

# 網路管理與數位素養

磐石高中 范村生

p041234@sphs.hc.edu.tw





- 磐石高中是一所天主教會學校。
- 為培養本校學生成為「優質磐石人」的願景與夢想。
- 達成「溫馨、適性、活潑、樂學、創新」的目標。



新竹市西大路683號

# 大綱

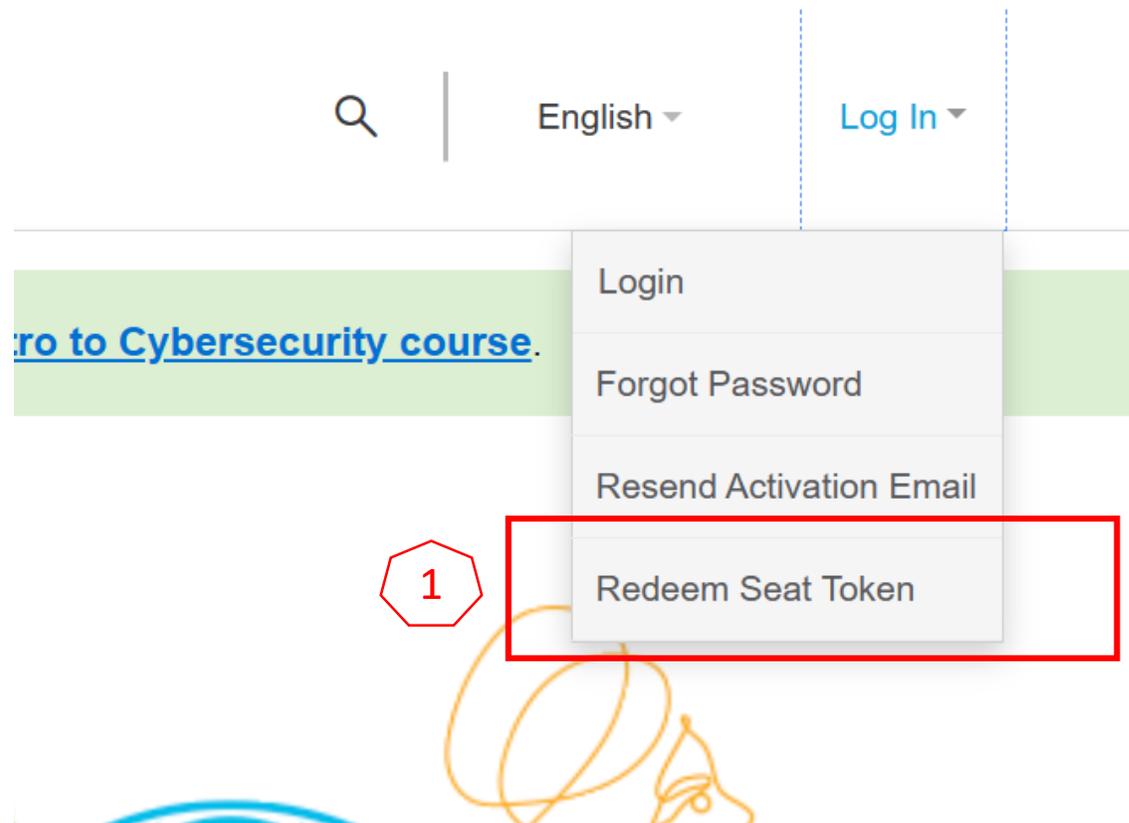
- 網路基礎
- 網路管理:Packet tracer實作
- 數位素養

# 加入網路課程

- <https://www.netacad.com/>
- 用Seat Token加入，請選一組



<https://reurl.cc/p5lrAe>



# 加入網路課程

## Redeem Seat Token

### Redeeming Your Seat Token

You can enroll in a course if you have a seat token for that course

I currently have a Networking Academy Login

I am new to Networking Academy

First Name \*

磐石高中

Last Name \*

范村生

Email Address \*

zzzz@gmail.com

(optional) Student ID or internal school ID

Seat Token \*

CCfsnf

Language

中文(繁體)

2.請收通知信

3.輸入新密碼

4.LOGIN登入即可

 Two NetAcad.com maintenance periods planned: 16 Dec 2023 and 5 Jan 2024

我正在學習

我已註冊的課程

★ 進行中

2023-1204-all  
網路基礎\_cisco  
台灣高中職推廣計畫

03 Dec 2023 - 31 Jul 2024  
CCNAV7: Introduction to Networks  
高中職推廣課程\_CISCO網路基礎課程2023...

Week  
1 of 34

Please finish by 31 Jul 2024

# TCP/IP:Internet通訊協定;一群通訊協定的總稱

協定名稱		用途
HTTP	超文件傳輸協定	瀏覽全球資訊網 (WWW)
FTP	檔案傳輸協定	檔案傳輸
SMTP	簡易郵件傳輸協定	傳送 ( 外寄 ) 郵件
POP3	電子郵件接收協定	接收 ( 內送 ) 並直接下載郵件
IMAP	網際網路訊息存取協定	存取遠端伺服器中的郵件
TELNET	遠端登錄協定	登錄遠端主機
DHCP	動態主機設定協定	動態主機設定及分配 IP 位址
DNS	網域名稱系統	轉換網域名稱和 IP 位址
TCP	傳輸控制協定	可靠的連線型傳送服務，確保資料能正確傳送
UDP	用戶資料元協定	非可靠的非連線型傳送，只負責傳送，速度比 TCP 快
IP	網際網路協定	選擇資料封包傳輸路徑
ARP	位址解析協定	使用 IP 位址查詢 MAC 位址
ICMP	網際網路控制訊息協定	檢測及確保連線的準確性

# TCP/IP:Internet通訊協定;一群通訊協定的總稱

TCP 和 UDP 的比較：

**TCP**

TCP提供**可靠**的資料流傳送服務，若接收端未收到訊息，傳輸端必須再重傳一次，因此屬於**連線型**。

vs.

