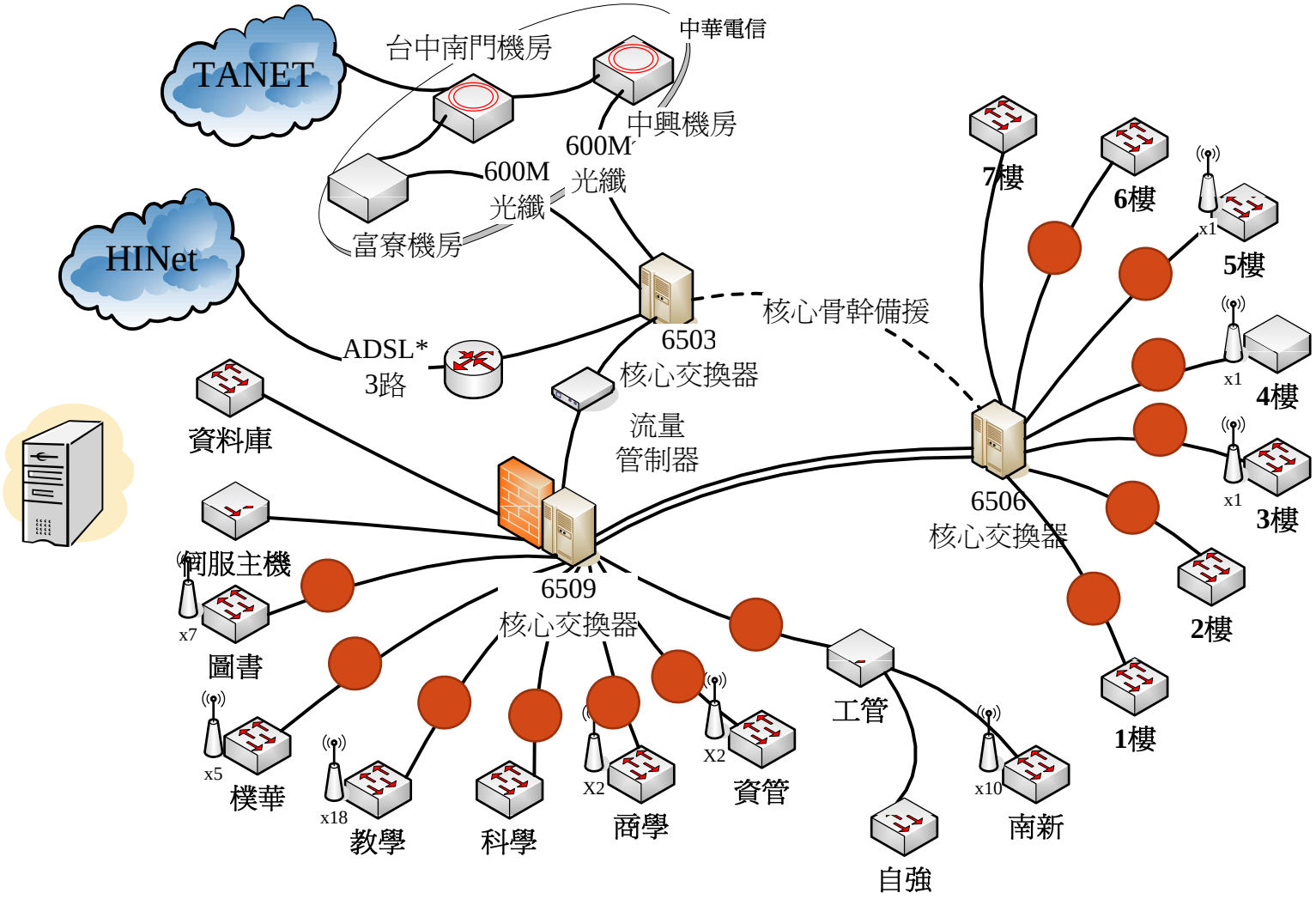
網管系統開發經驗分享

報告人:邱仁成

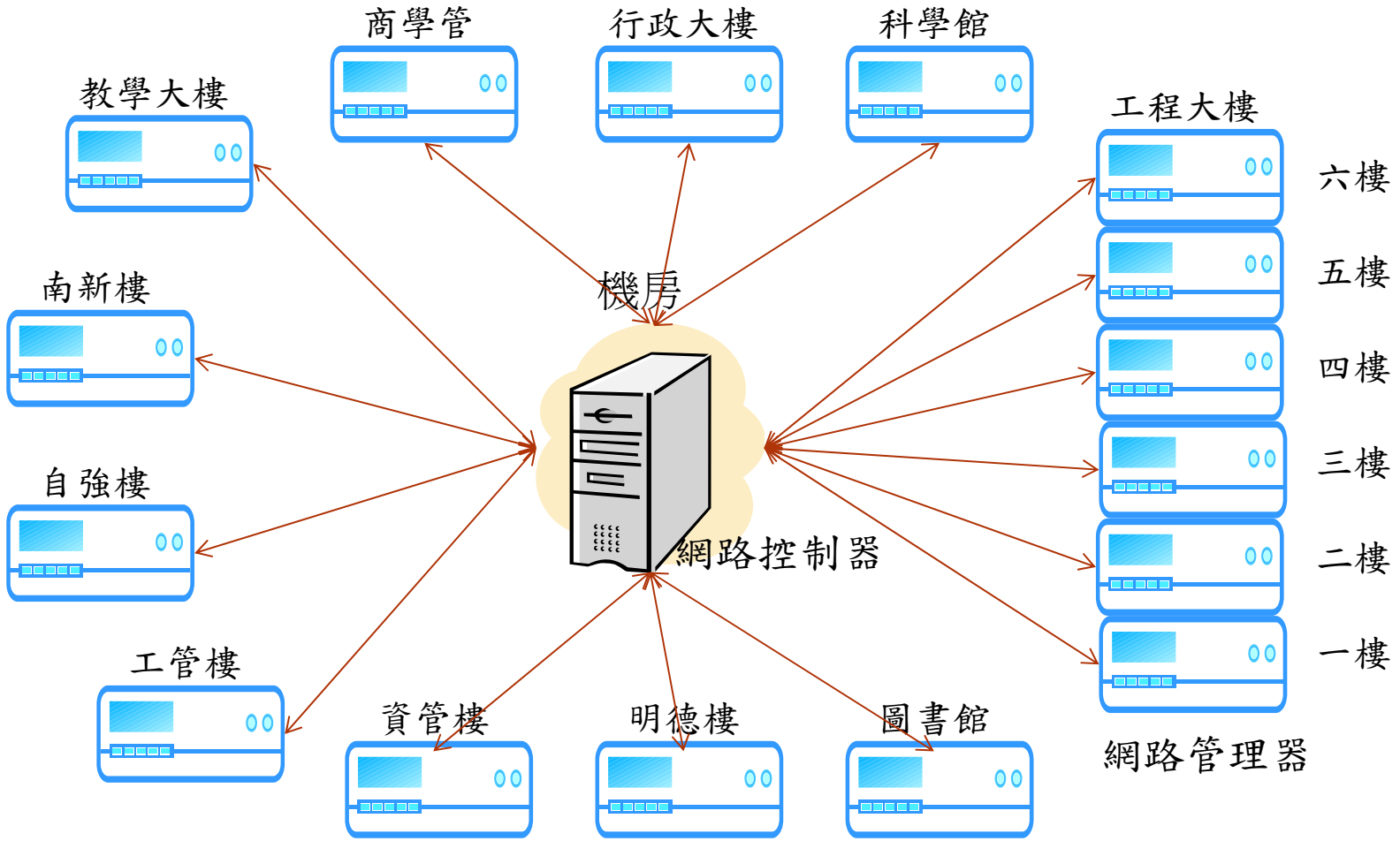
Outline

- 網路架構
- 網路管理器
- 網路控制器
- 網路管理系統

網路架構


TANET
台中南門機房
中華電信
中興機房
600M
光纖
600M
光纖
富寮機房
HINet
ADSL*
3路
6503
核心交換器
核心骨幹備援
資料庫
流量
管制器
6509
核心交換器
6506
核心交換器
7樓
6樓
x1
5樓
x1
4樓
x1
3樓
2樓
1樓
網服主機
x7
圖書
x5
樸華
x18
教學
科學
X2
商學
X2
資管
工管
自強
x10
南新

