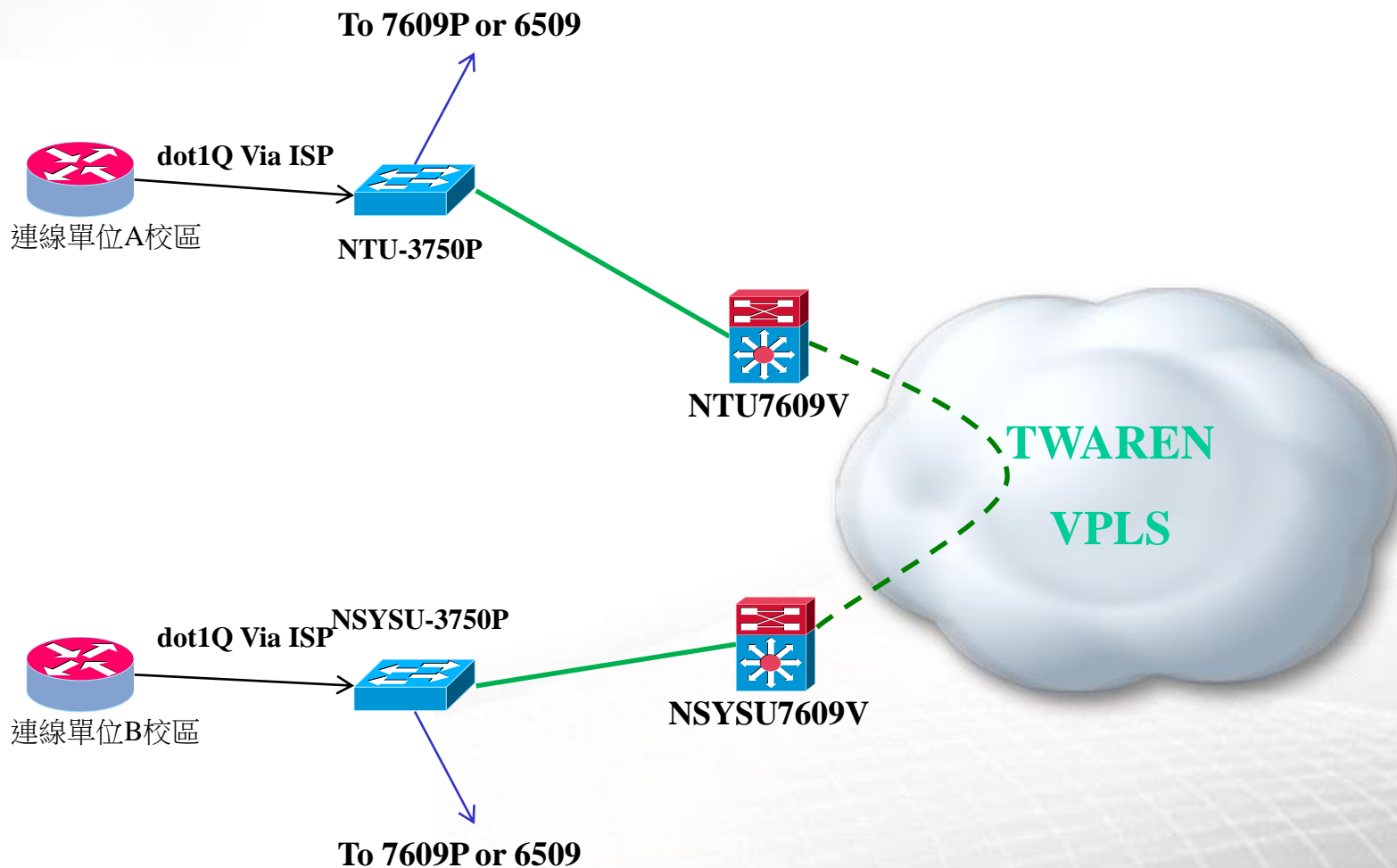
Gigapop使用VPLS服務 連線架構(邏輯架構)



