

Firewall & NAT

Teacher Assistants: Chia-Peng Lee,

Instructor: Prof. Phone Lin

Date: 2018/03/14



注意事項

❖ 實驗(一)上機實驗 (@ R204)

- 時間: 2017/03/08 14:20~17:10
 - 組別名單將公佈在課程網頁上

❖ 實驗(一)展演及實驗結報繳交 (@ R204)

- 時間: 2017/03/15 14:20~17:10
- 實驗結報繳交方式:
 - 一律使用電子郵件繳交電子檔，
 - 郵件主旨請依照 **[CNL實驗(一)結報繳交_組別]**

❖ 下次上課 (@ R204)

- 時間: 2015/7/22 14:20~17:10

實驗說明

- ❖ 本實驗是要將一台裝有兩張網路卡的個人電腦，設定成一台有防火牆功能的IP分享器。不過與市面上的防火牆不同的地方是，除了要防止外面危險的封包進來之外，也要防止未經授權的內部使用者送封包出去。
- 在Linux作業系統上建立自己的Firewall
 - 讓你的Linux成為NAT伺服器
 - 架設DHCP在你的Linux上

實驗說明

- ❖ 本實驗是要將一台裝有兩張網路卡的個人電腦，設定成一台有防火牆功能的IP分享器。不過與市面上的防火牆不同的地方是，除了要防止外面危險的封包進來之外，也要防止未經授權的內部使用者送封包出去。
- 在Linux作業系統上建立自己的Firewall
 - 讓你的Linux成為NAT伺服器
 - 架設DHCP在你的Linux上

實驗目的

- ❖ 了解NAT、Firewall和DHCP它們的運作原理之後，實際在Linux上架設。
- ❖ 透過設定過濾IP封包的過程中，在OSI架構中之網路層了解基礎的TCP/IP原理和上層各種不同應用程式的通訊協定 (如: Skype、FTP、HTTP等)。

實驗器材

❖ R204

- 一台電腦 with installed Virtual Box 。

❖ R202

- 一台hub 。
- 一台具兩張網路卡的個人電腦(架設NAT和Firewall，電腦A) 。
- 一台筆記型電腦或個人電腦(電腦B) 。
- 兩條網路線 。
- 兩條電源線 。

