《電腦網路》

試題評析
今年首次加考此科。試題中都是一些網路的基礎考題，並無特別困難的問題。包含client-server、peer-to-peer、switching技術與資訊安全PAP、CHAP等概念與TCP/IP、無線網路的主題。考生只要平常心作答，應可得80分，程度較佳的考生可得90分。

一、請說明網路系統中的主從式（Client Server）架構與對等式（Peer to Peer）架構，並簡述兩者之間的差別。（15分）

答：

(一)

1.對等式(Peer-to-Peer)網路：資料與資源分散在整個網路上，沒有集中式資訊儲存系統，也沒有中央伺服器的維護。每個使用者都可以將資料與資源分享出去，提供給其他電腦使用。

2.主從架構(Client-server architecture)：中央集權式的資源配置、管理架構。網路上的所有資源，由一部或數部電腦分配、管理。伺服器(server)是提供與管理資源的電腦。客戶端(client)是要求網路服務的電腦。其間所做的資訊流通必須透過連結的網路，且使用網路通訊協定彼此溝通。

(二)

1.對等式(Peer-to-Peer)網路：

(1)優點：

A.分散式系統資源，分散伺服器負擔。

B.並行處理能力佳。

C.系統處理容量遠大於Web-Base的Client-Server架構。

D.使用記憶體管理交換資訊，效能大幅提昇。

E.硬體成本低。

F.客戶端與客戶端採取直接即時的溝通。

(2)缺點：

A.架構較複雜，除開發伺服器端程式外，還要有專用的客戶端程式。

B.客戶端上線後才會有資源分享出，因此如果客戶端少的話，分享資源就少。

2.主從架構(Client-server architecture)：

(1)優點：

A.資源集中式安全管理。

B.現成的客戶端程式免費取得(IE、Firefox)。

(2)缺點:

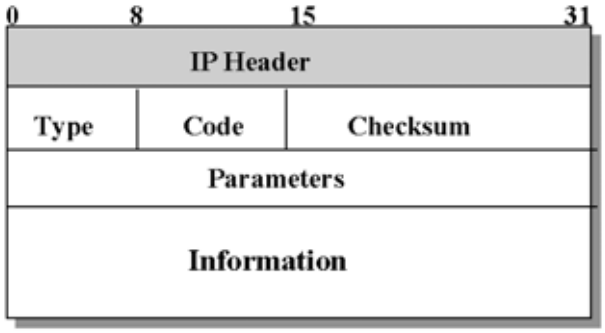
A.伺服器常成爲瓶頸所在，且不容易有效改善。

B.硬體成本高。

二、請說明ICMP與IP協定間的關係？協定運作的目的為何？一般常用的指令是否有運用ICMP方式進行通訊的，請舉出兩種常見的ICMP功能進行說明。（20分）

答：

(一)在OSI模型中，ICMP協定雖然與IP協定同爲第三層協定，但ICMP本身是不具備傳送能力的。實際上，它跟TCP/UDP一樣，也是靠IP幫忙進行傳送。其封包結構如下：



(二)ICMP(Internet Control Message Protocol)：Router與Router或之間發送錯誤或控制訊息的通訊協定。ICMP是用來控制在 Internet 的TCP/IP 通訊協定當中，各種控制命令所產生的結果，例如：資料在網際網路上傳遞是否到達目的地，或是找不到目的地、網路塞車等資訊。其功能主要有：

