《資通網路》

試題評析	本次命題集中於講義第三、第四回(第五回屬資訊安全範疇)，題目相當新穎靈活，對考生而言是相當大的挑戰。是以，在準備上除了基礎知識外，也要多補充熱門的網路議題，例如：IPv6 的相關資訊。
考點命中	第一題：《高點・高上資通網路講義》第四回，張又中編撰，頁 4-21。 第二題：《高點・高上資通網路講義》第三回，張又中編撰，頁 3-25～27； 《高點・高上資通網路講義》第四回，張又中編撰，頁 4-3～6、4-10～11。 第三題：《高點・高上資通網路講義》第三回，張又中編撰，頁 3-77。

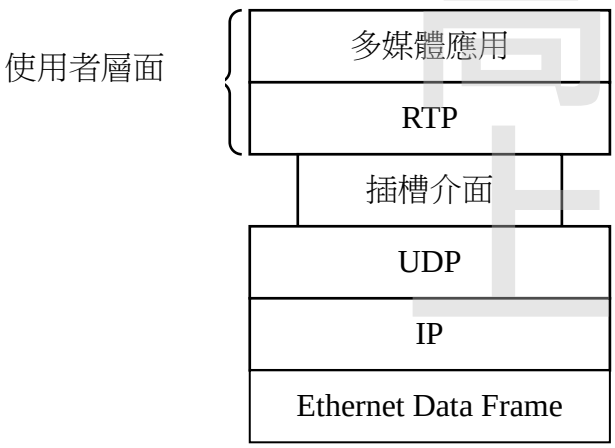
一、(一)網際網路（Internet）上常見的視訊串流（Video Streaming）應用中，接收端在播放前必須將收到的視訊資料存入一緩衝器（Buffer），試說明原因。(5分)

(二)網路電話的通話雙方透過網際網路將壓縮的語音訊號傳送至對方，除了UDP（User Datagram Protocol）之外，RTP（Real-time Transport Protocol）也是必要的協定。請說明這兩個協定在語音傳輸過程中的主要功能。(15分)

【擬答】

(一)由於網路傳輸會受到線路品質、網路壅塞等狀況之影響，並不能確保其流量一定能保持穩定，故接收端在播放前先將收到的視訊資料存入緩衝區中，當網路狀況不穩定時，其仍可就緩衝區的資料先行處理，維持視訊串流的播放品質。

(二)RTP 初始被設計為一多播協定，但後來被用在許多單播應用中。其將數個即時多媒體的資料串流經過多工處理，編碼為單一的 UDP 封包流並嵌入 IP 封包，之後放入訊框進行傳輸。適合即時傳輸的分散式應用，例如：視訊會議、現場視訊群播、VoIP、即時監控等。



二、一個使用者透過瀏覽器上網至 URL http://www.abc.com/xyz/home.index， 假設該使用者從未瀏覽過該網頁。在瀏覽器顯示網頁內容之前，必須先完成一些必要步驟，請說明這些步驟。(20 分)

【擬答】

1.使用者端向 DNS 伺服器發出 www.abc.com 的 DNS 查詢。
2.DNS 伺服器回傳使用者端 www.abc.com 之對應 IP。
3.使用者端利用三方交握法，向 www.abc.com 建立 TCP 連結。
4.使用者端向 www.abc.com 發出 HTTP Request。
5.www.abc.com 回傳使用者端 HTTP Response。

6.使用者端的瀏覽器解析 HTTP Response，並於瀏覽器呈現結果。

三、協定無關群播（Protocol Independent Multicast, PIM）為網際網路上常用的群播協定之一。假設參加某一個 PIM 群組的節點數目很少，遠小於網路上所有節點數目，且只有單一源端（Source），試說明這種狀況下 PIM 如何運作。（20 分）

【擬答】

使用 PIM-SM(Protocol Independent Multicast-Sparse Mode)，其為拉的方式，只有存在接收端的網段才會收到資料流，主要用於群組節點分佈相對分散、範圍較廣的廣域網路中。

PIM-SM 實現轉發群播封包的核心任務為建構與維護一棵單向共享樹，其選擇 PIM 中某一路由器作為公用根節點，即匯聚點(RP Rendezvous Point, RP)，連結接收端的路由器向 RP 傳送群組加入資訊，該資訊經過一個個路由器後到達 RP，所經過的路徑形成此共享樹的分支。

當欲傳送群播封包時，來源端將群播封包發送至 RP，透過 RP 沿共享樹向接收端轉發，群播封包被複製並沿著共享樹遞送，直到最終抵達接受端。由於封包複製僅發生於共享樹的分支處，故可有效降低網路流量，以及節點的處理負載。

四、在下一世代網際網路協定 IPv6 中制訂了 IP 任播（IP Anycast），請說明 IP Anycast 的主要用途與運作方式。（20 分）

【擬答】

定義於 RFC1546，是一種網路定址和路由的策略，可讓資料根據路由拓撲來決定送到最近或最好的目的地，通常使用 BGP 來實現。在任播中，傳送端與接收端之間存在一對多的關係，然在任何給定時間，只有其中之一的接收端可以收到傳送端傳送的資訊。

任播的主要用途有：

1.提供高可靠性和負載平衡

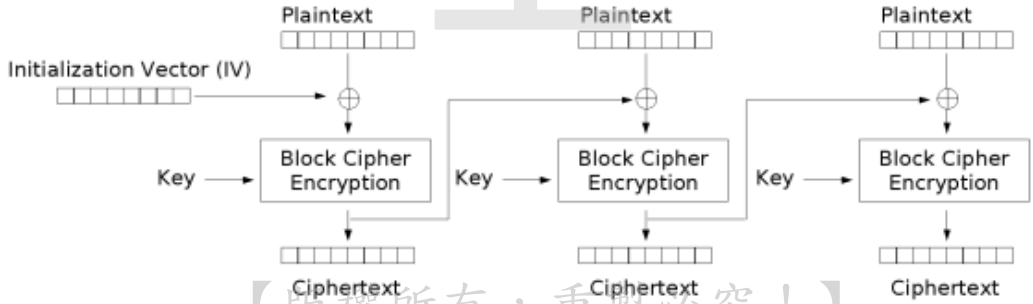
2.發展 IPv6 相容 IPv4

3.防禦網路攻擊

五、密碼塊連結（Cipher Block Chaining, CBC）為區塊加密（Block Cipher）之常用模式。試說明密碼塊連結之運作方式。（20 分）

【擬答】

1976 年 IBM 所發明，每個明文塊先與前一個密文塊進行 XOR 後再進行加密。於此方法中，每個密文塊皆依賴於其前面的所有明文塊。同時，為了保證每個資訊的唯一性，在第一塊中需要使用初始向量(Initial Vector, IV)來進行 XOR 運算。



Cipher Block Chaining (CBC) mode encryption

Source：https://upload.wikimedia.org/wikipedia/commons/d/d3/Cbc_encryption.png