Itinérance WGB : Détails et configuration internes

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Components Used](#)
[Conventions](#)
[Qu'est-ce qu'un pont de groupe de travail ?](#)
[Scénarios d'utilisation](#)
[Itinérance](#)
[Éléments de l'itinérance](#)
[Guide de configuration - Stratégies de sécurité](#)
[Configuration de WPA2-PSK](#)
[Configuration de WPA2 avec 802.1x](#)
[Configuration de WPA2 avec CCKM](#)
[Validation de la méthode utilisée](#)
[Configuration de l'itinérance](#)
[Nouvelles tentatives de paquets](#)
[Surveillance RSSI](#)
[Débit de données minimal](#)
[Analyser les canaux](#)
[Configurer les compteurs](#)
[Autres optimisations WGB](#)
[Relatif À La Radio](#)
[Lié au journal](#)
[Utilisation MFP](#)
[EAP-TLS sur WGB et « clock save interval »](#)
[Exemple de configuration complète](#)
[Analyse de débogage](#)
[Informations connexes](#)

Introduction

Cisco Workgroup Bridge (WGB) est un outil très utile pour la conception et le déploiement d'un réseau sans fil, car il permet aux périphériques non sans fil d'accéder à la mobilité. WGB fournit de nombreux détails sur l'itinérance, l'accès à la sécurité, etc., qui ont un impact sur les scénarios de déploiement selon vos besoins.

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

Ce document couvre différents aspects du fonctionnement d'un WGB, y compris les points de décision de l'algorithme d'itinérance, et comment le configurer pour le modèle d'utilisation prévu.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Solution LAN sans fil Cisco
- Pont de groupe de travail Cisco

Components Used

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Qu'est-ce qu'un pont de groupe de travail ?

Un WGB est essentiellement un point d'accès configuré pour agir en tant que client sans fil vers une infrastructure et pour fournir une connectivité de couche 2 aux périphériques connectés à son interface Ethernet.

Un déploiement WGB classique comporte les composants suivants :

- Périphérique WGB, généralement équipé d'au moins une radio et d'une interface Ethernet
- Une infrastructure sans fil, généralement appelée point d'accès racine, qui peut être autonome ou unifiée.
- Un ou plusieurs périphériques client câblés connectés au WGB. Ce document ne couvre pas les scénarios de rôles mixtes (une radio comme WGB, une radio comme racine sur le même AP).

Il existe trois principaux types de WGB :

- **Cisco WGB** : Cisco WGB est un point d'accès basé sur Cisco IOS® configuré comme WGB (1130, 1240, 1250, etc.). Ce mode utilise le protocole IAPP pour informer l'infrastructure réseau des périphériques que le WGB a appris sur son interface Ethernet. Dans ce cas, le

contrôleur de réseau local sans fil (WLC) ou point d'accès racine a une visibilité de couche 2 des périphériques « suspendus » du WGB.
- **WGB non Cisco :** Il s'agit d'un périphérique tiers agissant en tant que WGB, qui connecte un ou plusieurs périphériques câblés à l'infrastructure sans fil. Ils ne prennent pas en charge le protocole IAPP et ne permettent qu'un seul périphérique câblé, ou fournissent un mécanisme de traduction d'adresses MAC, masquant tous leurs clients câblés derrière une seule adresse MAC 802.11. Ces types de périphériques nécessitent une gestion spéciale sur les trames ARP (Address Resolution Protocol) et DHCP si l'infrastructure est un WLC en raison des contrôles de sécurité et de la gestion des trames effectués sur les contrôleurs.
- **Point d'accès Cisco configuré en tant que « WGB universel »** : Il s'agit d'un mode qui supprime le mécanisme IAPP, de sorte que le WGB peut être utilisé vers une infrastructure Cisco ou des points d'accès racine tiers. Dans ce cas, le WGB prend l'adresse de son client Ethernet, limitant le nombre de périphériques derrière lui à un.

La section suivante porte sur le scénario d'un WGB Cisco utilisé soit pour une infrastructure autonome, soit pour une infrastructure WLC.