**UDP**

UDP提供**非可靠**資料流傳送服務，只負責傳送，屬於**非連線型**。傳輸速度比TCP快，但**正確率較差**。

ARP 和 ICMP 的比較：

**ARP**

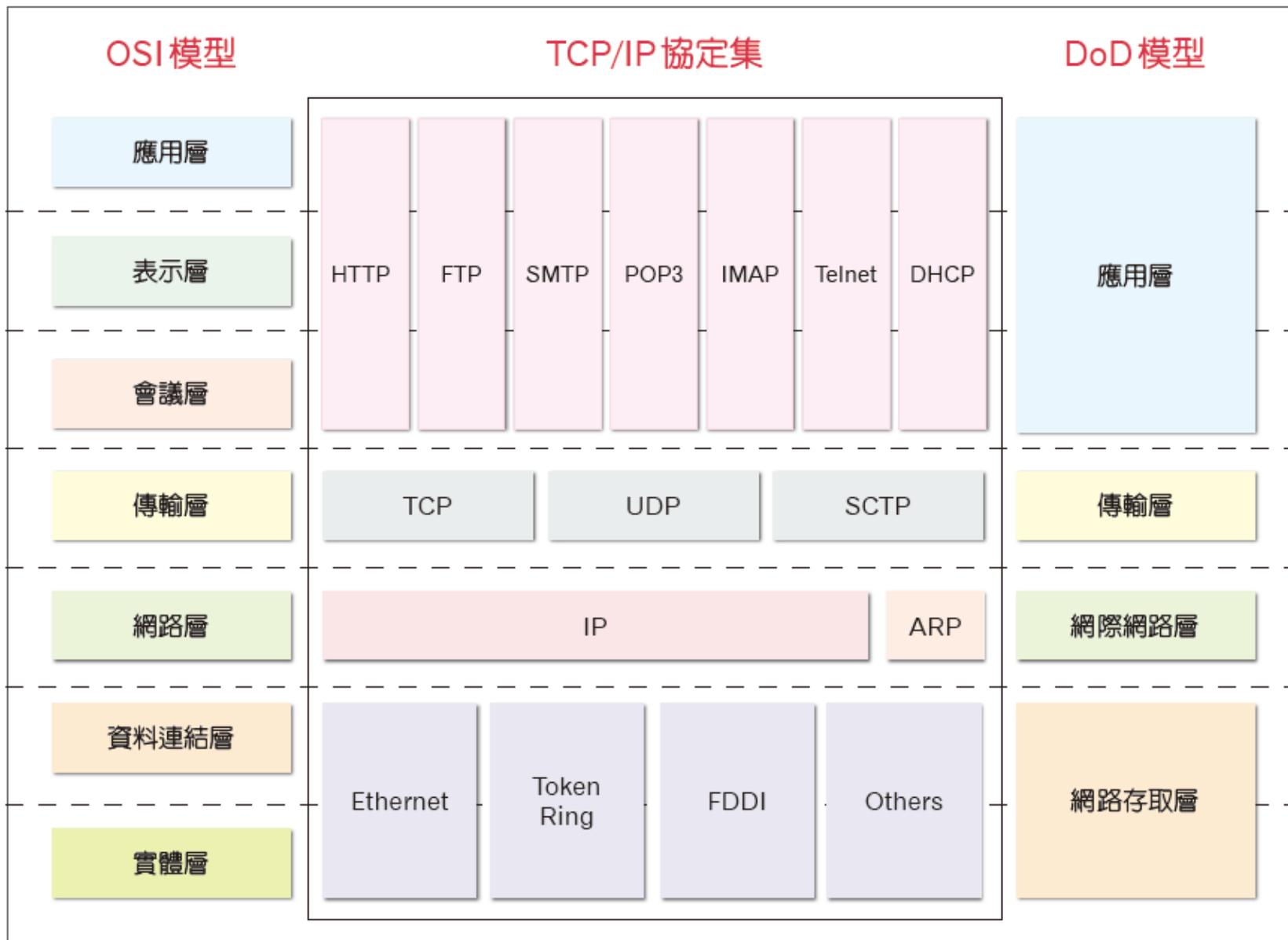
ARP可以使用**IP位址**來查詢其實體的**MAC位址**，使網際網路上的封包可繞送傳入區域網路送達目的地。

vs.

