

Guide de déploiement d'un maillage en intérieur

Contenu

[Introduction](#)

[Aperçu](#)

[Matériel et logiciels pris en charge](#)

[Intérieur et extérieur](#)

[Configuration](#)

[Mode C3 du contrôleur](#)

[Mettre à niveau le contrôleur vers le dernier code](#)

[Adresse MAC :](#)

[Enregistrer l'adresse MAC sur les radios](#)

[Saisissez l'adresse MAC et les noms des radios dans le contrôleur](#)

[Activer le filtrage MAC](#)

[Déploiement de maillage intérieur de couche 3](#)

[Définir les interfaces sur le contrôleur](#)

[Rôles radio](#)

[Nom du groupe de ponts](#)

[Configuration de la sécurité](#)

[Installation](#)

[Conditions préalables](#)

[Installation](#)

[Configuration de l'alimentation et du canal](#)

[Vérification RF](#)

[Vérification des interconnexions](#)

[Sécurité d'accès à la console AP](#)

[Pontage Ethernet](#)

[Amélioration du nom du groupe de ponts](#)

[Journaux - Messages, Sys, AP et interruptions](#)

[Journaux des messages](#)

[Journaux AP](#)

[Journaux de déROUTement](#)

[Performances](#)

[Test de convergence de démarrage](#)

[WCS](#)

[Alarmes de maillage intérieur](#)

[Rapport maillé et statistiques](#)

[Test de liaison](#)

[Test de liaison de noeud à noeud](#)

[Liaisons de voisinage de point d'accès à la demande](#)

[Test Ping](#)

[Conclusion](#)

[Informations connexes](#)

Introduction

Le point d'accès allégé 1242/1131 est un périphérique d'infrastructure Wi-Fi à deux radios pour certains déploiements intérieurs. C'est un produit basé sur le Protocole de point d'accès allégé (LWAPP). Il fournit une radio 2,4 GHz et une radio 5,8 GHz compatible avec les normes 802.11b/g et 802.11a. Une radio peut être utilisée pour l'accès local (client) pour le point d'accès (AP) et la deuxième peut être configurée pour la liaison sans fil. Le LAP1242/LAP1131 prend en charge les architectures P2P, P2MP et de type maillé.

Assurez-vous de lire le guide avant de tenter l'une des installations.

Ce document décrit le déploiement du maillage sans fil d'entreprise pour le maillage intérieur. Ce document permettra aux utilisateurs finaux sans fil de comprendre les principes fondamentaux du maillage intérieur, où configurer le maillage intérieur et comment configurer le maillage intérieur. Le maillage intérieur est un sous-ensemble du maillage sans fil d'entreprise Cisco déployé à l'aide de contrôleurs sans fil et de points d'accès légers.

Le maillage intérieur est un sous-ensemble de l'architecture de maillage d'entreprise déployée sur l'architecture sans fil unifiée. Le maillage intérieur est aujourd'hui demandé. Avec le maillage intérieur, une des radios (généralement 802.11b/g) et/ou la liaison Ethernet filaire est utilisée pour la connexion aux clients, tandis que la deuxième radio (généralement 802.11a) est utilisée pour fédérer le trafic client. La liaison peut être à un seul saut ou à plusieurs sauts. Le maillage intérieur vous apporte ces valeurs :

- Il n'est pas nécessaire d'exécuter le câblage Ethernet sur chaque point d'accès.
- Aucun port de commutateur Ethernet n'est requis pour chaque point d'accès.
- Connectivité réseau dans laquelle les fils ne peuvent pas fournir de connectivité.
- Flexibilité de déploiement, non limitée à 100 mètres d'un commutateur Ethernet.
- Facile à déployer un réseau sans fil ad hoc.

Les grandes surfaces sont très attirées par le maillage intérieur en raison des économies réalisées sur le câblage et des raisons mentionnées précédemment.

Les spécialistes de l'inventaire l'utilisent pour effectuer des inventaires pour les détaillants, les usines de fabrication et d'autres entreprises. Ils souhaitent déployer rapidement un réseau Wi-Fi temporaire sur le site d'un client afin d'activer la connectivité en temps réel de leurs périphériques portables. Séminaires éducatifs, conférences, fabrication et hospitalité sont quelques-uns des endroits où l'architecture en maillage intérieur est nécessaire.

Lorsque vous aurez terminé la lecture de ce guide, vous comprendrez où utiliser et comment configurer le maillage intérieur. Vous comprendrez également que le maillage intérieur dans les boîtiers NEMA ne remplace PAS le maillage extérieur. De plus, vous comprendrez également la supériorité du maillage intérieur par rapport à la flexibilité des rôles de liaison (maillage à un seul saut) utilisée par les AP autonomes.

Hypothèses :

Vous connaissez Cisco Unified Wireless Network, son architecture et ses produits. Vous

connaissez les produits Cisco Outdoor Mesh et certains termes utilisés pour les réseaux maillés.

Glossaire des acronymes	
LWAPP	Lightweight Access Point Protocol : protocole de contrôle et de tunnellation des données entre les points d'accès et le contrôleur de réseau local sans fil.
Contrôleur WLAN/Contrôleur/WLC	Contrôleur de réseau local sans fil : périphériques Cisco qui centralisent et simplifient la gestion réseau d'un réseau local sans fil en regroupant un grand nombre de terminaux gérés dans un système unifié unique, permettant un système de réseau WLAN d'informations intelligentes unifié.
RAP	Point d'accès racine/point d'accès sur le toit : les périphériques sans fil Cisco font office de pont entre le contrôleur et d'autres points d'accès sans fil. AP qui sont câblés au contrôleur.
CARTE	Points d'accès maillés : périphérique sans fil Cisco qui se connecte à un RAP ou à un MAP sur l'air sur une radio 802.11a et fournit également des services aux clients sur une radio 802.11b/g.
Parent	Un point d'accès (soit un RAP/MAP) qui fournit l'accès à d'autres points d'accès en direct sur une radio 802.11a.
Neighbor (voisin)	Tous les points d'accès d'un réseau maillé sont voisins et ont des voisins. RAP n'a pas de voisin, car il est connecté au contrôleur.
Enfant	Un point d'accès plus éloigné du contrôleur est toujours un enfant. Un enfant aura un parent et

	plusieurs voisins dans un réseau maillé. Si le parent meurt, le voisin suivant avec la meilleure valeur de facilité sera choisi comme parent.
SNR	Rapport signal/bruit
BGN	Nom du groupe de ponts
EAP	Protocole d'authentification extensible
PSK	Clé prépartagée
AWPP	Adaptive Wireless Path Protocol

Aperçu

Le point d'accès réseau maillé intérieur Cisco est un périphérique d'infrastructure Wi-Fi à deux radios pour certains déploiements intérieurs. C'est un produit basé sur le Protocole de point d'accès allégé (LWAPP). Il fournit une radio 2,4 GHz et une radio 5,8 GHz compatible avec les normes 802.11b/g et 802.11a. Une radio (802.11b/g) peut être utilisée pour l'accès local (client) du point d'accès et la deuxième radio (802.11a) peut être configurée pour la liaison sans fil. Il fournit une architecture de maillage interne, où différents noeuds (radios) communiquent entre eux via une liaison et fournissent également un accès client local. Ce point d'accès peut également être utilisé pour les architectures de pontage point à point et point à multipoint. La solution de réseau maillé intérieur sans fil est idéale pour une couverture intérieure étendue car vous pouvez bénéficier de débits de données élevés et d'une bonne fiabilité avec une infrastructure minimale. Voici les principales fonctionnalités introduites avec la première version de ce produit :

- Utilisé en environnement intérieur pour un nombre de sauts de 3. Maximum 4.
- Noeud et hôte de relais pour les clients d'utilisateur final. Une radio 802.11a est utilisée comme interface de liaison et une radio 802.11b/g pour la maintenance des clients.
- Sécurité des points d'accès maillés intérieurs - EAP et PSK pris en charge.
- Les MAP LWAPP dans un environnement maillé communiquent avec les contrôleurs de la même manière que les AP Ethernet.
- Pontage sans fil point à point.
- Pontage sans fil point à multipoint.
- Sélection optimale du parent. SNR, EASE et BGN
- Améliorations BGN. NULL et mode par défaut.
- Accès local.
- Liste noire parente. Liste d'exclusion.
- Self Healing avec AWPP.
- Pontage Ethernet.
- Support de base de Voice à partir de la version 4.0.
- Sélection dynamique de la fréquence.
- Anti-échouage - Basculement BGN et DHCP par défaut.

