WGB漫游：内部详细信息和配置

目录

简介

思科工作组桥(WGB)是设计和部署无线网络非常有用的工具，因为它允许非无线设备获得移动性。WGB提供了有关漫游、安全访问等的许多详细信息，这些详细信息会根据您的需求影响部署方案。

在代码版本12.4(25d)JA及更高版本中，思科引入了一组命令和更改，以优化WGB在高速漫游环境中的使用。

本文档涵盖WGB工作方式的不同方面，包括漫游算法决策点，以及如何根据预期使用模式配置它。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科无线局域网解决方案
- 思科工作组桥

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

什么是工作组桥？

WGB基本上是一个接入点(AP)，配置为作为指向基础设施的无线客户端，并为连接到其以太网接口的设备提供第2层连接。

典型的WGB部署具有以下组件：

- WGB设备，通常至少具有一个无线电接口和一个以太网接口
- 无线基础设施，通常称为根AP，可以是自治或统一。
- 连接到WGB的一个或多个有线客户端设备。本文档不介绍混合角色场景（一个无线电作为WGB，一个无线电作为根在同一AP上）。

WGB有三种主要类型：

- **Cisco WGB**:Cisco WGB是任何基于Cisco IOS®的AP，配置为WGB（1130、1240、1250等）。 此模式使用IAPP协议将WGB在其以太网接口上学习的设备通知网络基础设施。在这种情况下，无线局域网控制器(WLC)或根AP具有第2层可见性，可以看到WGB上“挂起”的设备。
- **非Cisco WGB:**这是充当WGB的第三方设备，将一个或多个有线设备连接到无线基础设施。这些设备不支持IAPP，并且仅允许单个有线设备，或者提供MAC地址转换机制，将其所有有线客户端隐藏在单个802.11 MAC地址后面。如果基础设施是WLC，则这些类型的设备需要对地址解析协议(ARP)和DHCP帧进行特殊处理，因为需要在控制器上执行安全检查和帧处理。
- **配置为“通用WGB”的思科AP**:这是抑制IAPP机制的模式，因此WGB可用于思科基础设施或第三方根AP。在这种情况下，WGB会获取其以太网客户端的地址，将其后面的设备数量限制为1。

下一节重点介绍用于自治或WLC基础设施的Cisco WGB的场景。

使用场景

典型的WGB使用示例包括：

- 将有线打印机连接到网络
- 不同的制造部署，在这种情况下，将电缆连接到有线设备是不可行或不切实际的
- 车载部署，其中WGB提供从汽车、城域列车等到室外无线网络的连接
- 有线摄像头

每个示例在以下方面都有自己的要求：

- 支持将在无线基础设施上运行的应用所需的带宽
- 漫游延迟容限 — 设备移动时，WGB从当前AP移动到下一个AP需要多长时间？
- 转发时间容限 — 每个漫游丢失多少帧？

打印机移动不多，因此漫游要求较低。另一方面，安装了WGB的列车需要对漫游组件进行微调，以确保在漫游时的正确行为。

视频流可能需要大的带宽，因此需要高的无线数据速率。但是，遥测应用程序可能不时只需要几个帧。

从一开始就正确定义这些要求非常重要，因为它们不仅会影响WGB的配置，而且会影响无线基础设施的设计。例如，AP位置、距离、功率电平、启用率等都会影响漫游特性。因此，如果需要高速漫游，所有内容都是关键点。

一般来说，您必须了解以下详细信息：

- 应用所需的带宽是多少？
- 漫游延迟容限是什么？
- 应用程序能否正确处理网络断开？是否有其他备份机制？
- 应用程序能否正确处理丢包问题？（即使采用最佳无线设计，您也必须预期数据包丢失百分比。）

本文档未介绍如何为高速漫游/室外设计RF环境的详细信息。请参阅室外网状网部署指南。

漫游

对于无线设备，漫游是其功能的一个非常关键的部分。

基本上，漫游意味着能够从一个AP到另一个AP，两者都属于同一无线基础设施。

由于漫游需要从当前AP更改到下一个AP，因此会导致断开连接或无服务的时间。这种断开可能很小。例如，如果安全需要在每个漫游事件上强制执行完全身份验证，则语音部署时间不到200毫秒，甚至更长，甚至几秒钟。

需要漫游，以便设备能够找到信号最好的新父设备，并能够继续正确访问网络基础设施。同时，过多的漫游可能导致多个断开连接或时间不提供服务，从而影响访问。对于WGB等移动设备而言，拥有具备足够配置功能的良好漫游算法以适应不同的RF环境和数据需求非常重要。

