《資通網路》

試題評析	今年考題在名詞解釋上有較重的配分，且當中包含寫出英文全名或以英文名稱作為專有名詞之表示方式，此外，時事相關之資訊安全議題亦為考點，整題而言難易度不高，細心準備之同學應可得80分以上。

一、目前在網際網路上有電腦遭遇到勒索病毒（Ransomware）感染，請說明什麼是勒索病毒？（10分）

試題評析	本題為資訊安全時事考題，考點為近日來日益嚴重之勒索軟體，課堂中於資訊安全部分亦有提及，同學應可順利應答。
考點命中	《高點・高上資通網路講義》第四回，石濟編撰，頁2以下。

答：

勒索軟體(Ransomware)會將被害者電腦資料透過加密技術加密為無法讀取之密文，企業或個人用戶若欲還原原本之內容必須支付相當高額之「贖金」才可，而此種軟體大多透過社交工程術欺騙用戶，如：釣魚郵件或廣告等方式，若被害者拒絕支付贖金，則可用以解密之金鑰將於數天內銷毀，被加密之資料將難以還原。

二、下列為網際網路常見的網路術語，請寫出它們的英文全名。（每小題3分，共15分）

(一)SSID

(二)IPS

(三)IPSec

(四)AES

(五)PGP

試題評析	本題為基本之名詞解釋，課堂中均有提及，同學應可順利應答。
考點命中	1.《高點・高上資通網路講義》第四回，石濟編撰，頁9以下。 2.《高點・高上資通網路講義》第四回，石濟編撰，頁18以下。

答：

(一) Service Set Identifier

(二) Intrusion Prevention System

(三) Internet Protocol Security

(四) Advanced Encryption Standard

(五) Pretty Good Privacy

三、一般電腦必須要有IP位址才能上網，而IP位址分配有固定IP設定與DHCP。

(一)請問DHCP英文全名為何？（5分）

(二)請詳細說明DHCP運作原理，即DHCP Client與DHCP Server之間的互動與傳遞訊息為何？（15分）

試題評析	本題為應用層中常見之考題，課堂中已有提及，同學應可順利應答
考點命中	《高點・高上資通網路講義》第三回，石濟編撰。

【版權所有，翻印必究！】

答：

(一)Dynamic Host Configuration Protocol

(二)動態主機配置協定可以讓區域網路中的電腦自動取得IP位址，並提供管理者中央控管的機制。而搭配與網路位址轉換一同使用的原因在於動態主機配置協定指派IP時，可通知網路位址轉換以更新轉換表以維持一致的內容。

當有新的設備在動態主機配置協定伺服器所處的區網內需要取得新的IP位址時，可透過發送廣播封包索取服務，該封包只有動態主機配置伺服器會給予回應，其他主機收到後將直接捨棄。伺服器收到該廣播封包後，將回傳相關設定資訊，包含幾個重要內容：(1)可使用的IP位址與可用時間、(2)預設閘道器的位址、(3)子網路遮罩。由於動態主機配置協議採取租約的概念，因此回傳時會指明可用時間，但詳細而言可分為二種分配方式：

1.自動分配(Automatic Allocation)

一旦設備第一次成功的從動態主機配置協定伺服器取得IP位址後，到使用結束前都使用該位址。

2.動態分配(Dynamic Allocation)

當設備第一次從動態主機配置協定伺服器端取得IP位址後，並不能永久的使用該位址，當回傳時所規定的時間到期，設備就必須釋放該IP位址，供其它設備使用。不過設備也可以延續(Renew)租約，或是重新租用其它IP位址。

上述的廣播封包在啟動任何網路連線之前就會發送，當設備不需要此IP位址時，會將該IP位址還給動態主機配置伺服器，以供其他設備使用。設備從動態主機配置協定伺服器取得IP位址以及相關網路設定的過程，可分為四個主要步驟：

1.尋找(Discovery)

此為設備端發起尋找動態主機配置伺服器的要求，透過廣播等待回應，若網路規模較大時，管理者會因效率考量佈建一個或多個動態主機配置伺服器的代理人(DHCP Relay Agent)，避免使用者向整個網路發送廣播封包，當代理人收到設備的廣播封包時，會將該需求轉送給動態主機配置伺服器，待伺服器處理完後，將結果回傳至代理人，代理人再轉發給設備。

2.提供(Offer)

當動態主機配置伺服器收到設備端發送的尋找封包後，便會回傳IP位址資料以及相關網路設定資料(如：子網路遮罩、使用期限、預設閘道器位址以及動態主機配置伺服器位址等)。

3.要求(Request)

