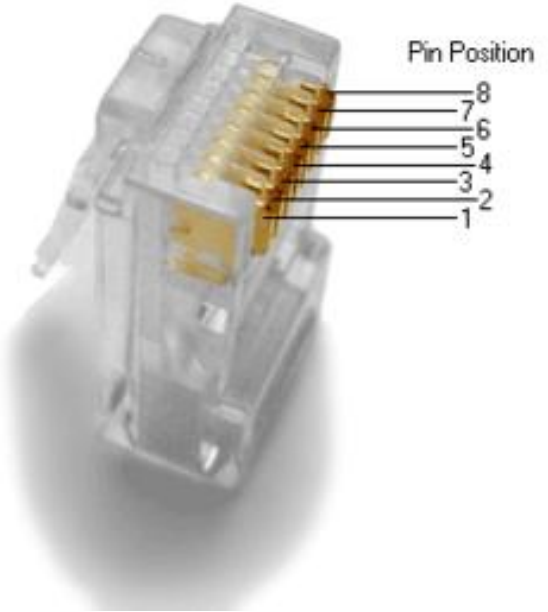
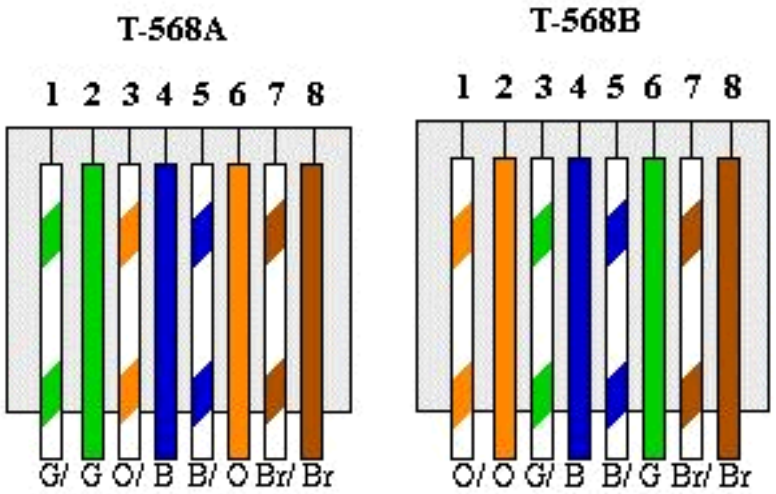
Review on Computer Network Experiments, 6-1-2010

Lab 1 區域網路線材製作

- 熟悉網路線製作過程
- 了解跳線與非跳線之區別與排列規則





Lab 2 網路協定觀察與分析 (1/2)

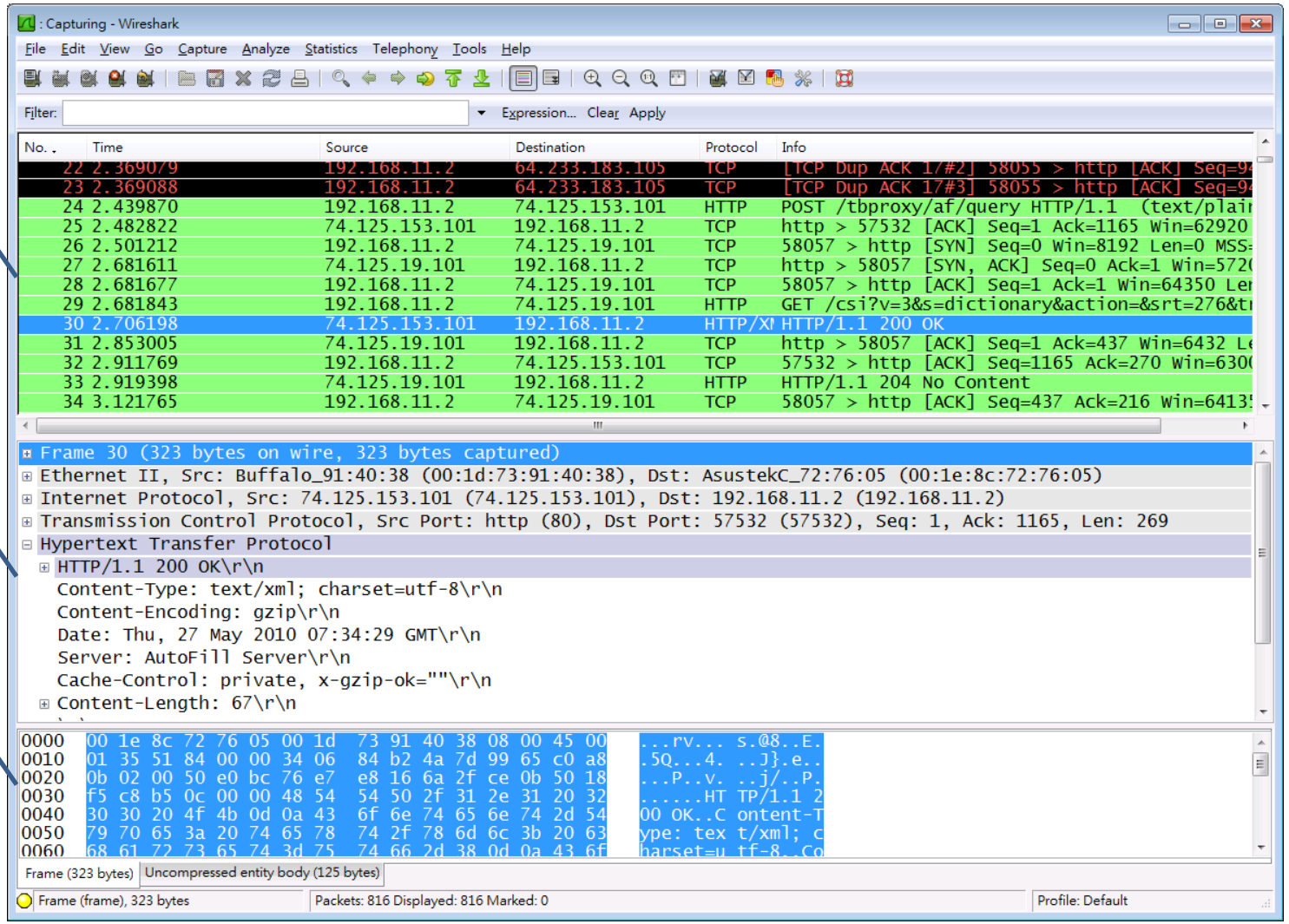
- 了解網路封包之分層方式
- 能使用工具抓取網路封包
- 分析 http 之傳輸流程及封包內容

