WGB漫遊：內部詳細資訊和組態

目錄

簡介

Cisco Workgroup Bridge(WGB)是設計和部署無線網路非常有用的工具，因為它允許非無線裝置獲得移動性。WGB提供了許多關於漫遊、安全訪問等詳細資訊，這些內容根據您的需求影響部署方案。

在代碼版本12.4(25d)JA和更新版本中，Cisco引入了一系列命令和更改，以最佳化在高速漫遊環境中使用WGB。

本檔案介紹WGB運作方式的不同方面，包括漫遊演演算法決策點，以及如何針對預期使用模式進行設定。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco無線LAN解決方案
- Cisco Workgroup Bridge

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

什麼是工作組橋？

WGB基本上是一個接入點(AP)，配置為充當通向基礎設施的無線客戶端，並為連線到其乙太網介面的裝置提供第2層連線。

典型的WGB部署具有以下元件：

- WGB裝置，通常至少具有一個無線電介面和一個乙太網介面
- 無線基礎設施，通常稱為根AP，可以是自治或統一。
- 連線到WGB的一個或多個有線客戶端裝置。本文檔未涵蓋混合角色場景（一個無線電作為WGB，一個無線電作為同一AP上的根節點）。

WGB主要有三種型別：

- **Cisco WGB**:Cisco WGB是任何基於Cisco IOS®的AP，配置為WGB（1130、1240、1250等）。 此模式使用IAPP協定通知網路基礎設施有關WGB在其乙太網介面上獲知的裝置的資訊。在這種情況下，無線LAN控制器(WLC)或根AP具有從WGB「掛起」的裝置的第2層可見性。
- **非Cisco WGB:**這是充當WGB的第三方裝置，將一個或多個有線裝置連線到無線基礎架構。它們不支援IAPP，或者僅允許單個有線裝置，或者提供MAC地址轉換機制，將所有有線客戶端隱藏在單個802.11 MAC地址後面。如果基礎架構是WLC，則這些型別的裝置需要對地址解析協定(ARP)和DHCP幀進行特殊處理，這是因為對控制器進行了安全檢查和幀處理。
- **配置為「通用WGB」的Cisco AP**:這是一種抑制IAPP機制的模式，因此WGB可用於思科基礎設施或第三方根AP。在這種情況下，WGB會獲取其乙太網客戶端的地址，將後面裝置的數量限製為1。

下一節將重點介紹用於自治或WLC基礎設施的Cisco WGB場景。

使用場景

典型的WGB使用示例包括：

- 將有線印表機連線到網路
- 不同的製造部署，在這些部署中，將電纜連線到有線裝置是不可行或不可行的
- 車載部署，其中WGB提供從汽車、地鐵等到室外無線網路的連線
- 有線監視器

每個範例在以下方面都有自己的要求：

- 支援將在無線基礎設施上運行的應用程式所需的頻寬
- 漫遊延遲容限 — 當裝置移動時，WGB從當前AP移動到下一個AP需要多長時間？
- 轉發時間容限 — 每次漫遊丟失多少幀？

印表機移動不多，因此漫遊要求較低。另一方面，安裝有WGB的列車需要對漫遊元件進行微調，以確保其移動時的正確行為。

影片流可能會有較大的頻寬需求，因此需要較高的無線資料速率。但是，遙測應用程式可能偶爾只需要幾幀。

必須從一開始就正確定義這些要求，因為它們不僅影響WGB的配置，而且影響無線基礎架構的設計方式。例如，AP位置、距離、電源級別、啟用速率等，都會影響漫遊特性。因此，如果需要高速漫遊，所有這一切都是一個關鍵點。

通常，您必須知道以下詳細資訊：

- 應用程式所需的頻寬是多少？
- 什麼是漫遊延遲容限？
- 應用程式能否正確處理網路連線斷開問題？是否有其他備份機制？
- 應用程式能否正確處理資料包丟失？（即使採用最佳無線設計，您也必須預計一定百分比的資料包丟失。）

本文檔沒有詳細說明如何為高速漫遊/室外設計RF環境。請參閱室外網狀部署指南。

漫遊

對於無線裝置而言，漫遊是其功能中非常關鍵的部分。

一般來說，漫遊意味著可以從一個AP移動到另一個AP，這兩個接入點都屬於同一個無線基礎架構。

由於漫遊需要從當前AP切換到下一個AP，因此會出現斷開連線或不提供服務的時間。這種斷線可能很小。例如，語音部署時間不到200毫秒，如果每個漫遊事件需要的安全性強制實施完全身份驗證，時間會更長，甚至幾秒鐘。

