無線訪客接入常見問題

目錄

簡介

本文檔提供有關無線訪客接入功能（思科統一無線網路的一部分）的最常見問題(FAQ)的資訊。

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

通向不安全網路區域的Ethernet over IP(EoIP)隧道是什麼？

思科建議使用專用於訪客流量的控制器。此控制器稱為訪客錨點控制器。

訪客錨點控制器通常位於非安全網路區域，通常稱為非軍事區(DMZ)。源自流量的其他內部WLAN控制器位於企業LAN中。在內部WLAN控制器和訪客錨點控制器之間建立EoIP通道，以確保訪客流量與企業資料流量的路徑隔離。路徑隔離是訪客訪問的一項關鍵安全管理功能。它確保安全和服務品質(QoS)策略可以分開，並在訪客流量和企業或內部流量之間加以區分。

Cisco Unified Wireless Network架構的一個重要功能是使用EoIP隧道將一個或多個調配的WLAN（即SSID）靜態對映到網路內的特定訪客錨點控制器。所有流量（包括往返於對映WLAN的流量）都經過在遠端控制器和訪客錨點控制器之間建立的靜態EoIP隧道。

使用此技術，所有關聯的訪客流量可以透明地通過企業網路傳輸到位於不安全網路區域中的訪客錨點控制器。

如何選擇要部署為訪客錨點控制器的正確控制器？

訪客錨點控制器的選擇是訪客流量量的函式，該流量由活動訪客客戶端會話數定義，或者由控制器上的上行鏈路介面容量定義，或者同時由兩者定義。

每個訪客錨點控制器的總吞吐量和客戶端限制如下：

- Cisco 2504無線LAN控制器 — 4 * 1 Gbps介面和1000訪客客戶端
- Cisco 5508無線LAN控制器(WLC)- 8 Gbps和7,000個訪客使用者端
- Cisco Catalyst 6500系列無線服務模組(WiSM-2)- 20 Gbps和15,000個使用者端
- Cisco 8500無線LAN控制器(WLC)- 10 Gbps和64,000使用者端

注意:Cisco 7500 WLC無法配置為訪客錨點控制器。如需支援訪客錨點功能的WLC清單，請參閱哪些控制器可用於在不安全網路區域支援訪客存取？。

每個控制器的資料庫中最多可儲存2048個訪客使用者名稱和密碼。因此，如果活動訪客憑證的總數超過此數字，將需要多個控制器。或者，訪客憑證可以儲存在外部RADIUS伺服器中。

網路中的存取點數量不會影響訪客錨點控制器的選擇。

訪客錨點控制器上可終止多少個Ethernet over IP(EoIP)通道？

一個訪客錨點控制器最多可以從內部WLAN控制器終止71個EoIP隧道。除WLC-2504外，所有型號的思科無線LAN控制器的此容量都相同。2504控制器最多可以終止15個EoIP隧道。如果需要其他通道，可配置多個訪客錨點控制器。