Remarque : Ces fonctionnalités ne seront pas prises en charge :

- Canal de sécurité publique 4,9 GHz

- Routage autour des interférences
- Analyse en arrière-plan
- Accès universel
- Prise en charge du pont du groupe de travail

Logiciel de maillage intérieur

Indoor Mesh Software est une version spéciale qui se concentre sur les points d'accès intérieurs, en particulier le maillage intérieur. Dans cette version, les points d'accès intérieurs fonctionnent en mode local et en mode pont. Certaines des fonctionnalités disponibles dans la version 4.1.171.0 ne sont pas mises en oeuvre dans cette version. Des améliorations ont été apportées à l'interface de ligne de commande (CLI), à l'interface utilisateur graphique (GUI - navigateur Web) et à la machine d'état elle-même. L'objectif de ces améliorations est d'obtenir des informations précieuses de votre point de vue sur ce nouveau produit et sa viabilité fonctionnelle.

Améliorations spécifiques au maillage intérieur :

- **Environnement intérieur** : le maillage intérieur est mis en oeuvre à l'aide des LAP1242 et LAP1131. Ils sont mis en oeuvre dans des environnements intérieurs où le câble Ethernet n'est pas disponible. La mise en oeuvre est simple et rapide pour fournir une couverture sans fil aux zones éloignées du bâtiment (par exemple, les centres de distribution au détail, l'éducation pour les séminaires/conférences, la fabrication, l'accueil).
- **Améliorations du nom de groupe de ponts (BGN)** : afin de permettre à un administrateur réseau d'organiser un réseau de points d'accès maillés intérieurs dans des secteurs spécifiés par l'utilisateur, Cisco fournit un mécanisme appelé nom de groupe de ponts (Bridge Group Name) ou BGN. Le BGN, en fait le nom de secteur, fait qu'un AP se connecte à d'autres AP avec le même BGN. Dans le cas où un point d'accès ne trouve aucun secteur approprié correspondant à son BGN, le point d'accès fonctionne en mode par défaut, et choisit le meilleur parent qui répond au BGN par défaut. Cette fonctionnalité a déjà reçu beaucoup d'appréciation de la part du terrain alors qu'elle se bat contre les conditions d'AP échouées (si quelqu'un a mal configuré le BGN). Dans la version du logiciel 4.1.171.0, les points d'accès, lorsqu'ils utilisent le BGN par défaut, ne fonctionnent pas comme un noeud maillé intérieur et n'ont aucun accès client. Il est en mode maintenance pour accéder via le contrôleur, et si l'administrateur ne répare pas le BGN, le point d'accès redémarre après 30 minutes.
- **Améliorations de la sécurité** - La sécurité sur le code maillé intérieur est par défaut configurée pour EAP (Extensible Authentication Protocol). Ceci est défini dans RFC3748. Bien que le protocole EAP ne se limite pas aux réseaux locaux sans fil et puisse être utilisé pour l'authentification des réseaux locaux câblés, il est le plus souvent utilisé dans les réseaux locaux sans fil. Lorsque le protocole EAP est appelé par un périphérique NAS (Network Access Server) compatible 802.1X, tel qu'un point d'accès sans fil 802.11 a/b/g, les méthodes EAP modernes peuvent fournir un mécanisme d'authentification sécurisé et négocier un PMK sécurisé (Pair-wise Master Key) entre le client et le serveur NAS. Le PMK peut ensuite être utilisé pour la session de cryptage sans fil qui utilise le cryptage TKIP ou CCMP (basé sur AES). Avant la version du logiciel 4.1.171.0, les points d'accès à maillage extérieur utilisaient PMK/BMK pour rejoindre le contrôleur. C'était un processus en trois cycles. Maintenant, les cycles sont réduits pour une convergence plus rapide. L'objectif global de la sécurité du maillage intérieur est de fournir : Configuration sans intervention pour la sécurité du provisionnement. Confidentialité et authentification des trames de données. Authentification mutuelle entre le réseau et les noeuds. Possibilité d'utiliser des méthodes EAP standard pour l'authentification des noeuds d'AP maillés intérieurs. Découplage de la sécurité LWAPP et

du maillage intérieur. Les mécanismes de détection, de routage et de synchronisation sont améliorés à partir de l'architecture actuelle pour prendre en charge les éléments requis pour prendre en charge les nouveaux protocoles de sécurité. Les points d'accès maillés intérieurs découvrent d'autres points d'accès maillés en analysant et en écoutant les mises à jour gratuites des voisins à partir d'autres points d'accès maillés. Toute carte RAP ou intérieure connectée au réseau annonce les paramètres de sécurité principaux dans ses trames NEIGH_UPD (comme les trames de balise 802.11). Une fois cette phase terminée, une liaison logique entre un point d'accès maillé intérieur et un point d'accès racine est établie.

- **Améliorations WCS** Des alarmes de maillage intérieur ont été ajoutées. Il est possible de générer des rapports maillés intérieurs indiquant le nombre de sauts, le pire SNR, etc. Le test de liaison (parent à enfant, enfant à parent) peut être exécuté entre les nœuds, ce qui montre des informations très intelligentes. Les informations du point d'accès affichées sont beaucoup plus importantes que les précédentes. Vous pouvez également afficher les voisins potentiels. La surveillance de la santé est améliorée et plus facile d'accès.

Matériel et logiciels pris en charge

Le matériel et les logiciels requis pour le maillage intérieur sont au minimum :

- Les points d'accès Cisco LWAPP AIR-LAP1242AG-A-K9 et AIR-LAP1131AG-A-K9 prennent en charge la configuration du maillage intérieur.
- Le logiciel Cisco Mesh version 2 prend en charge le maillage d'entreprise (produits intérieurs et extérieurs). Il peut être installé uniquement sur les contrôleurs Cisco, Cisco 440x/210x et les WISM.
- Le logiciel Cisco Enterprise Mesh version 2 peut être téléchargé sur Cisco.com.

Intérieur et extérieur

Voici quelques-unes des principales différences entre le maillage intérieur et extérieur :

	Maillage intérieur	Maillage extérieur
Environnement	Intérieur UNIQUEMENT, matériel couvert	Extérieur uniquement, matériel robuste
Matériel	Point d'accès intérieur utilisant LAP1242 et LAP1131AG	Point d'accès extérieur utilisant LAP15xx et LAP152x
Niveaux de puissance	2,4 Ghz:20 dbm 5,8 Ghz:17 dbm	2,4 Ghz:28 dbm 5,8 Ghz:28 dbm
Taille des cellules	Environ 150 pieds	Environ 1 000 pieds
Hauteur de mise en oeuvre	2 mètres du sol	10 à 10 m du sol

Configuration

Assurez-vous d'examiner attentivement le guide avant de commencer toute mise en oeuvre, en particulier si vous avez reçu du nouveau matériel.

Mode C3 du contrôleur

Les points d'accès à maillage intérieur peuvent être déployés en tant que réseau de couche 3.



