工作组网桥（WGB）实现漫游的内部细节和配置

介绍

思科工作组网桥（WGB）对于无线网络设计和部署是非常有用的工具，因为它允许非无线设备获得移动性。WGB 提供了许多漫游、安全接入等配置细节，根据您的具体需求，它将影响部署的方案。

在代码版本 12.4（25D）JA 和更高版本，思科推出了一套命令和变化，以优化高速漫游环境下 WGB 的使用。

本文档介绍了 WGB 如何工作，包括漫游算法的决策点，以及针对不同的用途模型如何配置它。

先决条件

要求

思科建议您具备下面这些知识：
* 思科无线局域网解决方案
* 思科工作组网桥

使用的组件

本文件并不限于特定的软件和硬件版本。

本文档中的资料是从一个特定实验室环境中的设备上生成的。本文档中使用的所有设备以缺省（默认）配置开始配置。如果您的网络是正在使用的生产系统，请确保您了解所有命令带来的潜在影响。

什么是工作组网桥（Work Group Bridge）？

WGB 基本上是一个无线接入点以无线客户端的行为关联基础设施并为第 2 层连接的设备提

供以太网连接。

典型的 WGB 部署需要下面这些组件：
* WGB 设备通常至少有一个无线电模块和一个以太网接口
* 无线网络基础设施通常被称为根无线接入点，它可以是自治型无线接入点或者被无线控制器管理的无线接入点。
* 一个或多个有线客户端设备可以连接到 WGB。本文档不包括混合部署的情况（例如同一双频无线接入点，一个无线电模块作为 WGB，另一个无线电模块作为根无线接入点使用）。

WGB 主要有三种类型：

* 思科 WGB：任何基于 Cisco IOS®操作系统的自治型无线接入点都可以配置为思科 WGB。这种模式使用 IAPP 协议将 WGB 以太网接口上学习的信息通知到网络基础设施。在这种情况下，无线控制器或根无线接入点就会具备对 WGB 2 层连接设备的可见性。
* 非思科 WGB：第三方设备配置作为 WGB 将一个或多个有线设备连接到无线网络基础设施。这些 WGB 不支持 IAPP，它们或者只允许一个单一的有线设备，或者提供 MAC 地址转换机制，将所有有线客户端隐藏在一个单一的 802.11 MAC 地址后面。这些类型的设备都需要对地址解析协议（ARP）和 DHCP 帧的特殊处理，如果无线网络基础设施是无线控制器，由于无线控制器上需要进行安全检查和帧处理，所以需要对这些 WGB 单独配置。
* 思科无线接入点配置为“通用 WGB”（uWGB）模式：此模式不需要 IAPP 的通告机制，所以该模式 WGB 可以连接思科无线网络基础设施或第三方无线接入点使用。在这种情况下，WGB 将使用其以太网客户端的地址，这限制了 WGB 背后的设备数量为一个。

下一节我们侧重于在配合自治型无线接入点或无线控制器这些网络基础设施工作的情况下如何配置和优化思科 WGB 的工作行为。

使用场景

使用 WGB 的典型例子包括：
* 连接有线网络打印机
* 不可能铺设电缆连接有线设备的生产环境部署
* 车辆内部署，WGB 提供车地连接
* 有线摄像机

每个例子有对应的要求：
* 支持无线基础设施上运行的应用程序所需的带宽
* 漫游延迟容忍 - WGB 从当前无线接入点漫游到下一个无线接入点需要多长时间？
* 转发时间容忍 - 每次漫游有多少帧丢失？

打印机安装后就不会移动，所以漫游的要求较低。另一方面列车安装 WGB 就需要对漫游的组成部分微调，以确保正确的漫游行为。

视频流对带宽要求高，因此，它需要无线数据传输速率高。然而，遥测技术的应用可能只需要每秒发送几个数据帧。

重要的是从一开始就正确定义需求，因为他们不仅会影响到如何配置 WGB，也会影响如何对无线网络基础设施进行设计。例如，无线接入点的部署位置、距离、发射功率水平、数据速率启用等，这都会影响漫游特性。因此如果需要高速漫游，上述所有的关键点都必须得到保证。

