

113 年特種考試地方政府公務人員及離島地區公務人員考試試題

考試別：地方政府公務人員、離島地區公務人員考試

等 別：四等考試

類 科：資訊處理

科 目：資通網路與安全概要

曹勝老師

一、(一)在設定電腦或設備的網路組態時，常需要設定子網路遮罩 (Subnet mask) 這個參數，請問子網路遮罩的用途為何？(5 分)

(二)若某電腦獲分配的 IP 位址為 168.199.170.82/27，則該電腦所在網段的 Network ID 為何？該網段的最後一個 IP 位址為何？(以上答案必須以十進位表示，並且需寫下計算過程才計分)(10 分)

(三)DHCP (Dynamic Host Configuration Protocol) 及 NAT (Network Address Translation) 這兩種方法都可以解決組織內 public IP 位址數量不夠的問題，請說明這兩種方法的區別。(10 分)

1. 《考題難易》★★

2. 《破題關鍵》：子網路遮罩劃分網路與主機部分，用於計算 Network ID 和廣播位址；DHCP 動態分配內部 IP 位址，NAT 在內外網間轉換 IP，解決公有 IP 位址不足問題。

【擬答】

(一)子網路遮罩的用途

子網路遮罩 (Subnet mask) 的主要用途是區分 IP 位址中的「網路位址 (Network Address)」與「主機位址 (Host Address)」部分，從而確定一個設備所在的子網範圍。它透過位元運算 (與運算 AND) 來將 IP 位址分成網路部分和主機部分。子網路遮罩的作用在於：

1. 有助於劃分大型網路為更小的子網路，提高網路管理效率。
2. 控制廣播範圍，減少廣播流量，提升網路性能。
3. 增加 IP 位址的利用率，支持網路的層級化設計。

(二)已知 IP 位址為 168.199.170.82/27。/27 表示子網路遮罩為 27 個 1 位元，即二進位表示為 11111111.11111111.11111111.11100000，十進位表示為 255.255.255.224。

1. 計算 Network ID

將 IP 位址轉為二進位：

168.199.170.82 → 10101000.11000111.10101010.01010010

子網路遮罩為：11111111.11111111.11111111.11100000

執行 AND 運算：

IP 位址 : 10101000.11000111.10101010.01010010

子網遮罩 : 11111111.11111111.11111111.11100000

結果 : 10101000.11000111.10101010.01000000

結果轉換為十進位：168.199.170.64

因此，Network ID 為 168.199.170.64。

公職王歷屆試題 (113 地方特考)

2. 計算最後一個 IP 位址 (Broadcast Address)

該網段的可用位址範圍為 $2^{(32-27)} = 32$ 個 IP 位址，從 Network ID 開始。最後一個 IP 位址是廣播位址，其位元表現為：Network ID 的網路部分不變，主機部分全為 1。

網路部分：10101000.11000111.10101010.01000000

主機部分：00000000.00000000.00000000.00011111

結果：10101000.11000111.10101010.01011111

結果轉換為十進位：168.199.170.95

因此，最後一個 IP 位址為 168.199.170.95。

(三) DHCP 與 NAT 的區別

1. DHCP (Dynamic Host Configuration Protocol)

自動分配內部網路中的設備 IP 位址。解決方式：

- (1) 使用 DHCP 將有限的 IP 位址池（內部或私有 IP）動態分配給設備。
- (2) 當設備不再需要 IP 時，回收並重新分配。
- (3) 節省公有 IP 位址的使用，特別適合組織內設備數量變動較大的情況。

2. NAT (Network Address Translation)

在內部網路與外部網路（如互聯網）之間轉換 IP 位址。解決方式：

- (1) 內部網路中的所有設備共用一個或少量的公有 IP 位址，通過 NAT 映射到私有 IP 位址。
- (2) 在傳送資料封包時，路由器將內部私有 IP 位址替換為公共 IP 位址，並記錄對應關係。
- (3) 適合解決內部網路設備需要存取互聯網的問題。

