爲網路使用者打造自由、行動與安全兼備的環境

Cisco Aironet Series—配備企業級安全功能的無線自由空間

對貴公司而言，比在網路上交換資料更重要的事，就是保持資料安全的能力。安全恐懼導致部分網路主管避免安裝無線區域網路（WLAN），而不考慮 WLAN 所帶來的多重效益。

無線安全的態勢已經改變，可讓 IT 主管更有信心地部署 WLAN。Cisco® Wireless Security Suite 這項適用於企業的標準化 WLAN 安全方案，即鎖定 Cisco Aironet® Series 產品與 Cisco Compatible WLAN 用戶端設備。

Cisco Wireless Security Suite 的功能包括：

- 支援 IEEE 802.11i 標準
- 支援 Wi-Fi 聯盟的安全認證 WPA（Wi-Fi Protected Access）與 WPA2（Wi-Fi Protected Access 2）
- 支援 IEEE 802.1X 的相互驗證功能與動態加密鑰管理
- 使用 TKIP（Temporal Key Integrity Protocol）、WEP（Wired Equivalent Privacy）或 AES（Advanced Encryption Standard）加密資料
- 支援市場上最多的 802.1X 驗證型態、用戶端設備與用戶端作業系統
- 減少主動式與被動式網路攻擊
- Cisco SWAN（Structured Wireless-Aware Network）支援
- 整合 Cisco Self-Defending Network

Cisco 身爲網路領導者與無線網路推動者，讓網路主管能在兼顧網路安全的前提之下，爲使用者提供渴求的自由空間。

將入侵者隔絕在外的安全性

網路主管必須爲終端使用者提供自由空間與行動能力，同時又不讓入侵者存取 WLAN 或無線網路所傳送接收的資訊。WLAN 使用在用戶端設備、基地台與存取器（可將基地台連至網路的乙太網路 WLAN 端點）之間傳送的無線電波，在空中以廣播的作法來傳輸資料。也就是說，任何位於存取器服務區域之內的 WLAN 用戶端設備，皆可從或向存取器傳輸資料。

由於無線電波在天花板、地板與牆壁之間傳送，資料傳輸可能會接觸到不同樓層甚或大樓外部的陌生接收者。WLAN 可移除網路的界線。但若未採取嚴謹的安全作法，安裝 WLAN 等於是將乙太網路埠散置各地，包括停車場在內。

此外，幾份研究報告與文章皆指出 WEP 密鑰加密與解密傳輸資料的漏洞。入侵者已有現成存取工具可破壞 WEP 密鑰，例如：AirSnort，可讓攻擊者暗中監看與分析資料封包，並使用該資訊來破壞加密封包的 WEP 密鑰。

網路主管必須再次確認解決方案能否保護 WLAN 環境免於上述漏洞，而且還能提供與有線區域網路同等級的安全性、管理能力與延展性。

WLAN 安全的重要性

即使在有線網路的世界裡，也沒人能保證網路環境百分之百安全，可隨時抵禦任何滲透動作。安全防護是動態且持續的工作，而非靜止不動。網路主管與 WLAN 製造商永遠都要領先駭客一步。

網路主管也必須啓動 WLAN 安全功能。在 2001 年時，一篇登在華爾街日報（Wall Street Journal）的文章詳述兩名駭客開著配備膝上型電腦與天線的車逛矽谷，探尋流散在外的 WLAN 訊號。駭客取得來自許多未啓用 WLAN 適當安全功能的公司的訊號。

安全專家建議，企業必須在網路的多重層級部署防禦之道，以減輕威脅。額外的安全功能元件包括防火牆、入侵偵測系統（IDS）與虛擬區域網路（VLAN）。網路主管也可透過無線網路的智慧型設計與安裝，包括實施經過實證的安全作法，以及使用由網路安全的專家所開發的產品與軟體，來降低風險。Cisco 身爲網路安全的產業領導者，爲 WLAN 導入工作提供了一系列絕佳的選擇。搭配 Cisco Wireless Security Suite 與 Cisco SWAN 屢獲獎項的安全功能，網路主管即可降低網路風險並提升 WLAN 安全性。

WLAN 安全解決方案

WLAN 的安全性和其他網路相同，都著重在存取控管與隱私性。堅實可靠的 WLAN 存取控管也稱爲驗證，阻擋未經授權的使用者透過存取器進行通訊。穩健的 WLAN 存取控管作法，有助於確保合法使用者僅連結受信賴的存取器，而非惡意或未經授權的存取器。

目前，已有 WLAN 的企業採用四種等級的 WLAN 安全作法，解決 WLAN 的存取控管與隱私課題：開放存取、基本安全、強化安全與遠端存取安全。不論部署哪種安全方案，Cisco 都建議企業組織先執行網路風險評估，再選擇並導入 WLAN 安全解決方案。

圖 1. 多個大小不一的 Cisco Aironet 存取器，是所有無線網路或有線與無線網路連接點的中心，可遍佈於整幢大樓或園區裡。

Cisco Aironet 存取器備有 Cisco Aironet 或 Cisco Compatible WLAN 用戶端轉接卡，可讓使用者在園區的覆蓋區域內自由移動。

Cisco Wireless Security Suite 可確保對所有網路資源百分百安全且不受干擾的存取，Cisco SWAN 也支援成千上百個 Cisco Aironet 存取器的部署、運作與管理。

開放存取

所有取得 Wi-Fi 認證的 WLAN 產品，包括 Cisco Aironet Series 產品在內，都會以「開放存取」的模式出貨，也就是關閉安全功能。對於公開場合如咖啡店、大學校園、機場或其他公共場所的熱點而言，開放存取或無安全功能是合宜且可被允許的作法，但不適合用在企業組

