《資料通訊》

試題評析

今年的考試題型與往年的題型類似，不同的地方是問題比較深入，針對各個主題必須要深入了解後，才能取得高分，例如第二、四、五題。其他的問題就比較一般化，只要平常應注意的概念夠清楚，就能取分。另外可以發現，有關TCP/IP的問題與子網路遮罩的概念幾乎是年年都會出的考題，考生應可拿到基本分數。對於實體層的概念也要注意，在配分上也是常見的題型。整體來說，只要小心應答，要拿60分並不難。

一、人類的資音頻帶大約在300Hz到3400Hz之間，所以以往電信網路中，一個音訊（voice signal）的頻道（channel）都以4 kHz來切割。在通訊理論上兩個重要的理論分別是Nyquist及Shannon的理論。Nyquist Bandwidth的公式為C=2B $\log_2$ M；Shannon Capacity的公式為C=B $\log_2(1+SNR)$。假設有一電信音訊頻道的SNR_{dB}是24dB，那麼根據這兩個理論，此頻道傳輸速率的上限為多少bits per second(C)？要達到此速率，每一signal要能切分成多少signaling levels(M)？目前我們使用的ADSL也是透過電話線來傳輸，其最高速率目前可達8 Mbps，請問，從Shannon的理論來看，為什麼ADSL可以傳送的速率比以往的電信網路的一個音訊頻道來的高？根據Shannon的理論，在SNR_{dB}為24dB的channel上要達到8 Mbps所需的頻帶（spectrum）要多大？（$10^{2.4}=251$）（15分）

答：

(一) $24\text{dB}=10*\log\frac{S}{N}\Rightarrow 2.4\text{dB}=\log\frac{S}{N}\Rightarrow\frac{S}{N}=251$

根據Shannon’s Law，C = B*$\log_2$(1+SNR) = 4 kHz * $\log_2$(1+251) = 4 kHz * $\log_2$(252) ≒ 4kHz * 8= 32 kHz

(二)C = B*$\log_2$(1+SNR) = 2*B* $\log_2$M

4kHz *$\log_2$(1+24) = 2*4kHz * $\log_2$M

$\log_2$(25) = 2*$\log_2$M

=> M = 5

(三)根據Shannon’s law，當SNR(Signal-Noise Ratio)越大，則可傳送速率越大，ADSL的雜訊小，SNR相對就高，因此，可傳送的最高速率也就越大。

(四)8Mbps = B* $\log_2$(1+24)

8Mbps = B* $\log_2$(25)

8Mbps = B* 4.6438

=> B = 1.7227 Mbps

二、Cyclic Redundancy Check（CRC）是一個常用的錯誤偵測碼。如果使用k-bit的CRC來對n-bit的訊息M做錯誤偵測的話，我們可以用以下的多項式公式來表示：

$$\frac{X^k\cdot M(X)}{G(X)}=Q(X)+\frac{R(X)}{G(X)}$$

$$T(X)=X^k\cdot M(X)+R(X)$$

其中$G(X)$是所謂的generator，$R(X)$就是CRC碼，而$T(X)$是最後要傳送出去的訊息。但實際應用上一些標準組織，像IEEE，會使用以下修正後的公式運算：

$$\frac{X^k \cdot M(X) + X^n L(X)}{G(X)} = Q(X) + \frac{R(X)}{G(X)}$$

$$T(X) = X^k \cdot M(X) + L(X) + R(X)$$

$$L(X) = \sum_{i=0}^{k-1} X^i$$

請解釋這個修正後的公式的意義（運算過程），它比原來的公式多了那些步驟？是為了解決什麼樣的問題？（15分）

答：

利用修正後的CRC公式，主要爲了能夠處理資料開頭(head)或結尾(tail)有k bits個0時，無法正確運算CRC檢測法的問題。因此，開始運算時就在最前面附加k bits個1(就是$X^n L(X)$，這樣保證資料一定是1開頭)，傳送出去前加上k bits個1(就是L(X))。這種修正法則會使用在軟體實作CRC規則上。修正版CRC運算方法如下：

發送端(Sender)：

$$[x^{32}F(x) + x^k L(x)]/G(x) = Q(x) + R(x)/G(x) \quad (1)$$

$$CRC = L(x) + R(x) \quad (2)$$

$$M(x) = x^{32}F(x) + CRC \quad (3)$$

接收端(Receiver)：

$$[x^{32}M(x) + x^{k+32}L(x)]/G(x) \quad (4)$$

$$x^{32}[M(x) + x^k L(x)]/G(x) \quad (5)$$

$$x^{32}[x^{32}F(x) + L(x) + R(x) + x^k L(x)]/G(x) \quad (6)$$

$$x^{32}[Q(x) + R(x)/G(x) + R(x)/G(x) + L(x)/G(x)] \quad (7)$$

$$x^{32}L(x)/G(x) \quad (8)$$

三、已知某一機器的IP為168.168.168.168，subnet mask是255.255.255.240。請問：

(一)該IP屬於那一class？

(二)subnet address為何？

(三)broadcast address為何？

(四)此subnet下有多少合法IP可使用？

(五)若subnet mask是固定的，與此IP address有相同的networK address的可用subnet有多少個？

(六)當此機器要傳送一個IP封包給168.168.168.123及168.168.168.172時，ARP及routing上會有何不同？

(七)當一個IP封包經過LAN傳給router再傳到WAN時，其IP header有那些欄位一定會改變？有那些可能會改變？ ((一)～(五)每題2分；(六)～(七)每題5分；共20分)

