GSN DNS Policy說明會

國家發展委員會
106年3月

大綱

一. 緣由
二. 常見機關DNS架構及風險
三. 架構調整說明
四. 機關配合事項
五. 參考範例

緣由

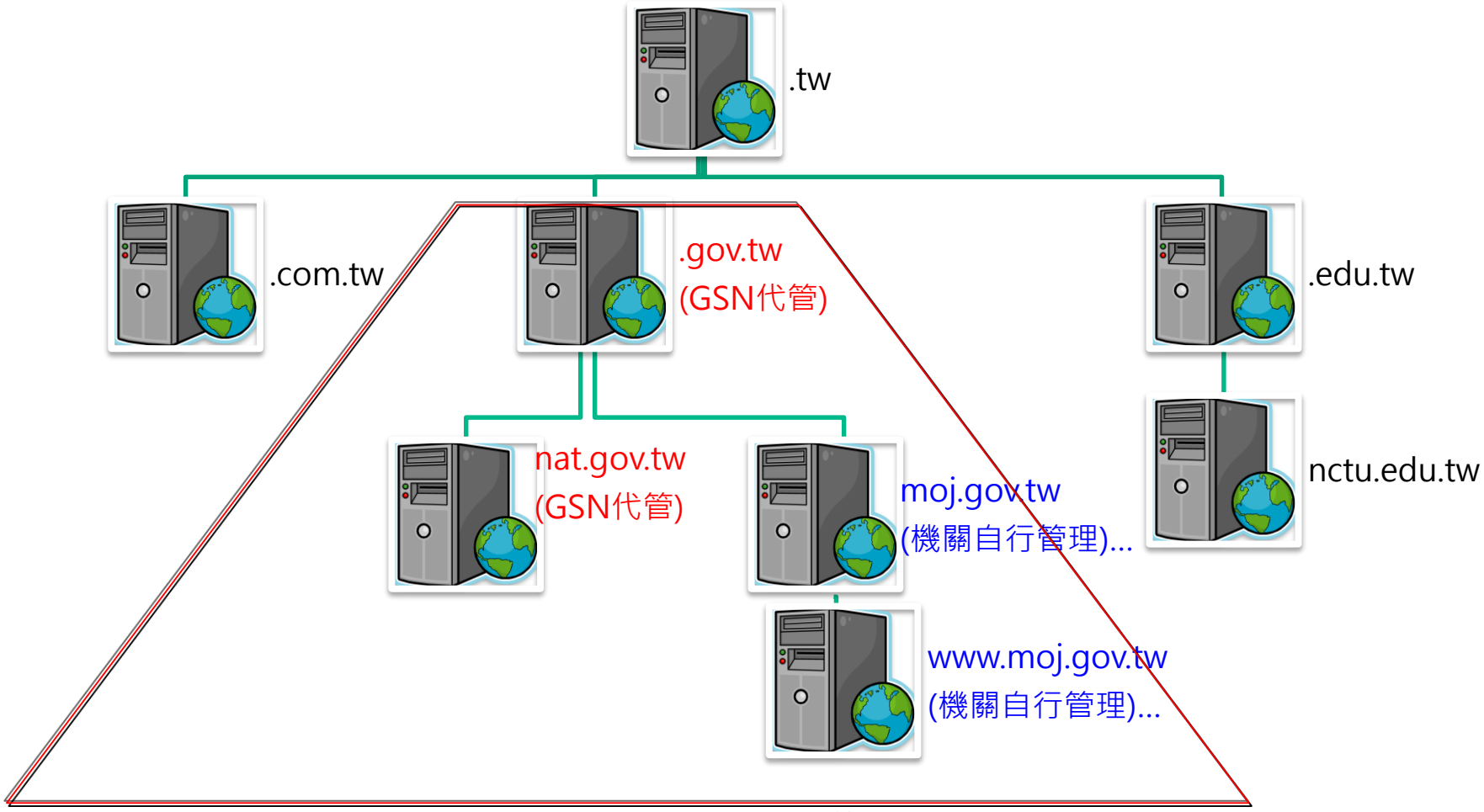
✓ 提升各機關資安防護服務

DNS運作

- ✓ 網域名稱系統
  - Domain Name System，DNS
  - 域名和IP位址相互對映的一個分散式資料庫，能夠使人更方便地存取網際網路

Domain Name	IP Address
www.hinet.net	202.39.224.7

政府機關DNS域名架構

