1. DNS 功能與運作原理。

DNS 的功能:

DNS 的全名為 Domain Name System，他主要的功能是將一串容易記住的網址轉換成比較難記的 IP 位置，在網頁上也可以透過 DNS 的名稱的不同來區別出不同的網頁，這樣可以達到一個網頁的伺服器能夠在同個 IP 上面提供不同網站。

DNS 的運作方式:

DNS 分為 Client 和 Server，Client 扮演發問的角色，也就是問 Server 一個 Domain Name，而 Server 必須要回答此 Domain Name 的真正 IP 地址。而當地的 DNS 先會查自己的資料庫。如果自己的資料庫沒有，則會往該 DNS 上所設的的 DNS 尋問，依此得到答案之後，將收到的答案存起來，並回達客戶。真正 DNS 的運作：有兩種詢問方法，Recursive 和 Iterative 兩種。前面是由 DNS 代理去問，問的方法是用 Iterative 方式，後者是由本機直接做 Iterative 式的詢問。

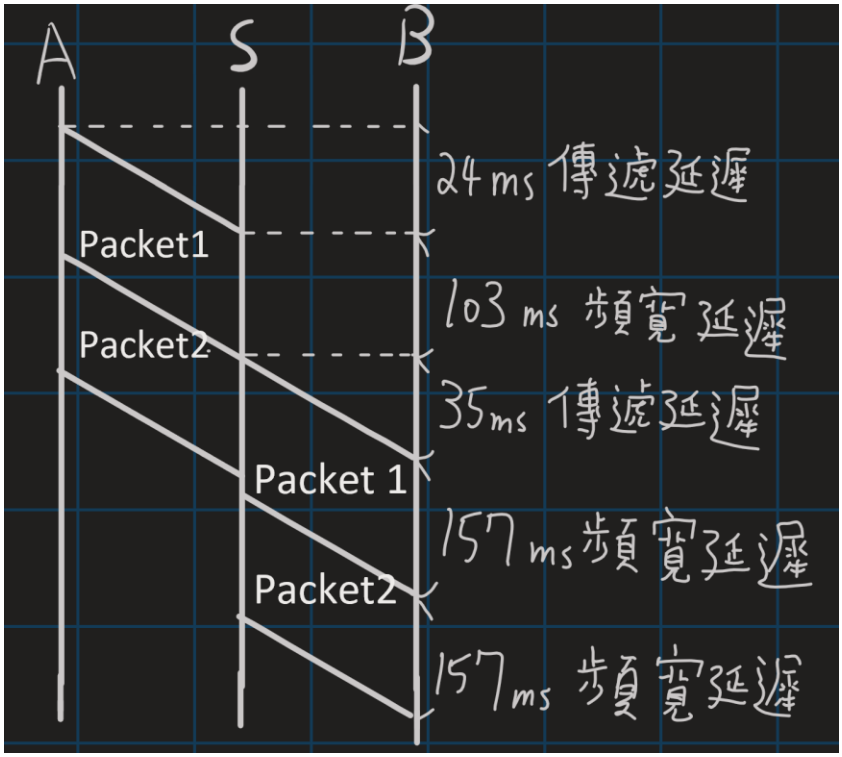
```
PS C:\Users\Yushiang> nslookup
預設伺服器:  UnKnown
Address:  192.168.100.1

> server 8.8.8.8
預設伺服器:  dns.google
Address:  8.8.8.8

> set q=ns
> google.com
伺服器:  dns.google
Address:  8.8.8.8

未經授權的回答:
google.com      nameserver = ns4.google.com
google.com      nameserver = ns2.google.com
google.com      nameserver = ns1.google.com
google.com      nameserver = ns3.google.com
>
```

1. 寫出一種 Routing-Update Algorithm

Link-State Routing-Update Algorithm(鏈路狀態路由更新演算法)：

Link-State Routing-Update Algorithm 會從其他路由器收集有關整個網路的路徑之訊，所以代表整個網路中的路由器會互相交換所知網路的路徑之訊，到最後每一個網路內的每個路由器都會對整個網路有一定的了解，這樣就可以在每個路由器上都彙整出一個路由表，最後每一台路由器就都可以計算出屬於自己的最佳路由，來達到增加風包傳遞效率的目的。而這個路由演算法是為了彌補 Distance Vector 路由演算法的缺點，因為他可以對網路的變更做出比較快速的回應。當網路發生變化的時候 Link-State 也會馬上跟其他路由器同步更新過後的路由資訊。

