應用層

使用SSL方式進行通訊

Html是WHATWG制定的

Web storage

<https://www.huanlintalk.com/2012/06/html5-web-storage.html>

**Web Storage 要點整理**

1. HTML5 的 Web Storage 是一種可讓網頁將資料儲存於本地端的技術，其作用如同 cookie。
2. 儲存於 Web Storage 中的資料，是以 key-value pair 的形式保存（如同 cookie）。
3. Cookie 儲存空間很小，最多僅能儲存 4 KB 的資料。HTML5 Web Storage 的儲存空間則大得多，且依各家瀏覽器的實作而不同。一般應該至少有 5 MB 的空間。
4. 儲存於 cookie 中的資料會在用戶端瀏覽器與伺服器之間旅行（每次瀏覽器送出 request 至伺服器時就會夾帶 cookies），Web Storage 則不會（純粹運作於用戶端）。這表示 Web Storage 不會占用網路頻寬。
5. Web Storage 分為兩種：local storage 和 session storage。細節稍後會說明。

**Web Storage 有兩種**

|  |  |  |
| --- | --- | --- |
|  | 壽命長短 | 有效範圍 |
| local storage | 生命週期較長 | 可以跨瀏覽器分頁（tab） |
| session storage | 較短，只要瀏覽器視窗或分頁（tab）關閉就會消失。 | session storage 則不行。 |

----------------------------------------------------------------------------------------------------------------

Port：pop3/110 dns=53 https=443(gmail有用ssl) DHCP=67 SMTP=25(寄信) SNMP=161/162 NTP(網路時間協定)=123(udp)

IMAP=143 (**I**nternet **M**essage **A**ccess **P**rotocol)(收信)

----------------------------------------------------------------------------------------------------------------

IMAP和[POP3](https://zh.wikipedia.org/wiki/POP3" \o ")（Post Office Protocol - Version 3，郵局協定第三版）是郵件存取最為普遍的Internet標準協定。

<https://zh.wikipedia.org/wiki/%E5%9B%A0%E7%89%B9%E7%BD%91%E4%BF%A1%E6%81%AF%E8%AE%BF%E9%97%AE%E5%8D%8F%E8%AE%AE>

電子郵件所使用的通訊協定：smtp、pop3、imap

無論使用POP3還是IMAP4來取得訊息，客戶端均使用[SMTP](https://zh.wikipedia.org/wiki/SMTP)協定來傳送訊息

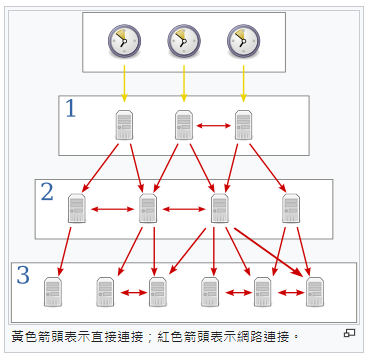
NTP(Network Time protocol)

<https://zh.wikipedia.org/wiki/%E7%B6%B2%E8%B7%AF%E6%99%82%E9%96%93%E5%8D%94%E5%AE%9A>

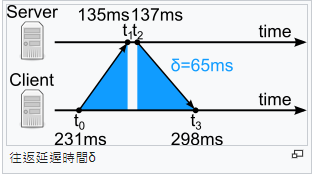
**網路時間協定**（英語：**N**etwork **T**ime **P**rotocol，縮寫：**NTP**）是在資料網路[潛伏時間](https://zh.wikipedia.org/wiki/%E6%BD%9C%E4%BC%8F%E6%97%B6%E9%97%B4)可變的[電腦系統](https://zh.wikipedia.org/wiki/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%B3%BB%E7%BB%9F)之間通過[封包交換](https://zh.wikipedia.org/wiki/%E5%88%86%E7%BB%84%E4%BA%A4%E6%8D%A2)進行[時鐘同步](https://zh.wikipedia.org/wiki/%E6%97%B6%E9%92%9F%E5%90%8C%E6%AD%A5)的一個網路協定，位於[OSI模型](https://zh.wikipedia.org/wiki/OSI%E6%A8%A1%E5%9E%8B)的[應用層](https://zh.wikipedia.org/wiki/%E5%BA%94%E7%94%A8%E5%B1%82)。