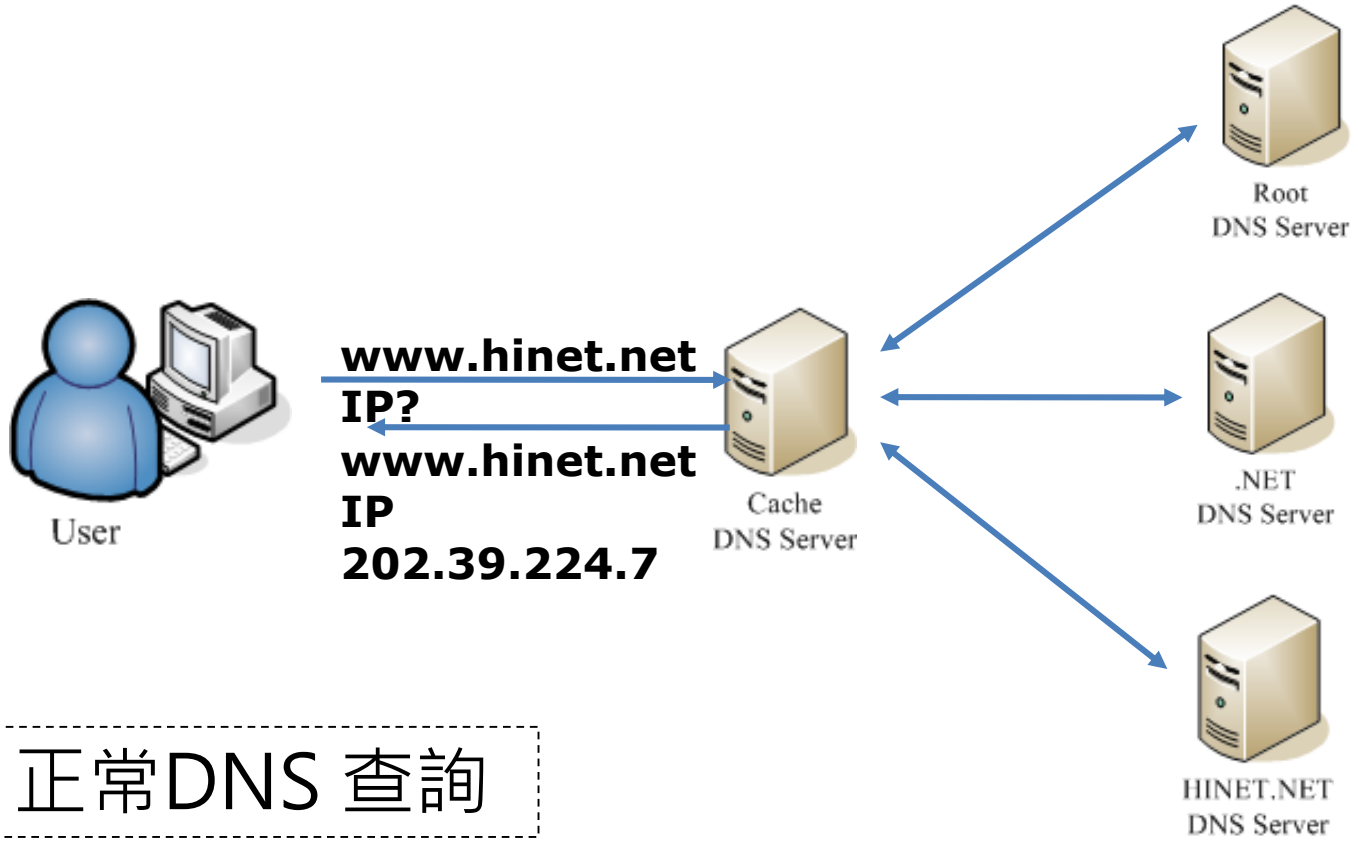


*註：Internet Assigned Numbers Authority，IANA

DNS可能風險

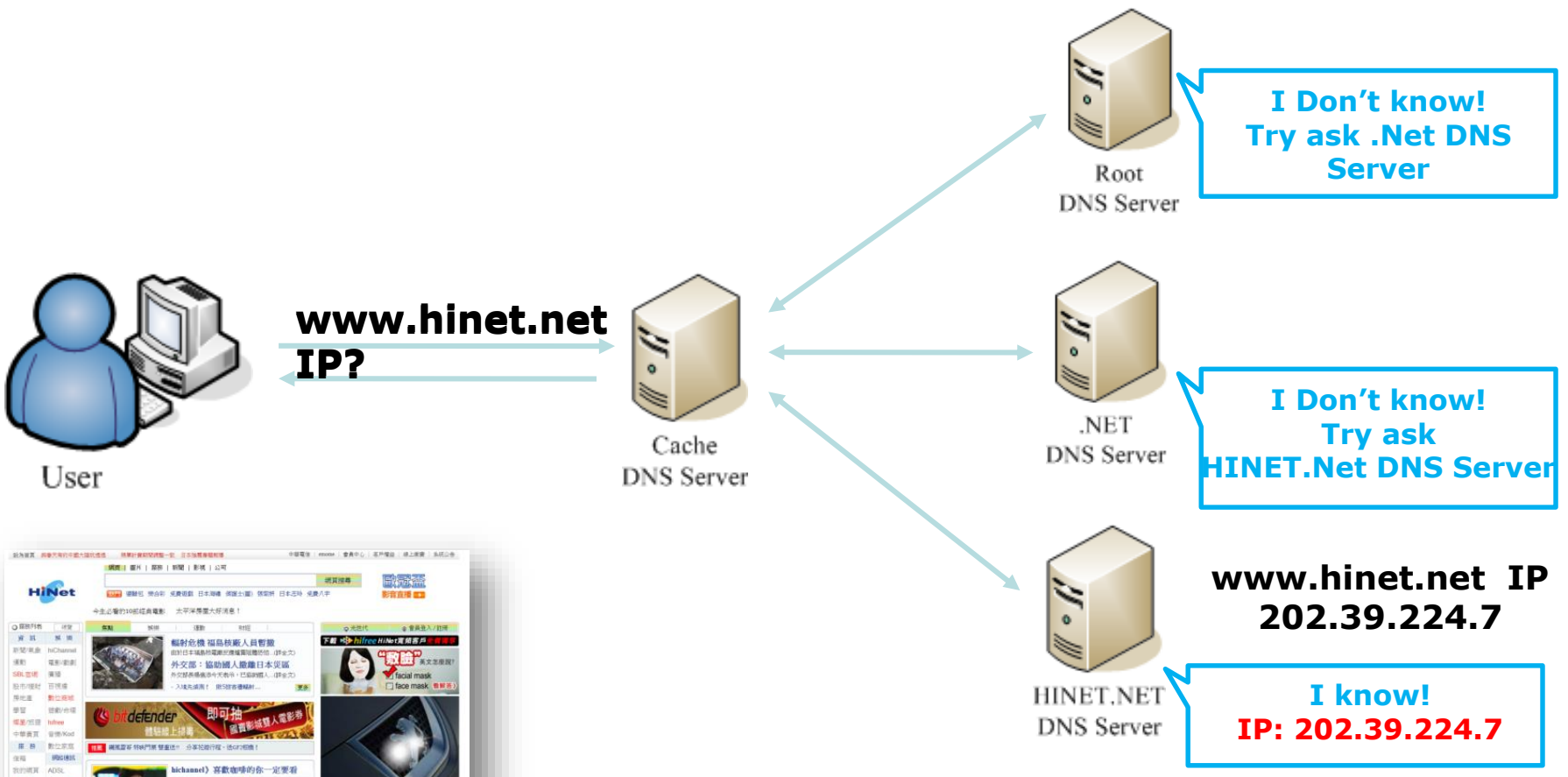
- ✓ DNS欺騙
  - DNS Cache Poisoning(DNS快取汙染)
  - Domain/DNS Hijacking(網域/DNS劫持)
  - Men in the middle(偽造DNS主機從中作梗)
- ✓ 常見手法
  - 因開放式的DNS不限來源的特性，遭DNS欺騙成功的機會越高
  - 若能縮小使用限制來源，再配合適當的DNS防護機制，可有效降低DNS欺騙的風險

