桃園大眾捷運股份有限公司 109 年度第二次新進人員招募甄試試題

專業科目：**1.電腦網路概論(50%)** **2.資訊管理與資通安全(50%)**	測驗時間：15:40-16:40	卷別：**乙卷**
招募類組	C01 工程員（企劃資訊類）	

※注意：本卷試題每題為四個選項，答錯不倒扣，全為**單一選擇題**，請選出一個正確或最適當的答案，依題號清楚劃記，複選作答者，該題不予計分。全份共計 50 題，每題 2 分，須用 2B 鉛筆在答案卡上依題號清楚劃記，於本試題卷上作答者，不予計分。測驗僅得使用簡易型電子計算器(招募簡章公告可使用之計算機)，但不得發出聲響，亦不得使用智慧型手機之計算機功能，其它詳如試場規則。

1. (A)將 IP 位址轉換為 MAC 位址的通訊協定是下列何者？ (A) ARP (B) DNS (C) RARP (D) IMAP。
2. (B)下列何者**不是**無線區域網路的通訊協定？ (A) IEEE 802.11n (B) IEEE 802.3 (C) IEEE 802.11ax (D) IEEE 802.11ac。
3. (C)下列哪個通訊協定通常是以 UDP 作為傳輸層？ (A) POP3 (B) FTP (C) DHCP (D) SNMP。
4. (C)下列何者**不是**虛擬私人網路(VPN)所使用的通道(tunneling)標準(技術)？ (A) L2TP (B) IPSec (C) HTTP (D) PPTP。
5. (D)下列哪個通訊協定屬於 TCP/IP 應用層？ (A) TCP (B) UDP (C) IP (D) DNS。
6. (B)下列何者**不是** TCP/IP 資料連結層的工作？ (A)流量控制 (B)邏輯定址 (C)錯誤控制 (D)媒介存取控制。
7. (C)與分公司間的網路連線若考慮到成本以及安全，使用何種方式連線最好？ (A) ISDN (B) ATM (C) VPN (D) Frame Relay。
8. (C)當你的部門電腦數量增加一倍，以下何者最不可能有效改善對外網路連線速度？ (A)將原先 Gigabat 網路交換器換為 10GbE 交換器 (B)將原先 Cat-5 網路線更換為 Cat-6 (C)新增無線 IP 分享器，讓電腦改用無線網路 (D)將原先 100Mbps 網路卡換為 Gigabit 網路卡。
9. (A)下列 IP 位址何者**不是**私有位址(private address) ？ (A) 140.113.4.20 (B) 192.168.254.1 (C) 10.1.1.1 (D) 172.31.10.55。
10. (B)下列哪個通訊協定**不是**採用廣播的方式？ (A) ARP (B) HTTP (C) DHCP (D) BOOTP 。
11. (C) ARP (Address resolution protocol)之功能為何？ (A)轉換已知的 Domain name 為 IP 位址 (B)轉換已知的 MAC 位址為 Domain Name (C)轉換已知的 IP 位址為 MAC 位址 (D)轉換已知的 MAC 位址為 IP 位址。
12. (A)下列何者為 connectionless 通訊協定？ (A) SNMP (B) FTP (C) HTTP (D) Telnet。
13. (C)有關全球資訊網(World Wide Web)的描述，下列何者有誤？ (A)全球網頁是由世界各地的人自願編寫而成，透過超連結(hyperlinks)彼此串聯 (B)網頁的格式主要為 HTML (C)網頁內容只能包含文字，因此圖片及影片只能透過 FTP 傳遞 (D)網頁存放在 Web server，當收到 HTTP request 時，便傳回給瀏覽器。
14. (A)在 IEEE 標準中，VLAN 標準的編號為？ (A) 802.1Q (B) 802.3ba (C) 802.5 (D) 802.11。
15. (C)下列何者**不是** VLAN 的特點？ (A)提高安全性 (B)隔離廣播封包 (C)提升傳輸速率 (D)不受實體位置限制。
16. (D)IEEE 802.11 沒有定義哪個傳輸技術？ (A)直接序列展頻 (B)跳頻式展頻 (C)紅外線 (D)藍牙。
17. (C)Frame Relay 改良自哪個通訊協定？ (A) ADSL (B) 802.11 (C) X.25 (D) PPPoE。