需要漫遊，以便裝置可以找到具有更好訊號的新父裝置，並且裝置可以繼續正確訪問網路基礎設施。同時，過多的漫遊可能會導致多個斷開連線或不使用服務的時間，從而影響訪問。對於流動裝置（例如WGB）而言，擁有良好的漫遊演算法以及足夠的配置功能以適應不同的RF環境和資料需求非常重要。

漫遊要素

- **觸發器**：每個客戶端實施都有一個或多個觸發或事件，當這些觸發或事件滿足時，裝置會移動到另一個父AP。示例：信標丟失（裝置不再偵聽來自AP的常規信標）、資料包重試、訊號級別、未收到資料、已收到取消身份驗證幀、使用中資料速率低等。可能的觸發器可能因客戶端實施不同而不同，因為它們未完全標準化。較簡單裝置的觸發設定可能較差，從而導致錯誤（粘滯客戶端）或不必要的漫遊。WGB支援前面介紹的所有元素。
- **掃描時間**：無線裝置(WGB)花一些時間搜尋潛在的父裝置。這通常意味著在不同通道上，對AP進行主動探測或被動偵聽。由於無線電必須掃描，這意味著WGB花費的時間與轉發資料不同。從此掃描時間起，WGB可以構建可以漫遊到的有效父級集合。
- **父選擇**：掃描時間之後，WGB可以檢查可能的父節點，選擇最佳父節點，並觸發關聯/身份驗證過程。有時，如果漫遊事件沒有顯著好處，則決策點可以是留在當前父交換機上（請記住，漫遊過多可能是不好的）。
- **關聯/身份驗證**：WGB繼續關聯到新的AP，通常涵蓋802.11身份驗證和關聯階段，並完成在SSID上配置的安全策略（WPA 2-PSK、CCKM、None等）。
- **流量轉發還原**：WGB在漫遊後通過IAPP更新更新其已知有線客戶端的網路基礎設施。此後，有線使用者端與網路的流量會重新傳輸。

配置指南 — 安全策略

在流動裝置上漫遊的一個重要方面是在基礎設施上實施的安全策略。有幾種選擇，每種都有好/壞點。以下是最重要的因素：

- **開啟** — 基本上沒有安全措施。這是所有策略中最快、最簡單的策略。主要的問題是不限制對基礎設施的未經授權的訪問，也不保護它不受攻擊，這會限制其在特定情形中的使用。例如，由於部署的純粹性，不可能有外部攻擊的地雷。
- **MAC地址身份驗證** — 安全級別基本上與開放級別相同，因為MAC地址欺騙是一種簡單攻擊。不建議使用，因為完成MAC驗證的時間增加了，這降低了漫遊速度。
- **WPA2-PSK** — 提供良好的加密級別(AES-CCMP)，但身份驗證安全取決於預共用金鑰的品質。對於安全措施，建議使用至少12個字元和隨機密碼。與預共用金鑰方法類似，由於金鑰在多個裝置上使用，如果金鑰被洩漏，需要在所有裝置上修改密碼。漫遊速度是可接受的，因為它是在6個幀交換中完成的，您可以計算完成漫遊速度所需的上/下時間界限，因為它不涉及任何外部裝置（無RADIUS伺服器等）。 一般情況下，這種方法在平衡問題和利益之後是首選方法。
- **802.1x的WPA2** — 使用可以單獨更改的每裝置/使用者憑據對以前的方法進行了改進。主要問題是對於漫遊，此方法無法在裝置快速移動或需要較短的漫遊時間時正常工作。通常，這使用相同的6幀加上EAP交換，EAP交換可在4到4之間。這取決於選擇的EAP型別和證書大小。通常，這需要10到20個訊框，加上radius伺服器處理的額外延遲。
- **WPA2+CCKM** — 此機制提供良好的保護，使用802.1x構建初始身份驗證，然後每次漫遊事件僅快速交換2幀。這樣可以快速漫遊。主要問題在於，在漫遊失敗的情況下，它會在802.1x上恢復。然後，在驗證CCKM後，再次開始使用CCKM。如果WGB上的應用程式在遇到問題時可以允許偶爾長時間漫遊，則可以將其用作PSK的最佳選項。