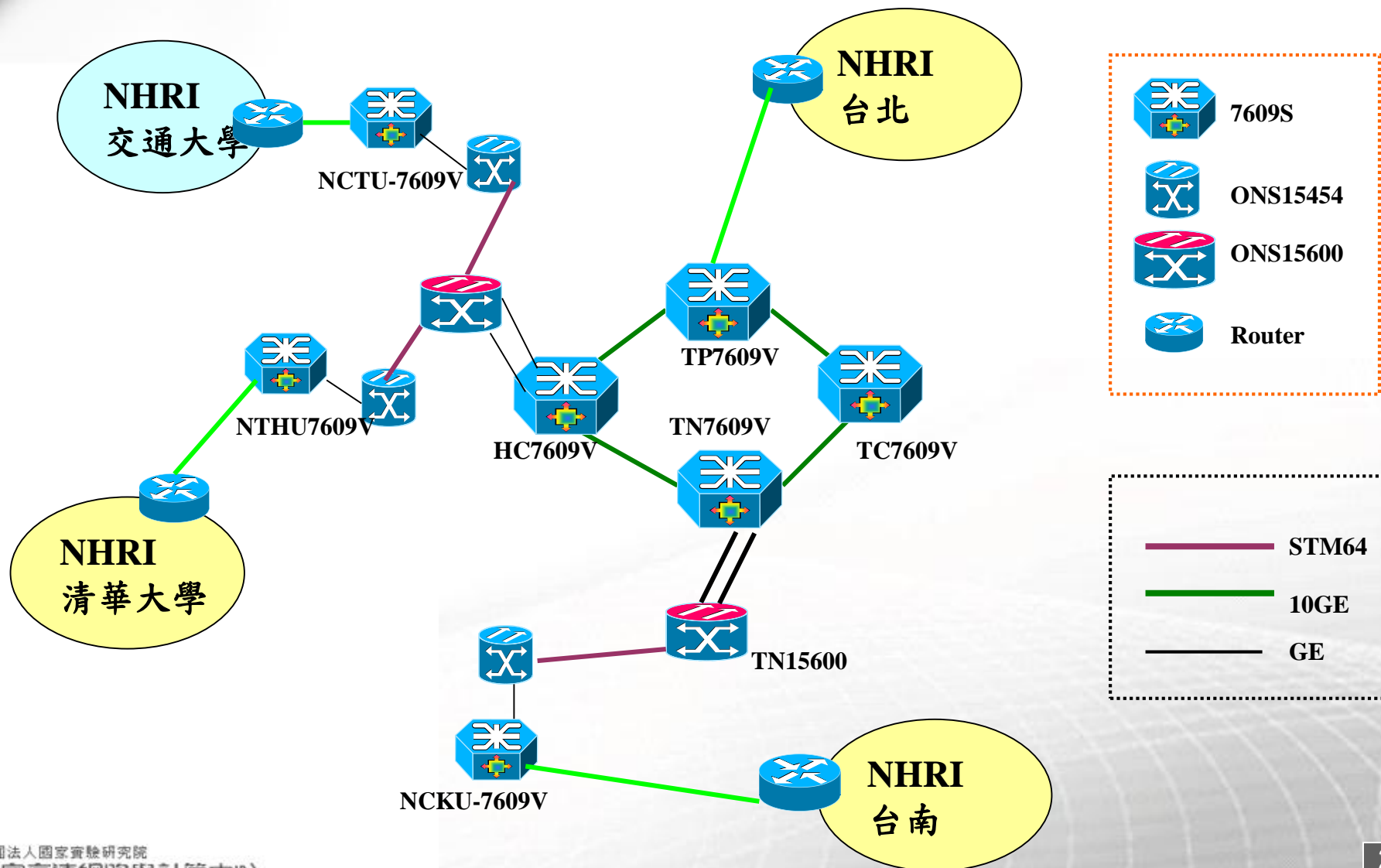
連線單位使用VPLS服務實體連線架構 1/2



連線單位使用VPLS服務實體連線架構 2/2



例：多點對多點連線：國衛院架構

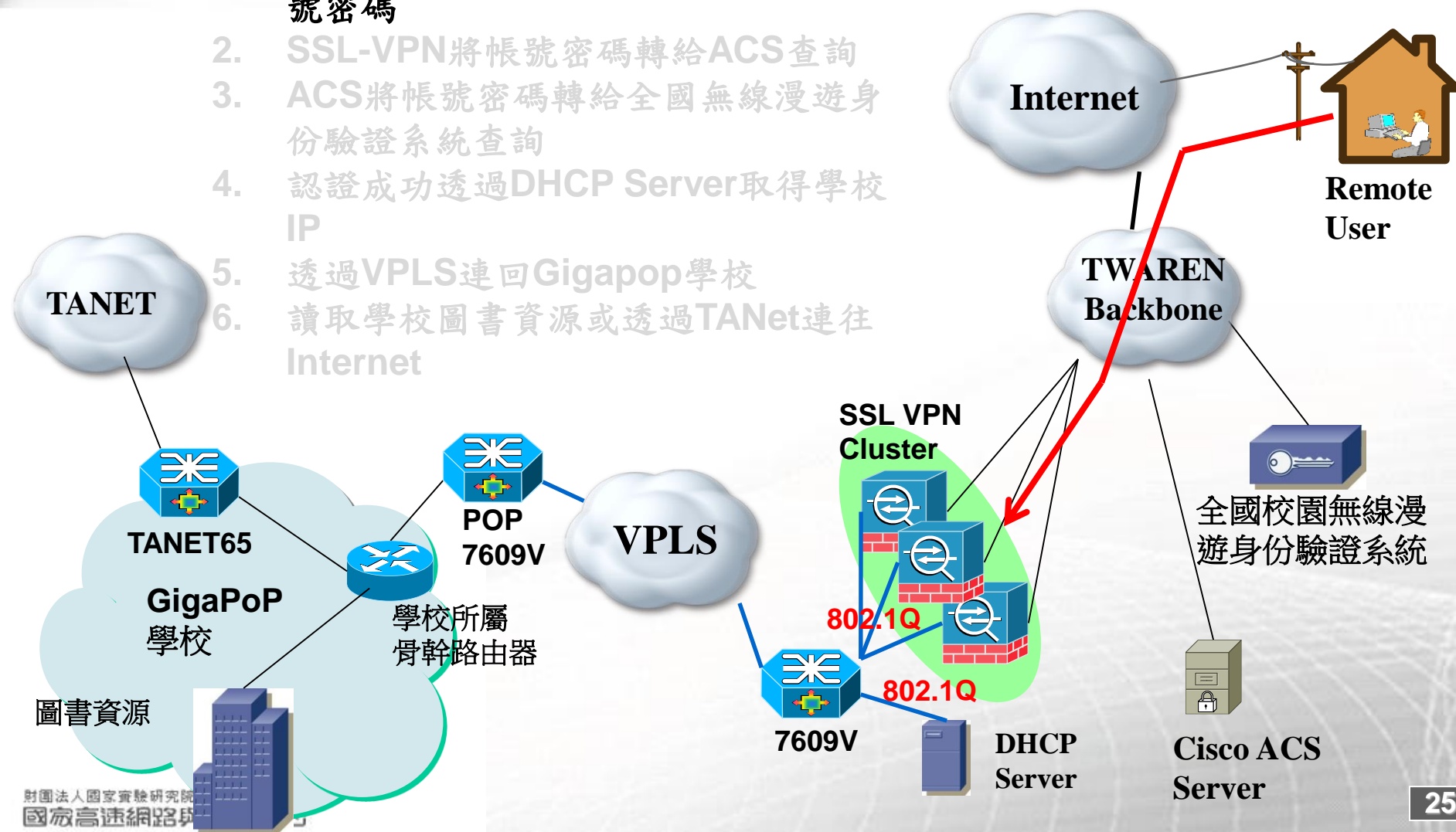




Gigapop使用SSL-VPN服務-1

GigaPoP學校使用者