Lab 2 網路協定觀察與分析 (2/2)

List of packets

Packet layering

Raw data



Lab 3 Linux 網路協定程式追蹤

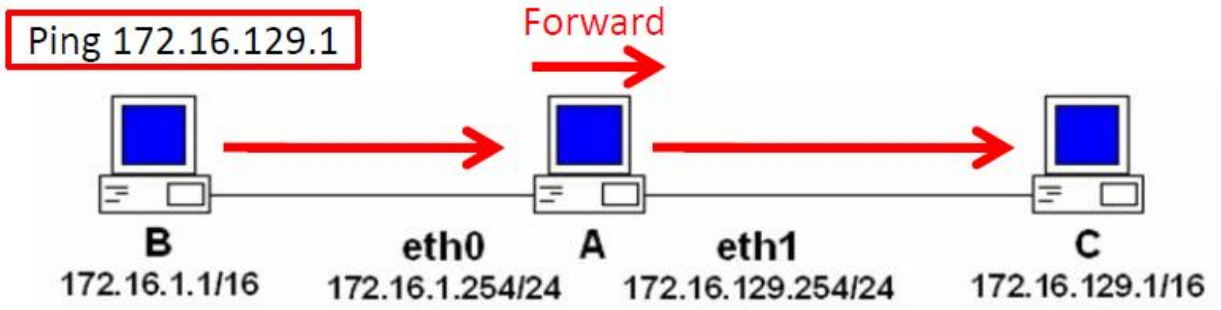
- 了解如何編譯核心
- 能搜尋，修改核心原始碼
- 追蹤開機過程中，網路模組的相關訊息

Add log message for tracing

```
int ip_fragment(struct sk_buff *skb, int (*output)(struct sk_buff *))
{
        printk(KERN_INFO "ip_output.c: ip_fragment()");
        struct iphdr *iph;
        int raw = 0;
        int ptr;
        struct net_device *dev;
        struct sk_buff *skb2;
        unsigned int mtu, hlen, left, len, ll_rs, pad;
        int offset;
        __be16 not_last_frag;
        struct rtable *rt = skb_rtable(skb);
        int err = 0;
```

Lab 4 Linux子網域分割之設定與觀察 (1/2)

- 了解subnet運作原理與netmask的用途
- 設定ARP-Proxy




```
[root@localhost ~]# arp -i eth0 -Ds 172.16.129.1 eth0 pub
[root@localhost ~]# arp -i eth1 -Ds 172.16.1.1 eth1 pub
[root@localhost ~]# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.1.1               *       *                   MP                    eth1
172.16.129.1             *       *                   MP                    eth0
```

ARP cache

Lab 4 Linux子網域分割之設定與觀察 (2/2)

