《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：

(一)橋接網路有迴路會造成什麼問題？（5分）

(二)擴張樹的目的為何？（5分）

(三)一個橋接網路找出其擴張樹的程度為何？（10分）

試題評析	本題出自於SPT協定，測試bridge與switch的迴路相關問題。
考點命中	《高點資通網路講義》第二回，王致強編撰，頁108。

答：

(一)橋接網路有迴路會造成訊框迴路，若迴路過多甚至會造成訊框風暴，訊框成指數增長，而造成網路癱瘓。

(二)找出橋接網路的擴張樹，任兩節點間可以使用唯一路徑來傳遞訊框，藉此可以避免訊框迴路以及訊框風暴問題。

(三)IEEE 802.1D STP(Spanning Tree Protocol)找出Spanning Tree的程序為：

(1)先選出root bridge，由root開始，往鄰接橋接器發送外發送訊框以計算cost。

(2)每個節點找出成本最低的路徑(root path)。

(3)每個節點將其餘成本較高的root paths停用。

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

(一)TCP連線的傳送端如何偵測網路發生雍塞的情形？（5分）

(二)何謂雍塞視窗Congestion window？（5分）

(三)何謂AIMD機制？（10分）

(四)何謂Slow Start機制？（5分）

試題評析	本題出自於TCP壅塞滑動窗口控制的特性相關問題。
考點命中	《高點資通網路講義》第四回，王致強編撰，頁55~57。

答：

(一)壅塞偵測使用ACK傳回的時間，是否在預估計算的RTT內來判斷，若未超過RTT，則沒有壅塞；若超過RTT，則為壅塞。每次RTT也是使用調適性公式，來彈性推估。

(二)壅塞窗口就是每次傳送的大資料量，通常傳送資料量必須不超過壅塞窗口與流量窗口的最小值。

(三)AI：在壅塞避免階段，一整組封包發送成功後(每個封包都在RTT時間內，其ACK被回覆)，壅塞窗口會被加一(門檻值也增加一)。MD：當一個封包發送失敗時(因ACK逾時)，就將Congestion Window/2做為門檻值，Congestion Window也要減少。

(四)Slow Start：

(1)在連線剛建立時，或剛經歷過壅塞狀況之後，會因為 Congestion Window 由 1 開始，因為太小而無法有效地傳輸。

(2)使用 slow start 方法，每次收到整個壅塞窗口區段的 ACK 後，就將壅塞窗口加倍，可以很快地提高加大窗口大小來改善傳輸效率。

(3)當整組封包傳送成功被確認時，效果是窗口相當於被加倍放大。

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：
(一)如果無線通道上沒有傳送（channel idle），此主機會如何處理？（5分）
(二)如果無線通道上已有傳送（channel busy），此主機會如何處理？（10分）
(三)CSMA/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？（10分）

試題評析	本題出自IEEE 802.11 無線區域網路的CSMA/CA協定問題。
考點命中	《高點資通網路講義》第五回，王致強編撰，頁1~5。

答：
(一)通道上沒有傳送時，傳送端會送一個要求傳送的控制框(RTS, request to send)，說明傳送的資料框長度，接收端回應(CTS, clear to send)後才開始傳送。
(二)通道上有傳送時，其他工作站可以根據先前RTS表明的資料長度，算出傳輸所需時間，在資料傳輸其間，稱為NAV(Network Allocation Vector)，其他工作站停止傳輸。等NAV時間過後，再發送出RTS。
(三)可能會碰撞的狀況是兩個節點，同時送出的RTS而產生碰撞，此時可以用二進位指數倒退演算法(Binary Exponential Backoff algorithm)，隨機等候一段時間的方式來解決。

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：
(一)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？（5分）
(二)何謂路由協定（routing protocol）？（5分）
(三)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）？（5分）

試題評析	本題為路由基本問題，具備正確觀念，應可拿到不錯的分數。
考點命中	《高點資通網路講義》第三回，王致強編撰，頁12~20。

答：
(一)IP是不可靠傳輸，可由下面幾點看出：
(1)整個封包沒有錯誤檢查(只有標頭有 checksum)。
(2)IP 沒有使用 ACK 來回覆來源端。
(3)TTL 可能造成封包被丟棄。
(二)routing protocol：是在路由器上，根據蒐集到的網路拓樸與連線資訊，計算出到每一個目的地的最佳路徑，並記錄到routing table。在封包由介面進來時，可查詢routing table，以便將封包可以switch到正確的介面，往目的地方向轉送出去。
(三)路由器收到封包之後，查詢其routing table，找出下一站(next hop)，將封包傳送至下一站；而下一站收到封包之後，也會查詢其routing table，繼續往下一站傳遞，直到封包到達目的地為止。

五、TCP SYN flooding是一種著名的網路阻斷服務攻擊（DoS）。說明：
(一)何謂阻斷服務攻擊（Denial of Service）？（5分）
(二)分散式阻斷服務攻擊（Distributed Denial of Service）的模式為何？（5分）
(三)SYN flooding攻擊的運作原理為何？（5分）

試題評析	本題為DoS觀念問題，大部份網路教材，應該都有說明，考生可拿到不錯的分數。
考點命中	《高點資通網路講義》第四回，王致強編撰，頁37。

答：
(一)攻擊者對伺服器的性能進行攻擊，或對相關網路進行攻擊，造成網路癱瘓或伺服器無法提供正常服務，需要伺服器的用戶端，無法得到正常的服務。

(二)聯合多個攻擊者，或藉由病毒感染多個電腦，在同一時間從不同的來源位址，對同一部伺服器發起攻擊，因為來源不同而使得伺服器無法防範的現象，稱為 DDoS。

(三)SYN阻斷服務攻擊(SYN Denial-of-Service, DoS)：又稱為TCP flooding attack。攻擊者假造大量不同來源IP，發送SYN偽造連線要求，其間會佔用TCP Socket Table等空間，癱瘓server的運作，使得需要服務的使用者，反而無法建立TCP連線。