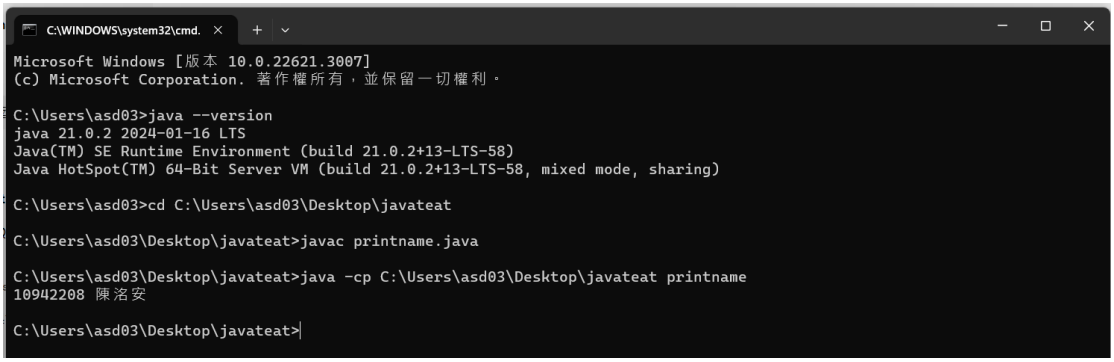
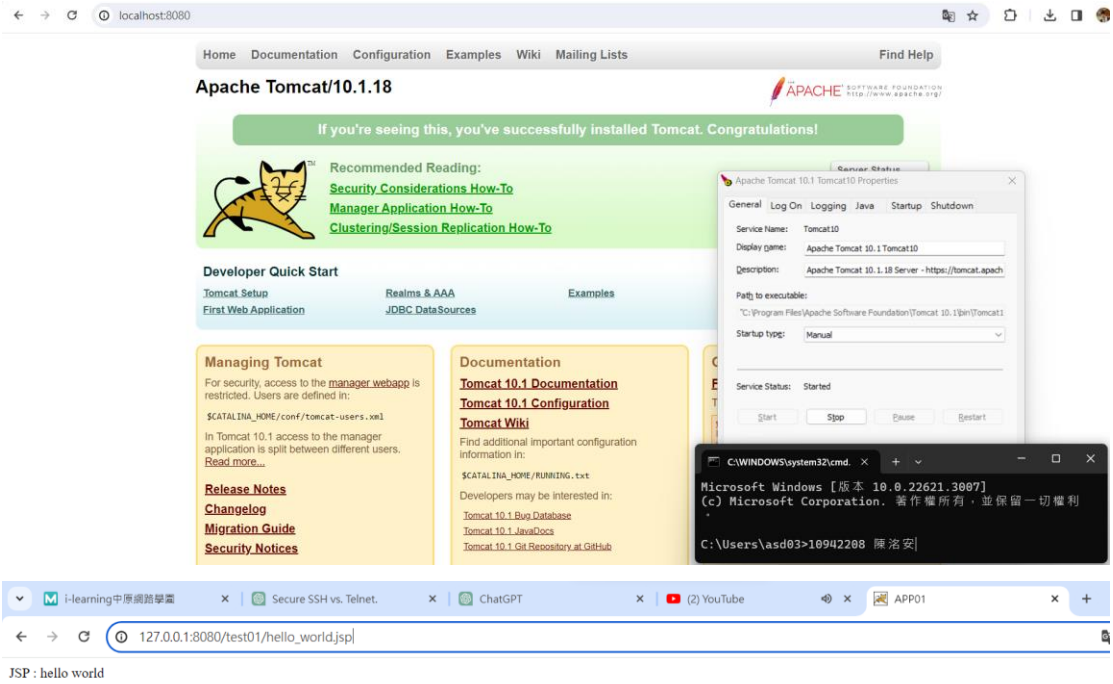
資工四乙 10942208 陳洛安

(一) JDK 安裝



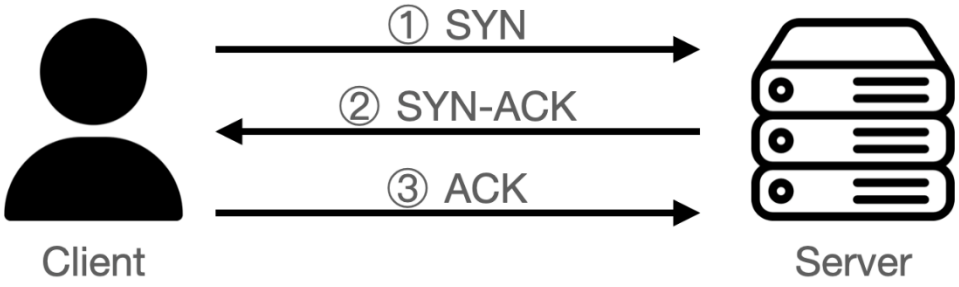
(二) TOMCAT 安裝

C:\Program Files\Apache Software Foundation\Tomcat 10.1



(三) TCP、UDP、FTP、HTTP、SMTP、SNMP、Telnet 介紹

TCP (Transmission Control Protocol)通訊控制協定



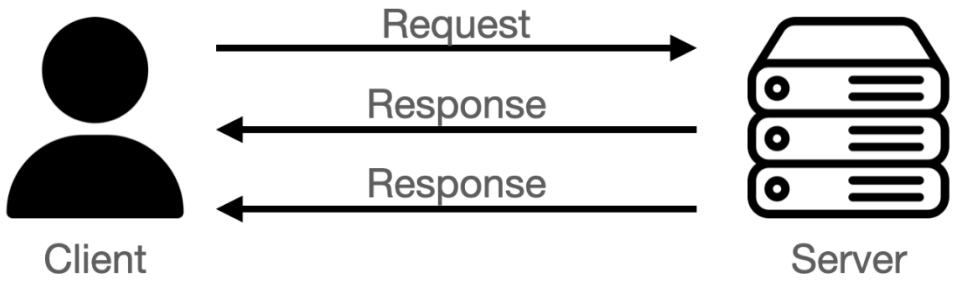
TCP 是一種面向連接的協定，為每個封包分配一個唯一的識別碼和一個序號，可以讓 TCP 擁有可靠的傳輸性，能夠確保：