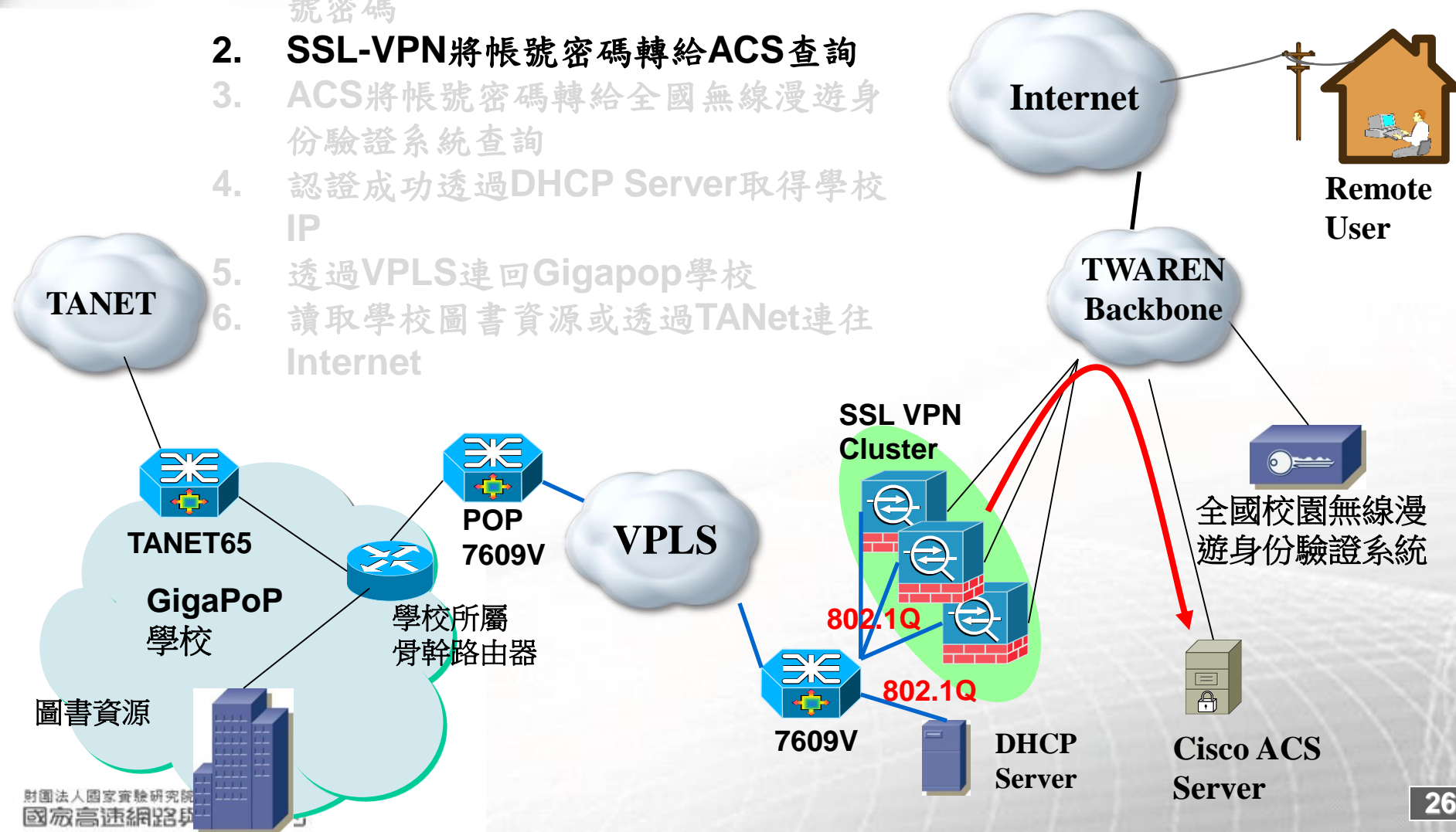
1. RemoteUser先連入SSL-VPN輸入帳號密碼
2. SSL-VPN將帳號密碼轉給ACS查詢
3. ACS將帳號密碼轉給全國無線漫遊身份驗證系統查詢
4. 認證成功透過DHCP Server取得學校IP
5. 透過VPLS連回Gigapop學校
6. 讀取學校圖書資源或透過TANet連往Internet



