Cisco Aironet 無線區域網路安全防護架構

為何需要無線區域網路？

無線區域網路（Wireless LAN; WLAN）正迅速改變電腦及網路界，隨著筆記型電腦與個人數位助理（PDA）等行動運算裝置日漸普及，以及使用者亟於擺脫有線的束縛，使現代企業開始採用並廣泛部署WLAN環境。

目前全球有許多企業安裝覆蓋範圍廣、獨立式且無線的WLAN網路環境，以提高員工生產力。藉由使用WLAN，網管人員可輕易移除、新增，並改變網路部署。此外，WLAN具備絕佳運作彈性，可克服老舊建築、租用空間，或是臨時工作環境佈線不易的問題。

使用者可透過WLAN存取電子郵件、安排會議行程，並且可在會議室、教室、辦公室，以及校園中任何地點，存取企業或大學網路中的檔案與應用。有了無線網路，不論使用者身在何處，都可隨時掌握重要的資訊與應用。

WLAN安全考量

當使用者越來越依賴WLAN，企業對於安全的疑慮也隨之升高，因此在提供使用者便利性與行動力的同時，網管人員必須確定駭客無法任意入侵WLAN，或攔截WLAN中傳輸的資訊。

WLAN透過無線電波以廣播（Broadcast）方式傳送資料，因此任何位於無線存取器（Access Point; AP）服務範圍內的WLAN用戶端裝置，皆可在此區域收送資料。由於無線電波可穿透天花板、樓面，以及牆面，因此位於其他樓層或大樓外的無心人士，也可接收網路中傳送的資料。由此可知，WLAN掙脫網路疆界的束縛，卻促成網路安全更多的威脅。

WLAN需配合嚴格的安全防護工具，否則整體企業網路將完全曝露在外。因為這些安全性的考量與無線網路加密機制（如WEP）的效能低落，使許多企業遲遲不願部署WLAN。許多研究報告指出，靜態WEP　密鑰存在許多安全漏洞；此外，駭客已成功使用AirSnort等工具破解WEP密鑰，並監視與分析封包中的資料。

啓動WLAN安全防護

為消除WLAN可能遭遇的威脅，網管人員須為整體網路建立堅固防護措施，但保護WLAN安全只是安全架構中的一環，其他要件尚包括防火牆、入侵偵測系統（IDS），以及網路區段規劃，皆應納入網路設計的整體考量。

此外，網管人員必須啓動WLAN安全防護機制，因為駭客可攔截未啓動防護機制的網路資訊。思科系統建議，企業在挑選與部署WLAN安全解決方案之前，應先執行網路風險評估。

傳統WLAN安全機制

和其他類型網路一樣，WLAN安全防護著重於存取控制與隱私保護。存取控制可避免未經授權的使用者擅用Access Point，並確保合法用戶端裝置連結可信任的Access Point。隱私保護則確保唯有預先設定的使用者才能解讀傳輸資料；此防護機制會將資料加密，只有預設的使用者才能使用密鑰將資料解密，以保護資料隱私性。

傳統WLAN安全保護機制包括Service Set Identifier（SSID）、開放系統認證（Open System Authentication）與分享密鑰認證（Shared-Key Authentication）、WEP，以及媒體存取控制（MAC）等。這些機制如果單獨使用很容易被駭客破解，但將其搭配使用，則可提供存取控制與隱私保護的能力。

IEEE專為WLAN發展的802.11標準，支援兩種用戶認證方式：開放系統認證與共享密鑰認證。使用者只需提供正確SSID即可完成開放系統認證；而共享密鑰認證則要求Access Point傳送Challenge Text Packet至用戶端裝置，用戶端裝置再將WEP加密後傳回Access Point。如果用戶端裝置使用錯誤的密鑰或無密鑰，則認證失敗，且不得連結Access Point。此外，當駭客偵測到共享密鑰訊號以及加密後之訊號，便可將WEP解密，所以共享密鑰認證的安全性不足。

如果使用開放系統認證，即使用戶端可完成認證並連結Access Point，仍可使用WEP阻止用戶端傳送與接收資料，除非用戶端提供正確WEP密鑰。

靜態WEP密鑰是另一種常用但安全性不佳的密鑰，網管人員需手動方式設定，並在Access Point與所有用戶端裝置中設定此密鑰，此機制可分為40-bit與128-bit兩種加密長度。如果使用靜態WEP密鑰，網管人員則需重複在所有WLAN裝置中使用相同的設定。