漫游要素

- **触发器**：每个客户端实施都有一个或多个触发器或事件，当遇到这些触发器或事件时，这些触发器或事件会导致设备移动到另一个父AP。示例：信标丢失（设备不再听到来自AP的常规信标）、数据包重试次数、信号级别、未收到数据、已接收取消身份验证帧、使用中数据速率低等。可能的触发器可能不同于客户端实施，因为它们没有完全标准化。较简单的设备可能具有较差的触发器集，这会导致不良（粘滞客户端）或不必要的漫游。WGB支持之前描述的所有以前

元素。

- **扫描时间**：无线设备(WGB)需要花一些时间搜索潜在父设备。这通常意味着在不同的信道上运行，对AP执行主动探测或被动侦听。由于无线电必须扫描，这意味着WGB花费的时间与转发数据不同。从此扫描时间起，WGB可以构建可漫游到的有效父代集。
- **父项选择**：扫描时间后，WGB可以检查潜在父项，选择最佳父项并触发关联/身份验证过程。有时，如果漫游事件没有显着优势，则可以保持当前父节点的状态（请记住，漫游过多可能是坏的）。
- **关联/身份验证**：WGB继续关联到新AP，该AP通常涵盖802.11身份验证和关联阶段，并完成在SSID上配置的安全策略（WPA 2-PSK、CCKM、无等）。
- **流量转发恢复**：WGB在漫游后通过IAPP更新更新其已知有线客户端的网络基础设施。此后，到/从有线客户端到网络的流量将恢复。

配置指南 — 安全策略

移动设备漫游的一个重要方面是将在基础设施上实施的安全策略。有多种选择，每种选择都有好坏分。以下是最重要的：

- **打开** — 基本上没有安全。这是所有策略中最快速且更简单的策略。这主要有以下问题：不限制对基础设施的未授权访问，不提供针对攻击的保护，这将其使用限制在非常具体的场景。例如，由于部署的纯粹性质，可能没有外部攻击的地雷。
- **MAC地址身份验证** — 基本上与开放级别的安全级别相同，因为MAC地址欺骗是一种琐碎的攻击。由于MAC验证的完成时间增加，因此不建议使用，这会减慢漫游速度。
- **WPA2-PSK** — 提供良好的加密级别(AES-CCMP)，但身份验证安全取决于预共享密钥的质量。对于安全措施，建议密码至少为12个字符且随机。与预共享密钥方法类似，因为密钥在多台设备上使用，如果密钥被破坏，则需要在所有设备上修改密码。漫游速度是可接受的，因为它在6个帧交换中完成，并且您可以计算完成漫游的上/下时间范围，因为它不涉及任何外部设备（无RADIUS服务器等）。 通常，在平衡问题和优点后，此方法是首选方法。
- **WPA2 with 802.1x** — 这通过使用可单独更改的每设备/用户凭证对先前方法进行了改进。主要问题是，对于漫游，当设备移动速度快或需要较短的漫游时间时，此方法无法正常工作。通常，这使用相同的6个帧加上EAP交换，该交换可以介于4和up之间。这取决于选择的EAP类型和证书大小。通常，这需要10到20个帧，加上RADIUS服务器处理增加的延迟。
- **WPA2+CCKM** — 此机制提供良好的保护，使用802.1x构建初始身份验证，然后在每个漫游事件上快速交换2帧。这提供了非常快的漫游时间。主要问题是，如果漫游失败，它会恢复到802.1x。然后，在CCKM进行身份验证后再次开始使用CCKM。如果WGB顶部的应用程序能够容忍偶尔的漫游时间，以防出现问题，则可将其用作与PSK相比的最佳选项。

本文档不介绍存在安全问题（如LEAP、WPA-TKIP、WEP等）的不推荐技术。

配置WPA2-PSK

在WGB上，这非常易于配置。您需要SSID定义和无线电上的正确加密。

```
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名称和预共享密钥必须与您的网络基础设施相匹配。

使用802.1x配置WPA2

它基本建立在之前的配置之上，添加了EAP配置文件和身份验证方法：

```
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

在WPA2上只有一个步骤，只有一个微小的变化：在SSID配置上使用CCKM标志。这假设WLAN仅在WLC端配置为CCKM:

```
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
```

验证使用的方法

快速检查WGB可报告使用中的加密和密钥管理，例如在CCKM中：

```
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
```

配置漫游

在WGB上，您可以修改影响漫游算法的多个参数。

数据包重试次数

默认情况下，WGB会重新传输帧64次。如果父级未正确确认(ACK)，则会假设父级不再有效，并启动扫描/漫游进程。将此漫游视为“异步”漫游触发器，因为它可以在传输失败的任何时刻完成。