Gigapop使用SSL-VPN服務-2

GigaPoP學校使用者

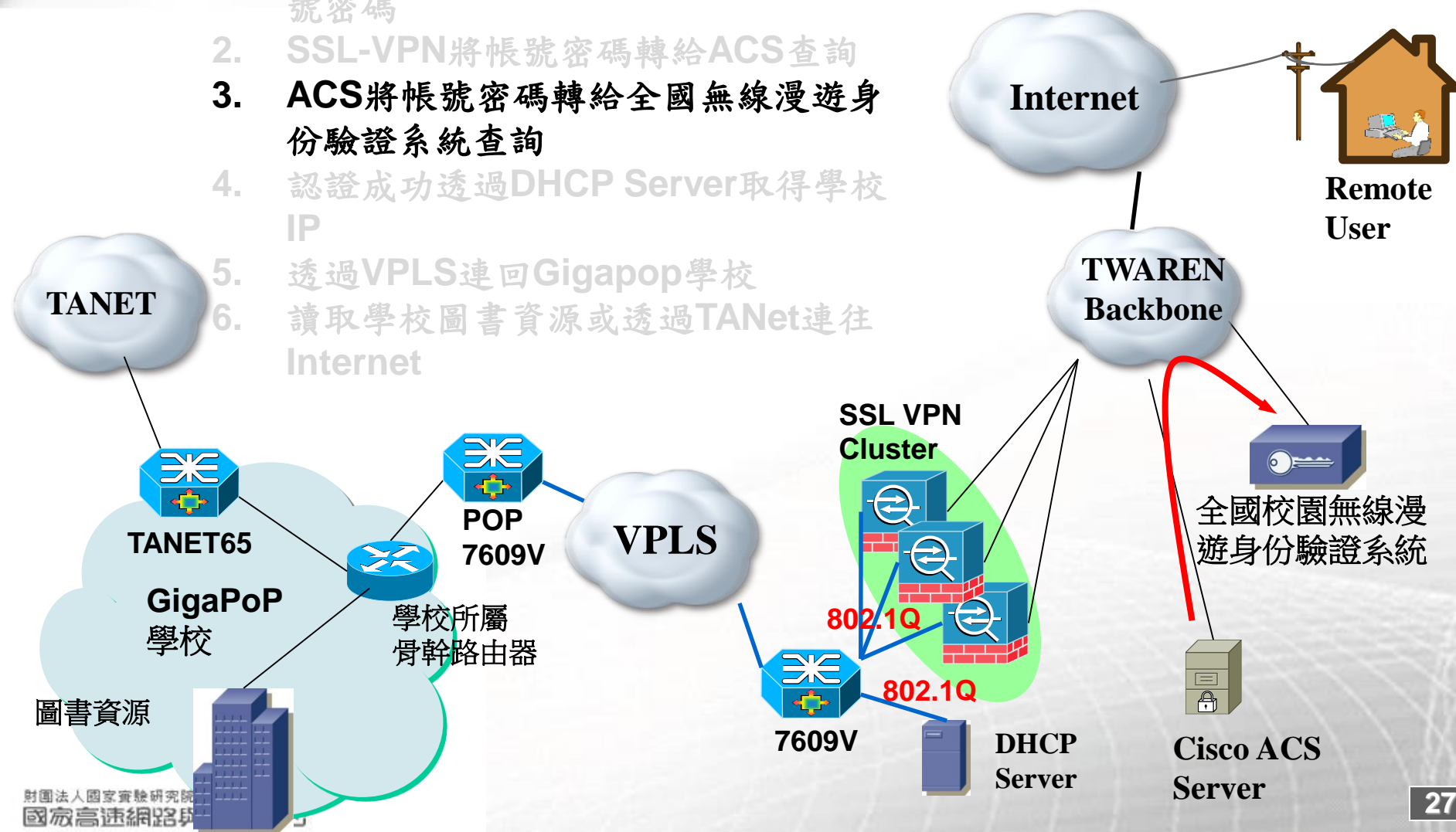
1. RemoteUser先連入SSL-VPN輸入帳號密碼
2. **SSL-VPN將帳號密碼轉給ACS查詢**
3. ACS將帳號密碼轉給全國無線漫遊身份驗證系統查詢
4. 認證成功透過DHCP Server取得學校IP
5. 透過VPLS連回Gigapop學校
6. 讀取學校圖書資源或透過TANet連往Internet



Gigapop使用SSL-VPN服務-3

GigaPoP學校使用者

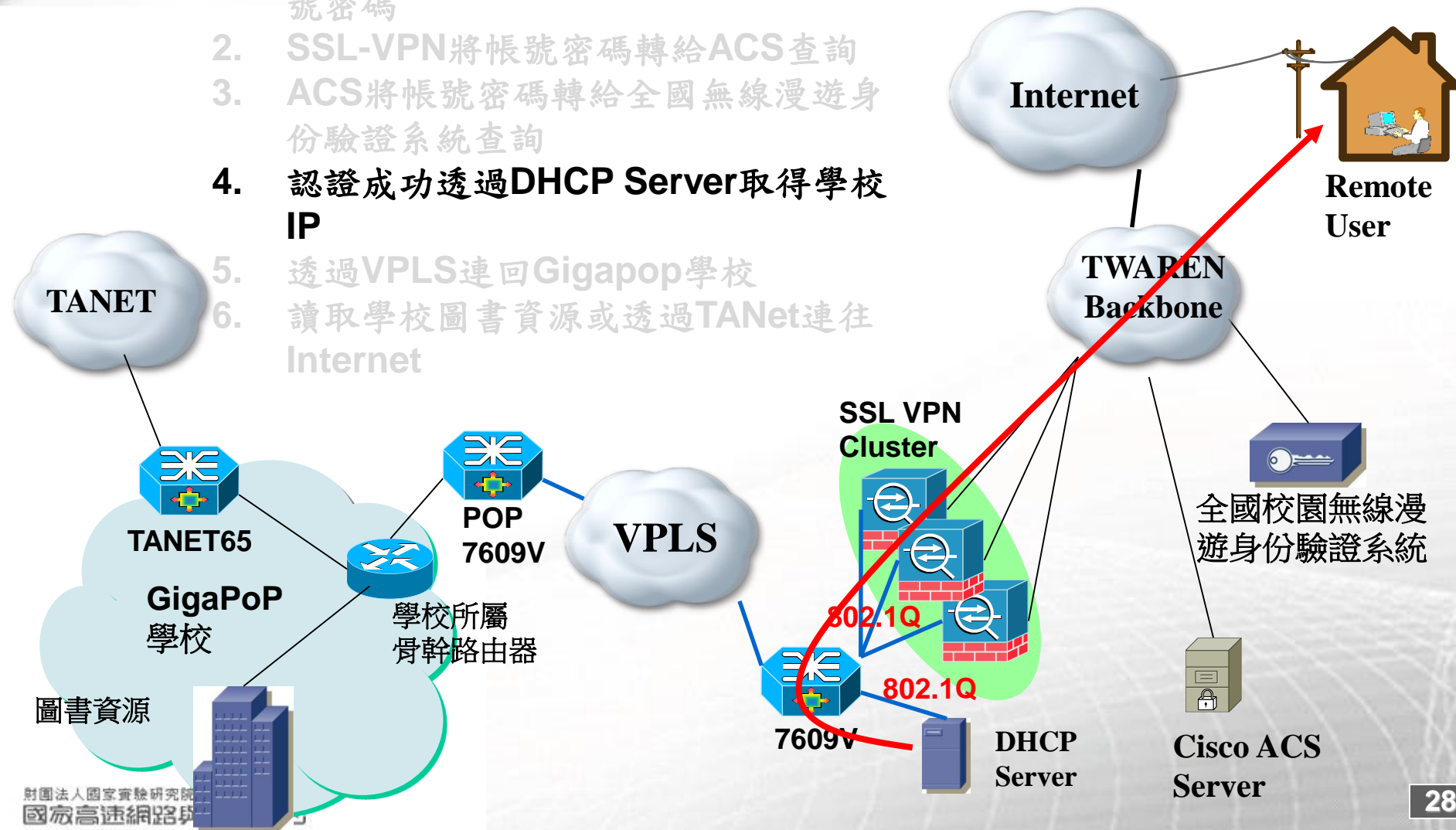
1. RemoteUser先連入SSL-VPN輸入帳號密碼
2. SSL-VPN將帳號密碼轉給ACS查詢
3. ACS將帳號密碼轉給全國無線漫遊身份驗證系統查詢
4. 認證成功透過DHCP Server取得學校IP
5. 透過VPLS連回Gigapop學校
6. 讀取學校圖書資源或透過TANet連往Internet



