無線訪客接入常見問題

目錄

簡介

本文檔介紹有關無線訪客接入功能（Cisco Unified Wireless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。

什麼是連線非安全網路區域的Ethernet over IP (EoIP)隧道？

思科建議為訪客流量使用一個專用控制器。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，通常稱為隔離區(DMZ)。流量來源的其他內部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隧道，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，並區分訪客流量和企業或內部流量。

Cisco統一無線網路架構的一個重要功能是能夠使用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（往返對映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透過企業網路傳輸到位於非安全網路區域中的訪客錨點控制器。

如何選擇正確的控制器以部署為訪客錨點控制器？

訪客錨點控制器的選擇是訪客流量量的函式，該流量量由活動訪客客戶端會話數定義，或由控制器上的上行鏈路介面容量定義，或兩者都定義。

每個訪客錨點控制器的總吞吐量和客戶端限制如下：

- Cisco 2504無線區域網控制器- 4 * 1 Gbps介面和1000個訪客客戶端
- Cisco 5508無線區域網控制器(WLC) - 8 Gbps和7,000個訪客客戶端
- Cisco Catalyst 6500系列無線服務模組(WiSM-2) - 20 Gbps和15,000客戶端
- Cisco 8500無線LAN控制器(WLC) - 10 Gbps和64,000個客戶端

註： Cisco 7500 WLC不能配置為訪客錨點控制器。有關支援訪客錨點功能的WLC的清單，請參閱哪些控制器可用於支援非安全網路區域中的訪客接入？。

每個控制器的資料庫最多可儲存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，就需要多個控制器。或者，訪客憑證可以儲存在外部RADIUS伺服器中。

網路中的存取點數目不會影響訪客錨點控制器的選擇。

在訪客錨點控制器上可以有多少個Ethernet over IP (EoIP)隧道終端？

一個訪客錨點控制器最多可以終止來自內部WLAN控制器的71個EoIP隧道。除WLC-2504外，任何型號的思科無線LAN控制器的此容量都相同。2504控制器最多可以端接15個EoIP隧道。如果需要額

外的隧道，可以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中隧道式WLAN或安全集識別符號(SSID)的數量無關。

在訪客錨點控制器與支援具有訪客客戶端關聯的存取點的每個內部控制器之間配置了一個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，遠端和錨點控制器必須執行相同版本的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隧道的無線區域網控制器軟體版本。

EoIP Tunnel Combination Between WLC Versions

Anchor / Remote	4.1.185	4.2.X	5.0.X	5.1.X	5.2.X	6.0.X	7.0.X
4.1.185	✓						
4.2.X		✓		✓	✓	✓	✓
5.0.X			✓	✓	✓	✓	✓
5.1.X		✓	✓	✓	✓	✓	✓
6.0.X		✓	✓	✓	✓	✓	✓
7.0.X		✓	✓	✓	✓	✓	✓

4.2.x = 4.2.61.0, 4.2.99.0, 4.2.112.0, 4.2.130.0, 4.2.173.0, 4.2.176.0, 4.2.205.0, 4.2.207.0, 4.2.209.0
5.0.x = 5.0.148.0, 5.0.148.2
5.1.x = 5.1.151.0, 5.1.163.0
5.2.x = 5.2.157.0, 5.2.178.0, 5.2.193.0
6.0.X = 6.0.182.0, 6.0.188.0, 6.0.196.0, 6.0.199.0, 6.0.199.4
7.0.X = 7.0.98.0, 7.0.116.0 , 7.0.220.0

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

是的，從Cisco統一無線網路軟體版本7.4開始，Cisco 2500系列無線區域網控制器可以終止（最多15個EoIP隧道）防火牆外的訪客流量。Cisco 2000系列無線區域網控制器只能發起訪客隧道。

Cisco Wireless LAN Controller Module for Integrated Services Routers （WLCM或WLCM2）能否用作非安全網路區域中的訪客錨點控制器？

否，WLCM或WLCM2無法終止訪客通道。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？

具有4.0版或更高版本軟體映像的以下思科無線區域網控制器平台支援訪客隧道錨點功能，包括EoIP隧道終端、Web身份驗證和訪客客戶端的訪問控制：

- 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，需要為訪客接入打開哪些防火牆埠？

在訪客錨點控制器和遠端控制器之間的任何防火牆上，這些埠都需要打開：

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

對於可選管理，需要打開以下防火牆埠：

- 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身份驗證/帳戶UDP埠1812和1813

在配置了網路地址轉換(NAT)的情況下，訪客流量能否透過防火牆？

透過防火牆的EoIP隧道必須使用一對一NAT。

在「錨點-外部WLC」方案中，哪個WLC將傳送RADIUS記帳？

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。

注意：在中央Web驗證(CWA)和/或授權變更(CoA)部署中，必須在錨點上停用RADIUS記帳，且僅用於外部WLC。

內部控制器和錨點控制器之間的訪客隧道出現故障。我在WLC中看到以下日誌：mm_listen.c：5373 MM-3-INVALID_PKT_RECVD：收到來自10. 40.220.18的無效資料包。Source member：0.0.0.0。source member unknown.。為什麼？

