《電腦網路》

一、(一)在 Stop-and-Wait 的協定中，舉例說明，在怎樣的情況下，接收者（receiver）會收到重複的封包（duplicate packet），請舉出兩種情況說明。(10 分)

(二)考慮一個半雙工(half-duplex)點對點鏈結(point-to-point link)，使用了 stop-and-wait 協定來傳送一系列的訊息。每個訊息被分割（segmented）成數個訊框（frames）來傳送。請問分割的訊框的大小，如何影響此 stop-and-wait 的效能，簡單分析之。(10 分)

試題評析	第一小題為 Stop-and-Wait 的基本觀念，第二小題為基本分析，難度適中。
考點命中	《高點資通網路講義》第二回，石濟編撰，頁 39 以下。

【擬答】

(一)停止並等待協定在傳送端送出一個訊框後必須保留剛才的內容，直到收到接收端送出的確認訊框為止，在等待過程中，傳送端不會發送新的訊框，接收端收到錯誤的訊框時，將回傳一個負面確認訊框，傳送端收到後將重新傳送，此外，傳送端亦會使用計時器，處理訊框遺失。發生以下事件時接收端可能收到相同內容：

1.若接收端回傳的確認訊框遺失時，發送端發生逾時事件後將重傳相同訊框，使接收端收到相同內容。

2.若接收端回傳的確認訊框因網路狀況不佳造成延遲，而延遲時間超過等待的最大時間，發生逾時事件時，將重傳相同訊框，使接收端收到相同內容。

(二)在半雙工點對點鏈結中，stop-and-wait 必須等到確認接收端收到並回復確認訊息後才發送下一個訊息，若是一訊息再被切割成 N 個訊框，則必須多 N 次確認才可收到一個完整的訊息，使傳輸效率進一步下降。

二、(一)IPv4 的位址，為何需要無分類編址（classless addressing），有何好處？（8 分）

(二)一個網路服務提供者（ISP：Internet Service Provider），被授有 IP 區塊（block）80.70.56.0/21。這個 ISP 需要將它的 IP 區塊，分配給兩間各需要 500 個 IP 位址的公司，和兩間各需要 250 個位址的公司，以及三間各需要 50 個位址的公司。

請問該怎麼分配這些 IP 給這七間公司較合適？請列出你分配給各間公司的 IP 區塊範圍(需要用無分類編址列出)，以及剩餘的未分配的 IP 區塊範圍。(12 分)

試題評析	本題為 IP 的基本觀念與計算，同學應可順利回答。
考點命中	《高點資通網路講義》第二回，石濟編撰，頁 67 以下。

【擬答】

(一)在等級式分類的網路中，由於高等級網路數量有限，租金較昂貴，且空間甚大，可能無法充分利用，因此衍伸出與切割子網路與合併子網路的方式，切割子網路是將高等的網路切成多個較小的子網路，而合併子網路則是將多個較低等級的網路合併為一個規模較大的網路。

(二)