Gigapop使用SSL-VPN服務-4

GigaPoP學校使用者

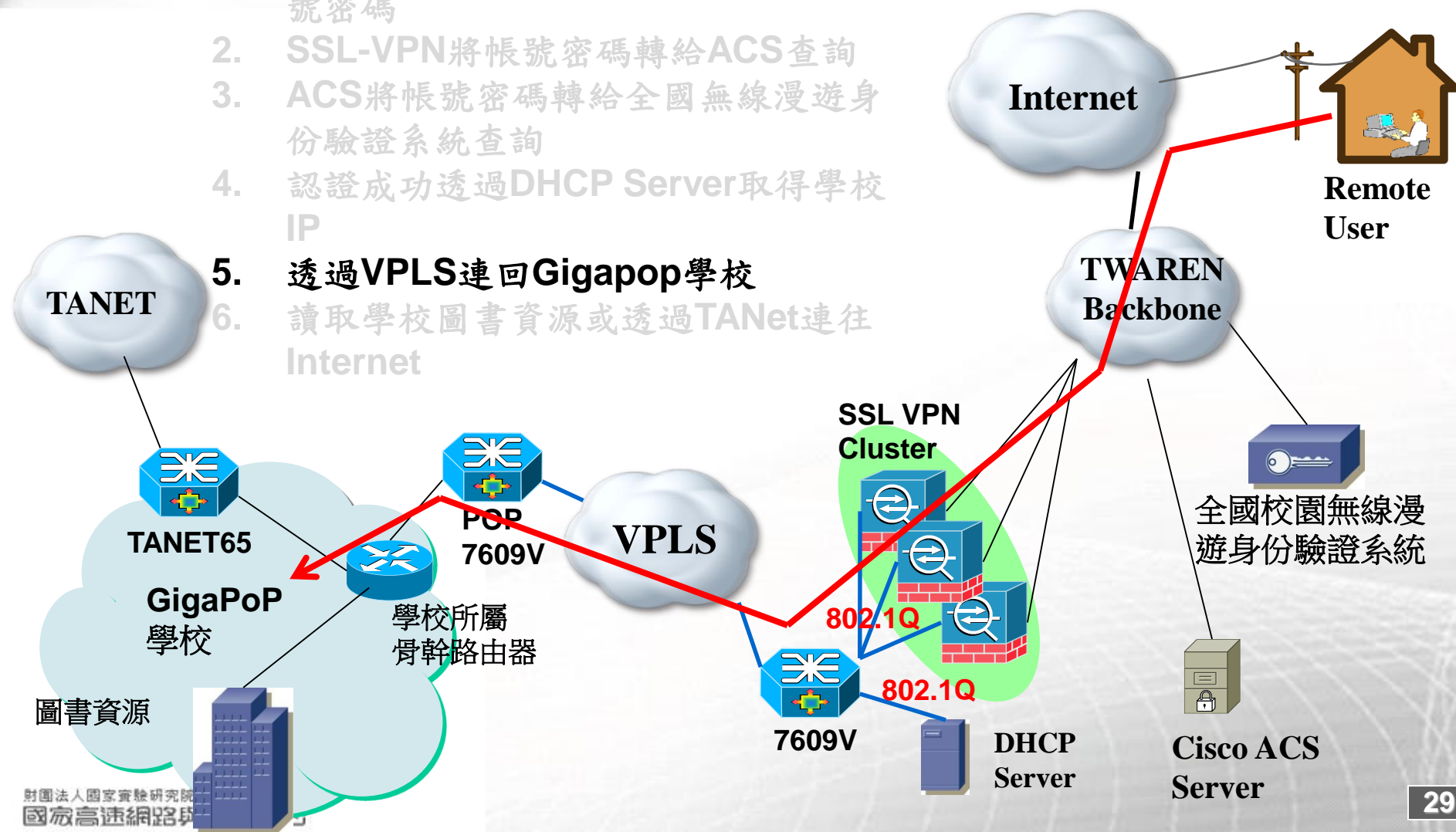
1. RemoteUser先連入SSL-VPN輸入帳號密碼
2. SSL-VPN將帳號密碼轉給ACS查詢
3. ACS將帳號密碼轉給全國無線漫遊身份驗證系統查詢
4. 認證成功透過DHCP Server取得學校IP
5. 透過VPLS連回Gigapop學校
6. 讀取學校圖書資源或透過TANet連往Internet



