國立臺灣師範大學

雲端建置與各校區網路架構分享

台師大資訊中心
網路系統組
陳昱甫 Blue Chen
Certified Ethical Hacker (C|EH) #ECC944645
ISO27001 ISMS LA #042307
BS10012 PIMS LA #886-1-10111
服務專線：02-7734-3734
TANet 網路電話：9766-3734
E-mail：blue@ntnu.edu.tw

2018/5/2

大綱

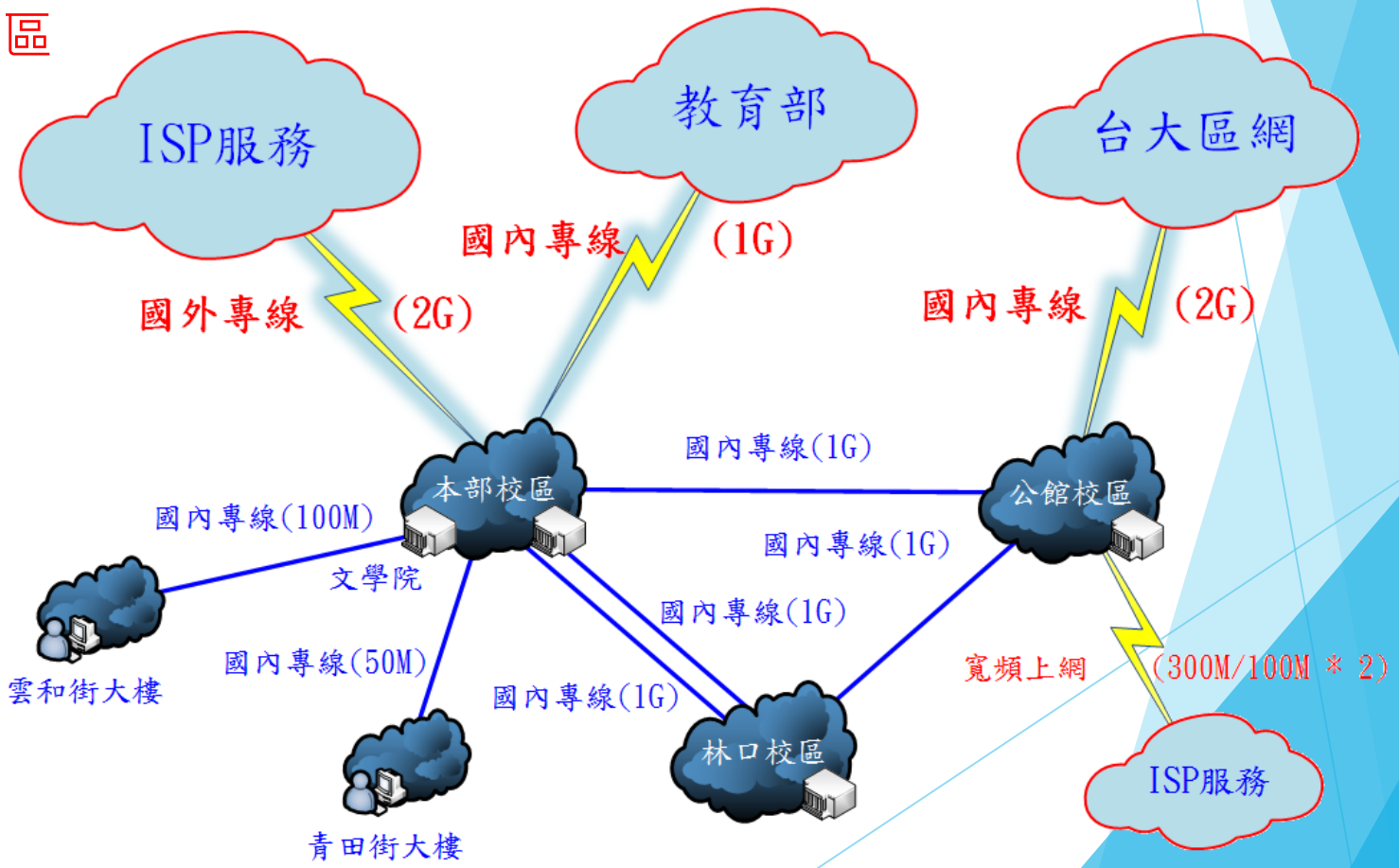
一、台師大雲端機房建置與備援機制：使用 Cisco OTV 技術分享

二、台師大不同校區(校本部、林口、公館)之網路架構與備援機制

雲端機房建置與備援機制：使用 Cisco OTV 技術分享

建置背景：跨校區使用相同網段及資源

- 既有核心設備 Cisco 6509 已停止所有軟硬體支援，對外連線中斷風險大幅提升
- 現狀網路無法支援10G/FCoE/DR，欠缺虛擬化資料中心所需相關網路技術
- 校園子網段能跨越多個校區，簡化網段的分配
- 虛擬化伺服器需二層網路透通，才能做到高度 HA



雲端機房建置與備援機制：使用 Cisco OTV 技術分享

Overlay Transport Virtualization (OTV)

OTV LAN Extensions

OTV delivers a virtual L2 transport

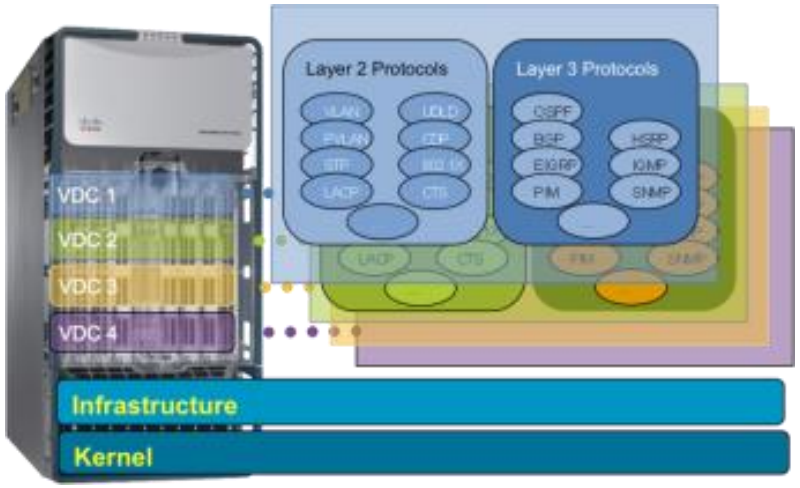
O — ***Overlay*** - A solution that is *independent of the infrastructure technology* and services, flexible over various inter-connect facilities

T — ***Transport*** - Transporting services for *layer 2 and layer 3* Ethernet and IP traffic

V — ***Virtualization*** - Provides *virtual* connections, *connections* that are in turn *virtualized and partitioned* into VPNs, VRFs, VLANs

雲端機房建置與備援機制：使用 Cisco OTV 技術分享

Virtual Device Contexts (VDC)