Scénarios d'utilisation

Exemples d'utilisation WGB types :

- Connexion d'une imprimante câblée au réseau
- Différents déploiements de fabrication, où il n'est ni possible ni pratique d'utiliser un câble vers le périphérique filaire
- Déploiements dans les véhicules, où le WGB fournit la connectivité d'une voiture, d'un train de métro, etc., à un réseau sans fil extérieur
- Caméras filaires

Chaque exemple a ses propres exigences en termes :

- Bande passante nécessaire pour prendre en charge l'application qui s'exécutera au-dessus de l'infrastructure sans fil
- Tolérance au délai d'itinérance : combien de temps faut-il au WGB pour passer du point d'accès actuel au point d'accès suivant pendant que le périphérique se déplace ?
- Tolérance de temps de transfert : combien de trames sont perdues sur chaque itinérance ?

Une imprimante ne bouge pas beaucoup, les besoins en itinérance sont donc plus faibles. Par contre, un WGB monté sur train doit être ajusté sur le composant d'itinérance afin d'assurer un comportement correct pendant qu'il se déplace.

Un flux vidéo peut nécessiter une large bande passante, de sorte qu'il nécessite des débits de données sans fil élevés. Cependant, une application de télémétrie peut ne nécessiter que quelques trames de temps en temps.

Il est important que les exigences soient correctement définies dès le début, car elles affectent non seulement la configuration du WGB, mais également la manière dont l'infrastructure sans fil doit être conçue. Par exemple, le positionnement des points d'accès, la distance, les niveaux d'alimentation, les débits activés, etc., affectent toutes les caractéristiques d'itinérance. Par conséquent, tous sont un point crucial si l'itinérance à grande vitesse est nécessaire.

En règle générale, vous devez connaître ces détails :

- Quelle est la bande passante requise pour l'application ?
- Quelle est la tolérance de délai d’itinérance ?
- L'application peut-elle gérer correctement les déconnexions réseau ? Existe-t-il un mécanisme de sauvegarde supplémentaire ?
- L'application peut-elle gérer correctement la perte de paquets ? (Même dans la meilleure conception sans fil, vous devez vous attendre à un pourcentage de perte de paquets.)

Ce document ne traite pas des détails sur la conception d'un environnement RF pour l'itinérance/extérieur à grande vitesse. Reportez-vous au guide de déploiement du maillage extérieur.

Itinérance

Pour un périphérique sans fil, l'itinérance est un élément essentiel de ses fonctionnalités.

En fait, l'itinérance signifie la capacité de passer d'un point d'accès à un autre, tous deux appartenant à la même infrastructure sans fil.

Comme l'itinérance nécessite un changement du point d'accès actuel au suivant, il en résulte une déconnexion ou un temps sans service. Cette déconnexion peut être faible. Par exemple, moins de 200 ms sur les déploiements vocaux ou plus, voire plus, secondes, si la sécurité requise impose une authentification complète sur chaque événement de itinérance.

L'itinérance est nécessaire pour que le périphérique puisse trouver un nouveau parent avec un signal plus performant, et qu'il puisse continuer à accéder correctement à l'infrastructure réseau. Dans le même temps, trop d'itinérance peut provoquer plusieurs déconnexions ou un temps sans service, ce qui affecte l'accès. Il est important qu'un appareil mobile, tel qu'un WGB, dispose d'un bon algorithme d'itinérance avec suffisamment de fonctionnalités de configuration pour s'adapter aux différents environnements RF et aux différents besoins en données.