- 完整性
- 重傳處理
- 順序性

三次交握 ACK

1. Client 向 Server 主動傳送一個要求連線封包
2. Server 接收並確認這個封包後，也會回傳一個相對應的封包給 Client 確認，並等待。
3. Client 收到 Server 的封包後，就確認了第一步驟發送的封包有被正確接收，如果 Client 也同意與 Server 建立連線，就會再回傳一個確認封包告知 Server。
4. Server 接收到也確認過後，就完成了三次交握，並建立連線。

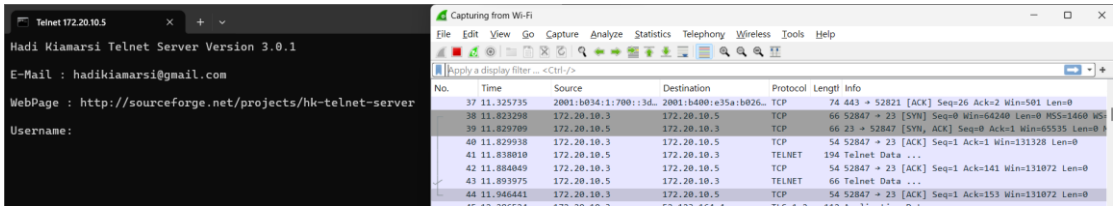
UDP(User Datagram Protocol) 用戶資料包協定



面向非連接的協定，它沒有保證傳送資料的可靠性，少了一些確認機制，不僅表頭資料會比較少，傳輸效率也比較好，適合應用的場景為：串流服務。

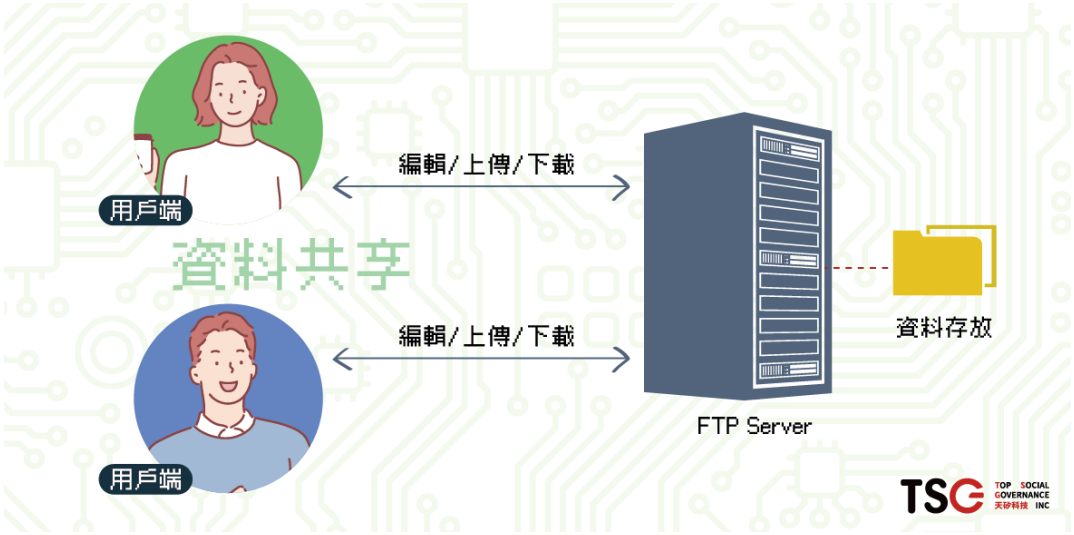
◎ 試試看 ：

對局域網下 172.20.10.5 建立 telnet 連線 ，會先進行 TCP 連線
用 wireshark 看到[SYN] [SYN,ACK] [ACK]