Mettre à niveau le contrôleur vers le dernier code

Procédez comme suit :

1. Pour mettre à niveau Mesh Release 2 sur un réseau maillé intérieur, votre réseau doit être exécuté sur 4.1.185.0 ou Mesh Release1, disponible sur Cisco.com.
2. Téléchargez le dernier code du contrôleur sur votre serveur TFTP. Dans l'interface GUI du contrôleur, cliquez sur **Commandes > Fichier de téléchargement**.
3. Sélectionnez le type de fichier comme **code** et indiquez l'adresse IP de votre serveur TFTP. Définissez le chemin d'accès et le nom du fichier.



Remarque : utilisez le serveur TFTP qui prend en charge les transferts de taille de fichier supérieure à 32 Mo. Par exemple, **ftpd32**. Sous Chemin d'accès au fichier, placez **"/** comme indiqué.

4. Une fois l'installation du nouveau micrologiciel terminée, utilisez la commande **show sysinfo** dans l'interface de ligne de commande pour vérifier que le nouveau micrologiciel est installé.

```
(Cisco Controller) >show sysinfo
Manufacturer's Name..... Cisco Systems Inc.
Product Name..... Cisco Controller
Product Version..... 4.1.175.19
RTOS Version..... 4.1.175.19
Bootloader Version..... 4.0.206.0
Build Type..... DATA + WPS

System Name..... CiscoMesh
System Location.....
System Contact.....
System ObjectID..... 1.3.6.1.4.1.14179.1.1.4.3
IP Address..... 10.13.10.20
System Up Time..... 1 days 22 hrs 3 mins 35 secs

Configured Country..... US - United States
Operating Environment..... Commercial (0 to 40 C)
Internal Temp Alarm Limits..... 0 to 65 C
Internal Temperature..... +38 C

State of 802.11b Network..... Enabled
State of 802.11a Network..... Enabled
--More-- or (q)uit
Number of VLANs..... 2
3rd Party Access Point Support..... Disabled
Number of Active Clients..... 3

Burned-in MAC Address..... 00:18:73:34:48:60
Crypto Accelerator 1..... Absent
Crypto Accelerator 2..... Absent
Power Supply 1..... Absent
Power Supply 2..... Present, OK
```

Remarque : Officiellement, Cisco ne prend pas en charge les mises à niveau pour les contrôleurs.

Adresse MAC :

Il est obligatoire d'utiliser le filtrage MAC. Cette fonctionnalité a fait de la solution Cisco Indoor Mesh une véritable " Zero Touch. " Contrairement aux versions précédentes, l'écran Mesh ne dispose plus de l'option de filtrage MAC.



Remarque : le filtrage MAC est activé par défaut.

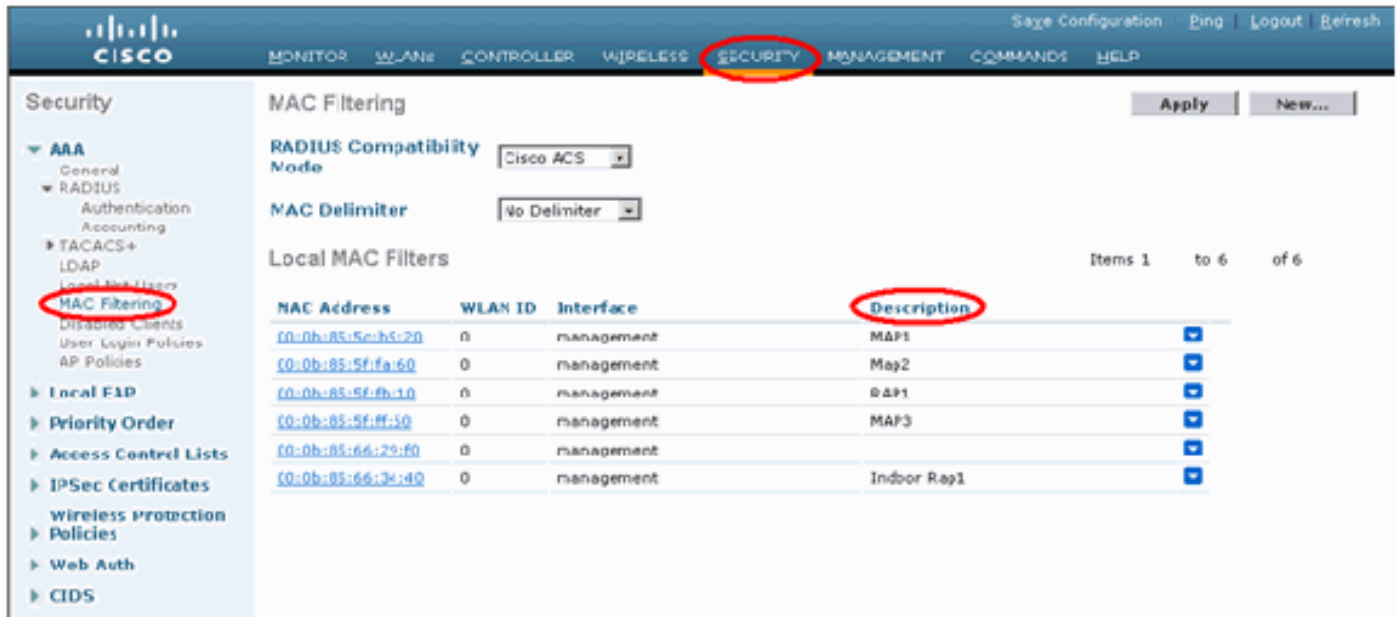
Enregistrer l'adresse MAC sur les radios

Dans un fichier texte, enregistrez les adresses MAC de toutes les radios d'AP maillées internes que vous déployez sur votre réseau. L'adresse MAC se trouve à l'arrière des points d'accès. Cela vous aide pour les tests futurs, car la plupart des commandes de l'interface de ligne de commande nécessitent que l'adresse MAC ou les noms des points d'accès soient entrés avec la commande. Vous pouvez également changer le nom des AP en quelque chose de plus facile à mémoriser, comme, " build number-pod number-AP type : les quatre derniers caractères hexadécimaux de l'adresse MAC "

Saisissez l'adresse MAC et les noms des radios dans le contrôleur

Le contrôleur Cisco tient à jour une liste d'adresses MAC d'autorisation de point d'accès interne. Le contrôleur ne répond qu'aux demandes de détection des radios internes qui apparaissent sur la liste d'autorisation. Saisissez les adresses MAC de toutes les radios que vous avez tendance à utiliser dans votre réseau sur le contrôleur.

Sur l'interface graphique du contrôleur, accédez à **Sécurité**, puis cliquez sur **Filtrage MAC** sur le côté gauche de l'écran. Cliquez sur **New** afin d'entrer les adresses MAC comme indiqué ici :



En outre, entrez les noms des radios pour plus de commodité sous **Description** (par exemple, emplacement, numéro de point d'accès, etc.) La description peut également être utilisée pour l'emplacement où les radios ont été installées pour une référence facile à tout moment.

Activer le filtrage MAC

Le filtrage MAC est activé par défaut.

Vous pouvez également choisir le mode de sécurité EAP ou PSK sur la même page.

