IP, ICMP, DNS, and DHCP

Prof. Michael Tsai 2012/10/22

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

192.168.55.254

140.112.28.0/
255.255.252.0

140.112.30.254

192.168.219.0/
255.255.255.0

192.168.219.254

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 0.0.0.0 140.112.30.254

IP封包的格式(v4)

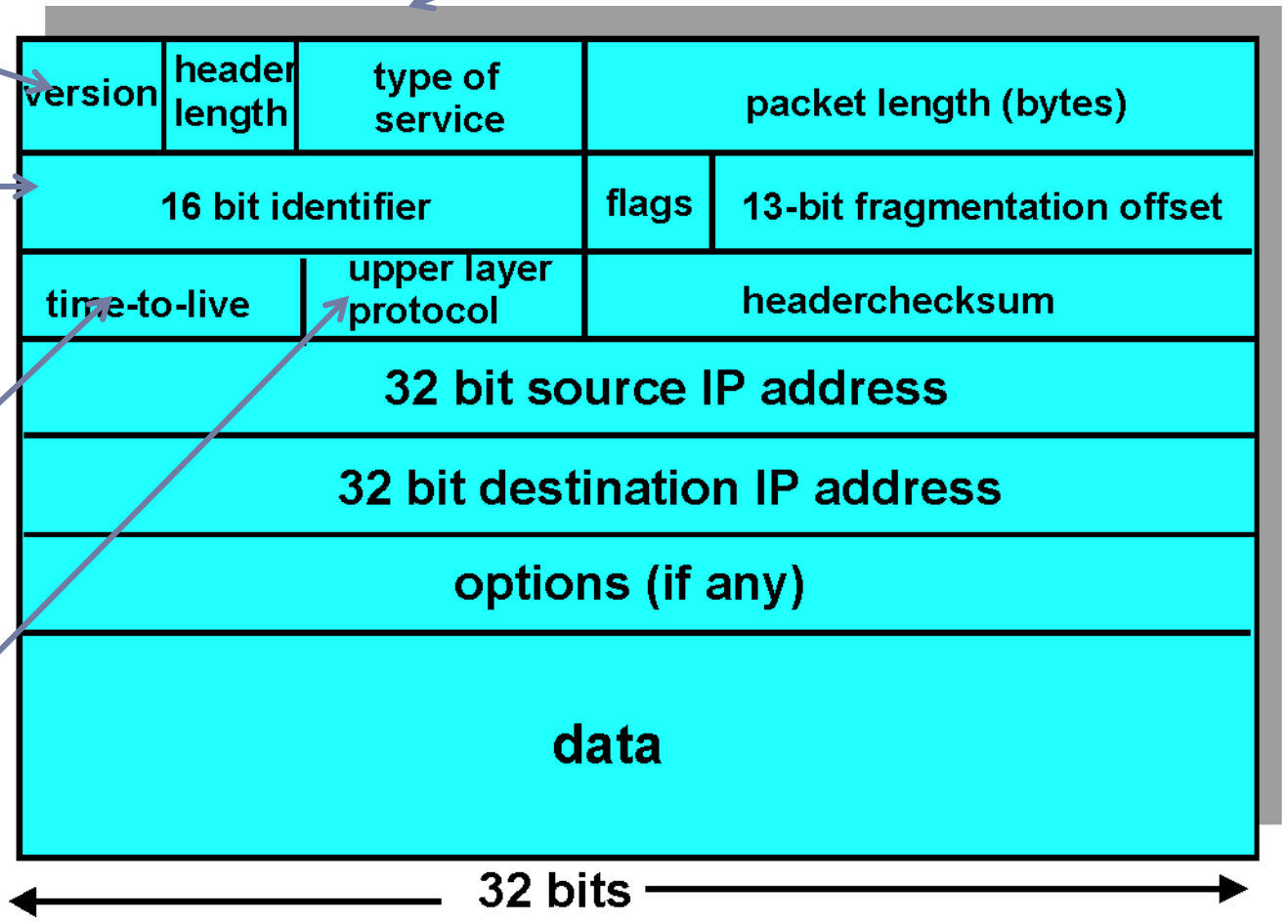
表示是否需要特殊處理(如即時的影像或聲音)

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)

DHCP (Dynamic Host Configuration Protocol)