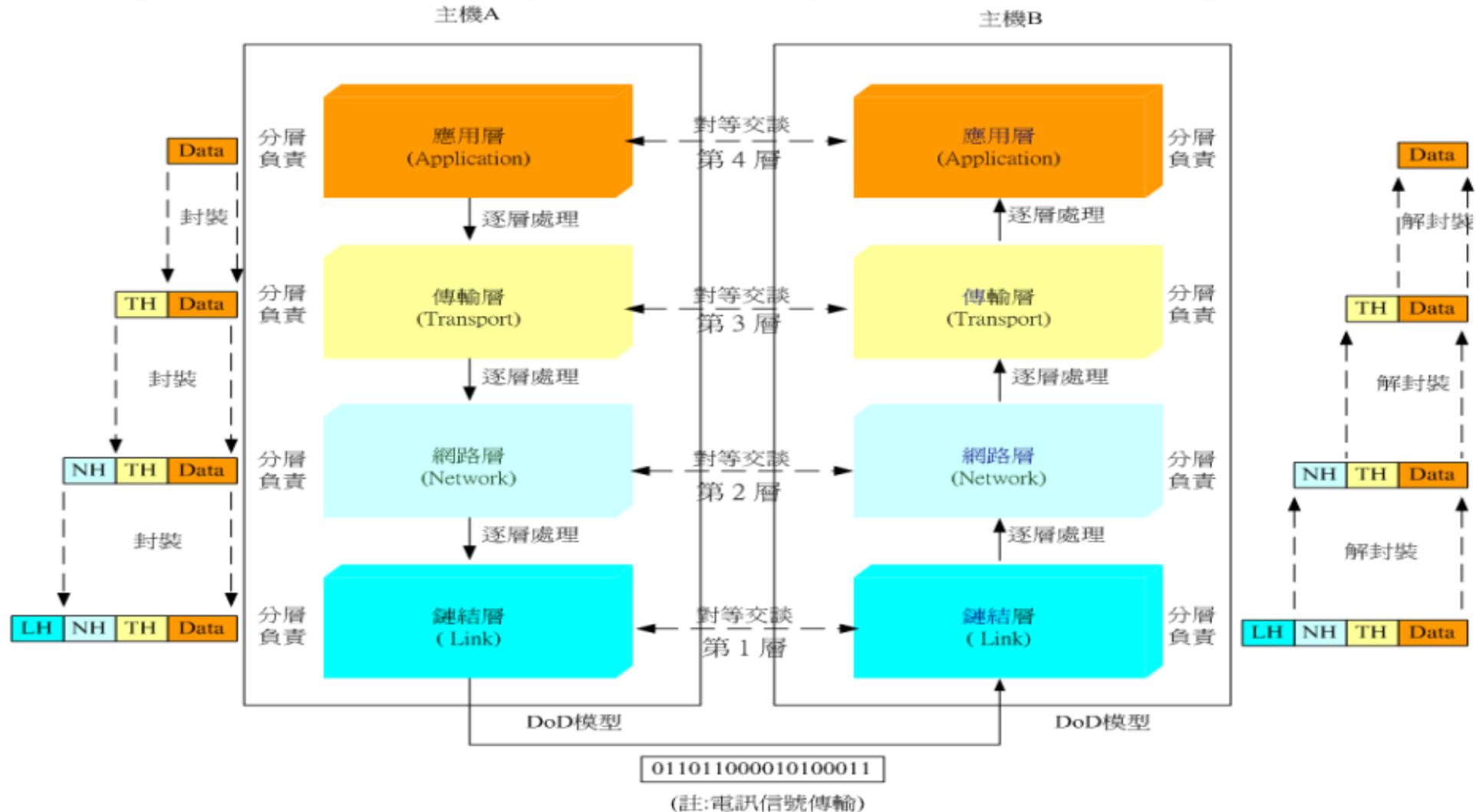
**ICMP**

ICMP的目的是檢測網路的**連線狀況**，確保連線的**準確性**。

# OSI與TCP/IP Model



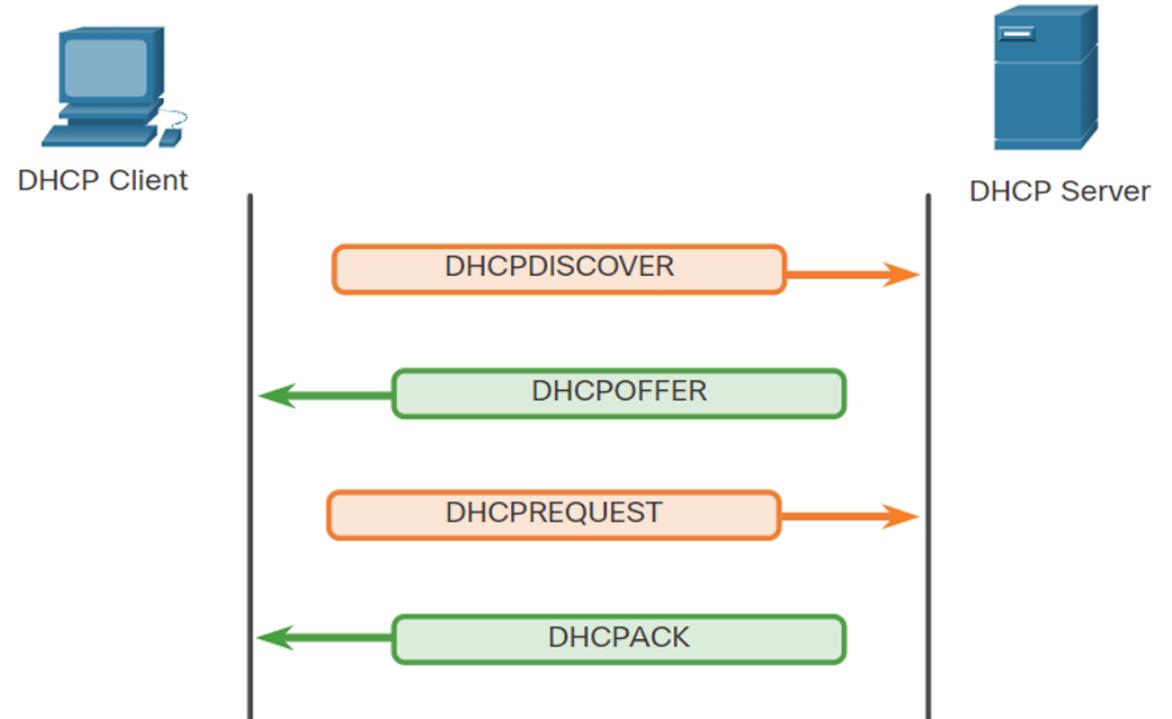
# 資料封裝/解封裝 (Encapsulation/Decapsulation)



# DHCP(Dynamic Host Configuration Protocol )

DHCP工作的基本動作包括以下幾個步驟：

- 1.發現（Discover）：裝置在連接到網路時，會向網路上的DHCP伺服器發送一個尋求IP位址和網路組態資訊的訊息。
- 2.提供（Offer）：DHCP伺服器接收到裝置的尋求訊息後，會回應一個IP位址和相關網路設定資訊的提供訊息。
- 3.請求（Request）：裝置收到一個或多個提供訊息後，會從中選擇一個提供的IP位址並向DHCP伺服器發送請求以確認選擇。
- 4.確認（Acknowledgment）：DHCP伺服器收到請求後，會確認提供該IP位址和網路設定資訊給該裝置，並且發送一個確認訊息。在確認後，DHCP伺服器將分配的IP位址和設定資訊授予裝置，通常會指定一個租用時間。裝置在這段時間內可以使用這個IP位址，過期後若需繼續使用則需要更新租用。