À partir de l'interface graphique utilisateur du commutateur, utilisez ce chemin :

Chemin de l'interface GUI : **Sans fil > Maillage intérieur**

Le mode de sécurité ne peut être vérifié que sur l'interface de ligne de commande à l'aide de cette commande :

(Cisco Controller) > **show network**

```
(Cisco Controller) >show network
RF-Network Name..... iMesh
Web Mode..... Disable
Secure Web Mode..... Enable
Secure Shell (ssh)..... Enable
Telnet..... Enable
Ethernet Multicast Mode..... Disable Mode: Ucast
Ethernet Broadcast Mode..... Disable
User Idle Timeout..... 300 seconds
ARP Idle Timeout..... 300 seconds
ARP Unicast Mode..... Disabled
Cisco AP Default Master..... Disable
Mgmt via Wireless Interface..... Disable
Mgmt via Dynamic Interface..... Disable
Bridge Mac Filter Config..... Enable
Bridge Security Mode..... EAP
Mesh Multicast Mode..... 802.11b/g/n
Mesh Full Sector DFS..... Enable
Over The Air Provisioning of AP's..... Enable
Mobile Peer to Peer Blocking..... Disable
Apple Talk..... Disable
AP Fallback..... Enable
--More-- o (quit)
Web Auth Redirect Ports..... 80
Fast SSID Change..... Disabled
802.3 Bridging..... Disabled
```

Déploiement de maillage intérieur de couche 3

Pour un réseau maillé intérieur de couche 3, configurez les adresses IP des radios si vous n'avez pas l'intention d'utiliser le serveur DHCP (interne ou externe).

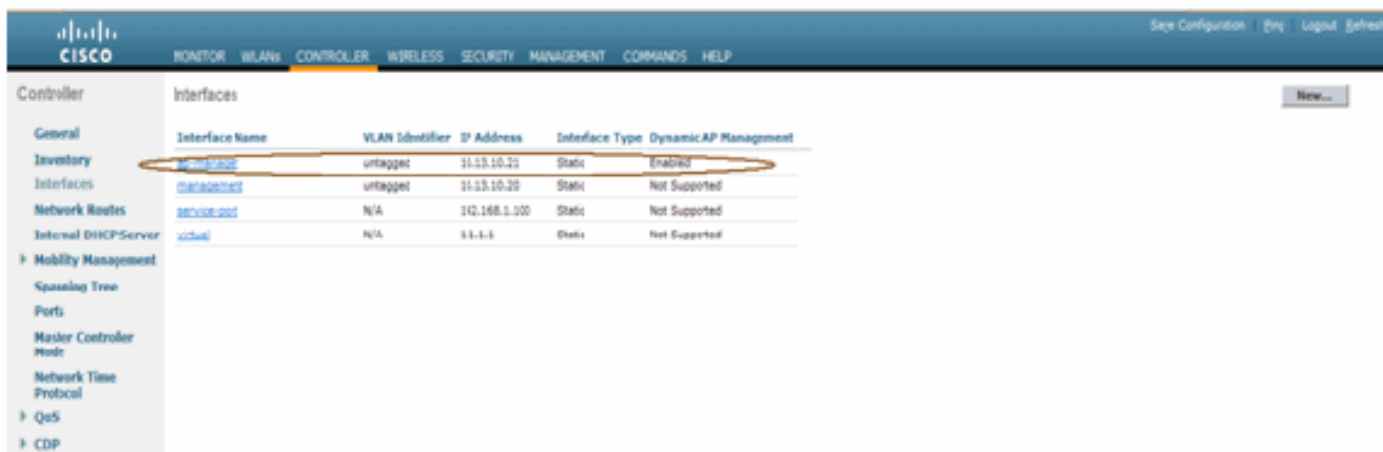
Pour un réseau maillé intérieur L3, si vous voulez utiliser le serveur DHCP, configurez le contrôleur en mode L3. Enregistrez la configuration et redémarrez le contrôleur. Assurez-vous de configurer l'option 43 sur le serveur DHCP. Après le redémarrage du contrôleur, les AP nouvellement connectés recevront leur adresse IP du serveur DHCP.

Définir les interfaces sur le contrôleur

Gestionnaire AP

Pour un déploiement L3, vous devez définir le **gestionnaire AP**. Le gestionnaire AP agit comme adresse IP source pour la communication du contrôleur aux points d'accès.

Chemin : **Controller > Interfaces > ap-manager > edit.**



Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
ap-manager	untagged	10.13.10.21	Static	Enabled
management	untagged	10.13.10.20	Static	Not Supported
MGMT-200	N/A	10.168.1.200	Static	Not Supported
control	N/A	10.1.1	Static	Not Supported

L'interface **AP-manager** doit se voir attribuer une adresse IP dans le même sous-réseau et VLAN que votre interface de gestion.



Interfaces > Edit

General Information

Interface Name: ap-manager
MAC Address: 00:18:73:34:4b:63

Interface Address

VLAN Identifier: 0
IP Address: 10.13.10.21
Netmask: 255.255.255.0
Gateway: 10.13.10.10

Physical Information

Port Number: 1
Backup Port: 0
Active Port: 1
Enable Dynamic AP Management:

DHCP Information

Primary DHCP Server: 10.13.10.10
Secondary DHCP Server:

Access Control List

ACL Name: none

Note: Changing the interface parameters causes the VLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

Rôles radio

Deux rôles radio principaux sont possibles avec cette solution :

- Point d'accès racine (RAP) : la radio avec laquelle vous voulez vous connecter au contrôleur (via un commutateur) jouera le rôle de RAP. Les RAP disposent d'une connexion câblée compatible LWAPP au contrôleur. Un RAP est un noeud parent vers n'importe quel réseau de pontage ou de maillage intérieur. Un contrôleur peut avoir un ou plusieurs RAP, chacun parent le même ou différents réseaux sans fil. Il peut y avoir plusieurs RAP pour le même réseau maillé intérieur pour la redondance.
- Point d'accès maillé intérieur (MAP) : la radio qui n'a pas de connexion câblée au contrôleur joue le rôle d'un point d'accès maillé intérieur. Ce point d'accès s'appelait auparavant Point d'accès Pole. Les MAP ont une connexion sans fil (via l'interface de liaison) à d'autres MAP peut-être et finalement à un RAP et donc au contrôleur. Les MAP peuvent également disposer d'une connexion Ethernet câblée à un LAN et servir de point d'extrémité de pont pour ce LAN (en utilisant une connexion P2P ou P2MP). Cela peut se produire simultanément, si configuré correctement en tant que pont Ethernet. Les clients de service MAP sur la bande ne sont pas utilisés pour l'interface de liaison.

Le mode par défaut d'un point d'accès est MAP.

Remarque : Les rôles radio peuvent être définis via l'interface utilisateur graphique ou CLI. Les points d'accès redémarrent après le changement de rôle.

Remarque : Vous pouvez utiliser l'interface de ligne de commande du contrôleur pour préconfigurer les rôles radio sur un point d'accès, à condition que le point d'accès soit physiquement connecté au commutateur ou que vous puissiez voir le point d'accès sur le commutateur en tant que RAP ou MAP.

```
(Cisco Controller) >config ap role ?
rootAP          RootAP role for the Cisco Bridge.
meshAP          MeshAP role for the Cisco Bridge.

(Cisco Controller) >config ap role meshAP ?
<Cisco AP>      Enter the name of the Cisco AP.

(Cisco Controller) >config ap role meshAP LAP1242-2
Changing the AP's role will cause the AP to reboot.
Are you sure you want to continue? (y/n)
```

Nom du groupe de ponts

Le BGN (Bridge Group Names) contrôle l'association des points d'accès. Les BGN peuvent logiquement regrouper les radios pour éviter que deux réseaux du même canal ne communiquent entre eux. Ce paramètre est également utile si vous avez plusieurs RAP dans votre réseau dans le même secteur (zone). Le BGN est une chaîne de dix caractères maximum.

Un nom de groupe de ponts défini en usine est attribué au stade de fabrication (valeur NULL). Il n'est pas visible pour vous. Par conséquent, même sans BGN défini, les radios peuvent toujours rejoindre le réseau. Si votre réseau comporte deux RAP dans le même secteur (pour plus de

capacité), il est recommandé de configurer les deux RAP avec le même BGN, mais sur différents canaux.

Remarque : Le nom du groupe de ponts peut être défini à partir de l'interface de ligne de commande et de l'interface utilisateur graphique du contrôleur.

```
(Cisco Controller) >config ap bridgegroupname set ?
<bridgegroupname> Set bridgegroupname on Cisco AP.
```

Après avoir configuré le BGN, l'AP se réinitialise.

