105 年公務人員特種考試警察人員、一般警察人員考試及 105 年特種考試交通事業鐵路人員試題

考試別：鐵路人員考試
等　別：高員三級考試
類　科：資訊處理
科　目：資料通訊

一、請試述下列名詞之意涵：
㈠電路交換（Circuit switching）
㈡同位檢查（Parity check）
㈢路由器（Router）
㈣進階加密標準（Advanced encryption standard）
㈤點對點協定（Point-to-Point protocol）

【擬答】：
㈠電路交換（Circuit Switching）：
當網路上兩個節點需要進行通訊時，必須先建立一條專用的線路。所建立的線路可能會經過數個中間節點，透過此一線路可以很快的傳到目的地。最常見的例子是電話系統，當撥通一通電話時，就會在雙方間建立一條專屬的線路，讓雙方進行通訊。。

㈡這是一種最常用的錯誤偵測碼，利用資料位元以外附加的同位位元，檢測資料儲存或傳送是否發生錯誤。偶同位檢查（Even Parity check）要求所儲存或傳送資料（包含資料位元與同位位元）含偶數個 1，否則即為錯誤。⑵奇同位檢查（Odd Parity check）要求所儲存或傳送資料（包含資料位元與同位位元）含奇數個 1，否則即為錯誤。

㈢路由器（Router）是一種電訊網路裝置，提供路由與轉送兩種重要機制，可以決定封包從來源端到目的端所經過的路由路徑（host 到 host 之間的傳輸路徑），這個過程稱為路由；將路由器輸入端的封包移送至適當的路由器輸出端（在路由器內部進行），這稱為轉送。路由工作在 OSI 模型的第三層(網路層)，例如網際協定（IP）。

㈣進階加密標準（Advanced Encryption Standard， AES），是美國聯邦政府採用的一種區塊加密標準。這個標準用來替代原先的 DES，已經被多方分析且廣為全世界所使用。演算法採用對稱區塊加密（symmetric block cipher），區塊長度固定為 128 位元，金鑰長度則可以是 128，192 或 256 位元。

㈤是用在 PC 與 ISP 的路由器間的點對點資料鏈結層協定，可以傳送 IP 訊簡到串列線路上，提供錯誤偵測以及資料壓縮的能力，在連接時可以自動分配 IP 地址，也提供身份確認、認證（authentication）的功能。

二、請回答下列相關問題：
㈠ ping 指令是用來診斷網路連線狀態與連線品質，若網路品質監測公用程式 ping 指令之執行如下⒜及⒝所示兩種結果，請問其所呈現的意義為何？試詳細說明之。
> ping www.wxyz.edu.tw [Enter]
⒜Ping www.wxyz.eud.tw[140.126.2.30] with 32 bytes of data:
Reply from 140.126.2.30 : bytes=32 time<1 ms TTL=234
Reply from 140.126.2.30 : bytes=32 time<1 ms TTL=234
Reply from 140.126.2.30 : bytes=32 time<1 ms TTL=234
Reply from 140.126.2.30 : bytes=32 time<1 ms TTL=234
⒝Bad IP address www.wxyz.edu.tw

㈡由於網路無遠弗屆，但常常碰到網路不通或網路很慢等問題，就這類問題檢測網路時，有那幾種可能原因導致網站無法連接？試詳細說明之。

【擬答】：

㈠(a)表示可以連上 www.wxyz.edu.tw(140.126.2.30)，反應時間小於 1 毫秒，TTL（Time To Live）值為 234，因此本機到 www.wxyz.edu.tw 通過 255-234 = 210 個路由。

(b)這個資訊表示可能沒有連接到 DNS 伺服器，所以無法解析這個 IP 位址，也可能是 IP 位址不存在。

㈡1.網路線材問題：包括網路線被截斷、網路線過度扭曲變形造成訊號不良、網路接頭品質不良、網路接頭與設備(如 Hub) 接觸不良。

2.網路設備問題：例如網路卡不穩定、品質不佳，或不相容度佳；各網路設備接觸不良造成訊號衰減；因網路設備所在環境導致；網路設備使用不良造成功能衰減 。或因網路線太長導致訊號衰減、使用錯誤的網路線、其他雜訊的干擾等。