在一般情况下，你必须知道下列这些细节：
* 什么是应用程序所需的带宽？
* 什么是漫游延迟容忍？
* 网络断开时如何妥善处理应用？有额外的备份机制吗？
* 应用程序是否可以正确处理丢包？（即使基于最佳的无线设计，你也必须考虑到丢包的百分比。）

本文档不讨论如何设计一个高速漫游/室外射频环境的细节。

漫游

对于无线设备，漫游是其非常关键的一部分功能。基本上，漫游是指客户端从一个无线接入点转换到另一个无线接入点，两个无线接入点都属于相同的无线网络基础设施。

因为漫游需要从当前无线接入点的连接发生变化，因此会导致断线或没有服务的时间。这断线的可能非常小。例如，如果需要强制执行的安全策略对每次漫游事件充分验证，那么语音部署会有小于 200ms 或更长时间的无服务时间。

漫游时客户端需要找到一个新的更好信号的父节点使其可以继续正常访问网络基础设施。在同一时间，太多的漫游可能会导致服务中断从而影响访问。WGB 作为一个重要的移动设备，需要有足够的配置能力和良好的漫游算法以适应不同的射频环境和数据需求。

漫游的要素

* 触发器：每个客户端实现都会有一个或多个触发器导致设备移动到另一个父无线接入点。例如：信标丢失（设备没有听到定期从无线接入点发出的信标），数据重传，信号水平，没有收到的数据，接收到取消认证（deauthentication）帧，使用低数据传输速率等。可能的触发条件因不同的客户端而实现不同，因为漫游算法没有被 802.11 完全标准化。简单的设备实现可能只使用一个简单的触发设置，从而导致不良的（粘性客户端）或不必要的漫游。WGB 支持前述所有触发器元素。

* 扫描时间：无线装置（WGB）花费一些时间寻找潜在的父节点。这通常意味着 WGB 要在不同的信道进行主动探测或被动地侦听。由于要进行无线电扫描，这意味着 WGB 花费时间做别的事情而无法进行数据转发。在此扫描时间内，WGB 可以建立一个有效的可漫游到的父节点列表。
* 父节点的选择：WGB 扫描后可以检查潜在的父节点，选择最好的一个并触发关联/认证过程。有时候，WGB 的决定是保持当前的连接而不漫游（记住漫游太多也不好）。
* 关联/验证：WGB 关联到新的无线接入点，通常涵盖 802.11 认证和关联阶段，再加上完成 SSID 安全政策（WPA-PSK、CCKM 或开放等）的执行。
* 流量转发还原：WGB 在漫游后通过 IAPP 更新其有线客户端到无线网络基础设施。完成这一点后，网络恢复到/从有线客户端的流量转发。

配置安全策略

漫游移动设备上一个重要的方面是将要实施的安全政策是什么。安全策略选项包括：

* 开放 - 基本上没有安全保障。这是所有政策中最快最简单的。它不限制未经授权的访问，无法保证网络基础设施免受攻击，这就限制了它的使用。
* MAC 地址认证 – 与开放策略基本相同的安全水平，因为 MAC 地址欺骗是一个非常常见的攻击。不推荐使用，且由于需要时间才能完成 MAC 地址验证，这将减缓漫游过程。
* WPA2-PSK - 提供良好的加密（AES-CCMP），但认证的安全性取决于预共享密钥的复杂程度。出于安全方面的考虑，推荐最低 12 个随机字符的密码。类似于其它预共享密钥方法，在多个设备上使用时，如果受到威胁，需要跨所有设备修改密码。它的漫游速度是可以接受的，漫游时需要交互 6 个帧，你可以计算出完成认证的时间边界，因为它不涉及任何外部设备（没有 RADIUS 服务器等）。一般情况下，这种方法是平衡问题和获益后的首选之一。
* WPA2 与 802.1x - 使用每设备/用户凭证提高了灵活性，可以单独改变用户身份凭证。它的主要问题是设备快速漫游或需要漫游时间短时这种方法工作不正常。一般情况下，WGB 和无线接入点之间使用相同的 6 个帧交互，还要加上 EAP 4 路握手交互。还取决于 EAP 认证类型的选择和证书的大小。通常需要 10 至 20 个帧交互，加上附加的 RADIUS 服务器处理延迟。
* WPA2 和 CCKM - 这种机制提供了良好的安全保护，使用 802.1x 建立初始身份验证，然后交互 2 个帧实现快速安全漫游。它的主要问题是，在失败的漫游的情况下，它恢复到基于 802.1x 的漫游认证方式，然后再开始使用 CCKM 再次验证。如果 WGB 支持的应用程序可以容忍在出现问题时一个偶然的较长的漫游时间，它可以用来作为与 PSK 等同的最佳选择。