Éléments de l'itinérance

- **Déclencheurs :** Chaque implémentation de client a un ou plusieurs déclencheurs ou événements qui, lorsqu'ils sont rencontrés, entraînent le déplacement du périphérique vers un autre AP parent. Exemples: perte de balise (le périphérique n'entend plus les balises normales du point d'accès), tentatives de paquets, niveau de signal, aucune donnée reçue, trame de déauthentification reçue, faible débit de données utilisé, etc. Les déclencheurs possibles peuvent être différents de la mise en oeuvre du client à un autre parce qu'ils ne sont pas entièrement normalisés. Les périphériques plus simples peuvent avoir un jeu de déclencheurs médiocre, ce qui entraîne des erreurs (clients rémanents) ou inutiles. Le WGB prend en charge tous les éléments précédents décrits précédemment.
- **Heure d'analyse :** Le périphérique sans fil (WGB) passe un certain temps à rechercher des parents potentiels. Cela implique normalement de passer sur différents canaux, de faire une recherche active ou d'écouter passivement les points d'accès. Comme la radio doit analyser, cela signifie que le WGB passe du temps à faire autre chose que de transmettre des données. À partir de cette période d'analyse, le WGB peut créer un ensemble valide de parents auxquels il est possible de faire appel.
- **Sélection parent :** Après l'analyse, le WGB peut vérifier les parents potentiels, sélectionner le meilleur et déclencher le processus d'association/authentification. Parfois, le point de décision peut être de rester sur le parent actuel s'il n'y a pas un avantage significatif d'un événement

d'itinérance (rappelez-vous que trop d'itinérance peut être mauvais).
- **Association/Authentification :** Le WGB procède à l'association au nouveau point d'accès, qui couvre normalement les deux phases d'authentification et d'association 802.11, ainsi que l'achèvement de la stratégie de sécurité configurée sur le SSID (WPA 2-PSK, CCKM, None, etc.).
- **Restauration du transfert du trafic :** Le WGB met à jour l'infrastructure réseau de ses clients filaires connus par le biais de mises à jour IAPP après l'itinérance. Après ce point, le trafic entre les clients filaires et le réseau reprend.

Guide de configuration - Stratégies de sécurité

L'un des aspects importants de l'itinérance sur les appareils mobiles est la politique de sécurité qui sera mise en oeuvre sur l'infrastructure. Il y a plusieurs options, chacune avec des points bons/mauvais. Voici les plus importantes :

- **Ouvrir** : en gros, aucune sécurité. C'est la politique la plus rapide et la plus simple. Cela pose le problème principal de ne pas restreindre l'accès non autorisé à l'infrastructure et de ne pas protéger contre les attaques, ce qui limite son utilisation à des scénarios très spécifiques. Par exemple, les mines où aucune attaque externe n'est possible en raison de la nature même du déploiement.
- **Authentification d'adresse MAC** - En gros, le même niveau de sécurité que les adresses ouvertes, car l'usurpation d'adresse MAC est une attaque banale. Non recommandé en raison du temps supplémentaire nécessaire à la validation MAC, ce qui ralentit l'itinérance.
- **WPA2-PSK** - Offre un bon niveau de cryptage (AES-CCMP), mais la sécurité de l'authentification dépend de la qualité de la clé prépartagée. Pour les mesures de sécurité, un mot de passe de 12 caractères minimum et aléatoire est recommandé. Comme pour la méthode de clé pré-partagée, comme la clé est utilisée sur plusieurs périphériques, si la clé est compromise, le mot de passe doit être modifié sur tous les équipements. La vitesse d'itinérance est acceptable, car elle est effectuée dans 6 échanges de trames, et vous pouvez calculer quelles seront les limites de temps supérieur/inférieur pour qu'elle se termine parce qu'elle n'implique aucun équipement externe (pas de serveur RADIUS, etc). En règle générale, cette méthode est la méthode préférée après avoir équilibré les problèmes et les avantages.
- **WPA2 avec 802.1x** : améliore la méthode précédente en utilisant des informations d'identification par périphérique/utilisateur, qui peuvent être modifiées individuellement. Le principal problème est que pour l'itinérance, cette méthode ne fonctionne pas correctement lorsque le périphérique se déplace rapidement, ou que des temps d'itinérance courts sont nécessaires. En général, ceci utilise les mêmes 6 trames plus l'échange EAP qui peut être compris entre 4 et plus. Cela dépend du type EAP sélectionné et de la taille des certificats. Normalement, cela prend entre 10 et 20 trames, plus le délai supplémentaire de traitement du serveur radius.
- **WPA2+CCKM** - Ce mécanisme offre une bonne protection, utilise 802.1x pour créer l'authentification initiale, puis effectue un échange rapide de seulement 2 trames sur chaque événement de itinérance. Cela permet un temps d'itinérance très rapide. Le problème principal est que, en cas d'échec d'une itinérance, elle revient sur 802.1x. Ensuite, recommence à utiliser CCKM après son authentification. Si l'application située au-dessus du WGB peut tolérer un temps d'itinérance occasionnel long en cas de problème, elle peut être

