如何驗證 DNS 加密 (DoT) 與過濾功能是否生效？

當您在路由器上啟用了 **DNS over TLS (DoT)** 或 **DNS 覆蓋解析** 功能後，建議透過以下方式驗證流量是否正確經過加密與過濾，以確保您的網路環境安全

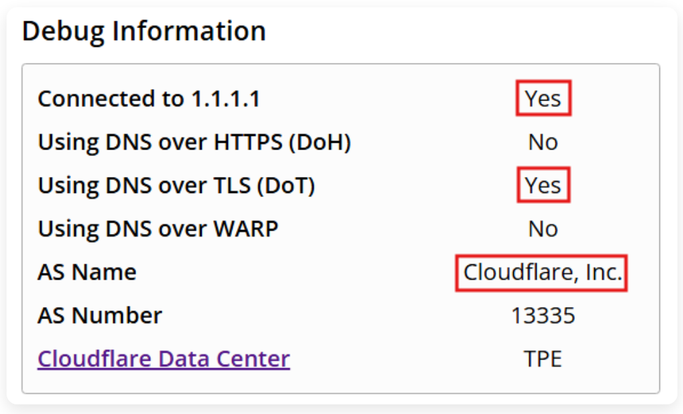
一、 Cloudflare 驗證方式

Cloudflare 提供專用的偵錯網頁，可快速檢查加密狀態

驗證步驟： 使用連接在該網路下的設備（手機或電腦）造訪：`https://1.1.1.1/help`

檢查重點：

1. **Using DNS over TLS (DoT):** 應顯示為 **Yes**（代表您的路由器加密成功）
2. **Connected to 1.1.1.1:** 應顯示為 **Yes**
3. **AS Name:** 應顯示為 **Cloudflare**



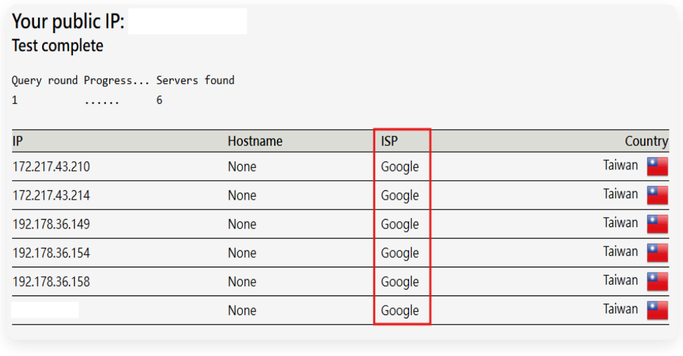
二、 Google Public DNS 驗證方式

Google 主要提供穩定解析，可透過命令列工具確認連線路徑

驗證步驟： 開啟電腦的命令提示字元 (CMD) 或終端機，輸入：`nslookup google.com`

檢查重點：

1. **Server (伺服器):** 應顯示為 **dns.google** 或 **8.8.8.8**
2. **進階測試：** 造訪 `dnsleaktest.com` 並執行 Standard Test，確認結果清單中的 ISP 僅顯示 **Google**



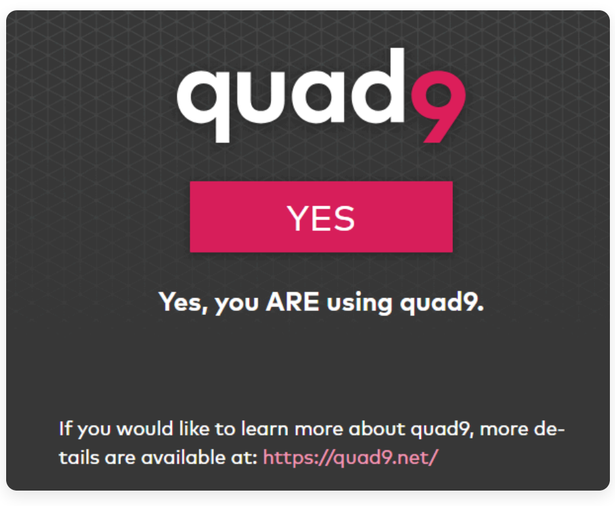
三、 Quad9 驗證方式

Quad9 具備主動攔截惡意軟體的功能，建議進行「攔截測試」來驗證

驗證步驟： 造訪官方測試頁：`https://on.quad9.net`

檢查重點：

1. **狀態確認：** 網頁應直接顯示 **YES**，代表您已受 Quad9 保護
2. **攔截功能測試：** 試著造訪測試網域：`is-it-blocked.quad9.net`
   - **成功：** 瀏覽器應顯示「無法連線」或「被拒絕存取」
   - **失敗：** 若能正常看到網頁內容，代表過濾機制未成功運作



經驗證後未成功運作的檢測

1. **開啟覆蓋所有客戶端的設定：**

   開啟後所有連上路由器的設備都強制使用路由器上的 DNS，避免單一設備自行設定造成的洩漏

2. **清除 DNS 快取：**

   更改設定後，請在電腦執行 `ipconfig /flushdns` 指令，避免舊的解析紀錄干擾測試結果

3. **檢查 IPv6 洩漏：**

   若測試結果顯示為「未配置」，通常是因為設備透過 **IPv6** 連網，而您的 IPv6 DNS 仍使用電信商預設值

4. **瀏覽器設定：**

   部分瀏覽器（如 Chrome/Edge）若開啟了內建的「安全 DNS」，可能會繞過路由器的設定
   測試時請確保瀏覽器的 DNS 設定為「使用目前的服務提供者」