實驗必備相關資料

☒ Linux安裝與設定。

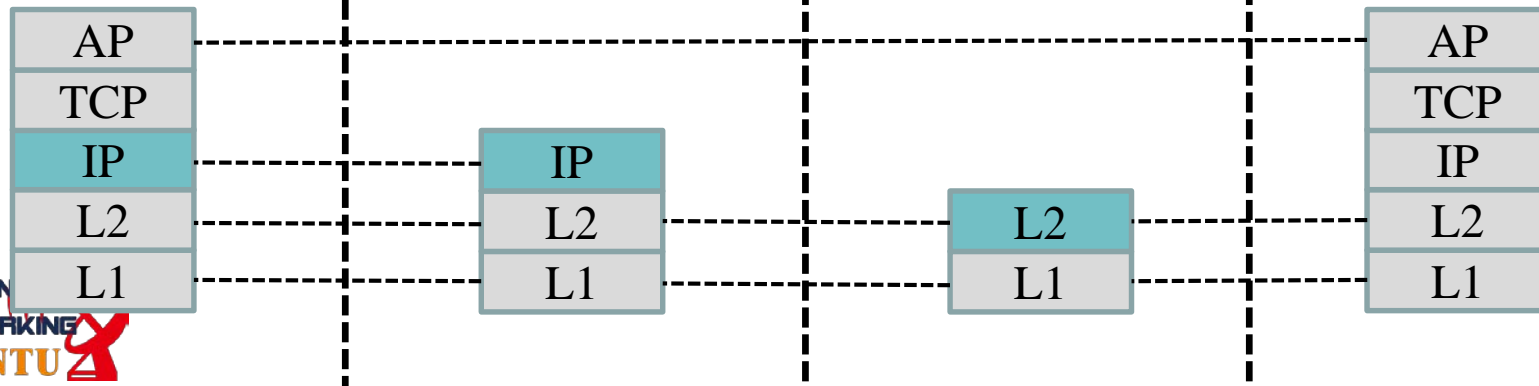
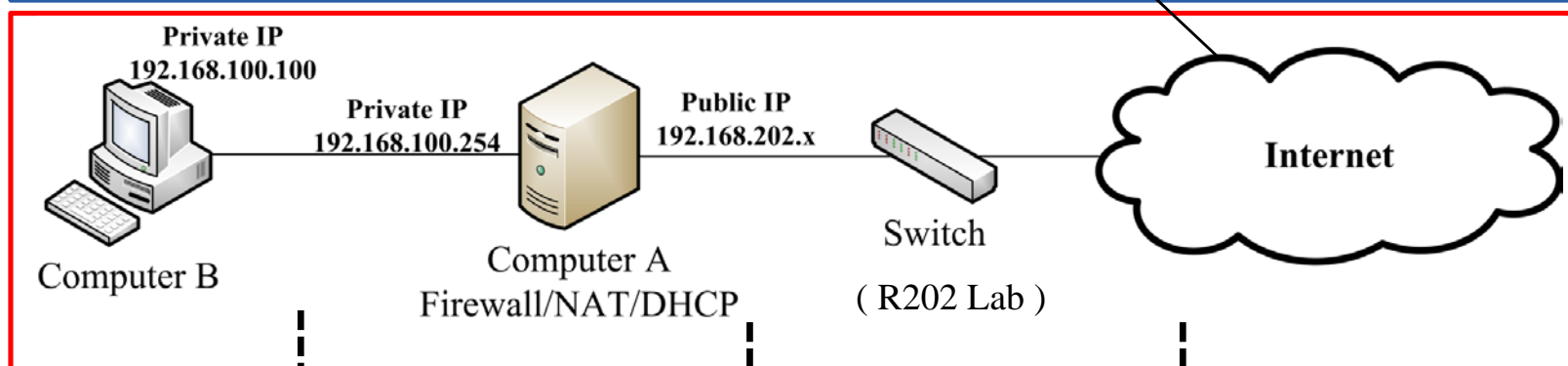
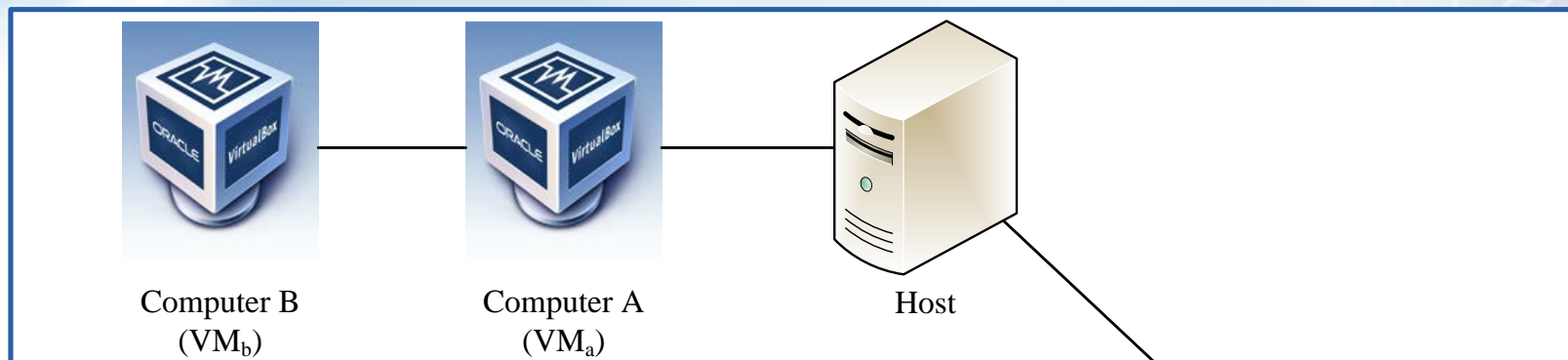
- <http://www.ubuntu.com/download/desktop/contribute/?version=14.04.2&architecture=amd64>
- <http://wiki.ubuntu-tw.org/index.php?title=%E9%A6%96%E9%A0%81>

☒ TCP/IP的基礎知識。

☒ Linux network programming。

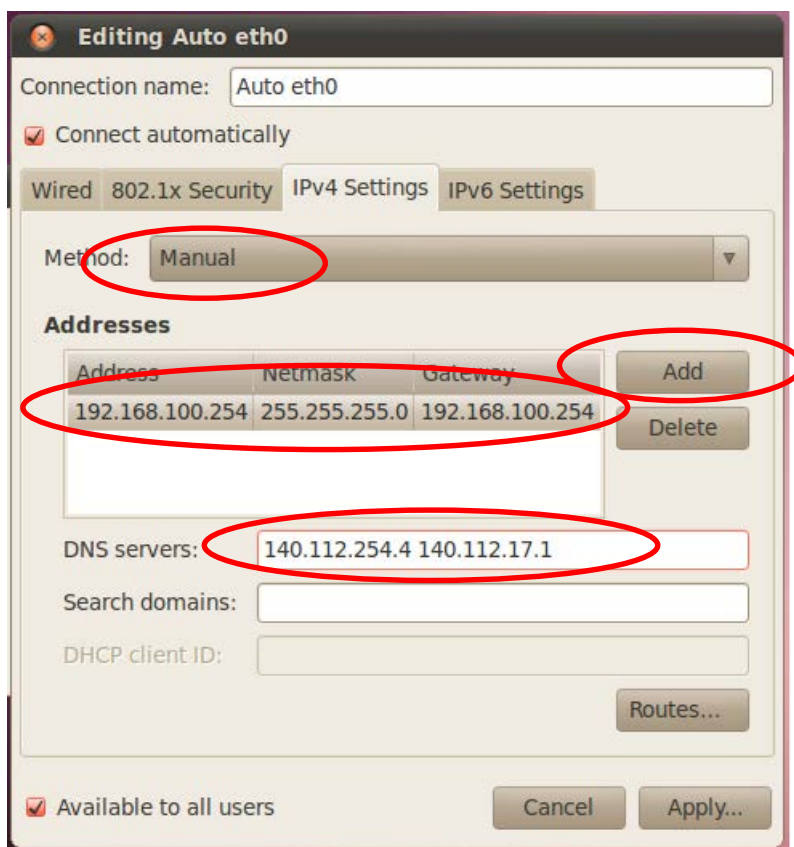
- Advanced Linux Programming, by Mark Mitchell, Jeffrey Oldham, and Alex Samuel, of Code Sourcing LLC