織。在企業環境的安裝過程中，無線設備就要具備安全性。如前所言，部分公司並未開啓 WLAN 安全功能。這些公司正將他們的網路曝露於嚴重的風險之中。

基本安全：SSID、WEP 與 MAC 位址驗證

基本安全是指使用 SSID（Service Set Identifiers）、公開或共享密鑰驗證、靜態 WEP 密鑰，或選擇式的 MAC（Media Access Control）驗證。這些組合提供了初步層級的存取控管與隱私，但每一個元件都有可能被破解。

「SSID」是 WLAN 次系統設備的常見網路名稱，它的角色是以邏輯性作法區隔次系統。SSID 可阻擋無 SSID 的用戶端設備的存取動作。但存取器預設以標識來廣播 SSID。即使關閉了 SSID 的廣播，入侵者或駭客仍能透過眾所皆知的「Sniffing」作法，或在不被偵測的情況下對網路進行監看，來偵測出 SSID。

802.11 標準是由 IEEE 針對 WLAN 所訂定的一組規範，支援兩種用戶端驗證作法：開放與共享密鑰驗證。開放驗證不只是提供正確的 SSID。共享密鑰驗證則可讓存取器傳送挑戰字串給用戶端設備，用戶端必須以正確的 WEP 密鑰加密，再回傳給存取器。若無正確密鑰，驗證即會宣告失敗，用戶端就無法連結存取器。一般認爲共享密鑰驗證並不安全，因爲入侵者可偵測未經編碼的挑戰字串，以 WEP 密鑰加密的該字串也可用於解譯 WEP 密鑰。

而在開放驗證中，即使用戶端完成驗證並連結存取器，WEP 的採用仍會阻擋用戶端從存取器傳送或接收資料，除非用戶端有正確的 WEP 密鑰。WEP 密鑰是由 40 或 128 位元所組成，通常是網路管理人員在存取器設定的靜態定義，所有用戶端皆據此與存取器溝通。採用靜態 WEP 密鑰時，網路管理人員必須執行耗時作業，在 WLAN 的每個設備輸入相同密鑰。

假如使用靜態 WEP 密鑰的設備遺失或遭竊，取得該失竊設備的持有人即可存取 WLAN。管理人員無法偵測到有未經授權的使用者潛入 WLAN。除非有人回報設備失竊，管理人員才會在與失竊設備使用相同靜態 WEP 密鑰的其他所有設備，進行 WEP 密鑰變更。在大型企業裡，WLAN 通常要支援成千上百位使用者，這將是一件可怕任務。更糟的是，假如靜態 WEP 密鑰是以類似 AirSnort 的工具潛入取得，管理人員根本無法得知密鑰已遭入侵者破解。

部分 WLAN 供應商支援以用戶端網路介接卡的實際位址或 MAC 位址進行驗證。存取器也僅允許符合驗證清單的用戶端 MAC 位址進行連結。但 MAC 驗證仍非完善的安全作法，因爲 MAC 位址可被僞造，而網路介接卡也可能失竊。

搭配 WPA 或 WPA2 PSK 的基本安全

基本安全的可用作法還有 WPA 或 WPA2 PSK（Pre-Shared Key）。PSK 會同時以用戶端與存取器的密碼或識別碼（亦稱爲通關密語）來確認使用者。假如用戶端的密碼符合存取器的密

碼，即可存取網路。PSK 也提供 TKIP 或 AES 爲各個封包的傳輸資料產出加密碼的密鑰素材。PSK 比靜態 WEP 更安全，但兩者都儲存於用戶端，一旦用戶端設備失竊，PSK 同樣會被破解。建議使用混合字母、數字與非字元符號的複雜化 PSK 通關密語。

基本安全結語

基本 WLAN 安全性，有賴於 SSID、開放驗證、靜態 WEP 密鑰、MAC 驗證或 WPA/WPA2 PSK 的組合，僅適用於規模很小或不透過 WLAN 網路委交關鍵任務資料的企業。除此之外的所有企業組織，皆需投資於穩固可靠的企業級 WLAN 安全方案。

強化安全—Cisco Wireless Security Suite 的優點

建議需要企業級安全的客戶選擇強化安全等級。Cisco Wireless Security Suite 即是一項強化安全的解決方案，以其 802.1X 相互驗證與 TKIP 或 AES 加密等建構模組，爲 WPA 與 WPA2 提供完整支援。下列爲 Cisco Wireless Security Suite 的部分功能：

- 以 802.1X 提供強大的相互驗證功能，以及個別使用者/通訊會期的動態加密鑰
- 以 TKIP 強化以 RC4 爲基礎的加密，例如：密鑰混雜（個別封包密鑰）、MIC（Message Integrity Check）、IV（initialization vector）異動，以及廣播金鑰輪替。
- 以 AES 提供政府級的高度安全資料加密

Cisco Wireless Security Suite 是一項強化安全的解決方案，讓網路管理人員有信心以企業級的安全與防護來部署 WLAN。

遠端存取 WLAN 安全

在特定情況下，企業需要端對端安全來保護他們的業務應用。管理人員可透過遠端存取安全來設定 VPN（Virtual Private Network），讓行動使用者可在公眾場所的熱點，例如：機場、旅館與會議中心，建立連回企業網路的通道。

企業部署強化安全方案時，例如：Cisco Wireless Security Suite，必須符合並超越 WLAN 安全需求，因此，無需將 VPN 用於企業 WLAN。在內部 WLAN 部署使用 VPN，將影響 WLAN 的效能，受限的漫遊功能則讓使用者的登入過程更爲複雜。因此，根本無需在內部 WLAN 再架上 VPN，而導致額外心力、諸多限制與投資費用。

