分支機構的REAP部署指南

目錄

簡介

本文提供部署遠端邊緣接入點(REAP)時需要考慮的資訊。 請參閱具有輕量AP和無線LAN控制器(WLC)的遠端邊緣AP(REAP)組態範例以瞭解基本REAP組態資訊。

註：WLC 3.2.215版之前支援REAP功能。從WLC 4.0.155.5版開始，此功能稱為混合REAP(H-REAP)，在7.0.x.x之前僅提供少量增強。自7.2.103版本起，此功能稱為FlexConnect。

基於傳統思科輕量型存取點通訊協定(LWAPP)的存取點(AP)（也稱為LAP），例如執行Cisco IOS®軟體版本12.3(7)JX或更新版本的1010、1020和1100和1200系列AP，允許透過思科無線LAN控制器(WLC)進行中央管理和控制。 此外，這些LAP還允許管理員將控制器用作無線資料聚合的單點。

雖然這些LAP允許控制器執行高級功能(例如QoS和訪問控制清單(ACL)實施)，但要求控制器是所有

無線客戶端流量的單一入口點和出口點，可能會阻礙（而非啟用）充分滿足使用者需求的能力。在某些環境（如遠端辦公室）中，在控制器上終止所有使用者資料可能過於佔用頻寬，尤其是在WAN鏈路上可用的吞吐量有限時。此外，在LAP和WLC之間的鏈路容易中斷的情況下（與通往遠端辦公室的WAN鏈路一樣），使用依靠WLC進行使用者資料終止的LAP會導致在WAN中斷期間無線連線中斷。

相反，您可以利用傳統LWAPP控制平面的AP架構來執行任務，例如動態配置管理、AP軟體升級和無線入侵檢測。這允許無線資料保留在本地位置，無線基礎設施得到集中管理，並可恢復廣域網中斷。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

1030 REAP架構簡介

Cisco 1030 REAP將LWAPP控制平面與無線資料平面分離，以便提供遠端功能。Cisco WLC仍以與常規LAP相同的方式用於集中控制和管理。不同之處在於，所有使用者資料都在AP本地橋接。在WAN中斷期間可以保持對本地網路資源的訪問。圖1顯示了基本REAP架構。

圖1:基本REAP架構圖

註：有關REAP功能與傳統LAP相比的基本差異的清單，請參閱附錄A。

何時應使用REAP AP?

Cisco 1030 REAP AP應主要在以下兩種情況下使用：

- 如果LAP和WLC之間的鏈路容易中斷，則可以使用1030 REAP在鏈路故障期間允許無線使用者不間斷地訪問資料。
- 如果所有使用者資料必須在本地終止（即在AP的有線埠終止，而不是在控制器終止，因為所有其他LAP都是如此），則1030 REAP可用於允許通過控制器介面和/或無線控制系統(WCS)進行集中控制。 這樣資料就能夠保留在本地位置。

如果覆蓋範圍或使用者密度要求單個站點上有兩個或三個1030 REAP AP，請考慮部署2006或2106 WLC。這些控制器最多可支援6個任意型別的LAP。與僅使用REAP的部署相比，這可以證明在財務上更可行，並提供一組超級特性和功能。

與所有1000系列AP一樣，單個1030 AP覆蓋面積約為5,000平方英尺。這取決於每個站點上的射頻(RF)傳播特性，以及所需的無線使用者數量及其吞吐量需求。在多數常見部署中，單個1000系列AP可同時支援12個使用者（在802.11b上為512kbps）和12個使用者（在802.11a上為2 mbps）。與基於802.11的所有技術一樣，介質訪問是共用的。因此，當更多使用者加入無線AP時，吞吐量會相應地共用。同樣地，隨著使用者密度增加和/或吞吐量要求的提高，請考慮新增本地WLC以節省每個使用者的成本並提高功能。

注意：您可以配置1030 REAP以與其他LAP相同的方式運行。因此，當新增WLC以擴展遠端站點的WLAN基礎設施時，可以繼續利用現有的REAP投資。

部署REAP

由於1030 REAP設計為放置在遠離WLC基礎架構的遠端站點，因此通常不採用用於發現和加入控制器的傳統零接觸方法LAP（如DHCP選項43）。相反，必須首先準備LAP，才能允許1030連線回中心站點的WLC。