自1985年以來，NTP是目前仍在使用的最古老的[網際網路協定](https://zh.wikipedia.org/wiki/TCP/IP%E5%8D%8F%E8%AE%AE%E6%97%8F)之一。NTP由[德拉瓦大學](https://zh.wikipedia.org/wiki/%E7%89%B9%E6%8B%89%E5%8D%8E%E5%A4%A7%E5%AD%A6" \o "德拉瓦大學)的[David L. Mills](https://zh.wikipedia.org/w/index.php?title=David_L._Mills&action=edit&redlink=1)設計。

NTP使用一個分層、半分層的時間源系統。該層次的每個級別被稱為「stratum」，頂層分配為數字0。



1. 時間戳：NTP使用64[位元](https://zh.wikipedia.org/wiki/%E4%BD%8D%E5%85%83)的時間戳，其中32位元表示秒，32位元表示秒的小數
2. 時鐘同步演算法：



時間偏移：

往返延遲：

## ------------------------------------------------------------------------DNS:<http://linux.vbird.org/linux_server/0350dns.php>

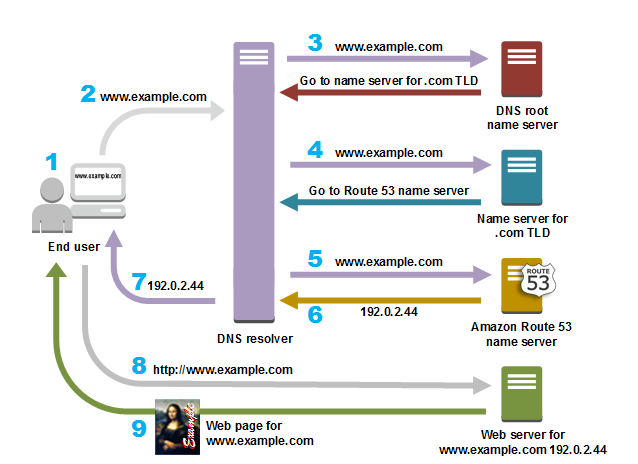
**網域名稱系統**（英語：**D**omain **N**ame **S**ystem，縮寫：**DNS**）是[網際網路](https://zh.wikipedia.org/wiki/%E4%BA%92%E8%81%94%E7%BD%91" \o "網際網路)的一項服務。

它作為將[域名](https://zh.wikipedia.org/wiki/%E5%9F%9F%E5%90%8D" \o "域名)和[IP位址](https://zh.wikipedia.org/wiki/IP%E5%9C%B0%E5%9D%80)相互[對映](https://zh.wikipedia.org/wiki/%E6%98%A0%E5%B0%84)的一個[分散式資料庫](https://zh.wikipedia.org/wiki/%E5%88%86%E5%B8%83%E5%BC%8F%E6%95%B0%E6%8D%AE%E5%BA%93)，能夠使人更方便地存取[網際網路](https://zh.wikipedia.org/wiki/%E4%BA%92%E8%81%94%E7%BD%91)。DNS使用[TCP](https://zh.wikipedia.org/wiki/%E4%BC%A0%E8%BE%93%E6%8E%A7%E5%88%B6%E5%8D%8F%E8%AE%AE" \o "傳輸控制協定)和[UDP](https://zh.wikipedia.org/wiki/%E7%94%A8%E6%88%B7%E6%95%B0%E6%8D%AE%E6%8A%A5%E5%8D%8F%E8%AE%AE" \o "使用者資料報協定)[埠](https://zh.wikipedia.org/wiki/TCP/UDP%E7%AB%AF%E5%8F%A3%E5%88%97%E8%A1%A8)53[[1]](https://zh.wikipedia.org/wiki/%E5%9F%9F%E5%90%8D%E7%B3%BB%E7%BB%9F#cite_note-1)。

通常 DNS 查詢的時候，是**以 udp 這個較快速的資料傳輸協定來查詢**的， 但是萬一**沒有辦法查詢到完整的資訊時，就會再次的以 tcp 這個協定來重新查詢**的

(透過DNS，可以由一部主機的完整網域名稱(FQDN,fully Qualified Domain Name)查到其IP位址)