utilisée comme la meilleure option par rapport au PSK.

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

Configuration de WPA2-PSK

Sur le WGB, il est assez simple à configurer. Vous avez besoin de la définition SSID et du chiffrement 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 votre clé pré-partagée doivent correspondre à votre infrastructure réseau.

Configuration de WPA2 avec 802.1x

Il s'appuie essentiellement sur la configuration précédente, avec l'ajout de profils EAP 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
```

Configuration de WPA2 avec CCKM

Une seule étape sur le WPA2 avec une seule modification mineure : utilisation de l'indicateur CCKM sur la configuration SSID. Ceci suppose que le WLAN est configuré pour CCKM uniquement 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

Une vérification rapide du WGB peut rapporter le chiffrement et la gestion des clés utilisés, 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
```

Configuration de l'itinérance

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

Nouvelles tentatives de paquets

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 lance un processus d'analyse/itinérance. Voir celle-ci comme un déclencheur d'itinérance « asynchrone » car il peut être fait à tout moment qu'une transmission échoue.

La commande permettant de configurer ceci s'insère dans l'interface dot11 et prend les options suivantes :

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

Num : Est compris entre 1 et 128, avec une valeur par défaut de 64. Un bon nombre pour un déclencheur d'itinérance rapide est généralement 32. Il est déconseillé d'utiliser un nombre inférieur dans la plupart des environnements RF.

déposer : S'il n'est pas présent, le WGB démarre un événement d'itinérance lorsque le nombre

maximal de tentatives est atteint. Lorsqu'il est présent, le WGB ne lance pas de nouvelle itinérance et utilise d'autres déclencheurs, tels que la perte de balise et le signal.

Surveillance RSSI

WGB peut mettre en oeuvre une analyse proactive des signaux pour le parent actuel et lancer un nouveau processus d'itinérance lorsque le signal tombe sous un niveau prévu.

Ce processus prend deux paramètres :

- Un minuteur, qui réveille le processus de vérification toutes les X secondes
- Niveau RSSI, utilisé pour démarrer un processus d'itinérance si le signal actuel est inférieur.

Exemple :

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

Le temps ne doit pas être inférieur à ce que le WGB prend pour terminer un processus d'authentification afin d'empêcher une « boucle de roaming » dans certaines conditions ou d'éviter un comportement d'itinérance trop agressif. En règle générale, il faut le tester pour voir quelles sont les adaptations nécessaires à la demande.

Pour PSK, il peut être inférieur à celui des méthodes basées sur EAP (généralement 2 et 4 pour les applications très agressives).

Le niveau RSSI est exprimé sous forme d'entier positif, bien qu'il s'agisse essentiellement d'un niveau normal -dBm mesuré. Vous devez utiliser un nombre légèrement supérieur au minimum requis pour que votre débit de données fonctionne correctement. Par exemple, si le débit minimal souhaité est de 6 mbits/s, un seuil RSSI de -87 doit être suffisant. Pour un débit de 48 Mbits/s, vous avez besoin de -70 dBm, etc.

Remarque : Cette commande peut également déclencher une modification du débit de données en itinérance, ce qui est trop agressif. Il doit être utilisé avec un taux minimum pour de bons résultats.

