IP Layer Basics, Firewall, VPN, and NAT

Prof. Michael Tsai 2013/4/29 and 2013/5/6

IP (Network layer) 的主要功能

1. Forwarding: Router通常有多個interface (網卡)。把packet從來源的interface移到目的地方向的interface並發送出去叫做forwarding。
   - 一般client並不會開啟此一功能!
2. Routing: 找出往目的地方向的一條路徑。通常由routing algorithms/protocol決定。

- 因為系上通常到特定的目的地都只有一條路徑，我們網管的工作通常只會接觸到第一部分。

系上防火牆的Routing table (部分)

192.168.48.0/
255.255.248.0

192.168.219.0/
255.255.255.0

192.168.55.254

192.168.219.254

140.112.30.254

140.112.28.0/
255.255.252.0

Routing Table:
192.168.48.0 255.255.248.0 192.168.55.254
192.168.219.0 255.255.255.0 192.168.219.254
140.112.28.0 255.255.252.0 140.112.30.254
0.0.0.0 0.0.0.0 140.112.x.x

IP封包的格式(v4)

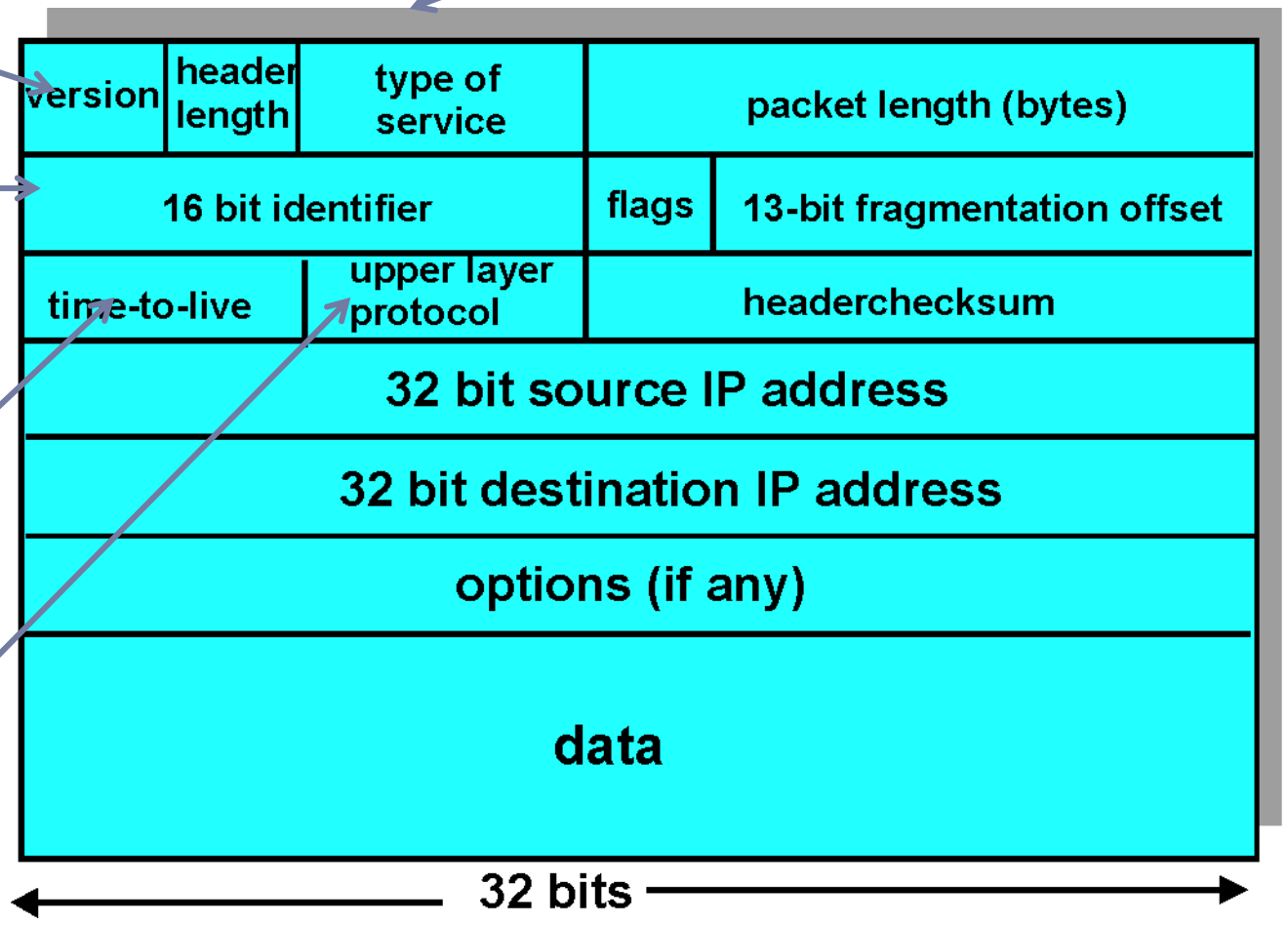
表示是否需要特殊處理(如即時的影像或聲音)

