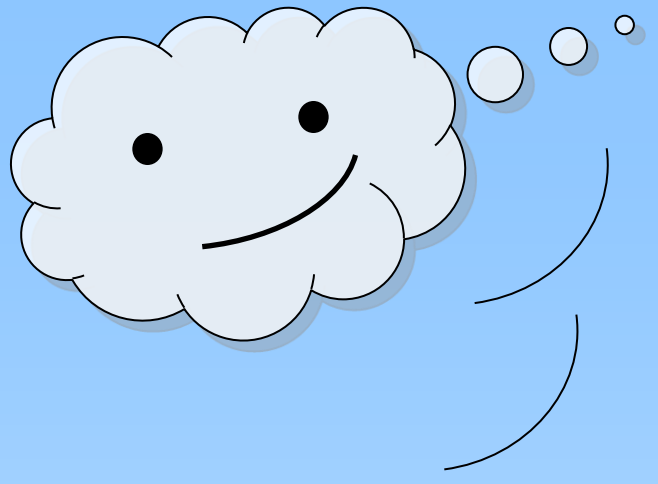
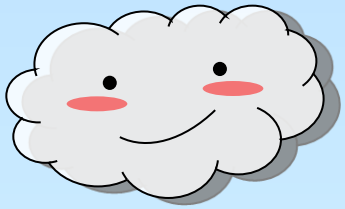


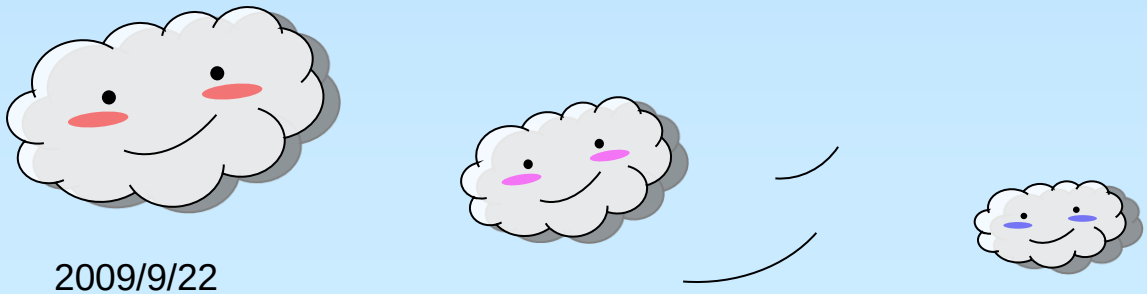
網路封包、流量解析與監控

CCU Campus Network Association
Wei-Shiang Huang 黃韋翔
maximum@mail.cna.ccu.edu.tw



2009/9/22

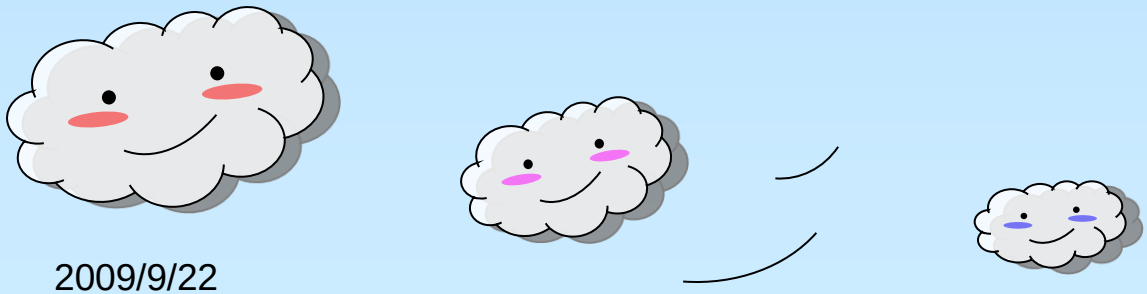
流量監控簡介



2009/9/22

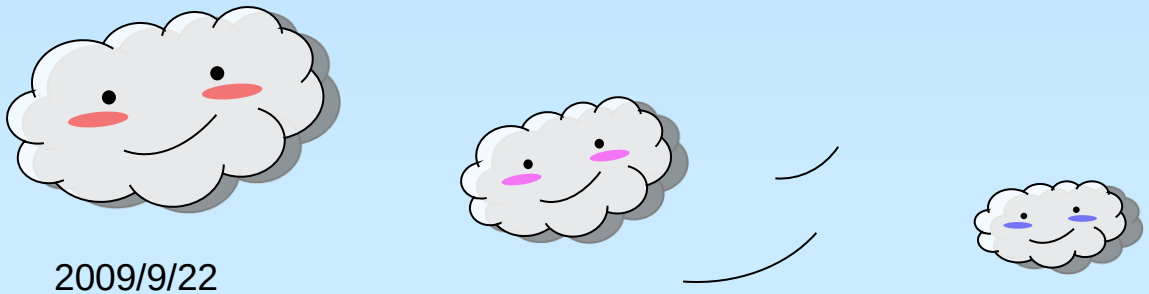
流量監控的背景

- 由於網際網路的蓬勃發展，對外連線頻寬的增加，加上應用系統類型的多樣化，使得對外網路的頻寬管理及流量監控與分析變得日益重要。



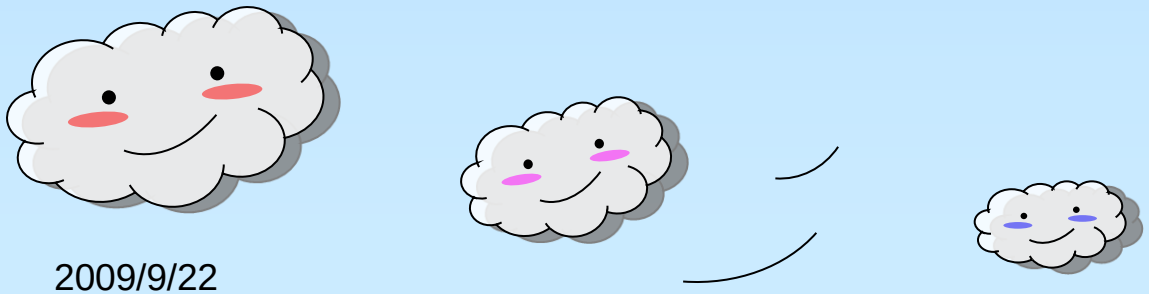
流量監控的好處(1/2)

- 提升網路效能，降低流量負荷
  - 資源是有限，不可能無限制的提供頻寬，透過流量監控可以對於找出消耗較多頻寬的使用者。
- 網路效益評估
  - 了解網路的瓶頸，事先規劃解決方案。

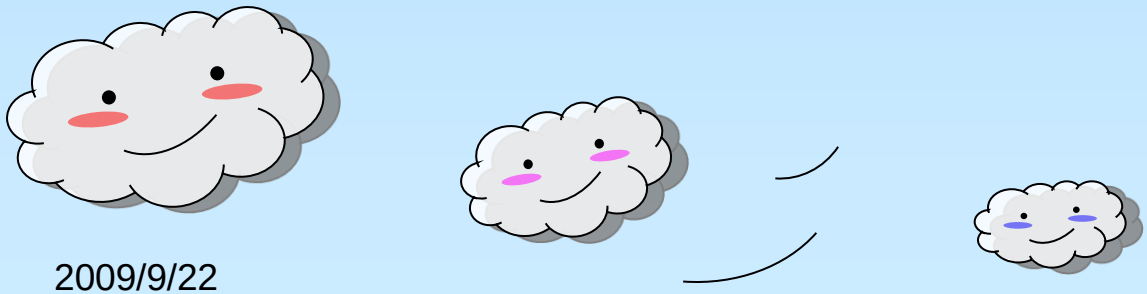


流量監控的好處(2/2)