如果使用靜態WEP密鑰的裝置遺失或遭竊，拾獲或持有此裝置的人便可存取WLAN，除非竊賊自首，否則網管人員是無法察覺未經授權的運作。一旦發現問題，與遭竊裝置使用相同WEP密鑰的裝置，都必須改變其靜態WEP密鑰。在擁有大量使用者企業的WLAN環境中，此工作極為費時費力。如果駭客用AirSnort這類工具破解靜態WEP密鑰，則網管人員根本無從得知密鑰是否已遭破解。

有些WLAN設備廠商使用MAC位址執行認證，即用戶端裝置MAC位址必須與Access Point認證表中位址相符，才能連上Access Point。MAC認證並非絕佳的安全防護機制，因為駭客可以偽造MAC位址，而網路卡也可能遺失或遭竊。

SSID、開放或共享密鑰、靜態WEP密鑰，或MAC認證等傳統WLAN安全機制並不足以保護企業網路安全。小型企業或禁止使用WLAN傳送重要資料的企業，可考慮使用這些傳統方案，但大型企業或機構則需部署更穩固的企業級WLAN安全防護解決方案。

思科無線網路安全套件（Wireless Security Suite）的優點

企業WLAN需要安全的企業級保護與管理性能，而WLAN解決方案則必須符合下列各點：

- 802.11標準
- 802.1X認證標準
- WEP密鑰管理
- 使用者與運作階段認證
- Access Point認證
- 非法Access Point偵測與定位
- 單點傳送（Unicast）密鑰管理
- 用戶端帳號記錄
- 防堵網路攻擊
- WLAN管理系統
- 作業系統支援

思科Aironet®系列產品使用思科無線網路安全套件，並提供兼具穩定性與效能的無線安全防護服務。此套件為網管人員提供企業級安全解決方案，使員工能在安全的網路環境中享有絕對的自由與行動力。

思科無線網路安全套件滿足企業對行動網路規劃的要求。此方案提供可擴充集中式安全管理，並支援動態WEP密鑰，以保護資料隱私性。其他特色包括雙向認證、訊息完整性檢查，以及每一個封包使用不同密鑰（Per-Packet Keying）等。

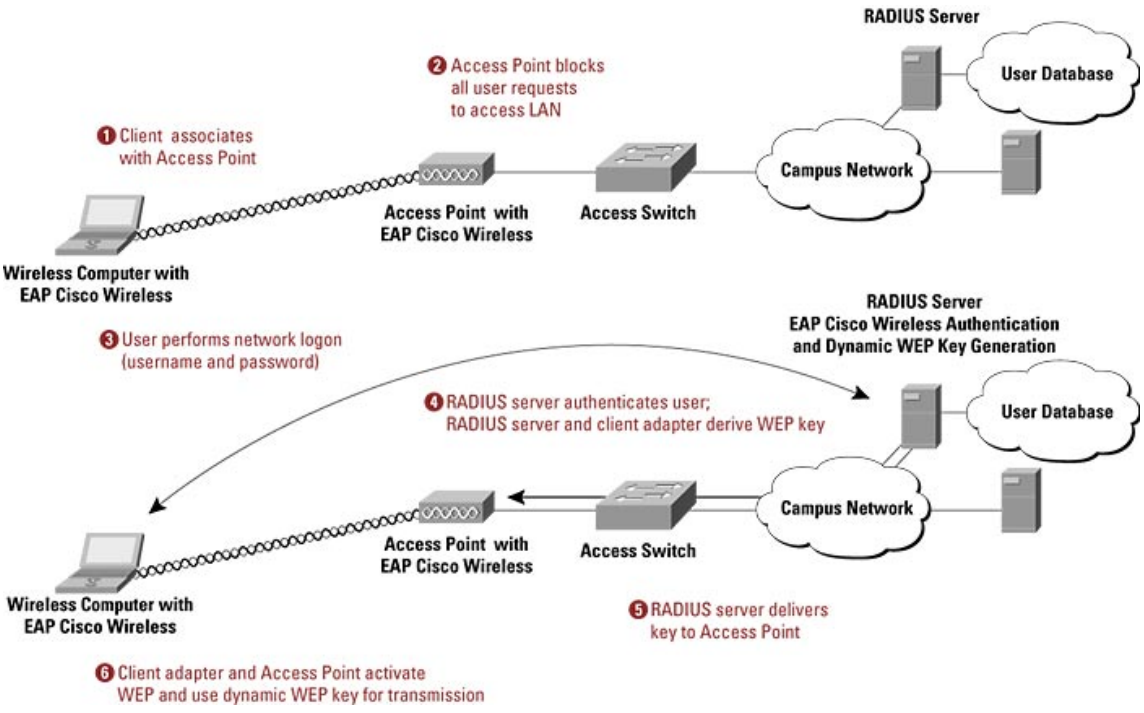
802.1X認證

IEEE已將802.1X訂定為有線與無線網路的新認證標準，使WLAN用戶端與認證伺服器間能夠進行雙向認證。此外，802.1X提供動態WEP密鑰，使網管人員負擔減輕，並解決因使用靜態WEP密鑰衍生的安全問題。