一. 網路設備整併

網路設備垂直或水平整併

減少實體設備數目

二. 彈性的調整與分配資源

依需求分配不同的硬體資源與介面模組給予每個VDC

三. 提供另一種網路實體隔離方案

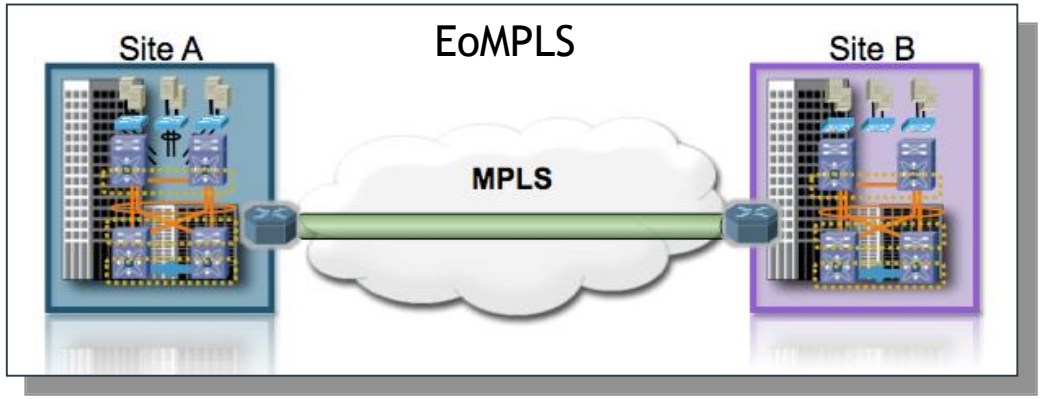
每個VDC可以獨立開關機，不同的管理設定與管理權限，需要實體線路相連才能互通，如同兩部實體網路交換器

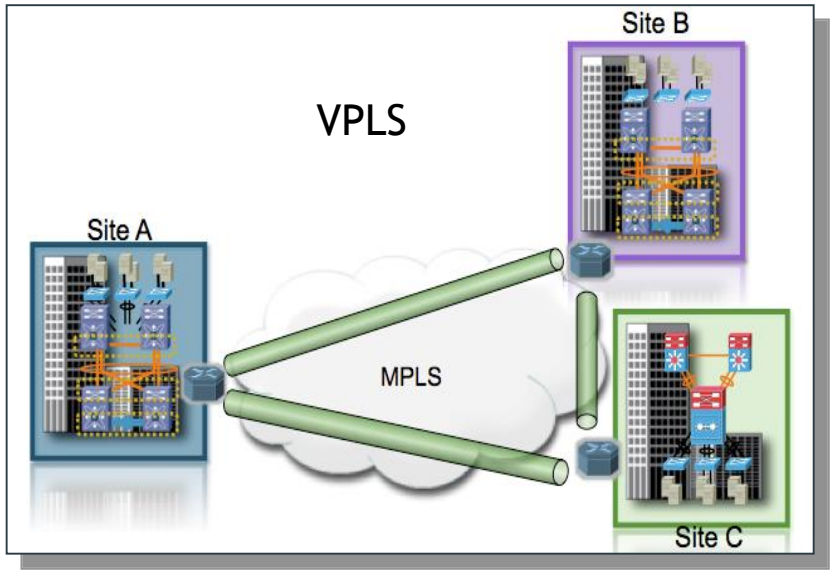
雲端機房建置與備援機制：使用 Cisco OTV 技術分享

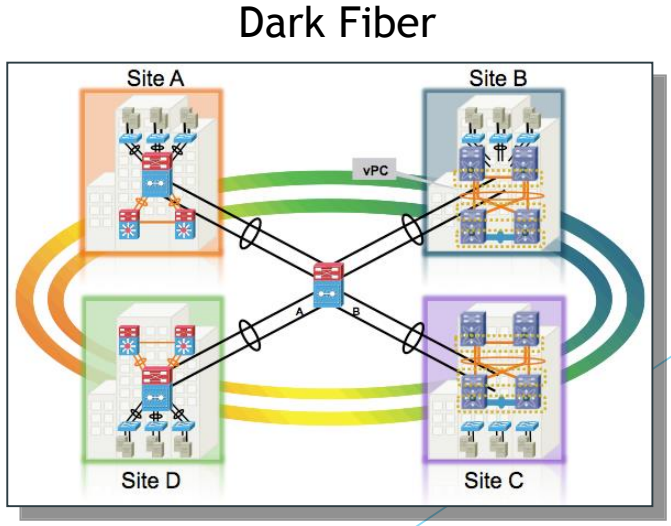
資料中心第二層互連技術

第二層互連技術可使兩地資源整合成單一資源池，任意調配資源

前提是必須建立一**高效能 Layer2 透通網路！**







雲端機房建置與備援機制：使用 Cisco OTV 技術分享

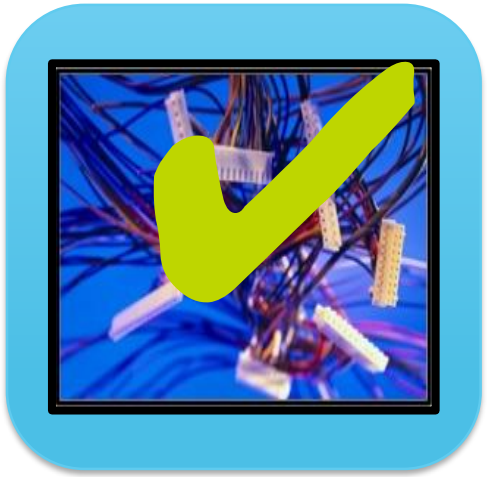
一般第二層互連技術常見問題

Flooding Behavior

- Unknown Unicast for MAC propagation
- Unicast Flooding reaches all sites

Control-Plane Based Learning

Pseudo-wire Maintenance



- Full mesh of Pseudo-wire is complex
- Head-End replication is a common problem

Dynamic Encapsulation

Multi-Homing

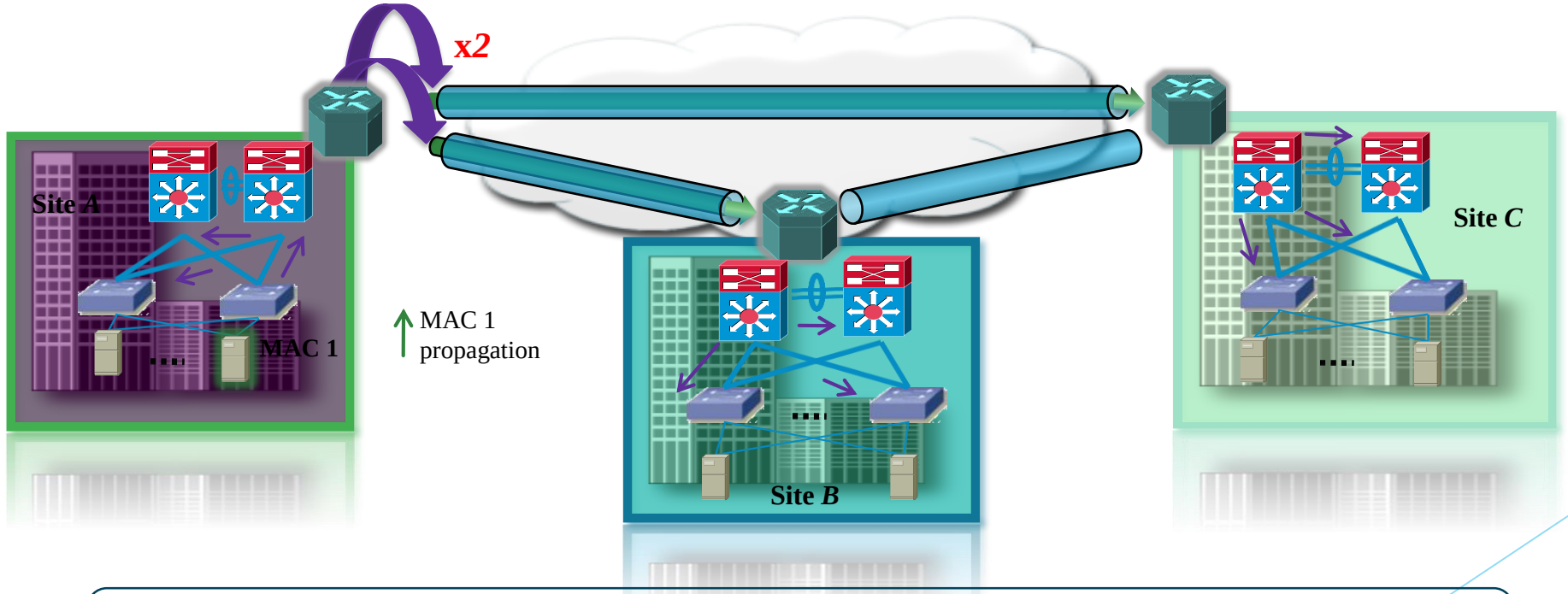
- Requires additional Protocols & extends STP
- Malfunctions impacts multiple sites