本文檔不涵蓋存在安全問題的不推薦的技術，例如LEAP、WPA-TKIP、WEP等。

配置WPA2-PSK

在WGB上，這非常容易設定。您需要SSID定義和無線電上的正確加密。

```
dot11 ssid wgbpsk
```

```
vlan 32
authentication open
authentication key-management wpa version 2
wpa-psk ascii YourReallySecurePSK!
no ids mfp client

interface Dot11Radio0
ssid wgbpsk
encryption mode ciphers aes-ccm
station-role workgroup-bridge
```

您的SSID名稱和預共用金鑰必須與您的網路基礎設施匹配。

使用802.1x配置WPA2

它基本上建立在以前的配置之上，增加了EAP配置檔案和身份驗證方法：

```
dot11 ssid wlan1
authentication open eap eap
authentication network-eap eap
authentication key-management wpa version 2
dot1x credentials wgb
dot1x eap profile eapfast
no ids mfp client
eap profile eapfast
!--- This covers the EAP method type used on your network. method fast ! ! dot1x credentials wgb
!--- This is your WGB username/password. username cisco password 7 1511021F0725 interface
Dot11Radio0 encryption mode ciphers aes-ccm ssid wlan1
```

使用CCKM配置WPA2

僅在WPA2上執行一個步驟，僅作一個小更改：在SSID配置上使用CCKM標誌。假設僅在WLC端為CCKM設定WLAN:

```
dot11 ssid wlan1
authentication open eap eap
authentication network-eap eap
authentication key-management cckm
dot1x credentials wgb
dot1x eap profile eapfast
no ids mfp client
```

所用方法的驗證

快速檢查WGB可以報告正在使用的加密和金鑰管理，例如CCKM:

```
wgb-1260#sh dot11 associations al
Address           : 0024.97f2.75a0     Name             : lap1140-etsi-1
IP Address        : 192.168.40.10      Interface        : Dot11Radio 0
Device            : LWAPP-Parent      Software Version : NONE
CCX Version       : 5                  Client MFP       : Off

State             : EAP-Assoc          Parent           : -
SSID              : wlan1
VLAN              : 0
Hops to Infra     : 0                  Association Id   : 1
```

```
Tunnel Address     : 0.0.0.0
Key Mgmt type      : CCKM                Encryption        : AES-CCMP

Current Rate       : m7.-                Capability        : WMM ShortHdr ShortSlot
Supported Rates    : 48.0 54.0 m0. m1. m2. m3. m4. m5. m6. m7.
Voice Rates        : disabled            Bandwidth         : 20 MHz
Signal Strength    : -59  dBm            Connected for     : 72 seconds
Signal to Noise    : 41  dB             Activity Timeout : 8 seconds
Power-save         : Off                 Last Activity     : 7 seconds ago
Apsd DE AC(s)      : NONE

Packets Input      : 12064               Packets Output    : 136
Bytes Input        : 2892798             Bytes Output      : 19514
Duplicates Rcvd    : 87                  Data Retries      : 8
Decrypt Failed     : 0                   RTS Retries       : 0
MIC Failed         : 0                   MIC Missing       : 0
Packets Redirected: 0                    Redirect Filtered: 0
```

配置漫遊

在WGB上，可以修改影響漫遊演算法的多個引數。

封包重試次數

預設情況下，WGB會重新傳輸64次幀。如果父節點未正確確認(ACK)，則會假設父節點不再有效，並開始掃描/漫遊進程。將此觸發器視為「非同步」漫遊觸發器，因為可以在傳輸失敗的任何時刻執行該觸發器。

用於配置此命令的命令位於dot11介面內，它採用以下選項：

```
packet retries NUM [drop]
```

編號:介於1和128之間，預設值為64。快速漫遊觸發器的正確數字通常為32。大多數射頻環境不建議使用較低的數字。

drop:如果不存在，WGB將在達到最大重試次數時啟動漫遊事件。存在時，WGB不會啟動新的漫遊，並使用其他觸發器，例如信標丟失和訊號。

RSSI監控

WGB可以為當前父節點實施主動訊號掃描，並在訊號低於預期水準時啟動新的漫遊過程。

此過程需要兩個引數：

- 計時器，每X秒喚醒一次檢查過程
- RSSI級別，用於在當前訊號低於該級別時啟動漫遊進程。

例如：

```
in d0
mobile station period 4 threshold 75
```

WGB完成身份驗證過程所需的時間不能更低，以便在某些情況下防止「漫遊環路」或避免過於激進的漫遊行為。一般情況下，應該測試它以檢視符合應用程式需求的裝置。

對於PSK，它可以低於基於EAP的方法（對於非常廣泛的應用程式，典型的是2和4）。

RSSI級別表示為正整數，儘管它基本上是正常的 — dBm測量級別。您應該使用比維持資料速率正常工作所需的最小值稍高的數字。例如，如果您希望的最小速率為6 mbps，則閾值RSSI為–87就足夠了。對於48 mbps，您需要–70 dBm等。