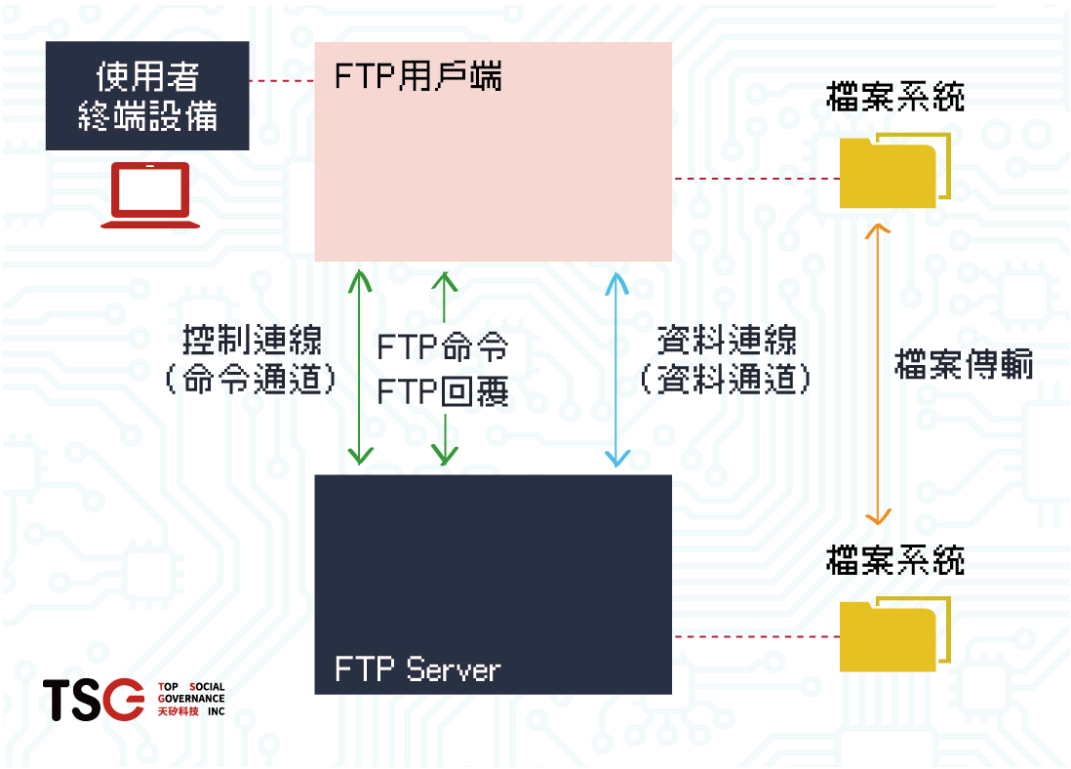
FTP (File Transfer Protocol) 檔案傳輸協定

用戶端與伺服器之間的檔案傳輸，也就是將共享檔案存放在 FTP 伺服器，讓用戶端可以透過網路在伺服器上編輯共享檔案，比如上傳、刪除、移動、修改或下載檔案，而用戶端則有可能是以應用程式或網頁形式呈現。



FTP 屬於主從式架構，也就是要運作一定要開啟 FTP Server 與 FTP 用戶端。

FTP 建立連線時，會需要兩個基本的通道，一個「資料通道」用於用戶端與伺服器之間傳輸資料，另一個「命令通道」則用於控制流量傳輸，啟動指令並攜帶資訊



兩種連接模式: 主動 、被動

HTTP 超文字傳輸通訊協定

◎ 作用 ：

HTTP 請求是網際網路通訊平台（Web 瀏覽器）索取其載入網站所需資訊的方式。

◎ 協定內容 ：

HTTP 請求包含以下內容：

- HTTP 版本類型
- 一個 URL
- 一個 HTTP 方法
- HTTP 請求標頭
- 選用的 HTTP 主體。

兩種最常見的 HTTP 方法 「GET」請求期望返傳回資訊（通常以網站的形式），而「POST」請求通常表示用戶端正在向 Web 伺服器提交資訊（例如表單資訊，如提交的使用者名稱和密碼）

HTTP 標頭包含存儲在索引鍵/值組中的文字訊息，並且它們包含在每個 HTTP 請求中。

★ 在 DoS 或 DDoS 攻擊的情況下，大量 HTTP 請求可被用於對目標裝置發起攻擊，並被視為應用程式層攻擊或第 7 層攻擊的一部分。

HTTP 回應是 Web 用戶端（通常是瀏覽器）從網際網路伺服器收到的用於回答 HTTP 請求的內容。這些回應會根據 HTTP 請求中要求的內容傳達有價值的資訊。

典型的 HTTP 回應包含以下內容：

- 一個 HTTP 狀態代碼
- HTTP 回應標頭
- 選用的 HTTP 主體

HTTP 狀態代碼是 3 位數代碼。狀態代碼分為以下 5 個區塊：
1xx 資訊內容
2xx 成功
3xx 重新導向
4xx 用戶端錯誤
5xx 伺服器錯誤
「xx」是指 00 到 99 之間的不同數字。
以數字「2」開頭的狀態代碼表示成功。
如果回應以「4」或「5」開頭，則表示出現錯誤，且不會顯示網頁。
以「4」開頭的狀態代碼表示用戶端錯誤（在 URL 中輸入錯字時，經常會遇到「404 NOT FOUND」狀態代碼）。以「5」開頭的狀態代碼意味著伺服器端出了問題。

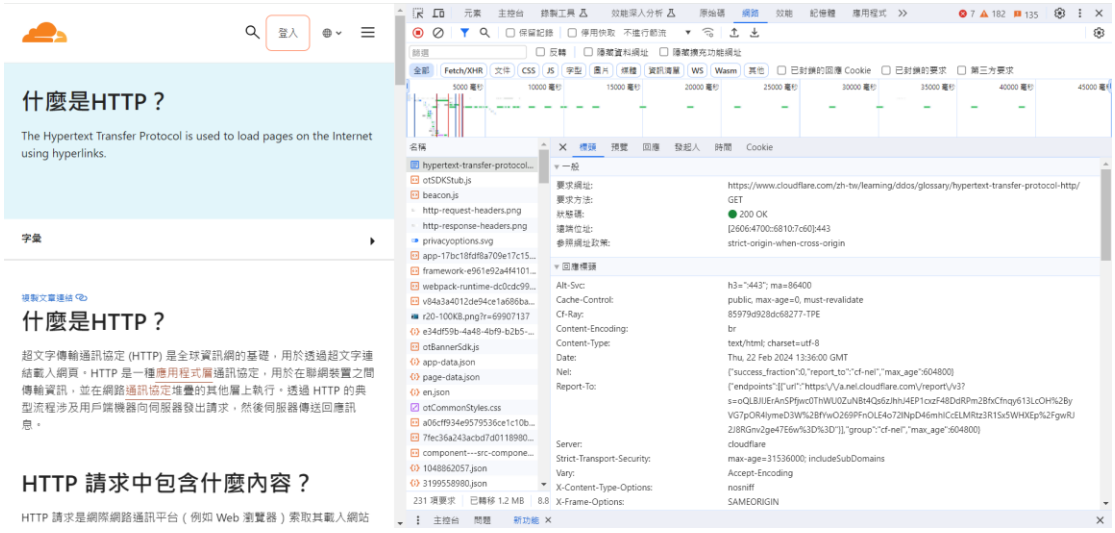
狀態代碼也可能以「1」或「3」開頭，分別表示資訊回應和重新導向。

HTTP 回應標頭與 HTTP 請求非常相似，HTTP 回應也帶有標頭，例如回應主體中傳送的資料的語言和格式。

▼ Response Headers

```
cache-control: private, max-age=0
content-encoding: br
content-type: text/html; charset=UTF-8
date: Thu, 21 Dec 2017 18:25:08 GMT
status: 200
strict-transport-security: max-age=86400
x-frame-options: SAMEORIGIN
```