- 方便網路資訊管理
  - 清楚的流量使用情形分析
  - 需求統計，提供解決方案
- 提升網路安全
  - 異常流量分析
    - 病毒與異常流量分析



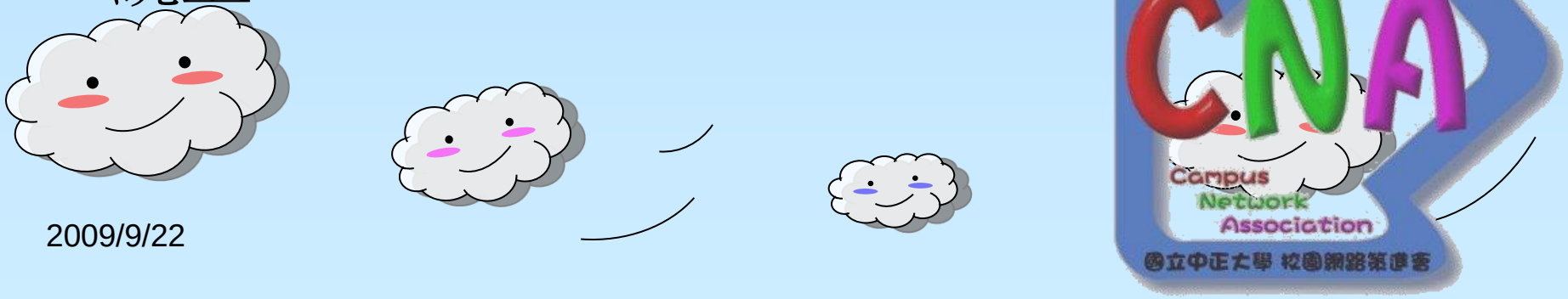
監測工具簡介



2009/9/22

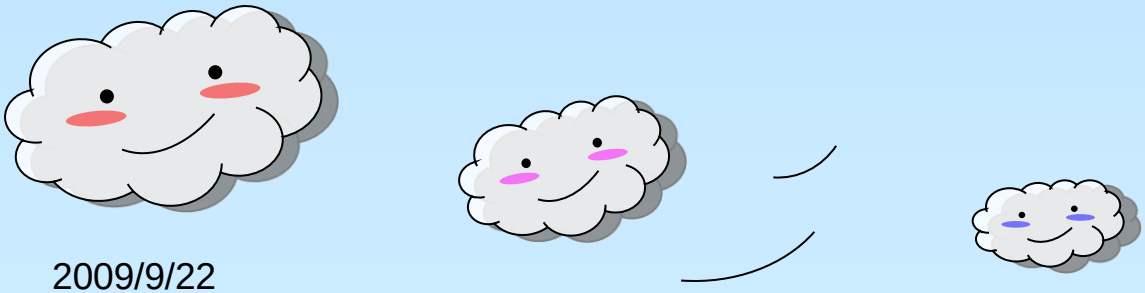
MRTG簡介(1/2)

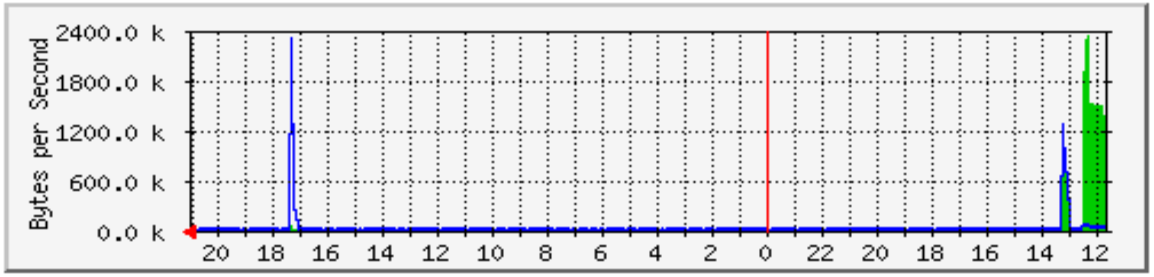
- MRTG（Multi Router Traffic Grapher）是一個監控網路流量負載的工具軟體， 透過SNMP協定從設備得到流量資訊，並將流量以圖形的方式呈現在網頁上。
- MRTG是個多平臺軟體，可以運行在Linux、Windows NT/2000/XP、FreeBSD等作業系統上。



MRTG介紹(2/2)

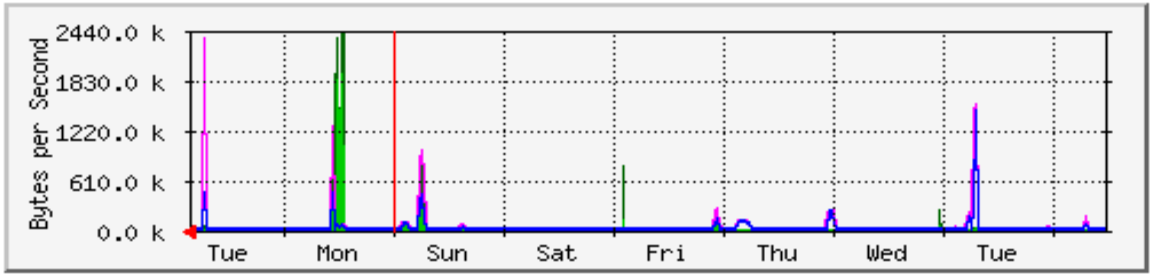
- MRTG主要分為兩個部份的程式組成
  - SNMP
    - 可透過系統內建的SNMP軟體(如bsnmpd)來傳送相關流量資訊。
  - MRTG
    - MRTG從SNMP接收到流量資料後，即會依照設定檔定時繪出即時流量狀態圖





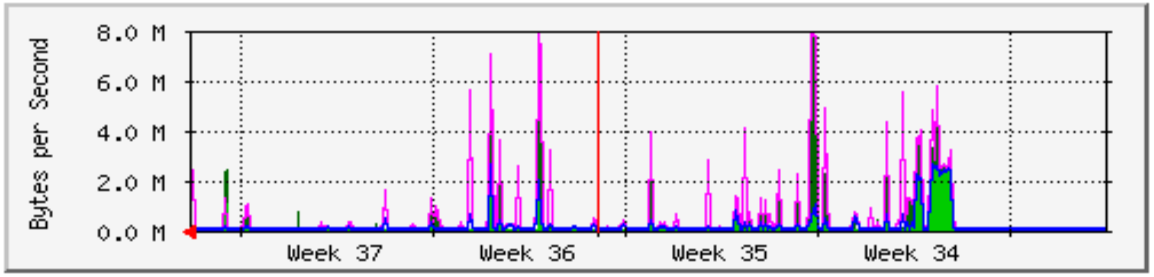
	最大	平均	目前
流入	0.0 B/秒 (0.0%)	0.0 B/秒 (0.0%)	0.0 B/秒 (0.0%)
流出	0.0 B/秒 (0.0%)	0.0 B/秒 (0.0%)	0.0 B/秒 (0.0%)

每週 圖表 (30 分鐘 平均)

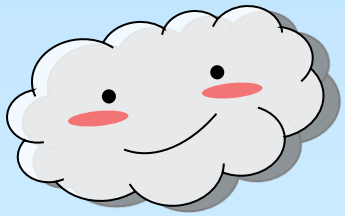


	最大	平均	目前
流入	2439.3 kB/秒 (19.5%)	20.6 kB/秒 (0.2%)	33.0 B/秒 (0.0%)
流出	2332.1 kB/秒 (18.7%)	13.8 kB/秒 (0.1%)	16.0 B/秒 (0.0%)

每月 圖表 (2 小時 平均)



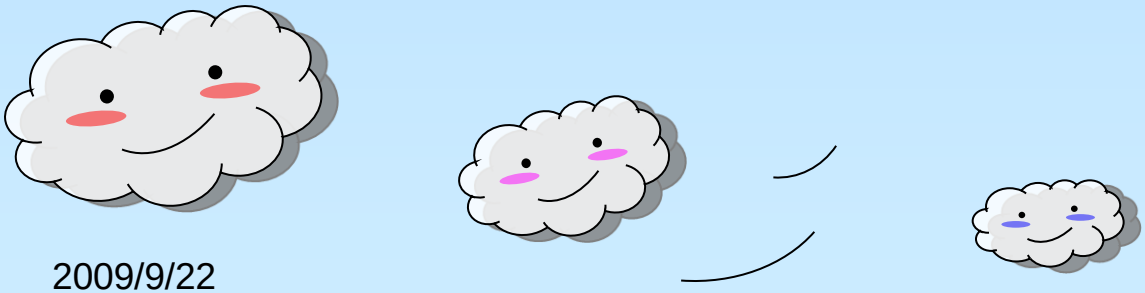
	最大	平均	目前
流入	7715.2 kB/秒 (61.7%)	108.5 kB/秒 (0.9%)	31.0 B/秒 (0.0%)