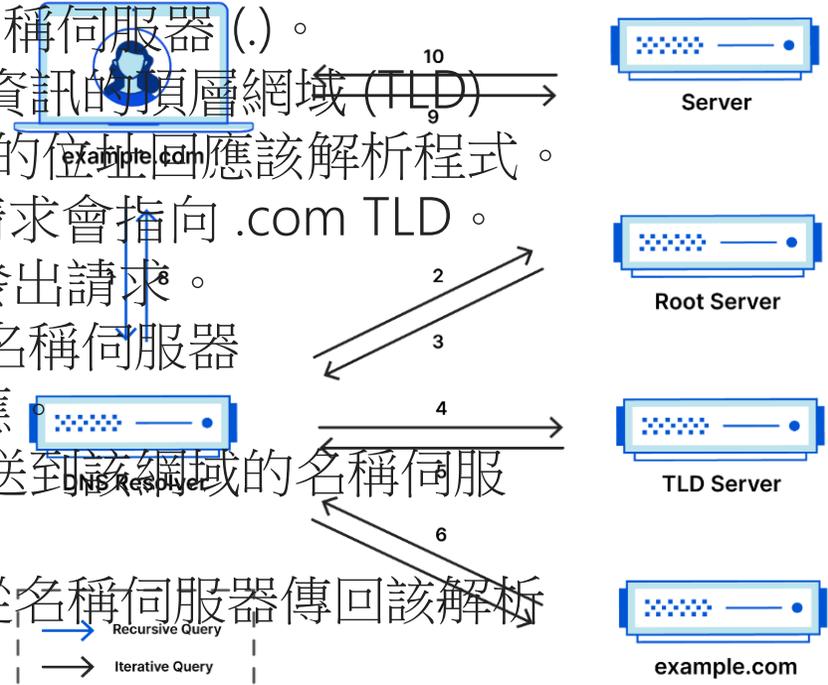


# DNS ( Domain Name System )

## DNS 尋找的步驟：

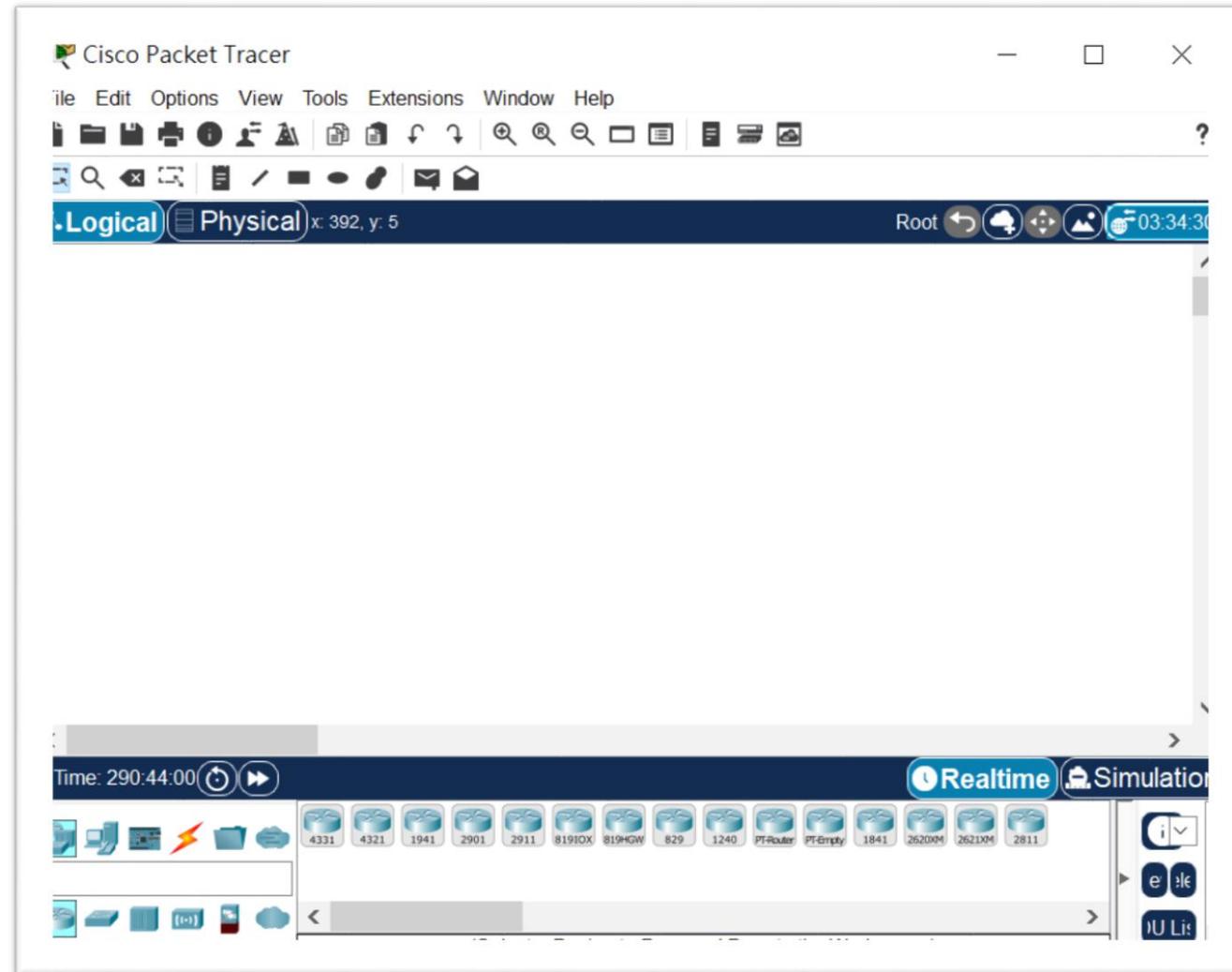
1. 使用者在網頁瀏覽器中鍵入「example.com」，查詢傳輸到網際網路中，然後 DNS 遞迴解析程式接收該查詢。
2. 接著該解析程式查詢 DNS 根名稱伺服器 (.)。
3. 然後根伺服器使用儲存其網域資訊的頂層網域 (TLD) DNS 伺服器 (例如 .com 或 .net) 的位址回應該解析程式。搜尋 example.com 時，我們的請求會指向 .com TLD。
4. 然後該解析程式向 .com TLD 發出請求。
5. TLD 伺服器隨後使用該網域的名稱伺服器 example.com 的 IP 位址進行回應。
6. 最後，遞迴解析程式將查詢傳送到該網域的名稱伺服器。
7. 接著 example.com 的 IP 位址從名稱伺服器傳回該解析程式。
8. 然後 DNS 解析程式使用最初請求的網域的 IP 位址回應網頁瀏覽器。