Native Automated Multi-Homing

雲端機房建置與備援機制：使用 Cisco OTV 技術分享

Layer 2 VPN 的 “Flooding 特性”

- Traditional Layer 2 VPN technologies rely on flooding to propagate MAC reachability.
- The flooding behavior causes failures to propagate to every site in the L2-VPN.

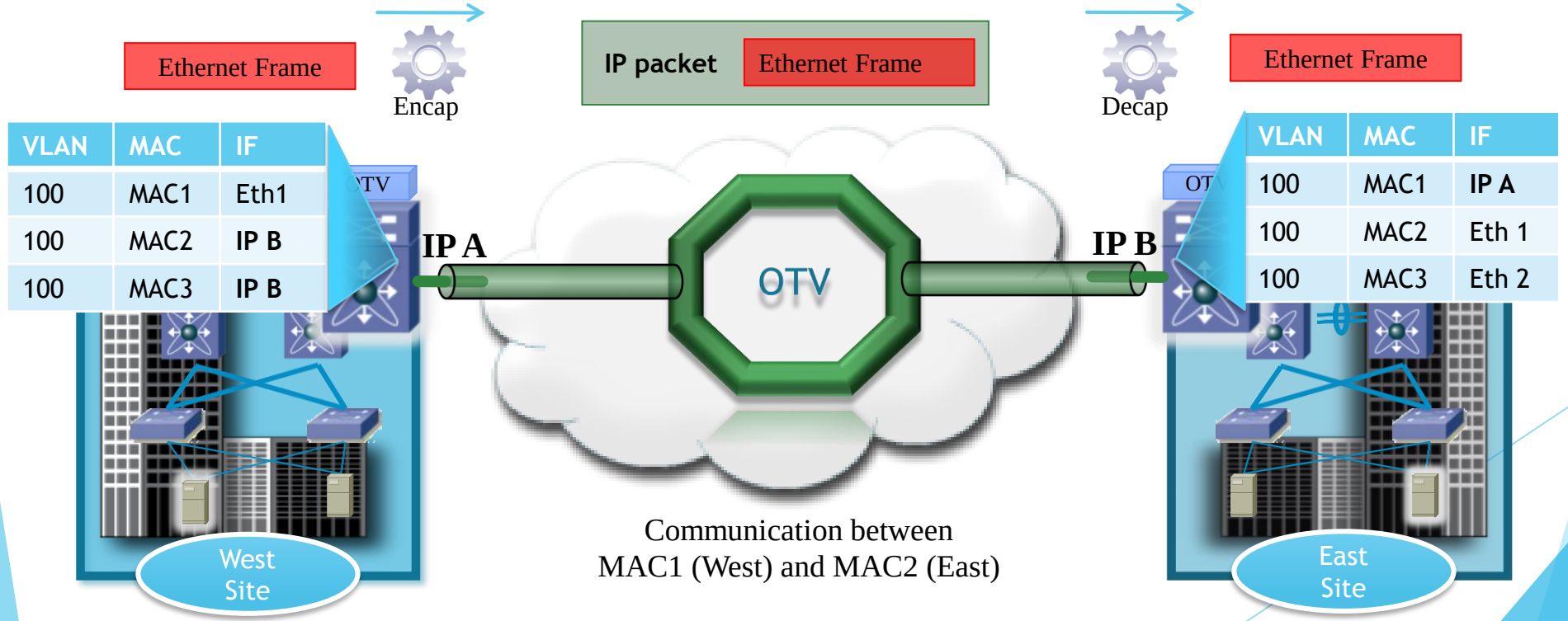


- A solution that provides layer 2 connectivity, yet restricts the reach of the flood domain is necessary in order to contain failures and preserve the resiliency.