當設備收到上一階段的封包後，便可得知目前提供服務的動態主機配置伺服器位址，但此階段設備仍然以廣播的方式發送封包，因為必須讓其他的動態主機配置伺服器或是代理人知道該設備已經取得服務。

4.確認(Acknowledge)

這是整個流程的最後一步，設備端回報確認IP位址的使用期限以及其他的設定資料。

以上是動態主機配置協議的主要內容，此協議運作時伺服器端透過用戶資料協議(User Datagram Protocol, UDP)的67埠與使用者端的68埠溝通，因此該協議運作在應用層而非網路層。

四、一般網路位址分配指派分為CIDR與Classful Addressing。

(一)請說明CIDR是如何分配網路位址區塊？（10分）

(二)請說明Classful Addressing是如何分配網路位址區塊？（10分）

試題評析	本題為網路層IP常見考題，同學應可順利應答
考點命中	《高點・高上資通網路講義》第四回，石濟編撰，頁2以下。

答：

【版權所有，重製必究！】

(一)由於高等級網路數量有限，租金較昂貴，且空間甚大，可能無法充分利用，因此衍伸出與切割子網路相反的方式，將多個較低等級的網路合併為一個規模較大的網路。達到這項目的的方法同樣是使用子網路遮罩，利用子網路遮罩重新定義較短的網路位址，也就是從網路位址借幾個位元做為機器位址，以便將現有2的冪次方個較小的網路合併為一個較大的超網路 (Supernet)。

舉例而言，若一個企業需要2,000個IP位址，該數量介於Class B可提供的65,535個與Class C可提供的255個IP位址之間。若直接申請Class B的IP則浪費非常多的空間，透過無類別跨網域路由的方式，分配一個網路位

址為21位元，主機位址11位元的IP，總共可容納2^{11} = 2,048個主機，與所需的2,000個IP位址數量較相近。

上例是將一個Class C的IP位址借3個位元給機器位址，等同於合併了2^3 = 8個Class C的網路，但必須使用連續的Class C網路位址進行合併，且合併的網路數量必須是2的冪次方。

將IP位址搭配子網路遮罩以切割子網路或合併為超網路，達到彈性分配目的的技術稱為無等級的IP位址(Classless IP)或稱無類別跨網域路由(Classless Inter-Domain Routing, CIDR)。

(二)Classful Addressing是網際網路初提出時採用的分類方法，設計IP時，考量到管理上的需求，因此制定了IP位址的等級 (Class) 。雖然此種規劃方式將導致位址不足的問題，但了解IP位址等級的內容，仍是必要的課題之一。IP位址除了從輸入的觀點將之分為四個部分之外，若以等級為依據，可切分成網路位址與主機位址兩部份，不同等級的IP其網路位址和主機位址長度亦有所差異。網路位址位於整體的前段，用以識別所屬的網路。當組織或企業申請IP位址時，所分配到的通常是連續的網路位址。同一網路上的所有裝置，都會有相同的網路位址。至於主機位址，則位於IP位址的後段，同一網路上的裝置間則是以主機位址來區別。

然而網路位址與主機位址間長度的分配是一個相當重要的取捨，若給予網路位址較長的長度，則主機位址長度勢必較小。舉例而言，若分配24個位元給網路位址，則主機位址便只剩8個位元，換言之，此網路下僅可容納2^8 = 256台設備。反之，若網路位址長度較短，假設為16個位元，則主機位址便有16位元可供使用，亦即此一網路位址下可有2^{16} = 65536台不同的設備。

就管理的角度而言，大型的網路應使用較短的網路位址，以容納更多的主機位址；較小的網路則應該使用較長的網路位址，避免浪費主機位址。因此衍伸出了IP位址的等級。此等級共分五種，但一般最常用到的僅為Class A、B、C三類的位址。這三種等級分別使用不同長度的網路位址，因此適用於大、中、小型網路。管理者可依據網路規模，給予適當等級的IP位址。

```
Class A
  0.  0.  0.  0 = 00000000.00000000.00000000.00000000
127.255.255.255 = 01111111.11111111.11111111.11111111
                  0nnnnnnn.HHHHHHHH.HHHHHHHH.HHHHHHHH

Class B
128.  0.  0.  0 = 10000000.00000000.00000000.00000000
191.255.255.255 = 10111111.11111111.11111111.11111111
                  10nnnnnn.nnnnnnnn.HHHHHHHH.HHHHHHHH

Class C
192.  0.  0.  0 = 11000000.00000000.00000000.00000000
223.255.255.255 = 11011111.11111111.11111111.11111111
                  110nnnnn.nnnnnnnn.nnnnnnnn.HHHHHHHH

Class D
224.  0.  0.  0 = 11100000.00000000.00000000.00000000
239.255.255.255 = 11101111.11111111.11111111.11111111
                  1110XXXX.XXXXXXXX.XXXXXXXX.XXXXXXXX

Class E
240.  0.  0.  0 = 11110000.00000000.00000000.00000000
255.255.255.255 = 11111111.11111111.11111111.11111111
                  1111XXXX.XXXXXXXX.XXXXXXXX.XXXXXXXX
```