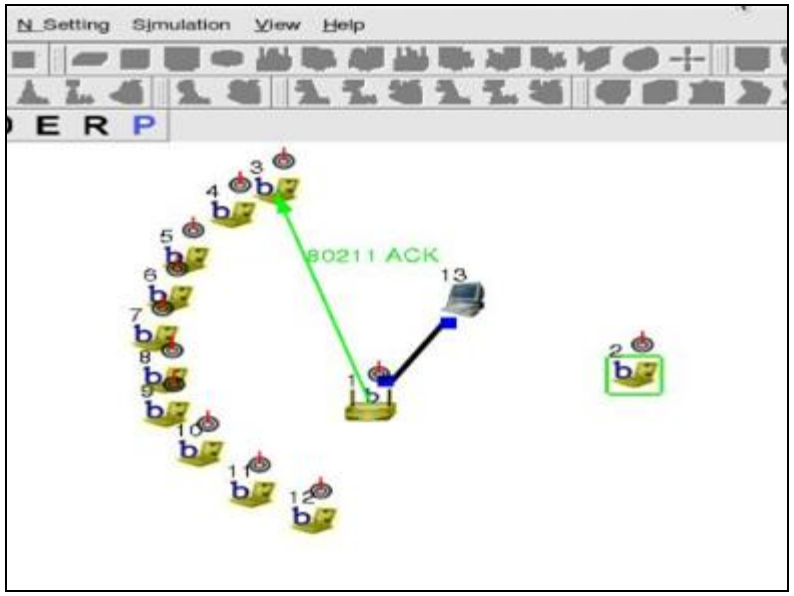
- 使用tcpdump觀察ICMP與ARP封包

```
[root@localhost ~]# tcpdump -n arp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
11:02:17.977096 ARP, Request who-has 172.16.1.254 tell 172.16.1.1, length 46
11:02:17.981470 ARP, Reply 172.16.1.254 is-at 08:00:27:12:10:b9, length 28
11:02:22.974058 ARP, Request who-has 172.16.1.1 tell 172.16.1.254, length 28
11:02:22.974891 ARP, Reply 172.16.1.1 is-at 08:00:27:a0:19:35, length 46
11:02:31.791721 ARP, Request who-has 172.16.129.254 tell 172.16.1.1, length 46
11:02:31.791801 ARP, Reply 172.16.129.254 is-at 08:00:27:12:10:b9, length 28
11:05:08.893929 ARP, Request who-has 172.16.129.1 tell 172.16.1.1, length 46
11:05:08.904546 ARP, Reply 172.16.129.1 is-at 08:00:27:12:10:b9, length 28
11:05:14.600907 ARP, Request who-has 172.16.1.1 tell 172.16.1.254, length 28
11:05:14.604034 ARP, Reply 172.16.1.1 is-at 08:00:27:a0:19:35, length 46
```

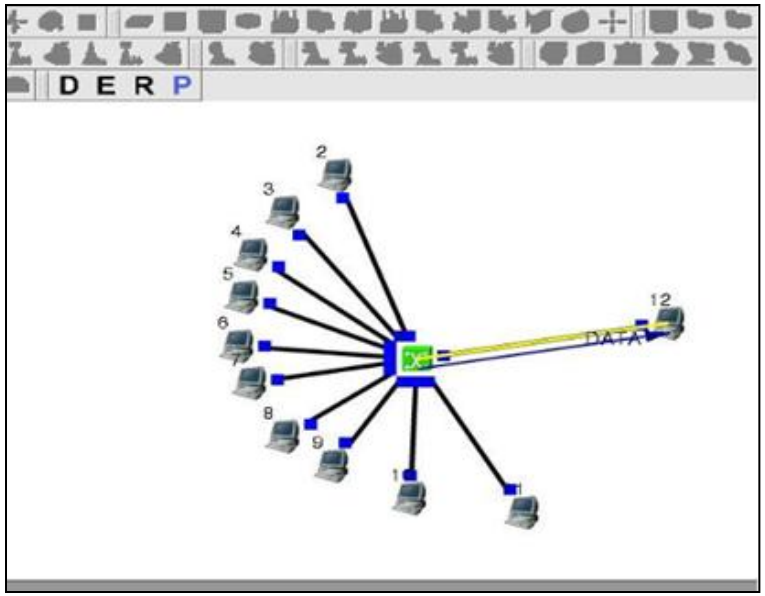
Snapshot of tcpdump

Lab 5 媒介存取協定模擬 (1/2)

- 用NCTUns建立含wireless AP 和 router/switch 的網路拓撲



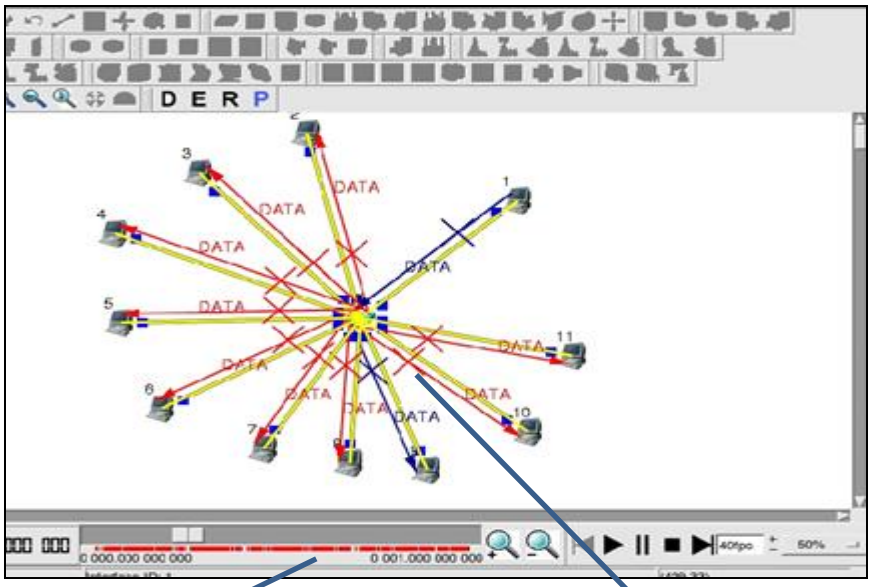
Wireless scenario (AP)