18. (A)小明辦公室只有一個公開 IP 位址，但是他一共有 4 台電腦都必須連上網路，於是小明架設了一台 IP 分享器，以下何者有誤? (A) IP 分享器相當於一台交換器(switch) (B)每一台電腦動態取得內部(private) IP 位址 (C)內部使用 DHCP server 負責管理內部 IP 位址(D)對外而言，小明每一台電腦連線都是透過同一個公開 IP 位址。
19. (C)承上題，除了 4 台上網的電腦之外，如果小明辦公室還需要架設一個網站供外面連線，以下何者正確？ (A)除了 IP 分享器，一定需要再增加其他網路設備，才有辦法達成 (B)小明只有一個公開 IP 位址，沒有辦法架網站 (C)小明只需要設定 IP 分享器的 port forwarding 功能，將網頁傳輸的封包 (目的 port: 80) 轉寄到網站伺服器上即可 (D)網站和 4 台上網的電腦不可能同時連上網路。
20. (C)關於路由器(router)，以下何者有誤？ (A) router 負責轉寄不同網段之間的封包 (B) routing 路徑可以人工指定，也可以動態決定 (C)網路交換器(Switch)通常都具有 router 的功能 (D) traceroute 工具可以顯示封包所經過的 router。
21. (B)Client-server 與 peer-to-peer 架構的差異，下列何者不正確？ (A) peer-to-peer 架構中每台電腦彼此互連，因此擴充性較佳 (B) client-server 架構的每台電腦角色都一樣 (C) peer-to-peer 架構常被應用來傳輸檔案 (D) client-server 架構中 server 負荷通常比較重。
22. (B)有關 TCP 通訊協定，下列何者有誤？ (A) TCP 在正式傳輸資料前，必須先建立連線 (B) client 送出 SYN 之後，server 回覆 SYN-ACK，就完成了三向交握 (C) TCP 之所以可靠，主要是依賴三向交握(Three Way Handshake) (D)如果 client 沒有正確結束連線，server 需要耗費較多資源等待 client 回應。
23. (A)下列何者屬於無線展頻技術？ (A) FHSS (B) CDMA (C) TDMA (D) OFDM。
24. (A)ATM Cell 的長度為？ (A) 53Bytes (B) 46Bytes (C) 64Bytes (D) 46 ~ 1500Bytes。
25. (C)設計展頻碼時必須滿足以下哪一點？ (A)自己內積為 0 (B)不同展頻碼內積為 1 (C)不同展頻碼內積為 0 (D)自己內積為 1。
26. (C)下列何者**不是**對稱式加密演算法？ (A) DES (B) AES (C) RSA (D) 3DES。
27. (B)下列何者是 stream cpher？ (A) Diffie-Hellman (B) RC4 (C) AES (D) SHA1。
28. (D)下列何者**不是**企業資訊安全管理考量的重點？ (A)加密儲存業務相關內容以免外洩 (B)防止外部駭客入侵 (C)注意重要資料備份 (D)控制員工上網時間。
29. (C)有關公司內部檔案安全管理，下列何者何者正確？ (1)郵件軟體都需要帳號登入，員工收發 e-mail 內容不會有別人看到 (2)每台電腦登入都需要密碼，所以檔案下載後直接放在桌面，不可能被竊取 (3)大部分公司電腦皆有網路連線，因此需注意是否有不明軟體自動下載執行，以免公司資料外洩 (4)若企業內部已經設置防火牆，每台電腦就不需再安裝防毒軟體，以免影響電腦速度。
30. (B)以下何者**不是** OLTP 注重的項目？ (A)交易速度 (B)與 OLAP 需求相同 (C)少量資料 (D)有計算需求。
31. (A)下列何者**不是**資訊安全管理的標準？ (A) ISO 9001 (B) ISO 27002 (C) BS 7799 (D) CNS 27001。
32. (C)在災害復原方案中，下列哪個方案是最後才要執行？ (A)緊急方案 (B)復原方案 (C)測試方案 (D)備份方案。
33. (B)有關 Secure Hash Function 的安全性，下列何者有誤？ (A) SHA-1, SHA-2 的差異在於 hash value 的大小 (B) hash value 的大小不會影響安全性 (C) SHA-3 的結構與 SHA-1, SHA-2 非常不同 (D) SHA-1 理論上是可能被破解的。
34. (D)有關無線網路安全相關的通訊協定，下列何者有誤？ (A)無線網路的存取控制通常是經由 IEEE 802.1x 進行 (B) 802.11i 是目前無線網路安全的標準 (C)無線網路上可能會有身分被竊取的風險 (D)中間人攻擊(man-in-the-middle attack)不會發生在無線網路。

