

# Itinérance WGB : Détails internes et configuration

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Quelle est une passerelle de groupe de travail ?](#)

[Scénarios d'utilisation](#)

[Erreur](#)

[Éléments de l'itinérance](#)

[Guide de configuration - Stratégies de sécurité](#)

[Configurer WPA2-PSK](#)

[Configurer le WPA2 avec le 802.1x](#)

[Configurer le WPA2 avec CCKM](#)

[Validation de la méthode utilisée](#)

[Configurer l'itinérance](#)

[Packet retries](#)

[Surveillance RSSI](#)

[Débit de données minimum](#)

[Canaux de balayage](#)

[Configurez les temporisateurs](#)

[D'autres optimisations WGB](#)

[Connexe par radio](#)

[Log associé](#)

[Utilisation MFP](#)

[EAP-TLS sur WGB et « clock save interval »](#)

[Exemple de configuration complète](#)

[Analyse de debug](#)

[Informations connexes](#)

## [Introduction](#)

Le pont de groupe de travail de Cisco (WGB) est un outil très utile pour la conception et le déploiement d'un réseau Sans fil parce qu'il permet à des périphériques de non-radio de gagner la mobilité. WGB fournit beaucoup de détails sur l'itinérance, l'accès sécurisé, etc., qui affectent des scénarios de déploiement selon vos besoins.

Dans des versions 12.4(25d)JA et ultérieures de code, Cisco a introduit un ensemble de commandes et de modifications afin d'optimiser l'utilisation de WGB sur les environnements à grande vitesse d'itinérance.

Ce document couvre différents aspects de la façon dont un WGB fonctionne, y compris des points de décision d'algorithme d'itinérance, et de la façon le configurer pour le modèle destiné d'utilisation.

## Conditions préalables

### Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Solution LAN de radio de Cisco
- Pont de groupe de travail de Cisco

### Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

### Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

## Quelle est une passerelle de groupe de travail ?

Un WGB est fondamentalement un Point d'accès (AP) configuré pour agir en tant que client sans fil vers une infrastructure, et pour fournir la Connectivité de la couche 2 pour les périphériques connectés à ses Ethernets reliez.

Un déploiement typique WGB a ces composants :

- Le périphérique WGB, normalement avec au moins une radio et un Ethernet reliez
- Une infrastructure Sans fil, normalement appelée l'AP racine, qui peut être autonome ou unifié.
- Un ou plusieurs périphériques de client câblé connectés au WGB. Ce document ne couvre pas les scénarios mélangés de rôle (une radio comme WGB, une radio comme racine sur le même AP).

Il y a trois types principaux de WGB :

- **Cisco WGB** : Cisco WGB est tout Cisco IOS® - AP basé configuré comme WGB (1130, 1240,

1250, etc.). Ce mode emploie le protocole IAPP pour informer l'infrastructure réseau des périphériques que le WGB a appris sur son interface Ethernet. Dans ce cas, le contrôleur LAN Sans fil (WLC) ou l'AP racine a la visibilité de la couche 2 des périphériques « pendant » du WGB.

- **Non Cisco WGB** : C'est un périphérique de tiers agissant en tant que WGB, connectant un ou plusieurs périphériques de câble à l'infrastructure Sans fil. Ceux-ci ne prennent en charge pas IAPP, et permettent seulement un périphérique de câble simple, ou fournissent un mécanisme de traduction d'adresse MAC, masquant tous leurs clients câblés derrière une adresse MAC simple de 802.11. Ces types de périphériques ont besoin d'offre spéciale manipulant sur le Protocole ARP (Address Resolution Protocol) et les trames DHCP si l'infrastructure est un WLC dû aux contrôles de Sécurité et à la manipulation de trame faits sur des contrôleurs.
- **Cisco AP configuré en tant que « universel WGB »** : C'est un mode qui supprime le mécanisme IAPP, ainsi le WGB peut être utilisé vers une racine aps d'infrastructure Cisco ou de tiers. Dans ce cas, le WGB prend l'adresse de son client Ethernet, limitant le nombre de périphériques derrière lui à un.

Les foyers de section suivante sur le scénario de Cisco WGB les ont utilisé vers l'infrastructure autonome ou WLC.