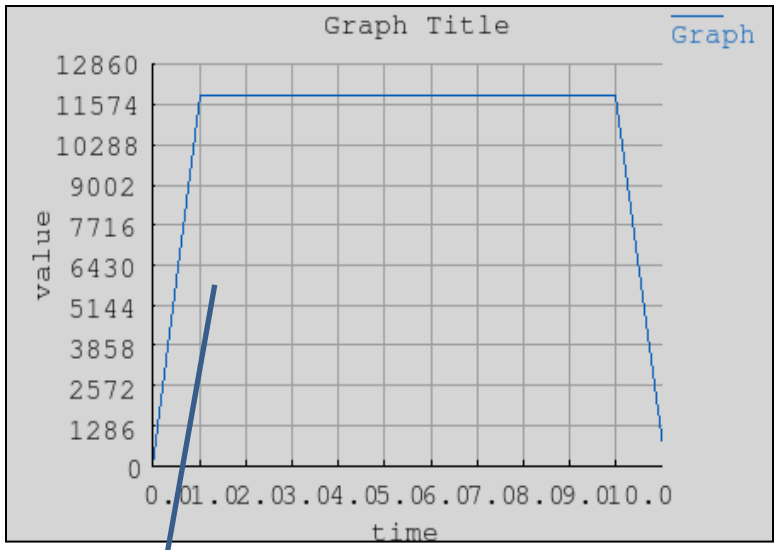


Wired scenario (Switch)

Lab 5 媒介存取協定模擬 (2/2)

- 設定與執行網路流量模擬





Control bar

Collisions

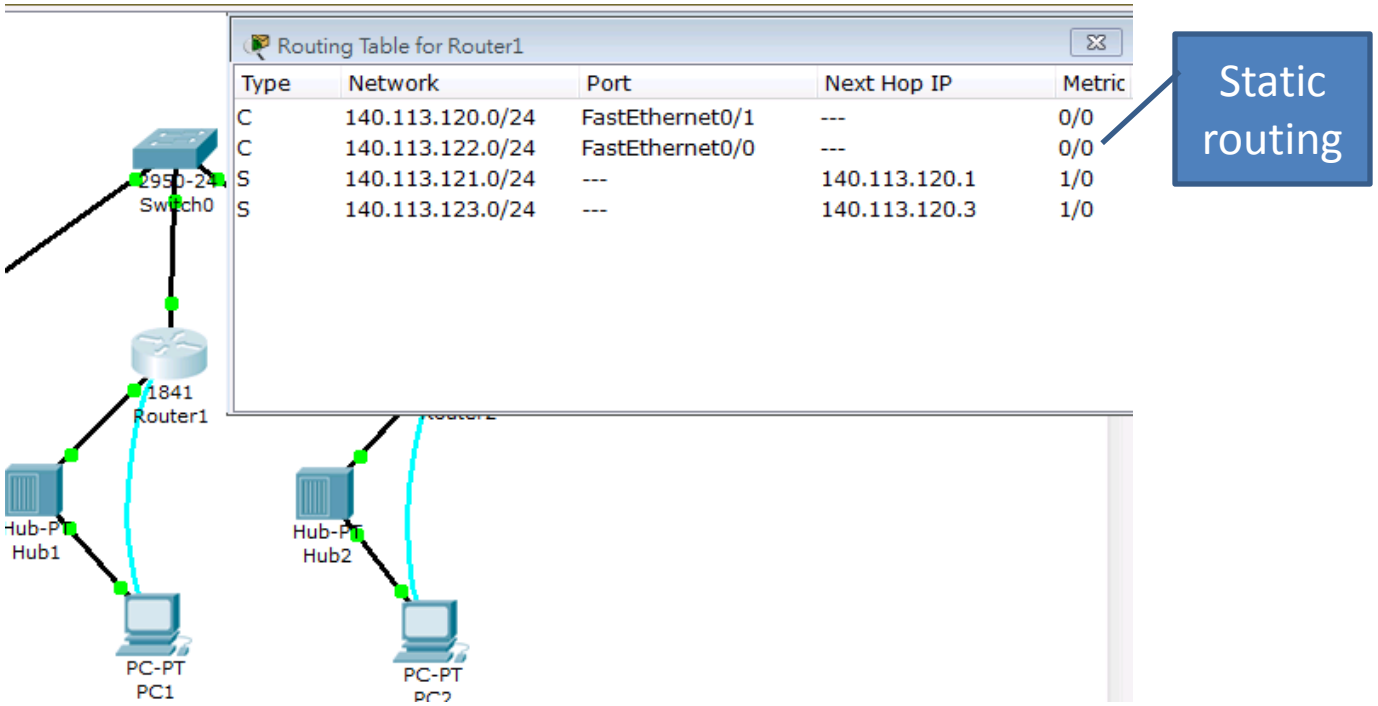
Throughput

Simulation result

- 改變node之間連線的capacity

Lab 6 路由器操作設定 (1/2)

- 建立一含 router 的基本網路拓撲
- 設定 static routing 使不同 subnet 的電腦能互相連通



Lab 6 路由器操作設定 (2/2)

```
Router>enable
Router#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 140.113.121.1 255.255.255.0
Router(config-if)#exit
Router(config)#ip route 140.113.123.0 255.255.255.0 140.113.120.3
```

- Set IP address and add static routing

Lab 7 Linux 路由器之建構與追蹤 (1/2)

- 在 kernel 中加上 kdb 的 patch
- 使用kdb追蹤 kernel function
- 設定 quagga 之 static routing 及 RIP

```
Entering kdb (current=0xc0769e80, pid 0) on processor 0 due to Keyboard Entry
[0]kdb> bp ip_rt_ioctl

Instruction(i) BP #0 at 0xc0509960 (ip_rt_ioctl)
    is enabled globally adjust 1Maddr at 00000000c0509960, hardtype=0, forcehw=0
, installed=0, hard=c08bb818

[0]kdb> go
```

