104 年公務人員高等考試三級考試試題

類 科：資訊處理
科 目：資通網路

一、一個橋接網路（bridged network）通常使用許多橋接器（bridges）將多個區域網路互相連結起來。而且為了提高網路可靠度，橋接器之間的鏈結（links）可能會形成許多迴路（loops）。橋接器中通常都會實作 IEEE 802.1D spanning tree algorithm 擴張樹演算法。
說明：
㈠橋接網路有迴路會造成什麼問題？
㈡擴張樹的目的為何？
㈢一個橋接網路找出其擴張樹的程序為何？

【擬答】：
㈠橋接網路中若有迴路除了可能造成訊框重覆接收之外，也會對橋接器之工作站學習過程造成困擾。
㈡如果我們將每一個區域網路和每一個橋接器看成一個點，每一個橋接器埠看成一個邊，則一個橋接網路便可以一個相對的圖形來表示。求此圖形的擴張樹便是找出圖形中的 n-1 條邊將所有 n 個點連接起來而且沒有迴路，而沒有迴路的橋接網路便可以看成是這個圖形的一個擴張樹。擴張樹(spanning tree)架構可將所有的區域網路連結起來而沒有造成迴路。
㈢IEEE 802.1D 標準所制定的擴張樹演算法，可讓每一個橋接器或區域網路到根點橋接器的最少成本路徑都在此擴張樹上，此一演算法主要包含三個步驟：
*1.*找出根點橋接器(Root Bridge)
⑴開始時，每一個橋接器因為不知道其他橋接器的情形，以為自己是根點橋接器並且將「橋接器通訊協定資料單元」(Bridge Protocol Data Unit，BPDU)傳進所有直接相連的區域網路中。其中 BPDU 中的「根點橋接器辨識碼」欄位填入自己的辨識碼，「根路徑成本」欄位填入 0，「橋接器辨識碼」欄位也填入自己的辨識碼，「埠辨識碼」欄位則填入傳送出該 BPDU 埠辨識碼。
⑵當一個橋接器由其埠 i 收到一筆 BPDU 時便比較 BPDU 上的根點辨識碼是否大於本身認定的根點辨識碼(開始時認定自己的辨識碼是根點辨識碼)。如果是，則表示此 BPDU 的優先權較低並且將其丟棄。否則，自己放棄當根點橋接器並且將認定的根點辨識碼暫時設定為 BPDU 上的根點辨識碼。且將此 BPDU 轉送到所有的埠上(埠 i 除外)。在此一過程當中，只有真正的根點辨識碼不會收到比自己更小的，且其 BPDU 會在一個「轉送延遲時間」之內征服其他橋接器。因此只要在二個轉送延遲時間內不收到比自己更小的根點辨識碼就可以確認自己是根點橋接器。根點橋接器每隔一段「問候時間」就要將其 BPDU 傳送進所有直接相連接的區域網路以問候其他橋接器。
*2.*找出橋接器根埠(Root Port)
⑴橋接器一旦確認自己不是根點橋接器後便立刻尋找自己的根埠。假設該 BPDU 是由埠 i 收到，則先暫時設定埠 i 為其根埠。並且將本身的根路徑成本設定為 BPDU 上根路徑成本與埠 i 的傳輸成本的和。表示由埠 i 到根點橋接器的路徑成本。當此 BPDU 由埠 j 轉送出去時，其上的根路徑成本欄位的值必須換成為橋接器的根路徑成本。這是通知所有與埠 j 相連網路上的橋接器，經由埠 j 到根點橋接器的成本(埠 j 的傳輸成本不計算，因為在此路徑上，其為接收埠)。
⑵在二個轉送延遲時間之內如果沒有收到更好的 BPDU（如較小的根點橋接器，或相同的根點辨識碼但有較小的根路徑成本)，則可設定埠 i 為根埠。否則重覆以上的步驟。
*3.*找出區域網路的代理埠
代理埠由所有和其相連的橋接器共同來尋找，當一個橋接器 X 在確定其某一個埠(如埠 i)為根埠後，便開始想知道其他的埠是否能分別成為與其連接區域網路的代理埠。橋接器於是將其根路徑成本 RPC(X)當成是與埠 j 相連接區域網路的根路徑成本，並且將之傳進區域網路中。當其他與此區域網路相連接的橋接器 Y 收到此訊框後(假設由埠 k 收到)便

檢查該值是否小於其根路徑成本 RPC(Y)。如果 RPC(X)＜RPC(Y)則表示傳送該訊息的橋接器 X 更合適成為此區域網路的代理橋接器，於是放棄競爭。如果 RPC(X)＞RPC(Y)則表示自己更適合，於是將自己的根路徑成本 RPC(Y)經由埠 k 送進區域網路中以通知該橋接器使其放棄。如果 RPC(X)＝RPC(Y)則以橋接器的辨識碼來決定。辨識碼小的橋接器有較高的優先權。這個競爭的過程可能一直持續進行，直到區域網路真正的代理橋接器將最少的根路徑成本送進區域網路為止。此時其他所有連接的橋接器都會被迫放棄競爭，由於每一個橋接器確認其根埠的時間不同，因此以上的過程並不是同步的。一個橋接器可能在自認為是某區域網路的代理橋接器一段時間後才收到更具優先權的訊息。一個原本已經暫定某個埠為根埠的橋接器 Z 也可能在其埠 m 收到更好的根路徑成本(RPC(X)＋TC(m)＜RPC(Z))後，變更其根埠為埠 m。