網路架構


商學管
行政大樓
科學館
教學大樓
工程大樓
六樓
五樓
南新樓
機房
四樓
三樓
自強樓
二樓
網路控制器
一樓
工管樓
資管樓
明德樓
圖書館
網路管理器

網路管理器


4GB
266x
CompactFlash
Transcend
JP1
JP2
card detect
Active power


G-MAX

網路管理器

- NAT 和 Bridge
- IP_MAC對應
- L7 netfilter
- 頻寬管理

NAT 和 Bridge

- NAT
  - iptables (Debian and Ubuntu)
  - echo "1" > /proc/sys/net/ipv4/ip_forward
  - iptables -t nat -A POSTROUTING -s x.x.x.x/24 -j MASQUERADE
- Bridge
  - 安裝 Bridge-utils
    - ifconfig eth0 down
    - ifconfig eth0 0.0.0.0 promisc
    - ifconfig eth1 0.0.0.0 promisc
    - brctl addbr b0
    - brctl addif b0 eth0
    - brctl addif b0 eth1
    - brctl stp b0 on
    - ifconfig b0 up

IP_MAC對應

- iptables (Debian and Ubuntu)
  - iptables -A FORWARD -s x.x.x.x -m mac --mac-source xx:xx:xx:xx:xx:xx -j ACCEPT

L7 netfilter

- 下載netfilter-layer7-v2.22.tar.gz
- 找合適的Kernel跟Iptables的Patch
  - 假設Kernel 的版本是2.6.26，則選kernel-2.6.25-2.6.28-layer7-2.22.patch
- 把kernel-2.6.25-2.6.28-layer7-2.22.patch丟到kernel source code裡，執行 patch -p1 < kernel-2.6.25-2.6.28-layer7-2.22.patch
- make menuconfig，進去選擇 Networking->Networking Options->Network packet filtering framework->Core Netfilter Configuration->"layer7" match support
- Make，產生kernel image。
- 開始Patch iptables，把libxt_layer7.c跟libxt_layer7.man 拷貝到iptables-xxxxx/extensions/下面
- 執行configure　./configure --with-ksource= path_linux path_linux代表kernel source的資料夾

L7 netfilter

- make compiler
- 當Kernel跟Iptables都Patch好了並且安裝好了。就可以開始用了
- 解開l7-protocols-2009-05-28.tar.gz 裡面可以找到很多副檔名是.pat的檔案
- cp l7-protocols-2009-05-28/protocols /etc/l7protocols -rf 把pattern 拷貝到預設路徑下
- 開始執行
  - 在Router上封鎖MSN
    - iptables -t mangle -I PREROUTING -m layer7 --l7dir /mnt/jffs2/ --l7proto msnmessenger -j DROP
  - 封鎖TFTP
    - iptables -I OUTPUT 1 -m layer7 --l7dir /mnt/jffs2/ --l7proto tftp -j DROP
- 依此類推可以針對特定的Protocol來做特定的事，類似上DCSP，丟掉DROP或是接受ACCEPT

頻寬管理

- tc (Debian and Ubuntu)
  - tc qdisc add dev eth0 root handle 1: htb default 24
  - tc class add dev eth0 parent 1: classid 1:1 htb rate 10 Mbps ceil 20 Mbps
  - tc filter add dev eth0 parent 1: protocol ip handle 100 fw classid 1:1
  - iptables -t mangle -A PREROUTING -p tcp -m layer7 --l7proto msnmessenger -j MARK --set-mark 100