註：此命令還可以觸發「按資料速率更改漫遊」，該操作過於激烈。它必須與最低比率一起使用，以便取得良好結果。

最小資料速率

從12.4(25d)JA開始，思科新增了一個可配置的引數，以控制WGB何時觸發新的漫遊事件（如果到父級的當前資料速率低於給定值）。

這有助於確保維持所需的速度下限，以便支援影片或語音應用。

在此命令可用之前，WGB在發現速率低於之前的時間時頻繁觸發漫遊。基本上按時間X+1，如果速率低於前一次X時間，則WGB開始漫遊過程。在日誌中，您會看到以下消息：

```
*Mar  1 00:36:43.490: %DOT11-4-UPLINK_DOWN: Interface Dot11Radio1, parent lost: Had to lower
data rate
```

這過於激進，通常，唯一的解決方案是在WGB和父AP上配置單個資料速率。

現在，建議的方法是無論何時使用移動台週期命令，始終配置此命令：

```
in d0
mobile station  minimum-rate 2.0
```

這樣，只有在當前速率低於配置值時，才會觸發新的漫遊進程。這減少了不必要的波動，並允許保持預期的速率值。

註：即使使用此配置，也可能會發生「必須降低資料速率」消息，只是現在應該看到，當觸發移動台週期檢查時間時，WGB是否以低於配置速度的速度進行TX。

掃描通道

WGB會在執行漫遊事件時掃描所有「國家/地區通道」。這意味著根據無線電域，您可以在2.4 Ghz頻段上掃描1到11通道，或掃描1到13通道。

每個掃描的通道都需要一些時間。在802.11bg上，大約為10到13毫秒。在802.11a上，如果通道啟用了DFS，則最大可以達到150毫秒（因此，不是探測，只是在那裡執行被動掃描）。

一個好的最佳化是限制掃描的通道僅使用基礎設施正在使用的通道。這一點在802.11a上尤其重要，因為通道清單很大，而且如果使用DFS，每個通道的時間可能會很長。

設計WGB/漫遊的通道計畫需要注意三個方面：

- 對於2.4 GHz頻段，嘗試固定到1/6/11以最小化側通道干擾。使用4等的任何其他通道計畫都很難在不增加干擾的情況下從RF的角度進行正確設計。
- 從掃描的角度來看，為所有AP使用單通道設定是一個好主意。只有在要支援的客戶端總數非常低，並且沒有高頻寬要求時，才有意義。這樣從掃描時間中消除了無線電改變時間。請注意，很少有環境可以從此選項獲益，因此請謹慎使用。
- 對於5.0 GHz頻段，如果當地法規允許的話，使用室內非DFS通道（36到48）允許更快的掃描

時間，因為WGB可以主動探測每個通道，而不是被動偵聽更長的時間。
用於部署的管道計畫可能需要滿足其他要求。使用常規RF設計建議。

若要設定掃描通道清單：

```
in d0
mobile station scan 1 6 11
```

注意：移動台僅在無線電上使用WGB角色時顯示。

注意：確保WGB掃描清單與您的基礎設施通道清單匹配。否則，WGB將找不到可用的AP。

配置計時器

從12.4(25a)JA開始，有幾種新命令可在發現問題時最佳化恢復計時器，這些命令僅在AP處於WGB模式時可用。

```
wgb-1260(config)#workgroup-bridge timeouts ?

  assoc-response  Association Response time-out value
  auth-response   Authentication Response time-out value
  client-add      client-add time-out value
  eap-timeout     EAP Timeout value
  iapp-refresh    IAPP Refresh time-out value
```

在assoc-response、auth-response、client-add等情況下，這些指示WGB等待父AP應答的時間長度，然後才將AP視為失效並嘗試下一個候選。預設值為5秒，對於某些應用程式來說太長。最小計時器為800 ms，建議大多數移動應用使用。

在eap-timeout中，WGB設定等待的最長時間，直到完成完整的EAP身份驗證過程。這從EAP請求方的角度起作用，以便如果EAP驗證方沒有回接，則重新啟動進程。預設值為60秒。請注意不要配置可能低於完成完整802.1x身份驗證所需的實際時間的值。通常，將此值設定為2到4秒對於大多數部署來說是正確的。