每個WLAN控制器對EoIP隧道進行計數，與每個EoIP中隧道化的WLAN或安全集識別符號(SSID)的數量無關。

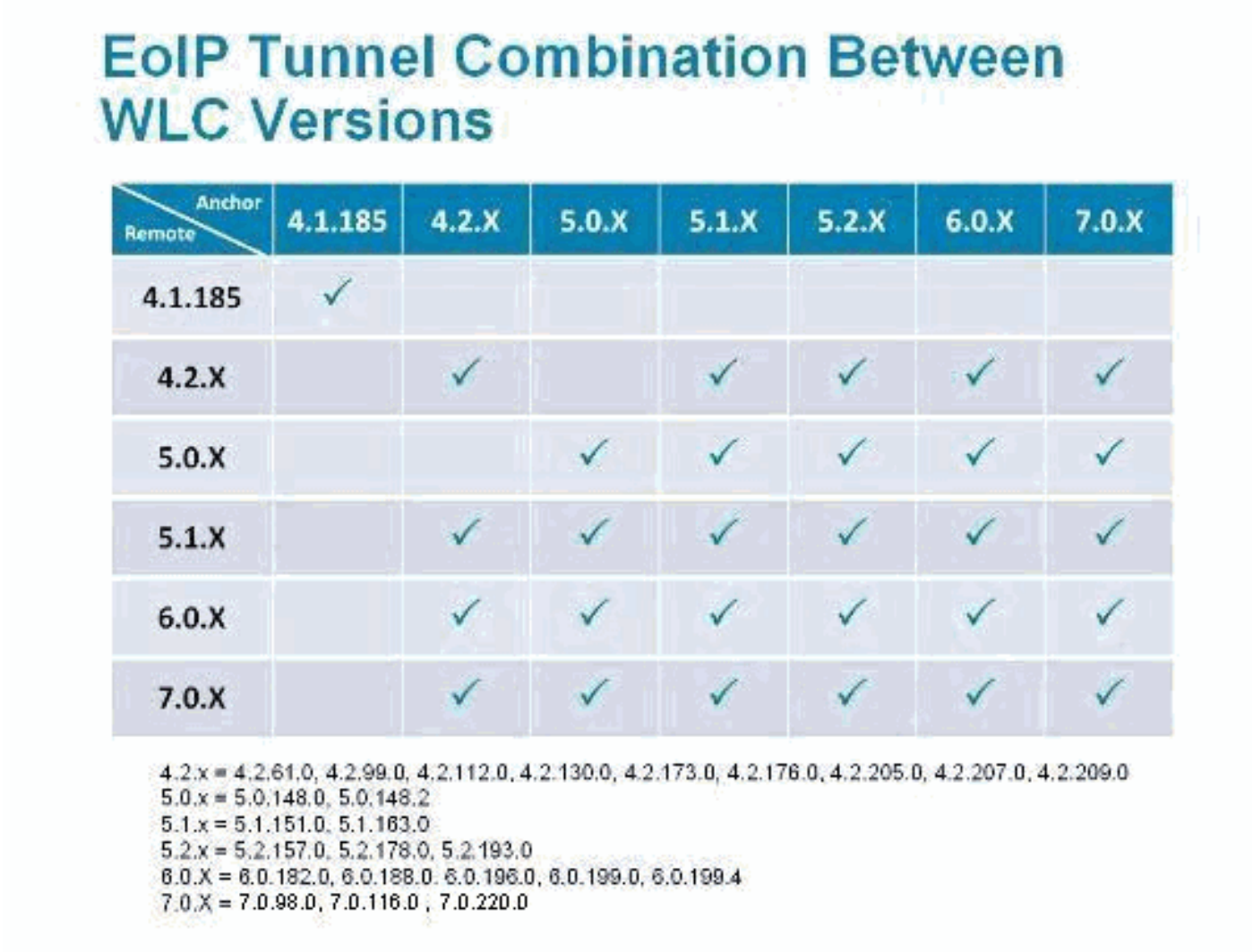
在訪客錨點控制器與每個支援具有訪客客戶端關聯的接入點的內部控制器之間配置一個EoIP隧道。

能否在運行不同軟體版本的控制器之間建立Ethernet over IP(EoIP)隧道？

並非所有無線LAN控制器軟體版本都支援此功能。在這種情況下，遠端和錨點控制器應執行相同版

本的WLC軟體。但是，最近的軟體版本允許遠端控制器和錨點控制器具有不同的版本。

此矩陣列出了可用於建立EoIP隧道的無線LAN控制器軟體版本。



Cisco 2100/2500系列無線LAN控制器能否用作非安全網路區域中的訪客錨點控制器？

是，從Cisco Unified Wireless Network Software 7.4版開始，Cisco 2500系列無線LAN控制器可以終止（最多15個EoIP隧道）防火牆之外的訪客流量。Cisco 2000系列無線LAN控制器只能發起訪客通道。

適用於整合式服務路由器（WLCM或WLCM2）的Cisco無線LAN控制器模組是否可作為訪客錨點控制器用於非安全網路區域？

不能，WLCM或WLCM2無法終止訪客隧道。WLCM只能發起訪客隧道。

哪些控制器可用於支援非安全網路區域中的訪客接入？

在具有版本4.0或更高版本軟體映像的思科無線LAN控制器平台中支援訪客隧道錨點功能，包括EoIP隧道終止、Web身份驗證和訪客客戶端訪問控制：

- Cisco Catalyst 6500系列無線服務模組(WiSM2)
- Cisco WiSM-2系列無線LAN控制器
- Cisco Catalyst 3750G整合式無線LAN控制器
- Cisco 5508 系列無線 LAN 控制器
- Cisco 2500系列無線LAN控制器（軟體版本7.4中引入的支援）