針對 WLAN 在 VPN 的使用，或安裝強化的 WLAN 安全解決方案等資訊，請詳閱白皮書：CISCO SAFE：Wireless LAN Security in Depth。Cisco 的 SAFE 藍圖是一套模組化的方法，制訂安全的設計、導入與管理程序，以保護 WLAN 網路。

令人安心的 Cisco Wireless Security Suite

Cisco Wireless Security Suite 是適用於企業的標準化 WLAN 安全方案，當管理者使用 Cisco Aironet Series 產品與 Cisco Compatible Extensions 產品或 Wi-Fi 認證的 WLAN 用戶端設備時，能有信心地確保資料的私密與安全。Cisco Wireless Security Suite 可與 Cisco Self-Defending Network 整合。

Cisco Wireless Security Suite 提供堅實的 WLAN 安全服務，可與有線區域網路的安全性緊密併用。它以領先業界的 WLAN 安全服務，滿足對一致、可靠與安全行動網路的需求。這項企業級的解決方案可減少複雜的 WLAN 攻擊，並與許多用戶端設備互通，以提供兼具可靠性與延展性的集中式安全管理。網路管理人員能以具延展性且零缺失的安全管理作業，來部署大規模的企業 WLAN，且不造成 IT 人員的額外負擔。

Cisco Wireless Security Suite 提供許多來自 Cisco 的創新強化功能，並支援 WPA（Wi-Fi Protected Access）與 WPA2（Wi-Fi Protected Access 2），透過個別使用者/通訊會期的相互驗證來提供存取控管，以及透過強大的動態加密功能來提供資料隱私性。

Cisco Wireless Security Suite 有來自 Cisco SWAN（Cisco Structured Wireless-Aware Network）的全面支援。Cisco Wireless Security Suite 與 Cisco SWAN 的結合可提供：

- WLAN 的安全連結—根據可組態的準則自動改變動態加密鑰，保護傳輸資料的隱私性。
  --WPA-TKIP 加密強化如 MIC、啓動無線電誘導混雜各個封包密鑰，以及廣播密鑰輪替
  --WPA2-AES 是高標準的資料加密

- WLAN 的信任與身分—堅實的 WLAN 存取控管，可確保合法用戶端僅能連結受信賴的存取器，而非惡意或未經授權的存取器。以 802.11X、各種 EAP（Extensible Authentication Protocol）型態與 RADIUS（Remote Authentication Dial-In User services），或驗證、授權與帳戶（AAA）伺服器，來提供個別使用者/通訊會期的相互驗證。
  --支援最多的 802.1X 驗證型態、用戶端設備與用戶端作業系統
  --支援 RADIUS 帳戶記錄，以涵蓋所有驗證嘗試動作

- WLAN 的威脅防禦—以 Cisco Wireless LAN Threat Defense 解決方案來偵測未經授權的存取、網路攻擊與惡意存取器。這項解決方案包含 Cisco SWAN WLAN IDS（Intrusion Detection System），可讓 IT 主管持續掃瞄 RF 環境、偵測惡意存取器，並在其進行連結時關閉交換埠。其他未經授權的事件與攻擊，亦可自動追蹤與清除。

WPA 與 WPA2 支援

Cisco Wireless Security Suite 支援 Wi-Fi 聯盟認證的 WPA 與 WPA2。WPA 是 Wi-Fi 聯盟在 2003 年發表。WPA2 則是 Wi-Fi 聯盟在 2004 年發表。通過 WPA2 Wi-Fi 認證的所有產品，都必須與 WPA Wi-Fi 認證的產品互通。

WPA 與 WPA2 爲終端使用者與網路管理人員提供高階保證，他們的資料可保有私密性，對於網路的存取則僅限於授權使用者。個人與企業的雙模式運作，可符合兩大市場區隔的獨特需求。企業模式使用 IEEE 802.1X 與 EAP 進行驗證。個人模式則使用 PSK 進行驗證。Cisco 並不建議企業組織或政府機關部署個人模式，對企業環境而言，用來驗證使用者驗證的 PSK 還不夠安全。

WPA 可解決在原始 802.11 安全導入裡的所有已知 WEP（Wired Equivalent Privacy）漏洞，爲企業與 SOHO（small office/home office）環境的 WLAN，提供立即可用的安全方案。

WPA2 則是新一代的 Wi-Fi 安全性。它是 Wi-Fi 聯盟針對已批准的 IEEE 802.11i 標準的互通導入功能。它引進 NIST（National Institute of Standards and Technology）建議採用的 CCMP（Counter Mode with Cipher Block Changing Message Authentication Code Protocol）AES 加密演算法。WPA2 也能促進對政府 FIPS 140-2 規範的遵循（表 1）。

表 1.　WPA 與 WPA2 模式型態比較表

	WPA	**WPA2**
企業模式 **（企業、政府、教育機構）**	驗證：IEEE 802.1X/EAP 加密：TKIP/MIC	驗證：IEEE 802.1X/EAP 加密：AES-CCMP
個人模式 **（SOHO、家庭/個人）**	驗證：PSK 加密：TKIP/MIC	驗證：PSK 加密：AES-CCMP

IEEE 802.1X 驗證與 EAP

IEEE 已經採用 802.1X 做爲有線與無線網路的驗證標準。802.1X 同時獲得 WPA-企業模式與 WPA2-企業模式的支援。802.1X 爲 WLAN 提供用戶端與驗證伺服器之間強大的相互驗證能力。此外，802.1X 還爲個別使用者/通訊會期提供動態加密鑰，免除與靜態加密鑰相關的管理重擔及安全課題。

透過 802.1X，用於驗證的憑證如登入密碼，不會在無線媒介以明碼或未經加密的狀態傳輸。802.1X 驗證型態爲 WLAN 提供強大的驗證能力，但同時也需要 TKIP 或 AES 加密功能與 802.1X 並用，以避免 802.11 WEP 驗證漏洞所引發的網路攻擊。