- 每個地方有自己的subnet及IP設定
- 到一個新的地方，一開始怎麼取得此一subnet的IP呢?
- 通常同一個subnet中會設置一台DHCP server
- 此server將負責"接待"新來的機器，分發未使用的IP給它們
- 想像全系如果都需要手動設定IP, 會發生什麼事情?
  - 網管需要分配IP給所有電腦 (全系有多少電腦???)
  - IP衝突 (同樣的IP被不同的電腦使用)

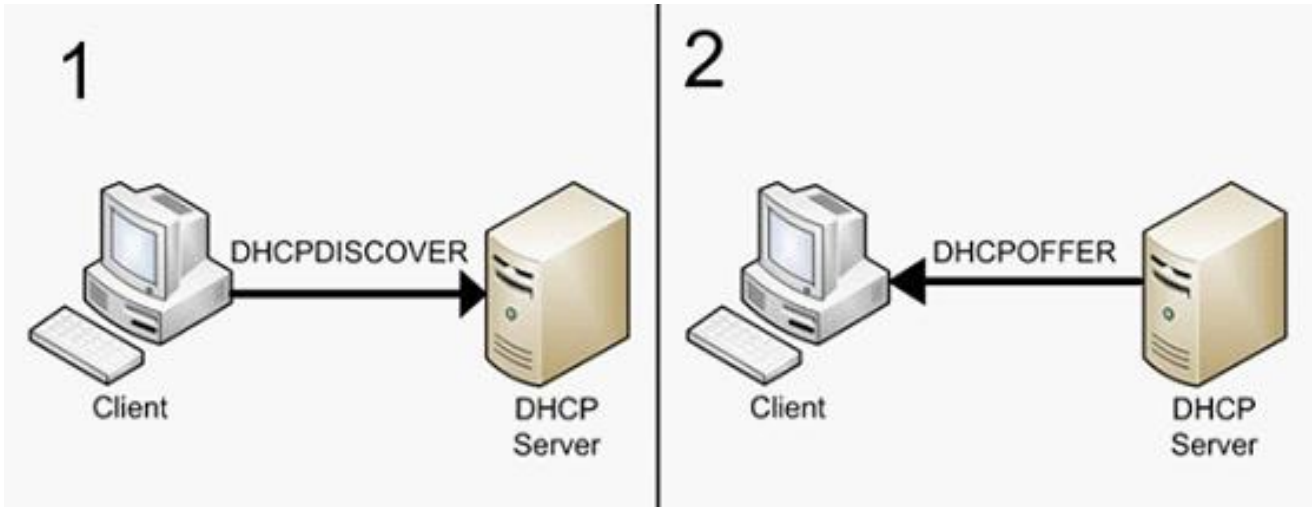
DHCP 4部曲

DHCP Discover: 請問有人可以發IP給我嗎?

Src: 0.0.0.0, 68
Dest: 255.255.255.255, 67
DHCPDISCOVER
Yiaddr: 0.0.0.0
Transaction ID: 654
Request:
Subnet Mask, Router, Domain Name Server

DHCP Offer:我這邊有一組IP看看你要不要用.

Src: 192.168.55.254, 67
Dest: 255.255.255.255, 68
DHCPOFFER
Yiaddr: 192.168.48.15
DHCP server ID: 192.168.55.254
Transaction ID: 654
Lifetime: 4 hrs
Netmask: 255.255.248.0
Router: 192.168.55.254
DNS: 140.112.30.21, 140.112.254.4