本文件不包括不推荐的有安全问题的技术，如 LEAP 、WPA-TKIP、WEP 等。

配置 WPA2-PSK

对于 WGB，这是相当简单的配置。您需要定义 SSID 和对无线电适当加密。

```
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
```

SSID 名称和预共享密钥需要匹配您的无线网络基础设施的配置。

配置 WPA2 与 802.1x

它基本上是建立在以前的配置上，增加了 EAP 配置和认证方法：

```
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

配置 WPA2 与 CCKM

配置只有一个微小的变化：在 SSID 配置中使用 CCKM 替换 WPA。只有无线控制器/自治型无线接入点在 WLAN 上配置了 CCKM 时可用：

```
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
```

验证所使用的方法

快速检查 WGB 报告中使用的加密和密钥管理方法，例如对于 CCKM：

```
wgb-1260#sh dot11 associations all
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

你可以修改 WGB 的参数来影响漫游算法。

数据包重传

默认情况下，WGB 将 64 次重传数据帧。如果没有适当的父节点的确认（ACK），WGB 假设当前连接的无线接入点不再是有效的，并开始扫描/漫游过程。您可以将其作为一个“异步”漫游触发，因为它可以在任何时刻发生。

到 dot11 接口配置下面命令可更改选项：

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

NUM 为 1 到 128 之间的数字，默认值为 64。保证良好快速漫游触发的数量通常为 32。大多数的射频环境不建议使用一个较低的数值。

drop：如果不配置，达到最大重试值后 WGB 开始漫游事件。如果配置，达到最大重试值后 WGB 不启动新的漫游，而是使用其他的触发器，如信标丢失和信号水平。

监测 RSSI

WGB 可以主动扫描当前父节点的信号，当信号低于预期水平开始一个新的漫游过程。

这个过程需要两个参数：
* 一个计时器，每 X 秒唤醒检查过程
* RSSI 水平，如果当前信号低于它则启动漫游过程

例如：

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

为了防止循环漫游，计时器时间不应低于 WGB 完成认证过程所需的时间，防止在一定条件下避免过于激进的漫游行为。在一般情况下，应通过测试确认应用需求后配置。

对于 PSK 安全策略，计时器时间数值可以低于 EAP 安全策略时的配置。

RSSI 水平为一个负的整数，基本上是一个正常的-dBm 水平。应该使用比最低需要保持的数据传输速率稍高的值。例如，如果您所需的最低数据传输速率为 6 Mbps，-87 阈值的 RSSI 应该是足够了。对于 48 Mbps，你需要-70 dBm。

注意：此命令也可以触发“数据传输速率变化引起的漫游”，这就漫游的太激进了。最好与最低数据传输速率一起使用才能获得最佳漫游效果。

最小数据速率

从 12.4(25d)JA 版本开始，思科添加了一个可配置参数，如果当前的数据传输速率低于给定值，WGB 触发新的漫游活动。这对于支持视频或语音应用，确保其在所需的数据传输速度是有益的。

