

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考試試題

代號：20160

全一張  
(正面)

考試別：一般警察人員考試

等別：二等考試

類科別：刑事警察人員電子監察組

科目：網路工程

考試時間：2小時

座號：\_\_\_\_\_

※注意：(一)禁止使用電子計算器。

(二)不必抄題，作答時請將試題題號及答案依照順序寫在試卷上，於本試題上作答者，不予計分。

一、不管是開放系統互連 (OSI) 協定模型或是 TCP/IP 協定模型都有網路層 (network layer)，定義網路路由器 (router) 轉送封包的功能。(每小題 10 分，共 20 分)

(一)請就路由表的產生、路由表的查詢，詳述 IP 路由器如何達成封包轉送的功能。

(二)請詳述現今 IP 網路如何控制路由表的大小 (size) 在合理的範圍。

二、802.11 無線區域網路 (wireless LAN) 技術和 LTE (Long Term Evolution) 都是現今廣泛使用的無線通訊技術。

(一)請就這兩個技術的傳輸距離、所使用的媒體存取控制 (medium access control) 機制、應用情境，作一說明並比較。(6 分)

(二)請說明使用這兩個技術的通訊系統如何共存。(4 分)

三、計算一個封包在網路中傳送的時間延遲 (delay) 須考慮封包傳輸時間 (transmission time)、訊號傳遞延遲 (propagation delay)、排隊延遲 (queuing delay)、處理時間 (processing time) 等因素。(每小題 8 分，共 16 分)

(一)請詳述此四項時間延遲是如何產生的。

(二)假設一個長度為 10,000 Byte 封包從來源端到目的地端需經過三個節點 (node)。由來源端至第一個節點的鏈結 (link) 的頻寬是 100 Mbps，距離是 1 公里，第一與第二、第二與第三節點之間鏈結的頻寬是 1 Gbps，距離是 10 公里，第三個節點至目的地端的鏈結的頻寬是 100 M，距離是 3 公里。一個節點從收到封包到決定如何轉送封包需花費 1 ms。假設訊號在鏈結上的傳遞速度 (propagation speed) 是 200,000,000 m/s，且網路上只有這個封包在傳送，請計算此一封包從來源端到目的地端的时间延遲。

四、為了因應 IPv4 位址的逐漸匱乏，IPv6 協定的制定允許更多的 IP 位址可以被使用，在由 IPv4 過渡到 IPv6 的期間，網路位址轉換 (Network Address Translation) 的技術被暫時用於因應 IP 位址不足的困境。

(一)請詳述網路位址轉換的原理。(8 分)

(二)一般大眾在家中或公司經由網路服務營運商 (Internet Service Provider) 取得上網的服務，其家中或公司內的多個主機就是透過 NAT 與外部網路溝通，請問在此情境下，家中或公司內架設伺服器以提供如網頁服務 (www service)、檔案傳輸 (file transfer) 服務等是否可能？如果可以的話是如何達成？(6 分)

(請接背面)

考試別：一般警察人員考試  
等別：二等考試  
類科別：刑事警察人員電子監察組  
科目：網路工程

五、考慮一個由通透式 (transparent) 乙太網路 (Ethernet) 交換器 (或橋接器) 組成的大型區域網路，用以連接眾多主機 (host)。

(一)一個交換器如何知道其它交換器和主機的存在？(4分)

(二)請詳述一個交換器如何決定轉送訊框 (frame) 到目的地主機？(6分)

(三)此一網路如何避免迴路 (loop) 的產生？(4分)

六、無線網路由於其訊號是在開放空氣 (open air) 空間中傳送，所以容易遭竊聽，其安全機制遠比有線網路更為必要。

(一)在 802.11 無線區域網路的第一版安全機制是稱之為 WEP (Wired Equivalent Privacy)，但是它很容易被破解，請問其設計有那些安全性的弱點？(6分)

(二)802.11 無線區域網路之後制訂了 WPA 和 WPA2 來取代 WEP，請問它們在那些方面做了改良？(4分)

(三)802.11i 的架構 (Robust Security Networks) 中採用了密鑰交握 (key exchange handshake) 方法避免使用者設備 (Station) 和接取點 (AP) 之間的密鑰被破解，請敘述其作法。(6分)

七、一個嚴謹的無線網路安全機制可以引進 802.1X 使用者認證 (authentication) 的架構。802.1X 的架構中包含受認證者 (supplicant)、認證者 (authenticator) 以及認證伺服器 (authentication server)。

(一)802.1X 如何確認受認證者是合法使用者？(4分)

(二)802.1X 允許受認證者和認證者相互認證，也就是說受認證者可以判斷認證者不是駭客偽裝的假認證者，請問這是如何做到的？(6分)