目前有數種 802.1X 驗證型態，每種都提供不同的驗證方案，但都依賴相同框架與 EAP 來溝通用戶端與存取器。Cisco Aironet 產品比其他 WLAN 產品支援更多的 802.1X EAP 驗證型態。支援型態包括：Cisco LEAP、EAP-FAST（EAP-Flexible Authentication via Secure Tunneling）、EAP-TLS（EAP-Transport Layer Security）、PEAP（Protected Extensible

Authentication Protocol）、EAP-TTLS（EAP-Tunneled TLS），以及 EAP-SIM（EAP-Subscriber Identity Module）。

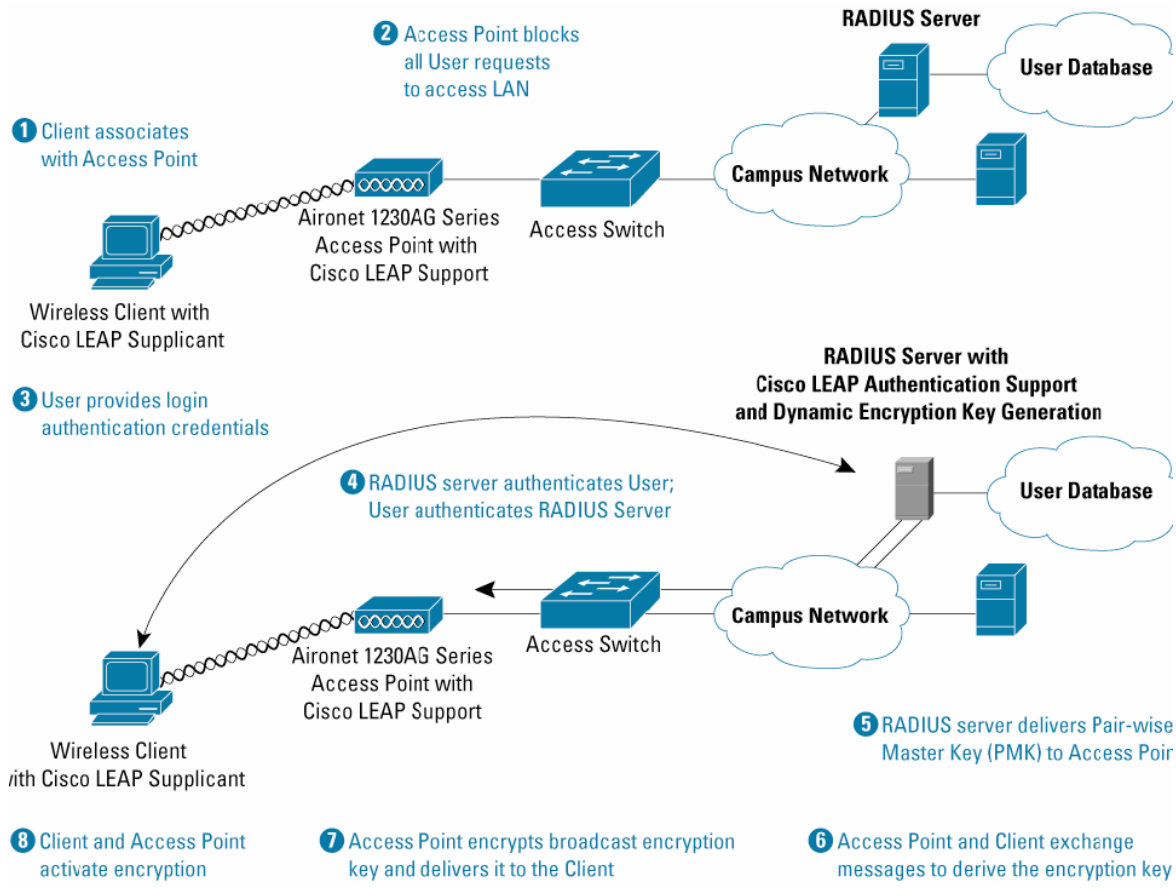
Cisco 建議客戶評估網路與安全環境，爲他們的 802.1X 部署選擇最佳的 EAP 驗證型態。在選擇 EAP 型態時，所需評估的領域包括安全憑證使用的安全機制型態、使用者驗證資料庫、用戶端目前使用的作業系統、可用的用戶端套件、使用者所需的登入型態，以及 RADIUS 或 AAA 伺服器。

每個 EAP 型態都有優缺點。EAP 型態管理能力、作業系統支援、用戶端設備支援、用戶端軟體與驗證訊息耗用、認證需求、使用者的易於使用性，以及 WLAN 基礎架構設備支援，都是在提供安全時必須取捨的條件。多重 EAP 型態也可用於網路，以符合特定驗證、用戶端設備或終端使用者的需求。

RADIUS 伺服器的廣泛選擇，例如：Cisco ACS（Cisco Secure Access Control Server）與 Cisco CNS Access Registrar®，或協力廠商的 AAA RADIUS 伺服器，例如：Funk Software（Steel-Belted RADIUS）與 Interlink Networks（AAA RADIUS），皆可用於 802.1X 驗證。

802.1X 驗證型態的使用，可透過使用者提供的憑證來驗證用戶端，相較於以實體用戶端設備驗證的作法，可將設備或 WLAN 網路轉接卡失竊造成的風險降至最低。802.1X 還具備其他效益，包括減少「中間人」驗證攻擊、搭配政策式密鑰輪替的集中式加密鑰管理，提供防護免於「強行破解」式的攻擊（圖 2）。