3. 比較

特性	DHCP	NAT
功能目標	分配 IP 位址	位址轉換
影響範圍	內部網路的設備管理	內外網路通訊
可用情境	組織內設備數量多、頻繁變動	公有 IP 位址不足時實現互聯網訪問

二、DNS (Domain Name System) 是非常重要的 TCP/IP 協定。請說明其功用與 DNS 的工作原理。和一般應用協定只使用 TCP 或 UDP 不同，DNS 同時使用 TCP 及 UDP 協定，請說明其理由。(25 分)

1. 《考題難易》★★★

2. 《破題關鍵》：DNS 將域名解析為 IP 位址，透過分層結構與遞歸查詢完成解析。DNS 使用 UDP 提升效率，當數據超過 512 字節或需區域傳輸時切換至 TCP 確保可靠性。

【擬答】

(一) DNS 的功用

DNS (Domain Name System) 的主要功能是將人類易於記憶的域名 (Domain Name) 轉換為計算機網路可以理解的 IP 位址，並提供反向解析功能 (將 IP 位址轉為域名)。功用包括：

1. 域名解析：將如 www.example.com 轉為對應的 IP 位址 (如 192.0.2.1)。
2. 分布式管理：使用層級化架構，有效管理全球的域名和 IP 位址映射。
3. 負載均衡：某些情境下，DNS 可以返回不同的 IP 位址，達到分散流量的目的。

(二) DNS 的工作原理

DNS 透過分層結構和遞歸查詢的方式完成域名解析，主要包括以下步驟：

1. 客戶端請求（查詢過程）

使用者在瀏覽器中輸入域名後，瀏覽器向本地的 DNS 解析器發送查詢請求。若本地 DNS 有該域名的緩存記錄，直接返回結果；否則，進一步請求。

2. DNS 查詢過程（逐步解析）

遞歸查詢：本地 DNS 解析器代替客戶端查詢完整解析結果，需向多個伺服器請求。

分層查詢：

(1)根域名伺服器：提供頂級域（如 .com、.org）的伺服器資訊。

(2)頂級域（TLD）伺服器：提供特定域（如 example.com）的權威伺服器資訊。

(3)權威 DNS 伺服器：返回最終的 IP 位址。

3. 回傳結果

本地 DNS 解析器將 IP 位址返回給客戶端。瀏覽器使用該 IP 位址向目標伺服器發起連接請求。

(三) DNS 同時使用 TCP 和 UDP 的理由

1. DNS 使用 UDP

預設情況下，DNS 查詢使用 UDP 協定的 53 號埠，因為：

(1)效率高：UDP 是無連接協定，沒有握手過程，適合快速傳遞小量數據（典型查詢封包小於 512 字節）。

(2)負擔低：對於輕量級查詢，UDP 減少了伺服器的負擔。

2. DNS 使用 TCP

某些情況下，DNS 使用 TCP 協定的 53 號埠：

(1)資料量較大：若查詢或回應資料超過 512 字節（例如 DNSSEC 驗證數據或大型記錄集），則切換至 TCP 傳輸，確保資料完整性。

(2)區域檔案同步：DNS 區域傳輸（Zone Transfer，伺服器之間同步資料）需要使用 TCP，以確保可靠的數據傳輸和順序。



資訊處理榮耀上榜

110地特四等 台北市狀元	110地特四等 金門縣狀元	111普考 全國榜眼	111地特三等 金門縣榜眼	110地特三等 桃園市第四	110地特三等 花東區第四	111地特四等 台北市第八	110普考 全國第十
于○	吳○展	羅○昌	李○杰	丁○妮	羅○哲	吳○進	陳○廷

普考榜眼

高普雙榜

半年考取

應屆考取



非常感謝補習班提供的題目資源，使得真正在上場考試時，總有這樣的心得：「好耶，這題我完全會寫。」當下真的非常開心，因為我先前沒有去報考其他考科練筆，完全依靠補習班資源，有這樣的結果實在太好了。

羅○昌 高普考-資訊處理

三、請說明何謂中間人攻擊 (Man-in-the-Middle Attack)，並舉例說明兩種不同中間人攻擊的方法。當面對中間人攻擊的威脅時，請說明可行的防範作法。(25 分)