用于配置此命令的命令进入dot11接口，它采用以下选项：

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

数字:介于1和128之间，默认值为64。快速漫游触发器的好数字通常为32。在大多数RF环境中，不建议使用较低的数字。

丢弃:如果不存在，WGB会在达到最大重试次数时启动漫游事件。当存在时，WGB不会启动新漫游，并使用其他触发器，如信标丢失和信号。

RSSI监控

WGB可以对当前父交换机实施主动信号扫描，并在信号低于预期电平时启动新的漫游过程。

此过程需要两个参数：

- 计时器，每X秒唤醒检查过程
- RSSI级别，用于在当前信号低于该级别时启动漫游过程。

例如：

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

WGB完成身份验证过程所花费的时间不应低于此时间，以防止在某些情况下出现“漫游环路”或避免过于主动的漫游行为。一般来说，应测试它，看它能满足应用需求。

对于PSK，它可能比基于EAP的方法低（典型的2和4对于非常严重的应用）。

RSSI级别表示为正整数，尽管它基本上是正常 — dBm测量级别。您应使用比保持数据速率正常运行所需的最小值稍高的数字。例如，如果所需的最小速率为6 mbps，则阈值RSSI应足以满足–87。对于48 mbps，需要–70 dBm等。

注意：此命令还可以触发“通过数据速率更改漫游”，这太过激烈。它必须与最低速率一起使用，才能取得良好效果。

最低数据速率

从12.4(25d)JA开始，思科添加了可配置参数，以控制WGB何时应触发新漫游事件（如果当前父级数据速率低于给定值）。

这有助于确保保持所需的速度下限以支持视频或语音应用。

在此命令可用之前，当发现速率低于上次时，WGB会频繁触发漫游。基本上按X+1时，如果速率低于之前的X时间，WGB将启动漫游过程。在日志上，您会看到以下消息：

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

这太过严重，而且通常唯一的解决方案是在WGB和父AP上配置单一数据速率。

现在，建议始终配置此命令，无论何时使用移动站period命令：

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

因此，仅当当前速率低于配置的值时才会触发新漫游进程。这可减少不必要的波动，并允许保持预期的速率值。

注：即使使用此配置“”，只是现在，只有在触发移动台周期检查时WGB的TX速度低于配置速度时，才应看到此消息。

扫描通道

WGB在执行漫游事件时扫描所有“国家/地区信道”。这意味着，根据无线电域，您可以扫描2.4 Ghz频段上的信道1到11，或1到13。

每个扫描的信道都需要一些时间。在802.11bg上，此值约为10至13毫秒。在802.11a上，如果信道已启用DFS，则最长可达150毫秒（因此不进行探测，只在那里执行被动扫描）。

一个好的优化是限制扫描的信道仅使用基础设施所服务的信道。这在802.11a上尤其重要，因为通道列表很大，并且如果DFS正在使用，每个通道的时间可能很长。

为WGB/漫游设计信道计划时需要三点：

- 对于2.4 GHz频段，请尝试保持为1/6/11，以尽量减小旁路干扰。从RF的角度来看，任何其它具有4个信道等的信道规划都很难在不增加干扰的情况下正确设计。
- 从扫描角度来说，对所有AP使用单通道设置是一个好主意。只有在要支持的客户端总数非常少且没有高带宽要求时，这才有意义。这从扫描时间中消除了无线电更改时间。请注意，很少有环境能从此选项中获益，因此请谨慎使用。
- 对于5.0 GHz频段，如果您的本地法规允许，使用室内非DFS信道（36到48）可以加快扫描时间，因为WGB可以主动探测每个信道，而不是进行更长时间的被动侦听。

您的部署使用的渠道计划可能需要满足其他要求。使用一般的射频设计建议。

要配置扫描通道列表，请执行以下操作：

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

注意：仅当在无线电上使用WGB角色时，才会显示移动台。

注意：确保您的WGB扫描列表与您的基础设施通道列表匹配。否则，WGB将找不到您的可用AP。

配置计时器

从12.4(25a)JA开始，发现问题时有几个新命令可优化恢复计时器，这些命令仅在AP处于WGB模式时可用。

```
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的情况下，这些指示WGB在将AP视为失效并尝试下一个候选之前等待父AP应答的时间。默认值为5秒，对于某些应用程序来说太长。最小计时器为800毫秒，建议用于大多数移动应用。

在eap-timeout中，WGB设置最长等待时间，直到完整的EAP身份验证过程完成。如果EAP身份验证器未回复，则从EAP请求方的角度执行此操作以重新启动进程。默认值为 60 秒。切记不要配置比完成完整802.1x身份验证所需的实际时间低的值。通常，将此值设置为2到4秒对大多数部署都正确。

对于iapp-refresh，默认情况下，WGB在漫游后生成到父AP的IAPP批量更新，以通知已知有线客户端。在关联10秒后，会再次重新传输。此计时器允许在关联后对IAPP批量执行“快速重试”，以克服第一个IAPP更新因RF或尚未安装在父AP上的加密密钥而丢失的可能性。对于快速漫游场景，可使用100毫秒。但是，请确保使用大量WGB。这会显着增加每次漫游后发送到基础设施的IAPP总数。

累积值示例：