1.偵測遠端主機是否存在。
2.建立及維護路由資料。
3.重導資料傳送路徑。
4.資料流量控制。

(三)ping指令：用來測試特定主機能否通過IP到達。ping的運作原理是向目標主機傳出一個ICMP echo要求封包，等待接收echo回應封包。程式會按時間和反應成功的次數，估計失去封包率(丟包率)和封包來回時間(網路時延)。

traceroute 命令：我們可以找出通往目的地的所有經過的路由位址，並以數字將路由順序標示出來。

1.首先，traceroute 命令會向目標位址送出UDP偵測封包，但將第一個送出的封包之TTL設爲1。這樣，第一個路由節點在處理這個封包的時候，減掉1，並發現TTL爲0，於是就不處理這個封包，並同時送回一個 ICMP 封包。這樣，發送端就知道第一個路由節點在哪裡了。
2.當接到第一個ICMP返回的時候，程式會檢查返回主機是否就是目標主機，如果不是，則再送出第二個封包，但 TTL 比上次增加 1。
3.這樣，第一路由節點接到的封包之TTL就不是0，那麼處理完畢後送給下一個節點，同時將TTL扣除1。這樣，當下一個站收到這個封包，再扣掉TTL爲0，也會送回ICMP封包，這樣，程式就知道第二個路由節點在哪裡了。
4.然後重覆上一個動作，直到找到目標主機爲止，或是封包的最大TTL(通常爲30) 都用光爲止。

三、請針對處理時間及可靠度比較說明TCP與UDP兩種協定的差異，並各舉出三種運用此協定的應用程式？（15分）

答：

(一)TCP(Transmission Control Protocol)

1.TCP具連線導向(Connection-oriented)與可靠性(Reliable)的通訊協定。來源端會與目的端建立連線而後開始傳送資料，也保證目的端必須正確收到資料，所以在處理時間上花費較久。
2.TCP來源端傳送資料後會啓動計時器功能，等待目的端的回應訊息(ACK)。若來源端計時器time-out則會重送資料給目的端。在目的端收到資料後會使用Checksum機制檢查資料的正確性，若驗證正確後則會發出ACK回應訊息給來源端，說明已正確收到資料。這是TCP保證可靠性的方式。

(二)UDP(User Datagram Protocol)

1.UDP具非連線導向(Connectionless)與不可靠性(Unreliable)的通訊協定。來源端直接傳送資料給目的端，不會知道目的端是否正確收到資料，也不會重送資料給目的端。因此相對TCP來說，所花的處理時間較少。
2.UDP目的端若收到資料時，會執行Checksum機制檢查資料的正確度。若資料正確就可使用資料，若檢查後資料有問題則將資料丟棄，也不會傳送ACK給來源端。來源端送出資料後不會等待任何ACK回應訊息，也不會重送資料，因此屬於不可靠性質的通訊協定。