DNS運作流程



正常DNS 查詢

DNS運作流程

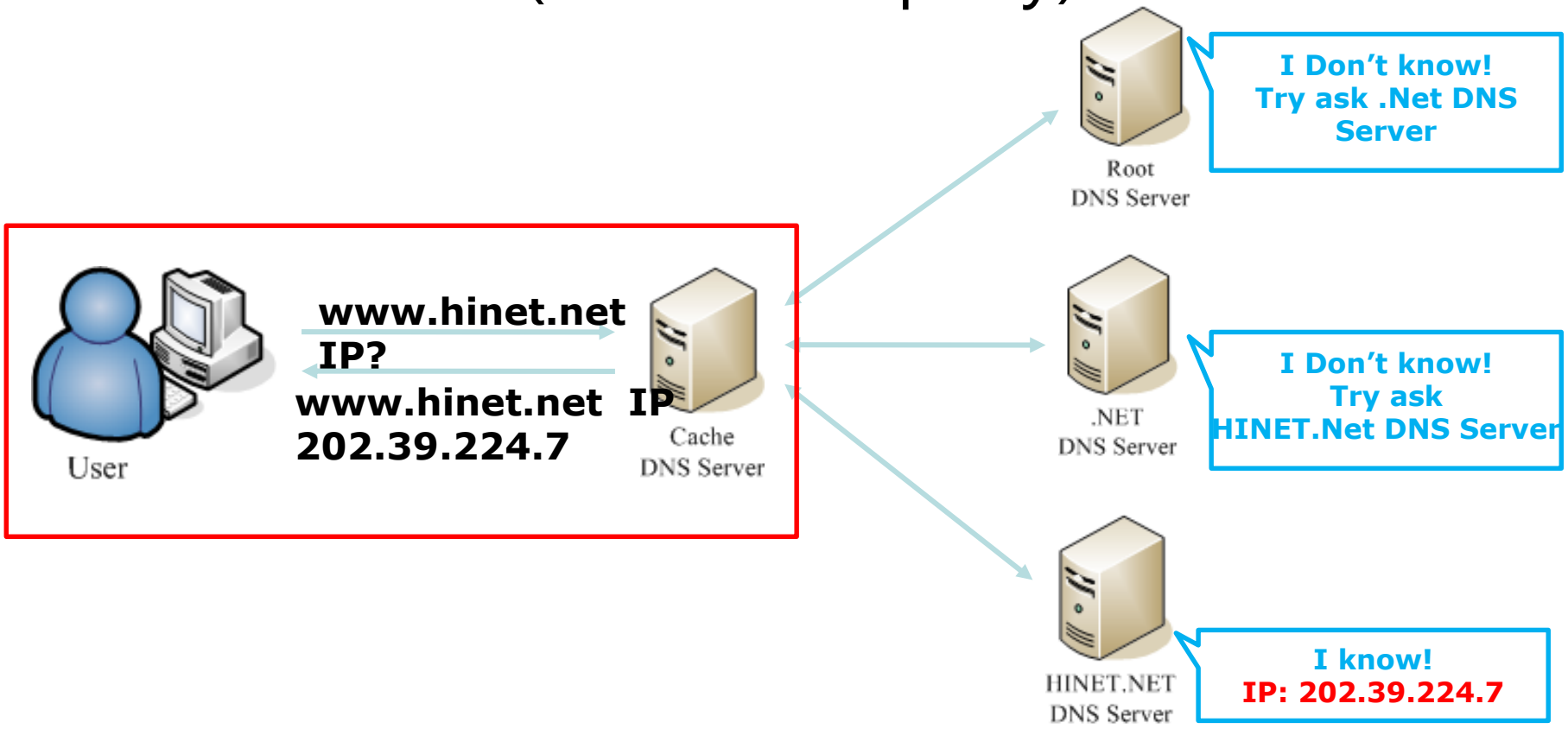

Root
DNS Server
I Don't know!
Try ask .Net DNS
Server
www.hinet.net
IP?
User
Cache
DNS Server
.NET
DNS Server
I Don't know!
Try ask
HINET.Net DNS Server
www.hinet.net IP
202.39.224.7
HINET.NET
DNS Server
I know!
IP: 202.39.224.7

DNS查詢模式

- ✓ 遞迴式查詢 (Recursive query)
  - ■ DNS用戶端向DNS Server的查詢模式
    將要查詢的封包送出去問，就等待正確名稱的正確回應
- ✓ 交談式查詢 (Iterative query)
  - ■ DNS Server間的查詢模式由Client端或是DNS Server上所發出去問，這種方式送封包出去問，所回應回來的資料不一定是最後正確的名稱位置
- ✓ 快取主機 (Cache Server)
  - ■ 負責遞迴式查詢，限制使用來源，如：GSN ：210.69.1.1、210.69.2.1
  - ■ 開放式：HiNet：168.95.1.1、168.95.192.1，Google：8.8.8.8、8.8.4.4
- ✓ 權威主機 (Authoritative Server)
  - ■ 管理並存有域名資料之主機
  - ■ 須對外全面開放，不可開啟遞迴式查詢功能
  - ■ 應建置至少兩部以上主機分別為Master與Slave相互備援

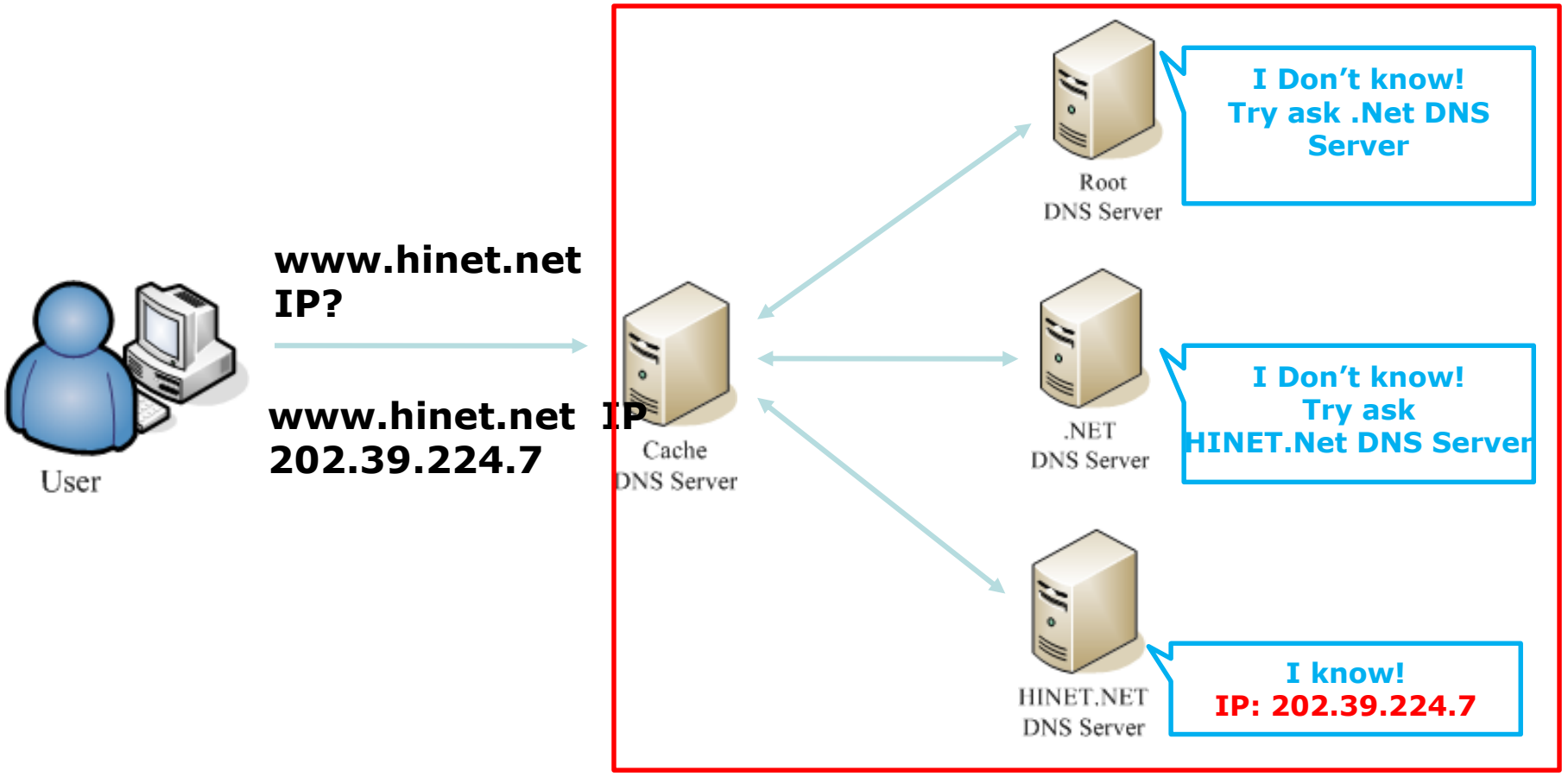
DNS查詢模式(1/5)

✓ 遞迴式查詢 (Recursive query)