## Scénarios d'utilisation

Les exemples typiques d'utilisation WGB incluent :

- Connecter une imprimante de câble au réseau
- Différents déploiements de fabrication, où il n'est pas faisable ou pratique pour exécuter un câble au périphérique de câble
- déploiements de Dans-véhicule, où le WGB fournit la Connectivité d'un CAR, d'une série de métro, etc., à un réseau de Technologie sans fil d'extérieur
- Caméras de câble

Chaque exemple a ses propres conditions requises aux conditions de :

- La bande passante a dû prendre en charge l'application qui fonctionnera sur l'infrastructure Sans fil
- Tolérance errante de retard - Combien de temps prend-elle pour que le WGB se déplace-t-il du courant AP au prochain tandis que le périphérique se déplace ?
- Tolérance de durée d'acheminement - Combien de trames sont perdues sur chaque itinérance ?

Une imprimante ne se déplace pas beaucoup, ainsi les conditions requises d'itinérance sont inférieures. Un WGB monté par série d'autre part, les besoins réglant avec précision sur le composant d'itinérance afin d'assurer le comportement correct tandis qu'il se déplace autour.

Un flux vidéo peut avoir une grande bande passante nécessaire, ainsi il a besoin de débits de données Sans fil élevés. Cependant, une application de télémétrie pourrait seulement avoir besoin de quelques trames de temps en temps.

Il est important que les conditions requises soient correctement définies du début, car elles affectent non seulement la configuration du WGB, mais également comment l'infrastructure Sans fil doit être conçue. Par exemple, le placement AP, distance, des niveaux de puissance, a activé des débits, etc., tout affectent des caractéristiques d'itinérance. Par conséquent, tout est un point

crucial si l'itinérance à grande vitesse est nécessaire.

Généralement vous devez connaître ces détails :

- Quelle est la bande passante nécessaire pour l'application ?
- Quelle est la tolérance de retard d'itinérance ?
- Peuvent-elles les déconnexions de réseau de traitement d'application correctement ? Y a-t-il un mécanisme de sauvegarde supplémentaire ?
- L'application peut-elle manipuler la perte de paquets correctement ? (Même sur la meilleure conception Sans fil, vous devez s'attendre à un pourcentage de la perte de paquets.)

Ce document ne s'adresse pas aux détails sur la façon dont concevoir un environnement rf pour l'itinérance à grande vitesse/extérieur. Référez-vous au guide extérieur de déploiement de maille.

## Errer

Pour un périphérique sans fil, errer est très un élément essentiel de sa fonctionnalité.

Fondamentalement, errer signifie la capacité pour aller d'un AP à l'autre, chacun des deux qui appartient à la même infrastructure Sans fil.

Car errer a besoin d'une modification du courant AP au prochain, il y a une déconnexion ou un temps résultante sans service. Cette déconnexion peut être petite. Par exemple, moins que 200ms sur des déploiements vocaux ou beaucoup plus long, même des secondes, si la Sécurité requise impose une pleine authentification sur chacun errant l'événement.

L'itinérance est nécessaire ainsi le périphérique peut trouver un nouveau parent avec un signal si tout va bien meilleur, et il peut continuer à accéder à l'infrastructure réseau correctement. En même temps, un trop grand nombre erre peut entraîner de plusieurs déconnexions ou temps sans service, qui affecte l'accès. Il est important pour un périphérique mobile, tel qu'un WGB, pour avoir un bon algorithme errant avec assez de capacités de configuration à adapter à différents environnements rf et besoins de données.

## Éléments de l'itinérance

- **Déclencheurs** : Chaque implémentation de client a un ou plusieurs déclencheurs ou les événements, cela une fois rencontrés, fait déplacer le périphérique à un autre parent AP. Exemples : ne balisez la perte (le périphérique n'entend plus les balises régulières d'AP), le packet retries, le niveau de signal, aucune donnée reçue, la trame reçue de deauthenticaton, le bas débit de données en service, etc. Les déclencheurs possibles peuvent être différents de l'implémentation de client à l'autre parce qu'ils ne sont pas entièrement normalisés. Des périphériques plus simples pourraient avoir un déclencheur pauvre réglé, qui entraîne mauvais (les clients Rémanents) ou inutile erre. Le WGB prend en charge tous les éléments précédents décrits avant.
- **Temps de balayage** : Le périphérique sans fil (WGB) passe une certaine heure recherchant les parents potentiels. Ceci implique normalement aller sur des différents canaux, faisant des aps de sondage ou écoutants passivement actifs. Comme la radio doit balayer, ce temps de moyens que le WGB passe faire autre chose différent des données d'expédition. De ce temps de balayage, le WGB peut établir un ensemble valide de parents aux lesquels peut être erré.
- **Sélection de parent** : Après temps de balayage, le WGB peut vérifier les parents potentiels,

