《資料通訊》

試題評析

今年的試題較往年來並沒有特別的題型，所涵蓋的範圍都是一般網路的主題，也包含目前一般生活中會使用到的網路功能。大致的方向仍以TCP/IP與乙太網路等主題爲出題方向，只要小心作答，一般考生可得60分，比較用功的考生可得80分。

一、請指出並簡要說明ADSL、FTP、HTTP、ICMP、IEEE 802.11、PPP、SIP、Telnet、UDP等標準或協定，各是對應到網路的那一個（或那幾個）分層（Physical Layer，Link Layer，Network Layer，Transport Layer，Session/Presentation/Application Layer）？（10分）

答：

(一)ADSL：Physical Layer，非對稱式數位用戶線路(Asymmetric Digital Subscriber Line)使用現有的電話線透過ADSL數據機提供在家上網的機制

(二)FTP：Session/Presentation/Application Layer，檔案傳送所使用的應用層協定。

(三)HTTP：Session/Presentation/Application Layer，全球資訊網所使用的應用層協定。

(四)ICMP：Network Layer，ICMP利用IP協定傳送。

(五)IEEE 802.11：Data Link Layer，無線網路(CSMA/CA)使用的資料連結層協定。

(五)PPP：Data Link Layer，電話網路所使用的資料連結層協定。

(六)SIP：Session/Presentation/Application Layer，VoIP所使用的會議起始協定(Session Initiation Protocol)。

(七)Telnet：Session/Presentation/Application Layer，模擬遠端終端機所使用的應用層協定。

(八)UDP：Transport Layer，網際網路上所使用的不可靠、無連線導向的傳輸層協定。

二、假設N個($N>1$)在線主機（active hosts）利用slotted ALOHA演算法對某一連結進行隨機存取。如果在任何一個時間，任一台主機正在傳送訊框的機率為p，請問該連結的傳輸效率（efficiency）為何？另外，p等於多少會使該連結有最高傳輸效率？有最高傳輸效率時，空時槽（empty slot）的機率是多少？（10分）

答：

(一)Slotted Aloha傳送成功的機率：

$f(p)=C^N_1*p*(1-p)^{N-1}=N*p*(1-p)^{N-1}$

計算最大產出量，對f(p)進行微分

$f'(p)=N*(1-p)^{N-1}+N*p*(1-p)^{N-2}*(-1)*(N-1)=0$

=>當p=1/N時有最大值

將p=1/N帶入，得

$f(1/N)=(1-1/N)^{N-1}$

p.s. 當N趨近無限大可得最大效率(efficiency)爲e^{-1}

(二)p=1/N時有最大值

(三)最大效率(efficiency)時，空時槽(empty slot)的機率爲

$f(p)=C^N_0*p^0*(1-p)^N=(1-p)^N$

p使用1/N帶入得 $(1-1/N)^N$

三、Ethernet和TCP都有錯誤偵測（error detection）的機制。請就「偵測錯誤的方法」以及「偵測到錯誤後的處置」兩方面，說明Ethernet和TCP在錯誤偵測機制上的不同。（10分）

答：

Ethernet：

1.偵測錯誤的方法：使用CRC檢測法檢查所收到的Frame。

2.偵測到錯誤後的處置：Ethernet將錯誤的資料丟棄後，等上層(如LLC)處理重送資料。

TCP：
1.偵測錯誤的方法：使用checksum檢查法檢查整筆TCP Segment的資料。
2.偵測到錯誤後的處置：TCP將不傳送ACK回應訊息給發送端，等待發送端Time out後會重新傳送資料。

四、請詳細說明網際網路中的主機A，如何透用ARP（Address Resolution Protocol）將資料(detagram)傳送到另一主機B（假設一開始A知道B的IP address，但不知道B的MAC address）。請就「A與B在同一個子網路」及「A與B在不同子網路」的情形分別說明。（20分）

答：
1.若Host B與Host A在相同的子網路上，則Host A透過ARP協定直接詢問Host B的MAC位址。
2.若Host B與Host A在不同的子網路上，則Host A透過ARP協定詢問所在子網路上的路由器的MAC位址，將資料先傳給路由器再轉送給Host B。

五、在封包交換網路（packet switched networks）中，造成封包延遲的因素包括propagation delay，transmission delay，processing delay，以及queuing delay等，請分別說明以上延遲的起因。在一個固定的網路架構中，那一個延遲因素的變動範圍最大？我們可以透過那些機制或技術，降低這一個延遲因素對即時多媒體服務（real-time multimedia service）的影響？（20分）