啟動是一個過程，在此過程中LAP會獲得它們可以連線的WLC清單。加入單個WLC後，LAP將獲知移動組中的所有控制器，並配備加入組中任何控制器所需的所有資訊。有關移動組、負載平衡和控制器冗餘的詳細資訊，請參閱部署Cisco 440X系列無線LAN控制器。

為了在中心站點(例如網路運營中心(NOC)或資料中心)執行此任務，必須將REAP連線到有線網路。這麼做可讓使用者發現單個WLC。連線到控制器後，LAP會下載與WLAN基礎設施對應的LAP OS版本。然後，移動組中的所有WLC的IP地址都將傳輸到AP。這允許AP在其遠端站點通電後，在提供IP連線的情況下，從其清單中發現並加入利用率最低的控制器。

注意：DHCP選項43和域名系統(DNS)查詢也適用於REAP。請參閱部署Cisco 440X系列無線LAN控制器，瞭解如何在遠端站點配置DHCP或DNS以允許AP查詢中央控制器的資訊。

此時，如果需要，可以為1030指定靜態地址。這可確保IP編址方案與目的遠端站點匹配。此外，可以輸入WLC名稱以詳細列出每個LAP將嘗試連線哪三個控制器。如果這三個控制器失敗，LWAPP的自動負載平衡功能允許LAP從集群中的其餘控制器清單中選擇負載最小的AP。可以通過WLC命令列介面(CLI)或GUI編輯LAP配置，也可以通過WCS更輕鬆地編輯LAP配置。

注意：1030 REAP需要連線到的WLC在第3層LWAPP模式下運行。這表示需要為控制器指定IP地址。此外，WLC要求每個遠端站點都有一個DHCP伺服器可用，或者在啟動過程中必須分配靜態地址。控制器中嵌入的DHCP功能不能用於為1030s LAP或其使用者提供地址。

在關閉1030 LAP電源以便將其傳送到遠端站點之前，請確保每個1030都設定為REAP模式。這一點非常重要，因為所有LAP的預設設定都是執行常規的本地功能，而1030需要設定才能執行REAP功能。這可以通過控制器CLI或GUI在LAP級別完成，也可以通過WCS模板更輕鬆地完成。

基本REAP啟動功能

在將1030個REAP連線到移動組內的WLC後（在遠端站點放置REAP時，REAP將連線到該移動組），可以提供以下資訊：

所需的REAP設定

- 移動組中WLC的IP地址清單（在控制器/AP連線時自動提供）
- REAP AP模式（必須將AP配置為在REAP模式下運行才能執行REAP功能）

可選REAP設定

- 靜態分配的IP地址（基於每個AP的可選設定輸入）
- 主要、次要和第三級WLC名稱（基於每個AP或通過WCS模板的可選設定輸入）
- AP名稱（每個AP的可選資訊設定輸入）
- AP位置資訊（每個AP或通過WCS模板輸入的可選資訊設定）

REAP到控制器的鏈路要求

當您計畫部署REAP時，需要記住一些基本要求。這些要求涉及REAP LWAPP控制流量將經過的WAN鏈路的速度和延遲。1030 LAP旨在用於WAN鏈路，例如IP安全隧道、幀中繼、DSL（非PPPoE）和租用線路。

注意：1030 REAP LWAPP實施假定AP和WLC之間有1500位元組MTU路徑。由於MTU小於1500位元組，在傳輸過程中發生的任何分段會導致無法預測的結果。因此，1030 LAP不適合路由器主動將資料包分段為小於1500位元組的環境（例如PPPoE）。

WAN鏈路延遲尤其重要，因為預設情況下，每1030 LAP每30秒向控制器傳送一次訊號消息。心跳消息丟失後，LAP會連續傳送5個心跳，每秒傳送一次。如果沒有成功，LAP將確定控制器連線已斷開，1030s將恢復為獨立REAP模式。雖然1030 LAP可以容忍自身和WLC之間的大量延遲，但必須確保在LAP和控制器之間的延遲不超過100ms。這是因為客戶端計時器限制了客戶端在計時器確定身份驗證失敗之前等待的時間。