◎ 動手試



SMTP (Simple Mail Transfer Protocol) 簡易郵件傳輸通訊協定

◎ 作用 ：

用來透過網際網路傳送和接收電子郵件程序的通訊協定。

郵件伺服器指的是收集、處理和傳遞電子郵件的系統。SMTP 伺服器特別是指使用簡易郵件傳送通訊協定 (SMTP) 傳送外送郵件之郵件伺服器的元件。郵件伺服器處理內送和外送的電子郵件，而 SMTP 伺服器只關注傳送和轉送外送電子郵件至其適當目的地的任務。

▲外送是從您的伺服器發出的郵件，內送是發送到您的伺服器的郵件

◎ 運作模式 ：

- **SMTP 連線開啟**：由於 SMTP 使用傳輸控制通訊協定 (TCP) 作為其傳輸通訊協定，因此第一步從用戶端與伺服器之間的 TCP 連線開始。開始電子郵件傳送程序。

- **電子郵件資料已傳輸**：用戶端向伺服器傳送一系列命令以及電子郵件的實際內容。

- **郵件傳輸代理 (MTA)**：伺服器執行稱為「郵件傳輸代理」(MTA) 的程式。MTA 檢查收件人電子郵件地址的網域，如果它與寄件人的網域不同，則會查詢 DNS 以查找收件人的 IP。

- **連線關閉**：當資料傳輸完成時，用戶端會提示伺服器，然後伺服器會關閉連線。此時，除非用戶端開啟新的 SMTP 連線，否則伺服器將不會從用戶端處接收額外的電子郵件資料。

第一個電子郵件伺服器通常並非實際的電子郵件最終目的地。伺服器收到來自用戶端的電子郵件後，會與另一台郵件伺服器重複此 SMTP 連線程序。第二台伺服器執行相同的程序，直到電子郵件最終到達收件人電子郵件提供者控制的郵件伺服器上的收件人收件匣。

如果要打開郵件仍需其他協定，接收方通常使用 POP3 或 IMAP 協定來檢索郵件

SNMP　(Simple Network Management Protocol) 簡易網路管理通訊協定

◎ 作用 ：

用於交換網路裝置之間的管理資訊。它是 TCP/IP 通訊協定組合的一部分。
SNMP 是用於管理和監視網路元素的廣泛接受的通訊協定之一。網路管理標準組成包括應用層通訊協定，以及資料庫結構描述架構。

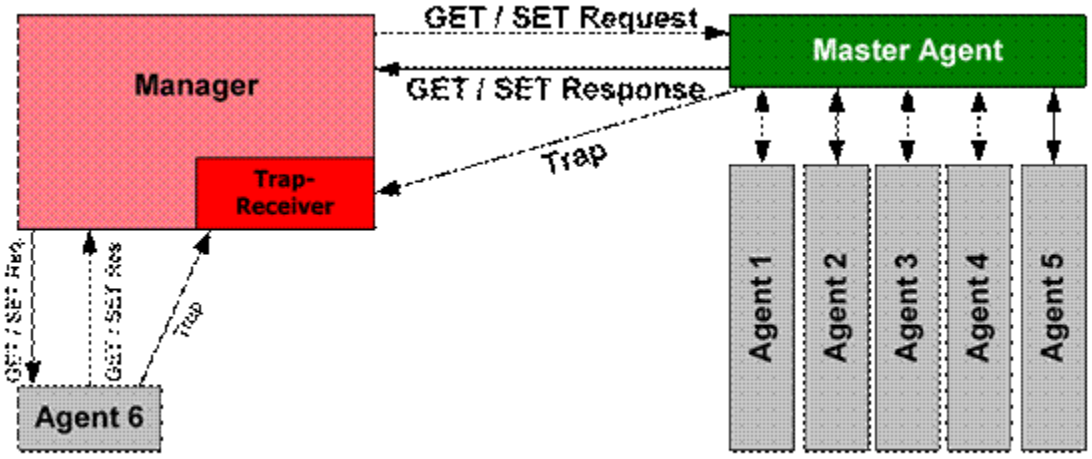
採用用戶端-伺服器模式。伺服器稱為管理程式，負責收集和處理網路裝置相關資訊。用戶端稱為代理程式，泛指網路上任何一類負責將資料傳送給管理程式的裝置。

SNMP 確實讓您能夠查看所有 IP 網路上的一舉一動(收集網路輸送量、使用量、效能問題以及安全漏洞)，伺服器、工作站、印表機、集線器、交換器以及路由器，全都一清二楚。
SNMP 還有另一項功能，那就是幾乎不影響裝置效能，傳輸要求也很低，因此不會影響網路流量。即使其他大多數網路應用程式失效，SNMP 仍然能夠繼續運轉。

◎ 運作模式 ：
作者： 江培文 / 臺灣大學計算機及資訊網路中心資訊網路組研究助理

SNMP 是運作於 OSI 模型之應用層，管理端經由 UDP 傳送 request 至代理者(port 161)，代理者透過來源埠傳送 response 至管理端。此外，當被監控設備發生異常事件時，例如 cold start 或 link down，代理者可經由 UDP 主動傳送 notification 至管理端(port 162)。
管理端一方面可經由 Get、GetNext 或 GetBulk 指令向代理者擷取被監控設備的相關資訊，另一方面亦可透過代理者經由 Trap 或 Inform 指令主動傳送資料。此外，管理端使用 Set 指令以達到系統管理之目的。