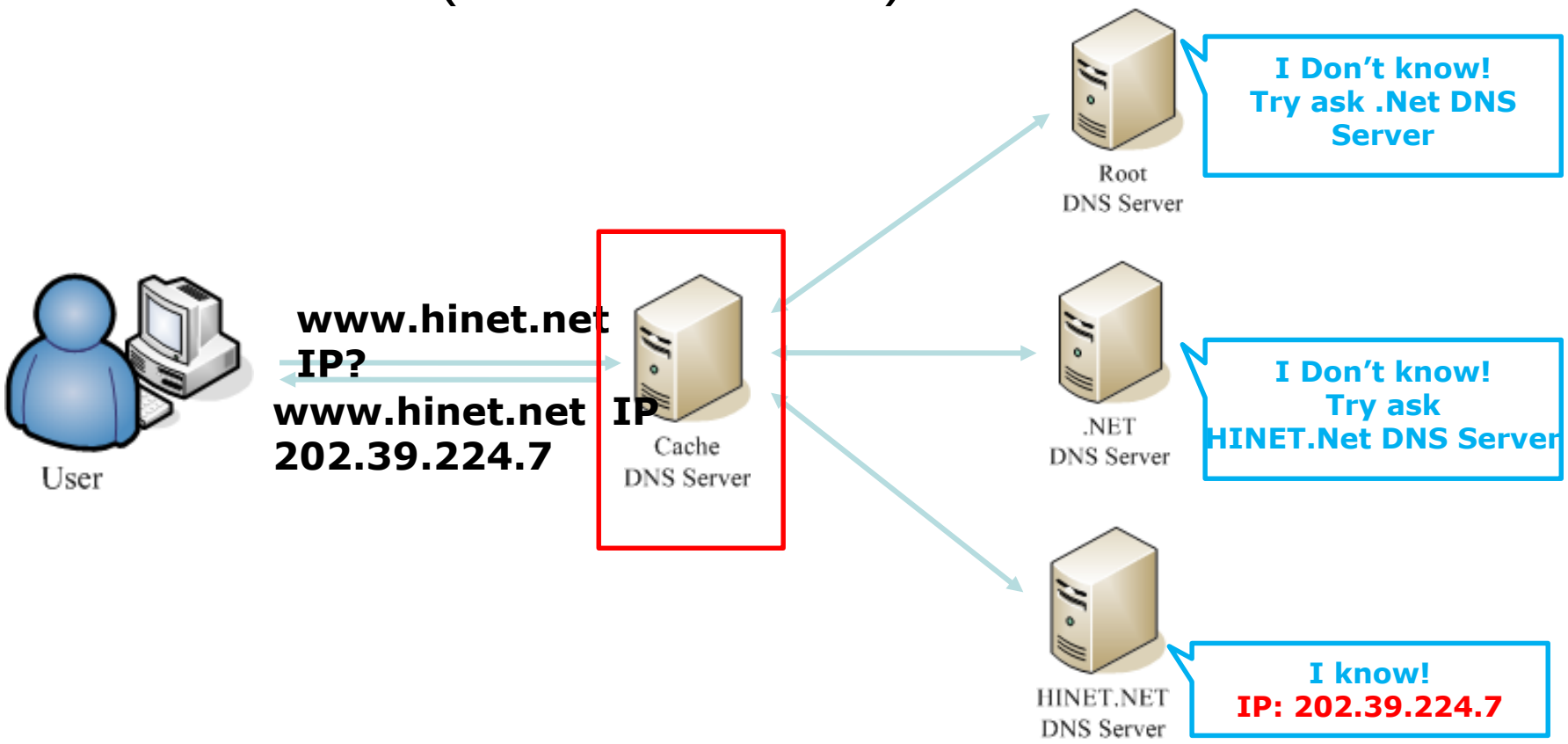
DNS查詢模式(2/5)

✓ 交談式查詢 (Iterative query)



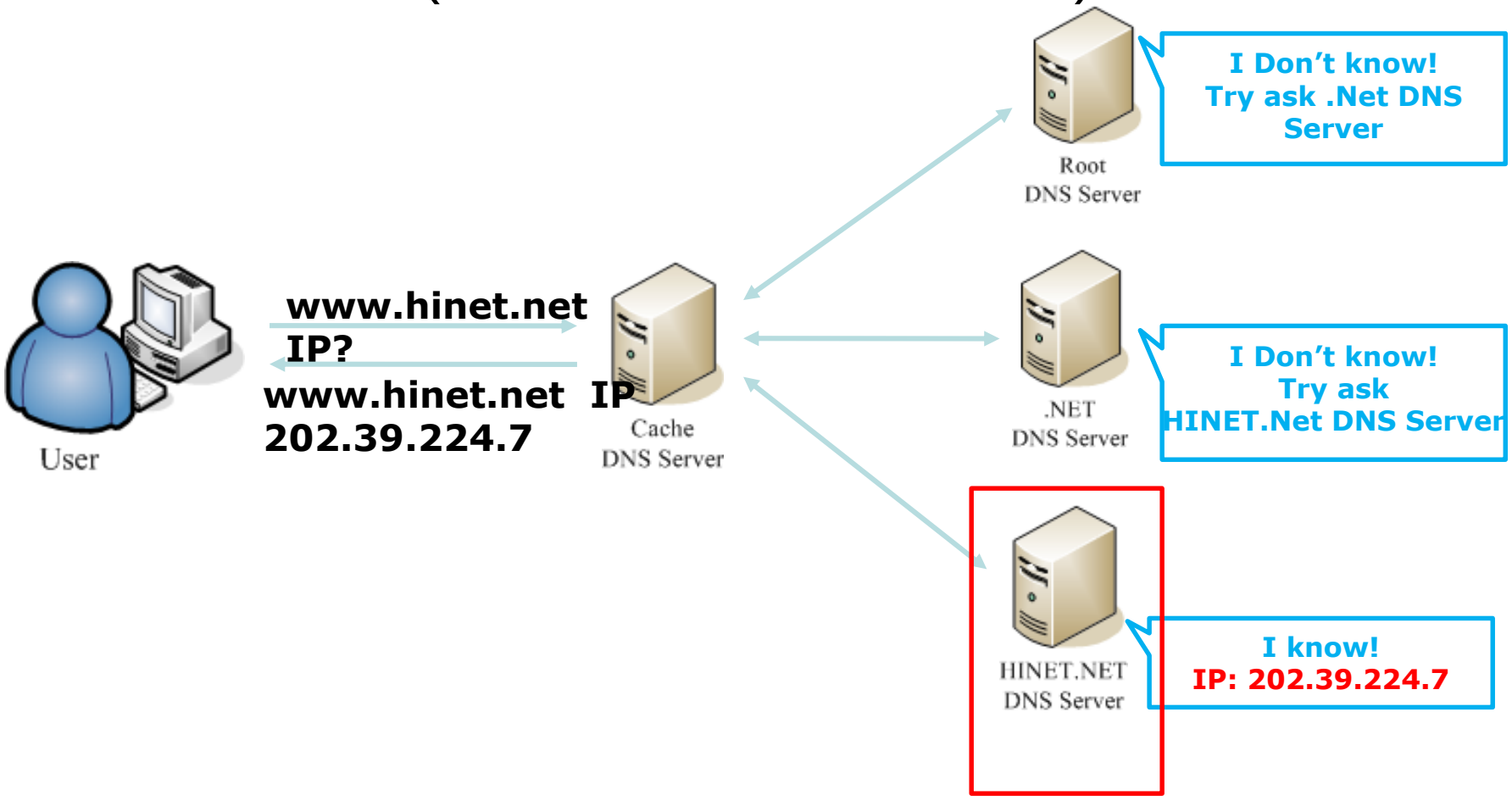
DNS查詢模式(3/5)

✓ 快取主機 (Cache Server)