### Complete DNS Lookup and Webpage Query

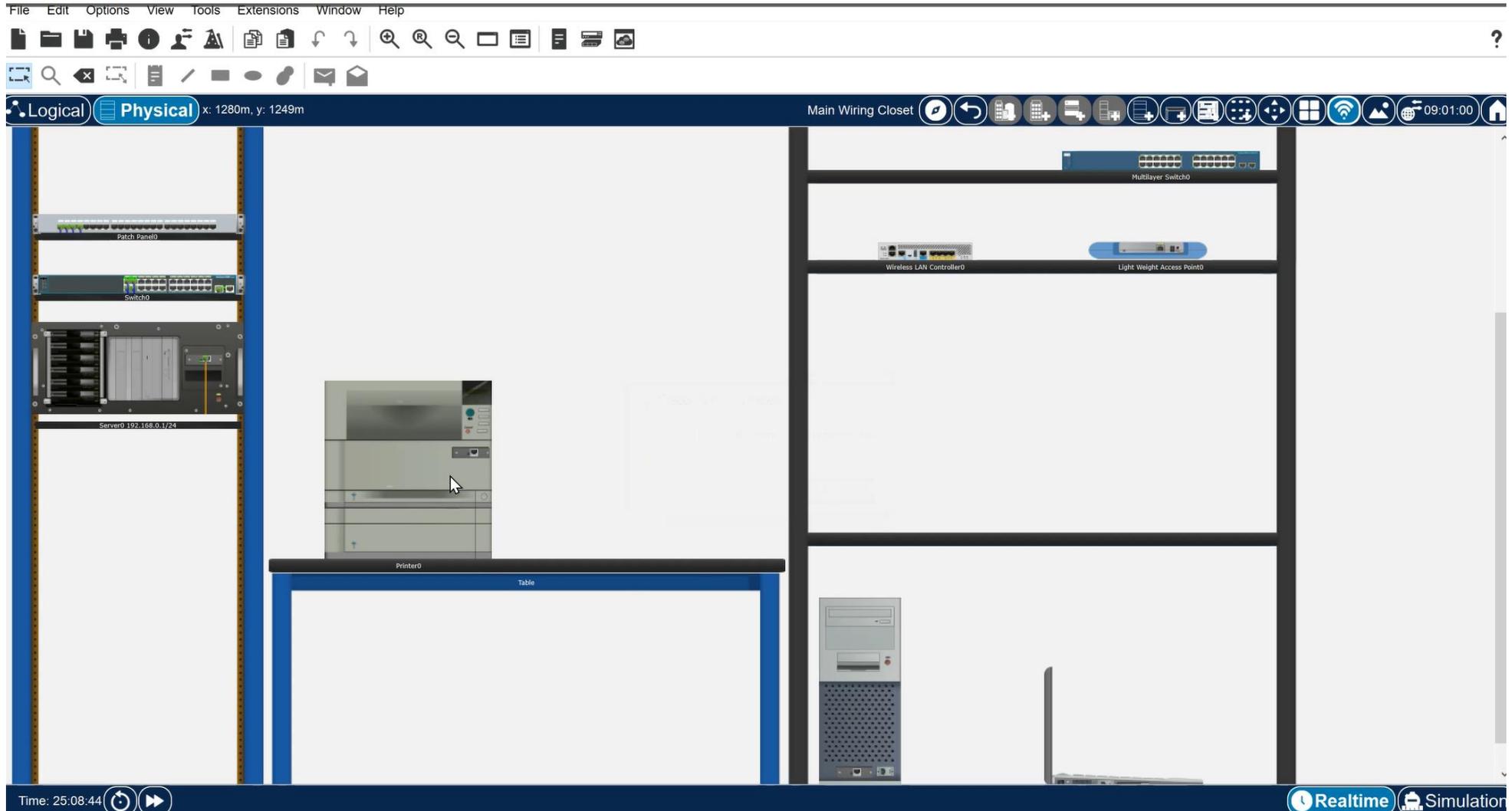


# Packet tracer實作

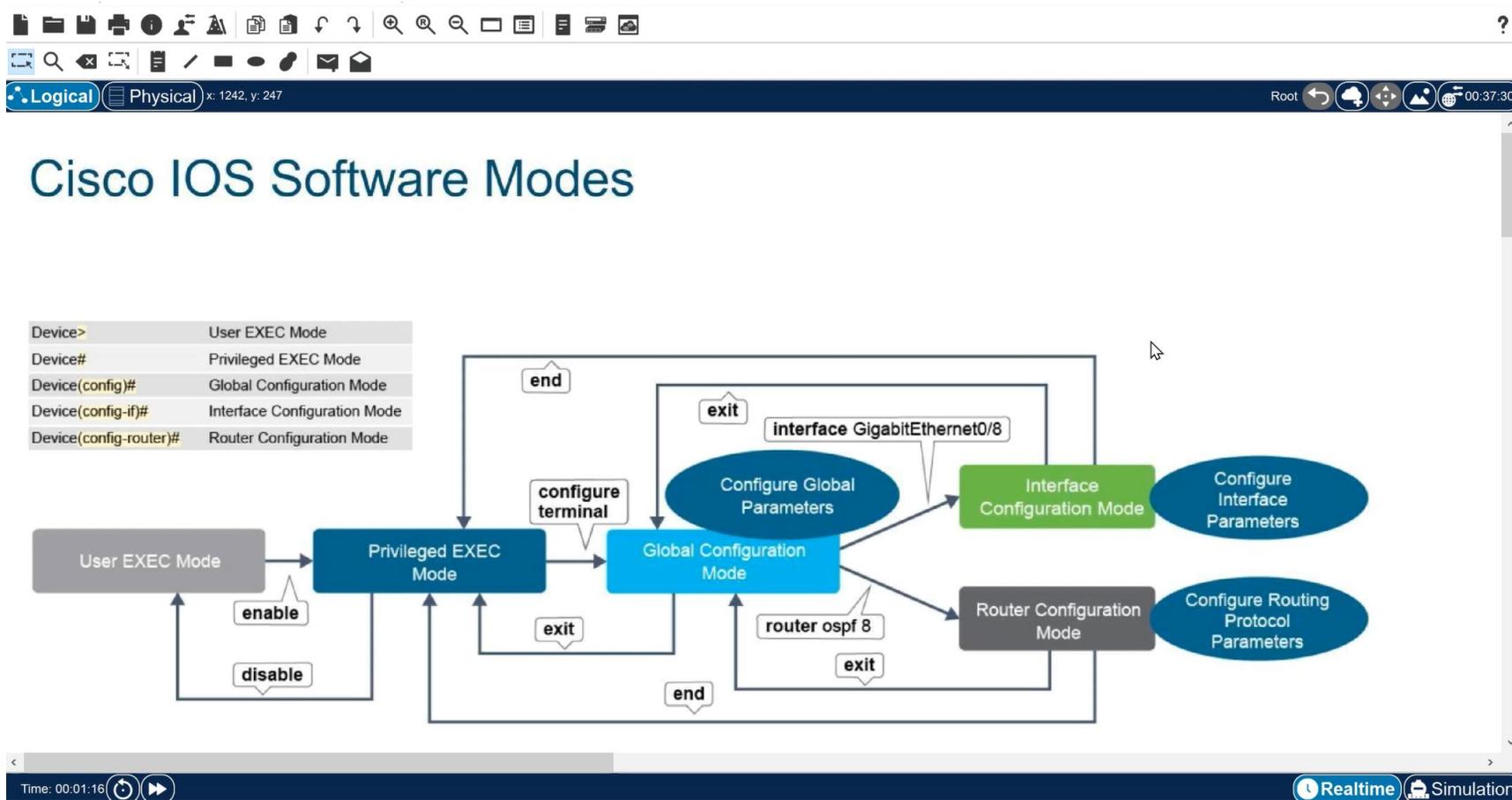
- Packet Tracer是一款由思科（Cisco）開發的網路模擬工具，用於設計、配置、測試和模擬網路。
- 它被廣泛用於教育和培訓環境中，特別是在教授網路和通信相關課程時。
- Packet Tracer提供了一個模擬環境，使使用者能夠模擬整個網路架構，包括路由器、交換機、終端設備等，並且進行實測。



# Packet tracer介紹



# Cisco IOS操作介紹



# 交換器的運作-MAC Address Table

The screenshot shows a network simulation environment. On the left, a diagram illustrates a Layer 2 Switch (Switch0) connected to five PCs: PC1, PC2, PC3, PC4, and PC6. A blue box highlights the configuration steps for the switch:

```
Step 2 [SWITCH  
> enable  
# show mac address-table  
# clear mac address-table  
# show mac address-table
```

Another blue box shows steps for PC1:

```
Step 1. [PC1]  
ping 192.168.1.255  
  
Step 3 [PC1] 搭配Simulation來觀察  
ping 192.168.1.102  
  
Step 4 [PC1] 搭配Simulation來觀察  
ping 192.168.1.103
```

On the right, a terminal window for PC6 shows the following output:

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed to up  
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up  
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed to up  
  