雲端機房建置與備援機制：使用 Cisco OTV 技術分享

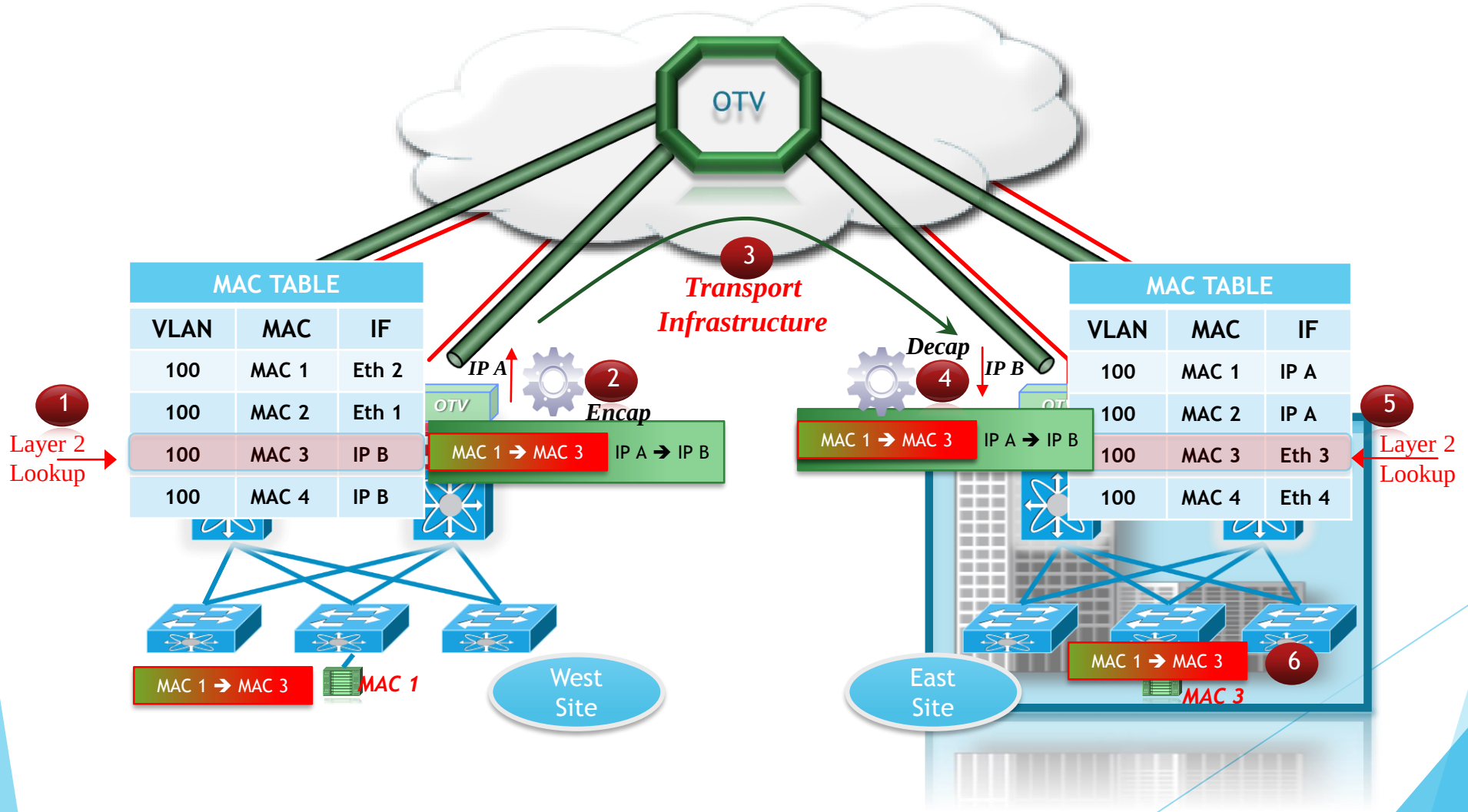
解決之道 : OTV

- “MAC in IP”
- 根據 MAC routing table 動態打包 MAC
- 所以不需要虛擬線路(Pseudo-Wire) 的建立及維護
- OTV技術原理是把Ethernet Frame再一次封裝進IP Packet中，然後才在Public Network中傳送到異地端，接著異地端交換器將外部IP Header拿掉再依MAC位址送給目的主機。整個封包傳送流程都是以IP完成，Public Network部分只要是IP路由網路都可以支援，當然也包含Internet。



雲端機房建置與備援機制：使用 Cisco OTV 技術分享

OTV Data Plane



雲端機房建置與備援機制：使用 Cisco OTV 技術分享

Cisco OTV 簡化資料中心連結

- **支援各式類型廣域網路**
  - Works over dark fiber, MPLS, or IP
  - Multi-data center scalability
- **更簡單的設定與管理**
  - Seamless overlay - No network re-design
  - Single touch site configuration
- **高可靠性與彈性**
  - Failure domain isolation
  - Seamless Multi-homing
- **流量最佳化**
  - Automated multi-pathing
  - Optimal multicast replication

多地機房 ，單一資料中心

雲端機房建置與備援機制：使用 Cisco OTV 技術分享

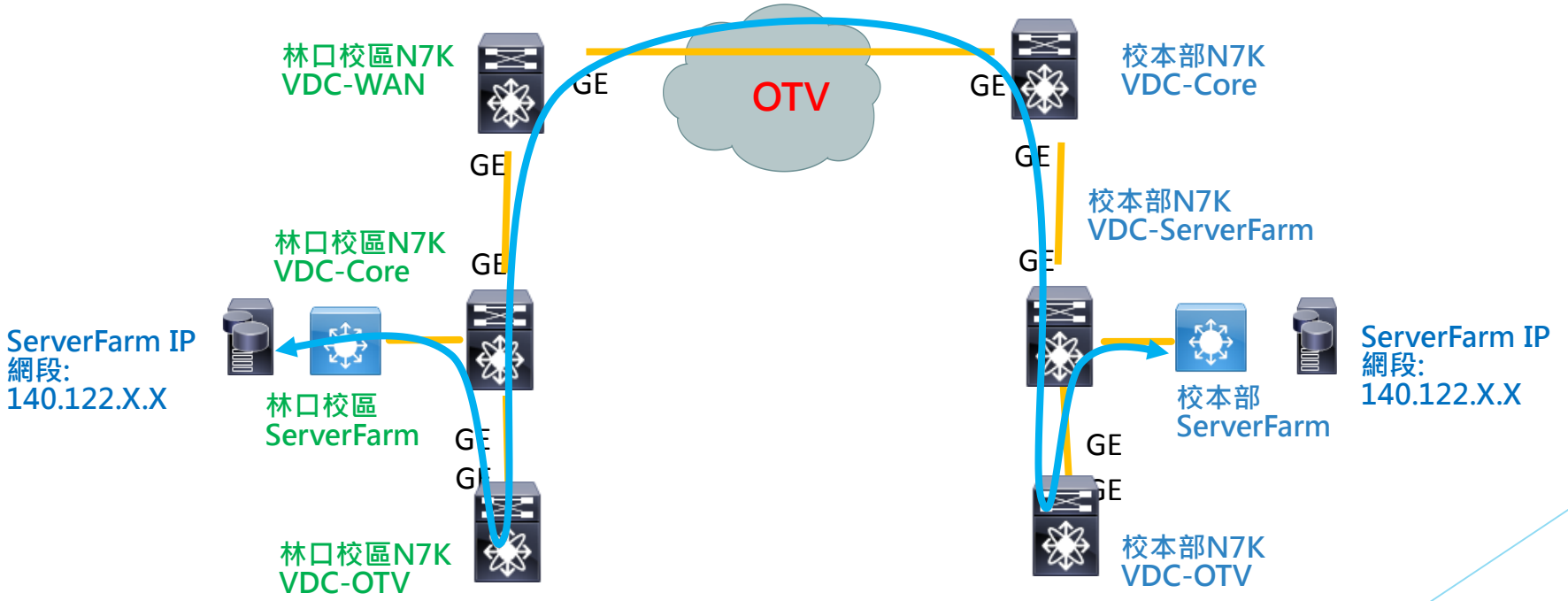
第二層互連技術比較

OTV	技術類型	MPLS (VPLS/EoMPLS)
Nexus 7K	支援設備	6500+Sup-2T
容易	設定管理	複雜(BGP、LDP)
任何L3網路(Internet、VPN)	適用環境	需具備完整的網路管理權限
P2P、MP	L2 型態	EoMPLS:P2P、VPLS:MP
自動、手動	Neighbor Discovery	手動
Control Plane Multicast	MAC Table	Data Plane Flooding
Drop	Unknown Unicast	Flooding
YES	ARP Cache	No
Local Site ONLY	STP	All site in one STP Domain
Per VLAN	Load Balance	No
Local Forward	FHRP Problem	Sub-optimal