Gigapop使用SSL-VPN服務-5

GigaPoP學校使用者

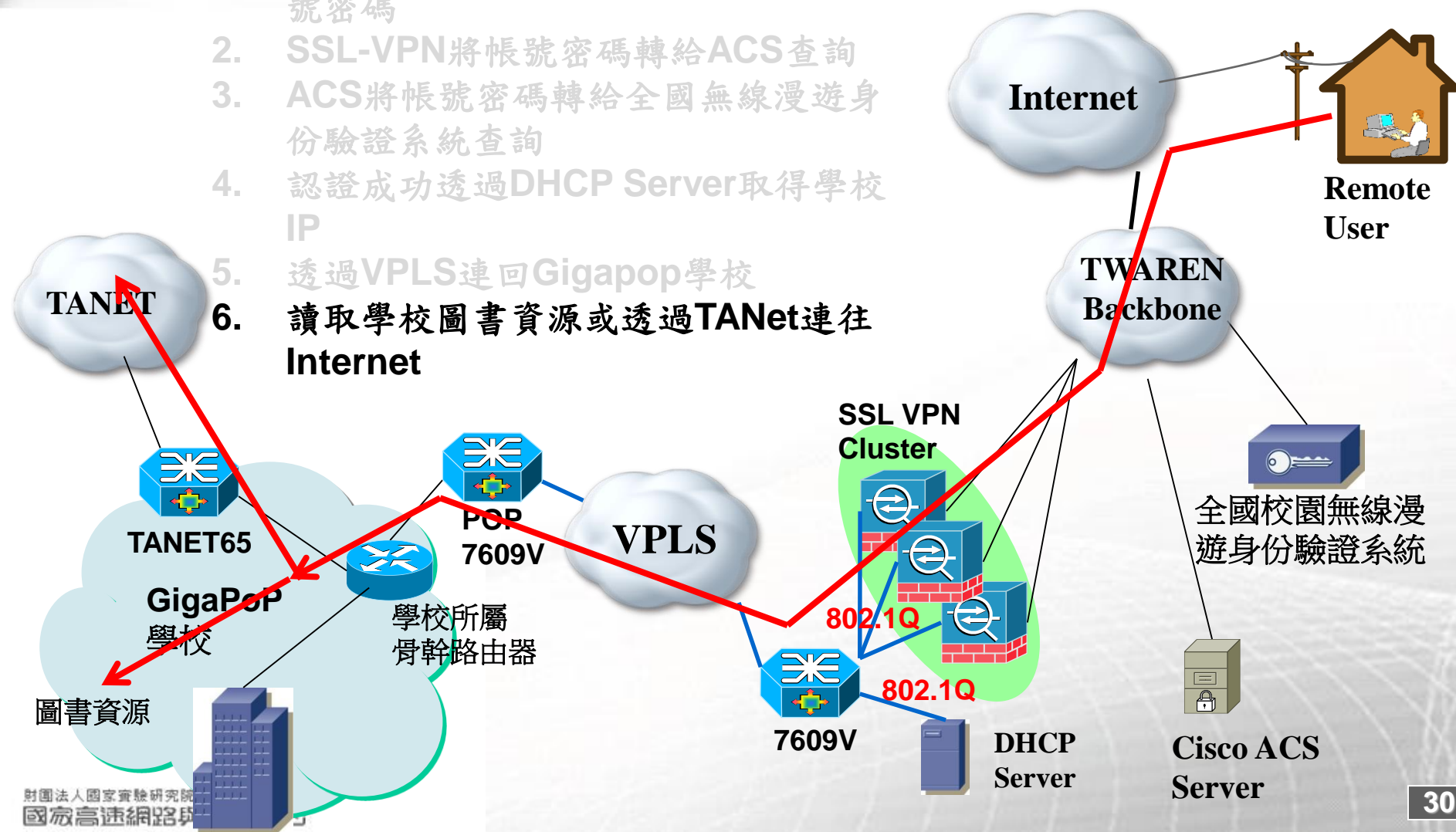
1. RemoteUser先連入SSL-VPN輸入帳號密碼
2. SSL-VPN將帳號密碼轉給ACS查詢
3. ACS將帳號密碼轉給全國無線漫遊身份驗證系統查詢
4. 認證成功透過DHCP Server取得學校IP
5. 透過VPLS連回Gigapop學校
6. 讀取學校圖書資源或透過TANet連往Internet