REAP限制

雖然1030 AP旨在進行集中管理，並在WAN鏈路中斷期間提供WLAN服務，但是REAP通過WLC連線提供的服務與連線中斷時提供的服務之間存在一些差異。

WLAN

1030 REAP最多可以支援16個WLAN（每個無線配置檔案包含服務集識別符號[SSID]，以及所有安全、QoS和其他策略），每個配置檔案具有自己的多基本服務集ID(MBSSID)，但是1030 REAP在與控制器的連線中斷時只能支援第一個WLAN。在WAN鏈路中斷期間，除第一個無線區域網外的所有無線區域網都將停用。因此，應將WLAN 1用作主WLAN，並相應地規劃安全策略。第一個WLAN的安全性尤為重要，因為如果WAN鏈路發生故障，後端RADIUS身份驗證也會發生故障。這是因為此類流量會通過LWAPP控制器平面。因此，沒有使用者被授予無線訪問許可權。

建議在第一個WLAN上使用本地身份驗證/加密方法，例如Wi-Fi保護訪問(WPA-PSK)的預共用金鑰部分。有線等效保密(WEP)已足夠，但由於已知的安全漏洞而不建議使用。在使用WPA-PSK（或WEP）時，配置正確的使用者仍可以訪問本地網路資源，即使WAN鏈路關閉。

注意：所有基於RADIUS的安全方法都要求身份驗證消息通過LWAPP控制平面傳輸回中心站點。因此，所有基於RADIUS的服務在WAN中斷期間不可用。這包括但不限於基於RADIUS的MAC身份驗證、802.1X、WPA、WPA2和802.11i。

1030 REAP只能駐留在單個子網上，因為它無法執行802.1q VLAN標籤。因此，每個SSID上的流量在有線網路上的同一子網中終止。這意味著，雖然無線流量可能在SSID之間通過空中分段，但在有

線端不會將使用者流量分開。

安全

1030 REAP可提供思科基於控制器的廣域網架構支援的所有第2層安全策略。這包括所有第2層身份驗證和加密型別，例如WEP、802.1X、WPA、WPA2和802.11i。如前所述，大多數這些安全策略都需要WLC連線進行後端身份驗證。WEP和WPA-PSK在AP級別完全實施，不需要後端RADIUS身份驗證。因此，即使WAN鏈路斷開，使用者仍可以連線。1030 LAP支援Cisco WLC中提供的客戶端排除清單功能。如果回到控制器的連線可用，則1030上的MAC過濾功能可以正常工作。

註：當AP處於獨立模式時，REAP不支援WPA2-PSK。

1030 LAP不提供所有第3層安全策略。這些安全策略包括Web驗證、基於控制器的VPN終止、ACL和對等阻塞，因為它們是在控制器上實施的。VPN傳遞對於連線到外部VPN集中器的客戶端起作用。但是，僅允許發往指定VPN集中器的流量（僅限VPN傳輸）的控制器功能則不允許。

網路位址轉譯(NAT)

REAP所連線的WLC不能駐留在NAT邊界之後。但是，如果用於LWAPP的埠(UDP埠12222和12223)轉發到1030，則遠端站點的REAP可以位於NAT盒後面。這意味著每個REAP必須具有靜態地址才能使埠轉發可靠地工作，並且每個NAT例項後面只能有一個AP。原因是每個NAT IP地址只能有一個埠轉發例項，這意味著在遠端站點的每個NAT服務後面只能有一個LAP。一對一NAT可以與多個REAP一起使用，因為LWAPP埠可以針對每個外部IP地址轉發到每個內部IP地址（靜態REAP IP地址）。

服務品質(QoS)

沒有基於802.1p優先順序位的資料包優先順序排序，因為REAP無法執行802.1q標籤。這表示不支援Wi-Fi多媒體(WMM)和802.11e。支援基於SSID和身份庫網路的資料包優先順序。但是，通過基於身份的網路分配的VLAN無法與REAP配合使用，因為它無法執行802.1q標籤。