2. 假設從 A 到 B 的網路路徑中間有一個 switch S： A-S-B. 傳遞延遲在 A-S 和 S-B 上分別為 24 微秒和 35 微秒。A–S 上的每 package 頻寬延遲和 S-B link 分別為 103 微秒和 157 微秒。下圖描述兩個發送從 A 到 B 的連續 package。在右邊標記時間間隔 (a) 到 (e)， 請說明出總計發送 package 的時間。



4. 請說明 ICMP, ARP, DHCP 功能與運作原理。

ICMP:

這個網路協定運用在網路七層協定中的第三層。該協定的最主要目的，是用來解析網路封包或是分析路由的情況，大多是透過所傳回來的錯誤訊息進行分析，而網路管理人員則利用這個協定的工具來了解狀況，進而使用其他措施解決所遇到的問題。

ARP:

是一個通過解析網路層位址來找尋資料鏈路層位址的網路傳輸協定，它在 IPv4 中極其重要。

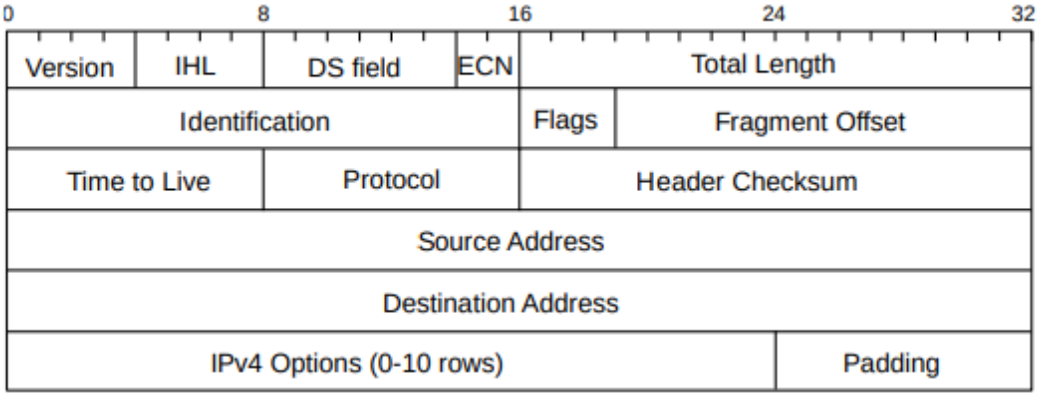
DHCP:

動態主機設定協定（英語：Dynamic Host Configuration Protocol，縮寫：DHCP），又稱動態主機組態協定，是一個用於 IP 網路的網路協定，位於 OSI 模型的應用層，使用 UDP 協定工作，主要有兩個用途：

用於內部網路或網路服務供應商自動分配 IP 位址給使用者

用於內部網路管理員對所有電腦作中央管理

5. 簡要說明 IPv4 Header 包含哪些資訊，以及其作用。



Version：IP 的版本(IPv4 為 0010)。

IHL：表示 header 的長度，單位為 4-byte，最小是 5(20-byte)，最大為 15(60-byte)。

DSCP (Differentiated Services Code Point)：DSCP 使用 6 個 bit，範圍為 0~63，他是拿來分類封包優先級的，像是 VoIP 就有用到這一欄。

ECN(Explicit Congestion Notification)：在網路阻塞的時候可以在這裡設定一個標記來代替丟棄封包，以表示封包阻塞即將發生。是由封包的接收端向傳送端的表示，讓傳送端降低傳送速度。

Total Length：有時候封包會超過 MTU 規定的大小，這時候就會被分段，這一欄就是表示整個封包的大小，單位是 Byte，最小是 20，最大是 65536。

Identification：，而這一欄就是標記這個片段是來自哪個封包，最大值是 65536。

Flags：總共 3bit，第一個 bit 通常為 0，第二個 bit (DF Don't Fragment)是用來表示說這個封包不能被分割傳送，第三個 bit (MF More Fragments)通常為 1 只有屬於封包最後一個分段時才會為 0。