3.網路卡設定錯誤：例如 IP 設錯會造成 IP 衝突，netmask 設定錯誤、網路卡驅動程式使用錯誤等。

4.閘道器問題：如預設閘道 (default gateway) 設定錯誤或介面不符都會讓封包無法送出。

5.通訊協定不合：通常發生在不同的作業系統之間的通訊傳輸，必須安裝特定通訊協定。

6.對方網站問題。

三、網路安全已是網路架構的標準配備，在公眾網路傳送或儲存在資料庫裡的資料，無論是商業機密，或是個人隱私資料，皆必須做好網路安全的工作，請回答下列相關問題：

㈠為什麼在網路系統中，需要進行使用者身分（Identity）及鑑別（Authentication）？試詳細說明之。

㈡對於基本的加解密系統中，為什麼加密方法或演算法需要公開？試說明之。

【擬答】：

㈠在網路系統中，使用者身分識別主要是要辨識某人是否為合法的系統使用者。可分為二部份：使用者身分（Identity）及鑑別（Authentication）。識別身分是系統必須能夠唯一識別每一位合法使用者。鑑別身分是系統必須不含糊地驗證使用者所宣稱之身分。不但要能夠唯一識別使用者身分，而且必須要有方法來預防冒充別人身分的能力。

㈡因為加密方法或演算法不公開，則無法被檢視其中是否存在後門或弱化的漏洞，而造成安全疑慮，例如 DES 由於開發過程中美國國安局介入，就被懷疑可能在未公開的演算法或可被容許輸出的系統中隱藏後門，因此在 AES 的徵求中，就被要求公開演算法。

四、TCP/IP 是一種網路通信協定，目前已成為一項國際標準協定，請回答下列相關問題：

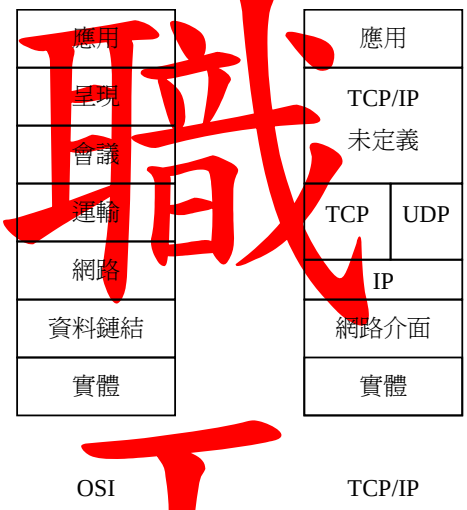
㈠ TCP/IP 主要功能為何？細分幾個層級（Layer）？試繪圖說明之。

㈡ IP 主要功能及 IP 資料頭格式包括那些重要欄位？IP 封包中的 port number 欄位用途為何？試加以詳細說明之。

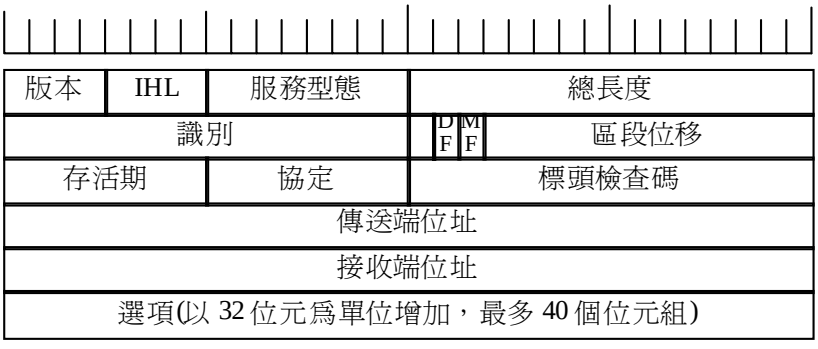
【擬答】：

㈠ TCP/IP 可以用來連接全世界各 LAN 的網路，提供點對點的連結機制，將資料應該如何封裝、定址、傳輸、路由以及在目的地如何接收，都加以標準化。它將軟體通訊過程抽象化為四個抽象層，採取協定堆疊的方式，分別實作出不同通訊協定：

1. 網路介面層(Link layer)：此層實際上並不是網際網路協定組中的一部分，但是它是封包從一個裝置的網路層傳輸到另外一個裝置的網路層的方法。這個過程能夠在網卡的軟體驅動程式中控制，也可以在韌體或者專用晶片中控制。進行添加報頭準備傳送、通過實體媒介實際傳送這樣一些資料鏈路功能。另一端則完成資料訊框接收、去除報頭並且將接收到的包傳到網路層。
2. Internet 層：此層定義的協定就是 IP（Internet Protocol），負責將 IP 分封傳到所要求的目的地，其功能相當於 OSI 中的網路層。
3. 運輸層（Transport layer）：此層設計來讓機器間可以進行持續的交談，其功能相當於 OSI 中的運輸層，包括 TCP 與 UDP 兩個協定。
4. Application 層：包括所有和應用程式協同工作，利用基礎網路交換應用程式專用的資料的協定。