v4 or v6

用來處理fragmentation

最多可以經過幾台機器(router)

Transport layer使用的協定(通常為TCP or UDP)



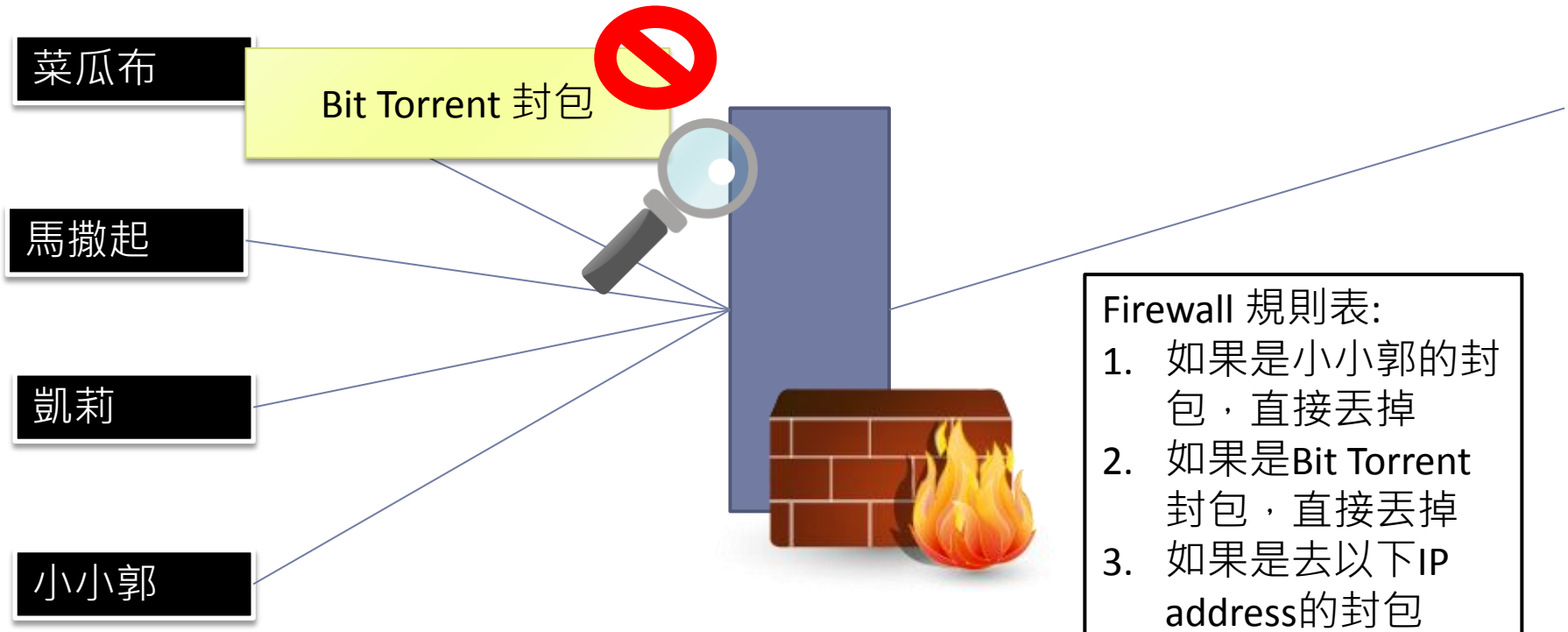
ICMP (Internet Control Message Protocol)