sélectionner le meilleur et déclencher l'association/procédure d'authentification. Parfois, le point de décision peut être de rester sur le parent en cours s'il n'y a pas un bénéfice important d'un événement d'itinérance (souvenez-vous qu'errer trop de peut être mauvais).

- **Association/authentification** : Le WGB poursuit à l'associé à nouvel AP, qui couvre normalement des phases d'authentification et d'association de 802.11, plus se terminer la stratégie de sécurité configurée sur le SSID (WPA 2-PSK, CCKM, aucun, etc.).
- **Restauration d'expédition du trafic** : Le WGB met à jour l'infrastructure réseau de ses clients câblés connus par des mises à jour IAPP après avoir erré. Après ce point, le trafic à/de les clients câblés au réseau reprend.

## Guide de configuration - Stratégies de sécurité

Un important aspect pour errer sur des périphériques mobiles est ce qui est la stratégie de sécurité qui sera mise en application sur l'infrastructure. Il y a plusieurs options, chacun avec bons/négatifs points. Ce sont les plus importants :

- **Ouvrez-vous** — Fondamentalement aucune Sécurité. C'est le plus rapide, et plus simple de toutes les stratégies. Ceci a le problème principal de ne limiter l'accès non autorisé à l'infrastructure et aucune protection contre des attaques, qui limite son utilisation aux scénarios très spécifiques. Par exemple, mines où aucune attaque externe n'est due possible à la nature pure du déploiement.
- **Authentification d'adresse MAC** — Fondamentalement le même niveau de sécurité qu'ouvert, comme mystification d'adresse MAC est une attaque insignifiante. En raison non recommandé de l'heure ajoutée de se terminer la validation de MAC, qui ralentit l'itinérance.
- **WPA2-PSK** — Offre le bon niveau de chiffrement (AES-CCMP), mais la Sécurité d'authentification dépend de la qualité de la clé pré-partagée. Pour des mesures de sécurité, un mot de passe des caractères du minimum 12 et un aléatoire est recommandé. Semblable à la méthode principale pré-partagée, comme clé est utilisé sur de plusieurs périphériques, si la clé est compromise le mot de passe doit être modifiée à travers tous les matériels. La vitesse d'itinérance est acceptable, comme elle est faite dans 6 échanges de trame, et vous pouvez calculer ce qui sera les limites supérieures et inférieures de temps pour qu'il se termine parce qu'il n'implique aucun équipement externe (aucun serveur de RADIUS, etc.). Généralement cette méthode est préférée après l'équilibrage des problèmes et des avantages.
- **WPA2 avec le 802.1x** — Ceci s'améliore sur la méthode précédente à l'aide d'a par périphérique/identifiant utilisateur, qui peuvent être individuellement changés. Le problème principal est celui pour errer, cette méthode ne fonctionne pas correctement quand le périphérique est déplacement rapide, ou les temps courts d'itinérance sont nécessaires. Généralement ceci utilise les mêmes 6 trames plus l'échange d'EAP qui peut être entre 4 et. Ceci dépend de quel type d'EAP est sélectionné et les tailles de certificat. Normalement, ceci prend entre 10 à 20 trames, plus le retard ajouté du traitement de serveur de rayon.
- **WPA2+CCKM** — Ce mécanisme offre la bonne protection, emploie le 802.1x pour établir l'authentification initiale, puis fait un échange rapide de juste 2 trames sur chacun errer l'événement. Ceci offre un temps très rapide d'itinérance. Le problème principal est celui en cas de manqué errer, il retourne de retour sur le 802.1x. Puis, débuts utilisant CCKM de nouveau après qu'il authentifie. Si l'application sur le WGB peut tolérer un long temps occasionnel d'itinérance en cas de problèmes, elle peut être utilisée comme meilleure option

contre PSK.

Ce document ne couvre pas les Technologies non-recommandées qui ont des problèmes de sécurité tels que le LEAP, le WPA-TKIP, le WEP, etc.