```
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
```

这些已在移动WGB部署方案上成功测试。

其他WGB优化

WGB部署方案还要考虑其他一些细微变化：

无线电相关

- 减少**rts重试 - rts retries 32。这可以节省一些RF时间在累积方案上。**通常不需要这样做。

- 天线类型:如果使用单个天线（无分集），则应配置无线电以提高一般性能：

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

天线分集是理想选择，但在车辆上实际安装天线时并不总能实现。正确选择天线对漫游至关重要。仅2 dB可能是一般漫游平均时间的巨大差异。

日志相关

- 为了节省一些毫秒，请将控制台日志记录级别降为仅错误： **记录控制台错误**。请勿完全禁用它，因为在某些情况下，它会对漫游性能产生负面影响。
- 理想情况下，从以太网端使用telnet或ssh来收集调试或日志。与通过控制台记录调试相比，这对性能的影响要小得多：**日志记录监控调试**。
- 要了解WGB漫游视点的情况，命令是**debug dot11 dot11 0 trace print uplink**。这对CPU的影响很小，但除非有指示，否则不要启用其他调试选项，因为每个选项都可能增加总漫游时间。
- 尽可能尝试使用SNTP。这将保持WGB同步时间，这对故障排除非常有帮助。

MFP使用

- 从安全角度来看，MFP非常有用。但是，缺点是，在漫游故障情况下，如果WGB和AP父交换机之间的加密密钥因任何原因出错，WGB不会接受来自AP的解身份验证帧来触发新的漫游。
- 在这些罕见的故障情况下，如果当前父级可以听到良好的RF信号，WGB可能会用5秒钟触发新扫描。如果在此期间未收到有效数据帧，WGB可以触发“全捕获”检测机制。
- 默认情况下，如果SSID使用WPA2 AES，WGB会尝试使用客户端MFP。
- 如果需要快速恢复时间（WGB对非保护的deauth帧做出响应），建议禁用客户端MFP。 这是安全需求与快速恢复时间之间的折衷。决策取决于对部署方案更重要的因素。

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

WGB上的EAP-TLS和“时钟保存间隔”

请参阅Cisco Aironet接入点和网桥的版本说明(Cisco IOS 12.4(21a)JY版)的同步IOS请求方时钟和节省时间设置到NVRAM部分。

请记住，如果使用uWGB，uWGB可能永远无法进行sntp同步，因为它通常与连接的MAC地址关联，并且uWGB BVI没有网络访问权限。因此，在uWGB的情况下，建议在NVRAM中至少在部署时获得良好的时钟同步。如果连接的以太网设备能够成为NTP源（以及通过其uWGB连接更新的客户端），则可以考虑将其中的uWGB sntp同步作为有效的NTP反射点。

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
```

调试分析

在出现任何问题时，首先必须捕获debug dot11 dot11 0 trace print uplink**命令的输出，**作为第一步。这可以很好地了解漫游过程中发生的情况。

以下是当前父代作为候选的示例：

```
 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
```

这是低信号的触发。它取决于移动台周期X阈值Y命令。第一条消息始终发送到控制台，第二条消息是上行链路调试跟踪的一部分。这不是问题，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
```

上行链路进程在开始信道扫描之前强制清除无线电队列。此步骤可能需要几毫秒到几秒，具体取决于信道利用率和队列深度。数据帧未超时。语音帧进行时间比较，因此应更快地丢弃。在噪音环境中可能会出现延迟。

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

这是正在进行的实际信道扫描。它为每个配置的信道保留大约10到13毫秒的无线电。

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

这是收到的探测响应列表。第一个数字是信道，第二个数字是接收信道所用的微秒。

```
 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
```

在以下详细信息中进行的实际比较：

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

父项选择

```
 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.
```

这是漫游“完成”的点。 IAPP帧一旦由父级处理，流量就会恢复。

父比较信息

```
 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“当前”AP仍是关联的WGB，则compare1将打印实际关联计数–1（因此WGB本身不在数字中），然后打印实际跳数和负载。

比较2会打印差异。这就是为什么可以看到负数的原因。如果测试的数值高于当前值，则显示负数。

根据当前关联计数、负载、信号差异、移动阈值，WGB可能选择或不选择新父级。

比较始终在两个AP之间进行，所选AP会替换当前的AP，以供下次迭代使用。因此，某些决策可能是由于一个环路上的RSSI，或是由于下一次测试中的其他因素。

相关信息

- 如何以EAP-TLS认证使用aIOS WGB在Cisco Unified 无线网络
- 技术支持和文档 - Cisco Systems