對於iapp-refresh，預設情況下，WGB會在漫遊後生成對父AP的IAPP批次更新，以便通知已知的有線客戶端。大約10秒後關聯後會進行第二次重新傳輸。此計時器允許在關聯後進行IAPP批次的「快速重試」，以克服由於RF或尚未在父AP上安裝加密金鑰而導致第一個IAPP更新丟失的可能性。對於快速漫遊方案，可以使用100ms。但是，請確保使用大量WGB。這顯著增加了每次漫遊後傳送到基礎設施的IAPP總數。

聚合值示例：

```
workgroup-bridge timeouts eap-timeout 4
workgroup-bridge timeouts iapp-refresh 100
workgroup-bridge timeouts auth-response 800
workgroup-bridge timeouts assoc-response 800
workgroup-bridge timeouts client-add 800
```

已在移動WGB部署方案上成功測試了這些功能。

其他WGB最佳化

對於WGB部署方案，還需要考慮其他細微更改：

無線電相關

- 減少**rts retries** - **rts retries 32**。這樣可以在大量情況下節省一些RF時間。通常不需要這樣做。
- 天線型別：如果使用單個天線（無分集），則應配置無線電以提高總體效能：

```
antenna transmit right-a
antenna receive right-a
```

天線分集是理想的，但在車輛上實際安裝天線時並非總是可行。正確的天線選擇對於漫遊至關重要。2dB就意味著普通漫遊平均時間的巨大差異。

日誌相關

- 為了節省幾毫秒，請僅將控制檯日誌記錄級別降低為錯誤： **記錄控制檯錯**誤。請不要完全禁用它，因為它可能會在某些情況下對漫遊效能產生負面影響。
- 理想情況下，從乙太網端使用telnet或ssh來收集調試或日誌。與通過控制檯記錄調試相比，它對效能的影響要小得多：**logging monitor debugging**。
- 用於瞭解WGB漫遊視點發生情況的命令是**debug dot11 dot11 0 trace print uplink**。這對CPU的影響較小，但不會啟用其他調試選項，除非發出指示，因為每個選項都可能會增加總漫遊時間。
- 儘可能使用SNTP。這樣可保持WGB的同步時間，這對故障排除非常有用。

MFP使用情況

- 從安全的角度來看，MFP非常有用。但是，缺點是在漫遊失敗的情況下，如果來自AP父節點的去身份驗證幀因任何原因而發生錯誤，WGB不會接受這些幀來觸發新的漫遊。
- 在這些罕見的故障情形中，如果能夠聽到當前父級的RF訊號良好，則WGB可能需要5秒來觸發新掃描。有一個「捕獲全部」檢測機制，如果在此期間沒有收到有效資料幀，WGB可以觸發該機制。
- 預設情況下，如果SSID使用WPA2 AES，WGB將嘗試使用客戶端MFP。
- 如果需要快速的恢復時間（WGB對未受保護的deauth幀做出反應），建議禁用客戶端MFP。這是安全需求和快速恢復時間之間的折衷。決定取決於對部署方案更重要的內容。

```
dot11 ssid wgbpsk
   no ids mfp client
```

WGB和「時鐘儲存間隔」上的EAP-TLS

請參閱適用於Cisco IOS版本12.4(21a)JY的Cisco Aironet存取點和橋接器版本說明的將IOS請求者時鐘和儲存時間設定同步到NVRAM一節。

請記住，如果使用uWGB，uWGB可能永遠沒有機會執行sntp同步，因為它通常與連線的MAC地址關聯，而uWGB BVI沒有網路訪問許可權。因此，對於uWGB，建議在部署時至少在NVRAM中獲得良好的時鐘同步。如果連線的乙太網裝置能夠成為NTP源（以及通過其uWGB連線更新的客戶端），則可以考慮將uWGB sntp sync從其作為有效的NTP反射點。