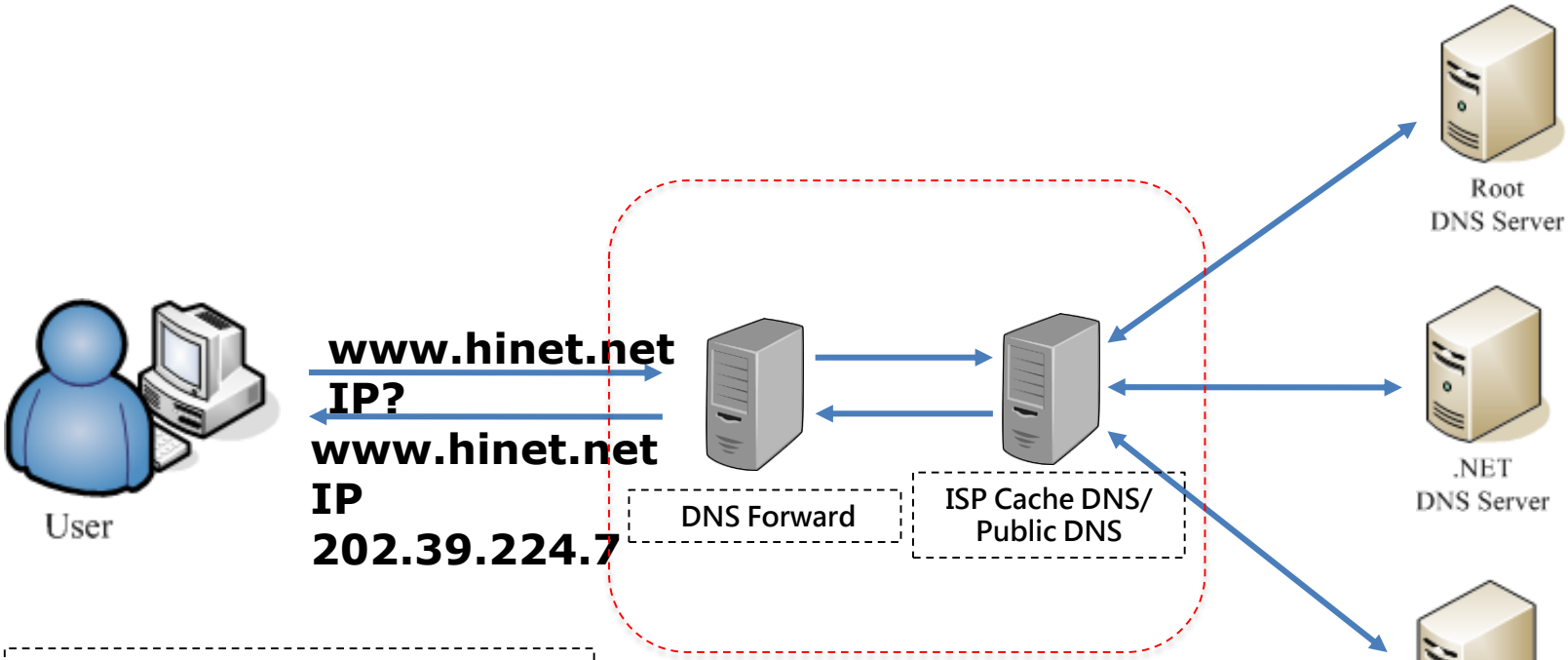


DNS查詢模式(4/5)

✓ 權威主機 (Authoritative Server)

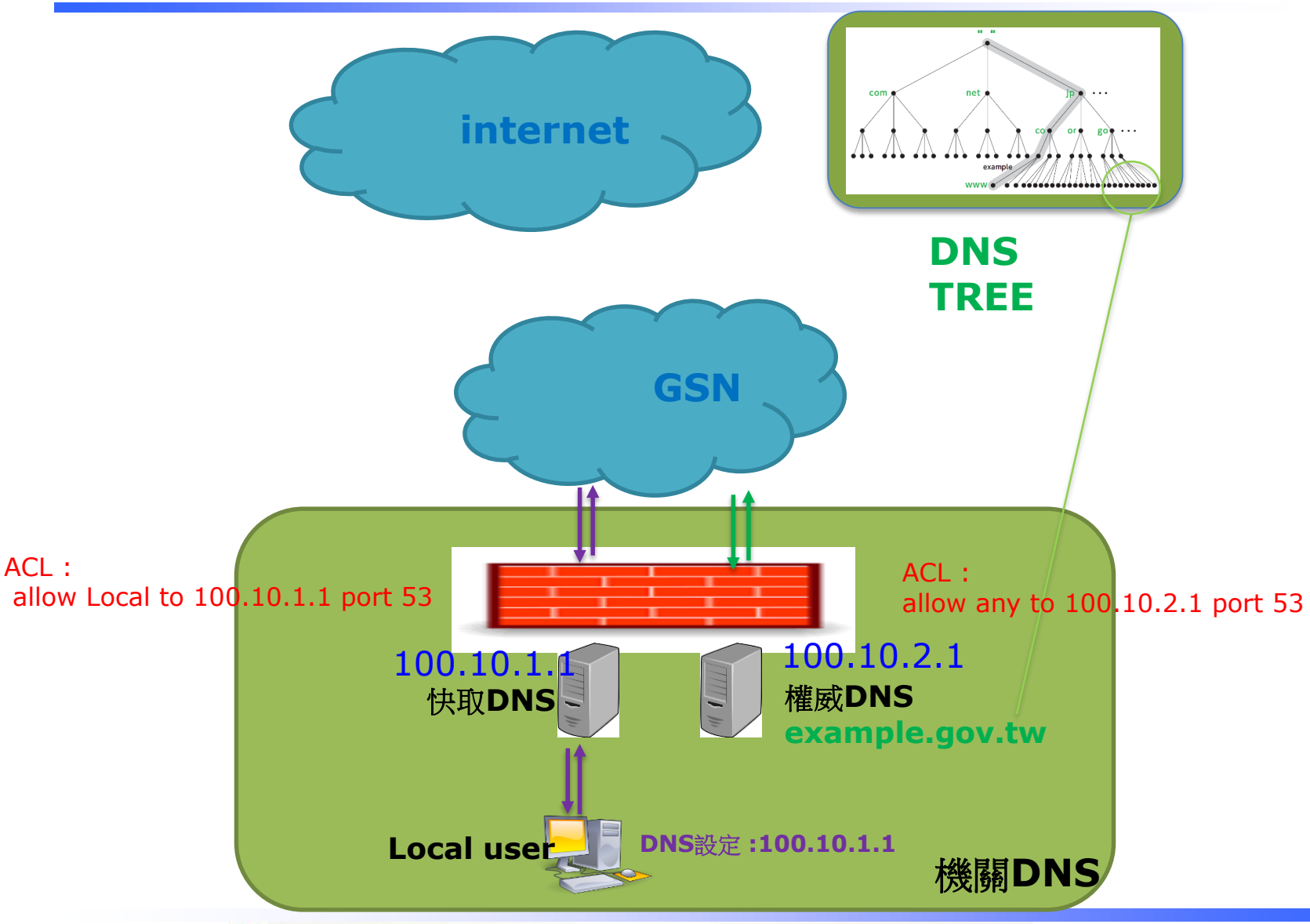


DNS查詢模式(5/5)