(三)使用TCP的應用層通訊協定有HTTP(80)、FTP(21)、TELNET(23)等，使用UDP的應用層通訊協定有

DNS(53)、DHCP(67)、SNMP(161)等。

四、常見的網路交換方式（Switching）有那三種？請簡要對其架構及特性進行說明。（15分）

答：

交換技術有下列三種：

(一)電路交換(Circuit switching): 與電話使用方法相同，當撥通後線路一直存在，直到斷線爲止。

1.連線導向(connection-oriented)特性

2.資料走固定路徑

3.每個連線使用固定頻寬

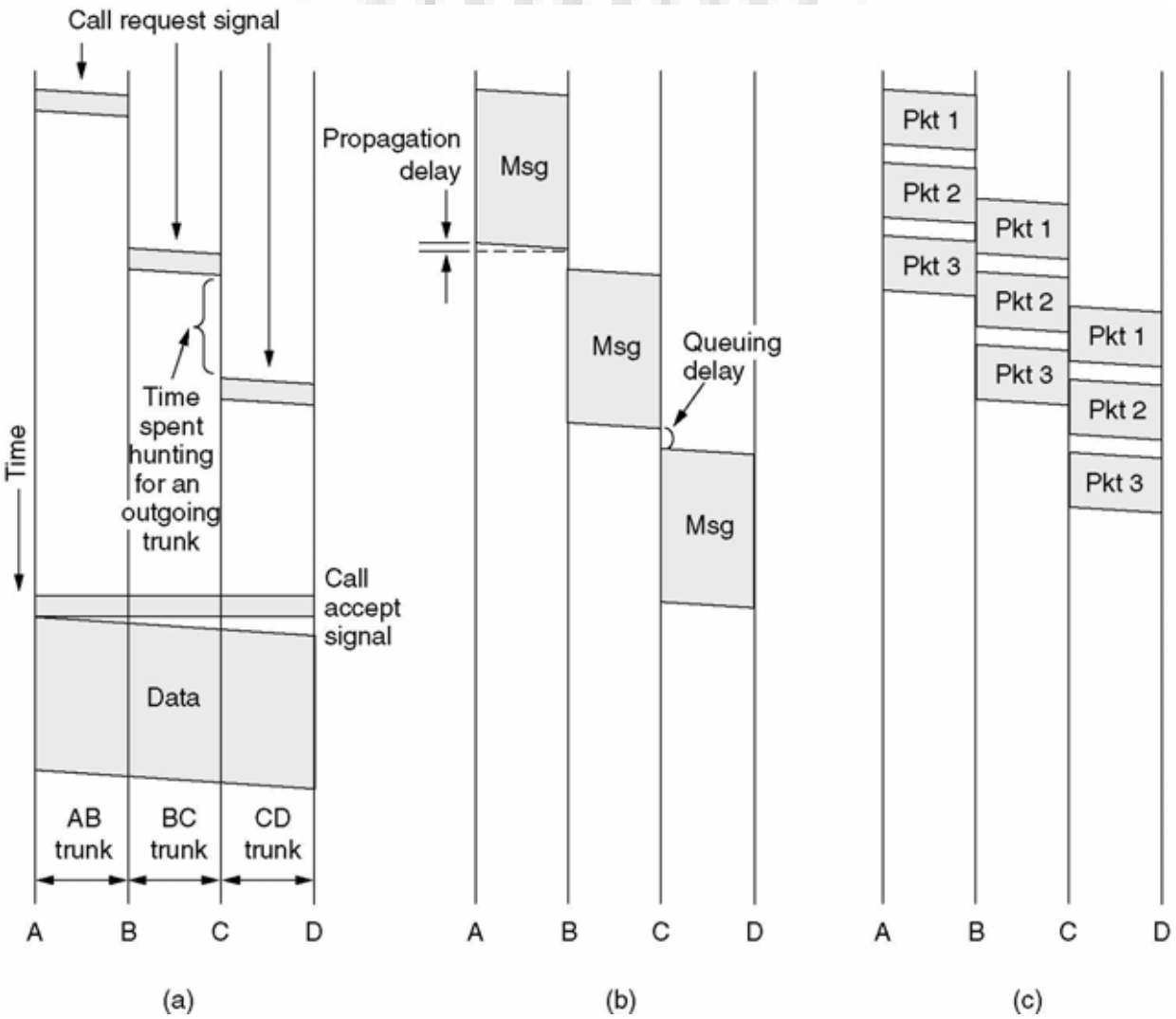
4.如電話網路(PSTN)

(二)訊息交換(Message switching)

將整個資料以一個訊息(message)爲單位傳送資料，不做任何的切割處理。

(三)分封交換(Packet switching)

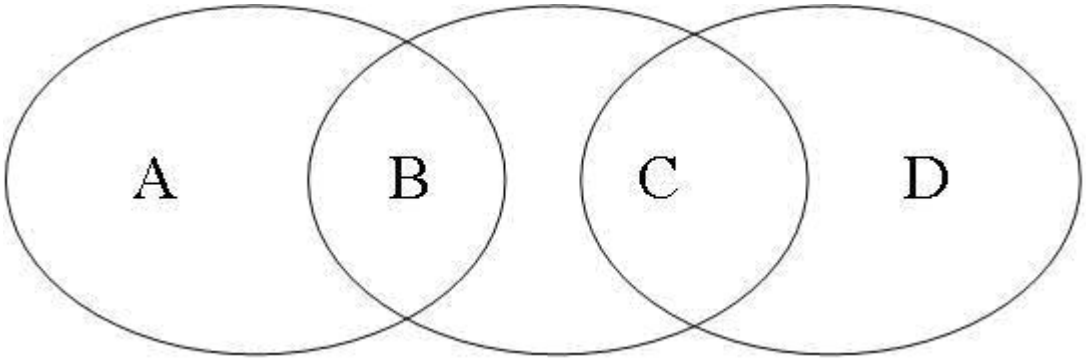
與訊息傳送方法相同，不過傳送時將資料切成封包(packet)傳出。網路上的路由器(router)負責做路徑選擇及轉存(Store and Forward)傳送，如IP網路。