漫遊和客戶端負載平衡

在存在多個REAP且預期存在AP間移動性的環境中，每個LAP必須位於同一個子網上。1030 LAP不支援第3層移動。通常，這不是限制，因為遠端辦公室通常沒有足夠的LAP來要求這種靈活性。

上游控制器連線可用時（僅在主機控制器上啟用了負載均衡），會在具有多個AP的站點中的所有REAP之間提供積極的客戶端負載均衡。

無線電資源管理(RRM)

當存在與控制器的連線時，1030 LAP會從WLC中的RRM機制接收動態通道和功率輸出。當WAN鏈路斷開時，RRM不起作用，並且通道和電源設定不會改變。

欺詐檢測和IDS功能

REAP架構支援所有與常規LAP相匹配的欺詐檢測和入侵檢測簽名(IDS)。但是，當與中央控制器失去連線時，不會共用收集的所有資訊。因此，遠端站點的RF域的可見性會丟失。

REAP限制摘要

附錄B中的表格總結了REAP在正常運行期間以及無法通過WAN鏈路連線到WLC時的功能。

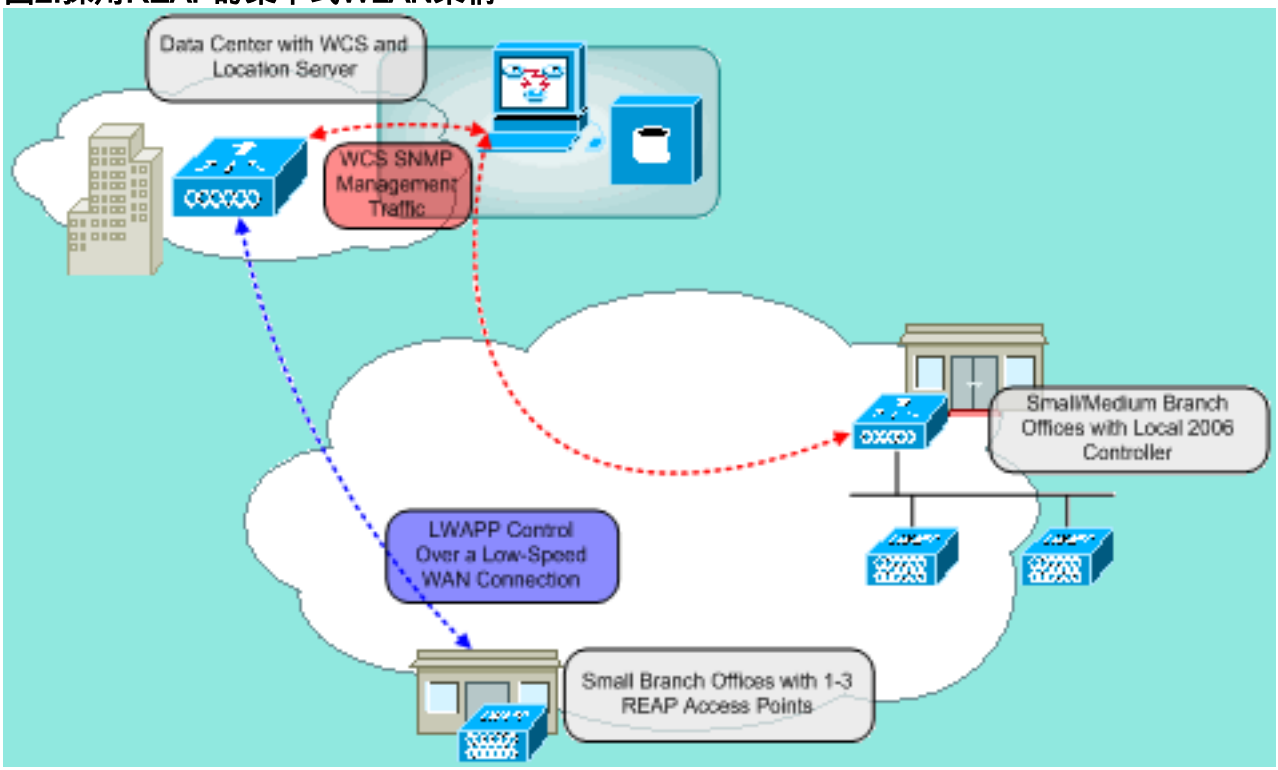
管理REAP和中央WLAN架構

1030 REAP管理與常規LAP和WLC無異。管理和配置全部在控制器級別完成，可通過每個控制器的CLI或Web GUI完成。通過WCS提供系統範圍的配置和網路可視性，所有控制器和AP（REAP或其他）都可以作為單個系統進行管理。當REAP控制器連線中斷時，管理功能也會中斷。

採用REAP的集中式WLAN架構

圖2顯示了集中式LWAPP架構的每個部分如何協同工作，以滿足各種無線網路需求。管理和定位服務通過WCS和2700定位裝置集中提供。

圖2:採用REAP的集中式WLAN架構



附錄A

REAP體系結構和常規LAP之間的主要區別是什麼？

- 如果DHCP選項43或DNS解析在遠端站點不可用，則必須首先在中央辦公室準備1030。然後，它將被運送到目標站點。
- WAN鏈路發生故障時，只有第一個WLAN保持活動狀態。需要RADIUS的安全策略將失敗。對於WLAN 1，建議使用WPA-PSK的身份驗證/加密。WEP工作正常，但不建議使用。
- 無第3層加密（僅第2層加密）