Débit de données minimal

Àpartir de 12.4(25d)JA, Cisco a ajouté un paramètre configurable pour contrôler quand le WGB doit déclencher un nouvel événement d'itinérance, si le débit de données actuel pour le parent est inférieur à une valeur donnée.

Ceci est utile pour s'assurer qu'une limite de vitesse inférieure souhaitée est maintenue afin de prendre en charge les applications vidéo ou voix.

Avant que cette commande ne soit disponible, le WGB déclenchait fréquemment une itinérance lorsque le débit s'est avéré inférieur au temps précédent. Fondamentalement à l'heure X+1, si le débit était inférieur à l'heure X précédente, le WGB a commencé un processus d'itinérance. Dans les journaux, les messages suivants s'affichent :

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

C'est trop agressif, et normalement, la seule solution était de configurer un débit de données unique à la fois dans WGB et sur les AP parents.

Maintenant, la méthode recommandée est de toujours configurer cette commande, chaque fois qu'une commande période de station mobile est utilisée :

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

Dans ce cas, le nouveau processus d'itinérance n'est déclenché que si le débit actuel est inférieur à la valeur configurée. Cela réduit les déplacements inutiles et permet de conserver une valeur de débit attendue.

Note : Le message `« Devez réduire le débit de données »` est attendu même avec cette configuration, juste que maintenant il ne doit être vu que si WGB était TX à une vitesse inférieure à celle configurée, lorsque le temps de vérification de la période de la station mobile a été déclenché.

Analyser les canaux

Le WGB analyse tous les « canaux de pays » lors d'un événement itinérant. Cela signifie que, selon le domaine radio, vous pouvez scanner les canaux 1 à 11 sur une bande de 2,4 Ghz, ou 1 à 13.

Chaque canal numérisé prend un certain temps. Sur la norme 802.11bg, cela fait environ 10 à 13 ms. Sur la norme 802.11a, elle peut atteindre 150 ms si le canal est activé DFS (donc pas de recherche, il suffit de faire une analyse passive là-bas).

Une bonne optimisation consiste à limiter les canaux analysés à utiliser uniquement ceux en service par l'infrastructure. Ceci est particulièrement important sur la norme 802.11a, car la liste des canaux est volumineuse et le temps par canal peut être long si DFS est utilisé.

Trois points doivent être pris en compte lors de la conception d'un plan de canaux pour WGB/Roaming :

- Pour la bande 2,4 GHz, essayez de rester sur 1/6/11 pour minimiser les interférences de canal latéral. Tout autre plan de canal avec 4, etc., tend à être difficile à concevoir correctement du point de vue RF, sans augmenter les interférences.
- L'utilisation d'une configuration à canal unique pour tous les points d'accès est une bonne idée du point de vue de l'analyse. Cela n'a de sens que si le nombre total de clients à prendre en charge est très faible et qu'il n'y a pas de besoins élevés en bande passante. Cela élimine l'heure de changement radio de l'heure d'analyse. N'oubliez pas que peu d'environnements peuvent bénéficier de cette option, donc utilisez avec soin.
- Pour la bande 5,0 GHz, si la réglementation locale le permet, l'utilisation de canaux internes non DFS(36 à 48) permet une analyse plus rapide, car WGB peut les sonder activement, au lieu de faire de l'écoute passive plus longtemps.

Le plan de canal utilisé pour votre déploiement peut nécessiter d'autres exigences. Utilisez les recommandations générales de conception RF.

Afin de configurer la liste des canaux d'analyse :

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

Remarque : la station mobile apparaît uniquement lors de l'utilisation du rôle WGB sur la radio.

Remarque : assurez-vous que votre liste d'analyse WGB correspond à votre liste de canaux d'infrastructure. Si ce n'est pas le cas, le WGB ne trouvera pas vos points d'accès disponibles.