Set breakpoint

Lab 7 Linux 路由器之建構與追蹤 (2/2)

```
root@ubuntu:~# route del default
Instruction(i) breakpoint #0 at 0xc0509960 (adjusted)
0xc0509960 ip_rt_ioctl:         int3

Entering kdb (current=0xf01657f0, pid 836) on processor 0 due to Breakpoint @ 0x
c0509960
[0]kdb> ssb

0xc0509961 ip_rt_ioctl+0x1:     mov    %esp,%ebp
0xc0509963 ip_rt_ioctl+0x3:     sub    $0xd0,%esp
0xc0509969 ip_rt_ioctl+0x9:     mov    %eax,0xffffff40(%ebp)
0xc050996f ip_rt_ioctl+0xf:     mov    %gs:0x14,%eax
0xc0509975 ip_rt_ioctl+0x15:    mov    %eax,0xfffffff0(%ebp)
0xc0509978 ip_rt_ioctl+0x18:    xor    %eax,%eax
0xc050997a ip_rt_ioctl+0x1a:    lea    0xffff76f5(%edx),%eax
0xc0509980 ip_rt_ioctl+0x20:    cmp    $0x1,%eax
0xc0509983 ip_rt_ioctl+0x23:    mov    %ebx,0xfffffff4(%ebp)
0xc0509986 ip_rt_ioctl+0x26:    mov    %edx,%ebx
0xc0509988 ip_rt_ioctl+0x28:    mov    %esi,0xfffffff8(%ebp)
0xc050998b ip_rt_ioctl+0x2b:    mov    %ecx,%esi
0xc050998d ip_rt_ioctl+0x2d:    mov    %edi,0xfffffffc(%ebp)
0xc0509990 ip_rt_ioctl+0x30:    mov    $0xffffffea,%edi
0xc0509995 ip_rt_ioctl+0x35:    ja     0xc05099b0 ip_rt_ioctl+0x50
[0]kdb> _
```

- Trigger break point function
- trace its execution flow

Lab 8 網路探測：路徑、延遲與流量統計 (1/2)

- 找出封包在網路上傳遞的路徑
  - 路徑探測工具的原理

Map

Routing path with RTT

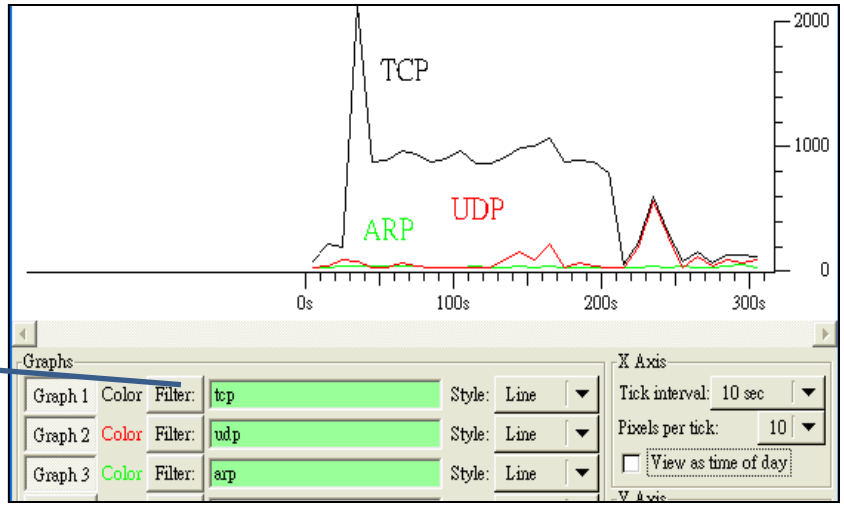
Information of a node

VisualRoute

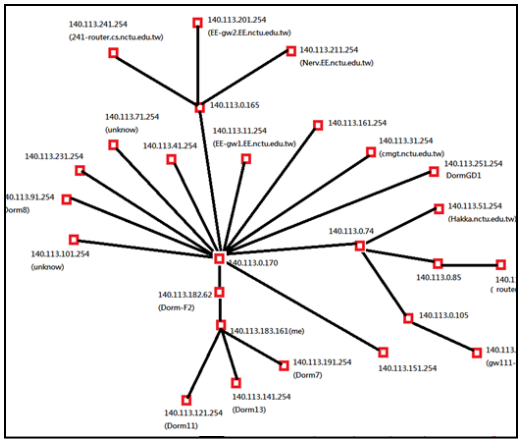
Lab 8 網路探測：路徑、延遲與流量統計 (2/2)

- 使用wireshark監測網路流量

Traffic filters



- 網路拓樸圖的建立



Network topology of NCTU

Lab 9 建置網路安全閘道器 (1/2)