Remarque : le BGN doit être configuré très soigneusement sur un réseau actif. Vous devez toujours commencer à partir du noeud le plus éloigné (dernier noeud) et vous diriger vers le RAP. La raison est que si vous commencez à configurer le BGN quelque part au milieu du multisaut, alors les noeuds au-delà de ce point seront supprimés car ces noeuds auront un BGN différent (ancien BGN).

Vous pouvez vérifier le BGN en exécutant cette commande CLI :

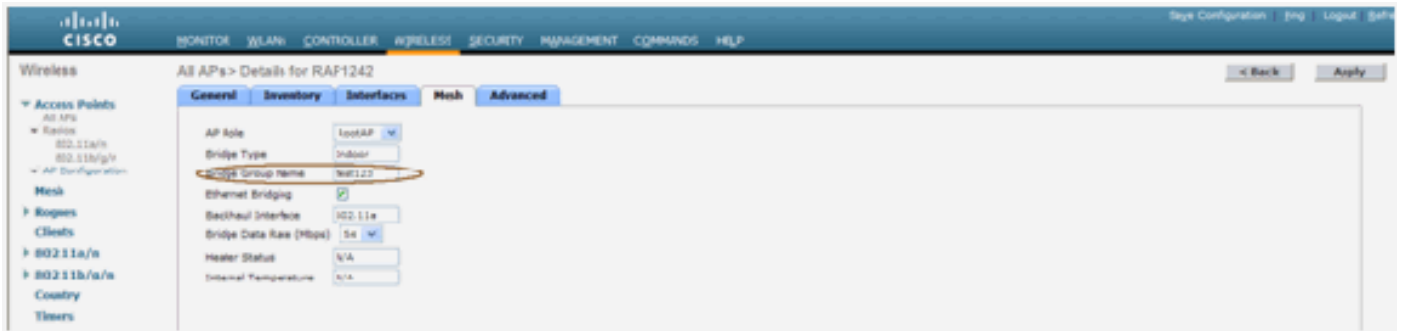
```
(Cisco Controller) > show ap config general
```

```
(Cisco Controller) >show ap config general RAP1242
Cisco AP Identifier..... 0
Cisco AP Name..... RAP1242
Country code..... US - United States
Regulatory Domain allowed by Country..... 802.11bg:-AR 802.11a:-A2
AP Country code..... US - United States
AP Regulatory Domain..... 802.11bg:-A 802.11a:-A
Switch Port Number ..... 1
MAC Address..... 00:18:74:fa:7d:1f
IP Address Configuration..... DHCP
IP Address..... 10.13.13.11
IP NetMask..... 255.255.255.0
Gateway IP Addr..... 10.13.13.10
Cisco AP Location..... default location
Cisco AP Group Name..... default-group
Primary Cisco Switch..... J2106-1
Secondary Cisco Switch.....
Tertiary Cisco Switch.....
Administrative State ..... ADMIN_ENABLED
Operation State ..... REGISTERED
Mirroring Mode ..... Disabled
AP Mode ..... Bridge
--More-- or (q)uit
AP Role ..... RootAP
Ethernet Bridging ..... Enabled
Bridge GroupName ..... test123
Public Safety ..... Disabled
Remote AP Debug ..... Disabled
S/W Version ..... 4.1.175.19
Boot Version ..... 12.3.7.1
Mini IOS Version ..... 3.0.51.0
Stats Reporting Period ..... 180
LED State..... Enabled
PoE Pre-Standard Switch..... Disabled
PoE Power Injector MAC Addr..... Disabled
Number Of Slots..... 2
AP Model..... AIR-LAP1242AG-A-K9
IOS Version..... 12.4(20070808:082741)
Reset Button..... Enabled
AP Serial Number..... FTX1035B3RH
AP Certificate Type..... Manufacture Installed
Management Frame Protection Validation..... Disabled
Console Login Name.....
Console Login State..... Unknown
AP Up Time..... 0 days, 02 h 43 m 38 s
AP LWAPP Up Time..... 0 days, 02 h 42 m 43 s
--More-- or (q)uit
Join Date and Time..... Sun Aug 19 11:59:07 2007
Join Taken Time..... 0 days, 00 h 00 m 24 s
Ethernet Port Duplex..... Unknown
Ethernet Port Speed..... Unknown
```

Vous pouvez également configurer ou vérifier le BGN à l'aide de l'interface graphique du

contrôleur :

Chemin : Sans fil > Tous les points d'accès > Détails.



Vous pouvez voir que les informations environnementales du point d'accès sont également affichées avec cette nouvelle version.

Configuration de la sécurité

Le mode de sécurité du maillage intérieur par défaut est EAP. Cela signifie que, à moins que vous configurez ces paramètres sur votre contrôleur, vos MAP ne se joindront pas :



CLI de configuration EAP de maillage intérieur

```
(Cisco Controller) >config mesh local-auth enable
enable Local Auth

(Cisco Controller) >config advanced eap ?
identity-request-timeout Configures EAP-Identity-Request Timeout in seconds.
identity-request-retries Configures EAP-Identity-Request Max Retries.
key-index Configure the key index used for dynamic WEP (802.1x) unicast key (PTK).
max-login-ignore-identity-response Configure to ignore the same username count reaching max in the E
AP identity response
request-timeout Configures EAP-Request Timeout in seconds.
request-retries Configures EAP-Request Max Retries.
```

Si vous devez rester en mode PSK, utilisez cette commande pour revenir au mode PSK :

```
(Cisco Controller) >config mesh security psk ?
(Cisco Controller) >config mesh security psk

All Mesh AP will be rebooted
Are you sure you want to start? (y/N)n
```

Commandes show EAP Maillage Intérieur

En mode EAP, vous pouvez vérifier ces commandes **show** pour vérifier l'authentification MAP :

(Cisco Controller) >show network

```
RF Network Name..... jaggi123
Web Mode..... Disable
Secure Web Mode..... Enable
Secure Shell (ssh)..... Enable
Telnet..... Enable
Ethernet Multicast Mode..... Disable Mode: Mcast 224.1.1.1
Ethernet Broadcast Mode..... Disable
User Idle Timeout..... 300 seconds
ARP Idle Timeout..... 300 seconds
ARP Unicast Mode..... Disabled
Cisco AP Default Master..... Disable
Mgmt Via Wireless Interface..... Enable
Mgmt Via Dynamic Interface..... Disable
Bridge MAC filter Config..... Disable
Bridge Security Mode..... EAP otherwise PSK
Mesh Multicast Mode..... 802.11b/g/n
Mesh Full Sector DFS..... Enable
Over The Air Provisioning of AP's..... Enable
Mobile Peer to Peer Blocking..... Disable
AP Fallback..... Enable
Web Auth Redirect Ports..... 80
--More-- or (q)uit
Fast SSID Change..... Disabled
802.3 Bridging..... Disable
```