相較於 SNMP version 1，SNMP version 2 主要是增加 SNMP 在位元串(bit string)、網路位址(network address)及計數器(counter)之功能；而 SNMPv3 是基於 SNMPv2，進而增加訊息安全(message security)及存取控制(access control)等功能。



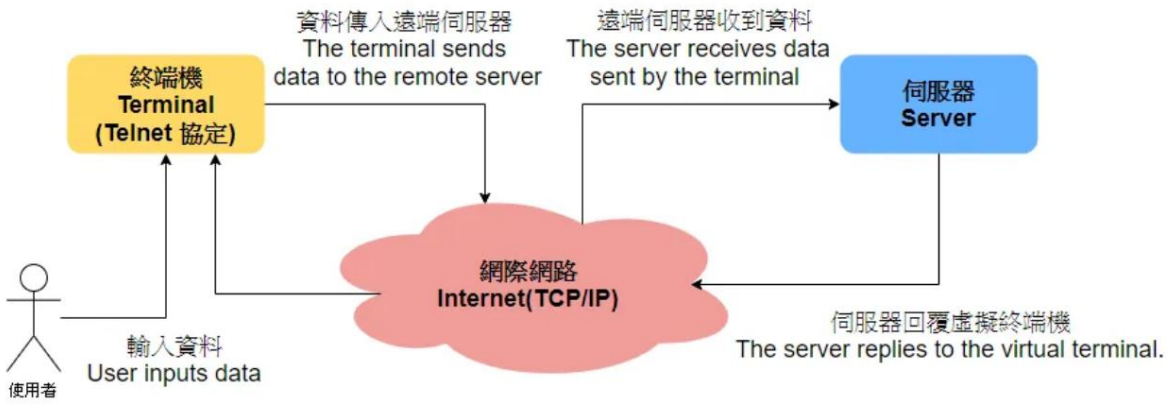
簡單網路管理協定不僅為網路設備管理時重要的通訊協定之一，亦可運用於無線網路用以偵測惡意無線基地台，網路管理人員依據偵測結果即時加以隔離處置，避免內部重要資訊洩漏或遭受外部蓄意攻擊，以維護資訊安全。

Telnet(Teletype Network) 遠端終端機協定

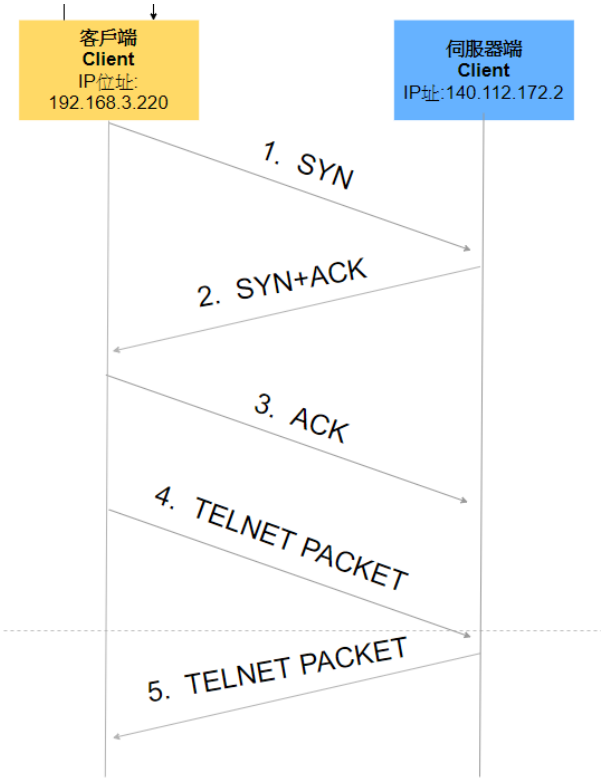
◎ 作用 ：

使用者透過 TCP 連線入遠端伺服器。使用於 web 或局域網中，以虛擬終端機的形式，提供雙向、以文字字串為主的命令列介面互動功能，使用者能使用 TELNET 協定從自己計算機連到伺服器，實現遠端連線概念。