2009/9/22

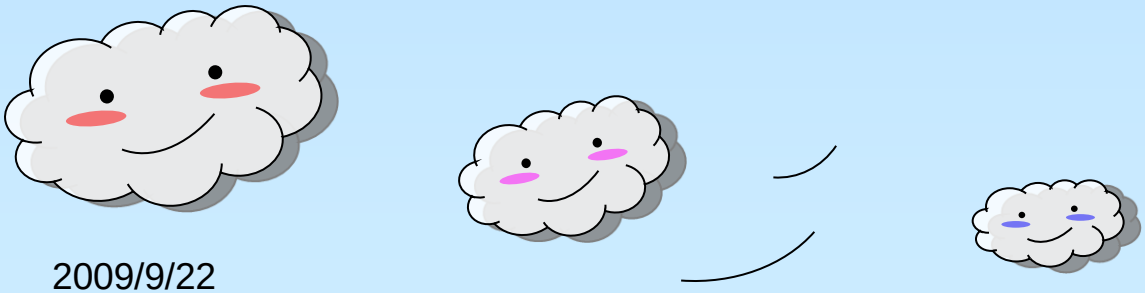
NTOP簡介(1/2)

- NTOP是一種功能類似Sniffer的網路監控工具。將它安裝在網路上後可以顯示網路的總流量，網段內各機器的流量，及各種服務所佔用的流量等等。甚至還能列出每個節點網路頻寬使用率，其所顯示的網路使用情況比MRTG更加詳細。

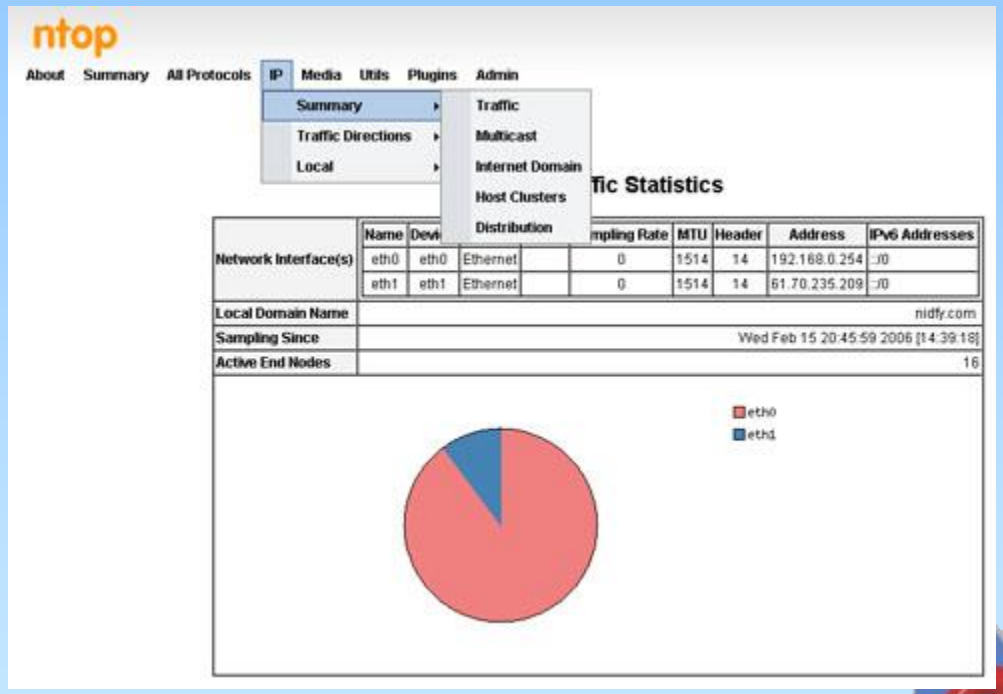


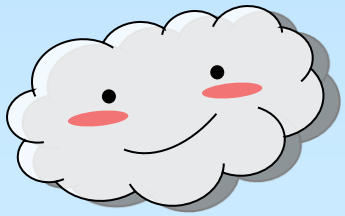
NTOP簡介(2/2)

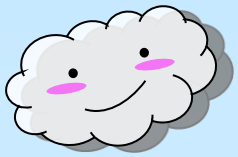
- 透過NTOP分析網路流量，可以得知網路上存在的問題；或判斷是否有駭客正在攻擊網路系統；還可以很方便地顯示出不同的網路協定、或顯示佔用大量頻寬的主機、各資料包的發送時間、傳遞資料包的延時等詳細資訊。



NTOP示意圖



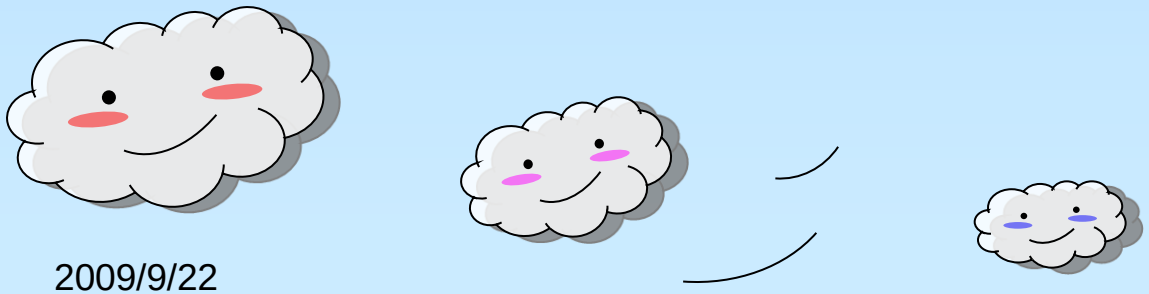




2009/9/22

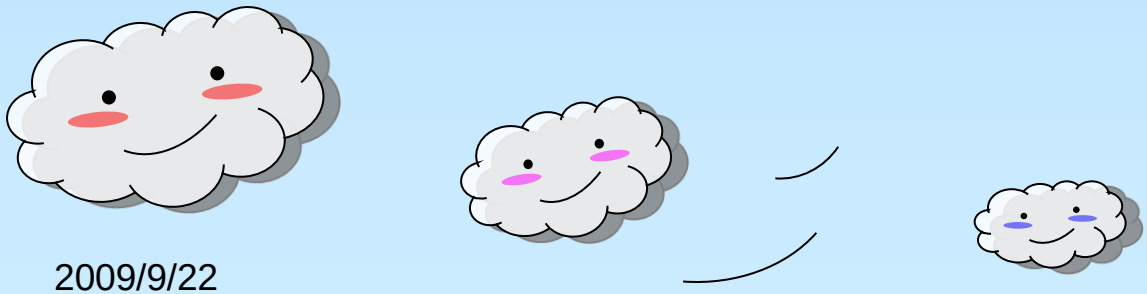
Cisco Netflow簡介(1/2)

- Cisco® NetFlow技術是Cisco IOS設備內嵌的一個功能。NetFlow資料記錄中包含了來源地址和目的地址，端到端會話所使用的協議和連接埠等資訊。