$(80.70.56.0)_{10}$ = $(01010000.01000110.00111000.00000000)_2$

$(255.255.248.0)_{10}$ = $(11111111.11111111.11111000.00000000)_2$

依題意需 500 空間 2 區、250 空間 2 區以及 50 空間 3 區，故：

500 空間代表需要 9 個位元產生 512 個位址，因此切割為：

80.70.56.0/23~80.70.57.255/23 => 共 508 個可用位址

80.70.58.0/23~80.70.59.255/23 => 共 508 個可用位址

250 空間代表需要 8 個位元產生 256 個位址，因此切割為：

80.70.60.0/24~80.70.60.255/24 => 共 253 個可用位址

80.70.61.0/24~80.70.61.255/24 => 共 253 個可用位址

50 空間代表需要 6 個位元產生 64 個位址，因此切割為：

80.70.62.0/26~80.70.62.63/26 => 共 62 個可用位址

80.70.62.64/26~80.70.62.127/26 => 共 62 個可用位址

80.70.62.128/26~80.70.62.191/26 => 共 62 個可用位址

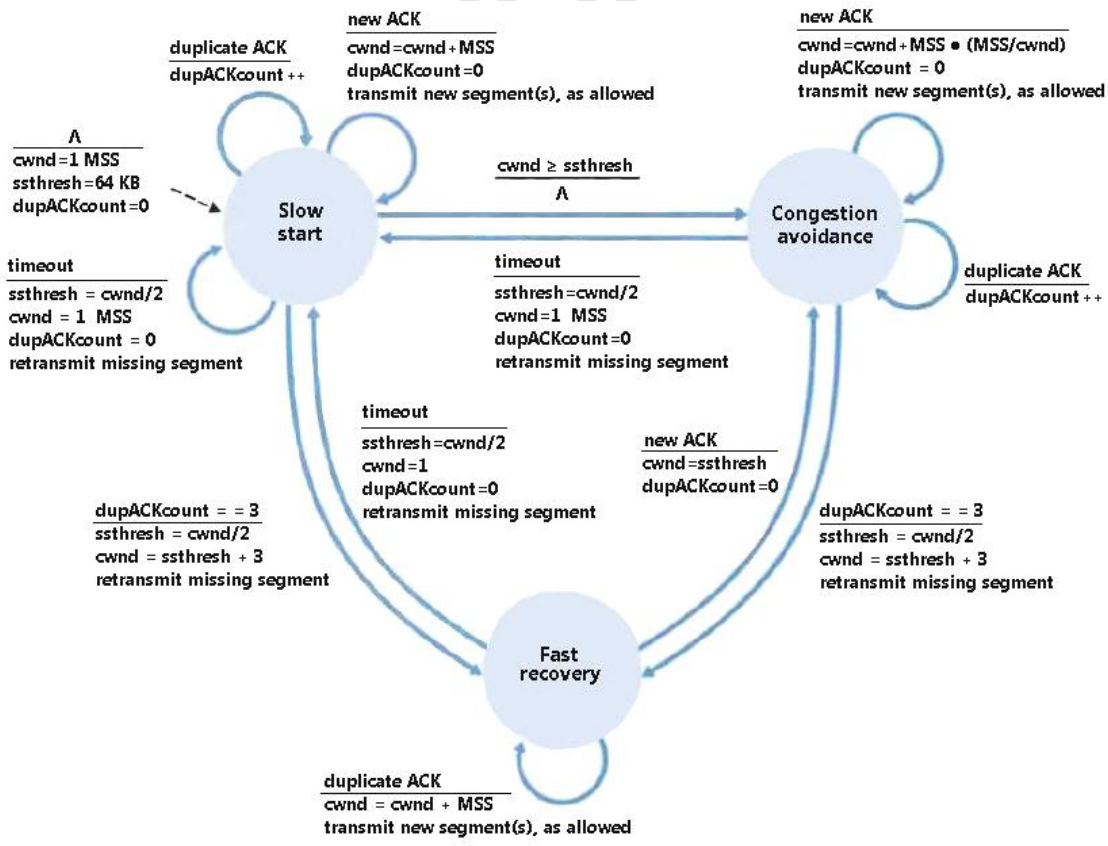
自 80.70.62.192 起皆未分配。

三、請針對 TCP 的壅塞控制，分別在緩慢啟動（SS：slow start）、壅塞避免（CA：congestion avoidance）及快速復原（FR：fast recovery）機制，是如何更動它的 cwnd（壅塞視窗：congestion window）、ssthresh（緩慢啟動臨界值：slow start threshold）。（20 分）

試題評析	本題為 TCP 壅塞控制基本觀念，同學應可順利應答。
考點命中	《高點資通網路講義》第三回，石濟編撰，頁 12 以下。

【擬答】

各階段機制如下圖所示：



四、(一)使用循環冗餘校驗（CRC：Cyclic redundancy check），資料字（dataword）101001111，除數（divisor）為 10111，請計算此 CRC 的碼字（codeword）為何？（10 分）