## Configurer WPA2-PSK

Sur le WGB, c'est assez simple pour configurer. Vous avez besoin de la définition SSID et du cryptage approprié sur la radio.

```
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
```

Votre nom SSID et clé pré-partagée doivent apparier votre infrastructure réseau.

## Configurer le WPA2 avec le 802.1x

Il construit fondamentalement sur le config précédent, en plus des eap profile et de la méthode d'authentification :

```
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
```

## Configurer le WPA2 avec CCKM

Seulement une étape sur le WPA2 avec juste une modification mineure : utilisant l'indicateur CCKM sur la configuration SSID. Ceci suppose que le WLAN est configuré pour CCKM seulement du côté WLC :

```
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
```

## Validation de la méthode utilisée

Un contrôle rapide sur le WGB peut signaler le cryptage et la gestion des clés en service, par exemple, dans 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
```

## Configurer l'itinérance

Sur le WGB, vous pouvez modifier plusieurs paramètres qui affectent l'algorithme d'itinérance.

### Packet retries

Par défaut, le WGB retransmet une trame 64 fois. S'il n'est pas correctement reconnu (ACK) par un parent, il suppose que le parent n'est plus valide, et commence un balayage/processus d'itinérance. Voyez celui-ci comme déclencheur « async » d'itinérance parce qu'il peut faire à tout moment qu'une transmission échoue.

La commande de configurer ceci, va à l'intérieur de l'interface dot11, et elle prend les options suivantes :

```
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

```

**Numérique** : Est entre 1 et 128, avec un par défaut de 64. Un bon nombre pour un déclencheur rapide d'itinérance est habituellement 32. Utilisant un nombre plus peu élevé n'est pas recommandé sur la plupart des environnements rf.

**baisse** : Sinon présentez, le WGB commence un événement d'itinérance quand des relances maximum sont atteintes. Quand le présent, le WGB ne commence pas la nouvelle itinérance et utilise d'autres déclencheurs, tels que la perte et le signal de balise.

## Surveillance RSSI

WGB peut implémenter un balayage proactif de signal pour le parent en cours et commencer un nouveau processus d'itinérance quand le signal tombe au-dessous d'un niveau prévu.

Ce processus prend deux paramètres :

- Un temporisateur, qui réveille le processus de contrôle des secondes chaque X
- Niveau RSSI, qui est utilisé pour commencer un processus d'itinérance si le signal en cours est soufflet il.

Exemple :

```

wgb-1260#sh dot11 associations a1
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
```

Le temps ne devrait pas être inférieur que ce qui le WGB prend pour compléter une procédure d'authentification afin d'empêcher « une boucle roaming » en quelques conditions ou éviter un comportement d'itinérance trop agressif. Généralement il devrait tester pour voir ce qui satisfait les besoins d'application.

Pour PSK il peut être inférieur que dans des méthodes basées par EAP (2 et 4 typiques pour des applications très agressives).

Le niveau RSSI expressed comme entier positif, bien que ce soit fondamentalement une normale - dBm mesuré de niveau. Vous devriez utiliser un nombre supérieur agréable à voir que le minimum requis pour continuer votre débit de données fonctionner correctement. Par exemple, si votre débit minimum désiré est 6 mbps, un seuil RSSI de -87 devrait être suffisant. Pour 48 mbps, vous avez besoin de dBm -70, etc.

**Remarque:** Cette commande peut également déclencher une « itinérance par la modification de débit de données », qui est trop agressive. Il doit être utilisé ainsi que le minimum-débit pour de bons résultats.

## Débit de données minimum

Commençant par 12.4(25d)JA, Cisco a ajouté un paramètre configurable pour contrôler quand le WGB devrait déclencher un nouvel événement d'itinérance, si le débit de données en cours au parent est soufflet par valeur indiquée.

Il est utile assurer ce qu'une limite inférieure désirée sur la vitesse est gardée afin de prendre en charge le vidéo ou les Applications voix.

Avant que cette commande ait été disponible, le WGB a déclenché error fréquemment quand le débit s'est avéré inférieur au temps précédent. Fondamentalement à l'heure X+1, si le débit était inférieur au temps précédent X, le WGB a commencé un processus d'itinérance. Sur les logs vous verriez ces messages :