如果在防火牆之外使用訪客錨點控制器，會開啟哪些防火牆埠供訪客訪問使用？

在訪客錨點控制器和遠端控制器之間的任何防火牆上，需要開啟以下埠：

- 傳統移動性：用於使用者資料流量的IP協定97,UDP埠16666
- 新移動性：UDP埠16666和16667

若要進行可選管理，需要開啟以下防火牆埠：

- SSH/Telnet - TCP埠22/23
- TFTP - UDP埠69
- NTP - UDP埠123
- SNMP - UDP埠161（獲取和設定）和162（陷阱）
- HTTPS/HTTP - TCP埠443/80
- 系統日誌 — TCP埠514
- RADIUS驗證/帳戶UDP埠1812和1813

訪客流量能否通過配置了網路地址轉換(NAT)的防火牆？

在穿過防火牆的EoIP隧道上必須使用一對一NAT。

在錨點 — 外部WLC的情況中，哪個WLC會傳送RADIUS計量？

在此案例中，驗證一律由錨點WLC完成。因此，錨點WLC會傳送RADIUS計量。

> **註**：在中央Web驗證(CWA)和/或授權變更(CoA)部署中，應在錨點上停用RADIUS計量，且只能在外部WLC上使用。

內部控制器和錨點控制器之間的訪客通道失敗。我在WLC中看到以下日誌：`mm_listen.c:5373 MM-3-INVALID_PKT_RECVD10.40.220.180.0.0.0.`為什麼？

您可以在WLANs頁面上從WLC GUI檢查通**道的狀**態。按一下WLAN附近的下拉框，然後選擇**Mobility Anchor**，其中包含控制狀態和資料路徑。出現錯誤訊息的原因如下：

1. 錨點和內部控制器位於不同版本的代碼上。確保它們運行相同版本的代碼。
2. 移動錨點配置中的配置錯誤。檢查DMZ是否自我設定為行動錨點，以及內部WLC是否將DMZ WLC設定為行動錨點。有關如何設定行動錨點的詳細資訊，請參閱思科無線LAN控制器組態設定指南7.0版中的設定自動錨點行動性一節。這將導致訪客使用者無法傳遞流量。

在無線訪客接入設定中，客戶端不會從DHCP伺服器接收IP地址。Thu Jan 22 16:39:09 2009: XX:XX:XX:XX:XX:XX:XX:XX DHCP dropping REPLY from Export-Foreign STA錯誤消息出現在內部控制器上。為什麼？

在無線訪客接入設定中，訪客錨點控制器和內部控制器中的DHCP代理設定必須匹配。否則，來自客戶端的DHCP請求將被丟棄，您將在內部控制器上看到以下錯誤消息：

```
Thu Jan 22 16:39:09 2009: XX:XX:XX:XX:XX:XX  DHCP dropping REPLY from Export-Foreign STA
```

使用以下命令以變更WLC上的DHCP代理設定：

```
(Cisco Controller) >config dhcp proxy ?

enable          Enable DHCP processing's proxy style behaviour.
disable         Disable DHCP processing's proxy style behaviour.
```

在兩台控制器上使用**show dhcp proxy**命令，以驗證兩台控制器是否具有相同的DHCP代理設定。

```
(Cisco Controller) >show dhcp proxy

DHCP Proxy Behaviour: enabled

(Cisco Controller) >
```

如果訪客流量通過隧道傳輸到不安全的網路區域，訪客客戶端從哪裡獲取IP地址？

訪客流量通過EoIP在第3層在企業內傳輸。因此，可以在訪客錨點控制器上本地實現動態主機配置協定(DHCP)服務的第一點，或者訪客錨點控制器可以將客戶端DHCP請求中繼到外部伺服器。這也是處理網域名稱系統(DNS)位址解析的方法。

思科無線區域網控制器是否支援用於訪客身份驗證的Web門戶？

思科無線LAN控制器（軟體版本3.2或更高版本）提供內建的Web門戶，可捕獲訪客憑證以進行身份驗證，並提供簡單的品牌功能，以及顯示免責宣告和可接受的使用策略資訊的功能。

如何自定義Web門戶？

有關如何自訂Web輸入網站的資訊，請參閱選擇Web驗證登入頁面。

如何管理訪客憑證？

您可以使用思科無線控制系統(WCS)版本7.0和/或網路控制系統(NCS)版本1.0集中建立和管理訪客憑證。網路管理員可以在WCS內建立一個許可權有限的管理帳戶，該帳戶允許「游說大使」訪問，以便建立訪客憑證。在WCS或NCS中，具有接待大使帳戶的人員能夠為充當訪客錨點控制器的控制器建立、分配、監控和刪除訪客憑證。

大堂大使可以輸入訪客使用者名稱（或使用者ID）和密碼，或者可以自動生成憑證。還有一個全域性配置引數，允許所有訪客使用一個使用者名稱和密碼，或者為每個訪客使用一個唯一的使用者名稱和密碼。