(二)假設我們用區塊編碼來加密(block cipher)，使用的加密矩陣為：$M=\begin{bmatrix}3 & 2\\ 7 & 5\end{bmatrix}$，而且使用 modulo 26（除以 26 後取餘數）的數學運算。

1.請驗證 M 的反矩陣 $M'=\begin{bmatrix}5 & 24\\ 19 & 3\end{bmatrix}$。（5 分）

2.以數字 0～25 分別代表字母 A～Z，則若收到的密文是 CKHC，則解開的明文的四個字母為何？（5 分）

試題評析	本題中第一小題為簡單的 CRC，第二小題為加密機制，熟悉資安的同學可拿高分。
考點命中	《高點資通網路講義》第一回，石濟編撰，頁 15 以下。

【擬答】

(一)1010011111<u>0101</u>

(二)題目所稱的區塊加密法實為密碼學中之希爾密碼 (Hill Ciphers) ，透過矩陣運算進行加解密，加解密金鑰即為題目所稱之加密矩陣。

1.驗證題目所示之矩陣是否為金鑰之反矩陣，若二矩陣相乘其結果為單位矩陣，則二者互為反矩陣：

$$\begin{bmatrix}3&2\\7&5\end{bmatrix}\begin{bmatrix}5&24\\19&3\end{bmatrix}\bmod 26=\begin{bmatrix}58&78\\130&183\end{bmatrix}\bmod 26=\begin{bmatrix}1&0\\0&1\end{bmatrix}$$ 故二矩陣互為反矩陣。

2.解密方式為：將密文和加密金鑰的反矩陣相乘，mod 26 後再對應至英文字母，每次解密運算時由於金鑰為 2x2 方陣，故只可每次解密二個字母：

CK HC = 3 11 8 3，每次對二個數字進行運算，如下：

$$\begin{bmatrix}5&24\\19&3\end{bmatrix}\begin{bmatrix}3\\11\end{bmatrix}\bmod 26=\begin{bmatrix}279\\90\end{bmatrix}\bmod 26=\begin{bmatrix}19\\12\end{bmatrix}$$ => SL

$$\begin{bmatrix}5&24\\19&3\end{bmatrix}\begin{bmatrix}8\\3\end{bmatrix}\bmod 26=\begin{bmatrix}112\\161\end{bmatrix}\bmod 26=\begin{bmatrix}8\\5\end{bmatrix}$$ => HE

五、(一)虛擬線路（virtual circuit）網路與線路交換（circuit-switched）網路，有何相同和不同之處？至少各舉兩個。(10 分)

(二)考慮下面虛擬線路網路的一個交換器（switch)，其交換表格如下：

進來的（Incoming）		出去的（Outgoing）	
埠（Port）	虛擬線路辨識碼（VCI）	埠（Port）	虛擬線路辨識碼（VCI）
1	14	3	22
2	71	4	41
2	92	1	45
3	58	2	43
3	78	2	70
4	56	3	11

1.從第 3 埠進來的封包，其虛擬線路辨識碼（VCI：virtual circuit identifier）為 78，會從那個埠出去？其帶有的虛擬線路辨識碼會變成多少？（5 分）

2.從第 2 埠進來的封包，其進來的虛擬線路辨識碼為 92，會從那個埠出去？其帶有的虛擬線路辨識碼會變成多少？（5 分）

試題評析	本題為虛擬線路和電路交換之基本比較，同學應可輕鬆拿分。
考點命中	《高點資通網路講義》第二回，石濟編撰，頁 14 以下。

【擬答】

(一)虛擬線路和電路交換網路類似，傳輸前必須先建立一條通道，但和電路交換的差異在於，建立通道時只會佔用路徑頻寬的一部分，剩餘頻寬仍可供其他使用者利用，並不像電路交換完全獨佔通道。二者比較如下：

比較項目	電路交換	虛擬線路
不同次傳輸路徑是否相同	是	可由網管人員調整
轉送依據	實體線路	虛擬線路辨識碼
是否潛在浪費頻寬	是	否
每個封包走相同路徑	是	是

(二)1.由 2 出去，編號變為 70

2.由 1 出去，編號變為 45