解決方案概述

動態分割

簡單且安全的存取方式，有效統一管理有線和無線網路

隨著物聯網裝置數量及對企業具關鍵性的行動裝置和雲端服務的用量激增，帶動了數位化工作場所的創新，進而引發以下的問題：網路邊緣(Edge)是否足夠聰明，可以安全地串連所有類型的裝置和使用者？傳統的有線和無線網路在建置時並未考慮到關鍵業務的行動性、物聯網存取或安全性。對於在整個園區和分支機構網路中不斷變化的行動和 IoT 裝置使用手動和靜態設定的當今作法，勢必會帶來新的安全風險，並且已成為 IT 團隊每天要面臨的繁瑣負擔。

為了簡化和保護網路，Aruba 動態分割統一涵蓋整個有線和無線網路的策略實施，確保流量的安全和獨立。現在，您可以輕鬆地讓企業網路安然無憂地同物聯網和 IT 管理的用戶端裝置並存，並最佳化網路體驗和 IT 作業的端對端流程。

動態分割運用從 Aruba 角色型基礎政策功能、使用者防火牆以及第 7 層豐富的應用程式可見度和整合的網頁內容過濾功能收集到的情報。

關鍵業務和技術推動因素

簡化政策管理

啟動物聯網和用戶端裝置通常需要多個接觸點，而這通常需要在網路的每一個跳躍節點手動設定新的 VLAN、ACL 或子網路。大型分散式網路的持續移動、新增和變更作業也很耗時，而且容易出錯。因此，在設計網路時，高安全性和低複雜度通常無法兼得。

強化使用者體驗

隨著使用者從一個桌面到另一個桌面、或是從一個站點到另一個站點的移動，他們期待在任何連線位置、任何連線方式 (有線或無線) 都能獲得相同的網路體驗。而要求他們使用虛擬私人網路 (VPN) 將會是一大挑戰。一旦網路無法順暢運作而需要等候IT 支援時，使用者往往抱怨連連。而使用者體驗 (無論是員工、訪客、來店消費的顧客或學生) 則會影響組織的成功與否。連接新裝置 (例如智慧型電話、印表機或視訊會議裝置) 通常是在不需要 IT 知識或支援的情況下完成的。一方面期望 IT 部門提供完美的體驗，另方面又希望維持對安全網路上所有項目的可見度和管理功能。

從智慧照明到監視器或徽章辨識器，IoT 裝置正迅速部署在各種規模的網路當中。新穎的 IoT 裝置帶來許多吸引人的好處，卻也使網路面臨安全風險，因為這些裝置與敏感的財務、醫療和業務關鍵資料跳躍在相同的途徑上。這些裝置很少內建強大的安全性，也缺乏可靠的身份驗證。密碼以純文字形式儲存，缺乏安全要求，設備本身通常也位於無法確保安全的公共區域，這無異是開啟網路漏洞的大門。

主要優點

- **更優異且一致的使用者體驗** — 將使用者角色、應用程式深層封包檢查和裝置剖析功能從無線延伸到有線網路
- **簡化網路操作** — 透過減少 SSID、ACL、子網路和有線連接埠所需的設定，以節省時間並避免 VLAN 蔓延
- **提高安全性和裝置可見度** — ClearPass 和政策執行防火牆 (PEF) 可提供更高的可見度和政策執行