網路控制器

- 更新管理器設定檔
- iptables 流量收集
- Netflow 流量收集

更新管理器設定檔

- ssh2_connect($controls_ip, 22)
- ssh2_auth_password($con, “帳號”,“密碼”)
- ssh2_scp_send($con, './bootsetup.sh', '/root/bootsetup.sh', 0655)
- ssh2_exec($con, "/root/bootsetup.sh")

iptables 流量收集

- iptables -L FORWARD -vnx > temp

```
Chain FORWARD (policy DROP 327 packets, 20815 bytes)
    pkts      bytes target     prot opt in     out     source               destination
     522    19261 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0           limit: avg 1/sec burst 1
   72130 18961343 ACCEPT     all  --  *      *       163.22.250.1         0.0.0.0/0           MAC 00:0D:61:16:78:98
  101407 113766503 ACCEPT     all  --  *      *       0.0.0.0/0            163.22.250.1
      37     2677 ACCEPT     all  --  *      *       163.22.250.8         0.0.0.0/0           MAC 00:1F:D0:A7:69:9A
       0        0 ACCEPT     all  --  *      *       0.0.0.0/0            163.22.250.8
     359    44567 ACCEPT     all  --  *      *       163.22.250.9         0.0.0.0/0           MAC 00:1D:60:B2:F5:76
     522   552294 ACCEPT     all  --  *      *       0.0.0.0/0            163.22.250.9
     431    56551 ACCEPT     all  --  *      *       163.22.250.10        0.0.0.0/0           MAC E0:CB:4E:BB:50:61
     292    36216 ACCEPT     all  --  *      *       0.0.0.0/0            163.22.250.10
```

- sscanf($buffer,"%d%d%s%s%s%s%s%s%s",$pkts,$bytes,$traget,$prot,$opt,$in,$out,$src,$des);
- iptables -t mangle -L FORWARD -vnx

```
Chain FORWARD (policy ACCEPT 18674429904 packets, 11654111426764 bytes)
    pkts      bytes target     prot opt in     out     source               destination
     562    70740 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0           LAYER7 l7proto bittorrent
       0        0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0           LAYER7 l7proto fasttrack
      60     3853 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0           LAYER7 l7proto edonkey
       0        0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0           LAYER7 l7proto gnutella
```

Netflow 流量收集

- Router 6509 和 6503
- /etc/init.d/nfdump
  - DATA_BASE_DIR="/var/cache/nfdump“
  - DAEMON_ARGS="-w -D -t 60 -p 9995 -l $DATA_BASE_DIR -P $PIDFILE“
- nfdump -R /var/cache/nfdump -N

Date flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2011-09-27 16:30:18.643	0.000	17	163.22.244.61:17500	->	255.255.255.255:17500	1	147	1
2011-09-27 16:30:18.643	0.000	17	163.22.244.61:17500	->	163.22.244.255:17500	1	147	1
2011-09-27 16:30:18.659	0.000	17	10.100.88.249:3501	->	255.255.255.255:0	1	916	1
2011-09-27 16:30:18.659	0.000	17	10.100.88.249:3501	->	255.255.255.255:10001	1	916	1
2011-09-27 16:30:07.647	10.500	17	163.22.239.42:137	->	163.22.239.255:137	16	1248	1
2011-09-27 16:30:07.983	10.500	17	163.22.239.155:137	->	163.22.239.255:137	16	1248	1
2011-09-27 16:30:11.047	8.236	17	163.22.242.168:137	->	163.22.242.255:137	12	936	1
2011-09-27 16:30:19.475	0.000	17	10.100.233.99:138	->	10.100.233.255:138	1	232	1
2011-09-27 16:29:59.091	20.800	17	163.22.242.204:51586	->	10.100.242.153:161	3	318	1
2011-09-27 16:30:20.375	0.000	17	0.0.0.0:68	->	255.255.255.255:67	1	378	1
2011-09-27 16:30:20.555	0.000	17	163.22.242.10:51825	->	10.100.200.42:4001	1	36	1
2011-09-27 16:30:20.887	0.000	17	163.22.242.10:51828	->	10.100.200.7:4001	1	36	1

網路管理系統

- http://ip.nkut.edu.tw/