實驗網路環境架構



實驗網路環境設定

Network Configuration of Computer A



Editing Auto eth0

Connection name: Auto eth0

☒ Connect automatically

Wired 802.1x Security IPv4 Settings IPv6 Settings

Method: Manual

Addresses

Address	Netmask	Gateway
192.168.100.254	255.255.255.0	192.168.100.254

Add Delete

DNS servers: 140.112.254.4 140.112.17.1

Search domains:

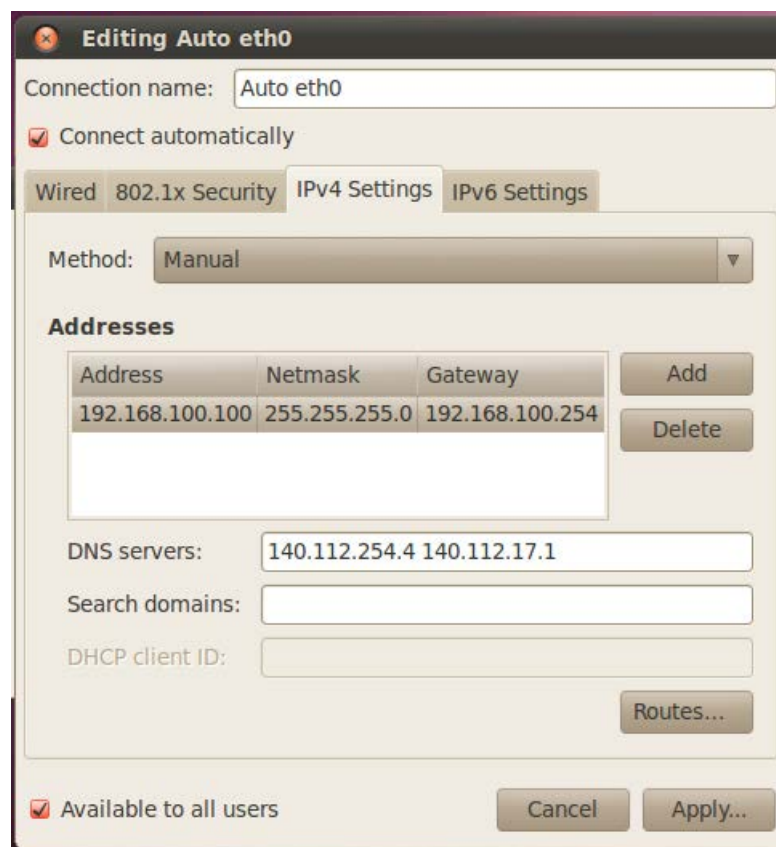
DHCP client ID:

Routes...

☒ Available to all users

Cancel Apply...

Network Configuration of Computer B



Editing Auto eth0

Connection name: Auto eth0

☒ Connect automatically

Wired 802.1x Security IPv4 Settings IPv6 Settings

Method: Manual

Addresses

Address	Netmask	Gateway
192.168.100.100	255.255.255.0	192.168.100.254

Add Delete

DNS servers: 140.112.254.4 140.112.17.1

Search domains:

DHCP client ID:

Routes...

☒ Available to all users

Cancel Apply...

實驗系統環境

- ❏ 作業系統: Ubuntu 14.04.2 LTS (不限制)
- ❏ Kernel版本: 2.6.32(不限制)
- ❏ 需要與安裝套件: vim, dhcp3-server

作業系統不限制Ubuntu!!

防火牆 (Firewall)

❖ 單一主機型

- Netfilter (封包過濾機制)
 - 分析進入主機的封包，擷取封包的header並判斷通過或阻擋。
- TCP Wrappers (程式控管)
 - 判斷程式的名稱並決定是否通行，與程式啟動的port無關。

❖ 區域型

- Netfilter
- Proxy (代理伺服器)
 - Proxy代理使用者的需求，使用者並非直接連上Internet，而是透過Proxy存取網路服務。

防火牆 (Firewall)

❖ 防火牆的功能

- 拒絕讓Internet的封包進入主機的特定port
- 拒絕讓某些來源IP的封包流入
- 拒絕讓帶有某些特殊旗標(Flag)的封包流入
- 分析硬體位址(MAC)來決定連線與否