```
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
```

C'est trop agressif, et normalement, la seule solution était de configurer un seul débit de données dans WGB et sur le parent aps.

Maintenant, la manière recommandée est de configurer toujours cette commande, toutes les fois qu'une commande de période de poste mobile est utilisée :

```
wgb-1260#sh dot11 associations a1
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
```

Avec ceci, le nouveau processus d'itinérance est seulement déclenché si le taux actuel est inférieur à la valeur configurée. Ceci réduit des roamings inutiles et laisse garder un teneur prévu en débit.

**Remarque:** On s'attend à ce que le message « a dû diminuer le débit de données » se produise même avec ce config, juste cela maintenant qu'il devrait seulement voir si WGB était TX à une vitesse plus humblement que configurée, quand le temps de contrôle de période de poste mobile a été déclenché.

## [Canaux de balayage](#)

Le WGB balaye tout le « pays creuse des rigoles » tout en faisant un événement errant. Ceci

signifie que selon le domaine par radio, vous pouvez balayer les canaux 1 11 sur la bande 2.4 gigahertz, ou 1 à 13.

Chaque canal balayé prend un certain temps. Sur 802.11bg c'est environ 10 à 13 ms. Sur 802.11a, ce peut être jusqu'à 150 ms si le canal est DFS activé (ainsi sondage, faisant juste le balayage passif là).

Une bonne optimisation est de limiter les canaux balayés pour utiliser seulement ceux en service par l'infrastructure. C'est particulièrement important sur 802.11a, car la liste de canal est grande, et le temps par canal peut être long si DFS est en service.

Il y a trois points à prendre en concevant un plan de canal pour WGB/Roaming :

- Pour la bande 2.4 gigahertz, essayez de coller à 1/6/11 pour réduire l'interférence latérale de canal. Il tend à être difficile de machiner n'importe quel autre plan de canal avec 4, etc., correctement du point de vue rf, sans interférence croissante.
- Utilisant le canal unique une installation pour tous les aps est une bonne idée de point de vue de balayage. Ceci semble seulement raisonnable si le nombre total de clients à prendre en charge est très bas, et il n'y a pas des conditions requises de bande passante élevée. Ceci élimine le temps par radio de modification du temps de balayage. Soyez conscient du fait que peu d'environnements peuvent tirer bénéfice de cette option, ainsi utilisation avec soin.
- Pour la bande 5.0 gigahertz, s'il est possible par vos réglementations locales, utilisant le non-DFS d'intérieur channels(36 à 48) accorde un temps plus rapide de balayage, car WGB peut activement sonder chacun, au lieu de faire le plus long temps écoutant passif.

Le plan de canal en service pour votre déploiement pourrait devoir faciliter d'autres conditions requises. Utilisez les recommandations de conception du général rf.

Afin de configurer la liste de canal de balayage :

```
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

**Remarque:** Le poste mobile apparaît seulement en utilisant le rôle WGB sur la radio.

**Remarque:** Assurez-vous que votre liste de balayage WGB apparie votre liste de canal d'infrastructure. Sinon, le WGB ne trouvera pas vos aps disponibles.

## Configurez les temporisateurs

Commencent par 12.4(25a)JA, là plusieurs nouvelles commandes d'optimiser le temporisateur de reprise où un problème est trouvé, qui sont seulement disponibles quand AP est en mode WGB.

```
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
```

Dans le cas de l'assoc-réponse, la réponse d'autorisation, client-ajoutent, ceux-ci indiquent combien de temps le WGB attendra le parent AP pour répondre, avant de considérer AP comme morts et essayer le prochain candidat. Les valeurs par défaut sont de 5 secondes, qui est trop long pour quelques applications. Le temporisateur minimum est 800 ms et est recommandé pour la plupart des applications mobiles.

Dans l'eap-délai d'attente, le WGB place un temps maximum pour attendre, jusqu'à ce que le plein procédé d'authentification EAP soit terminé. Ceci fonctionne d'un point de vue de suppliant d'EAP afin de redémarrer le processus si l'authentificateur d'EAP ne répond pas de retour. La valeur par défaut est de 60 secondes. Faites attention à ne jamais configurer une valeur qui peut être inférieure que le temps réel nécessaire pour se terminer une pleine authentification de 802.1x. Normalement, l'établissement de ceci à 2 à 4 secondes est correct pour la plupart des déploiements.