Ex: <https://aws.amazon.com/tw/route53/what-is-dns/>



|  |
| --- |
| [www.flag.com.tw](http://www.flag.com.tw).  ( 最後面的”點”，dns架構中最上層網域--**根網域(root domain)** ) |
| www 就是這台web伺服器的主機名稱 |
| Flag.com.tw 就是這台伺服器所在的網域名稱 |
| tw : **頂層網域** |
| com : **第二層網域** |
| www : **主機** |
| 每個網域都至少要有一部DNS伺服器負責  子網域自成區域，或有直接上下關聯的才能稱作”區域” |
| 主要名稱伺服器(primary name server)：   1. 只能有一部，且一定要有一部 2. 區域檔案 🡺這個區域內的資料有所變更時，直接寫到這台伺服器的資料庫   次要名稱伺服器(secondary name server)：   1. 不能修改內容 2. 主要伺服器的備份 3. \*\*primary/secondary 名稱伺服器 = Master/Slave 名稱伺服器 (架構)   快取伺服器(cache only server)   1. 本身沒有管理任何區域 2. 當用戶向他要求時，他會向指定的DNS server查詢，然後回覆 3. 查完後就放進自己的快取內。下次再查同樣的，直接拿出即可 4. 用”主要名稱伺服器+快取伺服器” ：可以節省頻寬 5. 快取伺服器一旦重啟，資料會消失 6. 僅負責查詢與回應，並將結果快取下來以備使用。🡺僅能由client端向外部DNS查詢資料 |
| nslookup [www.google.com](http://www.google.com) 🡸可以查詢ip名稱 |
| nslookup 會使用網路中指定的DNS進行查詢 |
| nslookup [www.google.com](http://www.google.com) 168.95.1.1 🡸改向HiNet的DNS主機查詢 |
| 轉送程式(forwarder)：若特定的dns伺服器無法在指定時間完成(為了節省頻寬，先在特定的dns伺服器找找看)，再去問根伺服器 |
| 解析程式 🡺 查詢本機快取 🡺查詢host file 🡺查詢快取 🡺查詢區域檔案  向”**根網路**”詢問www.flag.com.tw (告知.tw的dns的sv的ip位址)  輪詢：  🡺向管轄.tw的sv詢問 [www.flag.com.tw](http://www.flag.com.tw) 的ip位址  (告知.com.tw的dns的sv的ip位址)  🡺向管轄.com.tw的sv詢問 [www.flag.com.tw](http://www.flag.com.tw) 的ip位址  (告知 .flag.com.tw 的dns的sv的ip位址)  🡺向管轄flag.com.tw的sv詢問 [www.flag.com.tw](http://www.flag.com.tw) 的ip位址  (告知 www.flag.com.tw 的dns的sv的ip位址 **或說 不知道@@**) |

1. com, edu, gov, mil, org, .net 這種特殊領域以及

(2)以國家為分類的第二層的主機名稱了！這兩者稱為 Top Level Domains (TLDs)

封包格式：僅有查詢及回復兩種封包格式

查詢方式：遞迴查詢、反覆運算查詢

MX Record表示與郵件交換有關

當前，對於**每一級域名長度的限制是63個字元(bit)**，域名**總長度則不能超過253~255個字元(bit)。**

---------------------------------------------------------------------------------------------------

TFTP：小型文件傳輸協議

----------------------------------------------------------------------------------------------------

http封包回應資訊：

|  |  |
| --- | --- |
| 200 | 回應成功 |
| 400 | 表示有錯誤請求 |
| 404 | 此訊息代表客戶端在瀏覽網頁時，**伺服器無法正常提供訊息**，或是**伺服器無法回應且不知原因** |
| 500 | 伺服器內部錯誤 |
|  |  |

SNMP和MIB

|  |  |
| --- | --- |
| SNMP | 讓網路上不同設備具有共同的標準，並可支援網路管理 |
| MIB  Management Information Base  (網管資訊庫) | 架構在網路中監控與被監控的設備上，其目的是用來儲存各式各樣的SNMP物件 |

阻斷服務(Denial of service,Dos)與網路入侵

|  |  |
| --- | --- |
| Dos  阻斷服務  (Denial of Service) | 不需要取得系統使用權限  Ex:向攻擊對象發送大量且無意義的網路訊息。  (**TCP-SYN攻擊**、**UDP Flood Dos**、**ICMP Dos**…..等等) |
| DDos  分散式阻斷服務  (Distributed denial-of-service) | DDoS主要利用分散於不同地方的多部電腦主機，發送大量的偽造封包，進而達到癱瘓網路電腦主機伺服器的目的。 |
| 網路入侵 | 需要取得系統使用權限 |