預計到 2020 年連接到企業網路的 IoT/無頭式裝置 (headless device) 的數量將超過 200 億，隨之而來的是網路漏洞的威脅。

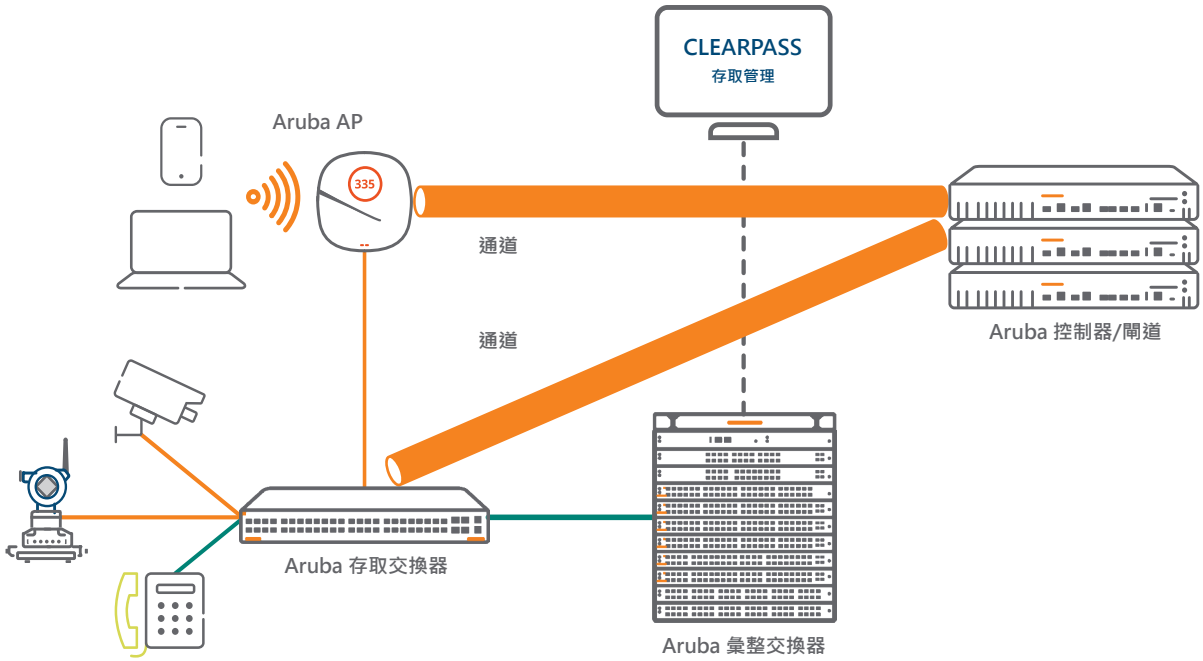
資料來源：Gartner (2017 年 1 月)

將 WLAN 創新技術延伸至交換器

動態分割延伸 Aruba 的安全政策管理和 WLAN 政策執行功能，讓有線網路存取變得簡單安全。此功能意味著可以根據連接埠或使用者角色為有線用戶端裝置動態指派政策，這對於在 2020 年前數量將達到 200 億的 IoT 裝置而言無異是最理想的選擇。Aruba 網路交換器由 ClearPass 支援政策管理、行動控制器支援政策實施，在統一網路存取方面扮演關鍵角色。

角色型政策

藉由動態分割技術，可以根據裝置類型、使用的應用程式，以及使用者或裝置的位置來擬訂角色型決策和存取權限。角色型政策最初用於解決無線安全問題，按照使用者類型 (如員工、來賓或承包商) 對網路流量進行細分，同時透過免除複雜而靜態的網路配置，大幅簡化網路管理。這項強大的功能可簡化 IT 工作流程 (例如管理存取權限和 BYOD 政策)，並確保應用程式效能最佳化。



動態分割是 Experience Edge 的一部分

針對所有的無線 AP 和有線交換器擴展角色型的動態政策管理，從最根本提供簡單、安全但又不同的方式來管理和實施行動化、物聯網和雲端的相關政策。實施 ClearPass 政策定義的 Aruba 行動控制器/閘道，現已能夠支援動態判讀和活用角色。此功能可透過動態指派政策，省去在管理複雜而靜態的 VLAN、ACL 和子網路時耗時且容易出錯的作業。