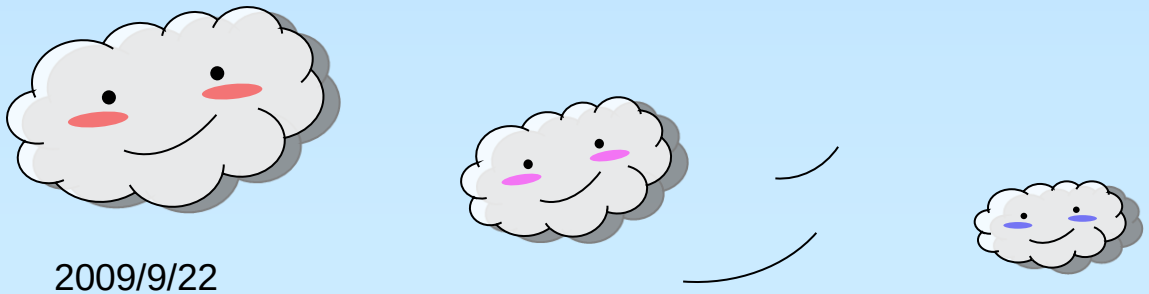
Cisco Netflow簡介(2/2)

- MRTG以及其它相似的工具提供的訊息僅侷限於接口的統計資料，卻不提供有關來源主機和目的主機的統計資料、封包明細、協定以及IP通訊的其它資料。

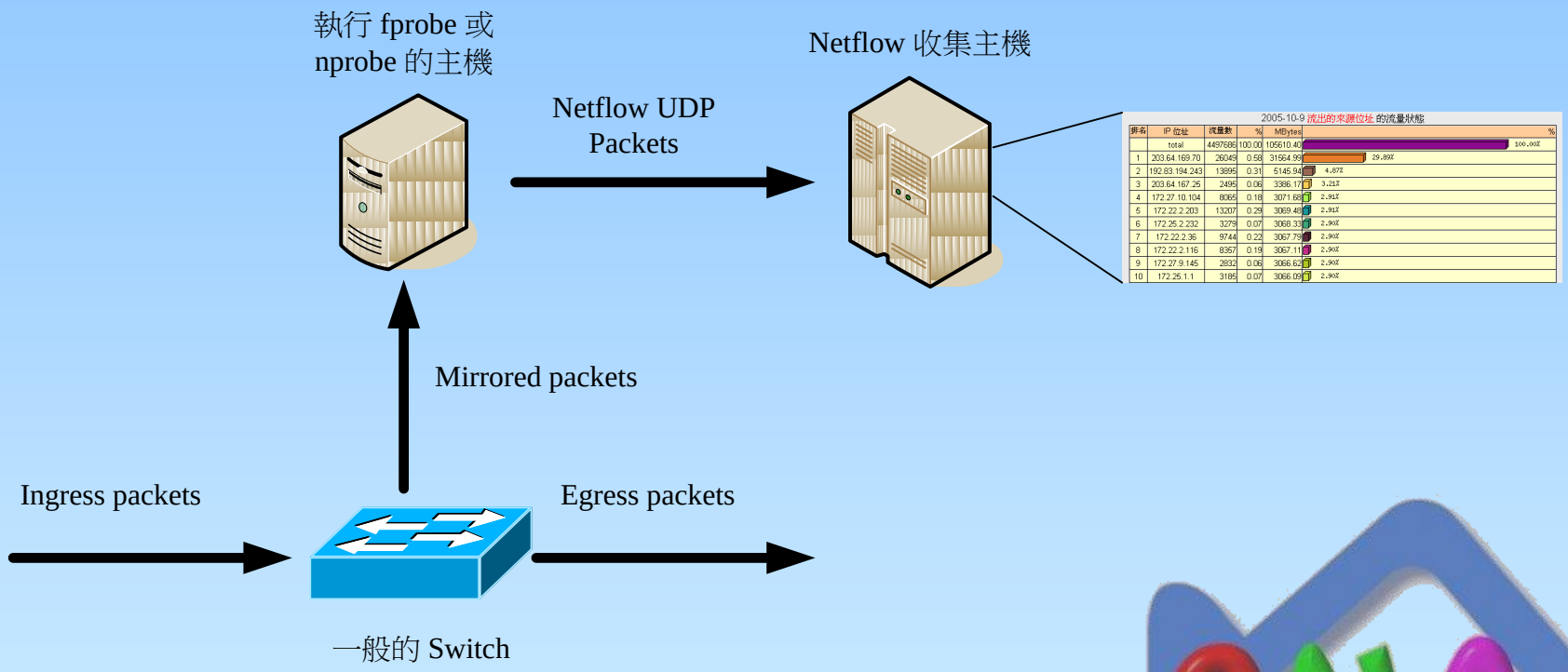


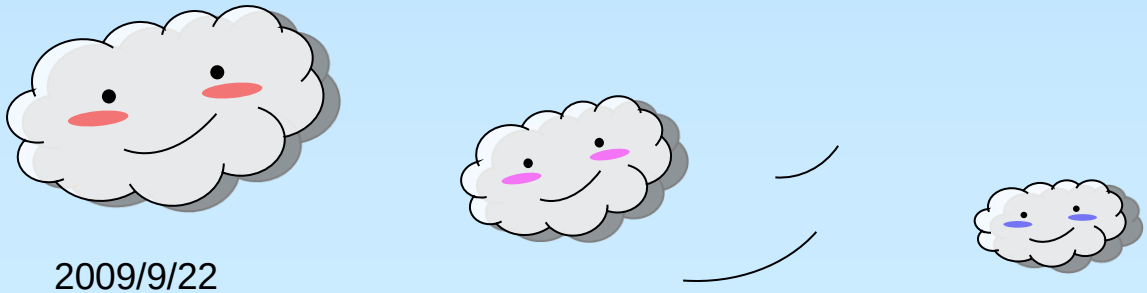
Netflow 運作方式

- 1.Cisco Router or 具有Port Mirror功能的設備。
- 2.接收流量的主機一台。
- 3.Packet Summary。



Netflow 的運作模式(1/2)

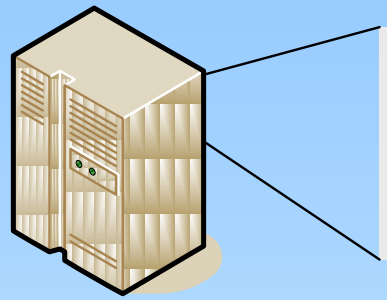




2009/9/22

Netflow 的運作模式(2/2)

Netflow 收集主機



2005-10-9 流出的來源位址 的流量狀態

排名	IP 位址	流量數	%	MBytes	%
	total	4497686	100.00	105610.40	100.00%
1	203.64.169.70	26049	0.58	31564.99	29.89%
2	192.83.194.243	13895	0.31	5145.94	4.87%
3	203.64.167.25	2495	0.06	3386.17	3.21%
4	172.27.10.104	8065	0.18	3071.68	2.91%
5	172.22.2.203	13207	0.29	3069.46	2.91%
6	172.25.2.232	3279	0.07	3068.33	2.90%
7	172.22.2.36	9744	0.22	3067.79	2.90%
8	172.22.2.116	8357	0.19	3067.11	2.90%
9	172.27.9.145	2832	0.06	3066.62	2.90%
10	172.25.1.1	3185	0.07	3066.09	2.90%