❖ 防火牆的缺點

- 不能有效的抵擋病毒或木馬程式
- 防火牆防護來自內部LAN的攻擊較差

IPTables

❏ chains

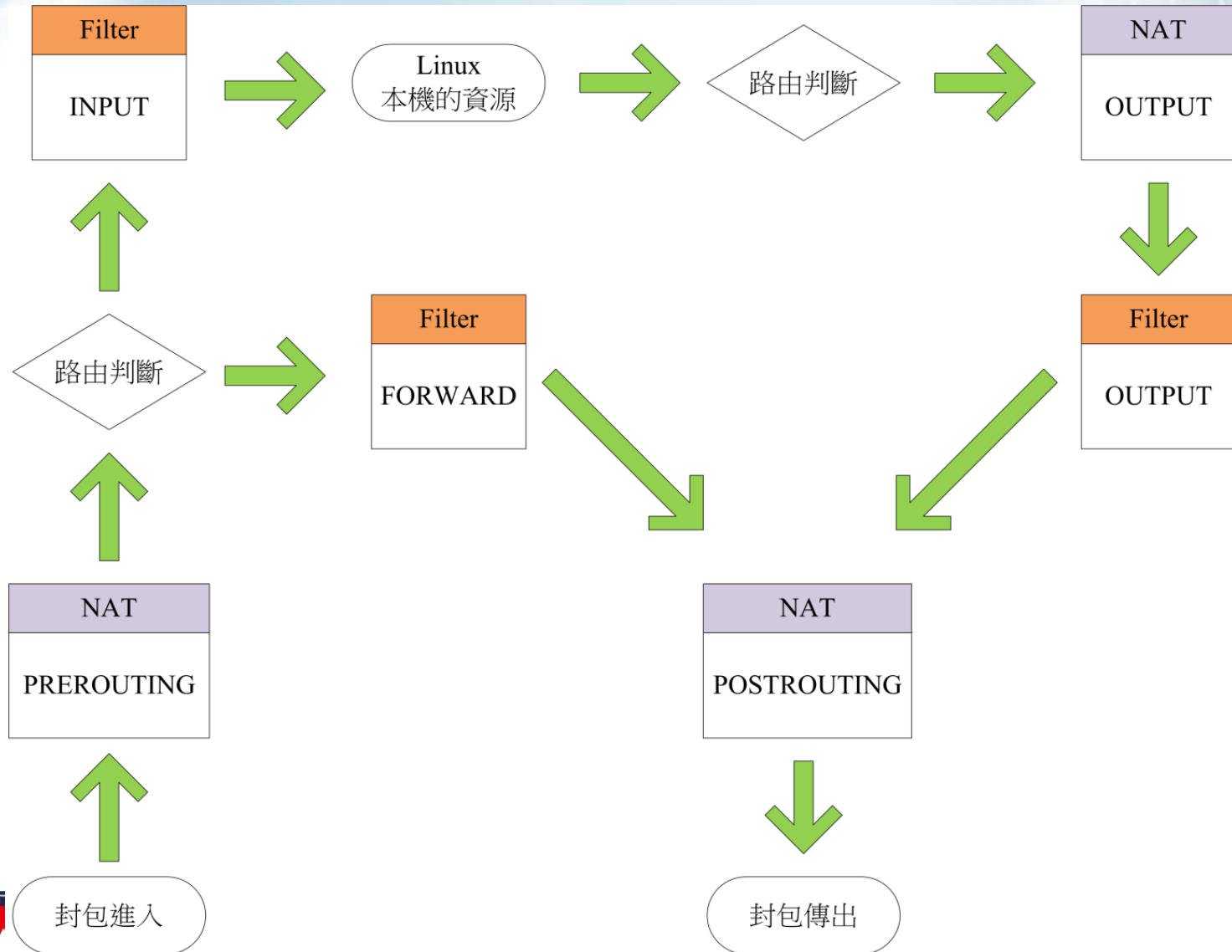
- PREROUTING
- INPUT
- FORWARD
- OUTPUT
- POSTROUTING