圖 2.　提供企業級安全的 Cisco Wireless Security Suite



WLAN 使用者的集中式政策管理

802.1X 驗證的另一個好處是 WLAN 使用者群組的集中式管理，包括政策式密鑰輪替、動態密鑰指派、動態 VLAN 指派與 SSID 設限。這些功能可輪替密鑰。也可將使用者指定至特定 VLAN，以確保使用者只能存取特定資源。

在成功地完成相互驗證之後，用戶端與 RADIUS 伺服器會各自衍生相同的加密鑰，用於加密所有交換資料。使用有線區域網路的安全通道，讓 RADIUS 伺服器可傳送密鑰至存取器，以便爲用戶端進行儲存。結果則能以個別使用者/通訊會期的加密鑰，搭配 RADIUS 伺服器儲存的通訊會期長度等既定政策。當通訊會期超出時限，或用戶端從某一存取器漫遊至另一存取器時，就會啓動重新驗證，並產出新的通訊會期密鑰。重新驗證對使用者而言完全透通。

結合加密鑰與重新驗證計時器，VLAN ID 與 SSID 的設限參數將傳送至存取器。當存取器收到指派給特定使用者的 VLAN ID 時，就會將使用者安置於特定的 VLAN ID。假如 SSID 許可清單也被傳送至存取器，存取器就能協助確保使用者提供有效的 SSID ID 以存取 WLAN。假如使用者提供的 SSID 未列入 SSID 許可清單，則存取器會拒絕使用者連結 WLAN 網路。

減少強行破解式攻擊

傳統的 WLAN 導入是以靜態加密鑰爲基礎，很容易招致強行破解式的網路攻擊。強行破解式的網路攻擊，是指入侵者試圖產出加密鑰並逐一試行。針對標準的 128 位元 WEP，這種作法最多需要 2104 組不同的密鑰。採用 802.1X 針對個別使用者/通訊會期的動態加密鑰，也有可能招致強行破解式的網路攻擊，雖然理論上可行，但實際上卻很難破解且徒勞無功。

WPA 加密—TKIP

Cisco Wireless Security Suite 支援 TKIP，這是一項 WPA 功能元件與 IEEE 802.11i 標準。TKIP 可強化 WEP 安全性。如同 WEP，TKIP 使用的是由工程師 Ron Rivest 開發的加密方法，一般稱爲 RC4（Ron’s Code 4）加密。不過，TKIP 提供更多作法來強化 WEP，例如：個別封包密鑰混雜、MIC 與廣播式密鑰輪替，以解決 WEP 的已知漏洞。

TKIP 使用 128 位元密鑰的 RC4 串流暗碼進行加密，以及 64 位元密鑰進行驗證。以密鑰加密的資料，僅可用於資料的目標收件人，TKIP 協助確保只有目標對象能得知這份傳輸資料。針對指定的資料封包，TKIP 加密最多可產出 280 兆組密鑰。

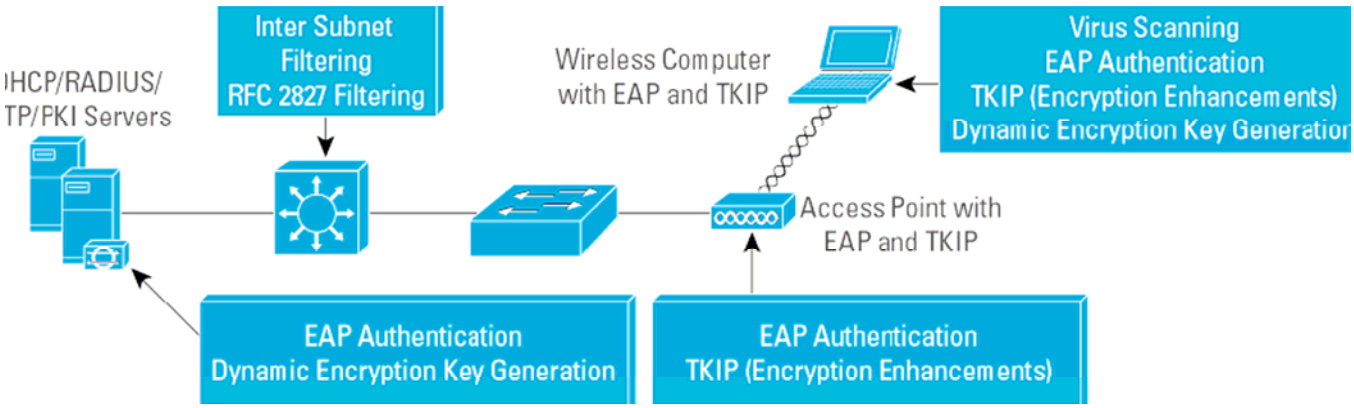
透過 Cisco Wireless Security Suite，無論是 Cisco Aironet 存取器與 Cisco Aironet 及 Cisco Compatible WLAN 用戶端設備，皆提供 Cisco TKIP 與 WPA TKIP 演算法。Cisco Aironet Series 存取器可在使用多重 VLAN 的同時，同步執行 Cisco TKIP 與 WPA TKIP。系統管理人員必須選擇一組 TKIP 演算法做爲企業的用戶端設備，因爲用戶端無法同時支援兩組 TKIP 演算法。Cisco 建議儘其可能地將 WPA TKIP 用於用戶端設備與存取器。

個別封包密鑰混雜以減少弱點 IV 攻擊

當 WEP 密鑰用於加密及解密傳輸資料時，個別封包都將內含一組 IV（initialization vector），它是 24 位元型態，並隨各個封包而異。TKIP RC4 的密鑰排程演算法，可從底層的 WEP 密鑰建立 IV。WEP 導入 RC4 的一個漏洞，則可能建立「弱點」IV，因而能透視底層密鑰。使用類似 AirSnort 的工具，入侵者可收集以相同密鑰加密的封包來刺探漏洞，並使用弱點 IV 來計算底層密鑰。