五、(一)在802.11標準中，AP（Access Point）會定期送出Beacon Frame，請問Beacon Frame包含何種資訊及其用途。（5分）

【版權所有，重製必究！】

(二)對於AP掃瞄（Scanning）分為主動掃描（Active Scanning）與被動掃描（Passive Scanning），請說明兩者運作模式。（10分）

試題評析	本題為無線網路相關考題，Beacon為無線網路連線起始溝通時使用之方法，同學應可順利應答。
考點命中	《高點・高上資通網路講義》第二回，石濟編撰，頁23以下。

答：

(一)Beacon封包內包含SSID訊息、支援的傳輸速率以及此AP的MAC位址等連線相關資訊。

(二)1.主動掃描：代表設備以主動的方式，在每個通訊頻道發出Probe Request frame，請求某個特定無線網絡予以回應。主動掃描是主動尋找網絡，而不是靜候無線網路通知本身的存在。使用主動掃描的設備將使用以下的方式掃描頻道表中列出的頻道：

(1)跳至某個頻道，並等候通知（indication of an incoming frame）或等到Probe Delay timer逾時。若在某一頻道收到frame，即代表該頻道有用戶使用，故可加以探測。而定時器可用來防止某個閒置頻道使整個過程卡住。

(2)利用基本的DCF方式取得媒介使用權，而後送出一個Probe Request Frame。

(3)等候至少一段最短的頻道時間（即Min Channel Time）。

a.若媒介並不忙碌，表示沒有網絡存在，故可跳至下個頻道。

b.若在Min Channel Time期間中媒介非常忙碌，就繼續等候一段時間，直到最長的頻道時間(即Max Channel Time)逾時。

2.被動掃描：

目前大部分移動式電子產品皆採被動掃描(passive scanning)的方式，因掃描過程中不需傳送任何訊號，故可節省電力。被動掃描中，裝置會在頻道列表所列的各個頻道間不斷切換，並靜候Beacon Frame。Beacon在設計上是為了讓工作站知道加入某個基本服務集(Basic Service Set, BSS)所需的參數，以便進行通信。

六、請回答下列問題：（每小題5分，共20分）

(一)什麼是Piggybacked Acknowledgement？

(二)什麼是Cumulative Acknowledgement？

(三)什麼是Premature Timeout？

(四)承(三)題，該如何降低Premature Timeout的發生？

試題評析	本題為網路層和傳輸層相關之名詞解釋，大多數課堂中皆已提及，同學應可順利應答。
考點命中	1.《高點・高上資通網路講義》第二回，石濟編撰。 2.《高點・高上資通網路講義》第三回，石濟編撰。

答：

(一)當frame到達接收端時，並不會馬上送出Acknowledgement Frame，而是等到接收端的有訊息要送給發送端時，把Acknowledgement附加在要送出的frame中。

(二)接收端收到資料時不需要每個訊息都回應確認訊息，一個確認訊息可同時確認多個先前發送出的訊息已成功由接收端接收，如：TCP採用之方法。

(三)TCP在RTT中使用一個timer計時，在time out後認定該訊息已漏傳，而該計時器逾時之閥值比實際之RTT為大，因一旦該閥點設的太小，會造成premature timeout，對方只是慢了一點就被判為timeout重送，造成頻寬浪費。

(四)將過去的RTT時間做一個平均，實際的計算公式為：

過去幾次測到的實際RTT平均值乘上一個常數α加上前次預估的RTT時間乘上(1-α)，α是0~1之間的一個數(α = 0.125)，EstimatedRTT = (1-α)*EstimateRTT + α*SampleRTT

公式中預估的佔0.875，實際的佔0.125，所得即為最新的EstimatedRTT。

因為timeout要確保真的比RTT還要大，而公式出來的是平均值，因此預估出的值還要加上一個標準差，做一個緩衝區 (safety margin)，故：

DevRTT = (1-β)*DevRTT + β*|SampleRTT-EstimatedRTT| (TCP裡設定β=0.25)

和前一個預估的公式類似，DevRTT利用前次算出之DevRTT和實際RTT與預估值相減所得之值合併，所得之變異數為4倍，因此，最後的Timeout Interval = EstimatedRTT + 4*DevRTT，才是Timeout的設定值。

【版權所有，重製必究！】