

# 《計算機網路》

試題評析	<p>第一題：使用 traceroute 指令來回答即可。</p> <p>第二題：路由器的繞路與轉送是基本問題。</p> <p>第三題：IP multicast 使用 IGMP 協定建立群組，並使用 class D 位址作為群播位址。</p> <p>第四題：802.11 的比較是上課強調的重點。</p> <p>第五題：防火牆考題已經出現很多次。</p> <p>綜合而言，今年題目適中，沒有太偏離主題的題目，一般程度學生可拿 60 分，詳細研讀上課內容者可拿 80 分以上。</p>
考點命中	<p>第一題：《高點電腦網路講義第三回》，許振明編撰，頁 13。</p> <p>第二題：《高點電腦網路講義第二回》，許振明編撰，頁 65。</p> <p>第三題：《高點電腦網路講義第三回》，許振明編撰，頁 19。</p> <p>第四題：《高點電腦網路講義第二回》，許振明編撰，頁 14。</p> <p>第五題：《高點電腦網路講義第三回》，許振明編撰，頁 82。</p>

一、在網際網路上，一部個人電腦與一遠端伺服器之間，用何種方法可以偵測到它們之間的傳輸路徑與約略封包來回之時間？並說明所用方法之原理。(20 分)

## 【擬答】

traceroute 命令，可以找出通往目的地所有經過的路由位址，並以數字將路由順序標示出來。最後會顯示所經路徑與所花的時間。

(一)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 設為 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 為 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。

(二)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。

(三)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 為 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。

(四)然後重覆上一個動作，直到找到目標主機為止，或是封包的最大 TTL(通常為 30) 都用光為止。

二、網際網路上，路由器 (Router) 提供了路由 (Routing) 與轉送 (Forwarding) 兩種重要機制。請說明這兩種機制的運作方式與其區別。(20 分)

## 【擬答】

**Routing(路由)：**根據 routing algorithms(繞送演算法)來決定該如何從一個 host 將封包送到另一個 host。在整個網路範圍中的過程，決定封包由來源端到目的端所採取的端點到端點路徑。

**Forwarding(轉送)：**該怎麼把封包從一個 router 送到下一個 router。在 router 內進行的動作，將封包從輸入連結介面傳送到適當的輸出連結介面。

	運作機制	區別
Routing	利用繞路演算法，如 RIP、OSPF 等，進行繞路資訊的收集，產生路由表(Routing)，提供路由器進行繞路的選擇。	產生路由表。
Forwarding	查詢路由表後，根據路由表的指示，將封包由輸入端送到指定的輸出端送出路由器。	根據路由表轉送封包。

三、群播 (Multicast) 協定在網際網路上的應用越來越廣，但傳統 IP Multicast 有些缺點，因而至今仍未被大量使用。試說明 IP Multicast 的基本運作方式與它在實際應用上的缺點。(20 分)

【擬答】

(一)使用 IGMP 建立群組

- 1.所有主機和多點傳送路由器間的通訊都使用 IP 多點傳送，所以 IGMP 訊息在傳送前必須先行壓縮至 IP Datagram 中，而目的地的 IP 位址則為代表所有主機多點傳送位址的 224.0.0.0。
- 2.多點傳送路由器並不傳送個別的要求訊息至每個多點傳送群組，而是在所有群組間傳送一個輪詢以要求資訊，但每分鐘的輪詢次數最多為一次。
- 3.多點傳送群組中的成員主機不會在同一時間內傳送多個回應訊息，而會在 IGMP 要求訊息到達時，由主機指定每個所屬群組一個 0 ~ 10 秒的延遲間隔時間，然後在此延遲時間到期時傳送一個回應訊息至此群組。
- 4.主機開始監聽由其他主機而來的回應。

(二)IP Multicast 缺點

- 1.UDP base 無法確認接收到的機制，可靠性低
- 2.沒有 QOS
- 3.QOS 需要由 Multicast 的應用層去控制
- 4.沒有序號，先後順序無法確定
- 5.Layer 2 會有問題，無法裝在 MAC Table 裏

四、試列表說明 IEEE 802.11 a/b/g/n 四種常見規格所用之頻率、調變 (Modulation) 方式、與最大傳輸速率；又那一種之涵蓋範圍最遠？(20 分)

【擬答】

(一)

	802.11a	802.11b	802.11g	802.11n
傳輸頻率	5GHz	2.4GHz	2.4GHz	2.4 或 5GHz
調變技術	OFDM	DSSS	OFDM	OFDM
頻寬	54Mbps	11Mbps	54Mbps	540Mbps
傳輸範圍	50 m	100 m	100 m	100 m

(二)802.11b, 802.11g, 802.11n 均可達 100m

五、防火牆的封包過濾器分成傳統式與狀態式的，傳統式的封包過濾有那些問題？而狀態式的封包過濾如何解決這些問題？(20 分)

【擬答】

- (一)傳統式封包過濾器(Packet Filtering)：封包過濾防火牆為第一代防火牆，提供網路層封包篩選的基本功能。依據定義好的存取規則，應用到每個流入或流出的 IP 封包上，以決定是否允許或阻止封包的進出。操作於路徑選擇器(Router)的程式。檢查主從式架構的 IP 分封，經由 IP 位址、port 及方向來控制資料的傳播，是網路層的防衛機制。優點是價格低、安裝簡便。缺點是安全性差。
- (二)狀態檢視防火牆(Stateful Inspection Firewall)：是一種動態封包過濾的防火牆技術，能夠更細部(more granularly)的檢視封包及連線工作階段的防火牆類型。
- 1.狀態檢視防火牆不僅採用封包過濾類似的方法來監控網路傳輸，還會更進一步檢查封包資料流的內容與行為，並非只是單純地過濾個別封包。
  - 2.持續追蹤連接狀態直到結束連線為止，藉以判斷是否為有效的連線而允許封包通過。
  - 3.建立每個連線階段的狀態表，然後根據此前後關聯狀況來判斷是否允許或拒絕此封包通過。
- 優點：狀態檢視防火牆可以透過連線狀態來判斷是否為合法授權的封包，所以安全性較靜態封包過濾防火牆為高。
- 缺點：效能較封包過濾稍差，無法處理應用層協定。