◎ 運作模式 ：



圖一、TELNET運作過程

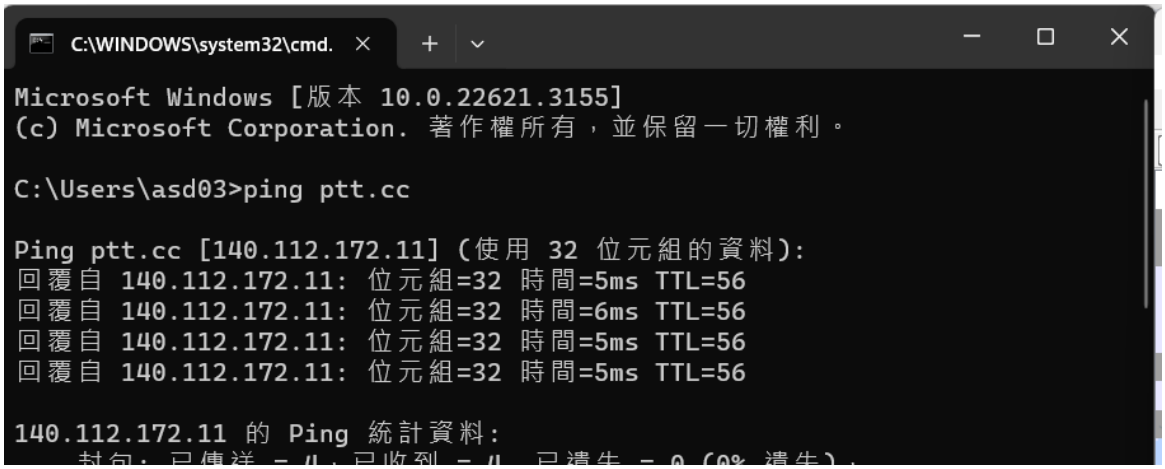


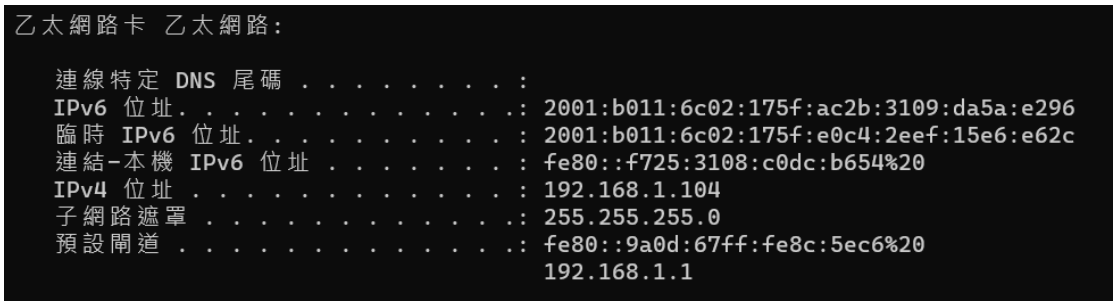
TELNET 是一個很簡易協定的遠端連線，早期網管人員會用此協定進行伺服器遠端登入，但使用 Wireshark 封包監聽軟體可得知，其實 TELNET 傳送的個人資訊、帳號、密碼容易遭到監聽、竊取，現在許多新版的作業系統會將此服務關閉，或是關閉連接埠 23。