- REAP連線的WLC不能駐留在NAT邊界之後。但是，如果每個內部靜態REAP IP地址都將LWAPP埠(12222和12223)轉發給它們，則REAP可以。**注意**：不支援具有過載的埠地址轉換(PAT)/NAT，因為源自LAP的LWAPP流量的源埠可能隨時間而更改。這將中斷LWAPP關聯。REAP的NAT實施也會出現相同的問題，因為埠地址可能會改變，例如PIX/ASA，這取決於配置。

- 只有LWAPP控制消息通過WAN鏈路。
- 資料流量在1030的乙太網路連線埠上橋接。
- 1030 LAP不執行802.1Q標籤(VLAN)。 因此，來自所有SSID的無線流量會終止在同一有線子網上。

附錄B

正常和獨立REAP模式的功能有何差異？

		REAP（正常模式）	REAP（獨立模式）
通訊協定	IPv4	是	是
	IPv6	是	是
	所有其他通訊協定	是（僅當客戶端還啟用了IP時）	是（僅當客戶端還啟用了IP時）
	IP代理ARP	否	否
WLAN	Number of SSIDs	16	1（第一個）
	動態通道分配	是	否
	動態功率控制	是	否
	動態負載平衡	是	否
VLAN	多個介面	否	否
	802.1Q支援	否	否
WLAN安全性	欺詐AP檢測	是	否
	排除清單	是	是（僅現有成員）
	點對點封鎖	否	否
	入侵檢測系統	是	否
第2層安全	MAC身份驗證	是	否
	802.1X	是	否
	WEP（64/128/152位）	是	是
	WPA-PSK	是	是
	WPA2-PSK	是	否
	WPA-EAP	是	否
	WPA2-EAP	是	否
第3層安全	Web驗證	否	否
	IPsec	否	否
	L2TP	否	否
	VPN傳輸	否	否

	存取控制清單	否	否
QoS	QoS設定檔	是	是
	下行鏈路QoS（加權輪詢隊列）	是	是
	802.1p支援	否	否
	每使用者頻寬合約	否	否
	WMM	否	否
	802.11e（未來）	否	否
	AAA QoS設定檔覆寫	是	否
行動化	子網內	是	是
	子網間	否	否
DHCP	內部DHCP伺服器	否	否
	外部DHCP伺服器	是	是
拓撲	直接連線(2006)	否	否

相關資訊

- 含輕量AP和無線LAN控制器(WLC)的遠端邊緣AP(REAP)組態範例
- 統一無線網路中的AP負載均衡和AP回退
- 部署Cisco 440X系列無線LAN控制器
- 無線LAN控制器和輕量型存取點基本組態範例
- 技術支援與文件 - Cisco Systems