要在WCS上配置前廳大使帳戶，請參閱思科無線控制系統配置指南7.0版中的建立訪客使用者帳戶部分。

除無線控制系統(WCS)或NCS外，思科無線LAN控制器中是否還提供大堂大使功能？

會。如果未部署WCS或NCS，則網路管理員可以在訪客錨點控制器上建立游說大使帳戶。使用接待大使帳戶登入訪客錨點控制器的人員將只能訪問訪客使用者管理功能。

如果有多個訪客錨點控制器，則必須使用WCS或NCS在多個訪客錨點控制器上同時配置使用者名稱。

有關如何使用無線LAN控制器建立大堂大使帳戶的資訊，請參閱思科無線LAN控制器組態設定指南7.0版中的建立大堂大使帳戶一節。

是否可以使用外部身份驗證、授權和記帳(AAA)伺服器對訪客進行身份驗證？

會。訪客驗證要求可以中繼到外部RADIUS伺服器。

訪客登入時會發生什麼情況？

當無線訪客透過Web輸入網站登入時，訪客錨點控制器會執行以下步驟來處理驗證：

1. 訪客錨點控制器檢查其本地資料庫的使用者名稱和密碼，如果存在使用者名稱和密碼，則授予訪問許可權。
2. 如果訪客錨點控制器上本地沒有使用者認證存在，訪客錨點控制器會檢查WLAN組態設定，以確認是否已為訪客WLAN設定外部RADIUS伺服器。如果是，控制器會使用使用者名稱和密碼建立RADIUS存取要求封包，並將其轉送到選定的RADIUS伺服器以進行驗證。
3. 如果沒有為WLAN設定特定RADIUS伺服器，控制器會檢查其全域RADIUS伺服器組態設定。任何設定有驗證「網路使用者」選項的外部RADIUS伺服器，都將使用訪客使用者的憑證進行查詢。否則，如果未選擇任何伺服器「網路使用者」，且使用者尚未通過步驟1或步驟2進行身份驗證，則身份驗證將失敗。

是否可以跳過訪客使用者身份驗證並僅顯示網頁免責宣告選項？

會。無線訪客訪問的另一個配置選項是完全繞過使用者身份驗證並允許開放訪問。但是，在授予訪問許可權之前，可能需要向訪客提供可接受的使用策略和免責宣告頁面。為此，可為訪客WLAN設定Web原則傳輸。在此案例中，訪客使用者被重新導向至包含免責宣告資訊的Web入口頁面。為了啟用訪客使用者的標識，直通模式還允許使用者在連線前輸入電子郵件地址。

我們是否需要在同一移動組上部署遠端控制器和訪客錨點控制器？

不能。訪客錨點控制器和遠端控制器可以位於不同的移動組中。

如果有多個訪客SSID，是否可以將每個WLAN(SSID)定向到唯一的網頁門戶？

會。單個或多個WLAN上的所有訪客流量都會重新導向至一個網頁。從WLC 4.2版或更高版本開始，每個WLAN均可定向到唯一的Web入口頁面。請參閱思科無線LAN控制器組態設定指南7.0版中的每WLAN分配登入、登入失敗和登出頁面一節。

WLC 7.0版（Mac過濾器失敗時的WebAuth）中的新設定有什麼功能？

如果WLAN同時設定了第2層(mac-filter)和第3層安全性(webauth-on-macfilter-failure)，則當其中任一端傳遞時，使用者端會移至RUN狀態。如果它發生第2層安全(mac-filter)，則客戶端會移至第3層安全(webauth-on-macfilter-failure)。

如果為代理伺服器配置了瀏覽器，客戶端是否正常運行？

在版本7.0之前，當瀏覽器中配置了代理伺服器時，客戶端無法建立TCP連線。版本7.0後，新增了此WebAuth Proxy伺服器支援，且可以在控制器上設定代理伺服器IP位址和連線埠。

是否有無線訪客接入部署指南？

這是指向部署指南的連結：

部署指南：使用思科無線LAN控制器的思科訪客接入

是否有有線和無線訪客接入設計手冊？

以下是設計手冊的連結：

- 思科整合無線訪客存取服務
- 使用Cisco WLAN控制器的有線訪客存取組態範例

相關資訊

- **使用Cisco WLAN控制器的有線訪客存取組態範例**
- **部署指南：使用思科無線LAN控制器的思科訪客接入，版本4.1**
- **技術支援與文件 - Cisco Systems**

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。