Fragment Offset：這一欄代表這個分段對於原始封包開頭的偏移量，以 8-byte 為單為。

Time to Live(TTL)：當封包每經過一個 Hop 時都會被減 1，當變為 0 時封包就不會再被轉發，目的是要防使封包無限循環。

Protocol：用來標示所使用的 IP 通訊協定。

1：ICMP

6：TCP

17：UDP

Header Checksum：用來做封包 Header 的錯誤檢查，當封包經過 NAT 之後這個欄位會被改寫。

Source/Destination Address：表示封包的來源及目的位置。

IP Options、Padding：長度為 1~40-byte，這裡是用來設定一些非預設的設定。

6. 以下哪一組是 IPV4 的相同的 subnet，請說明理由。

如何判斷一個 IP 是否屬於那個網段:

因為一個正常的 IP 跟子網路遮罩做 AND 會等於網路位置，所以我們只需要把 IP 跟

遮罩做 AND 就可以篩選出那些 IP 屬於這個子網路。

(a). 10.0.130.0/23: 10.0.130.23, 10.0.129.1, 10.0.131.12, 10.0.132.7

10.0.130.23 AND 255.255.254.0 = 10.0.130.0

10.0.129.1 AND 255.255.254.0 = 10.0.128.0

10.0.131.12 AND 255.255.254.0 = 10.0.130.0

10.0.132.7 AND 255.255.254.0 = 10.0.130.0

由此可知 10.0.130.23、10.0.131.12 屬於 10.0.130.0/23。

(b). 10.0.132.0/22: 10.0.130.23, 10.0.135.1, 10.0.134.12, 10.0.136.7

10.0.130.23 AND 255.255.252.0 = 10.0.128.0

10.0.135.1 AND 255.255.252.0 = 10.0.132.0

10.0.134.12 AND 255.255.252.0 = 10.0.132.0

10.0.136.7 AND 255.255.252.0 = 10.0.136.0

由此可知 10.0.135.1、10.0.134.12 屬於 10.0.132.0/22。

(c). 10.0.64.0/18: 10.0.65.13, 10.0.32.4, 10.0.127.3, 10.0.128.4

10.0.65.13 AND 255.255.192.0 = 10.0.64.0

10.0.32.4 AND 255.255.192.0 = 10.0.0.0

10.0.127.3 AND 255.255.192.0 = 10.0.64.0

10.0.128.4 AND 255.255.192.0 = 10.0.128.0

由此可知 10.0.65.13、10.0.127.3 屬於 10.0.64.0/18。

(d). 10.0.168.0/21: 10.0.166.1, 10.0.170.3, 10.0.174.5, 10.0.177.7

10.0.166.1 AND 255.255.248.0 = 10.0.160.0

10.0.170.3 AND 255.255.248.0 = 10.0.168.0

10.0.174.5 AND 255.255.248.0 = 10.0.168.0

10.0.177.7 AND 255.255.248.0 = 10.0.176.0

由此可知 10.0.173.3、10.0.174.5 屬於 10.0.168.0/21。

(e). 10.0.0.64/26: 10.0.0.125, 10.0.0.66, 10.0.0.130, 10.0.0.62

10.0.0.125 AND 255.255.255.192 =10.0.0.64

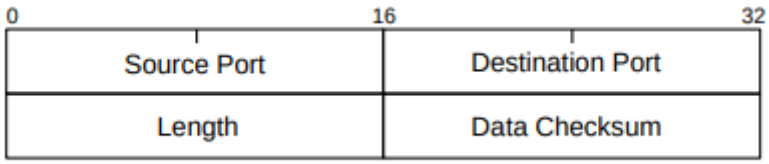
10.0.0.66 AND 255.255.255.192 =10.0.0.64

