電腦網路100（關務）

一、請說明 DNS（Domain Name System）的主要與次要伺服器之間的關係，以及 Cache 伺服器的功能。（15 分）

調90.2

二、請說明 TCP（Transmission Control Protocol）協定發生「逾時」（Timeout）之可能原因。（10 分）

Timeout 是因封包遺失引起的，如：

(1) 當終端主機送出去的封包，在傳送的過程中遺失。

(2) 當終端主機送出去的封包，正確無誤到達目的終端主機，但ACK在回應的過程中遺失。

(3) 當終端主機送出去的封包正確無誤到達目的終端主機，但ACK雖然回應，但在傳送過程中延遲到達。

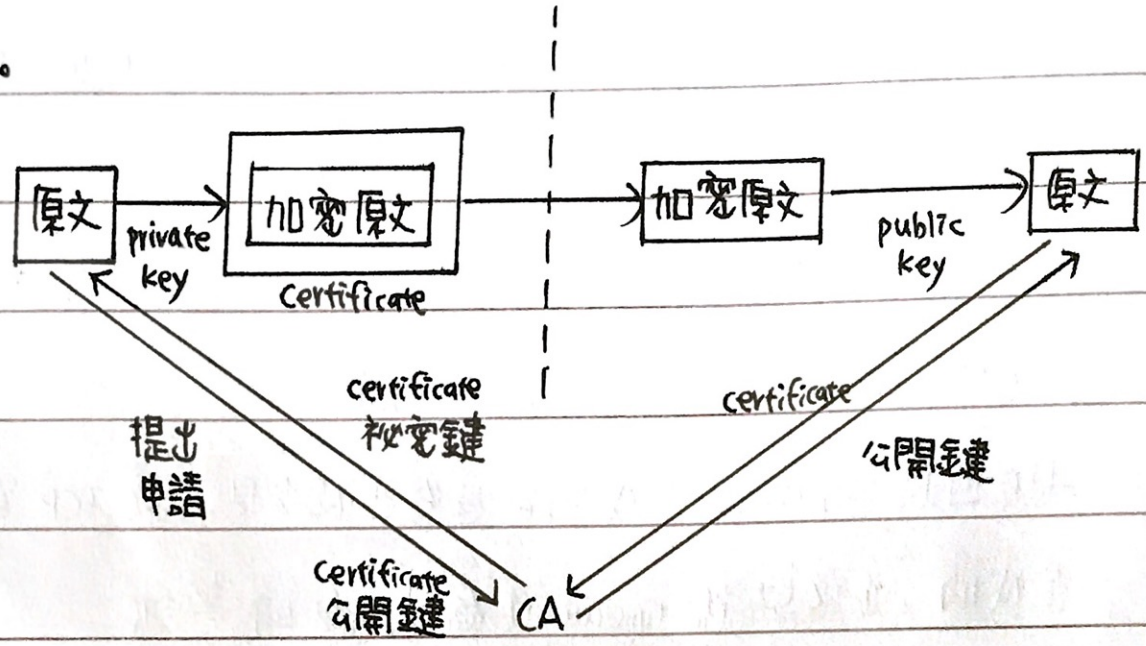
現在因傳輸錯誤造成封包遺失已很少見，故 TCP 皆假設 timeout 是由塞塞造成的，並以監視 timeout 作為問題的警訊。

三、若是 TCP 的「三向交握」（Three-Way Handshake）已完成前 2 個部分，而第 3 部分在傳送過程中遺失，則依然可開始傳送資料嗎？請說明原因。（10 分）

三向交握三步驟，不論第一（SYN1）或第二（SYN2+ACK1）的訊息封包遺失，都会直接造成連線的失敗；但縱使第三步（ACK2）沒有被完整的完成，此連線所需要的同步資訊 SYN1 和 SYN2 都已在前2步驟完成交換動作，故連線已可由 Client → Server 的傳輸，雖然 Server → Client 還無法正常傳輸，但當 Server 收到第一次由 Client → Server 的資料傳輸後，表示連線已完成，就取代第三步驟，故 Client 在送出最後階段的 ACK2 後，不必經過對方再確認，就馬上開始傳送資料給 Server。

四、如何使用公開金鑰密碼技術以同時達到身分驗證與資料保密？試繪圖說明之。（10 分）

如下圖，使用前 sender 必須先向 CA 申請，CA 驗證身份後發給 sender 的 private key 和权位憑證（certificate）；傳送時，sender 以 private key 加密原文，並搭配 certificate 傳出。sender 收到後，向 CA 遞交 certificate 和本身的身分憑證，CA 驗證無誤後会回傳 sender 的 public key，receiver 以此 public key 解密。此法可由 CA 驗證傳接双方身分，並達成傳輸保密性。



五、㈠若是 TCP/IP 協定組中沒有「傳輸層」，也就是沒有「連接埠」（Port）的存在，試問會有什麼結果？（10 分）

㈡為何「傳輸層」也稱之為「End-to-End」或「Host-to-Host」？（5 分）

(一) 由於Transport layer 負責定義連接埠(port)，可指定特定主機上的特定應用程式，若缺少此層，即無法完成此一指定，造成各主機只容許單一應用程式執行，否則会造成混淆。

故 Client 端主機在同一時間只能有一個應用程式和網路連線，server 端主機在同一時間只能提供一種服務，無法同時提供多種服務。

(二) 因 Transport layer 只負責 sender 到 receiver 之通訊，而不管中間所經過的子網路，只在 sender 和 receiver 主機上執行。

六、請說明 MAC 位址、IP 位址與網域名稱（Domain Name）之間的關係。另外，其彼此間轉換的協定各為何？（15 分）

(一) MAC address（獨一無二）代表主機在網路上的實体位址，通常每一張網路卡上都有一個 MAC address，此一位址在網路卡出廠時就燒在卡上了，每部機器則視其上網路卡枚量而有不同的 MAC address。

IP address 代表主機在網路上的邏輯位址，是連上 Internet 不可或缺且唯一的位址，但此一位址可以改動，通常由軟体系統維護。

Domain Name 是為了解決 IP address 均為数字難以記憶的問題而產生，用類似英文地址的方式編製。每個網域名稱對應到 1 個 IP address，但一個 IP address 可對應到多個網域名稱。

(二) MAC address → IP address：用 RARP、BOOTP、DHCP。

IP address → MAC address: ARP。

IP address ↔ Domain Name: DNS。

七、當封包經過 1 個網路設備時，網路介面卡可根據那 4 種方式來判斷該封包是否要往上層傳送？（10 分）

(一) 目的位址和本機位址相符。

(二) 目的位址為群播位址 (multicast)，而本機亦是該群播位址的一個成員。

(三) 目的位址為廣播位址 (broadcast)。

(四) 網路介面卡被啓動為混雜模式，指一台機器的網路卡能接收所有經過他的資料，而不論其目的位址是否是他。

八、(一)試說明 NAT（Network Address Translation）伺服器的運作原理。（10 分）
(二)試問何謂靜態 NAT 與動態 NAT？（5 分）

(一) NAT：詳92.6.4