答：
(一)
1.propagation delay：在網路線上傳輸所花費的時間，與網路線上電子訊號跑的速度有關。
2.transmission delay：網路卡將資料傳送(或接收)資料到網路線上所花的時間，與網路卡的傳送速度有關(如高速乙太網路傳送速度100Mbps)
3.processing delay：路由器處理Header與找路徑等所花費的時間。
4.queuing delay：在路由器上因爲某些因素無法立刻將傳送封包到網路上造成封包停留在buffer上所花費的時間。
在網路上propagation delay、transmission delay與processing delay都可根據相關參數(如封包大小、網路卡傳送速度等)計算所需時間，只有queuing delay必須根據網路當時情形才能獲知所需時間，因此queuing delay的變動性最大。
(二)對於多媒體服務(real-time service)的特性需要即時服務並且也需要降低jitter的情形，因此對於變動因素大的queuing delay需要特別處理，可透過下列相關技術降低queuing delay所造成的問題:
1.使用flow control機制控制網路流量，如使用sliding window機制。
2.使用congestion control機制控制網路上資料量壅塞的問題。
3.使用traffic shaping機制調整傳送資料量的方式，如leaky bucket或token bucket機制。
4.若在具提供QoS的網路上(如ATM網路)則可透過QoS機制預約相關資源以減低delay。

六、請問什麼是行動裝置(mobile node)的COA（care-of address）？另外，請說明行動裝置用agent solicitation取得COA的程序。（15分）

答：
(一)CoA（Care-of Address): 在行動式IP (Mobile IP)中用於行動式IP設備上的一個暫時性的IP位址，讓本地代理人(Home Agent)可將訊息傳送給行動設備。
(二)取得Care-of-Address
1.一個Mobile Host取得Care-of-Address的方法，是根據現有的ICMP Router Discovery通訊協定作擴充。這個通訊協定原本是用來告訴一個主機它的default routers，但是在此協定上再加上有關於Care-of-Address的資訊。
Home Agent和Foreign Agent每隔一段時間就會作”廣播”這個動作(broadcast)，發出有關於Care-of-Address的封包給LAN上的每個主機，如果LAN上有Mobile Host，就可以取得Care-of-Address。這麼作的原因是如

果Mobile Host現在不是在Home Network時，只能收到廣播的封包。當然，如果Mobile Host現在是在Home Network時，Home Network可以不提供任何的Care-of-Address。Router Advertisement再加上Care-of-Address時，這個訊息稱爲"Agent Advertisement"。

2.只靠廣播這個動作時，有時候Mobile Host會等不及，這時Mobile Host也可以主動的broadcast或者是multicast一個封包，來偵測現在是否有Home Agent 或Foreign Agent的存在。還有一個情形，就是Mobile Host已經隔一段時間都沒有收到任何的Agent Advertisement，就可以假設它現在已經不在這個Foreign Agent的管轄範圍。這時，Mobile Host也可以主動的隔一段時間，就送出一個封包。這個封包是使用Router Solicitation再加上一些資訊，例如Mobile Host需要這個Care-of-Address多久的時間，這整個訊息稱爲"Agent Solicitation"。當Agent收到這個封包時，就必須馬上送出Agent Advertisement 的訊息出去。作完以上動作，這時Mobile Host就已經取得了Care-of-Address

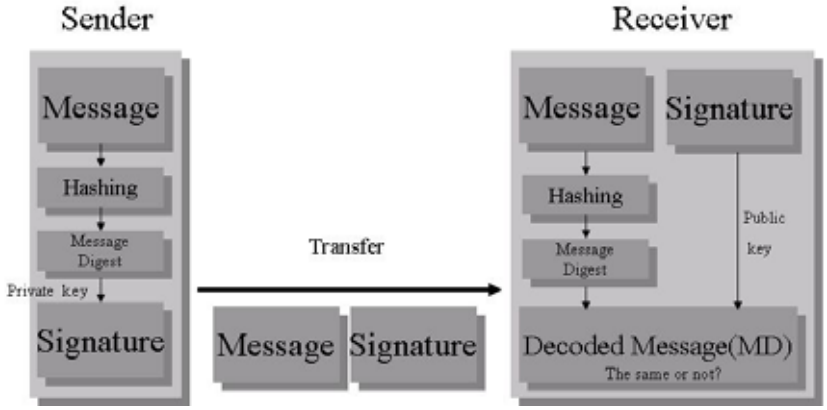
七、內政部自然人憑證IC卡採用公開金鑰（public key）密碼系統。請以自然人憑證IC卡進行網路報稅為例，說明以公開金鑰密碼系統進行「資料加解密」與「數位簽章」的運作原理，請一併說明其中的金鑰產生與管理方式。（15分）

答：

(一)

1.資料加解密：透過public key的加密演算法計算得到一對key，將其中一支key公開給發送端使用稱爲公開鎖鑰(public key)，另一支key保留在IC卡上用作解密稱爲私用鎖鑰(private key)。

2.數位簽章：發送端利用public key機制產生一對鎖鑰，將要傳遞的訊息利用hashing的方式產生訊息摘要(Message Digest)後，利用私用鎖鑰(private key)加密產生簽章後，將訊息與簽章傳送給接收端。接收端可利用發送端公布的公用鎖鑰(public key)與簽章進行確認身分的動作。



(二)金鑰是利用RSA演算法所產生，其中私用鎖鑰放在IC卡上。使用時透過內政部憑證管理中心所認可的憑證機構來進行網路安全機制的管控。