㈡ IP（Internet protocol）協定定義了一個不可靠（Unreliable）、盡力的（best-effort）、無連接（connectionless）的分封傳送機制。其中所謂不可靠是指傳送得不到保障，分封可能失去、重複、延遲或失序，系統對於這些問題都不會檢測，也不會通知傳送端或接收端；盡力則指軟體會儘可能的傳送分封，不會反覆無常的丟棄資料，除非資料耗盡或網路出錯；無連接則指每一分封都會獨立處理，同一機器發出的分封可能經由不同路徑前往目的地。IP 協定格式固定至少 20bytes，最多可達 60 bytes。包含下列欄位：



1. 版本：可以追蹤目前分封屬於哪一個版本的協定。
2. IHL（Internet Header Length）：說明標頭長度，最小為 5，最大為 15，每一單位表示一

個四位元組。

3. 服務型態：允許主機告訴子網路所需服務，包括可靠度與速度的組合。此欄最左邊是一個 3 位元的優先欄，表示優先權。
4. 總長度：表示整個分封的長度，最長可達 65535 bytes。
5. 識別：用來辨識新進入的區段屬於哪一個訊簡，同一訊簡的區段會含有相同的識別值。
6. DF（Don't Fragment）與 MF（More Fragment）：DF 表示不要產生區段，因為接收端可能無法還原；MF 表示更多區段，通常除了最後一個區段外，其餘區段都會設定這個位元，用來檢查訊簡所有區段有沒有完全到達。
7. 區段位移：用來說明該區段是在訊簡中的哪個位置，除了最後一個區段外，其餘區段都必須是 8 bytes 的倍數。因為此欄位有 13 bits，因此每個訊簡最多可分割為 8192 個區段，因此最大訊簡長度為 65536 bytes。
8. 存活期（Time to Live）：這個 8 位元欄位避免訊簡在網際網路中永遠存在（例如陷入路由環路）。存活時間以秒為單位，但小於一秒的時間均向上取整到一秒。在現實中，這實際上成了一個跳數計數器：訊簡經過的每個路由器都將此欄位減一，當此欄位等於 0 時，訊簡不再向下一跳傳送並被丟棄，以防止訊簡不停在外遊蕩。
9. 協定：說明採取何種運輸協定處理此一訊簡，可以是 TCP、UDP 等。
10. 標頭檢查碼：只檢查標頭，每次跳躍後都要重新計算。
11. 傳送端位址與接收端位址：用來表示網路與主機號碼。
12. 選項：變動長度，允許後續版本的協定可以增加新資訊。

㈢ IP 封包所載送資料包括 TCP 標頭，其中包括 port number，包含傳送端埠與接收端埠，用來辨識連結，此二者合成串接號碼。

五、網路對於生活影響程度與日俱增，駭客利用網路從事電腦犯罪也屢見不鮮，請回答下列相關問題：

㈠何謂分散式阻斷服務攻擊（DDoS）？試說明之。

㈡常見的網路系統安全威脅來自那三個來源？試說明之。

【擬答】：

㈠阻斷服務式（Denial of Service; DoS）攻擊是指任何導致伺服器不能正常提供服務的攻擊，分散式服務阻斷式攻擊（Distributed Denial of Service; DDoS）則是攻擊端分散在很多的主機上，同時對目標伺服器發動阻斷服務的攻擊。

㈡ *1.* 機密性（Confidentiality）：確保資訊的機密，防止機密資訊洩漏給未經授權的使用者，可透過資料加密的程序以達到此目標。

2. 完整性（Integrity）：保證資料內容僅能被合法授權者所更改，不能被未經授權者所篡改或偽造。為了確保資料能正確無誤的傳送到接收者可以採用雜湊函數、或將訊息加密。

3. 可用性（Availability）：確保資訊與系統持續運轉，以防止惡意行為導致資訊系統毀壞。當合法使用者要求使用資訊系統時，使用者均可在適當的時間內獲得回應，並完成服務需求。