二、TCP 協定的壅塞控制（congestion control）使用了 AIMD（Additive Increase Multiplicative Decrease）機制。說明：

㈠TCP 連線的傳送端如何偵測網路發生壅塞的情形？

㈡何謂壅塞視窗 Congestion window？

㈢何謂 AIMD 機制？

㈣何謂 Slow Start 機制？

【擬答】：

㈠目前只要有因為遺失分封而造成的逾時，都是因為壅塞而產生，因此所有的 TCP 壅塞偵測演算法都會去偵測是否發生逾時。

㈡ Internet 解決壅塞的方法在傳送端需要兩個窗口，其中一個是接收端已經同意的傳送窗口，另外還要靠壅塞窗口(congestion window)。實際傳送的 byte 數是取兩者的較小者。

㈢當 TCP 發送方感受到端到端路徑無壅塞時就線性的增加其發送速度，當察覺到路徑壅塞時就採乘法減小其發送速度。

㈣連結建立後，傳送端會將壅塞窗口的大小設成 1 個最大區段長度，接著將之送出，如果可以不必逾時就收到回覆，則傳送端會將壅塞窗口大小加倍，直到發生逾時或達到接收端窗口大小，此一方法稱為慢速起動(slow start)。

三、IEEE 802.11 無線區域網路使用的是 CSMA/CA（Carrier Sense Multiple Access with Collision Avoidance）協定來傳送封包。當一台無線主機想要傳送封包時，會先去偵測是否有其他封包正在無線通道上傳送。說明：

㈠如果無線通道上沒有傳送（channel idle），此主機會如何處理？

㈡如果無線通道上已有傳送（channel busy），此主機會如何處理？

㈢CSMA/CA 協定使用了避免衝撞（collision avoidance）的機制。那封包傳送時是否還會發生衝撞？為什麼？

【擬答】：

㈠當無線站台要發送資料時，並不會立即傳送出去，而是先產生一個隨機的延遲時間(IFS，Interval Frame Space)，在延遲時間裡，無線站台若發現頻道忙碌的話，則凍結延遲時間的計算工作，直到確認頻道是空閒的再繼續計算，直到延遲時間一到，再進行下面的工作。以 RTS-CTS-傳資料-ACK 過程達成，送出資料前，先送一段小小的請求傳送封包（Request to Send ,RTS）給接收端，等待接收端回應(Clear to Send ,CTS)封包後，才開始傳送。其他收到 RTS 與 CTS 的節點都要在此時暫停傳送，以解決隱藏節點問題。

㈡若頻道仍然未空閒則進入第二階段的等待，這時會給它一個 Backoff 的等待時間，發送端在這個競爭模式下會自動提高它使用頻道的優先權(Priority)，這個機制可以避免有些發送端一直無法取得頻道的使用權，而無法傳送資料。取得頻道使用權後，以 RTS-CTS-傳資料-ACK 過程達成，送出資料前，先送一段小小的請求傳送封包（Request to Send ,RTS）給接收端，等待接收端回應(Clear to Send ,CTS)封包後，才開始傳送。其他收到 RTS 與 CTS 的節點都要在此時暫停傳送，以解決隱藏節點問題。

㈢唯一會碰撞的只有兩個無線站台 B 與 C 同時向無線站台 A 送出 RTS，以致站台 A 無法判別

送出 CTS，就會造成碰撞，碰撞時會站台 B 與站台 C 會等待隨機後退(Back Off)時間，之後提高優先權再試。

四、網際網路（Internet）所使用的 IP（Internet Protocol）協定是以盡力式（best effort）的方式傳輸封包。也就是說 IP 所提供的服務是不可靠的。說明：

㈠使用 IP 協定在傳送封包可能發生那些事情使得其服務不可靠？

㈡何謂路由協定（routing protocol）？

㈢路由器（router）收到一個封包後，是如何將該封包送往目的地主機（destination host）？

【擬答】：

㈠IP 協定的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。

㈡ 這是網路層軟體的一部份，負責決定輸入的分封應該由那一條輸出路徑傳送出去。

㈢ 每個路由器必須維護一個 routing table，記錄本身到每個目的地的已知最佳距離，與需要經過的線路，在收到封包後，會根據所使用的查找演算法(最常用 longest prefix 演算法)查找，再根據找到的決定輸入的分封應該由那一條輸出路徑傳送出去。

五、TCP SYN flooding 是一種著名的網路阻斷服務攻擊（DoS）。說明：

㈠何謂阻斷服務攻擊（Denial of Service）？

㈡分散式阻斷服務攻擊（Distributed Denial of Service）的模式為何？

㈢SYN flooding 攻擊的運作原理為何？

【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，例如 Ping 到死(Ping of Death)攻擊就是用 Ping 工具程式，來產生超過 IP 協定所能允許的最大封包，由於 ICMP Echo Request/Reply 的封包格式 Option Data 欄位大小不固定，因此在 Option Data 欄位加入大量資料，形成大型的 ICMP 封包，利用大型封包來進行 Ping 到死(Ping of Death)攻擊。

㈡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，也讓目標伺服器難以防堵。

㈢TCP SYN Flood 攻擊就是利用 TCP 協定三向交握的弱點，惡意地送出許多 TCP SYN 封包，但後續沒有回覆確認(ACK)封包。