目前802.1X認證有多種類型，分別提供不同的認證方式，但卻以相同架構及延伸認證協定（Extensible Authentication Protocol; EAP）支援用戶端與Access Point間的通訊。

思科發展EAP Cisco Wireless（Cisco LEAP）的802.1X認證機制，並將其納入思科無線網路安全套件架構中。思科 Aironet產品同時支援Cisco LEAP及所有802.1X認證類型，包括EAP Transport Layer Security（EAP-TLS）。用戶端與RADIUS伺服器可使用Cisco LEAP和EAP-TLS等802.1X認證，以進行交互認證。

圖一：EAP Cisco Wireless（Cisco LEAP）雙向認證



如果使用傳統WLAN安全機制，任何位於WLAN網路中的使用者，都擁有此裝置的MAC位址與靜態WEP密鑰。假設某用戶端裝置遺失或遭竊，他人可毫不費力使用用戶端網路卡與MAC位址存取WLAN。Cisco LEAP 802.1X認證機制要求使用者輸入密碼以便進行用戶端認證，而非根據用戶端裝置認證，因此可將遺失裝置或網路卡的風險降至最低。

中間人（Man-In-The-Middle）認證攻擊

中間人認證攻擊指入侵者藉由攔截用戶端與Access Point間的認證訊息來發動攻擊，以便存取WLAN，此為封包攔截法的主動攻擊。中間人攻擊可趁機竊取企業資訊，並取得內部網路資源，進而暴露網路與用戶資訊。此外，尚包括服務阻斷（DoS）、傳輸資料損壞等。

以802.1X進行雙向認證可減輕中間人認證攻擊所帶來的威脅，並確保合法用戶端可連結經授權的Access Point。由於傳統802.11及MAC認證都是單向而非雙向認證，因此用戶端無法確定Access Point是否可信任。如果用戶端不小心連上非法Access Point並與之通訊，將導致網路威脅。利用雙向認證，用戶端會要求Access Point提出憑證，只有經授權的Access Point才能存取RADIUS伺服器以取得憑證。如果Access Point無法回應用戶端裝置的請求，將無法完成連線。

集中式WEP密鑰管理與政策式密鑰循環機制

集中管理WEP密鑰為802.1X認證的另一優點。完成雙向認證後，用戶端與RADIUS伺服器將產生相同WEP密鑰以便將所有傳輸資料加密，RADIUS伺服器使用有線網路連結將密鑰傳給Access Point，之後產生WEP密鑰。此外，根據Cisco ACS或Cisco Access Registrar RADIUS伺服器所定義的政策以決定連線時間長短。當連線有效時間截止，或用戶端已漫遊至其他Access Point，則需重新認證以產生新的密鑰。