Pour iapp-régénérez, le WGB par défaut génère une mise à jour en vrac IAPP au parent AP après qu'errant afin d'informer des clients câblés connus. Il y a une deuxième retransmission après association environ 10 secondes plus tard. Ce temporisateur laisse faire « jeûnent relance » du volume IAPP après qu'association afin de surmonter la possibilité que la première mise à jour

IAPP était due perdu au rf, ou des clés de chiffrement pas encore installées sur le parent AP. Pour les scénarios rapides d'itinérance, 100ms peut être utilisé. Cependant, assurez-vous qu'il y a un grand nombre de WGB en service. Ceci augmente de manière significative le nombre total d'IAPP envoyé à l'infrastructure après chaque itinérance.

Exemple pour des valeurs agressives :

```
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
```

Ceux-ci ont été avec succès testés sur les scénarios mobiles de déploiement WGB.

## [D'autres optimisations WGB](#)

Il y a d'autres modifications mineures à prendre en compte pour des scénarios de déploiement WGB :

### [Connexe par radio](#)

- Réduisez les **relances de rts** - les **relances 32 de rts**. Ceci peut épargner une certaine heure rf sur les scénarios agressifs. Normalement ce n'est pas nécessaire.
- Type d'antenne : Si à l'aide d'une antenne simple (aucune diversité), vous devriez configurer la radio pour améliorer la représentation générale :

```
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
Tunnel Address     : 0.0.0.0
Key Mgmt type      : CCKM
Encryption          : AES-CCMP
Association Id     : 1

Current Rate       : m7.-
Supported Rates    : 48.0 54.0 m0. m1. m2. m3. m4. m5. m6. m7.
Voice Rates        : disabled
Signal Strength    : -59 dBm
Signal to Noise    : 41 dB
Power-save         : Off
Apsd DE AC(s)     : NONE

Capability          : WMM ShortHdr ShortSlot
Bandwidth           : 20 MHz
Connected for      : 72 seconds
Activity Timeout    : 8 seconds
Last Activity       : 7 seconds ago

Packets Input      : 12064
Bytes Input        : 2892798
Duplicates Rcvd    : 87
Decrypt Failed     : 0
MIC Failed         : 0
Packets Redirected: 0

Packets Output     : 136
Bytes Output       : 19514
Data Retries       : 8
RTS Retries        : 0
MIC Missing        : 0
Redirect Filtered  : 0

```

La diversité d'antenne est désirable, mais pas toujours possible en installant physiquement des Antennes sur le véhicule. La sélection appropriée d'antenne est essentielle pour errer. Aussi peu que 2 dB peut être une différence énorme des durées moyennes générales d'itinérance.

## Log associé

- Afin de faire gagner quelques millisecondes, ramenez le niveau de journalisation console aux erreurs seulement : **erreurs de logging console**. Ne le désactivez pas complètement parce qu'il peut affecter négativement la représentation d'itinérance sur quelques conditions.
- Dans le meilleur des cas, le telnet d'utilisation ou le ssh du côté Ethernet à collecter met au point ou se connecte. Ceci a l'incidence un beaucoup inférieure sur la représentation par rapport à se connecter met au point au-dessus de la console : **se connecter l'élimination des imperfections de moniteur**.
- La commande de comprendre ce qui se produit pour le point de vue d'itinérance WGB est **liaison ascendante d'impression de suivi du debug dot11 dot11 0**. Ceci a la basse incidence sur la CPU, mais n'active pas autre mettent au point des options à moins qu'instruit parce que chacun pourrait incrémenter tout le temps d'itinérance.
- Essayez d'utiliser SNTP si possible. Ceci garde le temps WGB sur le sync, qui est extrêmement utile pour le dépannage.