在此命令可用之前，经常发现数据传输速率低于以前时 WGB 会频繁引发漫游。如果数据传输速率低于以前，WGB 开始漫游过程。在日志中你会看到下面消息：

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

这样漫游实在是太激进了，正常情况下，唯一的解决办法是在 WGB 和父节点上配置一个单一的数据传输速率。

现在推荐的方法是始终配置此命令：

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

如果目前的速度不低于配置的值，新的漫游过程不会触发，减少了不必要的漫游。

注意：之前的日志消息在配置了最低数据传输速率后仍然有可能出现，现在它只有在 WGB 以 RSSI 检测时间周期以低于配置的速率发送时被看到。

扫描信道

WGB 漫游时扫描所有信道。这意味着，根据国家不同在 2.4 GHz 频段它可以扫描信道 1 至 11 或 1 至 13。

扫描每个信道都需要一些时间。对于 802.11bg 大约需要 10 至 13 毫秒。对于在 802.11a 如果信道启用 DFS，它可以高达 150 毫秒（即使不主动探测，只是在做被动扫描）。

一个优化是限制扫描只有在提供服务的网络基础设施的信道。 这一点对于 802.11a 尤其特别重要。

设计 WGB /漫游信道计划时有三点注意事项：

* 对于 2.4 GHz 频段，尽量只扫描信道 1、6 和 11 以尽量减少信道干扰。
* 从扫描的角度看所有无线接入点使用单一信道设置是一个好主意。如果支持的客户端总数非常低且有不高的带宽要求时是适合的。这减少了无线电扫描时间。虽然一些环境可以受益于这个选项，但是请小心使用。
* 对于 5.0 GHz 频段，根据您所在国家地区的法规，使用室内非 DFS 信道（36 至 48）允许更快的扫描，WGB 可以使用主动探测机制而不是花较长时间的被动倾听每一个信道。

在您的部署使用的信道计划应尽可能适应用户需求。

为了配置扫描信道列表：

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

注意：mobile station 命令只在配置了 WGB 角色的无线电模块上显示。

注意：请确保您的 WGB 扫描列表匹配无线网络基础设施的信道列表。如果不匹配，WGB 将无法找到可用的无线接入点。

配置定时器

从 12.4(25a)JA 版本开始 WGB 加入了几个新命令以优化恢复定时器，当无线接入点作为 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

对于 assoc-response、auth-response、client-add 参数，它们指示 WGB 等待父无线接入点多长时间就认为其失效并考虑尝试下一个候选父无线接入点。默认值是 5 秒，这对于某些应用太长。最低的计时器数值是 800 毫秒，对大多数移动应用建议采用。

对于 EAP 超时(eap-timeout)参数，WGB 设置的最大等待时间，直到完整的 EAP 身份验证过程完成。如果 EAP 验证没有回答，这个参数从 EAP 请求者的角度重新启动该进程。默认值是 60 秒。小心配置该值，不应低于需要完成一个完整的 802.1x 认证所需的实际时间。通常情况下设置为 2 至 4 秒对于大多数部署是正确的。

对于 IAPP 刷新（iapp-refresh）参数，默认情况下 WGB 漫游后产生 IAPP 批量更新到父无线接入点以便将已知的有线客户端通知给无线网络基础架构。在重新关联 10 秒左右后进行第二次重传。此计时器可以实现关联后的 IAPP 批量更新“快速重传”，以克服由于射频或加密密钥尚未在父无线接入点安装造成的第一次 IAPP 更新丢失的可能性。在快速漫游的情况下，可以使用 100ms 数值。但显着增加了每次漫游后和无线网络基础设施之间 IAPP 交互的总数。

激进配置数值的例子如下：

```
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
```

上述数值已成功的在需要快速移动的 WGB 部署方案中测试验证。

其他 WGB 优化配置

考虑到 WGB 部署方案，另外还有其他一些小的配置改动可以进行优化：

无线电相关

* 降低 RTS 重试试 – 通过 rts retries 32 命令。激进漫游场景下这样可以节省一些射频时间。通常情况下，这是没有必要的。
* 天线类型：如果使用单一天线（不采用天线分集），应该配置以提高总体性能：