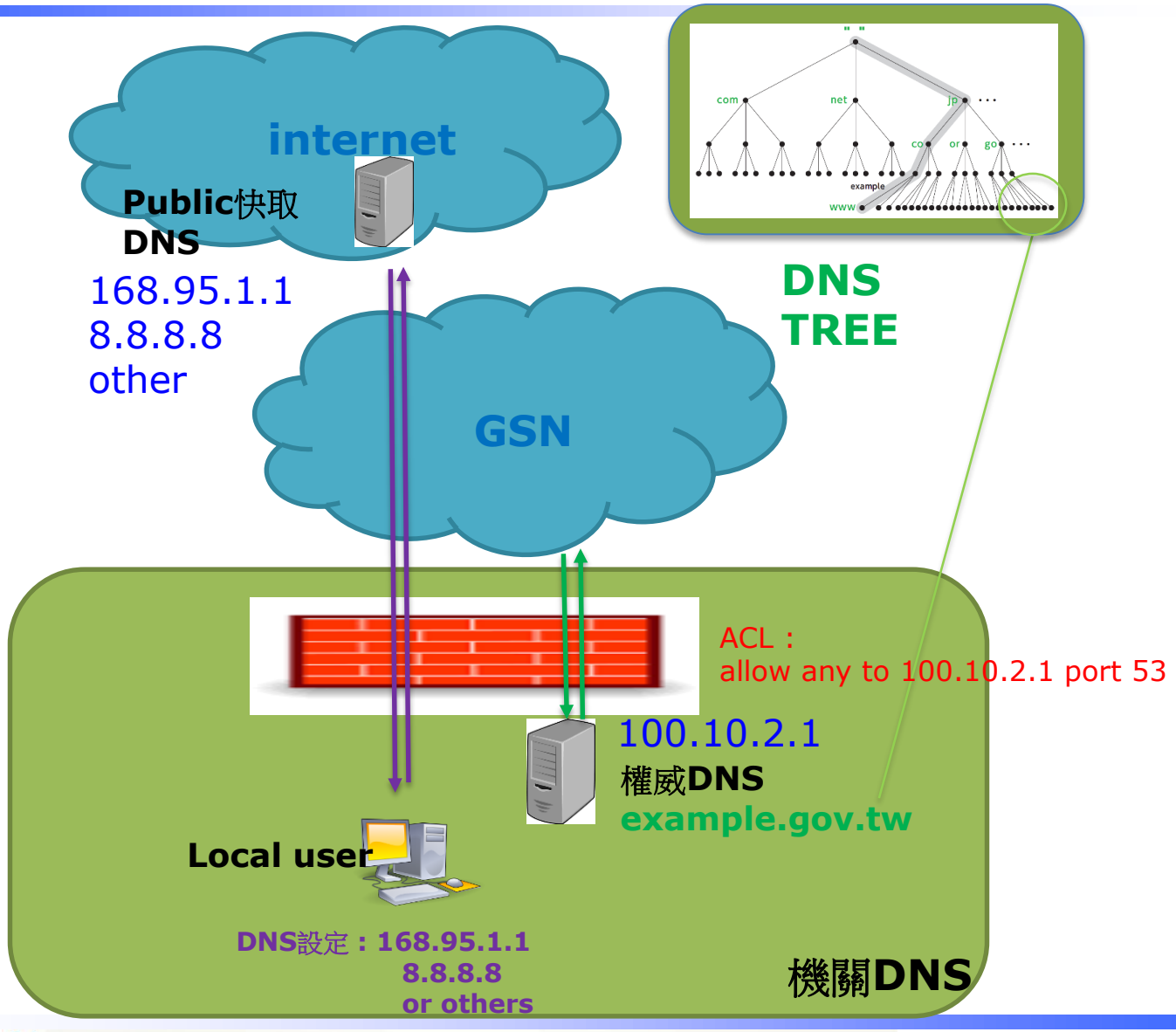


DNS 查詢
+Forwarders

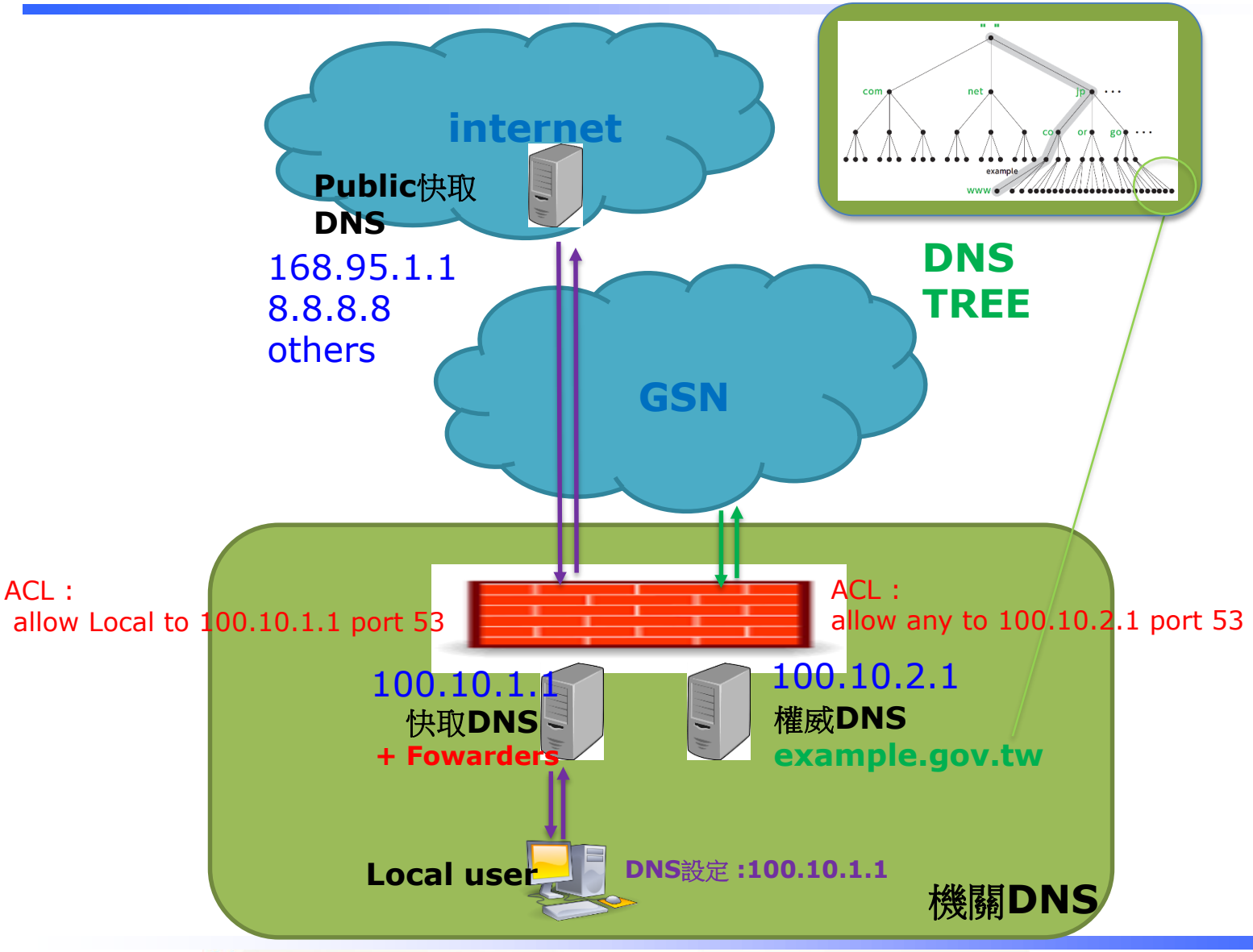
機關常見DNS架構(1/3)