第 4 至 7 層分割

Aruba 交換器所運用的第二項基本功能是分割。Aruba WLAN 架構透過使用AP與控制器或閘道之間的通道來確保流量安全和獨立。透過使用 Aruba 內建的政策執行防火牆 (PEF)，這種基於通道的分割功能得以提供安全性，例如對高風險流量進行防火牆檢查。PEF 提供精細的情境資訊 (使用者、裝置、應用程式、位置)，進而減輕對昂貴防火牆第一線詢問和防護的需求。藉由基於身份、裝置類型和位置的脈絡式政策，您可以使用單一網路配置滿足不同使用者群組的需求，讓流量來輕鬆適應指派的角色。

透過使用這種 WLAN 通道架構，Aruba 交換器現已可提供角色型分割法，而非傳統的手動使用本機 VLAN。這對於尚無法被信任的 IoT 裝置以及提供應用程式可見度的需求來說是一項理想的選擇，因為 Aruba 交換器現在可以像 AP一樣，將選定的流量經由動態通道的方式傳輸到控制器，以進行深層封包檢查和裝置身份驗證。例如，可以為監視器動態指派一個角色以及僅能將其流量傳輸到指定伺服器的權限，進而避免惡意進入網路其他部分的可能性。

這項新的分割功能，可以透過控制器進行所有身份驗證的連接埠型通道 (PBT) 或是透過在交換器上進行身份驗證的使用者型通道 (UBT) 進行設定，以改善安全性態勢。由於此分割是作為覆蓋層，因此可以透過運用在選定區域中的安全通道來與 VLAN 建置併存，而無需淘汰或更換整個交換器基礎架構。

透過將行動控制器建立為統一的政策執行引擎，動態分割可簡化並保護有線和無線網路。來自 AP 或交換器的流量被封裝在 GRE 通道中，以供政策執行防火牆 (PEF) 檢查。

解決方案元素

Aruba 無線 AP

滿足任何環境需求的 802.11ac 和 802.11ax Wi-Fi 效能。內建的 AI 智慧和位置服務，為 IT 提供使用者和 IoT 裝置最佳體驗所需的自動化和可見度。

Aruba 網路交換器

建立整合的無線基礎，為園區和分支網路提供可擴充性、安全性和高效能。動態分割採取獨特的設計，為 IT 團隊提供一種簡單的方式，可透過通道 (包括使用連接埠型通道 (PBT) 在控制器上進行身份驗證，或是使用者型通道 (UBT) 在 Aruba 交換器上完成身份驗證)，在網路上任何位置套用政策、運用進階服務以及安全地分割有線使用者和 IoT 流量。

Aruba 閘道和行動控制器

控制器或閘道為解決方案的關鍵部分，可作為有線和無線流量的政策執行者。Aruba 行動控制器 (執行 AOS 8.1 或更高版本) 可讓 IT 運用政策實施、頻寬合約和其他流量限制。在分支機構環境中，是由 Aruba Central 管理的分支閘道來執行此功能。政策實施防火牆可作為支援這兩種環境的基礎網路技術。

具有剖析功能的 Aruba ClearPass 政策管理器

集中管理和實施用於無線和有線存取控制的網路存取政策。其主要功能是裝置剖析、身份驗證以及授權和政策執行。藉由使用 ClearPass，角色和權限在定義之後，就會透過所有的有線

和無線存取追蹤使用者或裝置。因此，如果使用者變更為未知裝置，或使用不安全的網路，則該政策將自動變更授予權限。在 ClearPass 上設定可下載使用者角色 (DUR)，就不需要在交換器上定義角色或政策。

總結

為了更妥善處理業務關鍵的行動性和新興 IoT 連線功能的要求，Aruba 創新的動態分割解決方案透過動態實施統一的政策，以及在網路上的任何位置執行進階服務，以簡化 IT 作業並提高安全性。如此一來，可確保為所有無線和有線使用者和裝置，順利發佈、自動實施並獨立執行適當的存取權限和安全政策。

SO_DynamicSegmentation_SK_092419 a00058593enw