Netflow UDP Packets

Ingress packets

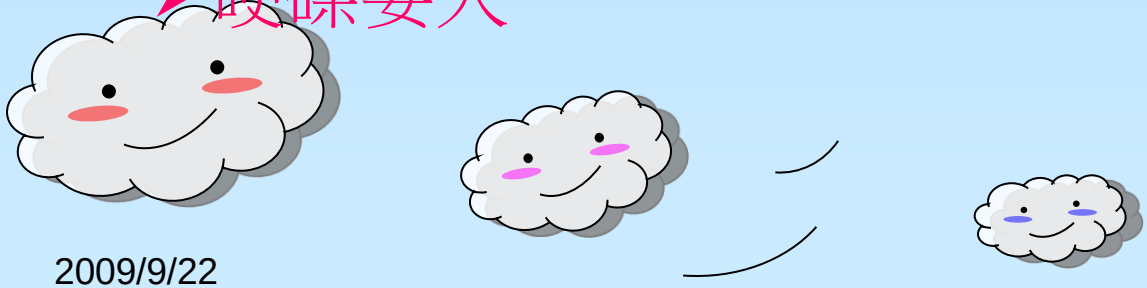
Egress packets

支援 Netflow 的 Router 或 L3 Switch

2009/9/22

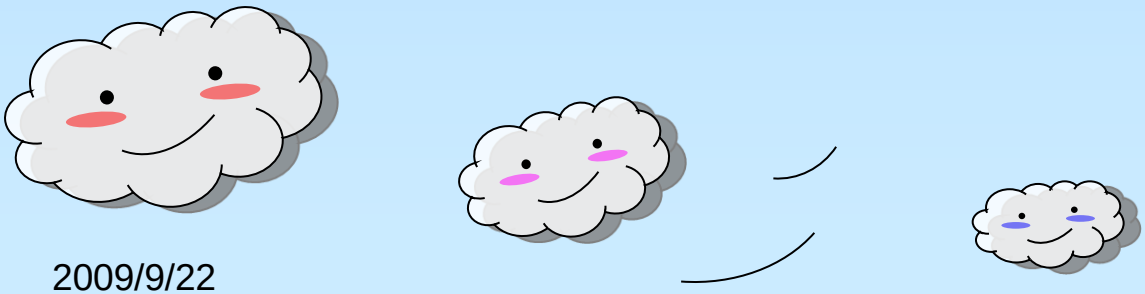
Netflow 的硬體需求

- 製造 flow 的工具
  - Cisco 高階router
  - NTOP 以及一顆有 Port Mirror 功能的 Switch
- 計算 flow 的工具
  - 一台 PC
  - 記憶體要大
  - 硬碟要大



產生 Flow 的軟體

- flow-tools
- NetflowExporter
- NTOP



Flow-tools示意圖

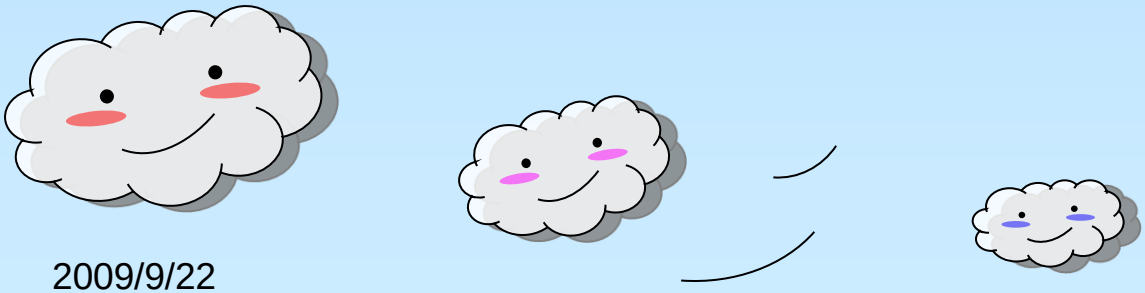
gateway.dorm.ccu.edu.tw [157x47]

連線(C) 編輯(E) 檢視(V) 視窗(W) 選項(O) 說明(H)

```
Start            End              Sif   SrcIPaddress    SrcP  DIf   DstIPaddress    DstP    P Fl Pkts       Octets

0910.00:00:40.152 0910.00:00:40.152 137   61.137.90.105   6000  140   140.123.235.115 8090  6   0  1          46
0910.00:10:51.276 0910.00:10:51.276 137   92.153.245.41   6881  140   140.123.235.115 17123 17  0  1          95
0910.00:11:31.284 0910.00:11:31.284 137   60.42.103.204   13914 140   140.123.235.115 17123 17  0  1          90
0910.00:11:35.893 0910.00:11:35.893 137   90.51.214.204   43918 140   140.123.235.115 17123 17  0  1          95
0910.00:26:44.038 0910.00:26:44.038 137   112.78.13.68    6000  140   140.123.235.115 2967  6   0  1          46
0910.00:31:36.266 0910.00:31:36.266 137   60.42.103.204   13914 140   140.123.235.115 17123 17  0  1          90
0910.00:38:19.088 0910.00:38:19.088 137   190.84.19.64    3015  140   140.123.235.115 4899  6   0  1          48
0910.00:39:16.816 0910.00:39:16.816 137   93.8.21.247     36789 140   140.123.235.115 17123 17  0  1          95
0910.00:45:40.869 0910.00:45:40.869 137   82.241.89.168   11151 140   140.123.235.115 17123 17  0  1          95
0910.00:46:59.158 0910.00:46:59.158 137   190.157.93.104  60979 140   140.123.235.115 4899  6   0  1          48
0910.00:51:07.089 0910.00:51:10.161 137   78.8.208.6      1896  140   140.123.235.115 3050  6   0  2          96
0910.00:51:40.350 0910.00:51:40.350 137   60.42.103.204   13914 140   140.123.235.115 17123 17  0  1          90
0910.00:51:50.076 0910.00:51:50.076 137   60.173.10.213   6000  140   140.123.235.115 1433  6   0  1          46
0910.01:03:36.442 0910.01:03:36.442 137   58.117.128.18   6000  140   140.123.235.115 2967  6   0  1          46
0910.01:11:37.657 0910.01:11:37.657 137   82.247.222.46   45124 140   140.123.235.115 17123 17  0  1          95
0910.01:19:07.721 0910.01:19:07.721 137   221.195.72.77   6000  140   140.123.235.115 2967  6   0  1          46
0910.01:31:51.532 0910.01:31:51.532 137   60.42.103.204   13914 140   140.123.235.115 17123 17  0  1          90
0910.01:48:10.680 0910.01:48:19.640 137   118.161.247.160 4392  140   140.123.235.115 808   6   0  3          144
0910.01:56:55.458 0910.01:56:55.458 137   93.11.50.245    10203 140   140.123.235.115 17123 17  0  1          95
0910.02:04:12.472 0910.02:04:12.472 137   62.147.159.107  62355 140   140.123.235.115 17123 17  0  1          95
0910.02:12:33.965 0910.02:12:33.965 137   87.226.91.60    26102 140   140.123.235.115 17123 17  0  1          90
0910.02:23:31.494 0910.02:23:31.494 137   90.42.156.251   10964 140   140.123.235.115 17123 17  0  1          95
0910.02:25:57.017 0910.02:25:57.017 137   88.183.178.128  55555 140   140.123.235.115 17123 17  0  1          95
0910.02:32:37.537 0910.02:32:37.537 137   87.226.91.60    26102 140   140.123.235.115 17123 17  0  1          90
0910.02:34:38.051 0910.02:34:38.051 137   140.136.144.113 24332 140   140.123.235.115 22    6   0  1          48
0910.02:35:52.152 0910.02:35:54.904 137   80.20.108.224   44448 140   140.123.235.115 22    6   0  2          120
0910.02:40:49.562 0910.02:40:49.562 137   190.128.125.210 3637  140   140.123.235.115 4899  6   0  1          64
0910.02:41:52.662 0910.02:41:52.662 137   222.73.204.18   6000  140   140.123.235.115 1433  6   0  1          46
0910.02:44:57.305 0910.02:44:57.305 137   212.156.84.98   1031  140   140.123.235.115 137   17  0  1          78
0910.02:48:23.013 0910.02:48:26.021 137   210.189.109.227 53096 140   140.123.235.115 21    6   0  2          120
0910.03:01:07.371 0910.03:01:07.371 137   219.150.187.30  6000  140   140.123.235.115 1433  6   0  1          46
0910.03:17:48.050 0910.03:17:48.050 137   60.173.10.213   6000  140   140.123.235.115 1433  6   0  1          46
0910.03:25:20.160 0910.03:25:20.160 137   59.60.151.7     25511 140   140.123.235.115 60786 6   0  1          46
0910.03:28:26.074 0910.03:28:26.074 137   88.161.228.248  59959 140   140.123.235.115 17123 17  0  1          95
0910.03:33:29.368 0910.03:33:29.368 137   219.150.187.30  6000  140   140.123.235.115 1433  6   0  1          46
0910.03:34:20.638 0910.03:34:20.638 137   79.83.31.219    25379 140   140.123.235.115 17123 17  0  1          95
0910.03:46:35.984 0910.03:46:35.984 137   123.196.116.12  6000  140   140.123.235.115 2967  6   0  1          46
0910.03:48:22.619 0910.03:48:22.619 137   200.85.95.44    27983 140   140.123.235.115 4899  6   0  1          48
0910.04:00:23.188 0910.04:00:23.188 137   125.219.128.15  6000  140   140.123.235.115 2967  6   0  1          46
0910.04:05:23.411 0910.04:05:23.411 137   61.191.191.73   6000  140   140.123.235.115 2967  6   0  1          46
0910.04:14:53.442 0910.04:14:53.442 137   82.121.202.104  33272 140   140.123.235.115 17123 17  0  1          95
0910.04:16:57.537 0910.04:16:57.537 137   91.205.41.176   80    140   140.123.235.115 32851 6   0  1          48
--More--(byte 5200)
 0 www   1 netflow /  2 mail  3 dsf  4 project  5 csh  6 csh  8 csh
 {0.00 0.00 0.00}  gateway.dorm.ccu.edu.tw                                  2009-09
```