❏ 更詳細的解釋可以在linux輸入“man iptables”查詢

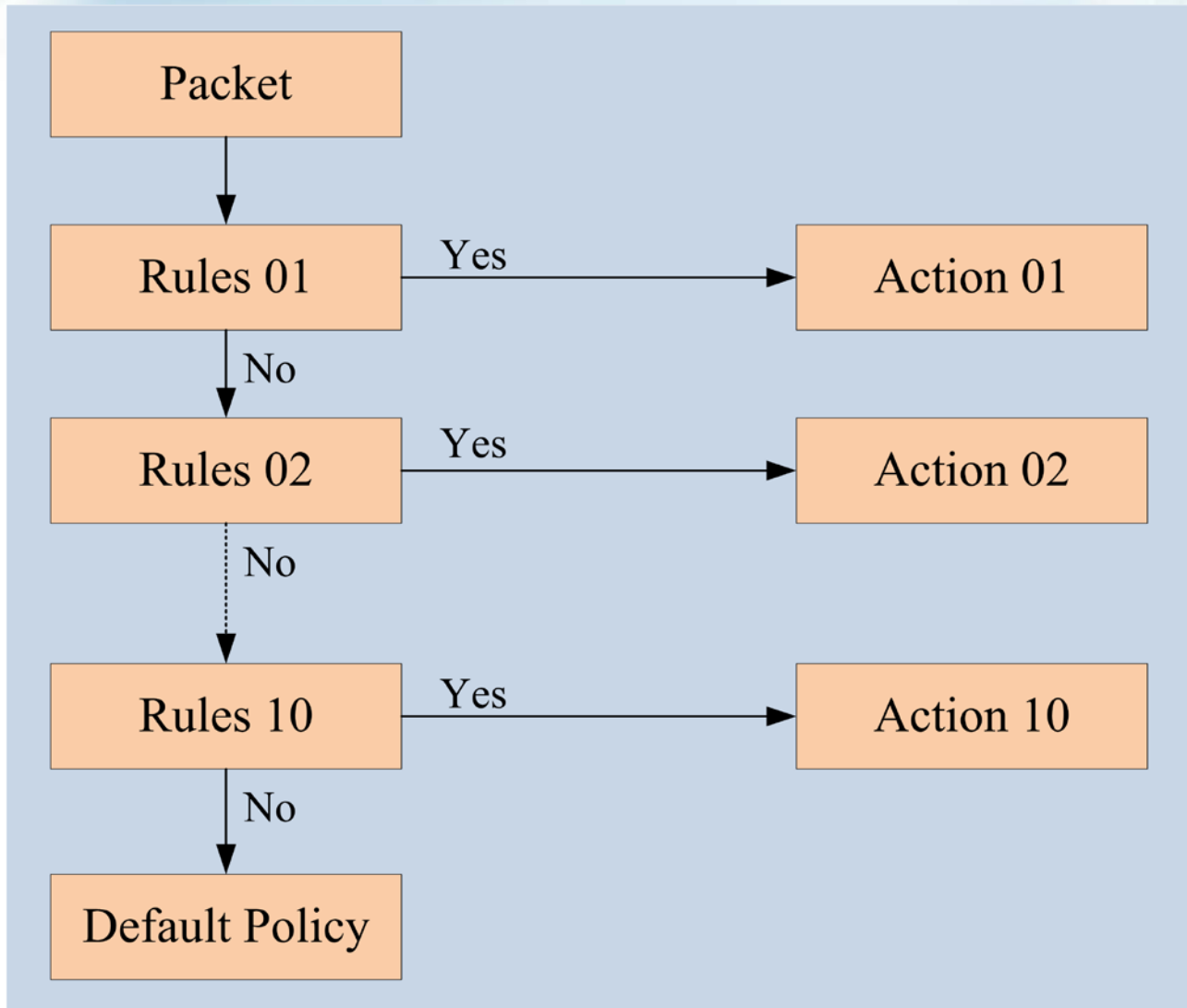
❏ 使用iptables指令時必須要有root的權限

- Ubuntu 加上 sudo

IPTables



封包過濾的規則與流程



IPTables

tables

- Filter (過濾器)
 - 處理進入與出去本機端的封包。
- NAT (位址轉換)
 - 來源與目的之IP與Port的轉換。
- Mangle (破壞者)
 - 處理特殊旗標
 - 較少使用
- Raw
 - 設定例外的狀況

查看Table

🌀 iptables [-t tables] [-L] [-nv]

```
r99944039@ubuntu:/$ sudo iptables -t filter -L -n
Chain INPUT (policy ACCEPT)
target      prot opt source                destination

Chain FORWARD (policy ACCEPT)
target      prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target      prot opt source                destination
```

Target	Prot	Opt	Source	Destination
進行的動作	封包協定	額外的選項	來源IP	目的IP

🌀 不指定Table時預設為filter table.

查看網路介面

🌐 ifconfig

```
r99944039@ubuntu:/$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:8e:4f:7e
          inet addr:192.168.81.128  Bcast:192.168.81.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe8e:4f7e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5962 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2557 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7393947 (7.3 MB)  TX bytes:174507 (174.5 KB)
          Interrupt:19 Base address:0x2024

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:480 (480.0 B)  TX bytes:480 (480.0 B)
```

清除防火牆的所有規則

☒ 指令

- iptables -F
- iptables -X
- iptables -Z (清空計數器)

定義預設政策 (Policy)

❏ iptables [-t tables] -P [INPUT, OUTPUT, FORWARD]
[ACCEPT, DROP]

```
r99944039@ubuntu:/$ sudo iptables -t filter -P INPUT DROP
r99944039@ubuntu:/$ sudo iptables -t filter -L -n
Chain INPUT (policy DROP)
target      prot opt source                destination

Chain FORWARD (policy ACCEPT)
target      prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target      prot opt source                destination
```

設定基本規則

❏ iptables [-AID 鏈] [-io 網路介面] [-p 協定] [-s 來源IP/網域] [-d 目的IP/網域] -j [ACCEPT | DROP | REJECT | LOG]

- -A 將rule放在chain的最後一個
- -I number 指定rule放在chain的位置
- -D 刪除rule
- -I 與INPUT配合
- -o 與OUTPUT配合

