《資通網路與安全》

一、對於TCP/IP網路的各項運營管理工作，IP表頭（IP Header）內各項欄位的識別是很重要的基礎知識，請詳細說明下列IP Header欄位的用途：（每小題4分，共20分）

(一) Total length

(二) Identification number

(三) Fragmentation offset

(四) Time-to-live

(五) Protocol

試題評析	本題屬網路層之IP標頭定義，學員可參考講義內容作答。
考點命中	《高點・高上資通網路講義》，張又中編撰，頁3-23~25，第3章。

答：

(一)封包總長度(標頭+資料)，範圍：576~65535 Bytes。

(二)資料段(Fragmentation)的識別編號，屬同一資料段會有相同識別值。

(三)目前分段在原始資料之位置，預設值為 0。

(四)每經過 1 個 Hop 時減 1，當值為 0 時丟棄該封包。

(五)目前承載的資料屬於那一個通訊協定。

二、5G行動網路日益普及，且除了5G公共服務外還提供 5G企業專用網路。請問：（每小題10分，共20分）

(一)相較於4G，5G行動網路的特點有那些？請詳細說明之。

(二)企業採用5G行動專網帶來的安全風險有那些？請條列並說明之。

試題評析	因應2023年6月1日我國數位發展部制訂「行動寬頻專用電信網路設置使用管理辦法」之考題。
考點命中	《高點・高上資通網路講義》，張又中編撰，頁5-53~54，第5章。

答：

(一)下一代行動網路聯盟(Next Generation Mobile Networks Alliance)定義5G如下：

1. 以 10 Mbps 資料速率支援以萬為單位之用戶。
2. 以 10 Mbps 資料速率支援都會區。
3. 以 1 Gbps 資料速率支援給在同一辦公室樓層的許多人員。
4. 支援以十萬為單位的無線感測器之同步連結。
5. 頻譜效率比 4G 更好。
6. 覆蓋率提高。
7. 強化訊號效率。
8. 延遲比 LTE 顯著降低。

(二)5G行動專網的資安風險有：

1. 整合存取及身分管理
   除了使用 SIM 或 eSIM 認證終端設備外，也要對終端設備進行其他認證，避免非授權終端設備連至 5G 專網。
2. UPF(User Plane Function)流量控制管理
   UPF 負責使用者流量控制、封包路由以及 QoS，故需確保 MEC(Mobile Edge Computing)至核心網路間所有元件的安全性，以確保流量安全。
3. 持續即時監控營運及登入
   需持續的即時監控營運及登入是否出現異常，包括時刻追蹤組態設定、偵測威脅，並確認安全控管措

施，評估安全團隊預防或快速應對資安威脅的能力。

4. 第三方代管 5G 核心網路與邊緣運算

受委託的第三方需可信任且具備足夠的資安與管控能力，可以確保 5G 核心網路與邊緣雲安全，並保護客戶的資料隱私。

三、DNS（Domain Name Service）是重要的網路服務，請回答下列有關DNS問題：

(一)何謂Zone file？請說明其用途及內容。（5分）

(二)請說明迭代式DNS查詢（iterative DNS query）的工作原理。（10分）

(三)當SOC（Security Operation Center）對受管理組織下某台主機發出「DNS Open Resolver弱點」的告警訊息時，代表後者可能存在的資安危害為何？請說明之。（5分）

試題評析	本題為DNS運作及其相關資安議題，亦屬熱門題型之一。
考點命中	1.《高點・高上資通網路講義》，張又中編撰，頁4-4~7，第4章。 2.《高點・高上資訊安全實務講義》，張又中編撰，頁3-6~7，第3章。

答：

(一) DNS server 內每個網域名稱皆有自己的檔案，這個檔案即稱為區域檔案(Zone file)，其用途將 DNS 網域名稱對應到指定類型的資源資訊，供網域名稱空間登錄或解析。

(二) 一般多用於伺服器對伺服器之間的查詢動作，如同對話一樣，在 DNS 伺服器的往來之間重覆查詢而成。簡而言之，迭代式 DNS 查詢的動作即為 DNS 伺服器回應：「此處無資料，請至他處查詢」，經多個 DNS 伺服器皆是相同回應，如同一來一往的反覆動作。