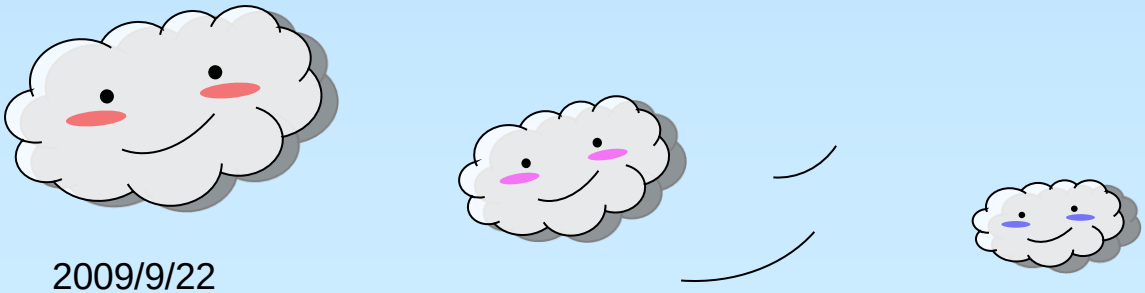
蠕蟲即時偵測



2009/9/22

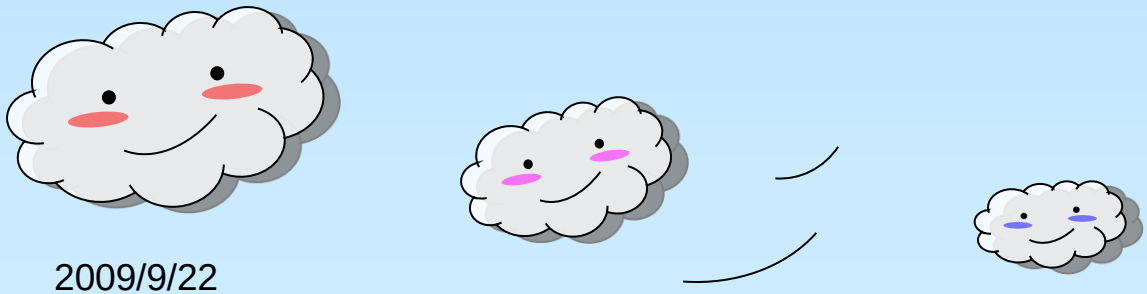
蠕蟲偵測技術簡介

- 台灣學術網路於2001 年 8月份遭嚴重病毒攻擊，各區網中心所受波及影響很大。近年來，網路攻擊行為與Internet Worm 造成嚴重的網路威脅，解決網路攻擊並提出一套有效即時預警系統是迫切而且必要的。透過這套技術我們可以有效的偵測到Code Red、Nimda。



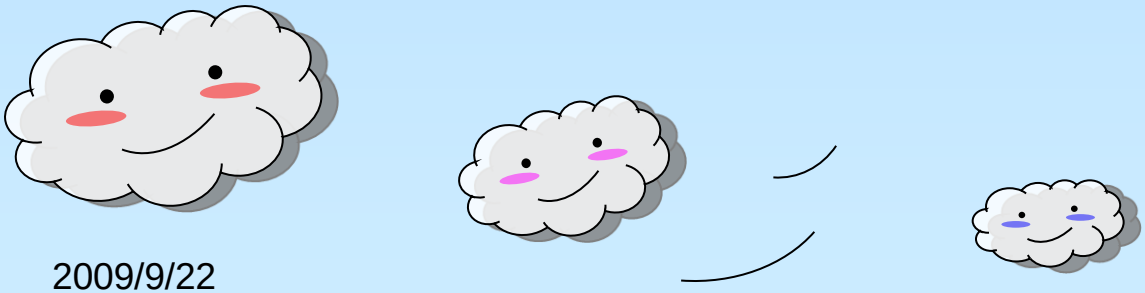
Code Red 簡介(1/2)

- Code Red 是一隻會自我繁殖入侵系統的惡意程式碼，利用微軟IIS WebServer 的安全性漏洞入侵，並在受害者主機上自我繁殖，入侵後留下後門，同時產生600 個執行緒，隨機產生IP 嘗試入侵沒有安裝修補程式的IIS WEB伺服器。



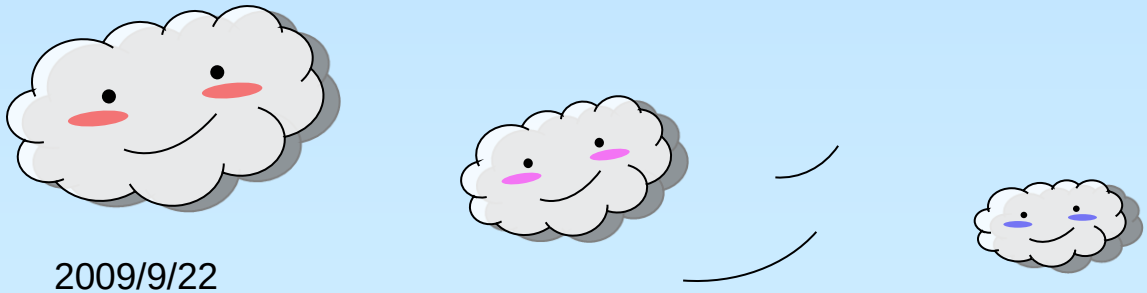
Code Red 簡介(2/2)

- 被植入Code Red 的主機可能同時多次掃瞄同一台主機，沒有受到感染的主機可能會成為Code Red 的攻擊目標，受到DOS(denial of service)的攻擊。由於持續變換目地IP 位置，消耗路由器資源，導致低階路由器當機，中高階路由器效能下降。



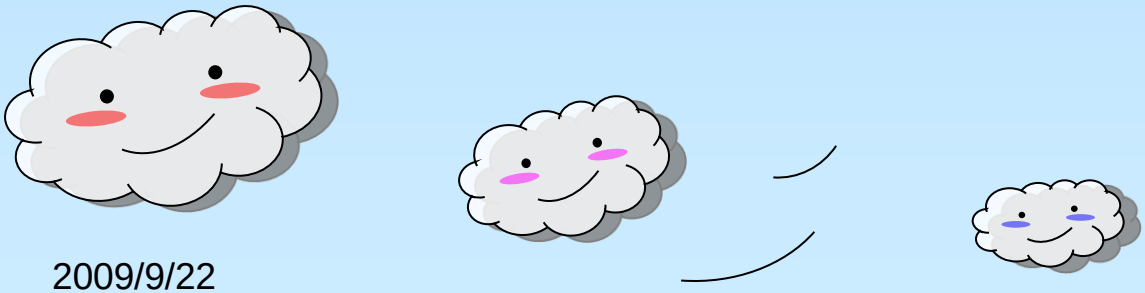
Nimda 簡介(1/2)