IPTables 範例

❖ 允許Http封包

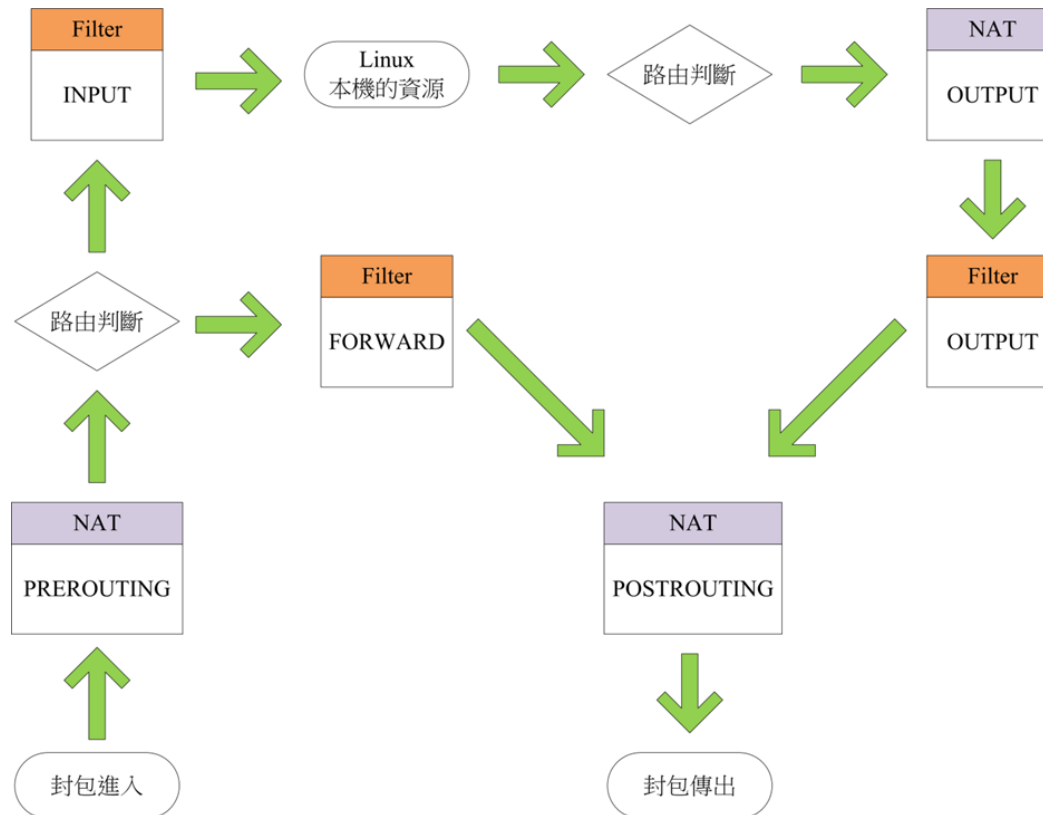
- iptables -A INPUT -i eth0 -p tcp --sport 80 -j ACCEPT
- iptables -A OUTPUT -o eth0 -p tcp -dport 80 -j ACCEPT

❖ 丟棄所有來自INPUT的封包

- iptables -P INPUT DROP

NAT

- ❏ NAT table的PREROUTING chain修改目的IP
- ❏ NAT table的POSTROUTING chain修改來源IP



NAT範例

❖ 將來自內部網路的封包傳送出去

- `iptables -t nat -A POSTROUTING -s 192.168.100.0/24 -o eth0 -j MASQUERADE`

❖ 將來自外部網路的封包轉到內部網路的Web主機上

- `iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to-destination 192.168.100.10:80`

❖ 主機上有二張網卡，讓主要機器成為路由器

- `echo "1" > /proc/sys/net/ipv4/ip_forward`

❖ 若發生/`proc/sys/net/ipv4/ip_forward` permission denied

- `sudo sh -c "echo 1 > /proc/sys/net/ipv4/ip_forward"`

DHCP Server

❏ 安裝DHCP

- `sudo apt-get install dhcp3-server`

❏ 設定發放IP的網路介面卡

- `sudo vim /etc/default/isc-dhcp-server`
- `INTERFACE = "eth1"`

❏ 設定DHCP Server

- `sudo vim /etc/dhcp/dhcpd.conf`

❏ 啟動DHCP Server

- `sudo /etc/init.d/isc-dhcp-server start`

DHCP Server

🌀 dhcpd.conf 基本設定

```
option domain-name "d98922029.stu";  
option domain-name-servers 140.112.254.4, 140.112.17.1;  
default-lease-time 6000;  
max-lease-time 72000;  
subnet 192.168.100.0 netmask 255.255.255.0{  
    range 192.168.100.20 192.168.100.100;  
    option routers 192.168.100.254;  
    option broadcast-address 192.168.100.255;  
}
```