Configurer les compteurs

Àpartir de 12.4(25a)JA, il existe plusieurs nouvelles commandes pour optimiser le compteur de récupération lorsqu'un problème est détecté, qui ne sont disponibles que lorsque l'AP est en mode WGB.

```
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
```

Dans le cas d'assoc-response, auth-response, client-add, ceux-ci indiquent combien de temps le WGB attendra que le point d'accès parent réponde, avant de considérer le point d'accès comme mort et d'essayer candidat suivant. Les valeurs par défaut sont de 5 secondes, ce qui est trop long pour certaines applications. Le compteur minimal est de 800 ms et est recommandé pour la plupart des applications mobiles.

Dans eap-timeout, le WGB définit un délai d'attente maximal, jusqu'à ce que le processus d'authentification EAP complet soit terminé. Cela fonctionne du point de vue du demandeur EAP afin de redémarrer le processus si l'authentificateur EAP ne répond pas. La valeur par défaut est de 60 secondes. Veillez à ne jamais configurer une valeur qui peut être inférieure au temps réel nécessaire pour terminer une authentification 802.1x complète. Normalement, la définition de 2 à 4 secondes est correcte pour la plupart des déploiements.

Pour l'actualisation des applications, le WGB génère par défaut une mise à jour en bloc IAPP au point d'accès parent après l'itinérance afin d'informer les clients filaires connus. Il y a une deuxième retransmission après association environ 10 secondes plus tard. Ce minuteur permet de faire une « tentative rapide » du bloc IAPP après l'association afin de surmonter la possibilité que la première mise à jour IAPP ait été perdue en raison de RF, ou des clés de chiffrement non encore installées sur le point d'accès parent. Pour les scénarios d'itinérance rapide, 100 ms peuvent être utilisés. Cependant, assurez-vous qu'un grand nombre de WGB est utilisé. Cela augmente considérablement le nombre total d'IAPP envoyés à l'infrastructure après chaque itinérance.

Exemple pour les valeurs agressives :

```
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
```

Ils ont été testés avec succès sur des scénarios de déploiement WGB mobiles.

Autres optimisations WGB

D'autres modifications mineures doivent être prises en compte pour les scénarios de déploiement WGB :

Relatif À La Radio

- Réduire **les tentatives rts** - **les tentatives rts 32**. Cela permet d'économiser du temps RF sur les scénarios agressifs. Normalement, cela n'est pas nécessaire.
- Type d'antenne: Si vous utilisez une seule antenne (sans diversité), vous devez configurer la radio pour améliorer les performances générales :

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

La diversité des antennes est souhaitable, mais pas toujours possible lors de l'installation physique des antennes sur le véhicule. Une sélection adéquate de l'antenne est essentielle pour l'itinérance. Aussi peu que 2 dB peut être une énorme différence sur les temps d'itinérance généraux moyens.

Lié au journal

- Afin d'économiser quelques millisecondes, réduisez le niveau de journalisation de la console aux erreurs uniquement : **consigner les erreurs de console**. Ne le désactivez pas complètement car il peut affecter négativement les performances d'itinérance dans certaines conditions.
- Idéalement, utilisez telnet ou ssh du côté Ethernet pour collecter les débogages ou les journaux. Cela a un impact beaucoup plus faible sur les performances que la journalisation des débogages sur la console : **débogage de logging monitor**.
- La commande permettant de comprendre ce qui se passe pour le point de vue d'itinérance WGB est **debug dot11 dot11 0 trace print uplink**. Cela a un faible impact sur le CPU, mais n'activez pas d'autres options de débogage sauf instructions car chacune d'elles peut incrémenter le temps d'itinérance total.
- Essayez d'utiliser SNTP lorsque c'est possible. Cela permet de synchroniser l'heure WGB, ce qui est extrêmement utile pour le dépannage.