- Nimda (別名W32/Nimda.A@mm, I-Worm.Nimda, Readme,Readme.exe 等)會利用現有網站提供受感染檔案下載，並利用end user 的主機掃描其他有漏洞的電腦，這使得Nimda 可輕易地入侵受防火牆屏障的intranet，強大的破壞力透過網際網路在全球迅速傳播，破壞力不遜於Code Red。



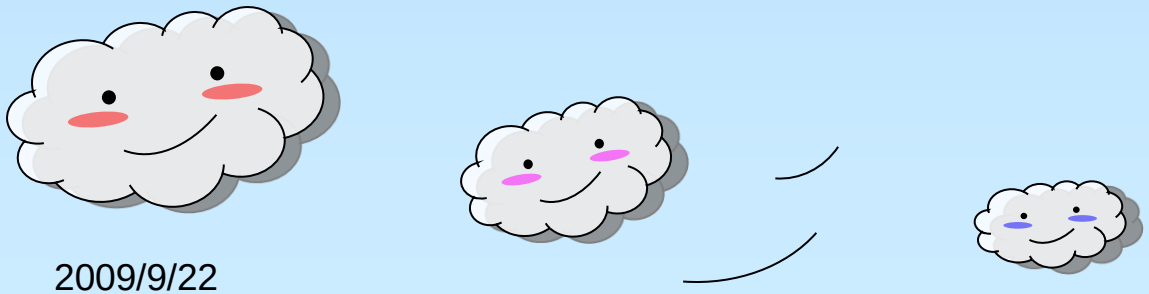
Nimda 簡介

- Nimda 會針對系統漏洞進行複製與散播，將C 磁碟機設為資源共享，任意複製、修改、刪除重要檔案文件、破壞受感染的系統，並加重網路承載。另外因為使用網路芳鄰，因此除了路由器效能受影響外，LAN 的效能也受影響。



流量特徵

- 因worm 的特性將造成異常流量，因此，應先找出正常與異常流量之特徵，才可比較分析何處發生worm 的感染。依照worm 所利用的安全弱點型式，有直接和間接的流量特徵。

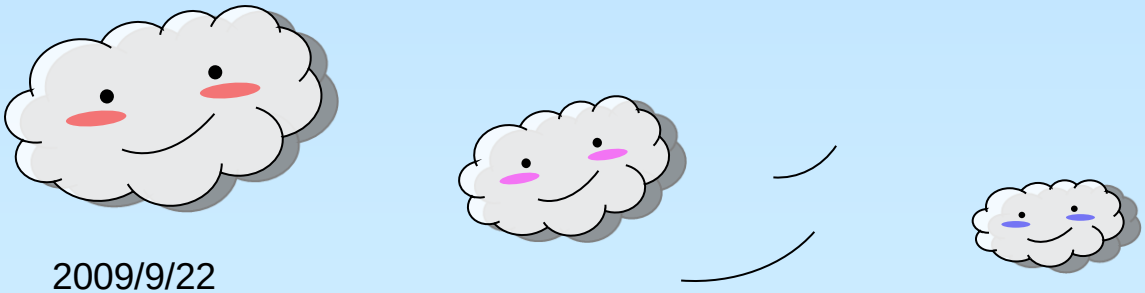


流量特徵

- 直接流量特徵為攻擊者對受害者的直接連線，利用作業系統漏洞(例：Remote Procedure Call)、伺服器的漏洞(例：透過 Web Server 入侵)。
- 已被感染的主機會產生大量對外攻擊的連線，因此可以先找出封包數量或flow 數量異常之主機，再分析相關之資料。

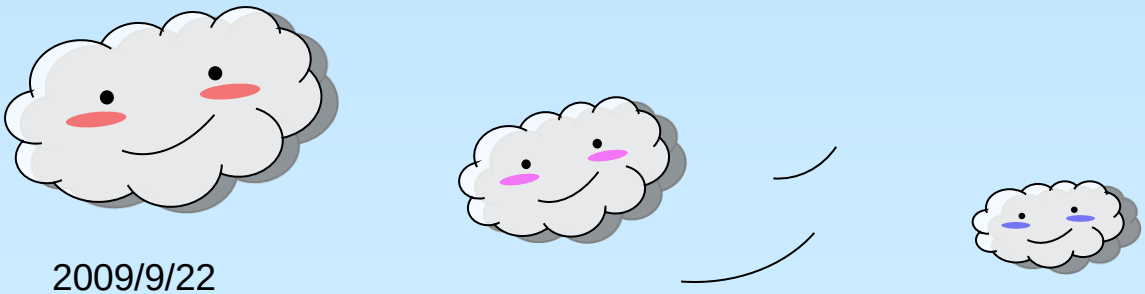
其他蠕蟲

- 疾風病毒
  - Port 445
- 殺手病毒
  - Port 135

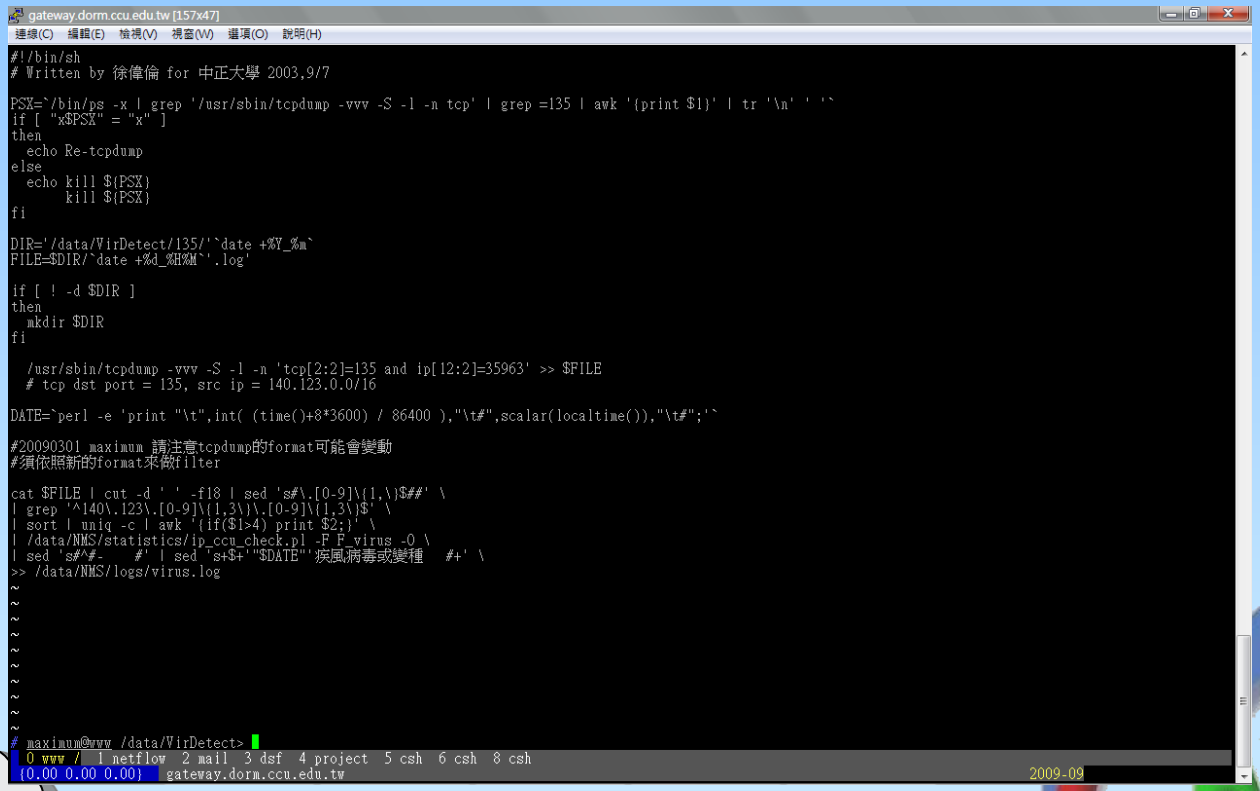


偵測工具(1/3)

- Tcpdump
- 分析程式(可利用perl或shell script來撰寫)