Switch>  
Switch>  
Switch>  
Switch>ena  
Switch>enable  
Switch#  
Switch#  
Switch#sho  
Switch#show mac add  
Switch#show mac address-table  
Mac Address Table  
-----  
Vlan    Mac Address      Type    Ports  
-----  
-----  
Switch#show mac address-table  
Mac Address Table  
-----  
Vlan    Mac Address      Type    Ports  
-----  
-----  
1       000a.41ad.1111   DYNAMIC Fa0/1  
1       000b.be82.3333   DYNAMIC Fa0/3  
1       0030.f261.4444   DYNAMIC Fa0/4  
1       0060.5c51.2222   DYNAMIC Fa0/2  
Switch#
```

# ARP(Address Resolution Protocol)介紹

The screenshot displays a network simulation environment. The main workspace shows a central switch labeled "Switch0" (2950-24TT) connected to five PCs (PC1-PC6). PC1 is highlighted with a green box and a cursor, with a text box indicating "[PC1] 顯示ARP快取 arp -a". The switch is labeled "VLAN 1 192.168.1.11/24" and has a text box "[Switch] 顯示ARP快取 show arp". Below the network diagram, a command window shows the command "ping 192.168.1.102".

The Simulation Panel on the right shows an Event List table:

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC1	ICMP
	0.000	--	PC1	ARP
	0.001	PC1	Switch0	ARP
	0.002	Switch0	PC2	ARP
	0.002	Switch0	PC3	ARP
	0.002	Switch0	PC4	ARP
	0.003	PC2	Switch0	ARP
Visible	0.004	Switch0	PC1	ARP
Visible	0.004	--	PC1	ICMP

At the bottom of the simulation panel, there are buttons for "Reset Simulation", "Constant Delay", and "Captured to: 0.004 s". Below these are "Play Controls" buttons (stop, play, next) and "Event List Filters - Visible Events" (ARP, ICMP) with "Edit Filters" and "Show All/None" options.

The bottom status bar shows "Time: 00:07:08.745" and "PLAY CONTROLS" buttons.

# 故障排錯案例



Logical Physical x: 860, y: 174

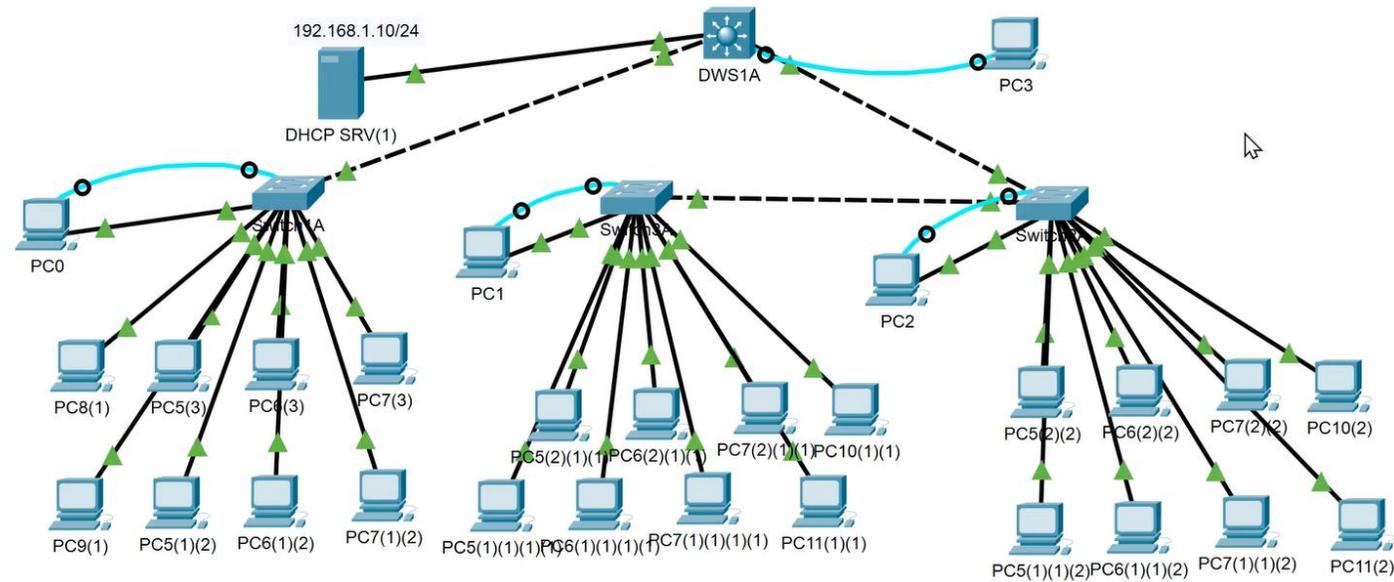
Root 06:52:00

任務1：單位防毒軟體偵測到1台電腦中加密病毒程式，IP=192.168.1.124，請於最短時間找到這台電腦並將它隔離（關閉）

所有的交換機都有啟動telnet服務，所有的密碼都是設定cisco  
請先在DSW1交換機上執行ping 192.168.1.255直連本地廣播

指令提示：  
show arp  
show mac address  
show cdp neighbors  
show cdp neighbors detail  
telnet xx.xx.xx.xx  
shutdown

任務1：單位防毒軟體偵測到1台電腦中加密病毒程式，IP=192.168.1.124，請於最短時間找到這台電腦並將它隔離



Time Elapsed: 00:16:00 Completion: 100%

Dock   1/1

Time: 00:13:12

# 個人資料防護基本概念

## 個人資料安全的保護

- 為了規範個人資料的合理使用，避免個人隱私權遭受侵害，政府特別制定了個人資料保護法（簡稱**個資法**），來保護個人隱私權。

## 常見的個人資料安全問題(網路攻擊)

- **惡意軟體入侵的問題**：當我們透過平板、智慧型手機等裝置來瀏覽網頁、下載檔案時，都可能使裝置遭到「惡意軟體」的入侵，導致個人資料的毀損或遭盜用。
- **駭客入侵的問題**：駭客透過各種手法，來竊取個人資料，或是影響個人資料安全。

# 數位素養評量

- <https://forms.gle/EiK4JVWwy9bCjBMz8>



# 網路攻擊

攻擊手法	攻擊行為	防範方式
蠕蟲 (Worm)	藉由不斷複製自己，透過網路散布或產生大量的封包，造成網路癱瘓無法正常使用。	不瀏覽不安全網站或下載來路不明軟體。  不隨意打開電子郵件附件，收到信件後如果無法辨別真偽，不要點信件上的連結。  提高瀏覽器安全等級設定。  定期下載修補套件(patch)修補安全性漏洞。
特洛伊木馬 (TrojanHorse)	用來竊取機密（如密碼）的程式（俗稱後門程式），加入一個正常的程式（俗稱木馬程式或後門宿主）。	
勒索軟體(Ransomware)	①俗稱勒索病毒，感染途徑與「木馬程式」一樣。 ②達到類似「阻絕服務」的目標，例如：加密電腦上的檔案或鎖住電腦系統，使 ③受害者必須付清贖金後才能解密或解鎖。	
跨站腳本攻擊 (XSS,Cross-Site Scripting)	跨站腳本攻擊又稱為跨網站指令碼攻擊，攻擊者入侵網站，在正常網頁上植入惡意連結，瀏覽該網頁會被植入木馬程式（即網頁掛馬）。	
鍵盤側錄(Keylogger)	側錄鍵盤按過的按鍵，取得輸入的個資，如：帳號及密碼、信用卡號碼。	
殭屍網路(BotNet)	駭客從遠端操控被入侵的電腦，用來進行攻擊。	

# 網路攻擊

攻擊手法	攻擊行為	防範方式
社交工程(Social Engineering)	利用各種社交手段（如套關係、冒充權威人士）降低他人戒心，趁機騙取資料。	確認網址的正確性，注意辨識網址是否正確（例如：0與o、1與l），或自行輸入網址。
網路釣魚(Phishing)	仿製網站登錄頁面，再利用郵件或通訊軟體發送連結，誘使使用者登入，騙取帳號、密碼。	隨時提高警覺，不要未經確認即提供資料。