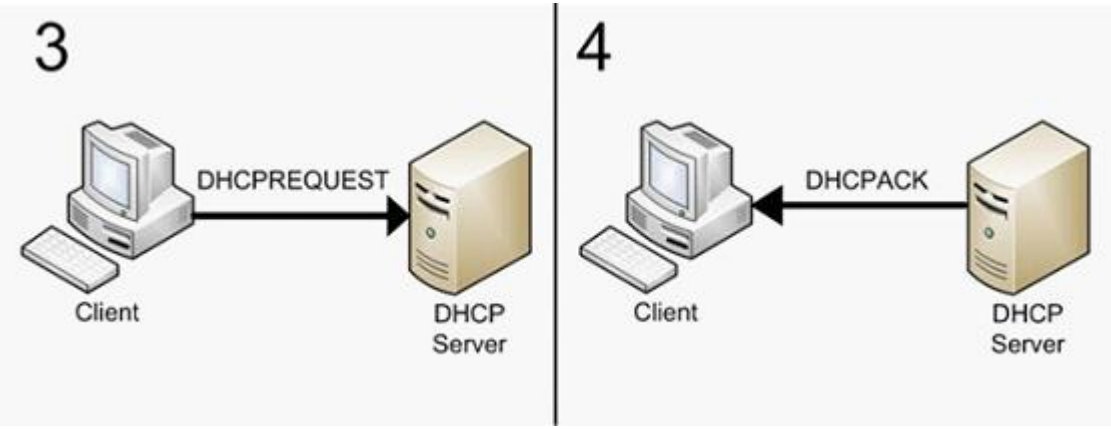
DHCP 4部曲

DHCP Request:那我要把這組IP拿走囉!

Src: 0.0.0.0, 68
Dest: 255.255.255.255, 67
DHCPREQUEST
Yiaddr: 192.168.48.15
Transaction ID: 655
DHCP server ID: 192.168.55.254
Lifetime: 4 hrs

DHCP Ack: 沒問題. 請用.

Src: 192.168.55.254, 67
Dest: 255.255.255.255, 68
DHCPACK
Yiaddr: 192.168.48.15
DHCP server ID: 192.168.55.254
Transaction ID: 655
Lifetime: 4 hrs
Netmask: 255.255.248.0
Router: 192.168.55.254
DNS: 140.112.30.21, 140.112.254.4



