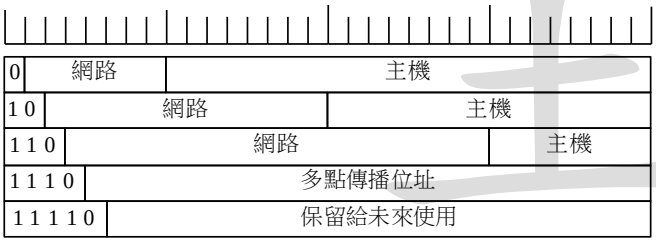
110 年公務人員特種考試關務人員、身心障礙人員考試及 110 年國軍上校以上軍官轉任公務人員考試試題

考 試 別：關務人員考試
等　　別：三等考試
類　　科：資訊處理
科　　目：資通網路
考試時間：2 小時
※注意：㈠禁止使用電子計算器。
㈡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。
㈢本科目得以本國文字或英文作答。

一、目前所使用的 32 位元的 IPv4 源於 80 年代早期，其 IP 位址範圍介於 0.0.0.0 到 255.255.255.255 之間。已知 IPv4 Class A 的「IP 位址分布範圍」是 0.0.0.0~127.0.0.0。請問：
㈠ IPv4 位址共分幾等級？（3 分）
㈡ IPv4 Class A 的「可用網路組」與「每一組可連結主機數目」各是多少？（8 分）
㈢ IPv4 Class B 的「IP 位址分布範圍」、「可用網路組」與「每一組可連結主機數目」各是多少？（12 分）
㈣ IPv4 Class C 的「IP 位址分布範圍」、「可用網路組」與「每一組可連結主機數目」各是多少？（12 分）

【擬答】：

㈠ IP 地址可分成 A、B、C、D、E 等五個等級，如下圖所示，其中 D 類為多點傳播位址，E 類則保留供搜尋、Internet 的實驗和開發用，實際主要分配的是 A、B、C 三類。



A 1.0.0.0~127.255.255.255
B 128.0.0.0~191.255.255.255
C 192.0.0.0~223.255.255.255
D 224.0.0.0~239.255.255.255
E 240.0.0.0~247.255.255.255

㈡ Class A 的「可用網路組」為 1-127，但其中 10 供私有 IP、127 供迴路測試用，實際可用為 125 組；「每一組可連結主機數目」為 2^24-2(扣除本機、廣播位址)。
㈢ Class B 的「IP 位址分布範圍」為 128.0.0.1~191.255.255.254；「可用網路組」有 2^14 個；「每一組可連結主機數目」為 2^16-2。
㈣ Class C 的「IP 位址分布範圍」為 192.0.0.1~223.255.255.254；「可用網路組」有 2^21 個；「每一組可連結主機數目」為 2^8-2=254 個。

二、請解釋與說明下列各問題：

㈠何謂殭屍網路（Botnet）？（6 分）

㈡常見的殭屍網路攻擊有那些？請舉出兩個例子。（7 分）

㈢如何防止殭屍網路的攻擊？請舉出兩個作為。（7 分）

【擬答】：

㈠殭屍網路（Botnet）是指駭客利用自己編寫的分散式阻斷服務攻擊程式將數萬個淪陷的機器，即駭客常說的傀儡機或「肉雞」（肉機），組織成一個個命令與控制節點，用來傳送偽造包或者是垃圾封包，使預定攻擊目標癱瘓並阻斷服務。

㈡ 1. 由殭屍網路所發起的分散式阻斷服務（Distributed Denial of Service，DDoS）即是主控者透過控制殭屍向目標的網路設備傳輸大量合法或偽造的請求以占用資源，從而導致受害方無法負荷造成無法提供正常的網路服務。

2. 此外也可以用來傳送垃圾郵件、竊取資料、甚至進行挖礦。

㈢ 1. 建立安全密碼：

創建安全密碼可增加暴力破解的難度，創建了高度安全的密碼，則暴力破解幾乎不再可能。

2. 定期系統抹除/還原：

自設定時間後還原為已知良好狀態，將移除系統收集的任何垃圾（包括殭屍網路）。此策略在作為預防措施使用時，即便在默默執行惡意程式碼，也可確保與垃圾一同移除。

3. 執行良好的連入和連出篩選操作：

在網路路由器和防火牆執行篩選操作，對可公開存取的資源具有最低限制，同時對您視為機密的資訊不斷加強安全性。此外，對跨越邊界的任何內容進行仔細檢查。採用高品質節選的做法後，更有可能在 DDoS 惡意軟體及其傳播方法和通訊進入或離開網路前將其攔截。