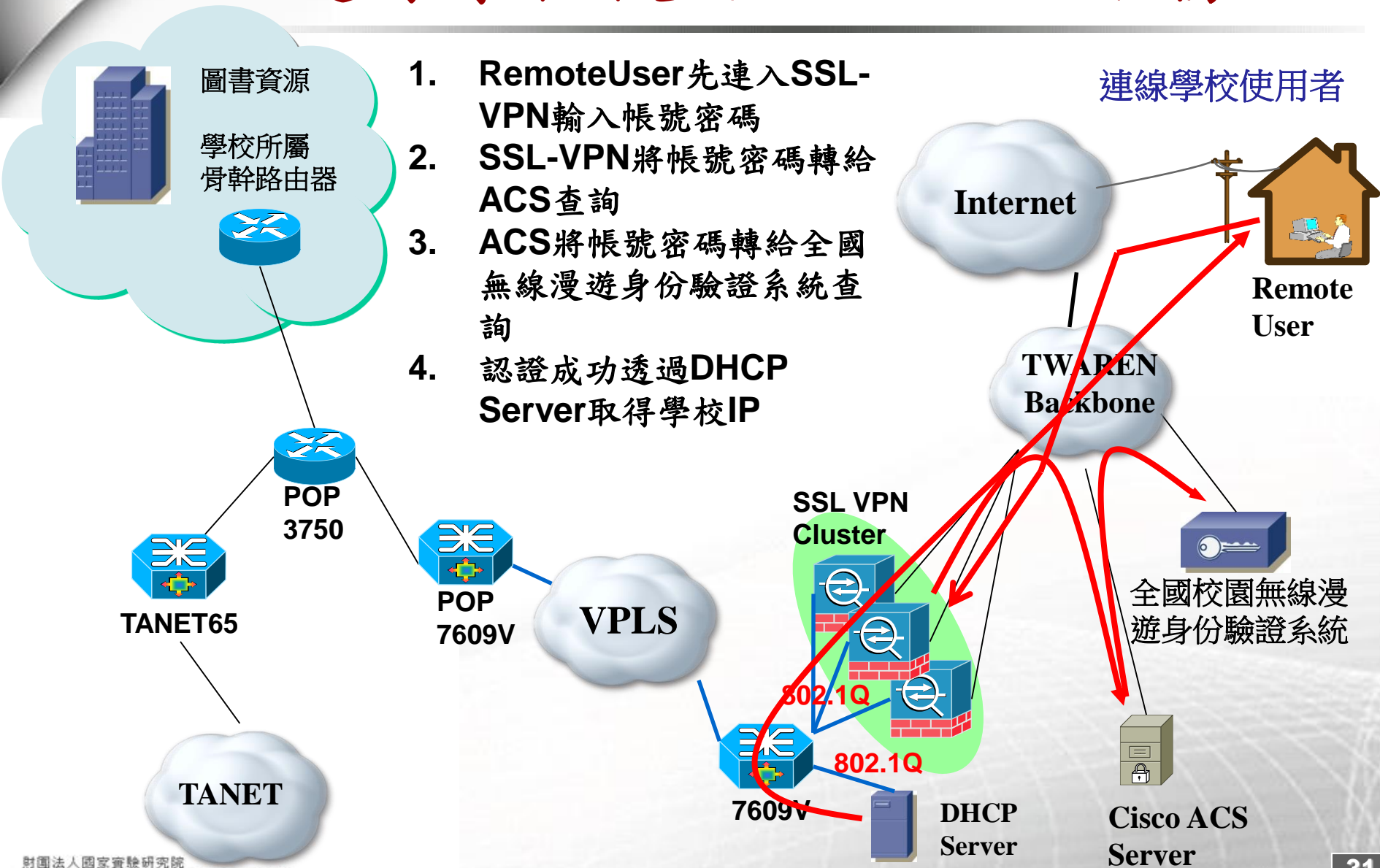
Gigapop使用SSL-VPN服務-6

GigaPoP學校使用者

1. RemoteUser先連入SSL-VPN輸入帳號密碼
2. SSL-VPN將帳號密碼轉給ACS查詢
3. ACS將帳號密碼轉給全國無線漫遊身份驗證系統查詢
4. 認證成功透過DHCP Server取得學校IP
5. 透過VPLS連回Gigapop學校
6. 讀取學校圖書資源或透過TANet連往Internet