TKIP 包含密鑰混雜或個別封包密鑰，可減少弱點 IV 攻擊。在存取器與所有相關用戶端設備同時導入密鑰混雜支援，讓資料傳輸者可混雜 IV 的底層密鑰，爲各個封包建立新密鑰。有助於確保每個封包都以不同密鑰加密，密鑰混雜可移除入侵者藉由刺探 IV 來判斷 WEP 密鑰的預測能力。（圖 3）

圖 3.WPA 可減緩攻擊—802.1X EAP/TKIP WLAN 設計



因應主動式網路攻擊的 MIC 防護

採用 MIC（message integrity check）可阻礙主動式網路攻擊，它的作法是判斷用於加密攔截封包的加密鑰。這種主動式攻擊是由位元翻轉（bit-flipping）式攻擊與重送（replay）攻擊所組成。在存取器與所有相關用戶端設備同時導入 MIC 支援，可讓封包傳送者在加密與傳輸封包時，預先加入一組字元（即 MIC）。在收到封包時，收件人進行解密並檢查 MIC。假

如訊框裡的 MIC 符合計算值（由 MIC 功能衍生），收件人就接受封包；假如不符，收件人則可拒絕封包。

透過 MIC，即可拒絕在傳送過程遭到惡意修改的封包。攻擊者無法使用位元翻轉式攻擊或主動重送攻擊來誤導網路給予驗證，Cisco Aironet 產品具備 MIC 功能，可辨認並拒絕遭變更的封包。

廣播式密鑰輪替

TKIP 可讓網路主管同時輪替用於加密廣播與多址傳從的單點播送密鑰與廣播加密鑰。網路主管可在存取器組態廣播密鑰輪替政策。由於靜態廣播密鑰與靜態 WEP 密鑰皆有易於攻擊的相同弱點，因此，針對廣播密鑰提供密鑰輪替值，將可免除這項弱點。

WPA2 加密—進階加密標準

Cisco Wireless Security Suite 支援 WPA2，其使用 AES 加密機制來提供隱密性與完整性。AES 是 TKIP 與 WEP 使用的 RC4 加密的替代加密機制。AES 尚無任何已知攻擊，可提供比 TKIP 與 WEP 更強大的加密功能。AES 是高度安全的暗碼演算法，根據目前的分析顯示，需要採取 2^120 次試行才能破解 AES 密鑰，這是現行技術所無法達成的結果。

AES 是一組暗號，屬於對稱式密鑰暗號的類型之一，加密與解密皆使用相同密鑰，並使用一組固定長度的字元。WEP 使用密鑰串並橫跨明文資料輸入串來進行加密，AES 針對明文的加密暗號組則是獨立計算而成。AES 標準指定 AES 每組暗號的大小爲 128 位元，且需搭配長度分別爲 128 位元、192 位元與 256 位元的三組候補密鑰。128 位元的密鑰長度可用於 WPA2/802.11i。每一輪 WPA2/802.11i AES 加密皆需分四階段進行。透過 WPA2/802.11i，每一輪皆需重複十次。

爲了同時提供資料隱密性與驗證效力，可於 AES 共用名爲 CCM（Counter-Mode/CBC-Mac）的新建構模式。CCM 以檢數器模式（CTR）來使用 AES，以達到資料隱密性，而 AES 則使用 CBC-MAC（Cipher block Chaining Message Authentication Code）來提供資料完整性。每次皆使用兩種模式（CTR 與 CBC-MAC）的單一密鑰，是一種全新型態的建構作法，已經獲得 NIST（Special Publication 800-38C）與標準社群（IETF RFC-3610）的接受。

48 位元的 IV 可用於 CCM。如同 TKIP，AES 不以 WEP 加密方法的相同形式來使用 IV。在 CCM 中，IV 是用來做爲加密與解密程序的資料輸入，以降低重送攻擊的風險。隨著 IV 空間擴增至 48 位元，牴觸 IV 的機會也呈指數成長，因而可帶來更好的資料防護能力。

由於 AES 密集運算的本質，因此建議以硬體執行 AES 加密（與解密）。Cisco Aironet 產品即以硬體執行 AES 加密。若以軟體爲多重用戶端同時執行 AES 加密，則需要很強的運算威力，例如：配備 2.5GHz Pentium 處理器的膝上型電腦。假如存取器以軟體來執行 AES 加密/

解密，同時還要服務眾多的連線用戶端，存取器必然面臨效能降級的問題，尤其是在存取器缺乏強大處理器與大量 RAM 及 ROM 時最嚴重。

WPA 與 WPA2 部署

思科建議客戶在支援 WPA2 的用戶端設備啓用 WPA2。雖然 WPA 仍被認爲安全，而 TKIP 也尚未遭破解，但 Cisco 仍建議客戶儘速轉移至 WPA2。因爲 WPA2 必須同時在存取器與用戶端設備進行組態變更，導入 WPA2 需經事先規劃，以在同時轉換大批用戶端設備與存取器時，將網路干擾降至最低。轉移至 WPA2 的機會之一，就是在新建、升級或擴充無線網路時。