雲端機房建置與備援機制：使用 Cisco OTV 技術分享

在校本部及林口校區間使用 Cisco N7K 上的 OTV 技術，建立兩校區的 Server Farm 相同的網段，等同於建立了一個大的 Layer 2 環境。

利用此大 Layer 2 特性可以讓 VM Server 在兩地移動及做 Server Farm 跨校備援。



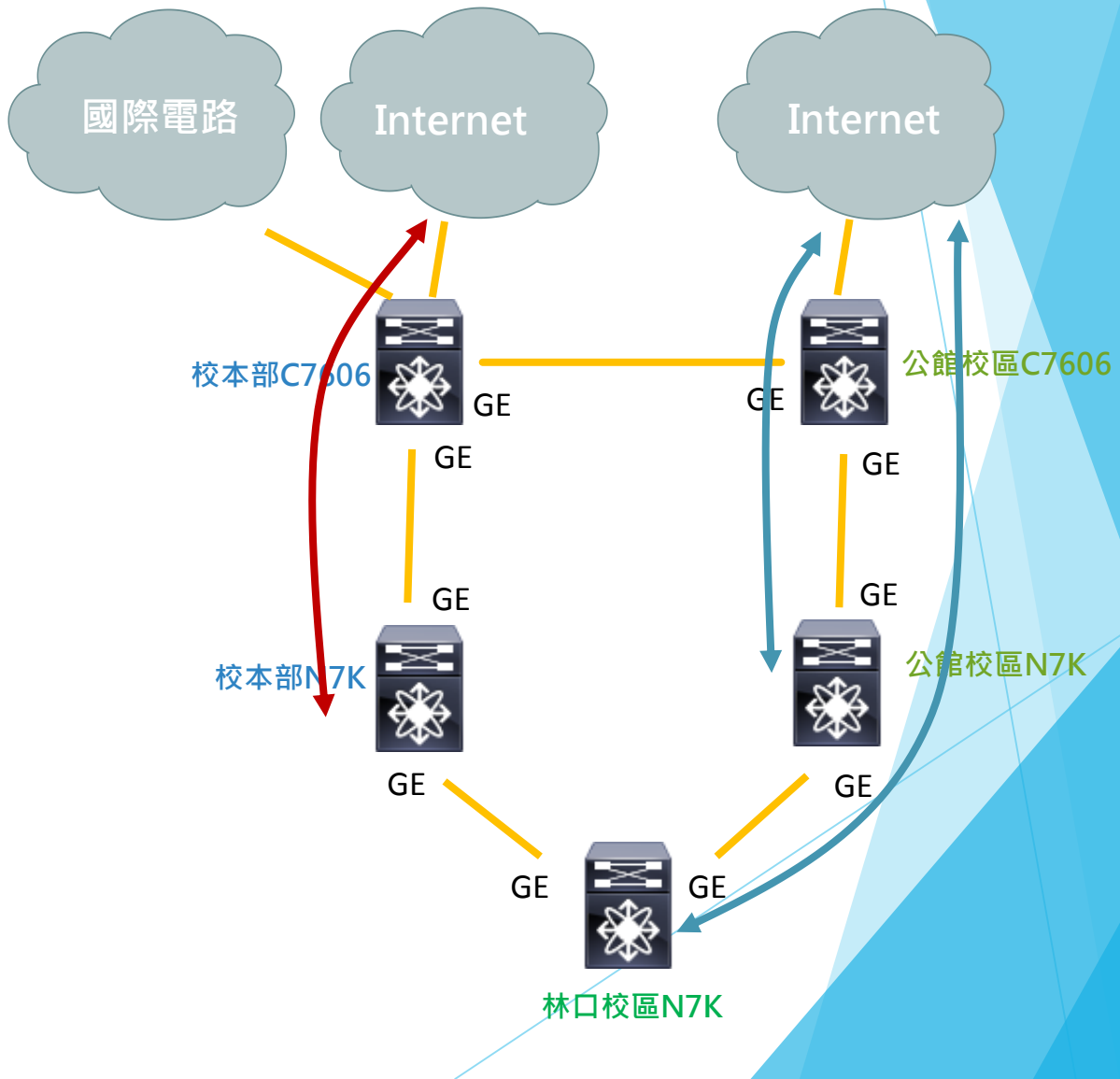
不同校區(校本部、林口、公館)之網路架構與備援機制 -國內及校內網路流向

校本部國內出口

公館校區及林口校區國內出口

三校區網路正常時網路流量走向

校本部及公館校區有各自上網出口
林口及公館校區共用同一個上網出口，
而校本部則是獨立。



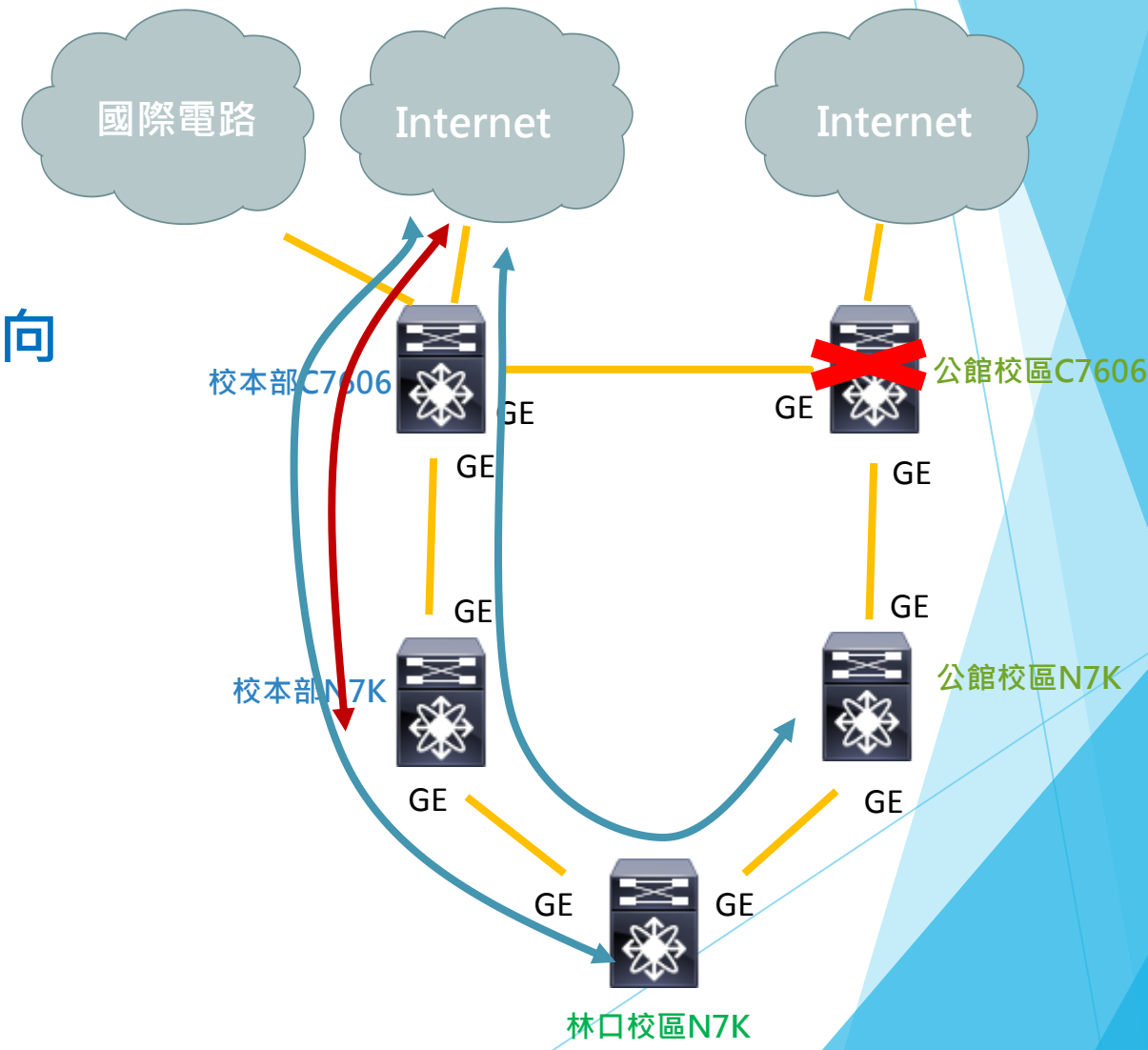
不同校區(校本部、林口、公館)之網路架構與備援機制 -國內及校內網路流向

校本部國內出口

公館校區及林口校區國內出口

公館校區C7606路由器異常時網路走向

當公館校區C7606路由器異常時，
公館校區及林口校區的網路皆會透過路