暴力攻擊

傳統WLAN架構因使用靜態WEP機制而容易受到暴力攻擊的威脅。暴力攻擊發動時，駭客會不停猜測文字與數字以便找出WEP密鑰。

如果採用標準128-bit WEP機制，則駭客最多必須猜測2的104次方的組合。理論上，動態WEP密鑰仍然可能被暴力攻擊法破解，但卻大大提高其困難度。

TKIP WEP強化機制

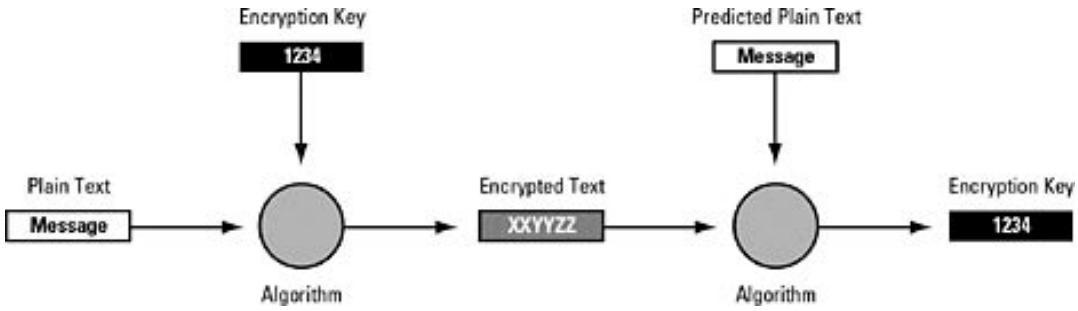
雖然802.1X和EAP認證為WLAN提供強大的認證功能，但還是無法抵擋網路攻擊。思科無線網路安全套件針對WEP密鑰提供多項強化功能，不論是靜態或動態WEP機制，皆需完成802.1X認證才能產生WEP密鑰，其功能包括尚未成為標準的Temporal Key Integrity Protocol（TKIP）、訊息完整性檢查（Message Integrity Check; MIC）、Per-Packet密鑰雜湊運算，以及Broadcast Key Rotation。

訊息完整性檢查（Message Integrity Check; MIC）防止主動網路攻擊

訊息完整性檢查可抵擋主動網路攻擊，這類攻擊須配合使用Bit-Flipping和Replay攻擊法，其攻擊過程如下：

- 駭客攔截WEP加密封包
- 駭客變動封包中位元，並重新計算完整性檢查值（Integrity Check Value; ICV）
- 駭客將內含初始向量（initialization vector; IV）的bit-flipped封包傳至Access Point
- 因為ICV無誤，Access Point開始接收並轉送封包
- Layer 3網路設備拒絕接收並送出可預期回應訊息
- Access Point將回應解密傳回駭客
- 駭客使用此回應產生密鑰

圖二主動攻擊：當駭客收到加密封包的資訊，即可找出密鑰，或稱串流式加密法（Stream Cipher），以便將訊息解密。



Per-packet 雜湊運算

如果Access Point和所有用戶端裝置已部署MIC機制，則發訊端在完成封包加密並開始傳送之前，會於封包中增加新位元組，而收訊端在收到封包後，則會進行解密並檢查MIC。如果封包中MIC與計算所得的數值（以MIC計算）相符，收訊端將接收封包；如果不符則將封包丟棄。

藉由使用MIC，在傳輸過程中遭非法竄改的封包將被丟棄。駭客不能使用Bit-Flipping或主動式Replay攻擊欺騙網路並完成認證，因為支援MIC功能的思科Aironet產品會找出並拒絕被修改封包。

Per-Packet 密鑰雜湊運算減輕“Weak IV”攻擊

使用WEP密鑰將傳輸資料加解密時，封包將內含24-bit初始向量，而且每一個封包的初始向量都不一樣。RC4 Key Scheduling演算法使用WEP密鑰產生初始向量，但此演算法有先天缺失，即是會產生Weak IV，因而透露基礎密鑰的資訊。駭客可使用AirSnort這類工具產生相同密鑰之封包，並使用Weak IV計算基礎密鑰，以找出安全漏洞。

思科無線網路安全套件支援TKIP演算法、密鑰雜湊運算，以及Per-Packet Keying。如果Access Point與所有用戶端裝置皆部署密鑰雜湊運算，則發訊端在送出資料前會先使用初始向量執行基礎密鑰雜湊運算，以便為每一封包產生新的密鑰。在每一封包都已使用不同密鑰加密後，密鑰雜湊運算可消除可預測訊息，以避免駭客藉由探測初始向量找出WEP密鑰。

Broadcast Key Rotation

思科無線網路安全套件可讓網管人員輪流使用Unicast密鑰與Broadcast WEP密鑰，並將廣播與多點傳送封包加密，而網管人員可輕易在Access Point中設定Broadcast-Key Rotation政策。此外，靜態Broadcast密鑰容易遭遇與Unicast或靜態WEP密鑰面臨的相同攻擊，因此為Broadcast密鑰提供Key Rotation Value以降低風險。

WLAN攻擊與減輕機制

表一列出常見的WLAN攻擊，以及減輕攻擊的機制及其效果。如表一所示，靜態WEP是所有防護機制中最脆弱的一種。與WEP搭配使用的Cisco LEAP可藉由雙向認證阻擋認證攻擊，然而，Cisco LEAP/WEP如未與思科無線網路安全套件中其他防護機制搭配使用，則很容易遭到Man-In-The-Middle及Fluhrer AirSnort WEP攻擊法的攻擊。使用電子憑證的EAP-TLS可有效減輕偽造認證、非法Access Point，以及暴力攻擊法帶來的衝擊。