Domain Name

DNS Server

預設使用者租約時間

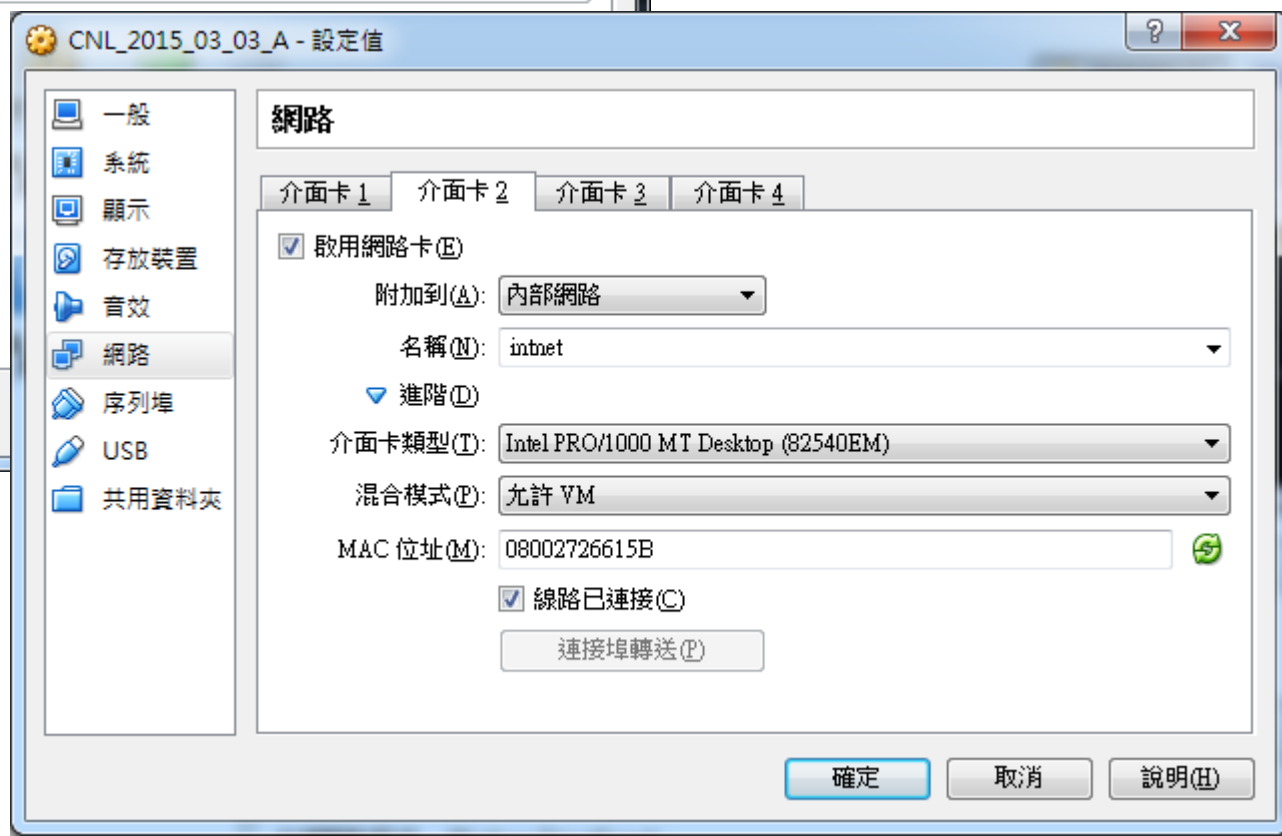
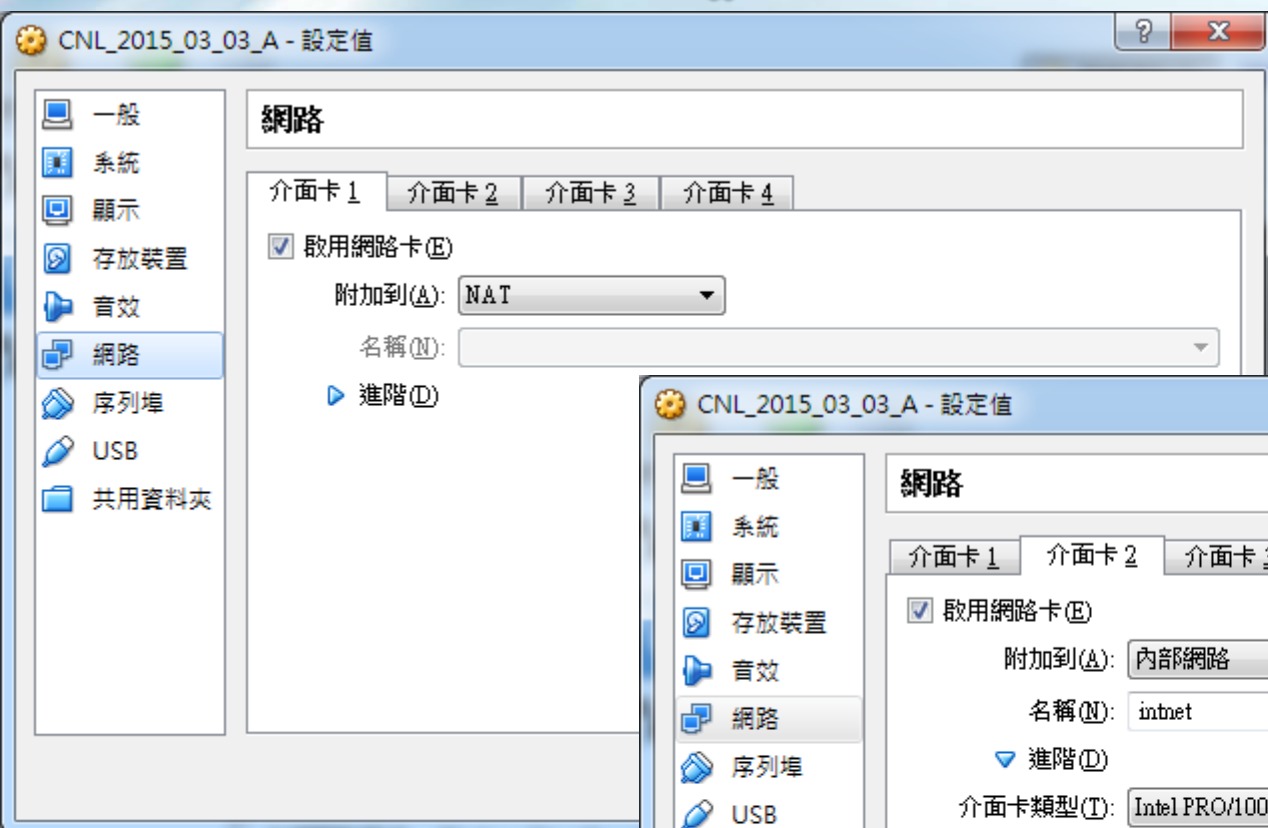
使用者租約時間上限