請在WLAN頁面上的WLC GUI中檢查隧道狀態。按一下WLAN旁邊的下拉框並選擇Mobility Anchors，其中包含控制和資料路徑的狀態。出現錯誤消息的原因如下：

1. 錨點和內部控制器位於不同的程式碼版本上。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。有關如何配置移動錨點的詳細資訊，請參閱Cisco無線LAN控制器配置指南7.0版中的配置自動錨點移動部分。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，客戶端不從DHCP伺服器接收IP地址。Thu Jan 22 16:39:09 2009： XX：XX：XX：XX：XX：XX：XX DHCP dropped 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此錯誤消息：

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

使用以下命令更改WLC上的DHCP代理設定：

```
<#root>

(Cisco Controller) >

config dhcp proxy ?


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

在兩個控制器上使用show dhcp proxy命令，以驗證兩個控制器是否具有相同的DHCP代理設定。

```
<#root>

(Cisco Controller) >

show dhcp proxy


DHCP Proxy Behaviour: enabled

(Cisco Controller) >
```

如果訪客流量透過隧道傳輸至非安全網路區域，那麼訪客客戶端從哪裡獲取IP地址？

訪客流量是在第3層透過EoIP在企業內傳輸的。因此，可以實施動態主機配置協定(DHCP)服務的第一點是在訪客錨點控制器上的本地點，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。

Cisco無線區域網控制器是否支援用於訪客身份驗證的Web門戶？

思科無線區域網控制器軟體版本3.2或更高版本提供了一個內建Web門戶，可捕獲用於身份驗證的訪客憑證並提供簡單的標籤功能，還能夠顯示免責宣告和可接受的使用策略資訊。

如何自定義Web門戶？

有關如何自定義Web門戶的資訊，請參閱選擇Web身份驗證登入頁。

如何管理訪客憑證？

可以使用Cisco Wireless Control System (WCS) 7.0版和/或Network Control System (NCS) 1.0版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，允許「接待大使」訪問，以便建立訪客憑證。在WCS或NCS中，擁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。

接待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。此外，還有一

個全局配置引數，它允許對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中配置接待大使帳戶，請參閱Cisco Wireless Control System配置指南7.0版中的建立訪客使用者帳戶部分。

除了Wireless Control System (WCS)或NCS以外，Cisco無線區域網控制器是否還提供了接待大使功能？

會。如果未部署WCS或NCS，網路管理員可以在訪客錨點控制器上建立接待大使帳戶。使用接待大使帳戶登入訪客錨點控制器的人員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。

有關如何使用無線區域網控制器建立接待大使帳戶的資訊，請參閱Cisco無線區域網控制器配置指南7.0版中的建立接待大使帳戶部分。

能否使用外部身份驗證、授權和記帳(AAA)伺服器對訪客進行身份驗證？

會。訪客身份驗證請求可以中繼到外部RADIUS伺服器。

當訪客登入時將發生什麼情況？

當無線訪客透過Web入口登入時，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，如果它們存在，則授予訪問許可權。
2. 如果訪客錨點控制器上沒有本機使用者認證，訪客錨點控制器會檢查WLAN組態設定，以檢視是否已為訪客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，並將其轉送到選取的RADIUS伺服器進行驗證。
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，都會使用訪客使用者的憑證進行查詢。否則，如果沒有伺服器選取「網路使用者」，且使用者尚未透過步驟1或2進行驗證，則驗證會失敗。

是否可以跳過訪客使用者身份驗證並只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式訪問。但是，在授予訪問許可權之前，可能需要向訪客顯示可接受的使用策略和免責宣告頁面。為此，可針對Web原則傳遞設定訪客WLAN。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入口網站。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。

遠端控制器和訪客錨點控制器是否需要位於同一移動組中？

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，能否將每個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將重定向到一個網頁。從WLC 4.2版或更高版本開始，每個WLAN都可以定向到唯一的Web門戶頁。請參閱Cisco無線區域網控制器配置指南7.0版中的按每個WLAN分配登入、登入失敗和註銷頁部分。

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配置了第2層(mac-filter)和第3層安全性(webauth-on-macfilter-failure)，則當任一安全選項透過時，客戶端都會進入RUN狀態。如果第2層安全失敗(mac-filter)，客戶端將被移動到第3層安全失敗(webauth-on-macfilter-failure)。

如果為代理伺服器配置了瀏覽器，客戶端是否可以正常工作？

在版本7.0之前，在瀏覽器中配置代理伺服器時，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的部署指南？

這是部署指南的連結：

部署指南：使用思科無線區域網控制器的思科訪客接入

是否有有線和無線訪客接入的設計手冊？

以下是設計手冊的連結：

- Cisco Unified Wireless Guest Access Services
- 使用Cisco WLAN控制器的有線訪客接入配置示例

相關資訊

- 使用Cisco WLAN控制器的有線訪客接入配置示例
- 部署指南：使用Cisco無線區域網控制器4.1版的Cisco訪客接入
- 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）。