而最右邊的思科無線網路安全套件解決方案可確實阻擋表中所列之所有網路攻擊—只有對字典攻擊法稍嫌薄弱，但可使用高強度密碼強化防禦力。

表一：WLAN減輕攻擊表

				Cisco Wireless Security Suite
攻擊	**靜態WEP**	**Cisco LEAP and WEP**	**EAP-TLS**	**Cisco LEAP, TKIP, Broadcast Key Rotation,MAC Authorization, and Per-packet Keying**
Man-In-The-Middle	脆弱	脆弱	脆弱	堅固
Authentication Forging	脆弱	堅固	堅固	堅固
Fluhrer（FMS Paper）	脆弱	脆弱	脆弱	堅固
Rogue Access Points	脆弱	堅固	堅固	堅固
Dictionary Attacks1	脆弱	堅固2	堅固2	堅固2

1. 字典攻擊法是一種暴力攻擊法。在發動字典攻擊時，網路駭客會使用一份已知的密碼清單，然後用不同排列組合試著猜出正確的密碼以存取網路。通常駭客會猜測簡單的使用者密碼或以密碼字典中的密碼來嘗試猜出密碼。
2. 需要高強度密碼

管理安全WLAN環境

網管人員正迫切尋找可提供無負擔安全管理的WLAN解決方案，以便減輕資訊人員的負擔。WLAN安全防護功能必須易於整合、管理、稽核，以及更新。

思科無線網路安全套件包含許多簡化WLAN管理與安全防護的強化功能，包括Cisco Wireless Utility Auto Installer、AAA RADIUS伺服器支援，以及RADIUS認證帳務記錄的能力。

無負擔安全防護

思科無線網路安全套件提供無負擔安全管理，以減少資訊人員的負擔。思科無線網路安全套件解決方案可容許網管人員自行選擇合適的保護方案，並提供穩固的全方位安全解決方案架構。利用此服務，網管人員無須管理靜態WEP密鑰，並可設定WLAN所需的重新認證功能。

思科無線網路安全套件支援各種作業系統，包括Microsoft Windows 95、98、NT、2000、Me，及XP；Mac OS；Linux and Windows CE等。

安全自動化用戶端更新與Web管理

Cisco Wireless Utility Auto Installer可自動安全地安裝與升級思科Aironet用戶端軟體工具、韌體，以及使用者檔案，包括安全設定、SSID、功率設定，及頻道選擇等，為網管人員節省大量時間。

使用支援思科安全發現協定（Cisco Discovery Protocol; CDP）的CiscoWorks2000自動偵測思科 Aironet Access Point和橋接器。並提供網頁管理和SNMP的功能，如監視、故障排除、軟體下載，以及登入等。此外，與用戶端程式整合的思科Site Survey Tool（SST）可快速且正確安裝Access Point。

AAA RADIUS伺服器支援

許多AAA RADIUS伺服器廠商，包括Funk Software（Steel-Belted RADIUS）及Interlink Networks（AAA RADIUS）等，都已支援 Cisco LEAP安全架構。如果搭配Cisco ACS與Cisco Access Registrar（AR）使用，則可提高網路部署的彈性與安全性。

RADIUS帳務記錄

思科無線網路安全套件可為每一用戶連線製作詳細RADIUS帳務記錄。這些記錄將傳送至AAA伺服器，以便記錄與稽核WLAN的使用量。此外，企業也可使用這些記錄進行網路偵查除錯。

專業WLAN安全防護解決方案

需要點對點WLAN安全防護以便保護重要應用的企業，可選擇虛擬私有網路（VPN）安全解決方案。多數企業客戶並不需要於內部網路中部署VPN，但是對安全效能有特殊需求的企業，如金融機構等，即可使用VPN並搭配安全防護機制，以強化網路安全環境。對絕大多數的企業網路而言，思科無線網路安全套件所提供的加強型安全解決方案已可滿足其安全需求。

總結

如果適當設定並啓動思科無線網路安全套件的防護功能，網管人員可確實保持企業資料的隱私性與安全性，並可提供使用者嚮往的自由性與行動力。使用思科Aironet系列產品，員工可暢遊於無線、安全的環境中自在工作。

台灣思科系統股份有限公司
台北市敦化南路二段333號6樓B座
電話：(886)2-8176-7100
傳真：(886)2-8176-7199

思科系統高雄辦事處
高雄市三多四路110號19樓-2座
電話：(886)7-338-1092
傳真：(886)7-338-1094

若您欲進一步了解相關之資訊，請連結至台灣思科網頁查詢
www.cisco.com.tw