由自動導往校本部網路出口。



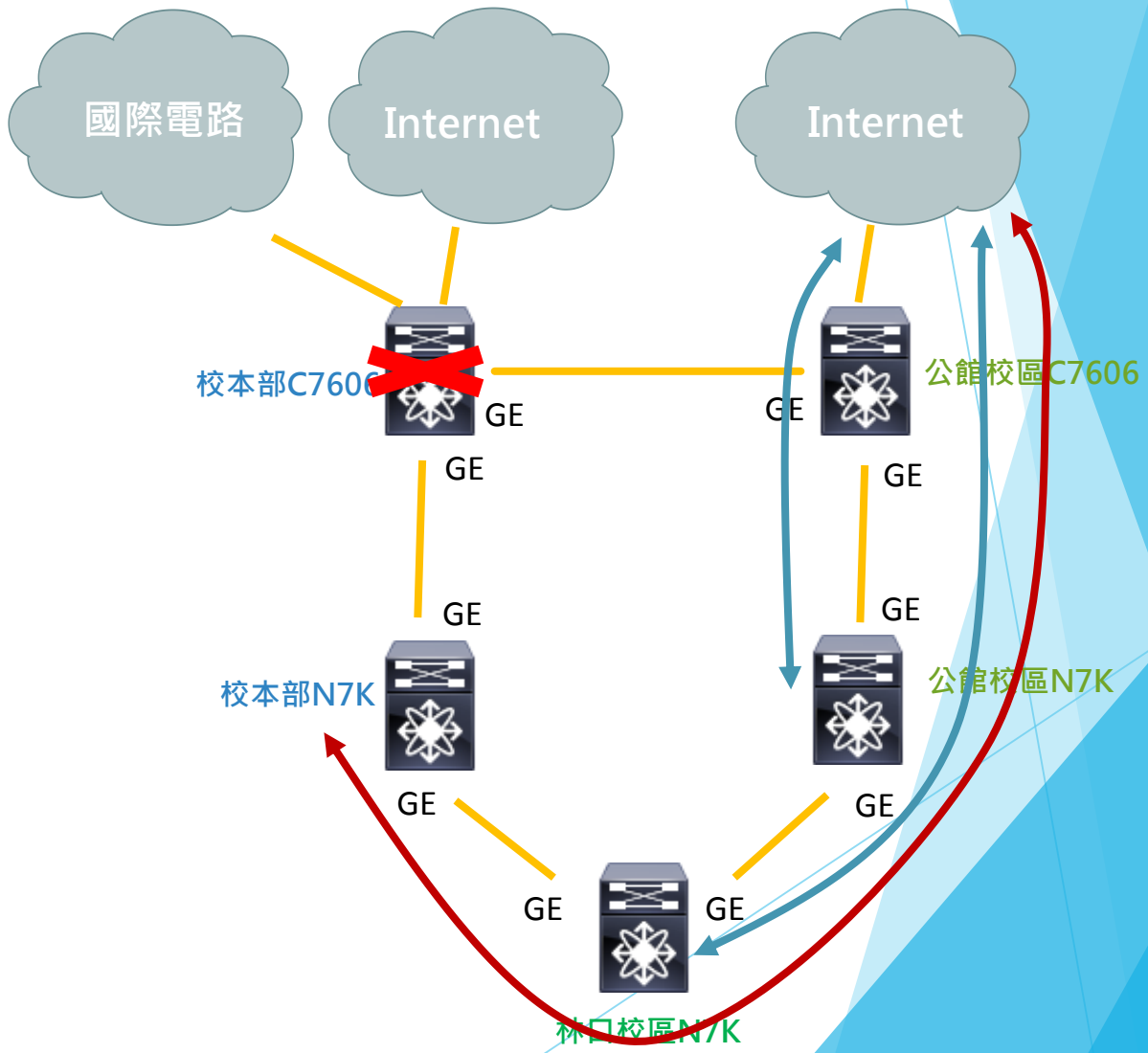
不同校區(校本部、林口、公館)之網路架構與備援機制 -國內及校內網路流向

校本部國內出口

公館校區及林口校區國內出口

校本部C7606異常時網路流量

當校本部C7606異常故障時，
校本部會後透過路由自動導往公館校區出口。



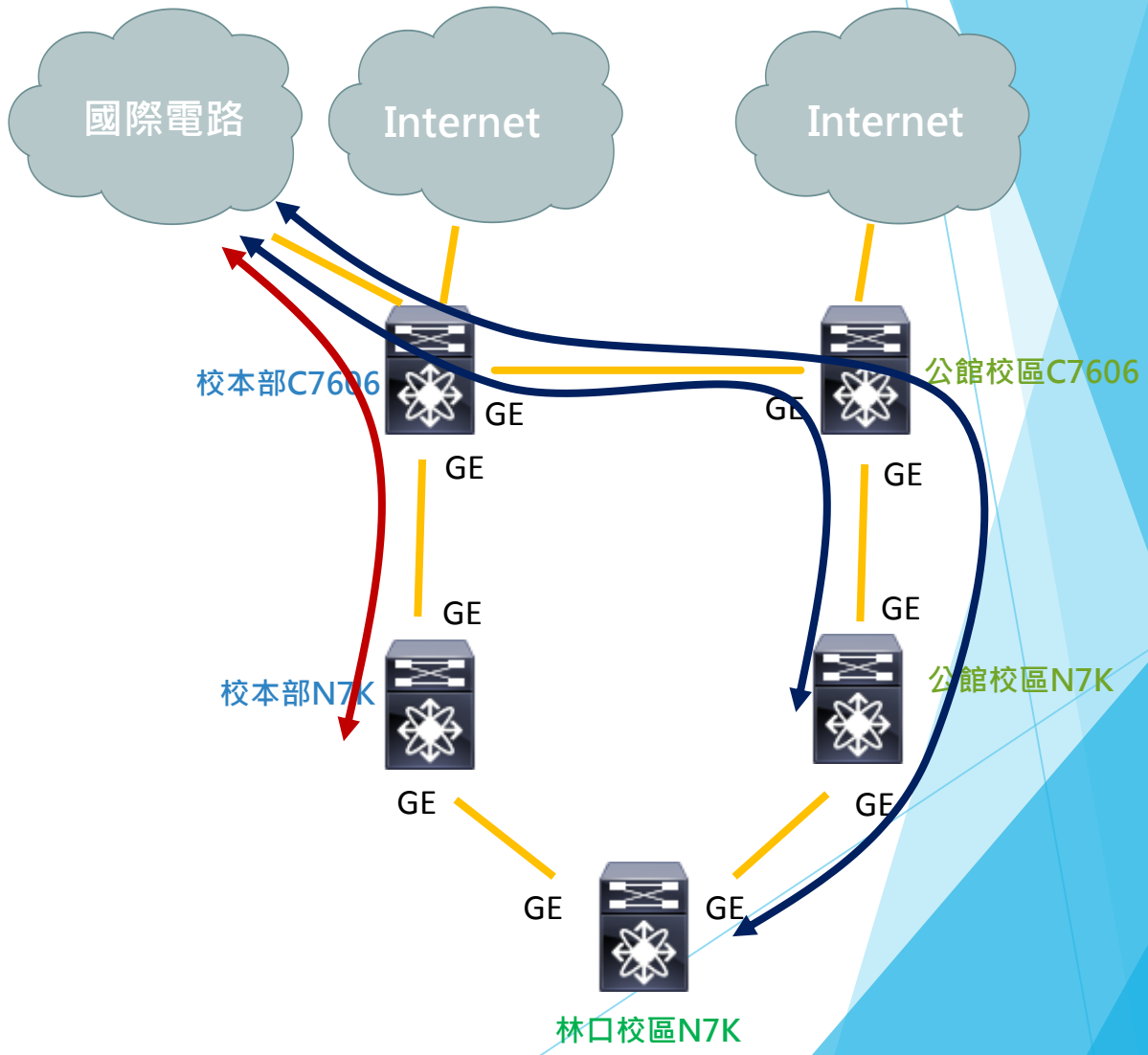
不同校區(校本部、林口、公館)之網路架構與備援機制 -國際網路網路流向

校本部國內出口

公館校區及林口校區國際出口

網路正常時國際網路流量走向

三校區校區共用同一條國際電路至國外



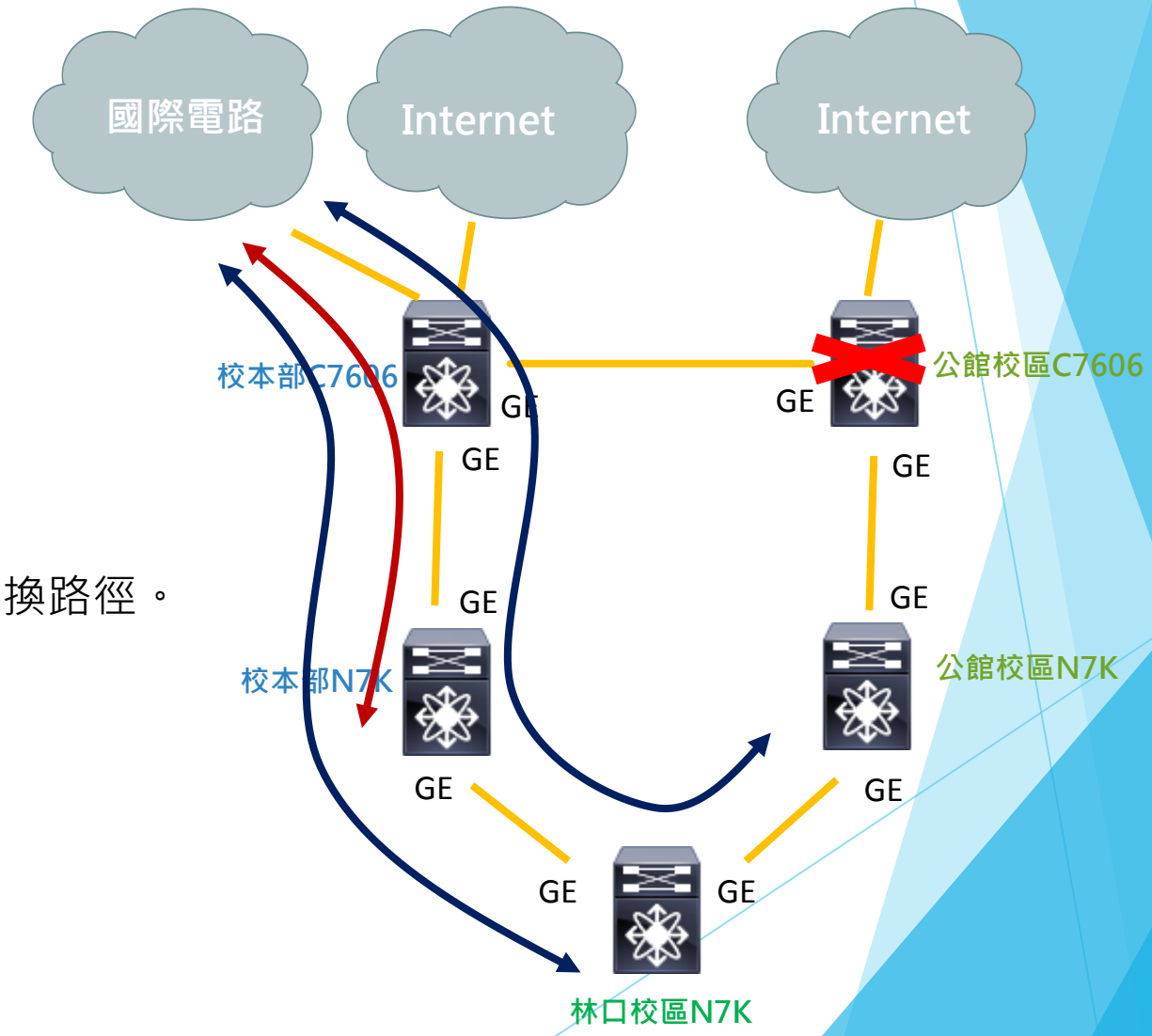
不同校區(校本部、林口、公館)之網路架構與備援機制 -國際網路網路流向

校本部國內出口

公館校區及林口校區國際出口

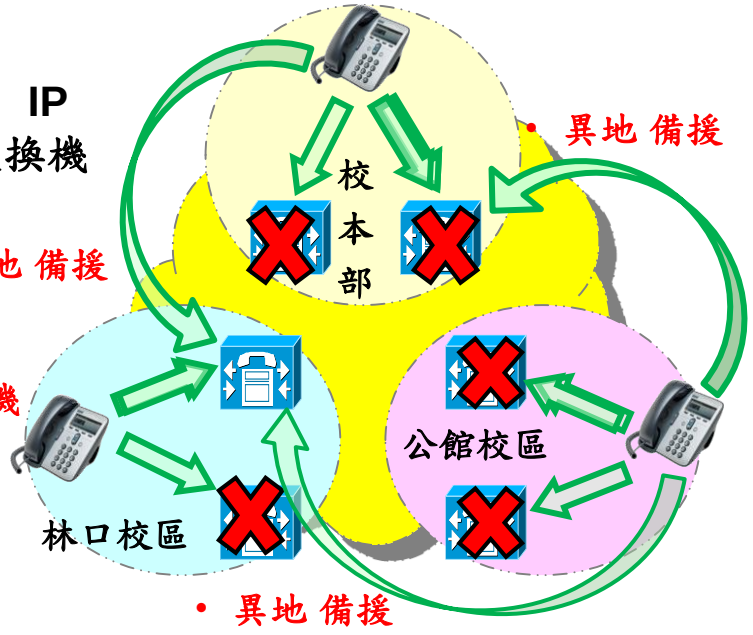
公館校區C7606路由器異常時 國際網路流量走向

三校區校區共用同一條國際電路至國外。
