《資通網路與安全》

一、某系所的網管人員於配置實驗室網路時，有設定每一台主機IP位址，但無法與同網段其他主機通訊，分析結果顯示是因為ARP封包無法正確解析，請說明ARP協定運作原理與流程。因為人工設定IP位址，若IP相衝會發生什麼結果？網管者如何檢測是否有IP位址相衝現象發生？（25分）

試題評析	ARP進階考題。
考點命中	《高點・高上資通網路與安全講義》第三章，張又中編撰，頁3-17、頁3-32~37。

答：

位址解析協定(Address Resolution Protocol, ARP)為主機可透過ARP協定來以IP位址詢問其實體位址(Physical Address)。例如：主機A欲查詢主機C的實體位址，主機A會先查詢自己的ARP Cache，發現沒有主機C的紀錄後，主機A將ARP Request包裝於Ethernet訊框，以廣播送出依主機C的IP查問其實體位址，主機C收到後回應其實體位址。

人工設定IP位址，若IP相衝可能發生以下結果：

(1)ARP對應混亂

其他主機在解析該IP位址時，可能取得不同的實體位址回應，造成ARP表中的IP→MAC映射反覆變動。

(2)通訊不穩定

因為封包有時被送到A主機，有時送到B主機，導致網路間歇性斷線。

(3)網路故障

如IP位址衝突發生於閘道器(Gateway)或重要網路設備，可能造成網段大規模故障。

網管者檢測IP位址相衝作法如下：

(1)觀察ARP表

以arp -a指令查看ARP表，若同一IP位址對應的實體位址不斷改變或出現異常，可能為IP衝突。

(2)IP位址偵測

以ping指令探測該IP位址是否已被使用，若有人回應則可能發生IP位址衝突或已被占用。

(3)掃描盤點網段IP、MAC清單

掃描全網段，整理IP、MAC對照表，比對是否有同IP位址對應不同實體位址。

(4)監控網路設備

如於交換器(Switch)上觀察MAC漂移(MAC Flapping/Move)，也可定位衝突所在。

二、某研究中心將IPv4網段192.168.10.0/22，分配給5個研究部門使用。請問每個研究部門可使用的IP數量為何？子網路遮罩（subnet mask）為何？若後續增加3個研究部門，請問舊有的研究部門可用的IP數量和子網路遮罩是否需要更動？（25分）

試題評析	子網路切割與遮罩。
考點命中	《高點・高上資通網路與安全講義》第三章，張又中編撰，頁3-12~13。

答：

(一)主機位元(Host Bits)為32-22=10位元，此意味需要從主機位元再借3個位元來做子網路切割，故每個研究部門可使用的IP數量為2^7-2=126(扣除主機位元全0及全1的網路表示及廣播)，子網路遮罩為255.255.255.128。

(二)另因已切割3個位元的子網路，故可提供2^3=8個子網路使用，符合題敘分配給5個研究部門使用，即使後續增加3個研究部門，舊有的研究部門仍不需變動可用的IP數量和子網路遮罩。

三、為提升資通訊系統之安全性，某政府組織導入SSDLC（Secure Software Development Life Cycle）。請說明SSDLC之開發流程，並說明其效益。（25分）

試題評析	近年熱門之安全系統開發生命週期考題。
考點命中	《高點・高上資通網路與安全講義》第八章，張又中編撰，頁8-43~46。

答：

此為賴溪松教授提出，在考量系統功能性的同時導入安全性的思維，於系統開發之初進行各項必要的安全防護

措施，雖然拉長了設計的時程，卻降低了系統後續維護的成本，以及遭受到攻擊行為的損失。
SSDLC開發流程如下：
(1)定義(Define)
配合相關人員的期望進行各項資安措施的分析與規劃，於符合成本考量下達成安全需求。
(2)設計(Design)
需考量系統任務目標、功能關聯、邊界範圍、各階層使用者的角色等各項內容，建立相關的控管程序及防護措施，作為程式實作階段的基礎。
(3)開發(Development)
為資安防護實作最為重要的一環，需針對各項可能的入侵手法考量其中的漏洞及威脅，建立層層的防護機制。
(4)測試(Test)
考量目前系統內各項控管程序與防護措施，是否能夠有效的防禦目前已知的攻擊手法，並依據測試結果進行必要的調整。
(5)部署(Deployment)
考量系統部署後，各項安全控管機制與防護措施的運作狀況，確保其正常無誤；另外，亦需針對委託單位相關員工，進行適當的資安教育與操作訓練。
(6)維護(Maintain)
著重於資安防護措施的持續維護以及變更管理，考量廠商的技術能力並掌控系統原始程式碼。
(7)變更(Change)
在資訊安全考量下，系統發展的各個階段均可能不斷地面臨資安威脅的挑戰。

四、某組織規劃將資訊系統遷移至公有雲平台。搬遷前應評估資安風險，並採取必要措施以降低資安風險。請說明降低雲端資安風險之措施，並比較公有雲和私有雲在資安管理之差異性。（25分）

試題評析	公有雲與私有雲之分析與比較。
考點命中	《高點・高上資通網路與安全講義》第一章，張又中編撰，頁1-6。

答：
(一)公有雲(Public Cloud)又稱外部雲(External Cloud)。
服務供應商提供極精細的IT資源動態配置，並透過Web應用提供網路自助式服務。所有IT資源皆由其供應，須具備資源監控與評量等機制，才能如公用運算(Utility Computing)般計價。對中小型企業而言，公有雲提供了最佳IT運算與成本效益的解決方案；但對有能力自建資料中心的大型企業來說，公有雲難免仍有安全與信任上的顧慮。
(二)私有雲(Private Cloud)又稱內部雲(Internal Cloud)。
IT資源與所提供的服務都由組織內部管理，且限制於企業內部使用，提供更高的安全掌控性，同時內部IT資源不論在管理、調度、擴展、分派、存取控制與成本支出上都更具精細度、彈性與效益。私有雲的優點為導入虛擬化、環保節能、節省IT預算，且實現集中化的軟硬體管理，精簡人力。