## Utilisation MFP

- MFP peut être utile d'un point de vue de la sécurité. Cependant, un inconvénient est celui sur des scénarios de panne d'itinérance, le WGB ne reçoit pas les trames De-auth du parent AP pour déclencher une nouvelle itinérance si la clé de chiffrement entre chacun d'eux est allée mal pour une raison quelconque.
- Sur ces scénarios de panne rares, le WGB peut prendre à 5 secondes pour déclencher un nouveau balayage, si le parent en cours peut être entendu avec le bon signal rf. Il y a un mécanisme de détection de « fourre-tout » que WGB peut déclencher si aucune trame de données valide n'est reçue pendant ce temps.
- Par défaut, les essais WGB pour utiliser le client MFP si le SSID a WPA2 AES en service.
- Il est recommandé pour désactiver le client MFP si les temps de rétablissement rapides sont nécessaires (WGB à réagir aux trames non-protégées de deauth). C'est une compromission

entre les besoins de Sécurité et les temps de rétablissement rapides. La décision dépend de ce qui est plus important pour le scénario de déploiement.

```
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
```

## [EAP-TLS sur WGB et « clock save interval »](#)

Référez-vous aux [horloges de Suppliquant IOS de synchronisation et sauvegardez le paramètre horaire à la section NVRAM de notes en version pour des Points d'accès et des passerelles de Cisco Aironet pour la Cisco IOS version 12.4\(21a\)JY](#).

Maintenez dans l'esprit qui si en utilisant l'uWGB, l'uWGB pourrait ne jamais obtenir une occasion de faire un sync de sntp parce qu'il est typiquement associé avec l'adresse MAC reliée et l'uWGB BVI n'a pas l'accès au réseau. Par conséquent, dans le cas d'un uWGB, il est recommandé pour se mettre un bon sync d'horloge dans NVRAM au déploiement au minimum. Si le périphérique relié d'enet a la capacité d'être un ntp source (aussi bien que client mis à jour par l'intermédiaire de sa connexion d'uWGB), alors il est possible de considérer avoir le sync de sntp d'uWGB de lui comme point efficace de réflexion de NTP.

## [Exemple de configuration complète](#)

```
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

```

## Analyse de debug

Dans toutes les questions se produisant, il est important de saisir la sortie de la commande de **liaison ascendante d'impression de suivi du debug dot11 dot11 0** dans un premier temps. Ceci fournit une bonne vue de ce qui se produit avec le processus d'itinérance.

C'est un parent en cours d'exemple comme candidat :

```

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

```

C'est déclencheur pour le bas signal rencontré. Il dépend de la commande du seuil Y de la période X de poste mobile. Le premier message est toujours envoyé à la console, deuxième fait partie de la liaison ascendante mettent au point des suivis. Ce n'est pas un problème, mais une partie du processus normal WGB.



```

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

```

Le processus de liaison ascendante force une purge par radio de file d'attente avant de commencer un balayage de canal. Cette étape peut prendre de quelques millisecondes à plusieurs secondes selon l'utilisation et la profondeur de la file d'attente de canal. Des trames de données ne sont pas chronométrées. Les trames voix ont une comparaison de temps faite, devraient ainsi être plus rapides abandonné. On pourrait observer un certain retard dans les environnements bruyants.

```

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

C'est le balayage réel de canal ayant lieu. Il gare le ms de la radio approximativement 10 à 13 par canal configuré.

```
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
```

C'est la liste de réponses de sonde reçues. Le premier nombre est le canal, deuxième est des microsecondes prises pour le recevoir.

```
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

## Comparaison réelle faite dans ces détails :

```
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
```

## Sélection de parent

```
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
```

C'est le point où l'itinérance est « de finition ». Trafiquez les reprises dès que des trames IAPP

seront traitées par le parent.

## Le parent compare les informations

```
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
```

Le compare1 imprime le compte réel -1 d'association (ainsi WGB lui-même n'est pas rentré le nombre) si le « courant » AP est l'un WGB est associé toujours, puis les sauts et le chargement réels.

Le compare2 imprime les différences. C'est pourquoi il est possible de voir un numéro négatif. Si le test a un nombre supérieur que le courant, vous voyez le négatif.

Selon le compte en cours d'association, le chargement, différence de signal, valeur seuil mobile, le WGB pourrait ou ne pourrait pas sélectionner un nouveau parent.

La comparaison est toujours entre deux aps, avec AP sélectionné remplaçant le courant pour la prochaine itération. Par conséquent, certaines des décisions peuvent être dues à RSSI sur une boucle, ou dues à d'autres facteurs sur le prochain test.

## [Informations connexes](#)

- [Comment utiliser un WGB IOS avec authentification EAP-TLS dans un réseau sans fil unifié Cisco](#)
- [Support et documentation techniques - Cisco Systems](#)