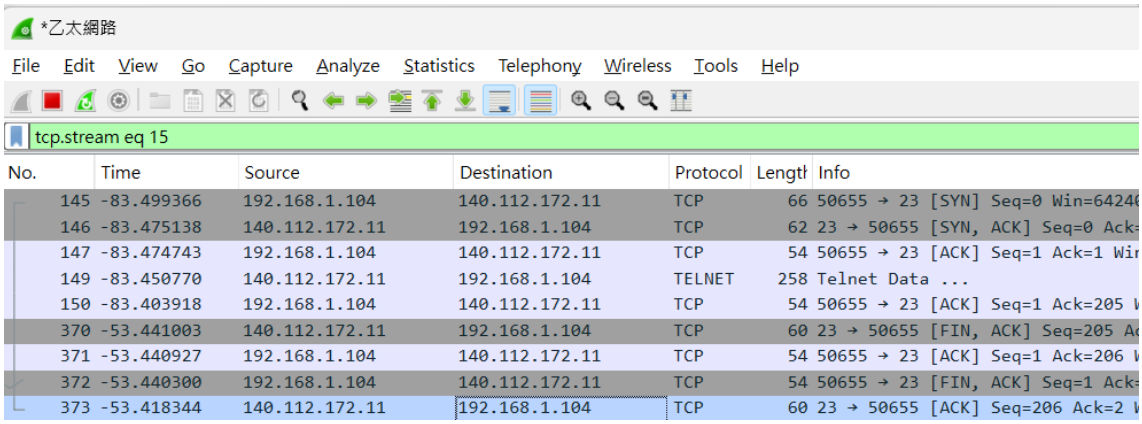
進而取代之是 Secure Shell（安全外殼協定，簡稱 SSH）協定

◎ 試試看 ：

※因為 ptt.cc 目前連線都需要 ssh ，只能看到 TCP 連線的部分

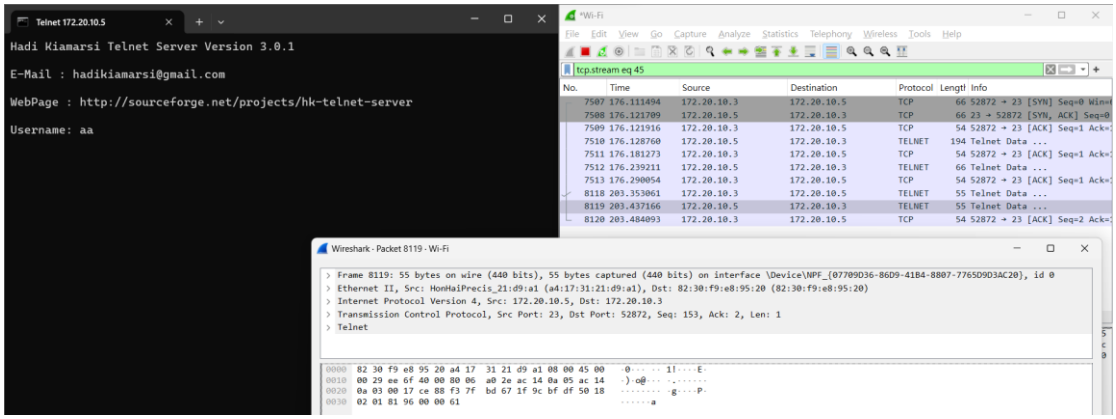


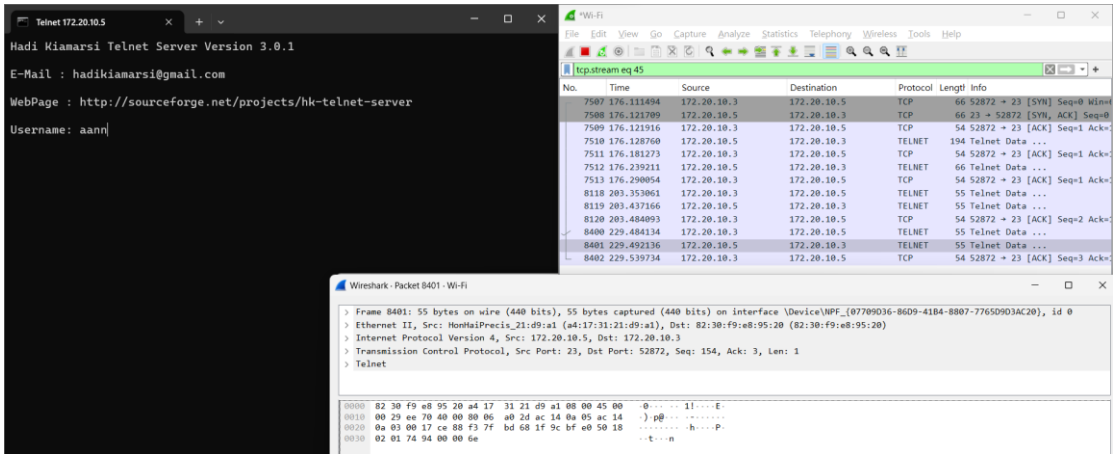


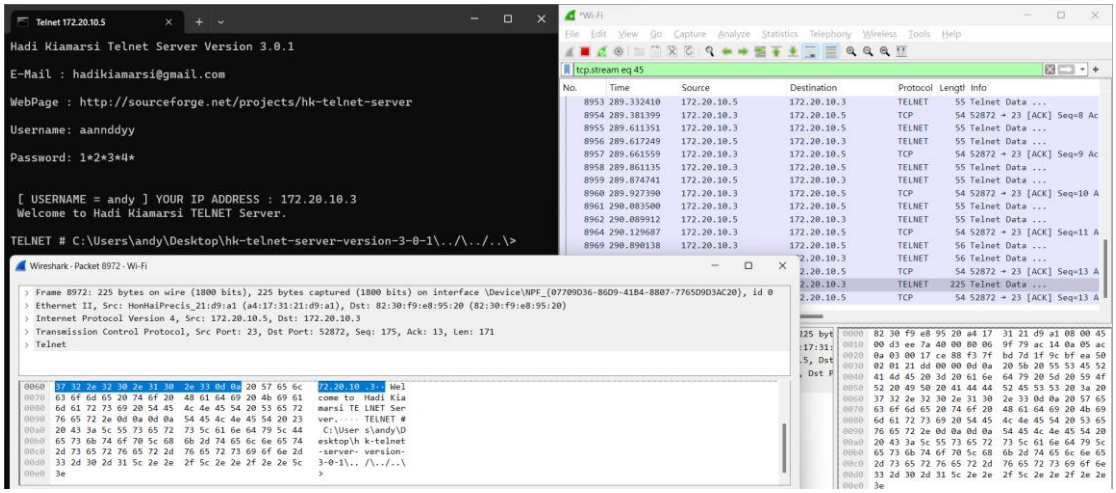


※對自己 172.20.10.3 局域網下另一台終端 172.20.10.5 發起 telnet 連線，並用 wireshark 捕獲封包，看到明碼傳輸的封包

172.20.10.5 作為 telnet server，傳輸使用者/密碼 andy/1234







※補充:

OSI 七層網路模型 將硬體跟軟體訂出七層標準，遵守共同標準才能互相溝通(EX : WINDOWS 要連 LINUX 的系統)

用 outlook 發送郵件

切割 ： 切成封包

Checknum： 檢查資料是否變質

Ack： 回應是否收到

IP 是哪台電腦 ， PORT 是要連那台電腦的甚麼東西

Port :

80 :HTTP 443 :HTTPS

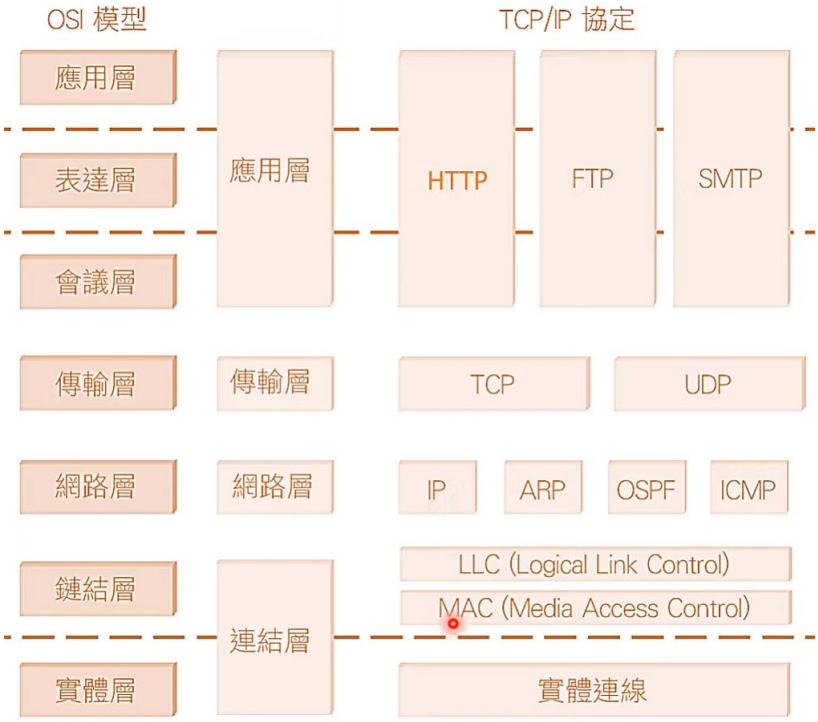
21 : FTP

25: SMTP。

- 連接埠 465 曾經專供具有 SSL 加密的 SMTP 使用。但是 SSL 已被 TSL 取代
- 連接埠 587 現在是電子郵件提交的預設連接埠。透過此連接埠進行的 SMTP 通訊使用 TLS 加密。
- 連接埠 2525 並未正式與 SMTP 相關，但部分電子郵件服務會在上述連接埠被封鎖時透過此連接埠提供 SMTP 傳遞。

OSI 模型 與 TCP / IP 模型對應

TCP/IP 模型



1. MAC (Media Access Control) 地址：是分配給網路設備的唯一識別碼。MAC 地址通常是一個由十六進制數字組成的六組（有時是六組以上）字元序列，通常用冒號（:）或連字符（-）分隔開來，例如：00:1A:2B:3C:4D:5E。