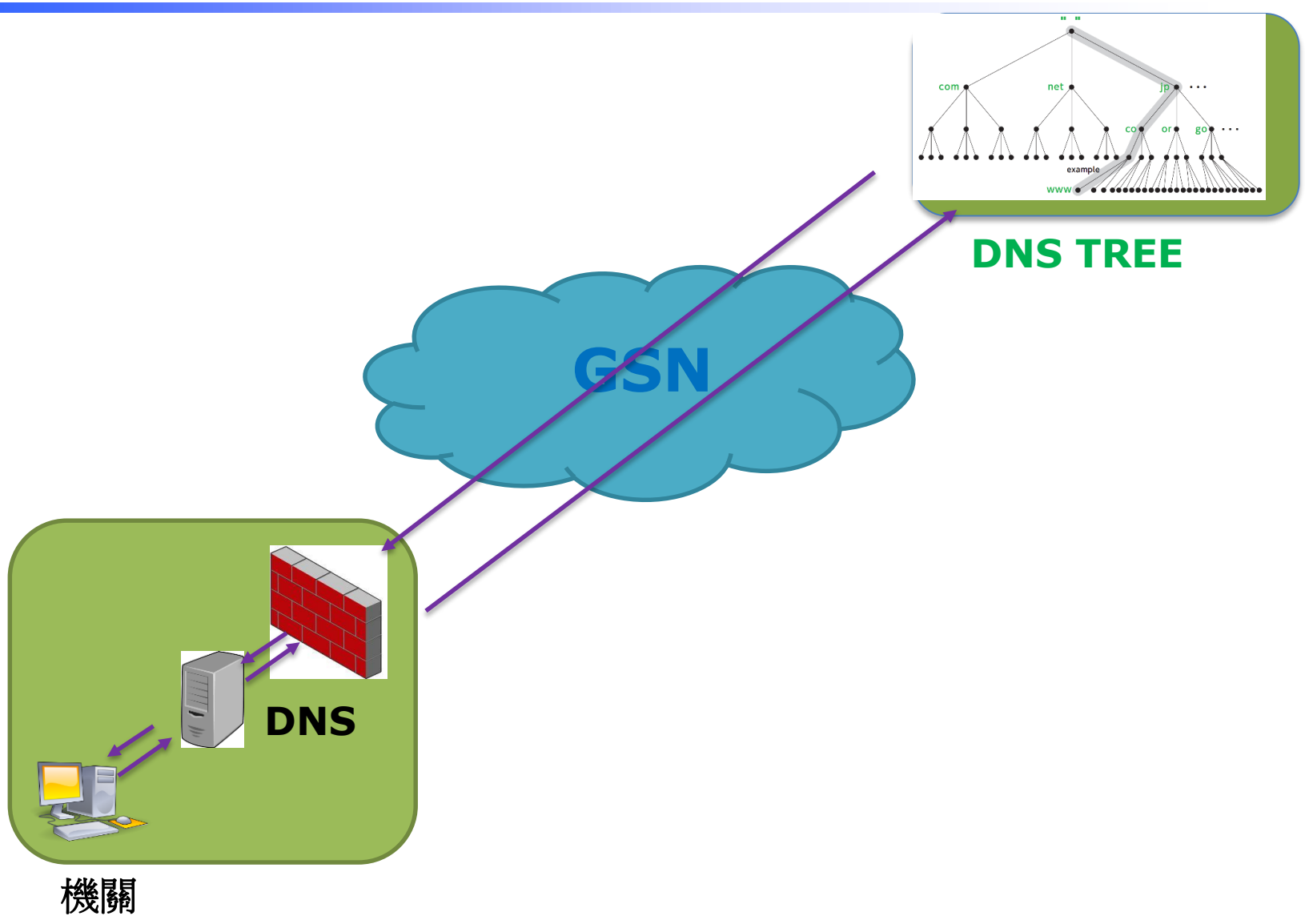
機關常見DNS架構(2/3)



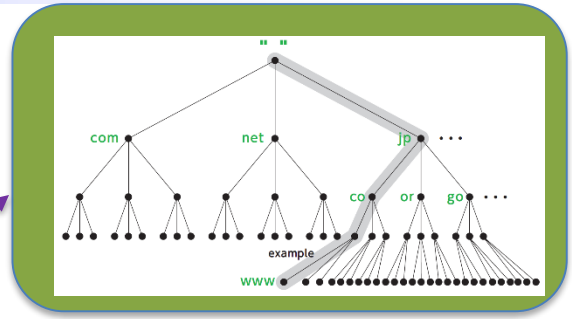
機關常見DNS架構(3/3)