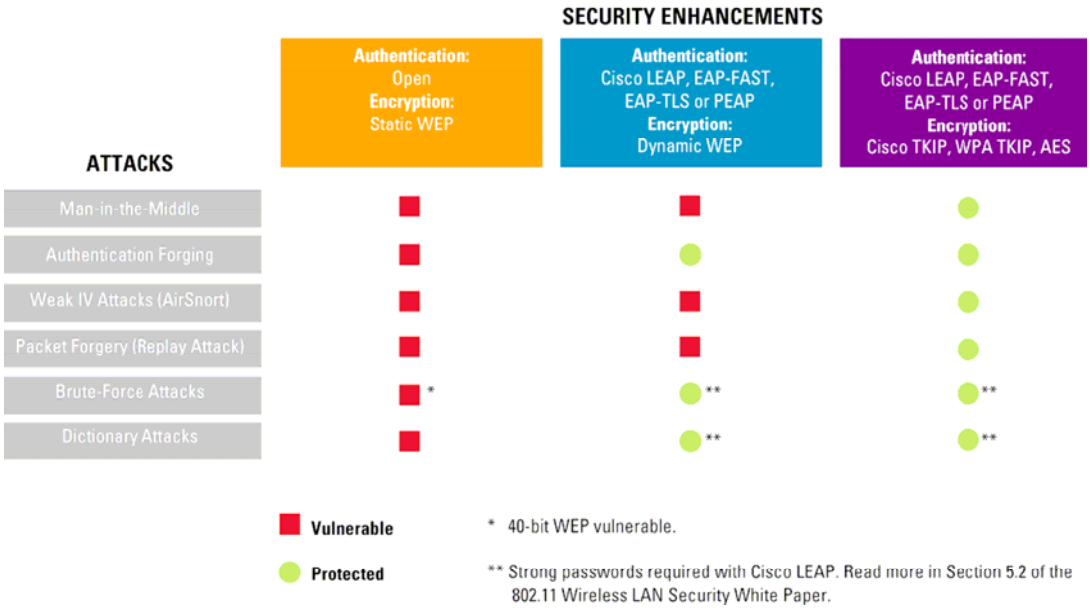
爲了簡化轉移至 WPA 與 WPA2 的工作，Cisco Aironet 存取器同時支援 WPA 遷移模式與 WPA2 混用模式。WPA 遷移模式是由 Cisco 制訂的存取器設定，可讓連至存取器的 WPA 與非 WPA 用戶端使用相同的 SSID。WPA 遷移模式支援 WEP 用戶端驗證，而且又有潛在的不安全性，因而只能做爲暫時使用的遷移模式。WPA2 混用模式的運作，准許 WPA 與 WPA2 用戶端並存於共同的 SSID。WPA2 混用模式是 Wi-Fi 認證的功能。因爲 WPA2 混用模式同時使用 TKIP 與 AES 進行驗證，因而有公認的安全性。

專用型 WLAN 用戶端設備無法執行也無法升級至 AES（與 WPA2）。因此，Cisco 建議企業組織應該在使用這些設備的同時，採用並部署 WPA。WPA 是所有網路的底限。
詳閱 Wi-Fi Protected Access, WPA2 and IEEE 802.11i Q&A 以取得更多資訊。

保護網路免於攻擊

各式各樣的攻擊皆瞄準 WLAN 而來。在使用 802.11X、EAP 型態與 TKIP 或 AES 時，WPA 與 WPA2 是保護網路免於各種攻擊的作法。（圖 4）

圖 4.　全新的安全強化功能可減緩網路攻擊

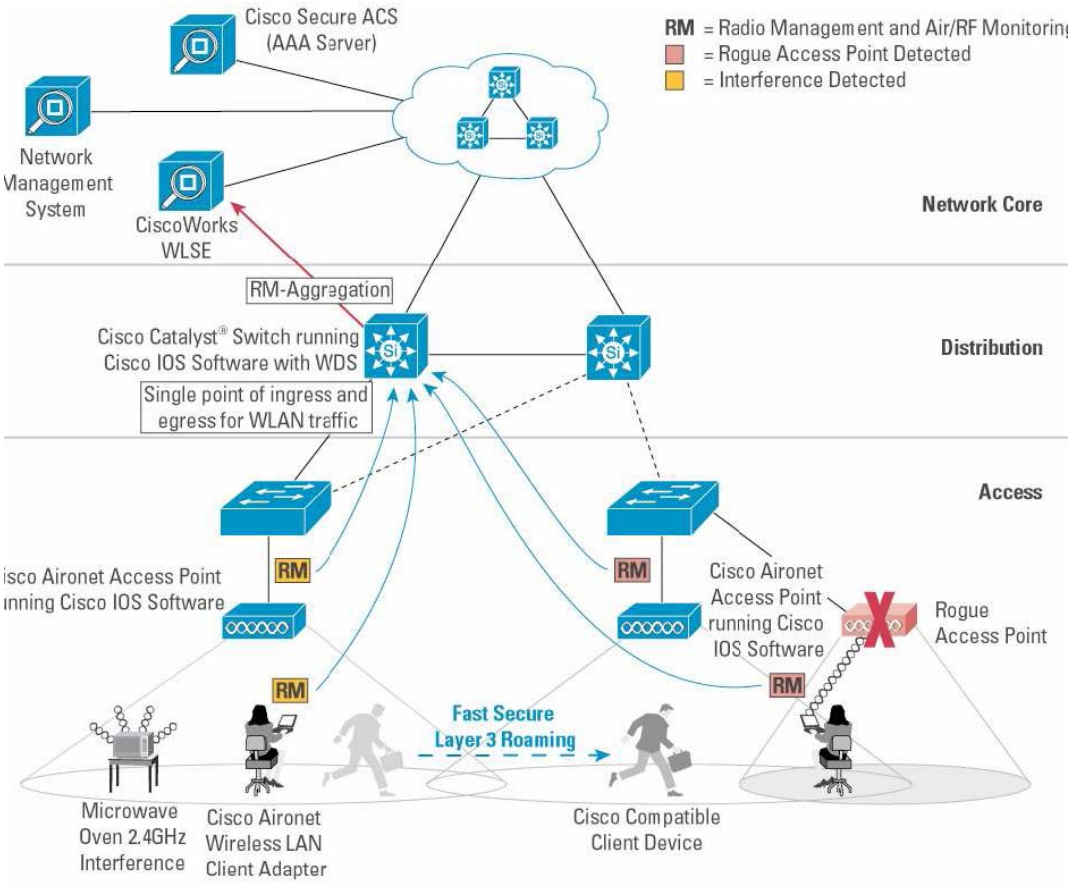


Cisco SWAN

網路主管期望 WLAN 提供與有線區域網路同級的安全性、延展性、可靠度、易於部署及管理功能。並可在日常運作執行安全政策監看。網路安全方案必須易於部署至數十個或成千上百個存取器。而且還要能偵測到員工或惡意入侵者安裝未經授權的存取器。

