《資通網路與安全概要》

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）

試題評析	為中層傳輸與高層應用之題型。
考點命中	《高點・高上資通網路講義》第3章，張又中編撰，頁3-13~14；第4章，頁4-17。

答：

(一)為了根據環境需求彈性運用 IP，可將網路再劃分子網路(Subnet)，將原有主機號碼的某些位元拿來作為子網路號碼，表示為[Network#, Subnet#, Host#]。

(二)168.199.170.82 AND 255.255.255.224=168.199.170.64；

該網段的最後一個 IP 位址為 168.199.170.95。

(三)DHCP Server 使用 UDP Port 67，DHCP Client 使用 UDP Port 68。採用 BOOTP 的格式並做小幅度修改，讓主機可自動取得如 IP 位址、網路遮罩、閘道器配置等網路組態資訊。

NAT 則為組織內部有多台主機，然只有少量公開 IP 位址，可於組織內部的多台主機使用內部 IP，並透過 NAT 將內部 IP 與外部 IP 作對應轉換。

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）

試題評析	屬高層應用之考題。
考點命中	《高點・高上資通網路講義》第4章，張又中編撰，頁4-4~7。

答：

DNS使用TCP、UDP Port 53的一種索引查詢服務，將人們可閱讀的ASCII字串形式主機名稱，對映轉換成數字形式的IP位址，亦支援郵件目的位址和IP位址間的對應。其採用階層式(Hierarchy)、領域基礎、由小至大的命名方式，網域大小寫對解析結果沒有影響。每一級網域長度限制為63字元，網域總長度不能超過253字元。

DNS同時採用TCP與UDP協定之原因，在於UDP封包不能大於512 Bytes，TCP封包則無此限制。然而，UDP封包由於構造簡單，故網路設備解析快，相較TCP封包傳輸效率較佳。因此，DNS使用UDP來交換小型資訊，如用戶端取得DNS Server之回應；惟若用戶端未能取得DNS Server回應，則在間隔3~5秒後使用TCP重新查詢。另為維持DNS區域資料庫之一致性，DNS一律採用可靠之TCP傳輸區域資料。

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）

試題評析	為資訊安全攻擊與防禦題型。
考點命中	《高點・高上資訊安全實務講義》第3章，張又中編撰，頁3-16。

答：

(一)中間人攻擊亦稱桶列攻擊(Bucket Brigade Attack)，攻擊者與通訊兩端分別建立獨立聯繫，並交換其所收到的資料，使通訊兩端認為他們正在與對方通訊，但事實上整個過程都被攻擊者完全控制。

(二)中間人攻擊可行的防範作法有：

1.第二校驗

密碼和金鑰有額外的保密需求，如公鑰可由憑證頒發機構驗證，並透過安全管道發送，亦可進行線上驗證。

2.延遲測試

例如：傳輸過程超過預期之延遲，則可能存在中間人。如加密通訊整體延遲為10秒，若通訊整體延遲超過30秒，則傳輸雙方之間可能存在中間人。

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）

試題評析	係屬資訊安全範疇之基礎題型。
考點命中	《高點・高上資通安全法規講義》第1章，張又中編撰，頁1-6~9、12~13。

答：

(一)對稱式密鑰和非對稱式密鑰優缺點比較：

1.對稱式密鑰加密方法 (Symmetric Encryption Method)：

又稱單一金鑰 (Single Key)、對稱金鑰(Symmetric Key)、秘密金鑰(Secret Key)加密法。

傳送方對明文的加密與接收方對密文的解密都是使用同一把金鑰進行XOR運算，易於以硬體實做，適用於大量資料的加解密。

此密鑰加密方法運算速度快，需較少的計算資源，主要缺點即密鑰的分發，增加安全上的風險。

2.非對稱式密鑰加密方法(Asymmetric Encryption Method)：

又稱非對稱式金鑰(Asymmetric Key)加密法。

傳送方對明文的加密與接收方對密文的解密使用兩把不同的金鑰，一把為公開金鑰(Public Key)，另一把為私密金鑰(Private Key)，適用於少量資料的加解密。

非對稱加密方法系統運行得非常緩慢，且因其密鑰長度長，因此需要更多的計算資源。

(二)非對稱式密鑰須使用PKI來管理公鑰憑證，PKI之意義與功用如下：

1.簽發憑證

使用者自行產生金鑰對(Public-private Key Pair)後，便可向CA(Certificate Authority)申請簽發憑證。CA審核使用者資料無誤後，便用自己的私密金鑰對該使用者的公開金鑰簽章，形成憑證。

2.註銷憑證

當使用者的金鑰對在到期前便已經不安全，此時必須立刻到CA註銷舊有的憑證，且註銷憑證的消息必須很快地傳遞給PKI的所有成員。

3.憑證的取得、解讀以及驗證

CA將使用者註冊的憑證放在經過檢查認可的目錄伺服器(Directory Server)，使用者可透過其取得指定的憑證。此外，CA也將憑證註銷表一併放在目錄伺服器上，以備驗證之用。