10.0.0.130 AND 255.255.255.192 =10.0.0.128

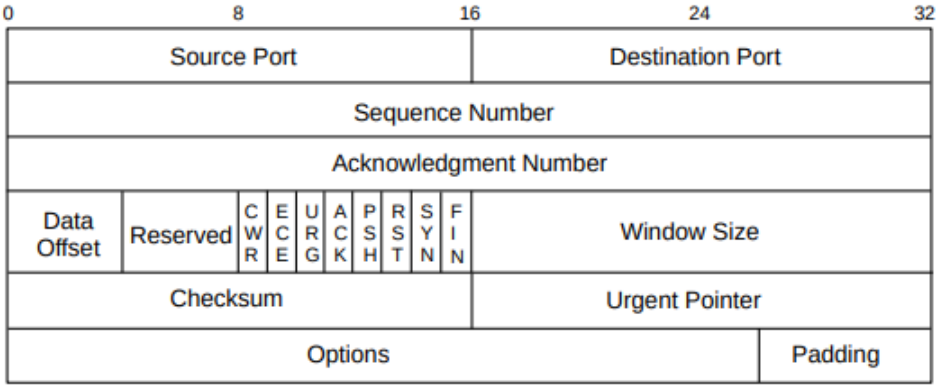
10.0.0.62 AND 255.255.255.192 =10.0.0.0

由此可知 10.0.0.125、10.0.0.66 屬於 10.0.0.64/26。

7. 請說明 UDP 和 TCP 的 package header 異同與傳輸方式異同。



UDP 的 Header。



TCP 的 Header。

可靠性	可靠	不可靠
速度	慢	快
傳輸方式	封包按順序傳輸	封包以串流方式傳輸
錯誤檢查與修正	有	無
壅塞控制	有	無
確認	有	只有檢查碼

8. 請簡要說明 chap 28 中，任五種網路安全弱點以極可能攻擊手法。

(1)Code-Execution Intrusion

利用漏洞攻擊系統的一個執行檔。通常配合社交攻擊利用有趣的檔案名稱來欺騙使用者開啟執行檔，並進行攻擊。

攻擊的案例：

莫里斯蠕蟲，莫里斯蠕蟲是第一隻非實驗室製造出來的蠕蟲，它利用 Unix 系統中幾項程序的已知漏洞進行傳播感染，以 C 語言撰寫。在當時感染了大約 6000 台 Unix 計算機， 美國的政府審計辦公室估算出該蠕蟲造成的損失為 1000 萬至 1 億美元。

(2) Stack Buffer Overflow

利用電腦程式把數據寫入內存時超出了資料結構的邊界。這會損壞相鄰數據的值，引發程序崩潰或者修改了函數返回地址從而導致執行惡意的程序。在被寫入的的相鄰區域，攻擊者可以寫入想要的東西，通常是 shellcode 讓攻擊者有權限控制電腦。

(3) Heap Buffer Overflow

跟上面得攻擊方式屬於同種攻擊，先造成緩衝區溢位後改變程序的流程，讓電腦執行攻擊者寫的代碼。

(4) Cross-Site Scripting (XSS)

XSS 攻擊是透過網也開發時留下的漏洞，透過某些手法將惡意指令注入網頁，讓使用者執行攻擊者製造的網頁。

(5)SQL Injection

利用程式的缺陷來改變 SQL 查詢的指令來達到攻擊者的需求，通常是獲取更高的權限或是獲取想要的資料。

9. 請簡要說明網路管理有哪些議題。

Fault(錯誤管理)：

錯誤管理的目的就是減少問題被客戶抓包的機會，利用監控的服務去監控網路、伺服器和其他的硬體是否有正常運作，並且監控外網能夠存取的資源，確保長時間或距離比較遠的連線能夠穩定，在錯誤時也可以馬上替換上正常工作的設備，盡量增加服務的容錯率和穩定性。

Configuration(組態管理)：

組態管理的目的是為了實做某個特定功能或讓網路性能達到最優，這包括設計拓樸、選用最適合的交換器和路由器、並且在未來需要變更到架構或設定的時候，讓服務可以最快達到最佳的狀態。

Accounting(會計管理)：

會計管理會紀錄及分析系統的資源占用，讓系統運行的成本及效率達到比較良好的平衡，並且在用戶需要使用多個網路環境時，計算總共費用。

Performance(效能管理)：

在錯誤管理之後，又發展出了效能管理，一個系統沒有錯誤管理和效能管理的話，就稱不上是一套系統，效能管理能夠讓使用者知道目前網路的使用效率。

Security(安全管理)：

安全管理是控制使用者對網路硬軟體設備的登入過程，也就是權限的控管，來避免惡意的使用者接近並且使用資源。

10. 請簡要說明 QUEUING 和 SCHEDULING 是要解決網路甚麼問題。

QUEUING 和 SCHEDULING 是為了解決每個使用者所使用到的頻寬不同的問題。在網路中實現這些流量管理是透過排隊機制，讓每個使用者可以拿到差不多的頻寬。