B03102082

陳孝思

NA

1. DHCP

   那台 DHCP 伺服器可能設有 DHCP reservation，針對特定電腦的 MAC address 給予保留的 IP

   ref: http://www.tomshardware.com/faq/id-1932491/difference-dhcp-reservation-dhcp-exclusion.html

2. (a).

   1. 只用一台 DNS 伺服器不可能處理所有的轉換，流量太大了
   2. 如果唯一那一台壞了，那所有人都無法轉換了，相反地，如果是分散式的，壞了一台還有別台可以替代
   3. 離 DNS 伺服器越近的地方速度越快，如果只有一台，放在哪勢必都會影響離該伺服器較遠的客戶端的連線速度，而分散式的就沒有這個問題，大家附近都有一台

   Ref: http://www.omnisecu.com/tcpip/advantages-of-distributed-dns-infrastructure-architecture.php

   (b). DNS 快取是把最近查詢過的網址所對應的 IP 記錄下來，每次要連到一個網址的時候，先檢查 DNS 快取裡有沒有這組網址所對應的 IP，好處是如果在短時間內要連到同個網址，不用重新去 DNS 伺服器查 IP

   Ref: https://www.lifewire.com/what-is-a-dns-cache-817514

   (c).

```
b03102082@linux1 [/tmp2/b03102082] ./dig.sh www.csie.ntu.edu.tw
00000000  00 00 81 80 00 01 00 01  00 03 00 03 03 77 77 77  |.............www|
00000010  04 63 73 69 65 03 6e 74  75 03 65 64 75 02 74 77  |.csie.ntu.edu.tw|
00000020  00 00 01 00 01 c0 0c 00  01 00 01 00 00 01 75 00  |..............u.|
00000030  04 8c 70 1e 1a c0 10 00  02 00 01 00 00 00 5f 00  |..p............_.|
00000040  08 05 63 73 6d 61 6e c0  10 c0 10 00 02 00 01 00  |..csman.........|
00000050  00 00 5f 00 09 06 63 73  6d 61 6e 32 c0 10 c0 10  |.._...csman2....|
00000060  00 02 00 01 00 00 00 5f  00 08 05 6e 74 75 6e 73  |......._...ntuns|
00000070  c0 15 c0 41 00 01 00 01  00 00 01 b5 00 04 8c 70  |...A...........p|
00000080  1e 0d c0 6a 00 01 00 01  00 00 e0 67 00 04 8c 70  |...j.......g...p|
00000090  03 10 c0 55 00 01 00 01  00 00 01 b5 00 04 8c 70  |...U...........p|
000000a0  1e 0e                                            |..|
000000a2
```

   ref: http://www.fauser.edu/~fuligni/files/classi5/sistemi-reti/project1-primer (DNS message structure).pdf

(d).

```
b03102082@linux1 [/tmp2/b03102082] ./dig.sh www.csie.ntu.edu.tw
00000000  00 00 81 80 00 01 00 01  00 03 00 03 03 77 77 77  |.............www|
00000010  04 63 73 69 65 03 6e 74  75 03 65 64 75 02 74 77  |.csie.ntu.edu.tw|
00000020  00 00 01 00 01 c0 0c 00  01 00 01 00 00 01 75 00  |..............u.|
00000030  04 8c 70 1e 1a c0 10 00  02 00 01 00 00 00 5f 00  |..p.........._.|
00000040  08 05 63 73 6d 61 6e c0  10 c0 10 00 02 00 01 00  |..csman.........|
00000050  00 00 5f 00 09 06 63 73  6d 61 6e 32 c0 10 c0 10  |.._...csman2....|
00000060  00 02 00 01 00 00 00 5f  00 08 05 6e 74 75 6e 73  |......._...ntuns|
00000070  c0 15 c0 41 00 01 00 01  00 00 01 b5 00 04 8c 70  |...A...........p|
00000080  1e 0d c0 6a 00 01 00 01  00 00 e0 67 00 04 8c 70  |...j.......g...p|
00000090  03 10 c0 55 00 01 00 01  00 00 01 b5 00 04 8c 70  |...U...........p|
000000a0  1e 0e                                            |..|
000000a2
```

csman: c010 0002 0001 0000005f 0008 0563736d616ec010

c010 是 name 的部分，且是表示 compression label，代表此 domain name 出現過，c 代表是 pointer，010 是 offset，從第 010 個字(此處為 04)

0002 為 type(RDATA 的 type)，此處為 name server

0001 為 Class，此處為 IN

0000005f 為 TTL

0008 為 RDLENGTH，也就是後面 RDATA 的長度

0563736d616ec010 為 RDATA，此處資料為 name server，格式同 name，此處開頭不是 c，所以是 data label，05 表示長度為 5，63736d616e 為 csman 的 ASCII，c010 為 compression label，表示接在後面的資料是從 offset 為 010 開始出現過的 domain name，所以整個 name server 為 csman.csie.ntu.edu.tw

csman2：c010 0002 0001 0000005f 0009 0663736d616e32c010

同理

ntuns: c010 0002 0001 0000005f 0008 056e74756e73c015

大部份相同，除了最後一部份 056e74756e73c015 中的 c015，此處接在後面的資料是從 offset 為 15(此處為 65)開始出現過的 domain name，所以整個 name server 為 ntuns.ntu.edu.tw

因為 DNS 使用 UDP 為傳遞機制，UDP 保護措施較少，封包遺失了也不見得會重傳，且封包越大越容易傳遞失敗或損毀，所以如果 DNS server 不壓縮較大的回覆封包的話，該回復封包出錯的可能會增加，甚至傳遞失敗，造成使用者要多查詢幾次才能連到使用者想去的網站，浪費網路資源。

Ref: http://www.fauser.edu/~fuligni/files/classi5/sistemi-reti/project1-primer (DNS message structure).pdf

Ref: http://www.keyboardbanger.com/dns-message-format-name-compression/

(e).

1. DNS cache poisoning，透過系統漏洞在 DNS 快取中放置假的 DNS 快取，讓網址對應到假的 IP，可以透過 transport layer 層(HTTPS)檢查數位簽章是否是預期的網站來得知有無 DNS cache poisoning，DNS 伺服器可以透過忽略回傳的網址與 IP 的對應關係中，與查詢的網址無關的 IP，和減少使用別的 DNS 伺服器的資訊來避免 DNS cache poisoning

Ref: https://en.wikipedia.org/wiki/DNS_spoofing

2. DNS amplification attack，透過偽造攻擊目標的 IP 來向 DNS 伺服器傳送大量查詢，將大量的查詢結果封包導向攻擊目標的 IP，進行 DDoS 攻擊。可以關掉遞迴查詢來避免。

Ref: https://security.stackexchange.com/questions/93820/dns-reflection-attack-vs-dns-amplification-attack

https://betangel.kayako.com/article/107-how-do-i-secure-my-dns-resolver-against-amplification-attacks

3. DNS flood，透過傳送大量 DNS 查詢到特定 DNS 伺服器，癱瘓該伺服器，導致其他用戶無法使用該 DNS 伺服器而無法解析網址，無法透過網址連到該網址的伺服器。解決辦法為過濾惡意查詢封包，封鎖惡意連線的網址。

Ref: https://en.wikipedia.org/wiki/DNS_Flood