完整配置示例

```
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname wgb-1260
!
logging rate-limit console 9
logging console errors
!
clock timezone CET 1
no ip domain lookup
!
!
dot11 syslog
!
!
dot11 ssid wgbpsk
   vlan 32
   authentication open
   authentication key-management wpa version 2
   wpa-psk ascii 7 060506324F41584B56
   no ids mfp client
!
!
!
!
!
!
username Cisco password 7 13261E010803
!
!
bridge irb
!
!
interface Dot11Radio0
no ip address
no ip route-cache
!
encryption mode ciphers aes-ccm
!
ssid wgbpsk
!
antenna transmit right-a
antenna receive right-a
  packet retries 32
station-role workgroup-bridge
rts retries 32
mobile station scan 2412 2437 2462
mobile station minimum-rate 6.0
mobile station period 3 threshold 70
bridge-group 1
!

interface GigabitEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
no keepalive
bridge-group 1
!
interface BVI1
ip address 192.168.32.67 255.255.255.0
```

```
no ip route-cache
!
ip default-gateway 192.168.32.1
no ip http server
no ip http secure-server

bridge 1 route ip

sntp server 192.168.32.1
clock save interval 1
workgroup-bridge timeouts eap-timeout 4
workgroup-bridge timeouts iapp-refresh 100
workgroup-bridge timeouts auth-response 800
workgroup-bridge timeouts assoc-response 800
workgroup-bridge timeouts client-add 800
```

調試分析

在任何發生的問題中，第一步必須捕獲**debug dot11 dot11 0 trace print uplink**命令的輸出。這樣可以很好地檢視漫遊過程中的情況。

以下是候選的當前父級示例：

```
 Sep 27 11:42:38.797: %DOT11-4-UPLINK_DOWN: Interface Dot11Radio0, parent lost: Signal strength
too low
 Sep 27 11:42:38.797: CDD051F1-0 Uplink: Lost AP, Signal strength too low
```

這是低訊號儀表觸發。它取決於移動台週期X閾值Y命令。第一個消息總是傳送到控制檯，第二個消息是上行鏈路調試跟蹤的一部分。這不是問題，而是正常WGB流程的一部分。

```
 Sep 27 11:42:38.798: CDD052C7-0 Uplink: Wait for driver to stop
```

上行鏈路進程在啟動通道掃描之前強制清除無線電隊列。此步驟可能花費幾毫秒到幾秒鐘，具體取決於通道利用率和隊列深度。資料幀未超時。語音幀已完成時間比較，因此應更快地丟棄。在雜訊環境中可能會觀察到一些延遲。

```
 Sep 27 11:42:38.798: CDD05371-0 Uplink: Enabling active scan
 Sep 27 11:42:38.799: CDD05386-0 Uplink: Scanning
```

這是正在發生的實際通道掃描。它為每個配置的通道將無線電保留大約10到13毫秒。

```
 Sep 27 11:42:38.802: CDD064CD-0 Uplink: Rcvd response from 0021.d835.ade0 channel 1 3695
```

這是收到的探測響應清單。第一個數字是通道，第二個數字是接收它所用的微秒。

```
 Sep 27 11:42:38.808: CDD078F1-0 Uplink: Compare1 0021.d835.ade0 - Rssi 58dBm, Hops 0, Count 0,
load 0
 Sep 27 11:42:38.809: CDD07929-0 Uplink: Compare2 0021.d835.cce0 - Rssi 46dBm, Hops 0, Count 0,
load 0
```

在以下詳細資訊中完成的實際比較：

```
 Sep 27 11:42:38.809: CDD07BDB-0 Uplink: Same as previous, send null data packet
```

父選擇

```
 Sep 27 11:42:38.809: CDD07BF7-0 Uplink: Done
 Sep 27 11:42:38.808: %DOT11-4-UPLINK_ESTABLISHED: Interface Dot11Radio0,
 Associated To AP AP1 0021.d835.ade0 [None WPAv2 PSK]Roaming completed.
```

這是漫遊已「完成」的點。 一旦父節點處理IAPP幀，流量就會恢復。

父比較資訊

```
 Sep 27 14:16:47.590: F515B1FF-0 Uplink: Compare1 0021.d835.7620 - Rssi 60dBm, Hops 0, Count 0,
load 3
 Sep 27 14:16:47.591: F515B238-0 Uplink: Compare2 0021.d835.e8b0 - Rssi 58dBm, Hops 0, Count -1,
load 0
```

如果「當前」AP仍與WGB關聯，則compare1將列印實際關聯計數–1（因此數字中不採用WGB本身），然後列印實際跳數和負載。

compare2列印差異。這就是可能看到負數的原因。如果測試的數值大於當前數值，則表示負數。

根據當前關聯計數、負載、訊號差異、移動閾值，WGB可能選擇也可能不選擇新的父項。

比較始終發生在兩個AP之間，所選的AP將替換下一個迭代的當前的AP。因此，某些決策可能是由於一個環路上的RSSI或下一個測試中的其他因素造成的。

相關資訊

- 如何在思科統一無線網路中使用帶EAP-TLS身份驗證的IOS WGB
- 技術支援與文件 - Cisco Systems