

工作項目

1. 查看某一天 IP 或是 MAC address 的紀錄
2. 以過去的紀錄來分析某個 IP 是否可能產生衝突，並將可能衝突的 IP 列出
3. 將 Perl 程式寫成網頁程式以利使用者方便查詢使用

內容摘要

大家使用網路時多少有遇過 IP 衝突的狀況，但如何找到搶占 IP 的那個人又是一件麻煩的事，因此，本專題設計一個 SNMP 程式，專門撈取 Layer2 Switch 的 MAC table 以及 Layer3 Switch 的 ARP table，再把資料存入 MySQL 資料庫，最後透過一些網頁程式用過濾條件列出可能的潛在衝突可能。程式分成兩個部分，一個是專門定期對 Switch 做 SNMP 撈取資料動作的程式，一個是提供查詢功能的網頁部分，利用已經存在資料庫的表單針對某段日期做取出的程式，取出之後就把同樣且不變的項目只留下一筆，最終比較有沒有 IP 與 MAC 的配對上存在不一樣的資料，就將該筆資料提出。

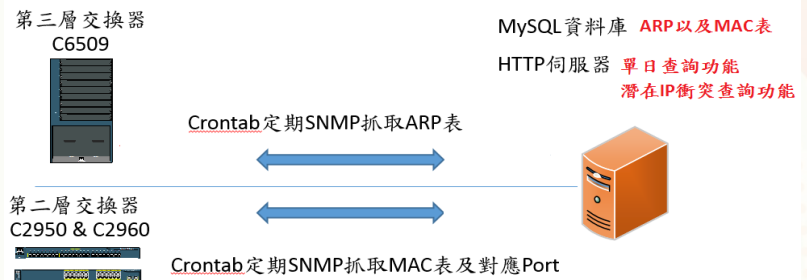


圖 1. 結構圖

實習成果

潛在 IP 衝突查詢的網頁我設計成有今日、7 天、30 天的範圍，而預設載入的值是今日，若我選擇其他範圍就要透過下拉式選單來送出選項，接下來左下方就會呈現出來那個範圍的粗略結果(Result)，每個 IP 分別呈現，另外加上一個名為 detail 的按鈕，這個按鈕的功用就是於右方呈現更詳細的結果(Detail)，而 Detail 呈現的內容為那個 IP 前面選擇時間範圍的全表完整的呈現紀錄，下圖示範以 MAC address 不同以及 Port 不同的時候會顯示的樣子，在多筆資料中可能就一段的時間被他人占用 IP，其他的數據都是正常的保持同 MAC address 與 Port，圖 3 為測試的結果。

ARP table

time range : 2015-08-01 ~ 2015-08-25

id	Date	CoreSWIP	IP	MAC	timestamp	hour
----	------	----------	----	-----	-----------	------

IP	MAC
A	1
A	2
B	3
C	4

A: 2 ▶ A有被盜用的可能
B: 1
C: 1

IP-A ▶ ARP table ▶ MAC table

圖 2. 過濾的方法

實際成功的範例有電子系上的 110 實驗室，IP 發生衝突時，同時仍在執行中的 SNMP 的程式有成功撈到異常的紀錄，這證明這一組程式，在實務上也是可以達成目的的，不過更完整的結果仍需實際程式上線才可以達成。

Result					
	Date	MAC Address	Switch IP	Port Name	
210.240.234.21 detail	2015-08-12	00-15-5d-ea-17-08	192.168.34.245	Gi0/1	
	2015-08-13	00-15-5d-ea-17-08	192.168.34.245	Gi0/1	
	2015-08-14	00-15-5d-ea-17-08	192.168.34.245	Gi0/1	
	2015-08-17	00-15-5d-ea-17-08	192.168.34.245	Gi0/1	
	2015-08-18	00-15-5d-ea-17-08	192.168.34.245	Gi0/1	
210.240.234.45 detail	2015-08-12	00-0c-29-64-d3-5c	192.168.34.245	Fa0/20	
	2015-08-13	00-0c-29-64-d3-5c	192.168.34.245	Fa0/20	
	2015-08-14	00-0c-29-64-d3-5c	192.168.34.245	Fa0/20	
	210.240.234.64 detail	2015-08-12	10-bf-48-d6-4e-44	192.168.34.245	Fa0/20
		2015-08-13	10-bf-48-d6-4e-44	192.168.34.245	Fa0/20
210.240.234.64 detail	2015-08-14	10-bf-48-d6-4e-44	192.168.34.245	Fa0/20	
	2015-08-12	11-11-11-11-11-11	192.168.34.245	Fa0/20	
	2015-08-12	11-11-11-11-11-11	192.168.34.245	Fa0/22	
	2015-08-12	10-bf-48-d6-4e-44	192.168.34.245	Fa0/20	
	2015-08-12	10-bf-48-d6-4e-44	192.168.34.245	Fa0/20	

Detail					
Date	IP Address	MAC Address	Switch IP	Port Name	Timestamp
2015-08-12	210.240.234.64	10-bf-48-d6-4e-44	192.168.34.245	Fa0/20	05:00:01
2015-08-12	210.240.234.64	10-bf-48-d6-4e-44	192.168.34.245	Fa0/20	05:00:01
2015-08-12	210.240.234.64	10-bf-48-d6-4e-44	192.168.34.245	Fa0/20	05:00:01
2015-08-12	210.240.234.64	11-11-11-11-11-11	192.168.34.245	Fa0/20	04:00:01
2015-08-12	210.240.234.64	11-11-11-11-11-11	192.168.34.245	Fa0/22	04:00:01
2015-08-12	210.240.234.64	11-11-11-11-11-11	192.168.34.246	Fa0/22	04:00:01
2015-08-12	210.240.234.64	10-bf-48-d6-4e-44	192.168.34.245	Fa0/20	06:00:01
2015-08-12	210.240.234.64	10-bf-48-d6-4e-44	192.168.34.245	Fa0/20	06:00:01
2015-08-12	210.240.234.64	10-bf-48-d6-4e-44	192.168.34.245	Fa0/20	06:00:01
2015-08-12	210.240.234.64	10-bf-48-d6-4e-44	192.168.34.245	Fa0/20	07:00:01
2015-08-12	210.240.234.64	10-bf-48-d6-4e-44	192.168.34.245	Fa0/20	07:00:01
2015-08-12	210.240.234.64	10-bf-48-d6-4e-44	192.168.34.245	Fa0/20	07:00:01
2015-08-12	210.240.234.64	10-bf-48-d6-4e-44	192.168.34.245	Fa0/20	08:00:01
2015-08-12	210.240.234.64	10-bf-48-d6-4e-44	192.168.34.245	Fa0/20	08:00:01
2015-08-12	210.240.234.64	10-bf-48-d6-4e-44	192.168.34.245	Fa0/20	09:00:01
2015-08-12	210.240.234.64	10-bf-48-d6-4e-44	192.168.34.245	Fa0/20	09:00:01
2015-08-12	210.240.234.64	10-bf-48-d6-4e-44	192.168.34.245	Fa0/20	09:00:01
2015-08-12	210.240.234.64	10-bf-48-d6-4e-44	192.168.34.245	Fa0/20	10:00:01
2015-08-12	210.240.234.64	10-bf-48-d6-4e-44	192.168.34.245	Fa0/20	10:00:01

圖 3. 結果輸出