(Cisco Controller) >show wlan 0

(Cisco Controller) >show wlan 0

```
WLAN Identifier..... 0
Profile Name..... Mesh_profile
Network Name (SSID)..... Mesh_ssid
Status..... Disabled
MAC Filtering..... Disabled
Broadcast SSID..... Enabled
AAA Policy Override..... Disabled
Number of Active Clients..... 2
Exclusionlist Timeout..... 60 seconds
Session Timeout..... 1800 seconds
Interface..... management
WLAN ACL..... unconfigured
DHCP Server..... Default
DHCP Address Assignment Required..... Disabled
Quality of Service..... Silver (best effort)
WMM..... Allowed
CCX - AironetIe Support..... Enabled
CCX - Gratuitous ProbeResponse (GPR)..... Disabled
Dot11-Phone Mode (7920)..... Disabled
Wired Protocol..... None
--More-- or (q)uit
IPv6 Support..... Disabled
Radio Policy..... All
Local EAP Authentication..... Enabled (Profile 'prfMaP1500L1EAuth93')
Security
  802.11 Authentication:..... Open System
  Static WEP Keys..... Disabled
  802.1x..... Disabled
  Wi-Fi Protected Access (WPA/WPA2)..... Enabled
    WPA (SSN IE)..... Disabled
    WPA2 (RSN IE)..... Enabled
    TKIP Cipher..... Disabled
    AES Cipher..... Enabled
    Auth Key Management
  802.1x..... Enabled
  PSK..... Disabled
  CCKM..... Disabled
  CKIP..... Disabled
  IP Security Passthru..... Disabled
  Web Based Authentication..... Disabled
  Web-Passthrough..... Disabled
  Conditional Web Redirect..... Disabled
  Auto Anchor..... Disabled
--More-- or (q)uit
H-REAP Local Switching..... Disabled
Infrastructure MFP protection..... Enabled (Global Infrastructure MFP Disabled)
Client MFP..... Optional
Tkip MIC Countermeasure Hold-down Timer..... 60

Mobility Anchor List
WLAN ID IP Address Status
```

(Cisco Controller) >show local-auth config

```
(Cisco Controller) >show local-auth config
User credentials database search order:
  Primary ..... Local DB
Timer:
  Active timeout ..... 300
Configured EAP profiles:
EAP Method configuration:
  EAP-FAST:
    Server key ..... <hidden>
    TTL for the PAC ..... 10
    Anonymous provision allowed ..... Yes
    Authority ID ..... 436973636f000000000000000000000000
    Authority Information ..... Cisco A-ID
(Cisco Controller) >show advanced eap
EAP-Identity-Request Timeout (seconds)..... 1
EAP-Identity-Request Max Retries..... 20
EAP Key-Index for Dynamic WEP..... 0
EAP Max-Login Ignore Identity Response..... enable
EAP-Request Timeout (seconds)..... 1
EAP-Request Max Retries..... 2
```

```
(Cisco Controller) >show advanced eap
```

Commandes de débogage EAP Maillage Intérieur

Afin de déboguer tout problème de mode EAP, utilisez ces commandes dans le contrôleur :

```
(Cisco Controller) >debug dot1x all enable
(Cisco Controller) >debug aaa all enable
```

Installation

Conditions préalables

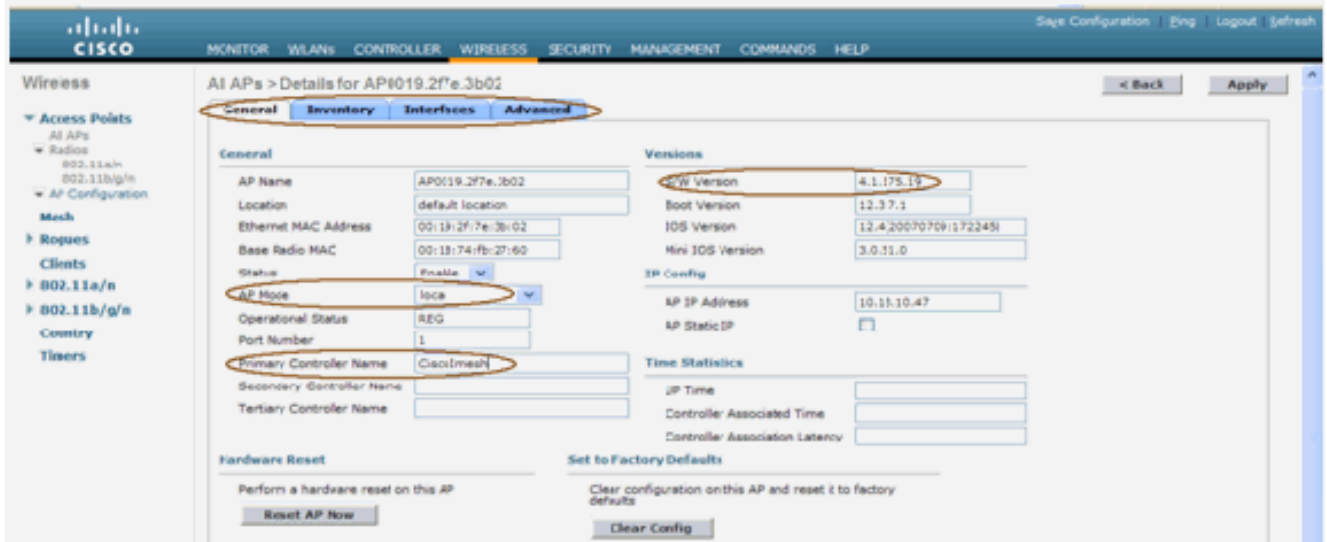
Le contrôleur doit exécuter la version recommandée du code. Cliquez sur **Monitor** pour vérifier la version du logiciel. Il est possible de vérifier la même chose via l'interface de ligne de commande.

```
(Cisco Controller) >show sysinfo
Manufacturer's Name..... Cisco Systems Inc.
Product Name..... Cisco Controller
Product Version..... 4.1.175.19
RTOS Version..... 4.1.175.19
Bootloader Version..... 4.0.206.0
Build Type..... DATA + WPS
System Name..... CiscoImesh
System Location.....
System Contact.....
System ObjectID..... 1.3.6.1.4.1.14179.1.1.4.3
IP Address..... 10.13.10.20
System Up Time..... 1 days 22 hrs 3 mins 35 secs
Configured Country..... US - United States
Operating Environment..... Commercial (0 to 40 C)
Internal Temp Alarm Limits..... 0 to 65 C
Internal Temperature..... +38 C
State of 802.11b Network..... Enabled
State of 802.11a Network..... Enabled
--More-- or (q)uit..... 2
Number of VLANs..... Disabled
3rd Party Access Point Support..... 3
Number of Active Clients.....
Burned-in MAC Address..... 00:18:73:34:48:60
Crypto Accelerator 1..... Absent
Crypto Accelerator 2..... Absent
Power Supply 1..... Absent
Power Supply 2..... Present, OK
```

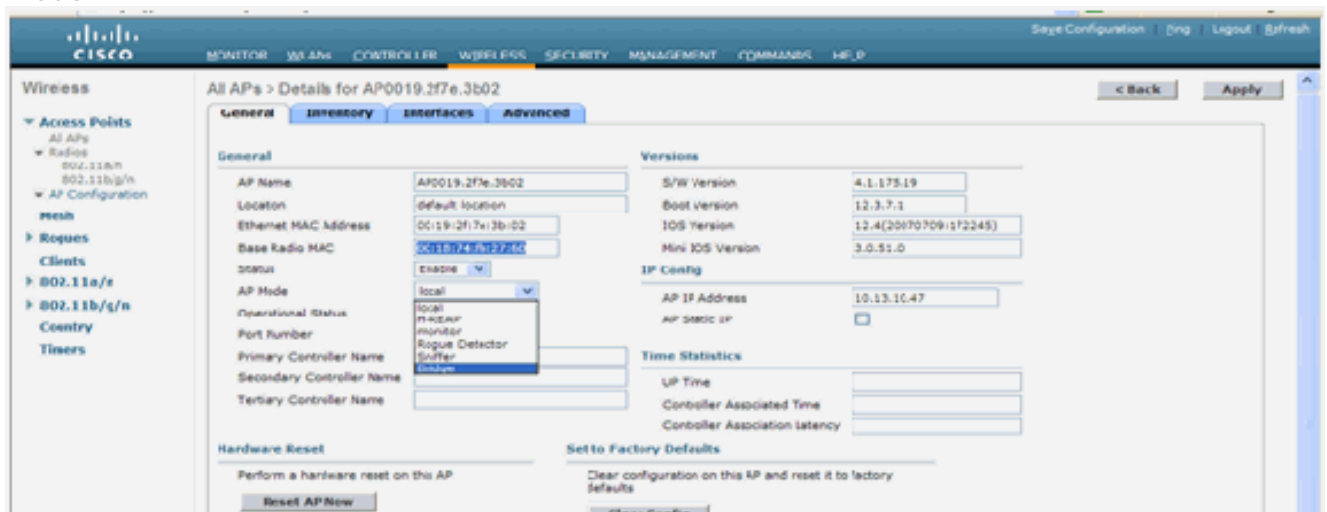
Les systèmes tels que le serveur DHCP, le serveur ACS et le serveur WCS doivent être accessibles.