殭屍帳號(Zombies)	①在社群網站上建立大量「虛擬」帳號。 ②例如：臉書的殭屍粉絲。因此需確認社群粉絲與按讚數量，不盲從。	提高警覺，檢查帳號是不是屬於朋友少、發文少的空殼帳號。
郵件炸彈(E-mail Bomb)	寄出大量垃圾信件，灌爆信箱使其無法正常運作。	若發信來源固定，可以用郵件規則封鎖。
猜密碼 (Password Guessing) 字典攻擊法 (Dictionary Attack)	藉由不斷猜測帳號與密碼入侵他人帳戶。	不要在網路上公佈個資，使用的密碼包含英文大小寫及特殊符號。

# 網路攻擊

攻擊手法	攻擊行為	防範方式
DoS阻絕服務 (Denial of Service)	①瞬間產生大量封包攻擊伺服器，導致無法提供服務。 ②若這些攻擊來自不同的IP，則稱為「分散式阻絕服務」(DDoS, Distributed Denial of Service)。	安裝偵測攻擊常駐程式工具。
資料隱碼 (SQL Injection)	利用資料庫的安全漏洞，將攻擊指令藏於網站查詢命令SQL中竊取或變更資料。	管制存取資料庫的權限。 定期下載修補套件(patch)修補安全性漏洞。

# 網路攻擊防範措施

## 駭客入侵的防範措施

- 安裝修補程式
- 刪除cookie檔案
- 謹慎使用公用電腦
- 避免落入網路釣魚陷阱
- 不開啟來路不明的連結

## 設定密碼的原則：

- 密碼至少8個字元以上
- 宜混合使用英文大小寫、數字、符號，避免使用**懶人密碼**
- 避免使用個人相關的資料
- 不定期更換密碼

## 防範惡意軟體入侵的方法

- 安裝防毒軟體
- 開啟軟體自動更新功能
- 不使用來路不明的軟體
- 不任意開啟來源不明的檔案
- 避免瀏覽高危險群的網站
- 定期備份資料

# 常見的手機個人資料安全問題與解決方法

Q1：我手機弄丟又沒設密碼，會發生什麼問題？

A1：你可能會面臨身分遭盜用、機密資料被公開的危險

Q2：我好像不小心安裝奇怪的App，會有什麼問題？

A2：若是惡意的App，則會竊取個資，或手機中毒

Q3：有未加密的Wi-Fi可以無線上網耶！連上去不會有危險吧？

A3：公開、未加密的Wi-Fi如果遭駭客監控，你透過網路傳輸的資料可能會被竊取

# 常見的手機個人資料安全問題與解決方法

## 解決方法

### ○設定手機鎖



○**不安裝來路不明的App**：  
避免在Play商店、App Store以外的網站下載安裝App，因為這些App沒有通過任何官方安全機制驗證，可能是惡意軟體。

# 常見的手機個人資料安全問題與解決方法

## ○ 避免下載權限不合理的App

一般手電筒App要求的權限



若手電筒App要求查看使用者身分、相片檔案等資料，就可能「不懷好意」

## ○ 安裝手機防毒軟體

## ○ 不連上未知的Wi-Fi



駭客建立的假全家超商Wi-Fi

真正的全家超商Wi-Fi

# 網路犯罪:網路駭客

犯罪行為	說明	刑責
入侵電腦	無故破解他人帳號密碼或利用系統漏洞入侵他人的電腦並竊取資料。	3年以下有期徒刑
干擾電腦	無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備。	10萬元以下罰金
破壞電磁記錄	無故取得、刪除或變更他人電腦資料。	5年以下有期徒刑 20萬元以下罰金
濫發商業電子郵件	無故大量發送垃圾郵給他人。	收信人每人每封可求償500~2000元
製作惡意軟體	製作、撰寫惡意電腦犯罪程式供自己或他人使用。	5年以下有期徒刑 20萬元以下罰金

# 生成AI介紹

- 生成式文本

- ChatGPT <https://chat.openai.com/>
- Microsoft Bing <https://www.bing.com/>
- Google Bard <https://bard.google.com/>
- Chateverywhere <https://chateverywhere.app/zh>
- Claude <https://claude.ai/login>

參考：ChatGPT指令大全 <https://www.explainthis.io/zh-hant/chatgpt>

- 各式圖像語法應用

- 語法轉圖像-Mermaid

<https://mermaid.js.org/intro/getting-started.html>

# 生成AI介紹

- 生成式影像
  - [Leonardo.Ai](#)
  - [Microsoft Image Creator](#)
  - Stable Diffusion Online <https://stablediffusionweb.com/>
  - Adobe Firefly [https://www.adobe.com/hk\\_zh/sensei/generative-ai/firefly.html](https://www.adobe.com/hk_zh/sensei/generative-ai/firefly.html)
  - 生成向量圖 <https://www.recraft.ai/>
  - 商品圖合成 <https://app.mokker.ai/login?redirectedFrom=%2F>

# 生成AI介紹

- AI圖庫
  - AI生成圖片的圖庫 <https://www.stockai.com/>
  - AI生成背景 <https://www.photoroom.com/backgrounds>
  - 360場景圖 [https://skybox.blockadelabs.com/?fbclid=IwAR0cTjba-j\\_DKt6lftoTbJx3fsbyeusolp4UalQX\\_x8bkb\\_1wqyLoIA7br8](https://skybox.blockadelabs.com/?fbclid=IwAR0cTjba-j_DKt6lftoTbJx3fsbyeusolp4UalQX_x8bkb_1wqyLoIA7br8)
  - [Vectorizer.AI](#) 把 Midjourney 生成 ICON、著色畫變無限放大向量圖 <https://www.playcesor.com/2023/04/vectorizerai-midjourney-icon.html>
  - AI生成3D <https://www.kaedim3d.com/>
- AI應用工具
  - LINE Moonshot 機器人繪圖教學，7招用中文版AI快速產生美圖 <https://mrmad.com.tw/line-moonshot>
  - DocuAsk(上傳文件以任何語言根據文件內與AI進行問答,摘要) <https://www.docu-ask.com/>
- 生成式簡報
  - Gamma <https://gamma.app/?lng=eng>
  - Slidesai(google slides) <https://www.slidesai.io>

# 感謝聆聽!

參考資料:

1. 思科網路學院

<https://www.netacad.com/zh-hant>

2. 全華圖書數位科技概論總複習第七章

3. 旗立資訊數位科技概論第十章

4. 燕秋老師教學頻道

5. 健行科大張木盛老師

藉單著的偉  
微事大的事  
小而能成  
簡而成就  
that by small  
and simple  
things are  
great things  
brought to  
pass