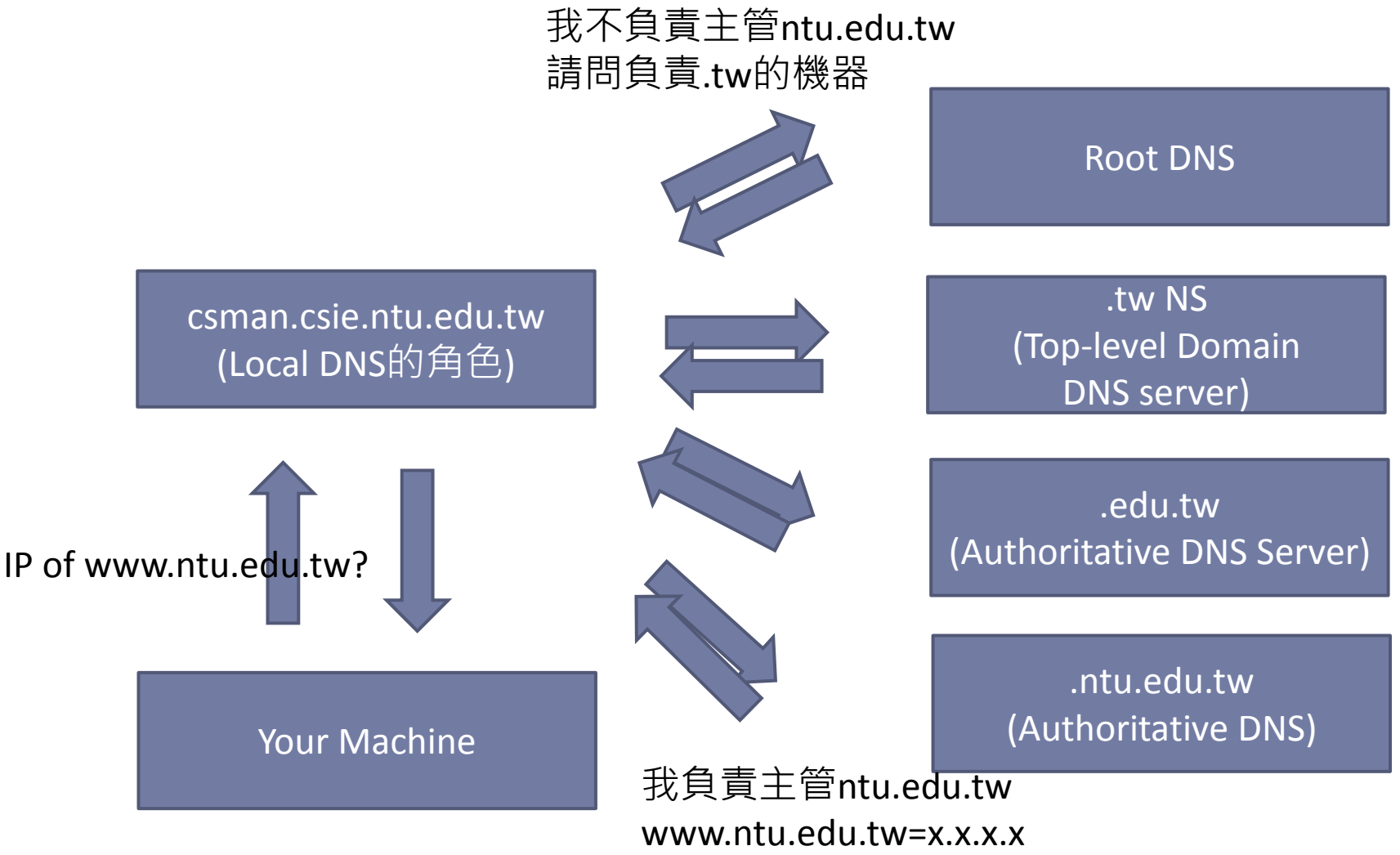
DHCP 的細節

- 一個subnet上可能有多個DHCP server. 因此發出DHCPREQUEST之後，可能收到多個DHCPOFFER。
- Client可以要求使用之前使用過的IP，但DHCP server可以拒絕(可能根本已經不在同一個網段，或是已經被別的client使用中)
- Authoritative & non-authoritative: 有主管權的DHCP server可以發出”拒絕”client使用某IP的要求，而沒有主管權的DHCP server則會忽略該要求(沒有回應)
- 想想看: DHCP server的安全漏洞. 如果有人接在系上網路上且開啟DHCP server，會發生什麼事情?

DNS (Domain Name Service)

- 一言以蔽之: 將名稱轉為IP的服務
- 常見的轉換種類:
  - Domain name -> IP (type A):
    ntucsv.csie.ntu.edu.tw -> 140.112.30.28
  - @domainname的mail server (type MX):
    csie.ntu.edu.tw -> ASPMX.L.GOOGLE.COM
  - Domain name -> domain name (type CNAME):
    www.csie.ntu.edu.tw -> ntucsv.csie.ntu.edu.tw
  - IP -> domain name (type PTR)
    1 40.112.30.21 -> csman.csie.ntu.edu.tw
- 可以多重宣告: 增加可靠度或分散性.
  - 例如www.google.com的A指到了6個IP!

分散式的架構: 分層負責 (recursive query)



DNS的細節

- 如果local DNS本身主管被查詢的domain，則可以直接回覆。
  - 稱為iterative query
  - 例如140.112.30.21如果被查詢www.csie.ntu.edu.tw
- Local DNS可以暫存之前查詢過的結果。
  - 主要用來減輕主管DNS server及網路的負擔。
  - 每筆在主管DNS server上的紀錄都有對應的TTL值，規範可以被占存多久。

作業

1. 使用tracert或traceroute搜尋從你的機器到google DNS (IP: 8.8.8.8)的路徑。用wireshark把所有發出的相關封包都擷取下來觀察。
   1. 請問發出用來偵測路徑的IP封包TTL欄位數值如何變化? 為什麼是這樣設計的?
   2. 請把由你的機器到8.8.8.8的路徑寫下來。為什麼中間有些機器沒有出現?
2. 使用工作站上dig指令練習查詢DNS。必要的時候，請用man dig指令查詢使用說明。(如果自己的機器有dig指令的話也歡迎使用)
   1. 請列出負責csie.ntu.edu.tw網域的主管DNS IP位址。請問你是用什麼指令查詢的?
   2. 請列出@ntu.edu.tw的郵件位址負責收信的主機IP位址。請問你是用什麼指令查詢的?
   3. 列出root DNS的IP位址。請問你是用什麼指令查詢的?
3. 為什麼DNS要使用分層負責的分散式架構? 如果有一台主機負責所有的名稱轉換，請列出三個此一集中式架構的壞處。
4. 為什麼目前的IP protocol需要使用IP address作為轉送到哪邊的依據，而不直接使用人可以閱讀的domain name就好?