1. 《考題難易》★★★

2. 《破題關鍵》：中間人攻擊攔截並竄改通訊，常見方法包括 ARP 欺騙和 Wi-Fi 假熱點。防範措施為使用 HTTPS、VPN、ARP 防護、MFA，更新設備，並提高用戶安全意識以避免敏感信息泄露。

【擬答】

(一)中間人攻擊 (Man-in-the-Middle Attack) 定義

中間人攻擊是一種網路攻擊形式，攻擊者偷偷攔截並可能竄改兩方之間的通訊，而通訊雙方通常無法察覺其存在。攻擊者可能進一步竊取敏感資訊（如密碼、信用卡資訊）或注入惡意數據。

(二)中間人攻擊的方法與舉例

1. 方法一：ARP 欺騙 (ARP Spoofing)

攻擊者偽造 ARP 資訊，將自己的 MAC 位址綁定到目標的 IP 位址，誘使資料流經過攻擊者的設備。使用者 A 與路由器通訊時，攻擊者 C 偽裝成路由器，讓 A 將資料發送給 C，而 C 轉發給路由器。C 在此過程中可竊取或修改資料。本地區域網路 (LAN) 中的設備容易受到此類攻擊。

2. 方法二：Wi-Fi 攻擊 (Evil Twin)

攻擊者建立一個與合法 Wi-Fi 熱點名稱相同的假冒熱點，誘使使用者連接，從而攔截使用者的流量。例如在咖啡廳，攻擊者建立一個名為 "Coffee_WiFi" 的假熱點，當使用者連接後，攻擊者即可監控所有傳輸的資料（如網站登入憑證或聊天訊息）。公共 Wi-Fi 環境中，此方法尤其常見。

(三)防範中間人攻擊的方法

1. 使用 HTTPS 協定

確保瀏覽器與網站之間的通訊使用加密的 HTTPS 協定 (TLS/SSL)，以防止通訊過程被攔截和竄改。檢查網站是否有有效的 SSL 憑證，並留意是否有憑證錯誤警告。

2. 啟用 VPN (虛擬私人網路)

使用 VPN 加密所有網路流量，即使在不安全的公共網路中，也能保護通訊安全。VPN 將所有數據包通過加密通道傳輸，防止被第三方攔截。

3. 啟用網路層防禦

ARP 欺騙防護：使用靜態 ARP 表或啟用交換機的 ARP 防禦功能（如 Dynamic ARP Inspection, DAI）。Wi-Fi 防護僅連接受信任的 Wi-Fi 熱點，並避免使用開放式 Wi-Fi 網路。

4. 多因子認證 (MFA)

即使攻擊者獲取了使用者的登入憑證，多因子認證可以增加額外的身份驗證步驟，阻止未授權訪問。

5. 更新設備與軟體

確保作業系統、防毒軟體、瀏覽器及其他應用程式均為最新版本，以修補可能被利用的漏洞。

6. 教育與警惕

提升使用者對網路安全的意識，學會辨別可疑行為（如 Wi-Fi 假冒或憑證警告）。

志光 學儒 保成

順利考取有訣竅



一年考取 高普雙榜

112高普考資訊處理
涂○瑋

各科老師都會詳細解說考試重點，讓我好好學習那些不熟悉的知識。考前總複習班各科老師以最短的時間來帮大家複習重點及預測考試的命題趨向，對於一整年的課程有畫龍點睛的功效。



非本科系 高普雙榜

112高普考資訊處理
傅○華

老師都是以實例還有時事去講解，所以非常的清楚也好記憶，跟著老師的步驟，配合每一次章節結束的歷屆試題講解，就知道遇到題目時該如何解題，讓非本科生的我受益良多。

想了解更多訣竅？

歡迎至 志光.學儒.保成 全國門市洽詢

四、密碼學在資通安全扮演極為重要的角色，請比較對稱式密鑰和非對稱式密鑰兩種加密方法的優缺點，並說明非對稱式密鑰須使用公鑰憑證(public key certificate)的理由。公鑰憑證要由 PKI (Public Key Infrastructure) 提供，請說明 PKI 之意義與功用。(25 分)