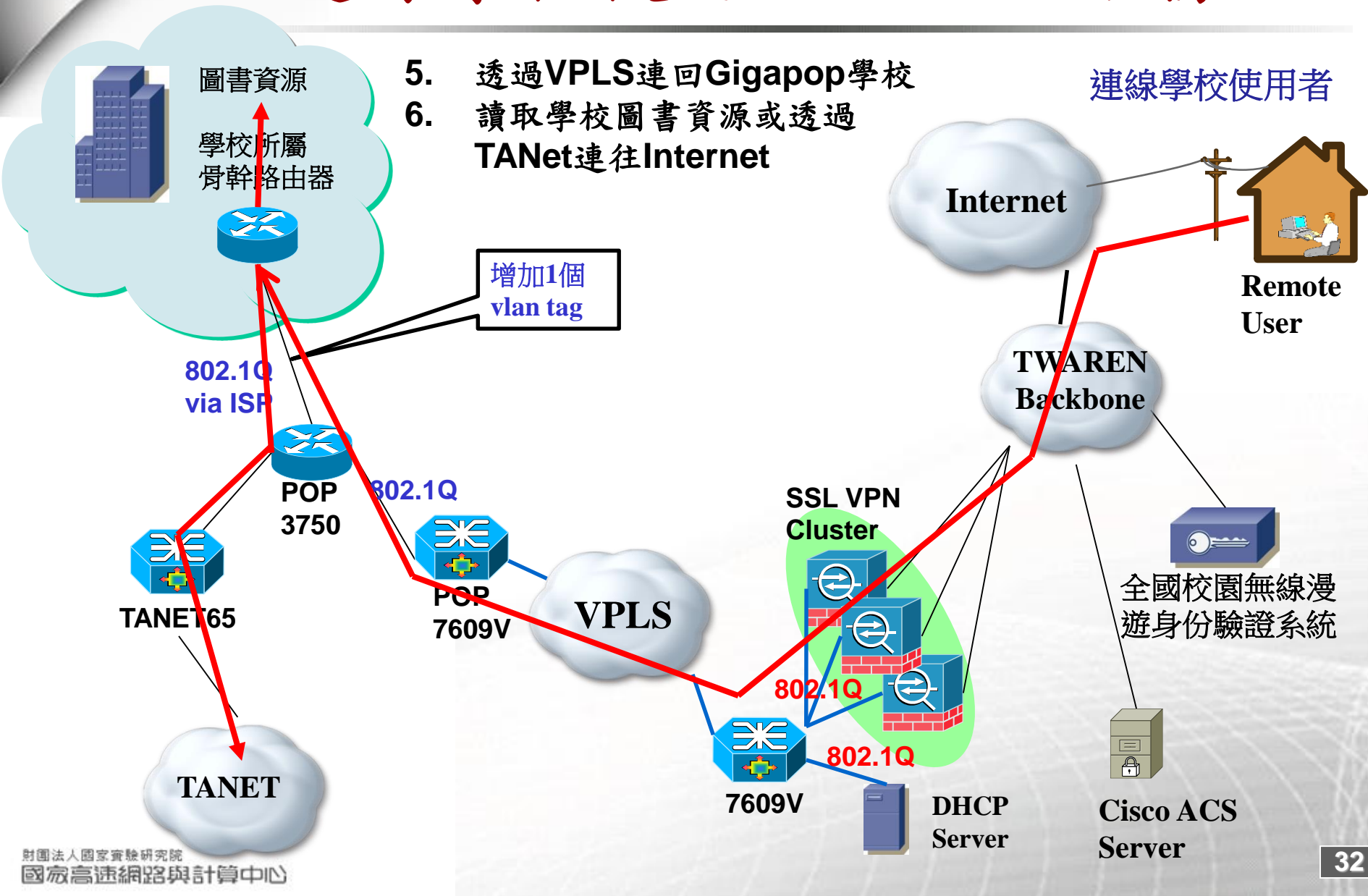
連線學校使用SSL-VPN服務-1



連線學校使用SSL-VPN服務-2

5. 透過VPLS連回Gigapop學校
6. 讀取學校圖書資源或透過TANet連往Internet

連線學校使用者

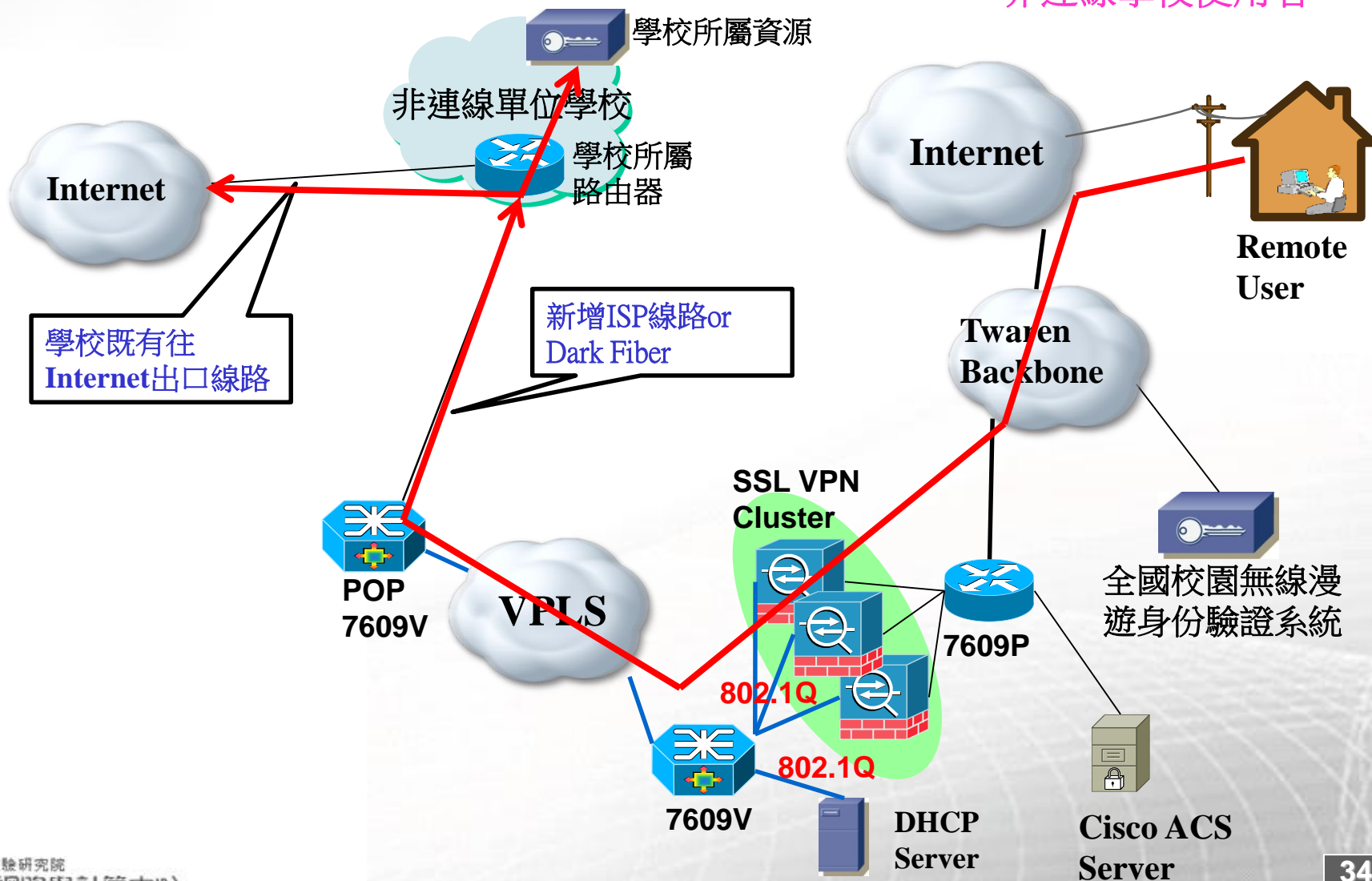


非連線單位學校使用SSL-VPN服務-1

- 已接入各Gigapop機房的學校，使用TANet或TWAREN服務者
 - 透過放置於各Gigapop機房的Cisco 3750P進行VLAN分流
- 尚未接入Gigapop機房的學校
 - 可新增一條專線(ISP線路或Dark Fiber)進入各Gigapop機房，再連入VPLS網路
 - 新增的專線，也可申請使用TWAREN連線服務，或其他TWAREN增值應用，所有服務，皆可放置於各Gigapop機房的Cisco 3750P進行VLAN分流

非連線單位學校使用SSL-VPN服務-2

非連線學校使用者



學校使用SSL VPN準備工作

學校需準備...	國網對應工作
1 IP pool範圍	設定於DHCP server
2 學校內部所有網段Prefix	將該校routing設定於ASA
3 線路調整或新增連線至VPLS骨幹 (連線學校:既有連接於PoP3750線路增加第三個vlan id) (非連線學校需新增線路連接PoP7609V)	➡ 設定學校所屬VPLS vlan id ➡ 調整PoP3750及PoP7609V之vlan id ➡ 連接學校線路於PoP7609V
4 是否加入校園無線漫遊認證機制 是否	➡ 新增該校的Group於ACS ➡ ASA直接與該校認證伺服器進行認證
5 學校規劃該校SSL登入Portal	將該校Portal內容設定於ASA
6 SSL Client透過學校出Internet是否需進行NAT，若需要請將IP pool於出口路由器或防火牆設定NAT	

歡迎大家踴躍使用VPLS與 SSL-VPN服務

Thanks

<http://www.nchc.org.tw>

<http://www.twaren.net>

<http://noc.twaren.net>