當公館校區C7606路由器異常時，
林口校區及公館校區皆會透過路由自動學習而切換路徑。



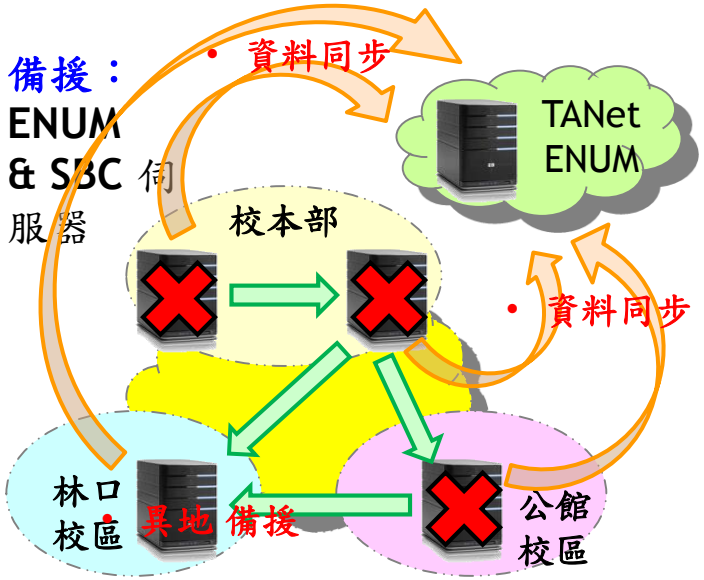
不同校區(校本部、林口、公館)之網路架構與備援機制 -網路電話設備及服務備援

1. 備援： IP 電話交換機

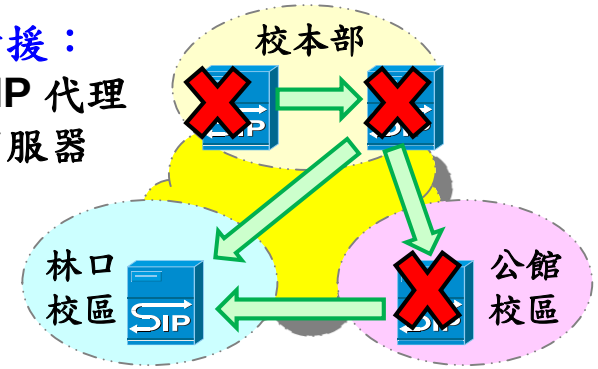


- 同地與異地硬體及虛擬機HA機制
- 同地備援

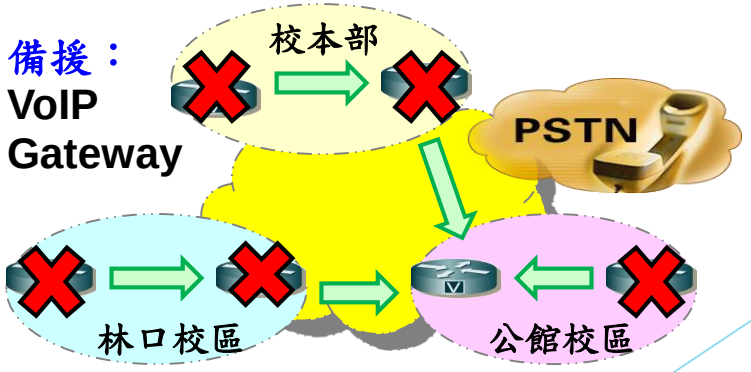
2. 備援： ENUM & SBC 伺服器



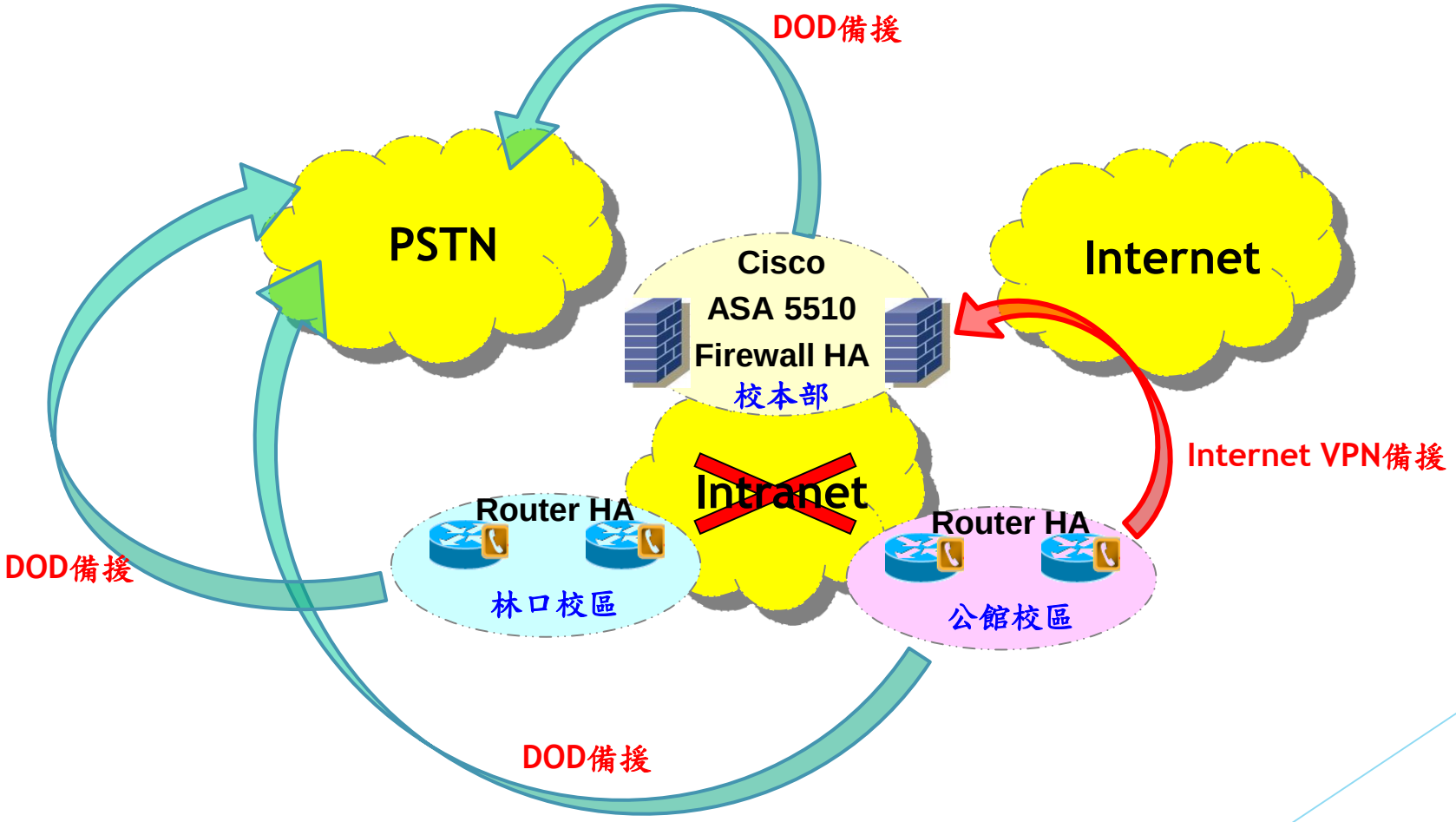
3. 備援： SIP 代理伺服器



4. 備援： VoIP Gateway



不同校區(校本部、林口、公館)之網路架構與備援機制 -網路電話Intranet備援



淺談 Cisco OTV 導入經驗

Cisco OTV優勢

- 雖然OTV是利用Layer2的技術，但是它會過濾掉原有在Layer2的一些Frame，包含Spanning-Tree、Broadcast Storm、Unicast Flooding等
- 使用OTV並不需要更動現有的網路架構(所以稱為“Overlay”，覆蓋在既有的網路架構上)，因此當有一個新的資料中心加入時並不需要更動到其他資料中心的網路架構，依照官方的說法最多只需四行指令就可以搞定

建置注意事項

- 跨校區專線電路MTU值必須大於1500 (Jumbo Frame)

所遭遇問題

- 因OTV封包特性，即使兩路專線電路作EtherChannel仍無法有效達到Load Sharing
- 校本部N7K VDC aclmgr Process異常導致VDC自動重啟
- 公館N7K VDC snmpd Process異常導致VDC自動重啟失敗及N7K Reload後Config遺失

總結

以二層網路為基礎的資料中心設計，對於許多網路管理人員來說其實是一項非常大的變革，卻也是不得不做的改變。

且其中影響架構的人員相當廣泛，諸如伺服器管理員、虛擬化管理員與儲存系統管理員，已非從前只要從網路的思考就可以完成。

也因此網路管理者在組織內部需要更廣泛的了解各項資訊技術，提出對於學校最佳的解決方案。

簡報完畢，謝謝！