SWAN（Cisco Structured Wireless-Aware Network）提供整合及擴充有線與無線網路的框架，讓企業以最低的 TCO（total cost of ownership）部署 WLAN。Cisco SWAN 可將「無線感知」擴充爲網路基礎架構的重要元件之一，爲 WLAN 提供企業組織在有線網路行之有年的同級安全性、延展性、可靠度、易於部署及管理功能。Cisco SWAN 的彈性可讓網路主管設計符合特定需求的網路，無論是高度整合的網路設計或簡單的覆蓋式網路皆可。（圖 5）

圖 5.　Cisco SWAN



Clients and Access Points (AP) send their Radio Management (RM) data to the Cisco AP, switch or router running wireless-aware Cisco IOS Software with Wireless Domain Services (WDS).

Cisco AP, switch or router running wireless-aware Cisco IOS Software with WDS uses RM-Aggregation to remove redundant RM data received from the access points and client devices. The WDS device then forwards the aggregated data to the CiscoWorks WLSE.

Cisco SWAN 透過下列的部署、管理與安全優化功能，將 TCO 降至最低，無線網路運行時間則提至最高：

- 統整有線與無線網路，爲所有 WLAN 傳輸提供單一控制點
- 針對無線傳輸所設計，內容豐富的智慧型 Cisco 基礎架構設備集
- 簡化數十個或成千上百個集中或遠端存取器的管理
- 企業級安全與安全政策監看，可順利地推出強化的網路安全方案
- 以據點分析輔助，簡化 WLAN 的部署
- WLAN 管理與運作支援的效率化
- 空中/RF 掃瞄與監看
- 偵測干擾以隔離並安置網路干擾
- 強化的故障排除與診斷工具，可主動地監看效能與故障
- 可自我療癒的 WLAN 能提供更高可用性
- WLAN IDS（Intrusion Detection System）可偵測並刪除惡意存取器、偵測非授權設備，以減緩網路攻擊

WLAN IDS

具備偵測惡意存取器、非授權用戶端設備與專用網路的能力，對於保持 WLAN 安全而言非常重要。這些事件都導致潛在的安全缺口，使 WLAN 連結變得不安全，讓整個網路蒙受風險。員工或入侵者皆有可能安裝惡意（未經授權）的存取器。員工可能還會使用非授權用戶端設備來搜尋 WLAN 存取器，或未經授權的入侵者探測網路弱點。專用網路是指經由 802.11a/b/g 直接互連但不通過授權 WLAN 的電腦或設備。

透過 Cisco SWAN WLAN IDS，惡意存取器、非授權用戶端與專用網路的偵測過程可自動化。IT 主管可輕鬆自動地偵測、安置並解除惡意存取點與其連結的交換埠。Cisco SWAN 還可監看無線電環境，找出非授權用戶與專用網路，並在上述事件發生時，自動產生告警。Cisco SWAN WLAN IDS 能以整合或單一解決方案的形式部署。

WAN 連結遠端據點受損存活功能

Cisco SWAN 支援遠端據點受損存活功能。這項功能來自存取點的 802.11X 本端驗證服務。透過 802.11X 本端驗證服務，Cisco Aironet 存取器可被組態做爲本端驗證伺服器，在 AAA 伺服器無法使用時，驗證無線用戶端。此舉可爲未配備 RADIUS 伺服器與備用驗證服務的遠端或分支辦公室 WLAN，提供安全驗證服務，在 WAN 連結伺服器故障時，仍能存取本端資源如檔案伺服器或印表機。

結語

適當地組態並執行 Cisco Wireless Security Suite 的安全功能，讓網路管理人員能確信保持公司資料的隱密性與完整性。加入 Cisco SWAN，則可爲無線網路提供與有線網路同級的安全

性、延展性、可靠度、易於部署及管理功能。這些解決方案皆可與 Cisco Self-Defending Network 整合，讓網路主管爲使用者提供自由與行動空間，而且無需犧牲網路安全性。

Cisco Aironet 產品線可與現有網路輕鬆整合。它的行動性、彈性與易於安裝，使它成爲安全無線網路的最佳方案。Cisco TIS（Total Implement Solutions）可提供部署協助，Cisco SMARTnet®支援則提供技術操作面的協助。輕輕鬆鬆就能在貴公司推出安全的 Cisco Aironet 無線網路。

Cisco Aironet 產品的更多資訊，詳閱 http://www.cisco.com/go/aironet

Cisco Wireless Security Suite的更多資訊，詳閱http://www.cisco.com/go/aironet/security

Cisco SWAN的更多資訊，詳閱http://www.cisco.com/go/swan

Cisco Self-Defending Network的更多資訊，詳閱 http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns413/networking_solutions_package.html

WPA、WPA2與802.11i的更多資訊，詳閱 http://www.cisco.com/en/US/products/hw/wireless/ps430/products_qanda_item0900aecd801e3e59.shtml

Wi-Fi聯盟WPA認證的更多資訊，詳閱http://www.wi-fi.com/OpenSection/protected_access_archive.asp

Wi-Fi聯盟WPA2認證的更多資訊，詳閱http://www.wi-fi.com/OpenSection/protected_access.asp