Installation

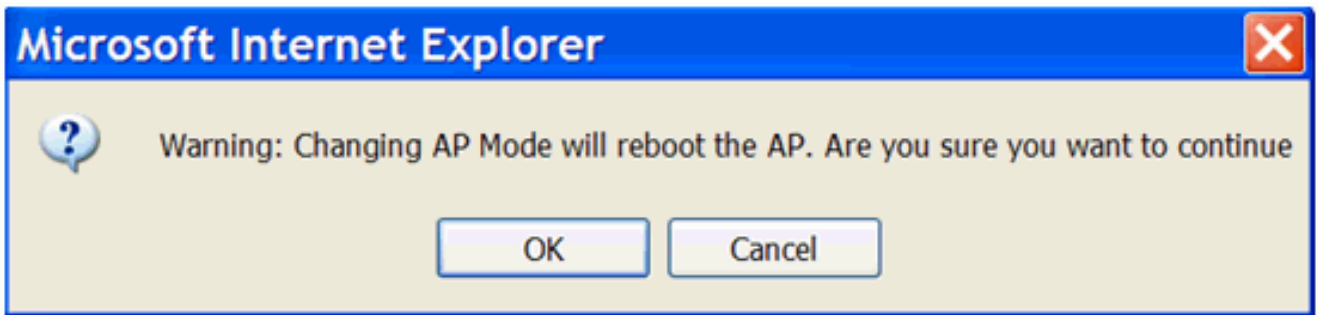
1. Connectez tous les LAP (1131AG/1242AG) à un réseau de couche 3 sur le même sous-réseau que l'adresse IP de gestion. Tous les points d'accès se joindront au contrôleur en tant que points d'accès en mode local. Dans ce mode, attribuez un premier au point d'accès le nom du contrôleur principal, le nom du contrôleur secondaire et le nom du contrôleur tertiaire.



2. Capturez l'adresse MAC radio de base du point d'accès (par exemple, 00:18:74: fb : 27:60).
3. Ajoutez l'adresse MAC du point d'accès pour que le point d'accès se connecte en mode pont.
4. Cliquez sur **Security > MAC-filter > New**.
5. Ajoutez l'adresse MAC copiée et nommez les points d'accès dans la liste de filtrage MAC et la liste des points d'accès.
6. Choisissez **Bridge** dans la liste **AP Mode**.



7. Il vous invite à confirmer, car cela redémarrera l'AP.



8. Le point d'accès redémarre et joint le contrôleur en mode Pont. La nouvelle fenêtre AP comporte un onglet supplémentaire : MAILLAGE. Cliquez sur l'onglet **MESH** pour vérifier le rôle, le type de pont, le nom du groupe de ponts, le pontage Ethernet, l'interface de liaison arrière, le débit de données du pont, etc.



9. Dans cette fenêtre, accédez à la liste des rôles AP et sélectionnez le rôle approprié. Dans ce cas, le rôle par défaut est un MAP. Le nom du groupe de ponts est vide par défaut. L'interface Back-haul est 802.11a. Le débit de données du pont (c'est-à-dire le débit de données du back-haul) est de 24 Mbits/s.
10. Connectez le point d'accès que vous voulez comme RAP au contrôleur. Déployez les radios (MAP) aux emplacements souhaités. Allumez les radios. Vous devriez pouvoir voir toutes les radios sur le contrôleur.

```
(Cisco Controller) >show ap summ
Number of APs..... 3
AP Name           Slots  AP Model          Ethernet MAC      Location          Port  Country
-----
RAP1242           2      AIR-LAP1242AG-A-K9  00:18:74:fa:7d:1f default location  1     US
LAP1242-1         2      AIR-LAP1242AG-A-K9  00:1b:2b:a7:ad:bf default location  1     US
LAP1242-2         2      AIR-LAP1242AG-A-K9  00:14:1b:59:07:af default location  1     US
```

11. Essayez d'avoir des conditions de visibilité directe entre les noeuds. Si les conditions de visibilité directe n'existent pas, créer des zones de dégagement Fresnel pour obtenir des conditions de proximité de la ligne de site.
12. Si plusieurs contrôleurs sont connectés au même réseau maillé intérieur, vous devez spécifier le nom du contrôleur principal sur chaque noeud. Sinon, le contrôleur qui est vu en premier sera pris comme principal.

[Configuration de l'alimentation et du canal](#)

Le canal de liaison peut être configuré sur un RAP. Les MAP se brancheront au canal RAP. L'accès local peut être configuré indépendamment pour les MAP.

À partir de l'interface utilisateur graphique du commutateur, suivez le chemin : **Wireless > radio 802.11a > configure**.



Remarque : le niveau d'alimentation Tx par défaut sur la liaison est le niveau d'alimentation le plus élevé (niveau 1) et la gestion des ressources radio (RRM) est désactivée par défaut.

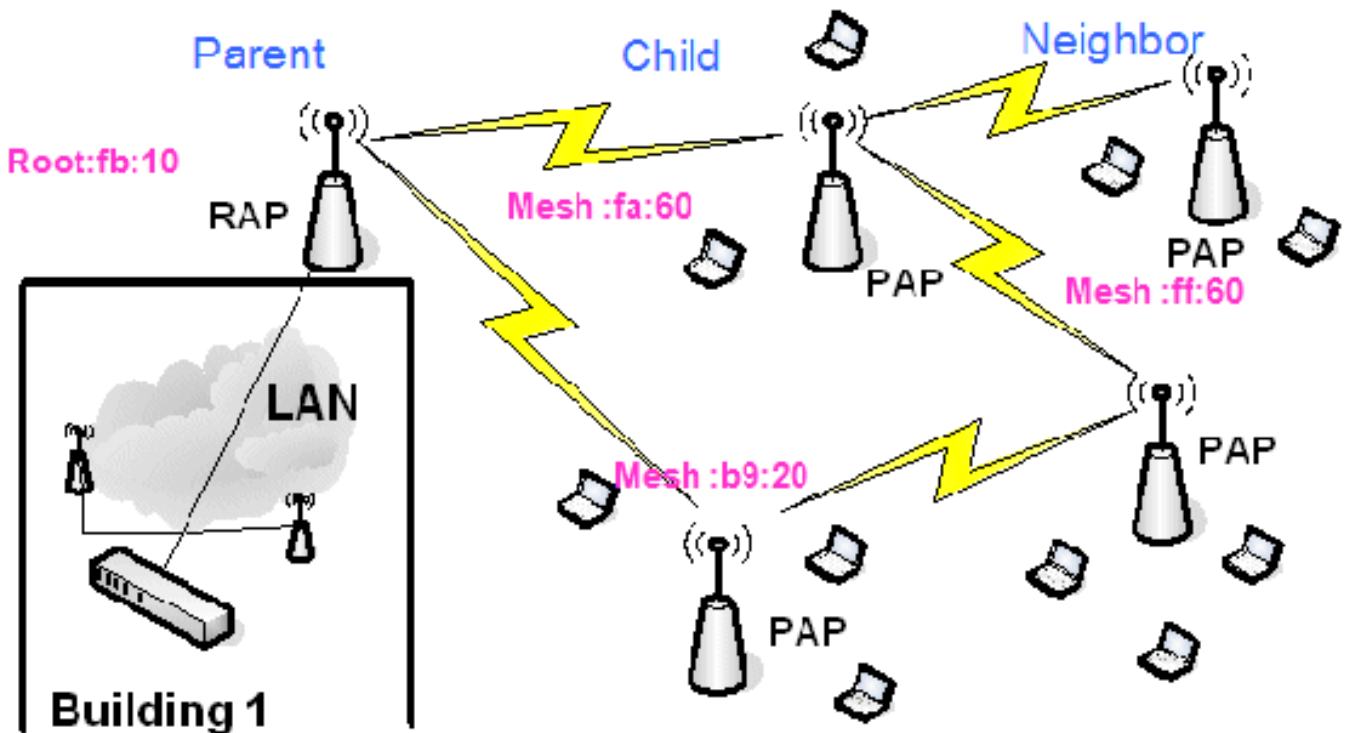
Si vous collez des RAP, nous vous recommandons d'utiliser d'autres canaux adjacents sur chaque RAP. Cela réduira les interférences entre canaux.