Utilisation MFP

- Les MFP peuvent être utiles du point de vue de la sécurité. Cependant, un inconvénient est que dans les scénarios d'échec de l'itinérance, le WGB n'accepte pas les trames de désauthentification du parent de l'AP pour déclencher une nouvelle itinérance si la clé de chiffrement entre les deux a mal tourné pour une raison quelconque.
- Dans ces rares scénarios de défaillance, le WGB peut prendre jusqu'à 5 secondes pour déclencher une nouvelle analyse, si le parent actuel peut être entendu avec un bon signal RF. Il existe un mécanisme de détection globale que WGB peut déclencher si aucune trame de données valide n'est reçue au cours de cette période.
- Par défaut, le WGB tente d'utiliser la MFP du client si le SSID utilise WPA2 AES.
- Il est recommandé de désactiver la MFP du client si des temps de récupération rapides sont

nécessaires (WGB pour réagir aux trames de mort non protégées). Il s'agit d'un compromis entre les besoins de sécurité et les temps de récupération rapides. La décision dépend de ce qui est le plus important pour le scénario de déploiement.

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

EAP-TLS sur WGB et « clock save interval »

Reportez-vous à la section Synchroniser les horloges du demandeur IOS et le paramètre d'économie de temps sur la mémoire NVRAM des Notes de version pour les points d'accès et ponts Cisco Aironet pour Cisco IOS version 12.4(21a)JY.

N'oubliez pas que si vous utilisez uWGB, le uWGB n'aura peut-être jamais la chance d'effectuer une synchronisation sntp car il est généralement associé à l'adresse MAC jointe et le uWGB BVI n'a pas d'accès réseau. Par conséquent, dans le cas d'un uWGB, il est recommandé d'obtenir une bonne synchronisation d'horloge dans la mémoire NVRAM au minimum lors du déploiement. Si le périphérique connecté a la capacité d'être une source NTP (ainsi qu'un client mis à jour via sa connexion uWGB), il est alors possible d'envisager d'avoir la synchronisation uWGB sntp à partir de celle-ci comme point de réflexion NTP efficace.

Exemple de configuration complète

```
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
```

Analyse de débogage

En cas de problème, il est important de capturer la sortie de la commande **debug dot11 dot11 0 trace print uplink** comme première étape. Ceci fournit une bonne vue de ce qui se passe avec le processus d'itinérance.

Voici un exemple de parent actuel en tant que candidat :

```
 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
```

Ceci est le déclencheur pour le signal faible atteint. Cela dépend de la commande Y threshold X de la station mobile. Le premier message est toujours envoyé à la console, le second fait partie

des traces de débogage de liaison ascendante. Ce n'est pas un problème, mais une partie du processus WGB normal.

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

Le processus de liaison ascendante force une purge de file d'attente radio avant de commencer une analyse de canal. Cette étape peut prendre de quelques millisecondes à plusieurs secondes selon l'utilisation du canal et la profondeur de la file d'attente. Les trames de données ne sont pas temporisées. Les trames vocales font l'objet d'une comparaison temporelle, et doivent donc être abandonnées plus rapidement. Un certain retard peut être observé dans les environnements bruyants.

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

Il s'agit de l'analyse de canal en cours. Il place la radio environ 10 à 13 ms par canal configuré.

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

Il s'agit de la liste des réponses de sonde reçues. Le premier numéro est le canal, le second est la microseconde prise pour le recevoir.

```
 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
```

Comparaison réelle effectuée dans ces détails :

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

Sélection des parents

```
 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.
```

C'est le point où l'itinérance est « terminée ». Le trafic reprend dès que les trames IAPP sont traitées par le parent.

Informations de comparaison parente

```
 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
```

La comparaison1 imprime le nombre d'associations réel -1 (WGB lui-même n'est pas pris dans le nombre) si le point d'accès " actuel " est toujours le seul WGB est associé, puis sauts réels et charge.

La comparaison2 imprime les différences. C'est pourquoi il est possible de voir un nombre négatif. Si le nombre de tests est supérieur au nombre actuel, vous obtenez un résultat négatif.

En fonction du nombre d'associations, de la charge, de la différence de signal, de la valeur du

seuil mobile, le WGB peut sélectionner ou non un nouveau parent.

La comparaison se fait toujours entre deux points d'accès, avec le point d'accès sélectionné remplaçant le courant pour l'itération suivante. Par conséquent, certaines des décisions peuvent être dues à RSSI sur une boucle, ou 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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.