- 一些管理用的訊息，用來通知client關於網路的狀況。
- 常用的用途:
  1. 通知client此路不通。(Destination network/host/protocol/port unreachable or unknown)
  2. Ping使用的echo request & reply

```
C:\Users\Administrator>ping 8.8.8.8

Ping 8.8.8.8 (使用 32 位元組的資料):
回覆自 8.8.8.8: 位元組=32 時間=20ms TTL=128
回覆自 8.8.8.8: 位元組=32 時間=20ms TTL=128
回覆自 8.8.8.8: 位元組=32 時間=20ms TTL=128
回覆自 8.8.8.8: 位元組=32 時間=20ms TTL=128

8.8.8.8 的 Ping 統計資料:
    封包: 已傳送 = 4，已收到 = 4，已遺失 = 0 (0% 遺失)，
大約的來回時間 (毫秒):
    最小值 = 20ms，最大值 = 20ms，平均 = 20ms

C:\Users\Administrator>_
```

  3. TTL expire (用來偵測或預防路徑中的loop或是traceroute使用)

Firewall



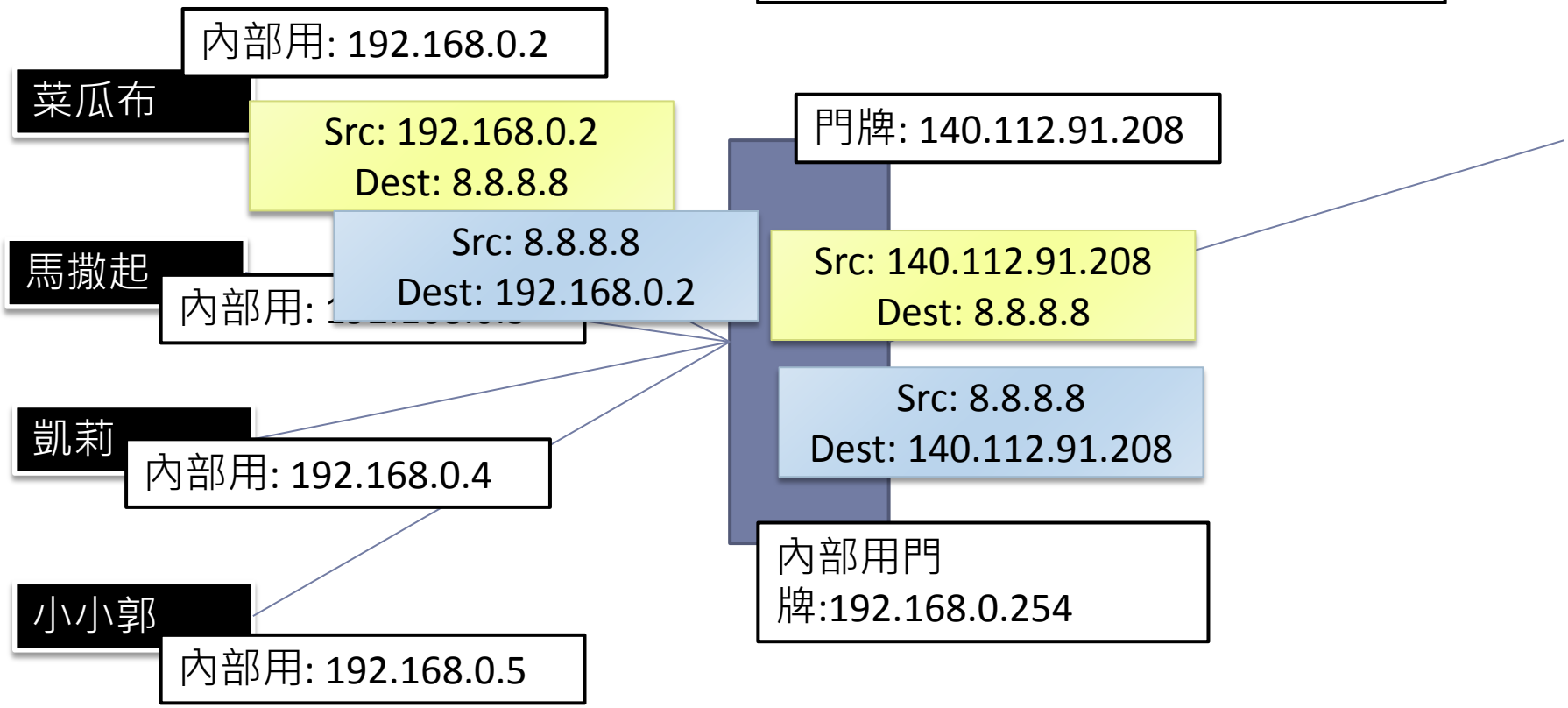
Firewall 規則表:

1. 如果是小小郭的封包，直接丟掉
2. 如果是Bit Torrent封包，直接丟掉
3. 如果是去以下IP address的封包 (x.x.x.x, y.y.y.y, z.z.z.z)直接丟掉
4. 剩下的可以過

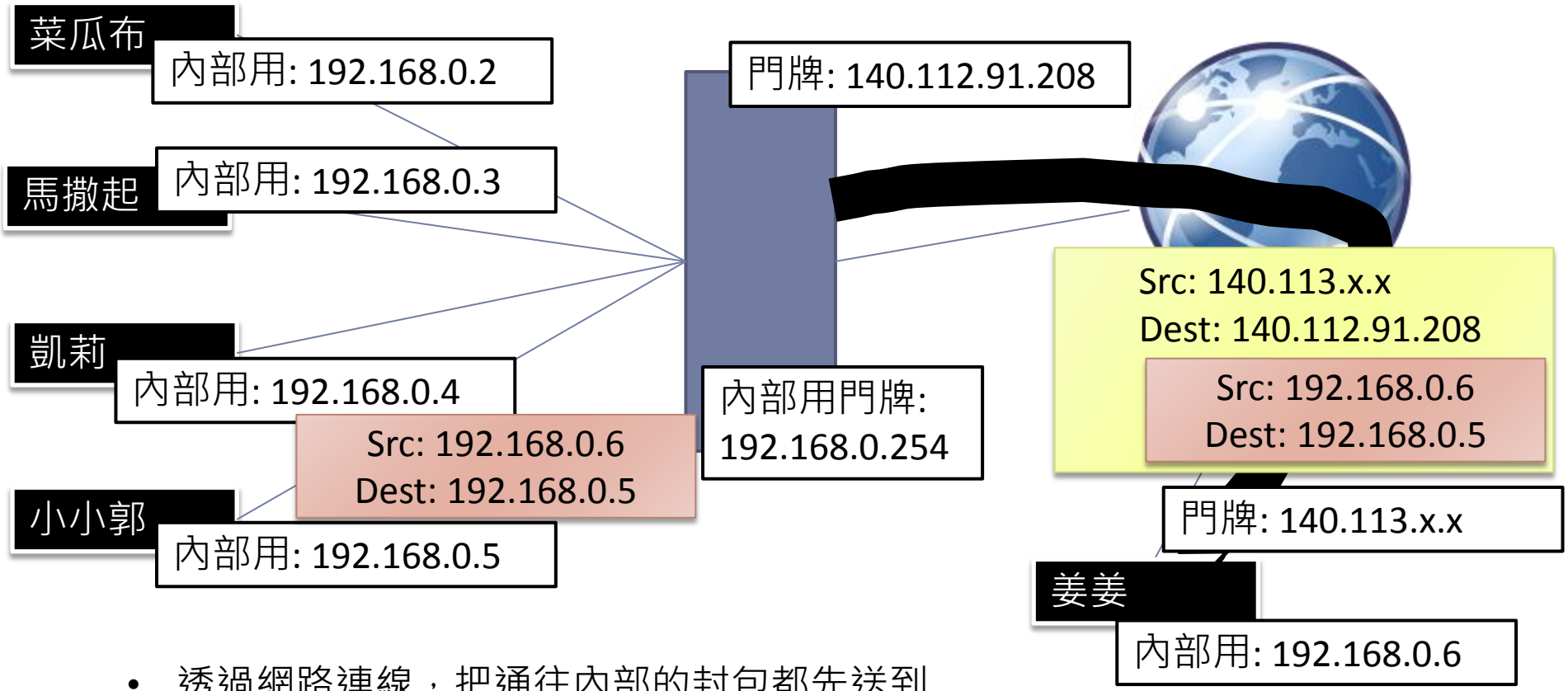
NAT (Network Address Translation)

只有一塊門牌發給我們，怎麼辦呢?

對照表:
- 菜瓜布有連到8.8.8.8
- 要找助教請轉到192.168.0.4



VPN (Virtual Private Network)



- 透過網路連線，把通往內部的封包都先送到140.112.91.208，然後再解開轉送到真正的目的地