(三) Open DNS Resolver 弱點係指 Caching Recursive DNS 伺服器對外公開提供名稱遞迴解析服務，可能存在的資安危害有：

1. 發生暫存中毒(Cache Poison)。
2. 易被攻擊或耗損系統及網路資源。
3. 易被利用發動DoS或DDoS攻擊。

四、零信任架構（Zero Trust Architecture, ZTA）是目前政府大力推動的資訊安全架構：（每小題10分，共20分）

(一)請詳細說明ZTA的概念和推動ZTA的動機。

(二)實現ZTA的核心機制有那些？請條列並說明之。

試題評析	零信任架構為政府近期大力推動的資訊安全架構，屬熱門題型，學員需多加留意。

答：

(一)依據國家資通安全研究院之定義，零信任主要目的是解決現今網路環境複雜造成信任邊界不明之資安窘境，期望透過對任何資料存取皆永不信任且必須驗證的原則，達成不論在何時何地存取資料皆保證一致安全性之相關技術。

1. ZTA的概念：
   (1)不是保護網路存取，而是保護資料/應用存取。
   (2)無具體邊界，使用者/設備與資料/應用無處不在。
   (3)任何資料存取永不信任且必須驗證。
2. 推動ZTA的動機
   (1)依據「國家資通安全發展方案(110 年至 113 年)」之「善用智慧前瞻科技、主動抵禦潛在威脅」推動策略，發展零信任架構資安防護環境，推動政府機關導入零信任架構，以完善政府網際服務網防禦深廣度。
   (2)導入零信任架構是一段逐步成熟之過程，不是一次大規模替換基礎架構與存取流程，且與傳統模式會同時混合運作。
   (3)藉由提供導入建議，協助政府機關實施零信任架構，強化資安防護能力。

(二) 目前參考美國國家標準暨技術研究院(National Institute of Standards and Technology, NIST)零信任架構，同時結合向上集中之防護需求，採取資源門戶基礎部署方式(Resource Portal-Based Deployment)，包含下列 3 大核心機制：
1. 身分鑑別：多因子身分鑑別與鑑別聲明。
2. 設備鑑別：設備鑑別與設備健康管理。
3. 信任推斷：使用者情境信任推斷機制。

五、防火牆（Firewall）是當今企業常見的安全防護設備，請問：
(一)企業常用防火牆隔離出一個網段，稱為DMZ（Demilitarized Zone），請詳細說明其用意為何。（5分）
(二)WAF（Web Application Firewall）和傳統的封包過濾式防火牆（Packet filtered Firewall）有何不同？請詳細說明。（10分）
(三)防火牆常根據從外部收到的IOC（Indicator of Compromise）來做規則調整，請問IOC的意義為何？（5分）

試題評析	本題為資訊安全之防火牆種類及安全網路架構之題型。
考點命中	《高點・高上資通安全講義》第二回，金乃傑編撰，頁14～28，第三章防護架構，二、防火牆（Firewall）與相關技術。

答：
(一) DMZ（Demilitarized zone）是介於內外路由器間的區域，用於放置組織對外重要的伺服器。DMZ 照字面直翻是指非軍事區域，而電腦網路中 DMZ 可以解析為一個既不屬於內部網域同時也不屬於外部網域的一個特殊區域，其目的就是了為防止外來入侵者直接存取內部機密資料，針對不同資源而提供不同安全級別的保護區域。一般企業將網路伺服器放在 DMZ 供網際網路使用者查詢使用，這些伺服器無法連接到內部資料，因此如果不幸被外來入侵者侵入，重要的資料仍不至於外洩。
(二) WAF（Web Application Firewall）提供應用層的訊息過濾與轉送處理，主要依據應用層的資訊來決定是否放行封包流量。與傳統的封包過濾式防火牆相較，WAF 可過濾傳送的資料內容與命令，確保應用層協定的安全；亦可過濾封包內容與命令，阻斷針對應用協定的攻擊。
(三) IOC 為電腦鑑識中的工具器物(Artifact)，其可從網路或作業系統中觀察，與電腦入侵高度相關。傳統的 IOC 包含病毒特徵、IP 位址、惡意檔案的 MD5 雜湊值，或是殭屍網路(Botnet)命令與控制伺服器的網址或網域名稱。通過事件回應與電腦鑑識的處理過程識別 IOC 後，其可用於入侵檢測系統(Intrusion Detection System, IDS)與防病毒軟體，對未來的攻擊嘗試進行早期檢測。