無線接入點術語表

目標

本文包含用於設定、配置和排除Cisco無線接入點(WAP)故障的術語清單。

適用裝置

- 無線存取器

一般術語清單

- 基於802.1Q的VLAN - IEEE 802.1Q規範建立了使用VLAN成員資訊標籤乙太網幀的標準方法，並定義了VLAN網橋的操作，允許定義、操作和管理橋接LAN基礎架構中的VLAN拓撲。802.1Q標準旨在解決如何將大型網路劃分為更小的部分的問題，以便廣播和組播流量不會使用不必要的更多頻寬。該標準還有助於在內部網段之間提供更高級別的安全性。
- 802.1X Supplicant客戶端 — 客戶端是802.1X IEEE標準的三個角色之一。802.1X的開發目的是在OSI模型的第2層提供安全保護。它由以下元件組成：Supplicant客戶端、身份驗證器和身份驗證伺服器。Supplicant客戶端是連線到網路以便訪問該網路上的資源的客戶端或軟體。 它需要提供憑證或憑證以取得IP位址，並成為該特定網路的一部分。請求方在經過身份驗證之前不能訪問網路的資源。
- ACL — 訪問控制清單(ACL)是網路流量過濾器和相關操作的清單，用於提高安全性。它阻止或允許使用者訪問特定資源。ACL包含允許或拒絕訪問網路裝置的主機。ACL可以用以下兩種方式之一定義：通過IPv4地址或IPv6地址。
- 頻段導向 — 高級負載平衡（更確切地稱為頻段導向）是一種檢測能夠在5 GHz頻段傳輸的裝置的功能。2.4 GHz頻段經常擁塞，並且會受到來自不同裝置（例如藍芽甚至微波爐）的干擾。此功能允許您的接入點將裝置引導到更最佳化的無線電頻率，從而提高網路效能。
- 頻寬利用率 — 頻寬利用率允許您設定通過通訊路徑成功傳輸資料的平均閾值。一些用於改進此功能的技術包括頻寬調節、管理、上限和分配。
- Bonjour — Bonjour允許使用組播DNS發現接入點及其服務。它向網路通告其服務並回答對其支援的服務型別的查詢，從而簡化小型企業環境中的網路配置。當在支援的WAP裝置上啟用Bonjour時，任何Bonjour客戶端都可以發現並訪問基於Web的實用程式，而無需事先配置。Bonjour同時在IPv4和IPv6網路中工作。
- 強制網路門戶 — 強制網路門戶方法強制網路上的LAN使用者或主機在正常訪問公共網路之前檢視特定網頁。強制網路門戶將Web瀏覽器轉變為身份驗證裝置。在允許訪問使用網路之前，網頁需要使用者互動或身份驗證。
- 通道隔離 — 已啟用通道管理的裝置會自動將無線無線電通道分配給集群中的其他WAP裝置。自動通道分配可降低與其集群之外的其他接入點的干擾，並最大化Wi-Fi頻寬以幫助保持無線網路上的通訊效率。
- 客戶端QoS — 客戶端服務品質(QoS)關聯是一個部分，它提供用於自定義無線客戶端QoS的其他選項。這些選項包括允許傳送、接收或保證的頻寬。使用者端QoS關聯也可以透過使用存取控制清單(ACL)來操作。
- 事件日誌記錄 — 系統事件是系統中需要注意的一些活動，以及為順利運行系統和防止故障而需要採取的必要措施。這些事件將記錄為日誌。系統日誌使管理員能夠跟蹤裝置上發生的特定事件。事件日誌對於網路故障排除、調試資料包流和監控事件非常有用。
- 快速漫遊 — 無線接入點之間的快速漫遊允許快速、安全、不間斷的無線連線，以實現即時應用（如FaceTime、Skype和Cisco Jabber）的無縫移動體驗。
- HTTPS — 超文本傳輸協定安全(HTTPS)是一種比HTTP更安全的傳輸協定。配置

HTTP/HTTPS伺服器時，可以通過HTTP和HTTPS連線管理接入點。某些Web瀏覽器使用HTTP，而其它瀏覽器使用HTTPS。存取點必須具有有效的安全通訊端層(SSL)憑證才能使用HTTPS服務。