IP發放範圍

指定的Routers

Broadcast Address

VM_a's configuration



Editing Wired connection 1

Connection name: **Wired connection 1**

General Ethernet 802.1x Security IPv4 Settings IPv6 Settings

Method: Automatic (DHCP) ▼

Addresses

Address	Netmask	Gateway

Add

Delete

Additional DNS servers:

Additional search domains:

DHCP client ID:

☐ Require IPv4 addressing for this connection to complete

Routes...

Cancel Save...

Editing Wired connection 2

Connection name: **Wired connection 2**

General Ethernet 802.1x Security IPv4 Settings IPv6 Settings

Method: Manual ▼

Addresses

Address	Netmask	Gateway
192.168.100.254	255.255.255.0	192.168.100.254

Add

Delete

DNS servers:

Search domains:

DHCP client ID:

☐ Require IPv4 addressing for this connection to complete

Routes...

Cancel Save...

VM_b's configuration

Left Window: CNL_2015_03_03_B - 設定值

網路 (Network)

介面卡 1 | 介面卡 2 | 介面卡 3 | 介面卡 4

☒ 啟用網路卡(E)

附加到(A): 內部網路

名稱(N): intnet

進階(D)

介面卡類型(T): Intel PRO/1000 MT Desktop (82540EM)

混合模式(P): 允許 VM

MAC 位址(M): 080027C1ACAA

☒ 線路已連接(C)

連接埠轉送(P)

確定

Right Window: Editing Wired connection 1

Connection name: Wired connection 1

General | Ethernet | 802.1x Security | IPv4 Settings | IPv6 Settings

Method: Automatic (DHCP)

Addresses

Address	Netmask	Gateway	
			Add
			Delete

Additional DNS servers:

Additional search domains:

DHCP client ID:

☐ Require IPv4 addressing for this connection to complete

Routes...

Cancel Save...

實驗一展演要求

❖ (5%)電腦B能夠透過DHCP伺服器得到private IP address.

- Private IP 發放參考下表

Address Range	mask
192.168.0.0 - 192.168.255.255	192.168.0.0/255.255.0.0

❖ (11%)利用Shell scripts撰寫你的Firewall和NAT規則並說明程式架構與邏輯。

❖ (10%)電腦B要能用電腦A上的NAT獲得private IP並與外部網路連結。(ex., ping www.google.com)

實驗一展演要求

- ❏ (24% ;1個應用程式4%)電腦B要能夠正常運作指定的程式。除了基本的DNS、HTTP、FTP、Telnet和ICMP之外，各組還要依組別號碼除以4的餘數來選擇第六個應用程式。其餘的封包一律檔掉。展演時，除了上述的應用程式可以正常使用之外，還要用抓封包的軟體來證實你們設計的firewall是正確的。

餘數	應用程式
餘0	Line
餘1	SSH
餘2	POP3/SMTP
餘3	Skype

實驗一結報要求

1. (30%)將你們設計的Firewall與NAT裡面的chains畫成流程圖，清楚說明裡面的規則，並在旁邊附上解釋。
2. (10%)用抓封包的軟體(wireshark)抓一些封包來證明你們設計的Firewall與NAT是正確的。請先整理好，列出關鍵的封包。
3. (10%)請寫下本次實驗內容如何應用於實際情況，請詳盡描述情境與假設條件。
4. 結報請在展演時一起交上。
5. 結報請填上貢獻度。

參考資料

❏ <http://www.netfilter.org/>

- Document -> HOWTOs

❏ <http://linux.vbird.org/> 鳥哥的Linux私房菜

❏ <http://www.thegeekstuff.com/2011/01/iptables-fundamentals/>

R204實驗注意事項

- ❏ 螢幕、鍵盤、滑鼠、網路線請使用204電腦原本的線材，實驗完畢後請記得歸位。