- iptables 操作
- 使用 squid 過濾 http 連線
- 以 openvpn 建立 site-to-site vpn

iptable rule for dropping packet

```
root@ubuntu:~# iptables -A FORWARD -d 140.113.88.160 -o eth0 -j DROP
root@ubuntu:~# iptables -L -v
Chain INPUT (policy ACCEPT 158 packets, 49432 bytes)
 pkts bytes target     prot opt in     out     source               destination


Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

    0     0 DROP       all  --  any    eth0    anywhere             140.113.88.1
60

Chain OUTPUT (policy ACCEPT 10 packets, 728 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Lab 9 建置網路安全閘道器 (2/2)

- Squid ACL rules
  - aclEXEFileurlpath_regex/*.exe
  - http_access deny EXEFile

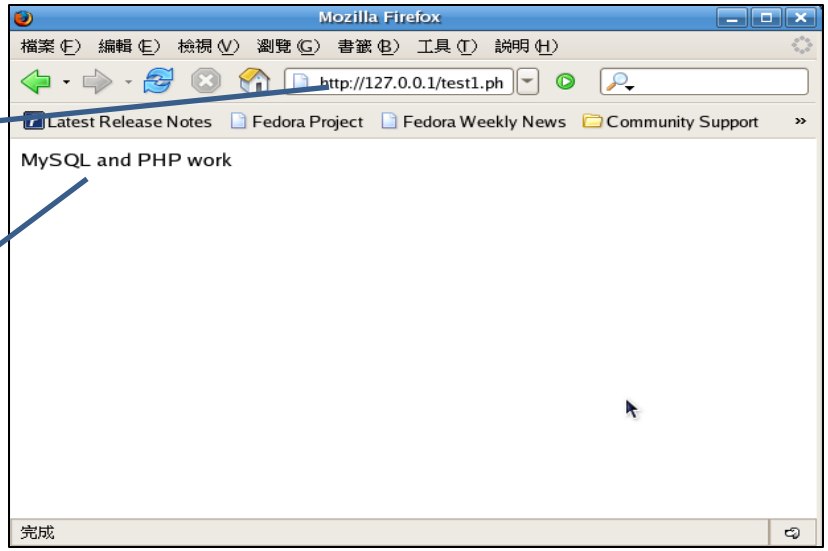
  - acl Badsite url_regex dstdomain www.sex.com
  - http_access deny Badsite

Lab 10 以Linux架設Internet/Intranet伺服器 (1/2)

- 架設Web Server (Apache/PHP/MySQL)

Local address

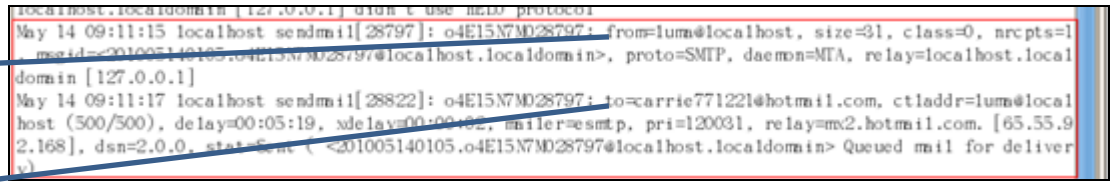
Test for PHP & MySQL



- 架設Mail Server (Qmail)

Sender's address

Receiver's address



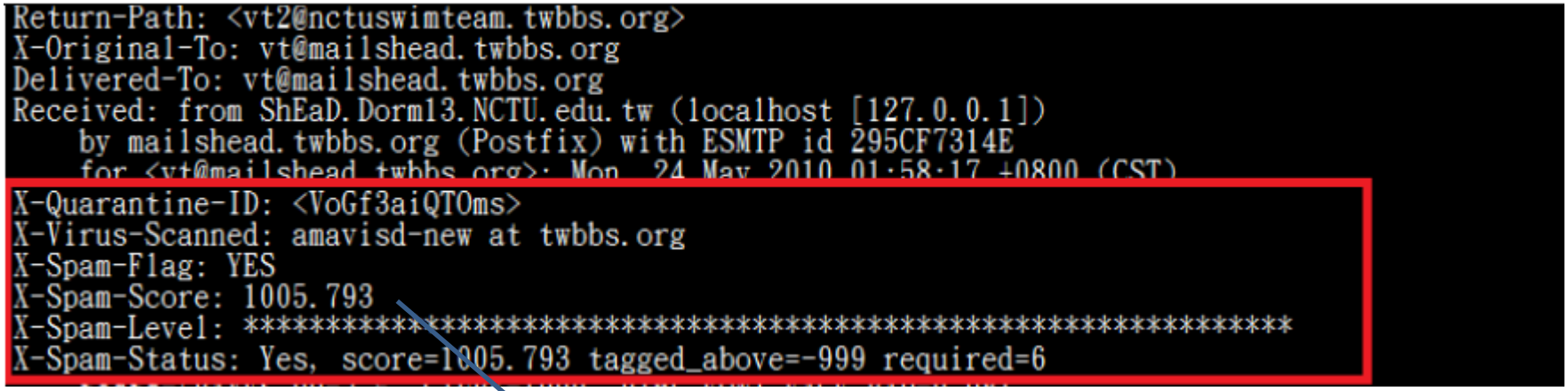
Mail log

Lab 10 以Linux架設Internet/Intranet伺服器 (2/2)

- 架設 FTP server (vsftpd)
- 架設 Samba server

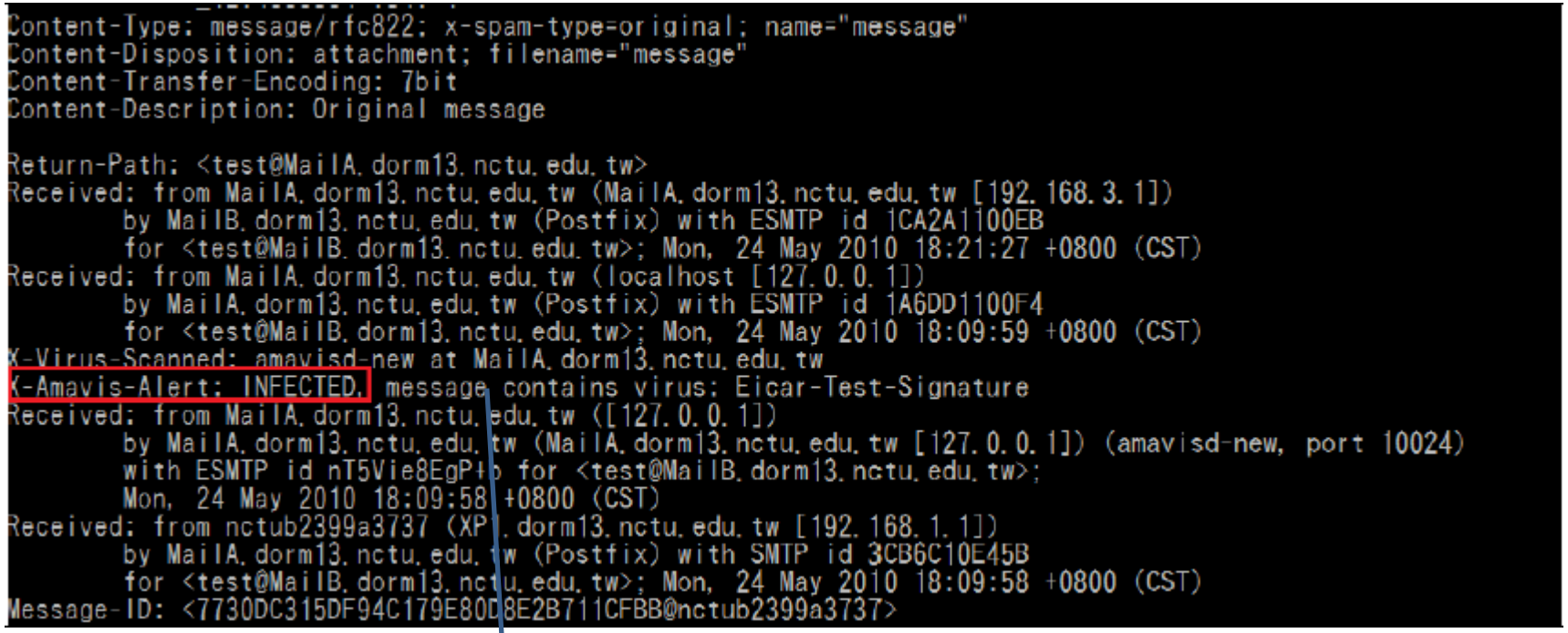
Lab 11 建置防範病毒信及廣告信之郵件伺服器 (1/2)

- 安裝設定Postfix, Amavisd-new, SpamAssassin, 和 ClamAV
- 廣告信件之攔截