- IPv4 - IPv4是用於識別網路中裝置的32位元定址系統。它是大多數電腦網路（包括Internet）中使用的編址系統。
- IPv6 — IPv6是用於識別網路中裝置的128位編址系統。它是IPv4的後繼路由器和電腦網路中使用的最新版本定址系統。IPv6目前正在全球推廣。IPv6地址由八個十六進位制數字欄位表示，每個欄位包含16位。IPv6地址分為兩部分，每部分由64位組成。第一部分是網路地址，第二部分是主機地址。
- LLDP — 鏈路層發現協定(LLDP)是在IEEE 802.1AB標準中定義的發現協定。LLDP允許網路裝置向網路中的其他裝置通告有關自身的資訊。LLDP使用邏輯鏈路控制(LLC)服務來向其他LLDP代理傳送和接收資訊。LLC為存取LDP提供連結服務存取點(LSAP)。每個LLDP幀作為單個MAC服務請求進行傳輸。LLC實體在MAC服務接入點(MSAP)處接收每個傳入LLDP幀作為MAC服務指示。
- 負載平衡 — 負載均衡是一種網路術語，用於將工作負載分佈到多台電腦、網路鏈路和多種其他資源上，以實現適當的資源利用率、最大化吞吐量、最大化響應時間，並主要避免過載。
- MAC ACL — 基於訪問控制清單(ACL)的介質訪問控制(MAC)是源MAC地址的清單。如果資料包從無線接入點傳到LAN埠，反之亦然，則此裝置將檢查資料包的源MAC地址是否與此清單中的任何條目匹配，並檢查ACL規則是否與幀內容匹配。然後使用匹配的結果來允許或拒絕此資料包。但是，將不會檢查從LAN到LAN埠的資料包。
- 多個SSID — 您可以在接入點上配置多個服務集識別符號(SSID)或虛擬接入點(VAP)，並為每個SSID分配不同的配置設定。所有SSID可能同時處於活動狀態。客戶端裝置可以使用任何SSID與接入點關聯。
- 工作模式 — WAP裝置可以充當單點對點模式接入點、點對多點網橋和中繼器。在點對點模式下，單個WAP裝置接受來自客戶端和網路中其他裝置的連線。在點對多點橋接模式下，單個WAP裝置作為多個接入點之間的公共鏈路運行。WAP裝置也可以作為中繼器，它可以在相距遙遠的接入點之間建立連線。無線客戶端可以連線到此中繼器。可以將無線分佈系統(WDS)角色系統與中繼器的角色進行比較。
- 資料包捕獲 — 資料包捕獲是網路裝置的一項功能，通過該功能，您可以捕獲並儲存裝置傳送和接收的資料包。網路協定分析器可以分析捕獲的資料包，以排除故障或最佳化效能。捕獲的資料包檔案可以通過HTTP/HTTPS或TFTP伺服器下載。它可以被共用，然後進一步分析以理解網路中的資料包流。Packet Capture（資料包捕獲）頁可用於配置遠端或本地資料包捕獲、下載資料包捕獲檔案或檢視當前捕獲狀態。
- QoS — 服務品質(QoS)允許您為不同的應用程式、使用者或資料流確定流量的優先順序。它還可以用來保證效能達到指定的水準，從而影響客戶的服務品質。QoS通常受以下因素影響：抖動、延遲和丟包。
- RADIUS伺服器 — 遠端驗證撥入使用者服務(RADIUS)是一種用於連線和使用網路服務的裝置的驗證機制。用於集中身份驗證、授權和記帳。RADIUS伺服器透過輸入的登入憑證驗證使用者的身分，以調控網路的存取。例如，在大學校園中安裝了公共Wi-Fi網路。只有具有密碼的學生才能訪問這些網路。RADIUS伺服器會檢查使用者輸入的密碼，並在適當情況下授權或拒絕存取。
- 遠端管理 — 遠端管理從遠端位置操作網路裝置的設定。這通常在電腦、交換機、路由器等具有IP地址的裝置上完成。它使網路管理員能夠快速響應請求或挑戰，因為他們不必親臨現場。在遠端管理中訪問裝置與本地操作幾乎一樣，不同之處在於，裝置的本地IP地址用於在本地訪問裝置，而在遠端裝置上訪問裝置時則使用裝置的WAN IP。
- 無管理AP檢測 — 無管理AP(AP)是指未經系統管理員明確授權而安裝在網路上的接入點。欺詐接入點會帶來安全威脅，因為任何能夠訪問該區域的人都可以故意或不知情地安裝無線接入點，以允許未經授權的使用者訪問網路。您的接入點上的Rogue AP Detection（欺詐AP檢測）功

