朝陽科技大學
CHAOYANG UNIVERSITY OF TECHNOLOGY

朝陽科大校園網路管理

經驗分享

朝陽科技大學 電算中心網路組 楊振欣

大綱

1.網卡資訊紀錄.

2.地域網路流量分析.

網卡資訊紀錄

起源:

1.校園所有網路的架構在Layer 2的網路環境,為了方便找尋主機的使用位置.

2.網路管理有時候要細部追查那個MAC從那上來, 但登入到交換器時使用者已經離線, 無從查起, 因些設定交換器主動記錄MAC.

3.便利其他同仁查詢相關資訊.

網卡資訊紀錄

建置環境:

1.校園內交換器提供MAC NOTIFICATION的網路設備.

2.snmptrapd Server, perl script(處理mac notification的資訊,並轉進資料庫).

3.Postgresql DB.

網卡資訊紀錄

Cisco交換器設定:

switch(config)#mac-address-table notification interval **300**
#設定多久檢查一次mac-address 的異動

switch(config)#mac-address-table history-size **100**
#設定要在交換器上儲存幾筆歷史記錄供 查詢

switch(config)#mac-address-table notification
#啟用功能

網卡資訊紀錄

Cisco交換器設定:

switch(config)#interface fastethernet 0/1
switch(config-if)#snmp trap mac-notification **added | removed**
當介面學到的MAC或移除(超過時效)的MAC都送出trap

switch(config)#snmp-server host 163.17.x.x **cyutxx**
設定啟用snmptrap 目地主機位置

switch(config)#snmp-server enable traps mac-notification
設定啟用snmptrap mac-notification的功能

網卡資訊紀錄

snmptrapd資訊:

2011-10-27 23:30:25 T2-8-0.cyut.edu.tw [10.1.1.106] (via UDP: [10.1.1.106]:50682) TRAP, SNMP v1, community cyutR1trap
SNMPv2-SMI::enterprises.9.9.215.2 Enterprise Specific Trap (1) Uptime: 95 days, 12:27:21.22
SNMPv2-SMI::enterprises.9.9.215.1.1.8.1.2.72 = Hex-STRING: **01 00 E4 00 40 CA 6B 39 54 00 05** 01 00 E4 00 E0
98 4D 1C 4B 00 08 01 00 E4 00 1E E5 AF FA 77 00
05 01 00 E4 00 40 CA 74 7C D9 00 08 01 00 E4 1C
C1 DE 80 05 C4 00 0A 01 00 E4 00 09 6B 09 C1 AE
00 05 01 00 E4 E4 1F 13 30 73 40 00 05 01 00 E4
00 48 54 5A FD 22 00 05 01 00 SNMPv2-SMI::enterprises.9.9.215.1.1.8.1.3.72 = Timeticks: (825284122) 95 days, 12:27:21.22

01 狀態

00 E4 Vlan

00 40 CA 6B 39 54 mac

00 slot

05 port

網卡資訊紀錄

資料庫:

資料行 | 索引? | 約束? | 觸發器? | 規則?

Column	類型	不允許空值	預設值	約束	功能	註釋
hostname	character(30)	NOT NULL			瀏覽 修改 特權 刪除	
time	timestamp without time zone	NOT NULL			瀏覽 修改 特權 刪除	
vlan	character(5)	NOT NULL			瀏覽 修改 特權 刪除	
mac	macaddr	NOT NULL			瀏覽 修改 特權 刪除	
port	character(3)	NOT NULL			瀏覽 修改 特權 刪除	
status	character(12)	NOT NULL			瀏覽 修改 特權 刪除	

瀏覽 | 選取 | 插入 | 空 | 刪除 | 加入新資料欄 | 修改

網卡資訊紀錄

操作介面：

朝陽科技大學mac&device歷史查詢

為加快查詢請務必輸入MAC或選設備名稱

開始日期 2012 年 12 月 16 日 0 時 結束日期 2012 年 12 月 16 日 15 時

設備 G-8-0.cyut.edu.tw Port 10 VLAN 215 關鍵字(MAC): 絕對 顯示全部 查詢

DEVICE	時間	VLAN	MAC	PORT	STATUS
G-8-0.cyut.edu.tw	2012-12-16 02:08:01	215	00:90:cc:c5:40:76	10	NOW REMOVE
G-8-0.cyut.edu.tw	2012-12-16 00:02:01	215	00:90:cc:c5:40:76	10	NOW ADD
G-8-0.cyut.edu.tw	2012-12-16 00:02:01	215	00:90:cc:c5:40:76	10	NOW ADD
G-8-0.cyut.edu.tw	2012-12-16 00:02:02	215	00:90:cc:c5:40:76	10	NOW REMOVE
G-8-0.cyut.edu.tw	2012-12-16 00:02:03	215	00:90:cc:c5:40:76	10	NOW REMOVE
G-8-0.cyut.edu.tw	2012-12-16 00:10:00	215	00:90:cc:c5:40:76	10	NOW ADD
G-8-0.cyut.edu.tw	2012-12-16 00:10:01	215	00:90:cc:c5:40:76	10	NOW ADD
G-8-0.cyut.edu.tw	2012-12-16 00:10:03	215	00:90:cc:c5:40:76	10	NOW REMOVE
G-8-0.cyut.edu.tw	2012-12-16 00:10:04	215	00:90:cc:c5:40:76	10	NOW REMOVE
G-8-0.cyut.edu.tw	2012-12-16 00:13:19	215	00:90:cc:c5:40:76	10	NOW ADD
G-8-0.cyut.edu.tw	2012-12-16 00:13:19	215	00:90:cc:c5:40:76	10	NOW ADD
G-8-0.cyut.edu.tw	2012-12-16 00:13:21	215	00:90:cc:c5:40:76	10	NOW REMOVE
G-8-0.cyut.edu.tw	2012-12-16 00:13:21	215	00:90:cc:c5:40:76	10	NOW REMOVE
G-8-0.cyut.edu.tw	2012-12-16 00:20:07	215	00:90:cc:c5:40:76	10	NOW ADD
G-8-0.cyut.edu.tw	2012-12-16 00:20:08	215	00:90:cc:c5:40:76	10	NOW ADD
G-8-0.cyut.edu.tw	2012-12-16 00:20:12	215	00:90:cc:c5:40:76	10	NOW REMOVE

地域網路流量分析

起源:

1.2012/12 月接獲圖書館反應,論文大量被下載利用(CN國家).

2.往常分析資料並未涵蓋目的位置國家,希望可以分析利用.

地域網路流量分析

Address資料來源:

IANA=>APNIC

http://www.potaroo.net/tools/ipv4/index.html

http://bgp.potaroo.net/stats/

AFRINIC

APNIC(亞太地區)

ARIN

RIPENCC

LACNIC

地域網路流量分析

處理方式:

內容

apnic|AU|ipv4|134.178.0.0|65536|19890701|allocated
apnic|JP|ipv4|134.180.0.0|65536|19890701|allocated
apnic|CN|ipv4|134.196.0.0|65536|19920327|allocated
apnic|TW|ipv4|134.208.0.0|65536|19890724|allocated
apnic|AU|ipv4|134.211.0.0|65536|19890724|allocated

摘要

CN,134.196.0.0/16

.....

地域網路流量分析

比對方法:

iptables

target use log

-j LOG --log-prefix "This is CN"

地域網路流量分析

分析結果:

中國IP	流量(M)
111.161.54.10	791
114.249.233.9	262
124.115.10.64	230
124.115.10.68	223
124.115.4.215	221
183.69.206.27	199
118.195.65.64	163
117.135.129.73	150
.....	