Lab 11 建置防範病毒信及廣告信之郵件伺服器 (2/2)

- 病毒信件之攔截



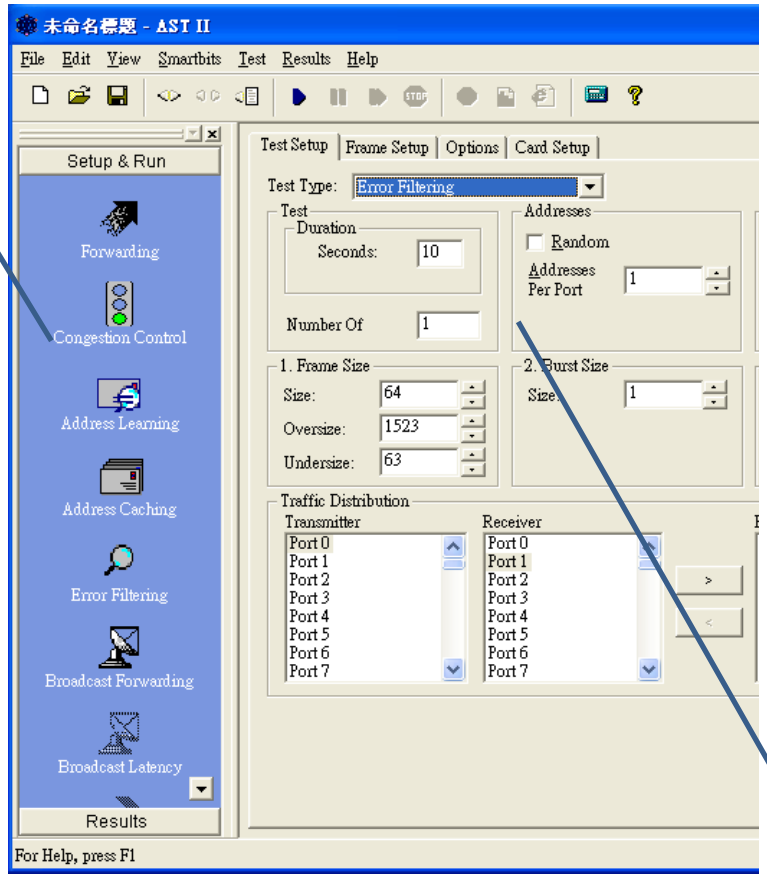
Lab 12 建置入侵偵測防禦系統及弱點偵測掃瞄系統

- 了解 bridge 用處及如何建立 bridge
- 熟悉 snort rule 格式

- reject tcp any any -> 192.168.1.21 22 (sid:1001; content:"/bin/sh"; msg:"Possible SSH buffer overflow";)

Lab 13 以SmartBits來測試Layer 2/3交換器 (1/2)

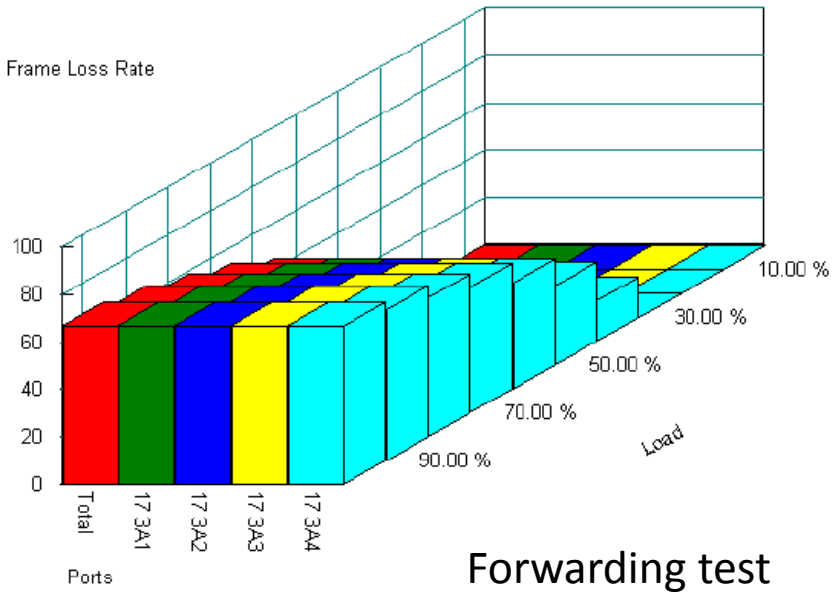
- 利用AST II測試Layer2 switch



AST II

Test Items

Configurations

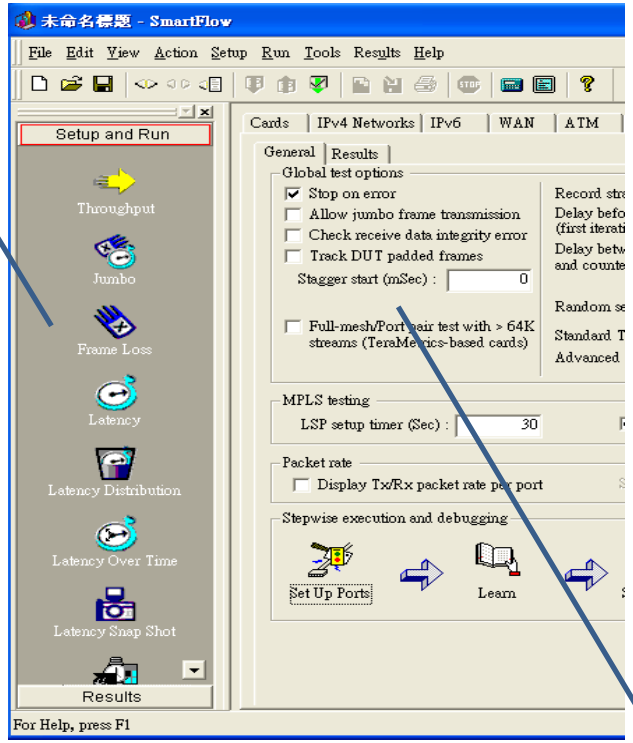


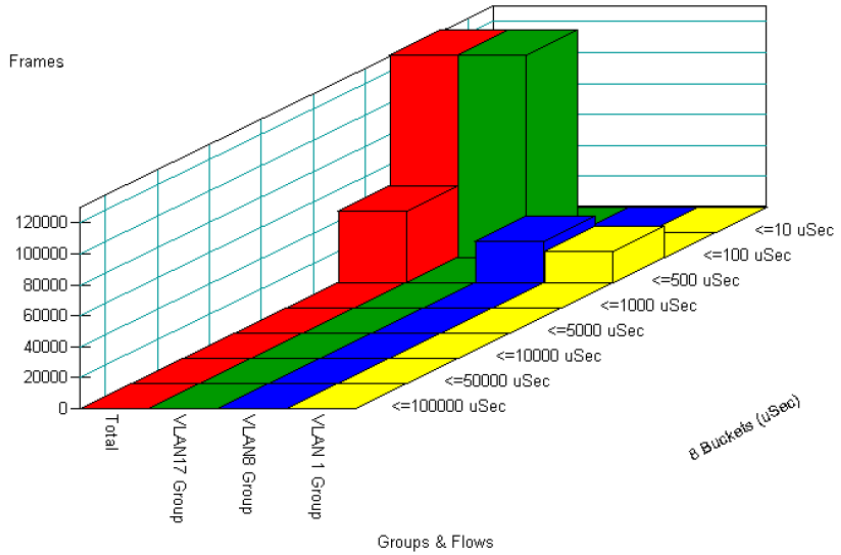
Forwarding test

Lab 13以SmartBits來測試Layer 2/3交換器 (2/2)

- 利用SmartFlow測試Layer3 router

Test Items





Latency distribution test

Configurations