三、請回答下列問題：

㈠何謂 DoS 攻擊？（5 分）

㈡何謂 DDoS 攻擊？（5 分）

㈢ 3 如何防止外來的 DDoS 攻擊？請舉兩個作為進行說明。（10 分）

【擬答】：

㈠阻斷服務攻擊（denial-of-service attack，DoS 攻擊）是一種網路攻擊手法，其目的在於使目標電腦的網路或系統資源耗盡，使服務暫時中斷或停止，導致其正常使用者無法存取。

㈡當駭客使用網路上兩個或以上被攻陷的電腦作為「殭屍」向特定的目標發動「阻斷服務」式攻擊時，稱為分散式阻斷服務攻擊（distributed denial-of-service attack，簡稱 DDoS 攻擊）。

㈢ *1.* 防火牆

防火牆可以設定規則，例如允許或拒絕特定通訊協定，埠或 IP 位址。當攻擊從少數不正常的 IP 位址發出時，可以簡單的使用拒絕規則阻止一切從攻擊源 IP 發出的通信。防火牆能有效地防止使用者從啟動防火牆後的電腦發起攻擊。

2. 交換機

大多數交換機有一定的速度限制和存取控制能力。有些交換機提供自動速度限制、流量整形、後期連接、深度包檢測和假 IP 過濾功能，可以檢測並過濾阻斷服務攻擊。例如 SYN 洪水攻擊可以通過後期連接加以預防。基於內容的攻擊可以利用深度包檢測阻止。

3. 黑洞啟動

黑洞啟動指將所有受攻擊電腦的通信全部傳送至一個「黑洞」（空介面或不存在的電腦位址）或者有足夠能力處理洪流的網路裝置商，以避免網路受到較大影響。

4. 流量清洗

當流量被送到 DDoS 防護清洗中心時，通過採用抗 DDoS 軟體處理，將正常流量和惡意流量區分開。正常的流量則回注回客戶網站。這樣一來可站點能夠保持正常的運作，處理真實使用者存取網站帶來的合法流量。

四、TCP 採用滑動窗口（sliding window, SW）來執行網路流量控制，並啟用 Go Back N 機制，設定 Timeout 為 20ms。已知一個封包在 end-to-end 網路中的 round-trip-time（RTT）為 10ms。今不計 packet arrival time 與 packetprocessing time。請計算下列問題：

㈠假設網路非常穩定不遺失封包，且 SW=1，請問從傳送端將 100 個 TCP 封包完整地送到接收端，需花多久時間？（5 分）

㈡假設網路非常穩定不遺失封包，且 SW =20，請問從傳送端將 100 個 TCP 封包完整地送到接收端，需花多久時間？（8 分）

㈢假設網路不穩定，且每兩個封包就會遺失一個封包。然後傳送端經過重傳該遺失封包一次後，才被接收端成功地接收。請問，如果 SW=10，從傳送端將 100 個 TCP 封包完整地送到接收端，平均需花多久時間？（12 分）

【擬答】：

㈠在網路非常穩定不遺失封包，且 SW=1，從傳送端將 100 個 TCP 封包完整地送到接收端，需花 100*10ms=1000ms=1sec。

㈡本題未給 transmission delay(但必小於 10ms)，無法判定是否可以持續無間斷傳送，若每個封包的 transmission delay 為 0.5ms，本小題可以無間斷傳送，本題的傳送時間為 100*0.5+19.5=69.5ms。

㈢因為 Go Back N 機制有錯就要回到錯誤處全部重傳，且需要 20ms 才知道封包遺失，接著依照題意傳送端經過重傳該遺失封包一次後，才被接收端成功地接收，因此需要 30ms 才能確定完成傳送；因此平均 30ms 才能確定完成兩個封包的傳送，共需 100/2*30=1500ms 才能將 100 個 TCP 封包完整地送到接收端。