五、在無線區域網路的環境中，何謂隱藏節點（Hidden Terminal）問題？會產生何種通訊上問題？IEEE 802.11協定如何解決？（20分）

答：

(一)隱藏的工作站問題(hidden station problem)：這是指在無線傳輸時因爲與競爭者之間的距離過大，所以工作站無法偵測到傳輸的競爭對手，以下圖爲例，如果工作站A要傳送資料給工作站B，但因爲是無線網路，所以工作站C無法偵測到，如果這時工作站C也要傳送資料給工作站B，則會造成碰撞。



(二)會發生同時間兩台電腦彼此不知對方，同時對同一台電腦傳送資料，造成接收端電腦發生碰撞而無法正確收到資料。

(三)應用IEEE802.11協定(Multiple Access Collision Avoidance, MACA)，可以提供以下的解決方式：
工作站A在正式傳送資料給工作站B之前，先傳出一個RTS(Request To Send)訊框(30個位元組)給工作站B，然後工作站B也會回傳一個CTS(Clear To Send)訊框給工作站A，之後才可以進行資料傳輸。則任何聽到RTS的工作站則必須保持靜肅，直到CTS正確的回傳爲止；而任何聽到CTS工作站必須等到二個工作站的資料傳送完畢爲止，才能進行其他的資料傳送。

六、何謂PPP協定？何謂PAP協定？何謂CHAP協定？請簡要說明之。（15分）

答：

(一)PPP(Point-to-Point Protocol)是點對點的通訊協定，在Internet上的使用者和它的ISP(網路連線提供者)通常是使用PPP的通訊協定，利用電話、數據機和Internet連上線。PPP是一種全雙工的連結層通訊協定，它可以用在兩個路由器(router)或是橋接器(bridge)之間，傳送TCP的封包，所以十分適合用於Internet上。
1.不僅可使用在撥接網路，也可使用在router與router之間的專線上。
2.能夠很清楚找出一個frame的開始與結束，也可處理錯誤偵測。
3.連線控制協定用來把連線建立、測試等選項，並將不需要的連線自然的關閉。
4.提供與網路層協商的方式，與所使用的網路層無關。
5.以位元組爲導向。

(二)PAP(Password Authentication Protocol)認證，顧名思義就是使用者以密碼來作爲主要的身分驗證依據，其流程爲認證者(Authenticator)將密碼明文送給認證伺服器(Authentication Server)，認證伺服器再利用使用者所傳來的密碼進行密碼比對。由於伺服器所收到的是密碼原文，因此可以支援多種後端使用者帳號系統，無論使用者密碼是經過特殊編碼的UNIX shadow/password，或是能夠支援明碼密碼的LDAP、SQL伺服器等。但是PAP的缺點是使用者的個人密碼必須透過網路傳送，因此會有被竊取的風險。

(三)CHAP(Challenge-Handshake Authentication Protocol)運作方式
1.在鏈路建立完成後，驗證者向對端發送一個「challenge」信息。
2.對端使用一個「one-way-hash」函數，例如：MD5，計算出的值響應這個信息。
3.驗證者使用自己計算的hash值校驗響應值。如果兩個值匹配，則驗證是承認的，否則連接應該終止。
4.在隨機時間，驗證端發送一個「challenge」給對端，重複1到3步驟。