35. (B)一個密碼系統(對稱及非對稱)的安全性主要取決於下列何項條件？ (A)加解密演算法不可公開 (B)私密金鑰不可公開 (C)明文格式必須隱藏 (D)密文無法取得。
36. (C)有關資訊安全的概念，下列何者有誤？ (A) public-key cryptography 使用成對的 public key 以及 private key (B)加密演算法的安全主要取決於 key size (C) public-key cryptography 比對稱式加密要安全 (D)對稱式加密與 public-key cryptography 用途不完全相同，都有存在的必要。
37. (B)有關雲端安全，下列何者有誤？ (A)雲端儲存空間仍然有可能有資料外洩的風險 (B)雲端硬碟需要帳號密碼才能登入，資料內容不會被竊取 (C)將資料上傳至雲端空間時，網路傳輸過程也可能有資料外洩風險 (D)雲端硬碟業者雖然會幫忙備份資料，但是仍有可能發生資料遺失。
38. (D)有關無線網路安全，下列何者有誤？ (A)行動裝置必須先透過 access point 取得網路使用權 (B) 如果發現可疑的行動裝置，access point 可以負責拒絕其無線網路的存取 (C)無線網路通常潛在的安全威脅比有線網路要大 (D)多台 access point 彼此間獨立運作。
39. (C)委外屬於風險管理的哪種方式？ (A)風險承擔 (B)風險逃避 (C)風險轉移 (D)風險移除。
40. (A)下列何者為 IPSec 協定中用來管理金鑰交換程序()之協定？ (A) IKE (B) AH (C) PAP (D) ESP。
41. (B)PKI 的構成元件不包括？ (A)憑證機構 (B)網路管理 (C)憑證廢止清冊 (D)安全政策。
42. (A)下列何者**不是**特洛伊木馬程式的特徵？ (A)需要使用者的允許才能控制電腦 (B)程式體積小 (C)執行時不會佔用太多系統資源 (D)執行後可能自動複製到其他資料夾中。
43. (A)封包路由的原理是下列何者？ (A)跳到下一站的路由 (B)建立連線的路由 (C)找到目的地的路由 (D)依據來源端指定路徑的路由。
44. (C)有關 Alice 與 Bob 通訊過程的 authentication，下列何者有誤？ (A) Alice 以其 private key 加密，Bob 可以用 Alice 的 public key 解開，驗證寄件人身分 (B) Alice 以 Bob 的 public key 加密，只有 Bob 能以其 private key 解開，可確認只有收件人收得到 (C) Alice 與 Bob 如果要互相交換 public key， 必須透過公正的第三方 (D) Alice 與 Bob 可以透過公正的第三方，進行身分驗證。
45. (B)關於資訊安全所使用 hash function 的特性，下列何者有誤？ (A) hash function 可以將不定長度的訊息輸入，算出固定長度的輸出 (B)不同的資料不會 hash 到同一個值 (C) hash function 的計算通常要相對的快 (D)從 hash value 要回推其對應輸入，通常要很難計算。
46. (C)有關數位簽章 (digital signature)，下列何者有誤？ (A)數位簽章是由寄件者簽名，收件者驗證其簽名 (B)寄件者和收件者都必須事先各自產生一對金鑰 (C)經過數位簽章之後，我們能夠確保訊息內容不會被第三方知道 (D)數位簽章的目的通常在於驗證寄件者的身分，也就是說，可以避免冒名寄信。
47. (B)非對稱式加解密系統所產生的兩把 key 稱為？ (A) first & second (B) public & private (C) single & double (D) secret & nonsecret。
48. (D)一般而言，用發送者私鑰(privatekey)加密是為了什麼目的？ (A)加速傳輸 (B)保密 (C)自動回應 (D)確認身分。
49. (D)訊息鑑別碼(Massage Authentication Code, MAC) 主要的用途為何？ (A)加密 (B)解密 (C)防止訊息遺失 (D)身分驗證。
50. (D)下列何者**不是**資訊安全的目標？ (A) Integrity (B) Confidentiality (C) Authentication (D) Stability。

本試卷試題結束