DNS查詢路徑-調整前



DNS查詢路徑-調整後



DNS TREE

GSN

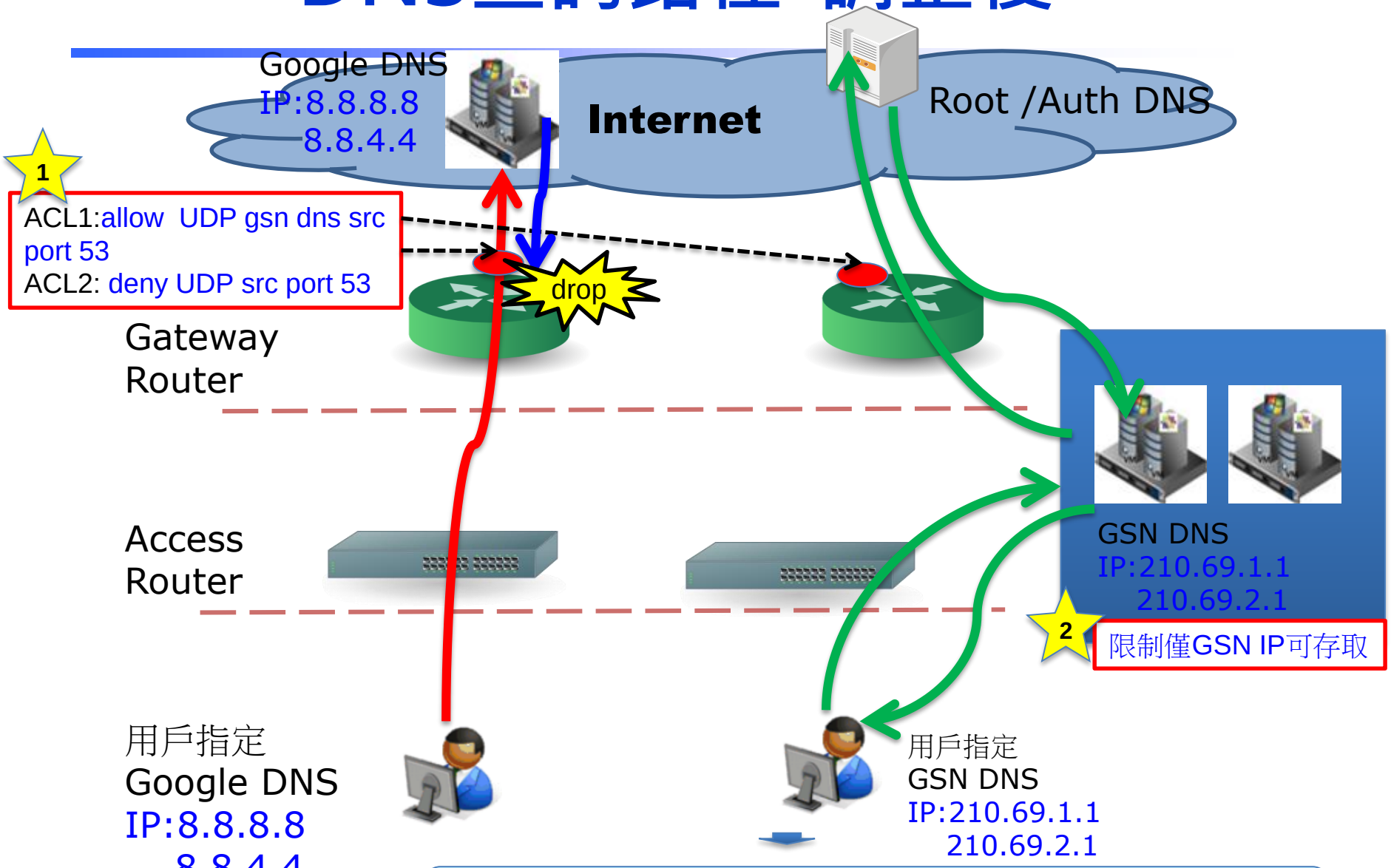
GSN Cache DNS

210.69.1.1、210.69.2.1

DNS + Forwarders

機關

DNS查詢路徑-調整後



只允許由GSN DNS發起的DNS封包進出GSN網路
其餘禁止，用戶須透過GSN DNS進行網址解析

機關配合事項

- ✓ 機關DNS Server
  - ■ 將DNS服務設定指向GSN Cache DNS(210.69.1.1與 210.69.2.1)
- ✓ 其他應用服務(如AP)
  - ■ 機關於GSN建置應用服務或熱點時，應確定設置DNS位置為210.69.1.1與 210.69.2.1
- ✓ DNS紀錄障礙查測，請改用網頁版服務
  - ■ CMD指令僅能存取GSN DNS，如需要查測請改用網頁版服務，如：
    http://networking.ringofsaturn.com/Tools/dig.php
- ✓ 請各機關於106年4月30日前完成調整

參考範例

- ✓ BIND DNS Forwarders設定範例
  - **options** {

    .....

    // 將所有DNS Query請求轉交GSN Cache DNS

    forward only; //只允許 forward

    forwarders { 210.69.1.1; //設定forwarder的IP

    210.69.2.1; };

    };
  - 亦可視需要加上IPv6 :
    - 2001:4420::1
    - 2001:4420::2:1

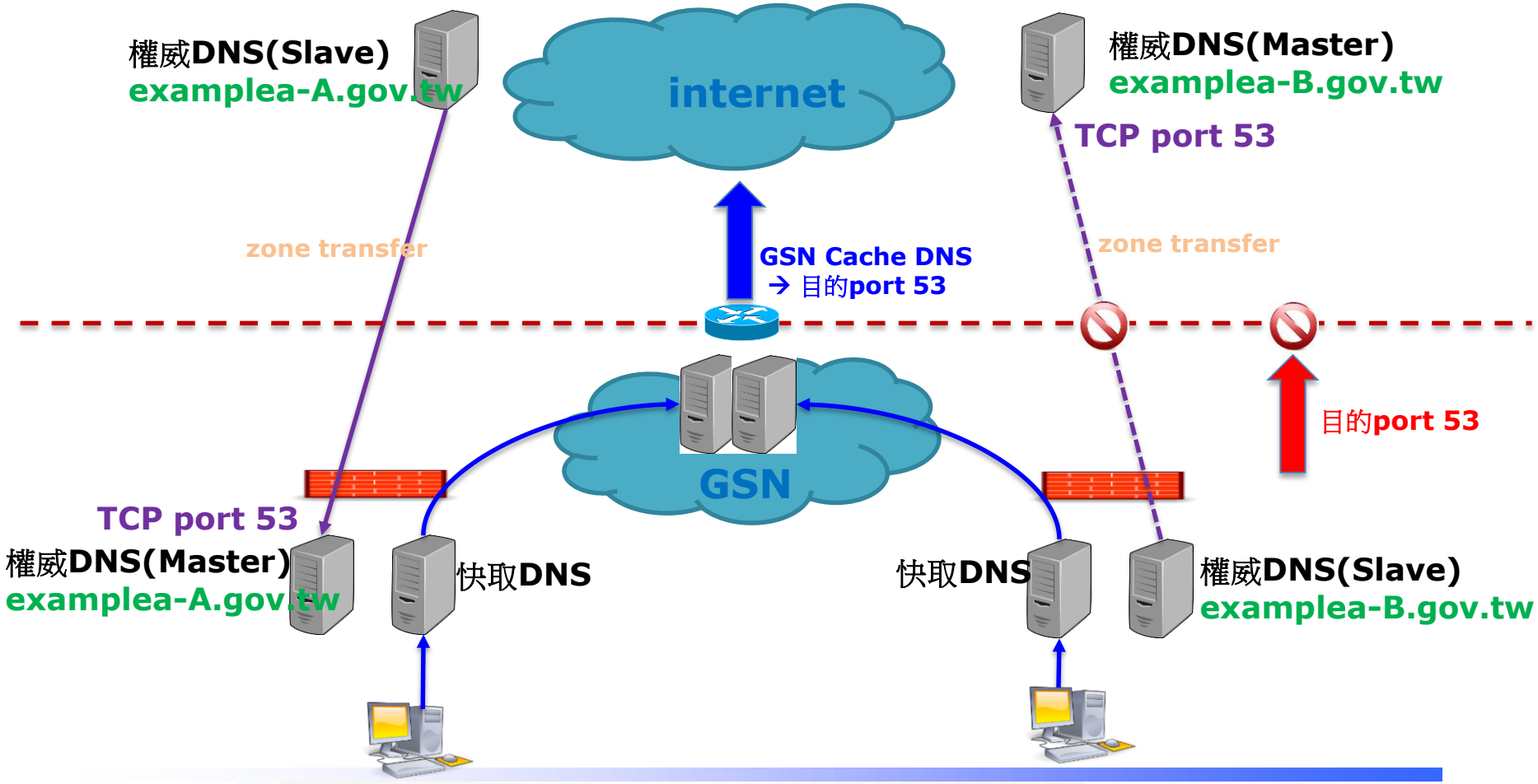
參考範例

- ✓ Windows DNS Forwarders
  - ■ 設定 DNS 伺服器以使用具有 Windows 介面的轉寄站
    1. 開啟 [DNS 管理員]。
    2. 在主控台樹狀目錄中按一下適用的 DNS 伺服器。
       - ● 位置

         DNS/適用的 DNS 伺服器
    3. 在 [執行] 功能表，按一下 [內容]。
    4. 在 [轉寄站] 索引標籤上的 [DNS 網域] 之下，按一下網域名稱。
    5. 在 [已選取的網域轉寄站 IP 位址清單] 中，輸入轉寄站的 IP 位址，然後按一下 [新增]。
- ✓ 參考連結
  - ■ https://technet.microsoft.com/zh-tw/library/cc754941(v=ws.11).aspx#BKMK_winui

參考範例

- ✓ 若限制TCP port 53對權威DNS的備援的影響
  - ■ 若跨網佈署權威DNS(master/slave)時，請將機關內部於GSN建置的DNS設定為master，非GSN建置的設定為slave



簡報完畢
謝謝指教