能允許它檢視該範圍內的這些欺詐接入點，並在基於Web的實用程式中顯示其資訊。您可以將任何授權接入點新增到受信任接入點清單。

- RSTP — 快速生成樹協定(RSTP)是STP的增強功能。RSTP可在拓撲更改後提供更快的生成樹收斂。STP可能需要30到50秒來響應拓撲更改，而RSTP在配置的Hello時間的3倍之內做出響應。RSTP向後相容STP。
- 排程程式 — 無線排程程式有助於為虛擬接入點(VAP)或無線電的運行安排時間間隔，這有助於節省電源並提高安全性。最多可以將16個配置檔案關聯到不同的VAP或無線電介面，但每個介面只允許一個配置檔案。每個配置檔案可以具有特定數量的時間規則，用於控制相關VAP或WLAN的運行時間。
- 單點設定 — 單點設定是一種簡單的多裝置管理技術，允許您部署和管理一組支援此功能的接入點。它提供了從單個點配置一組接入點而不是單獨配置它們的便利性。它還允許您本地或遠端管理接入點。
- SNMP — 簡單網路管理協定(SNMP)是儲存和共用有關網路裝置資訊的網路標準。SNMP可促進網路管理、疑難排解和維護。
- 生成樹 — 生成樹協定(STP)是LAN上使用的網路協定。STP的目的是確保LAN無環路拓撲。STP通過一種演算法消除環路，該演算法保證兩個網路裝置之間只有一個活動路徑。STP可確保流量在網路中採用儘可能最短路徑。如果活動路徑出現故障，STP還可以自動重新啟用冗餘路徑作為備份路徑。
- SSID — 服務集識別符號(SSID)是無線客戶端可以連線到無線網路中所有裝置或在無線網路中所有裝置之間共用的唯一識別符號。區分大小寫，並且不得超過32個字母數字字元。這也稱為無線網路名稱。
- SSID廣播 — 當無線裝置在區域內搜尋其可以連線的無線網路時，它將通過其網路名稱或SSID檢測其範圍內的無線網路。預設情況下，SSID的廣播已啟用。但是，您也可以選擇禁用它。
- TSPEC — 流量規範(TSPEC)是從支援QoS的無線客戶端傳送到請求為其代表的流量流(TS)進行一定數量網路訪問的WAP裝置的流量規範。
- VLAN — 虛擬區域網(VLAN)是一種交換網路，它按功能、區域或應用進行邏輯分段，而不考慮使用者的物理位置。VLAN是一組主機或埠，它們可以位於網路中的任何位置，但進行通訊的方式就像它們位於同一個物理網段上一樣。VLAN允許您在不更改任何物理連線的情況下將裝置移動到新的VLAN，從而有助於簡化網路管理。
- WDS — 無線分佈系統(WDS)是一種功能，可在網路中實現接入點的無線互連。它使使用者可以通過多個接入點無線擴展網路。WDS還會保留接入點之間鏈路上的客戶端幀的MAC地址。此功能至關重要，因為它為漫遊客戶端提供了無縫體驗，並允許管理多個無線網路。
- WMM - Wi-Fi多媒體(WMM)是一項為不同型別的流量分配不同進程優先順序的功能。WMM也是QoS功能，它通過根據以下四個類別設定無線資料包的優先順序來增強無線網路的效能：語音、影片、盡力而為和背景。預設情況下，WMM已啟用。如果應用程式不需要WMM，則其優先順序低於影片和語音。
- 無線隔離 — 阻止連線到不同SSID的電腦之間的通訊和檔案傳輸。一個SSID上的流量不會轉發到任何其他SSID。
- WPA/WPA2 — Wi-Fi保護訪問（WPA和WPA2）是用於無線網路的安全協定，用於通過加密無線網路傳輸的資料來保護隱私。WPA和WPA2都與IEEE 802.11e和802.11i向前相容。與有線等效保密(WEP)安全協定相比，WPA和WPA2改進了身份驗證和加密功能。

Mesh網路中的術語清單

- **接入點(AP)**:網路中用於允許使用者以無線方式連線到網路的裝置。根據其功能，可能會新增特定的標籤：主要、遠端、根、從屬等
- **無線網狀網路：**無線接入點彼此連線以中繼資訊的一種拓撲。這些網路可動態調整需求並保持所有使用者的連線。

- **主AP:**主AP提供對無線網路和拓撲的管理和控制。它是使用Internet服務提供商(ISP)連線到外部網路其餘部分（通常是Internet）的網橋。 主AP直接連結到本地路由器，而本地路由器又將流量路由到WAN ISP介面。主AP是網狀網路中提供無線服務的所有節點的協調器。它管理來自網路上節點的資訊、每個客戶端的連線品質和鄰居資訊，以便做出最佳路由決策，將最佳化的無線服務輸出到移動客戶端。
- **主要主要：**當前負責管理WLAN的AP。
- **首選主要：**一種設定，其中將特定支援Primary的AP列為首選。如果主AP發生故障，首選主AP將接管。首選AP恢復後，不會自動切換回。您沒有指定首選主要。
- **主要支援的AP:**具有回網路的物理有線連線的AP。此AP需要連線到乙太網，並且如果主AP出現故障，可以成為主AP。
- **網狀延伸器：**網路中未連線到有線網路的遠端從屬AP。
- **從屬AP:**一個通用術語，可以應用於未配置為主節點的任何網狀AP。
- **父AP:**父AP是提供返回主AP的最佳路由的AP。
- **子AP:**子AP是網狀延伸器，它選擇父AP作為返回主AP的最佳路由。
- **上游AP:**上游AP是一個通用術語，指從客戶端到伺服器的資料流經AP的方向。
- **下游AP:**下游AP將資料從Internet向下傳輸到客戶端。
- **共置AP:**回傳通道的廣播範圍內的網狀延伸器。
- **節點：**在本文中，AP稱為節點。一般來說，節點描述在網路中建立連線或進行互動的任何裝置，或者能夠傳送、接收和儲存資訊、與網際網路通訊並具有IP地址的任何裝置。在網狀網路中，所有節點上的最佳化無線電引數可確保最大無線覆蓋範圍，同時減少節點之間的無線電干擾，以提供卓越的資料速度和吞吐量。
- **回傳：**在無線網狀網路中，區域網(LAN)中的資訊需要到達有線接入點才能到達網際網路。回傳是將資訊傳回有線存取點的程式。