答：

(一)168.168.168.168是168開頭，介於128 ~ 191之間，所以屬於Class B

(二)$(168.168.168.168)_{10}$ = $(10101000\ 10101000\ 10101000\ 10101000)_2$
$(255.255.255.240)_{10}$ = $(11111111\ 11111111\ 11111111\ 11111000)_2$
Subnet address = $(10101000\ 10101000\ 10101000\ 10101000)_2 \oplus (11111111\ 11111111\ 11111111\ 11110000)_2$
= $(10101000\ 10101000\ 10101000\ 10100000)_2$
= $(168.168.168.160)_{10}$

(三)broadcast address = $(10101000\ 10101000\ 10101000\ 10101111)_2$
= $(168.168.168.175)_{10}$

(四)$(168.168.168.160)_{10}$ ~ $(168.168.168.175)_{10}$再扣兩個address(subnet address與broadcast address)，則可用的IP address共有14個

(五)Class B的mask爲255.255.0.0，但subnet mask爲255.255.255.240，因此將host欄位挪用了12bits作爲subnet欄位，因此可以有2^{12} = 4096個 subnet可用

(六)168.168.168.123與168.168.168.168 隸屬不同的區域網路，因此資料會由Router轉送，ARP詢問的對象也會是Router的網路卡位址。
168.168.168.123 與 168.168.168.172 隸屬相同的區域網路，因此資料會由直接傳給接受端(168.168.168.172)，ARP詢問的對象會是接受端(168.168.168.172)的網路卡位址。

(七) IP Packet執行Store and Forward時，IP Header一定會改變的欄位有：TTL。
有可能改變IHL、Check Sum、Options

四、IPv6可以解決IPv4的位址空間不足問題，但要實施IPv6時：
(一)ICMPv6有那些改變？（4分）
(二)DNS需要配合做什麼改變？如何更容易支援re-numbering及multi-homing？（6分）
(三)舉出兩種可以讓我們從IPv4的網路過渡到IPv6網路的策略（IPv4-IPv6 transition mechanisms）。（5分）

答：

(一)ICMPv6有下列的改變：
1.Error Message的擴充，如Type 2的“Packet too Big“
2.Information Message的擴充，如Type 152的“Mobile Prefix Solicitation Message Format“
3.Multicast Listener Discovery(MLD)：取代IPv4 網際群組管理通訊協定(IGMP)的第2版，以管理子網路多點傳播成員身份。
4.Neighbor Discovery (ND)：Neighbor Discovery 取代位址解析通訊協定(ARP)、ICMPv4 Router Discovery以及ICMPv4 Redirect 訊息。

(二)
1.IPv6中對網域名稱系統(DNS)所做的改進，這些改進包括以下新的要素：(a)主機位址(AAAA) 資源記錄(b)反向查詢使用的IP6.INT網域
RFC1886中描述對DNS的支援，提出一種簡單的方法，將主機名稱對應到IPv6位址，並提供反向名稱解析。但是，這個支援並不提供將這些更新傳播到AAAA記錄的簡便方法，這是由於站台重新編號或者在任意位元邊界上指派反向尋找區域(IP6.INT以半位元組爲界)。這些問題可使用一個新的“A6“資源記錄來解決。
2.Re-numbering機制叫做Router Renumbering ("RR")，這個機制允許路由器位址 prefixes 可以被配置，也允許Neighbor Discovery和位址 Autoconfiguration結合在主機上運作時，可以容易地重新配置。這提供了一個方法讓網路管理人員可以利用IPv6路由器更新prefixes並且藉由IPv6路由器廣播出去。
Multi-homing可使用位址處理的機制，如PI(Provider Independent)Addressing、PA(Provider Aggregatable) Addressig或Metro Addressing。

(三)
1.Tunneling：在現有的兩個Ipv4的端點間，建立Ipv6的隧道，使兩個端點使用Dual Stack作業系統的User可以使用Ipv6互通。
2.Translato：透過轉換機制可以讓支援Ipv4的User，可以與支援Ipv6的使用者連線。反之亦然。