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

尽管天线分集是可取的，但物理安装在车辆上的天线并不总是可能实现分集。选择适当的天线是漫游的关键。即使是 2 分贝的差异对于漫游的平均时间影响也是巨大的。

日志相关

* 为了节省几毫秒，控制台日志级别为 errors，通过 logging console errors 命令实现。不要完全禁用它，因为它可能在一定条件下对漫游性能产生不利影响。
* 理想情况下，从以太网端口使用 telnet 或 ssh 收集调试信息或日志。这比在控制台收集调试信息或日志对性能的影响要低得多：通过 logging monitor debugging 命令实现。
* 查看 WGB 漫游时发生事件的命令：debug dot11 dot11 0 trace print uplink。这个命令对 CPU 的影响低，除非特别指示不要使用其他调试选项，因为可能会增加总的漫游时间。
* 在可能的情况下使用 SNTP 让 WGB 保持时间同步，这非常有利于故障排除。

管理帧保护（MFP）的使用

* MFP 从安全的角度来看是有益的。然而美中不足的是，漫游失败的情况下，WGB 并不能接受父无线接入点的取消认证帧触发一个新的漫游，因为两者之间的加密密钥已经不匹配了。
* WGB 对这些罕见故障的情况可以使用 5 秒时间触发一个新的扫描，如果当前的父无线接入点具有良好的射频信号可以被听到。如果没有有效的数据帧在这段时间内收到 WGB 将采取一个“抓所有的”检测机制。
* 如果 SSID 采用 WPA2/AES，默认情况下，WGB 尝试使用客户端 MFP。
* 如果需要快速恢复时间，建议禁用客户端 MFP。这是一个安全需求和快速恢复时间之间的妥协。取决于对于部署方案什么需求更重要。

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

WGB 和 EAP-TLS 以及“时钟保存时间间隔”

请参阅思科 Aironet 无线接入点和思科 IOS 版本 12.4（21A）JY 发行说明关于同步的 IOS 请求者时钟和保存时间设定到 NVRAM 中的描述 。

请记住，如果使用 uWGB，uWGB 永远不会有机会进行 SNTP 同步，因为它通常使用以太网连接的客户端的 MAC 地址且 BVI 接口不能访问网络。因此，在使用 uWGB 的情况下，建议在部署时有良好的时钟同步到 NVRAM 中。如果 uWGB 连接的以太网装置有能力成为一个 NTP 源，那么可以考虑将它作为有效的 NTP 反射点使得 uWGB 进行 SNTP 同步。

完全配置示例

```
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

发生任何问题时第一步就是捕获 debug dot11 dot11 0 trace print uplink 命令的输出。它可以提供漫游过程中发生事件的良好记录。

当前父节点作为候选的例子：

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

这由低信号水平触发。取决于 mobile station period X threshold Y 命令。第一条消息总是被发送到控制台，第二条是上行调试跟踪的一部分。本条日志没有什么问题，是正常 WGB 漫游过程的一部分。

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

上行过程中启动信道扫描前强制无线电队列清除。这一步可以从几毫秒到几秒钟的时间，根据信道的利用率和队列深度决定。在嘈杂的环境里可能会有一些延迟。

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

这是实际发生的信道扫描。对于配置的信道无线电大约花费 10 至 13 毫秒时间。

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

这是收到探测回复。第一个数字代表信道，第二个数字代表接收毫秒。

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

实际比较父节点：

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

父节点的选择：

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”点。父无线接入点处理 IAPP 帧后流量恢复。

父节点比较消息：

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

如果当前的无线接入点仍然关联 WGB，则相关的比较输出的实际关联计数为-1，后面是实际的跳数和负载。

根据目前的关联计数、负载、信号差异、移动阈值，WGB 可能会也可能不会选择一个新的父无线接入点。

比较始终是在两个无线接入点之间，选定的无线接入点取代当前连接无线接入点。因此，一些决定可能是基于 RSSI 条件，接下来可能基于其他因素作出。

原文链接：http://www.cisco.com/en/US/products/ps6087/products_tech_note09186a0080b90500.shtml
翻译人：谢清
译于 2013 年 12 月