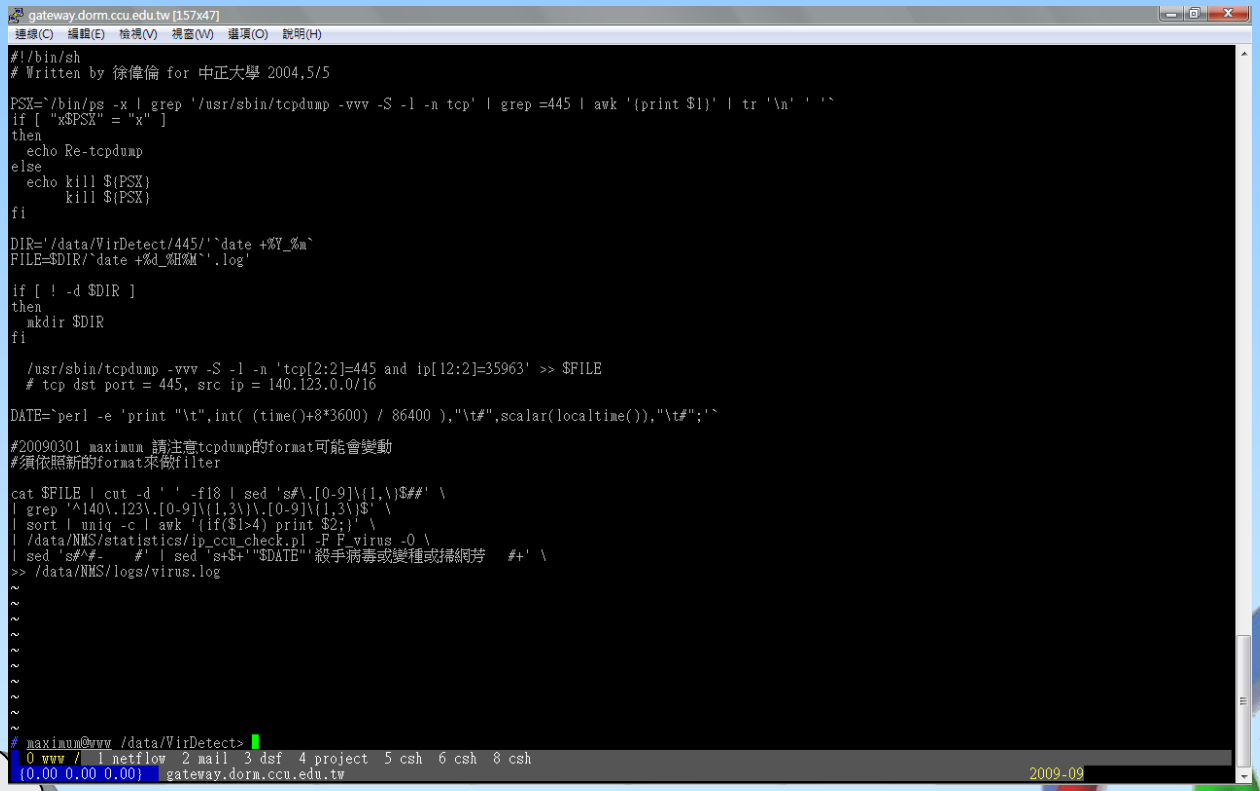


偵測工具(2/3)



2009/9/22

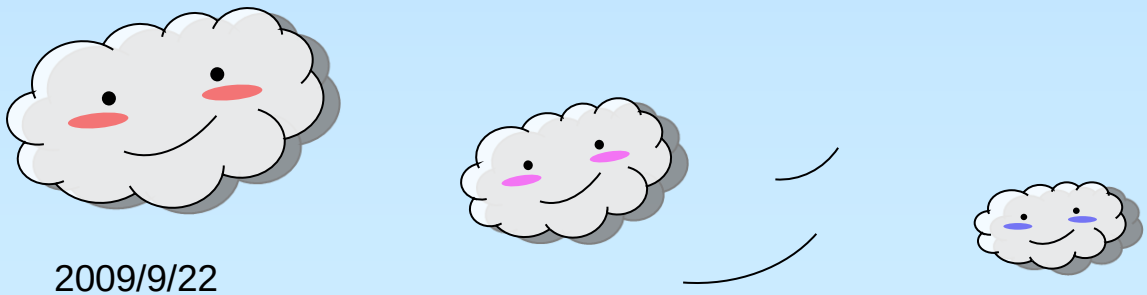
偵測工具(3/3)



2009/9/22

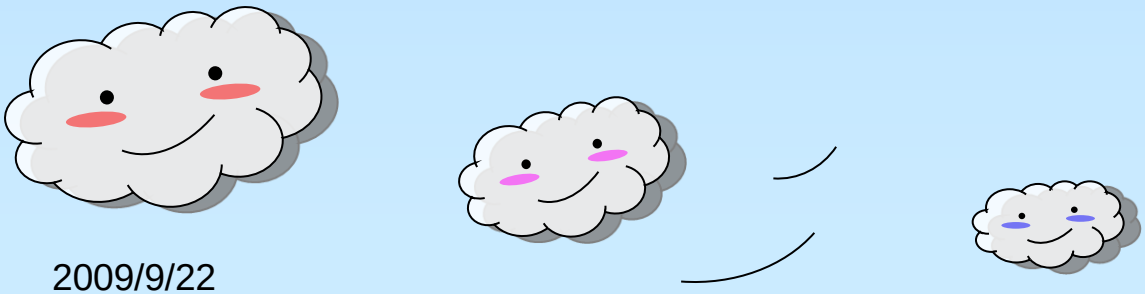
異常流量

```
22:41:54.159790 IP (tos 0x0, ttl 126, id 45576, offset 0, flags [DF], proto TCP (6), length 48) 140.123.122.12.3710 > 140.123.241.21.135: S, cksum 0x02a
rrect), 934787764:934787764(0) win 64240 <mss 1460,nop,nop,sackOK>
22:42:56.574502 IP (tos 0x0, ttl 126, id 50387, offset 0, flags [DF], proto TCP (6), length 48) 140.123.122.12.1436 > 140.123.241.102.135: S, cksum 0xe8
orrect), 1031198716:1031198716(0) win 64240 <mss 1460,nop,nop,sackOK>
22:42:58.385469 IP (tos 0x0, ttl 126, id 50498, offset 0, flags [DF], proto TCP (6), length 48) 140.123.122.12.1468 > 140.123.241.111.135: S, cksum 0xad
orrect), 1033245308:1033245308(0) win 64240 <mss 1460,nop,nop,sackOK>
22:43:27.091454 IP (tos 0x0, ttl 126, id 52824, offset 0, flags [DF], proto TCP (6), length 48) 140.123.122.12.2183 > 140.123.241.190.135: S, cksum 0xce
orrect), 1074850821:1074850821(0) win 64240 <mss 1460,nop,nop,sackOK>
```



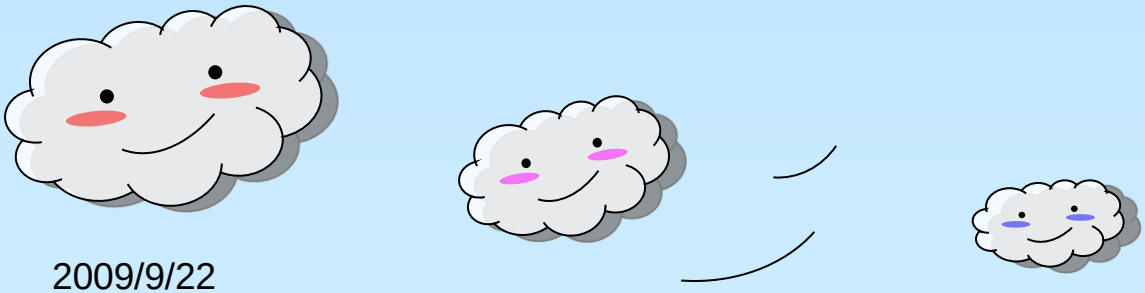
2009/9/22

Any Question?



2009/9/22

Thank You !!!



2009/9/22