1. 《考題難易》★★

2. 《破題關鍵》：對稱式密鑰效率高但密鑰分發困難；非對稱式密鑰支持數位簽章但速度慢。公鑰憑證和 PKI 確保公鑰可信，防止中間人攻擊，通過憑證管理建立信任關係與數據完整性。

【擬答】

(一)對稱式密鑰與非對稱式密鑰加密方法的比較

1. 對稱式密鑰加密

對稱式加密使用相同的密鑰進行資料的加密與解密。優點是速度快：加密和解密過程較非對稱加密效率高，適合處理大規模數據。算法簡單：對稱加密算法計算量小，資源需求低。缺點則是密鑰分發困難：需要安全的渠道將密鑰傳遞給通信雙方，若密鑰洩漏，資料安全性無法保障。也不支持數位簽章：對稱式加密無法直接提供身份驗證或數位簽章功能。

2. 非對稱式密鑰加密

非對稱式加密使用一對密鑰：公鑰 (Public Key) 與私鑰 (Private Key)。公鑰用於加密，私鑰用於解密；反之亦然。優點是密鑰管理更安全：只需保護私鑰，公鑰可公開分享，無需建立安全通道傳遞密鑰。也支持數位簽章：提供身份驗證與數據完整性驗證功能，能防止數據被篡改。缺點是效率低：加密與解密過程計算量大，速度較慢，不適合處理大量數據。算法複雜：實現與運算成本較高。

(二)非對稱式密鑰需使用公鑰憑證的理由

非對稱式加密的安全性依賴於公鑰和私鑰的配對，但若攻擊者冒充合法方提供假公鑰，通

訊安全將無法保障。公鑰憑證的作用：

1. 驗證公鑰的真實性：確保公鑰的所有者是聲稱的主體，而非冒充者。
2. 建立信任關係：通過信任的憑證頒發機構 (Certificate Authority, CA) 簽署，證明公鑰的合法性。
3. 防止中間人攻擊：若無公鑰憑證，攻擊者可能冒充合法方攔截或竄改通訊。

(三) PKI 的意義與功用

1. PKI 的意義

PKI (Public Key Infrastructure, 公鑰基礎建設) 是一套以公開密鑰加密技術為核心的架構，用於管理公鑰的生成、分發、儲存、驗證及撤銷。

2. PKI 的功用

- (1) 憑證管理：提供公鑰憑證的簽署、發佈與撤銷，確保通訊中的公鑰可信。
- (2) 身份驗證：確保通訊雙方的身份真實性。
- (3) 數據完整性：透過數位簽章驗證數據是否被篡改。
- (4) 建立信任鏈：透過憑證頒發機構 (CA) 和信任層級，為參與方建立安全信任。

(四) 公鑰憑證與 PKI 的運作流程

1. 憑證申請：主體向 CA 提交公鑰及身份資訊。
2. 憑證簽署：CA 驗證申請者身份後，用其私鑰對公鑰與身份資訊進行簽署，生成公鑰憑證。
3. 憑證分發：公鑰憑證由 CA 分發給申請者，並登錄於憑證目錄供查詢。
4. 憑證驗證：接收者檢查公鑰憑證，通過驗證 CA 的數位簽章，確保公鑰的真實性。
5. 憑證撤銷：若公鑰洩漏或不再有效，CA 將撤銷憑證並發佈撤銷列表 (CRL)。



志光 學儒 保成 高普考.地方特考

資訊處理上榜養成規劃

 基礎架構課程 考科概念建立 適應教學模式	 正規課程 規劃完整堂數 雙循環雙師資	 進階課程 獨家圖解階段複習 解題技巧灌輸
 趨勢講座 時事考點補充 命題趨勢分析	 題庫班 精選題目教學 學習快速解題	 總複習班 科目重點整理 考前強化記憶

詳細課程內容，歡迎至志光學儒保成全國門市洽詢