   每個網路設備，如網路介面卡（Network Interface Card, NIC）、無線網路卡（Wireless Network Card）、路由器等，都會有一個唯一的 MAC 地址。

   在全球範圍內每個 MAC 地址都是唯一且不重複的(除非廠商惡意製造)。

2. IP (Internet Protocol) 地址：IP 地址是指分配給設備的網絡層地址，IP 地址通常是一個 32 位元組（IPv4）或 128 位元組（IPv6）的數字序列，它們是全球唯一的且不重複的。

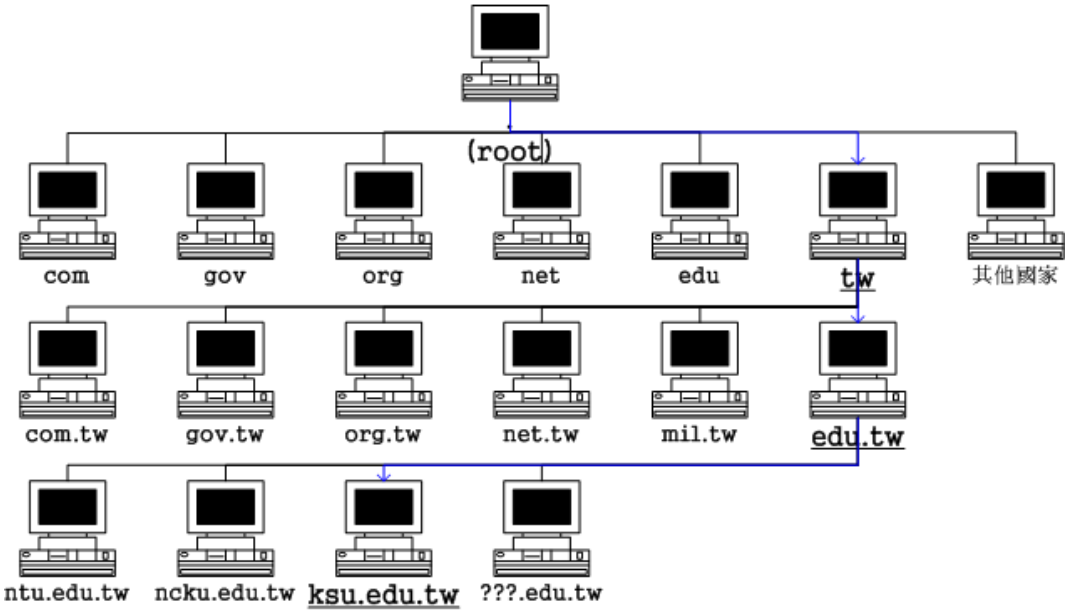
   ARP (Address Resolution Protocol) 是一種用於在網路中將 IP 地址轉換為對應的 MAC 地址的通訊協議。

   ※ARP 欺騙工作原理

   如果局域網內計算機 C 對計算機 A，發送假的 ARP 應答(IP 是計算機 B，MAC 為假造)，則計算機 A 變會更新本地的 ARP 緩存，由於局域網中是透過 MAC 地址傳輸，便導致計算機 B 無法連網，計算機 A 也 PING 不到計算機 B

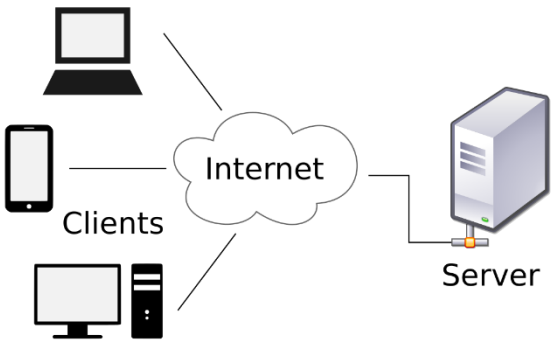
NAT 用於將私有網路中的 IP 地址轉換為公共網路中的 IP 地址，以實現多個設備共享單一公共 IP 地址的功能。
在運作中，路由器或防火牆通常會將內部私有網路中的設備（個人電腦、智慧型手機、平板電腦等）的內部 IP 地址轉換為路由器所屬的公共 IP 地址，當這些設備發送請求到互聯網時，看起來像是來自同一個公共 IP 地址。當互聯網上的服務器回應時，路由器再將這些回應對應到正確的內部 IP 地址，從而實現通訊。

DNS 階層架構



主從式架構

是一種網路架構，將客戶端（Client）與伺服器（Server）區分開來。任何一個客戶端軟體都可以向一個伺服器或應用程式伺服器發出請求。



參考資料來源 ：

阿彬電腦 網路紮根概念 2- 網路七層與 TCP/IP
https://www.youtube.com/watch?v=gxoIrBFfpDU&ab_channel=%E9%98%BF%E5%BD%AC%E9%9B%BB%E8%85%A6

Chatgpt https://chat.openai.com/share/d16bf8bc-2f7b-42ff-92a5-4791c3dac15f

https://www.tsg.com.tw/blog-detail4-164-0-ftp.htm
https://www.cloudflare.com/zh-tw/learning/ddos/glossary/hypertext-transfer-protocol-http/
https://www.pptrar.tw/2011/03/ftp-winxp-filezilla-server.html
https://www.cloudflare.com/zh-tw/learning/email-security/what-is-smtp/
https://gordonfang-85054.medium.com/telnet%E5%B0%81%E5%8C%85%E5%AF%A6%E6%88%B0-e9306216fba0
https://dic.vbird.tw/linux_server/unit09.php
https://www.cc.ntu.edu.tw/chinese/epaper/0047/20181220_4707.html
https://www.whatsupgold.com/tw/blog/what-is-snmp
https://hackmd.io/@Willie-The-Lord/BJ7ZP2hgY