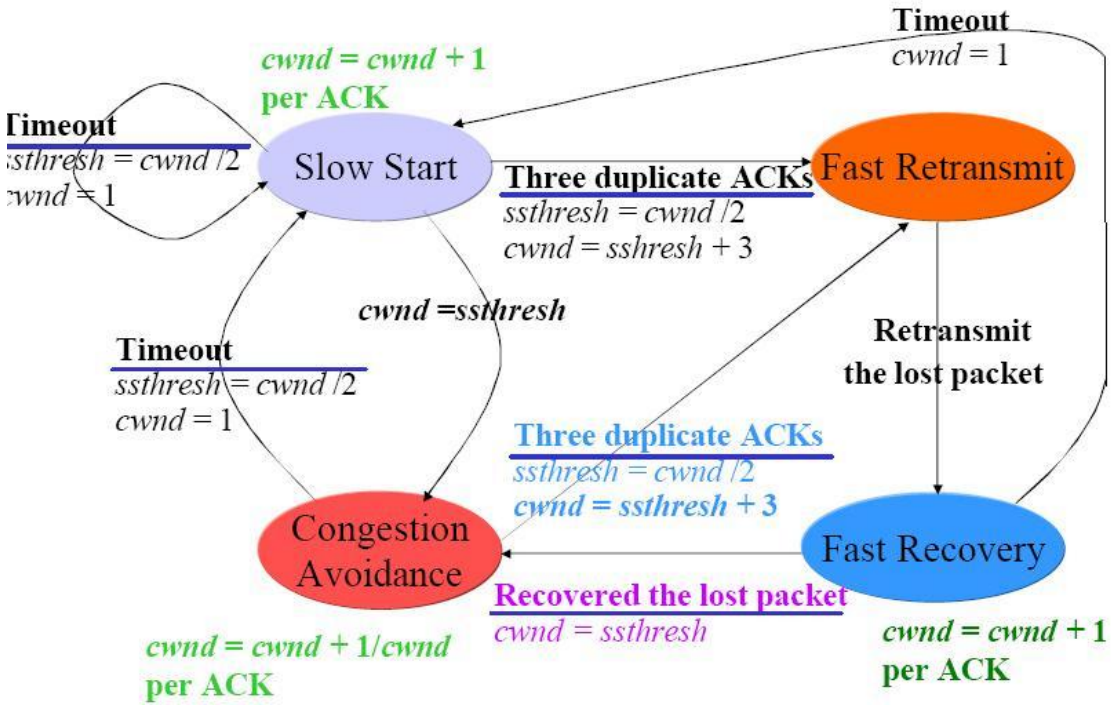
五、以TCP Reno的擁塞控制為例，請問在什麼條件下它會進入congestion avoidance、進入fast re-transmission、離開fast recovery？造成receiver送duplicate ACK的原因是什麼？（12分）

答：

(一)cwnd：congestion window

(二)ssthresh：slow-start threshold

(三)TCP擁塞控制最早於1997年提出，目前網路中最常使用的版本就是TCP Reno。TCP Reno是以window爲基礎的擁塞控制機制，依據RFC 2001，其主要分爲四個狀態：(a)Slow Start (b)Congestion Avoidance (c)Fast Retransmit (d)Fast Recovery



六、甲君家裏是以ADSL連線上網。他裝有IP分享器，上面有4個Ethernet port，1個WAN port。有一天他將一台機器開機後，開啟瀏覽器觀看某一購物網站：

（一）請依時間順序說明何時會用到以下協定：ARP, BGP, CSMA/CD, DNS, DHCP, HTTP, IP, NAT, TCP。（18分）

（二）他決定用信用卡買一商品，此時使用HTTPS跟SET的差別是什麼？何者需要輸入C.V.C. number（信用卡片背面的末三碼）（5分）

答：

(一)開機時先使用DHCP取得IP位址，打開瀏覽器後，打上網址進行連線，先啓動HTTP協定包裝，並進行TCP、IP連線，此時透過DNS服務取得IP位址後，接下來使用CSMA/CD預備將資料傳出，傳出前，使用ARP找出接收端MAC Address。當連線到達ISP時便會使用NAT取得實體IP位址後，在網際網路上繞路便會使用到BGP協定。

(二)

1.兩者同爲安全協定系統，保護及確保消費者資料隱密性和傳輸過程的完整與安全。

(1)SSL利用公開金鑰的加密技術(RSA)來做爲用戶端與主機端在傳送機密資料時的加密通訊協定。而SET是用來保護消費者在開放型網路持卡付款交易安全的標準。

(2)SSL是目前電子商務網站上較常用的一種安全資料傳輸形式，但是它還是有一些問題有待克服，例如：缺乏認證機構、無法確認消費者是否爲持卡本人、店家與收單銀行缺乏標準傳輸介面資料不易整合，信用卡資料是傳給店家，因此資料有可能會被店家非法使用。SET需向銀行申請網路信用卡及取得憑證的動作與時間。

2.使用SSL時，需輸入CVC Number配合Payment Gateway的驗證。