Vérification RF

Dans un réseau maillé intérieur, nous devons vérifier la relation parent-enfant entre les noeuds. Le **saut** est une liaison sans fil entre les deux radios. La relation parent-enfant change lorsque vous parcourez le réseau. Cela dépend de l'emplacement du réseau maillé intérieur.

La radio la plus proche du contrôleur dans une connexion sans fil (saut) est un **parent** de la radio de l'autre côté du saut. Dans un système à sauts multiples, il existe une structure de type arborescence où le noeud connecté au contrôleur est un RAP (**parent**). Le noeud immédiat de l'autre côté du premier saut est un **enfant**, et les noeuds suivants du deuxième saut sont les **voisins** de ce parent particulier.

Figure 1 : Réseau à deux sauts



Dans la Figure 1, les noms des points d'accès sont mentionnés pour des raisons de commodité. Dans la capture d'écran suivante, le **RAP(fb:10)** fait l'objet d'une enquête. Ce noeud peut voir (dans le déploiement réel) les points d'accès maillés intérieurs (**fa:60 et b9:20**) comme enfants et **MAP ff:60** comme voisins.

À partir de l'interface graphique du commutateur, suivez le chemin : **Wireless > All AP > Rap1 > Neighbor Info**.



Assurez-vous que les relations parents-enfants sont établies et gérées correctement pour votre réseau maillé intérieur.

Vérification des interconnexions

show Mesh est une commande informative permettant de vérifier l'interconnectivité dans votre réseau.

Vous devez donner ces commandes à chaque noeud (AP) à l'aide de l'interface de ligne de commande du contrôleur, et télécharger les résultats dans un fichier Word ou texte sur le site de téléchargement.

```
(Cisco Controller) >show mesh ?
env          Show mesh environment.
neigh       Show AP neigh list.
path        Show AP path.
stats       Show AP stats.
secbh-stats Show Mesh AP secondary backhaul stats.
per-stats   Show AP Neighbor Packet Error Rate stats.
queue-stats Show AP local queue stats.
security-stats Show AP security stats.
config      Show mesh configurations.
secondary-backhaul Show mesh secondary-backhaul
client-access Show mesh backhaul with client access.
public-safety Show mesh public safety.
background-scanning Show mesh background-scanning state.
cac         Show mesh cac.
```

Dans votre réseau maillé intérieur, choisissez une liaison à plusieurs sauts et émettez ces commandes à partir du RAP. Téléchargez le résultat des commandes sur le site de téléchargement.

Dans la section suivante, toutes ces commandes ont été émises pour le réseau maillé intérieur à deux sauts illustré à la Figure 1.

[Afficher le chemin de maillage intérieur](#)

Cette commande affiche les adresses MAC, les rôles radio des noeuds, les rapports signal/bruit en dBs pour liaison ascendante/descendante (SNRUp, SNRDown) et le SNR de liaison en dB pour un chemin particulier.

```
(Cisco Controller) >show mesh path RAP1242
AP Name/Radio Mac Channel Snr-Up Snr-Down Link-Snr Flags State
-----
RAP1242 is a Root AP.
(Cisco Controller) >show mesh path LAP1242-2
AP Name/Radio Mac Channel Snr-Up Snr-Down Link-Snr Flags State
-----
LAP1242-1 56 29 29 27 0x86b UPDATED NEIGH PARENT BEACON
RAP1242 56 41 32 34 0x86b UPDATED NEIGH PARENT BEACON
RAP1242 is a Root AP.
```

[Afficher la synthèse des voisins maillés intérieurs](#)

Cette commande affiche les adresses MAC, les relations parent-enfant et les SNR de liaison ascendante/descendante en dB.

```
(Cisco Controller) >show mesh neigh ?
detail      Show Link rate neigh detail.
summary     Show Link rate neigh summary.
(Cisco Controller) >show mesh neigh summary RAP1242
AP Name/Radio Mac Channel Snr-Up Snr-Down Link-Snr Flags State
-----
LAP1242-2 56 0 0 0 0x860 BEACON
LAP1242-1 56 0 33 0 0x960 CHILD BEACON

(Cisco Controller) >show mesh neigh summary LAP1242-1
AP Name/Radio Mac Channel Snr-Up Snr-Down Link-Snr Flags State
-----
LAP1242-2 56 30 29 28 0x961 UPDATED CHILD BEACON
RAP1242 56 43 46 31 0x86b UPDATED NEIGH PARENT BEACON
```

À ce stade, vous devriez être en mesure de voir les relations entre les noeuds de votre réseau et

de vérifier la connectivité RF en voyant les valeurs SNR pour chaque liaison.

Sécurité d'accès à la console AP

Cette fonctionnalité offre une sécurité renforcée à l'accès console du point d'accès. Un câble console pour le point d'accès est requis pour utiliser cette fonctionnalité.

Celles-ci sont prises en charge :

- Une CLI pour pousser la combinaison ID utilisateur/mot de passe vers le point d'accès spécifié

```
(Cisco Controller) >config ap username Cisco password Cisco ?  
all          Configures the Username/Password for all connected APs.  
<Cisco AP>  Enter the name of the Cisco AP.
```

- Une commande CLI pour transmettre la combinaison nom d'utilisateur/mot de passe à tous les points d'accès enregistrés au contrôleur

```
(Cisco Controller) >config ap username Cisco password Cisco all
```

Avec ces commandes, la combinaison userid/password poussée du contrôleur est persistante à travers le rechargement sur les AP. Si un point d'accès est effacé du contrôleur, il n'y a pas de mode d'accès de sécurité. L'AP génère une interruption SNMP avec une connexion réussie. Le point d'accès génère également une interruption SNMP lors d'une défaillance de connexion à la console pendant trois fois consécutives.

Pontage Ethernet

Pour des raisons de sécurité, le port Ethernet sur les MAP est désactivé par défaut. Il ne peut être activé qu'en configurant le pontage Ethernet sur le RAP et les MAP respectifs.

Par conséquent, le pontage Ethernet doit être activé pour deux scénarios :

- Lorsque vous souhaitez utiliser les noeuds de maillage intérieurs comme ponts.
- Lorsque vous souhaitez connecter un périphérique Ethernet (PC/ordinateur portable, caméra vidéo, etc.) sur le MAP à l'aide de son port Ethernet.

Chemin : **Wireless** > Cliquez sur n'importe quel point d'accès > **Mesh**.



Il existe une commande CLI qui peut être utilisée pour configurer la distance entre les noeuds effectuant le pontage. Essayez de connecter un périphérique Ethernet tel qu'une caméra vidéo à chaque saut et observez les performances.

Amélioration du nom du groupe de ponts

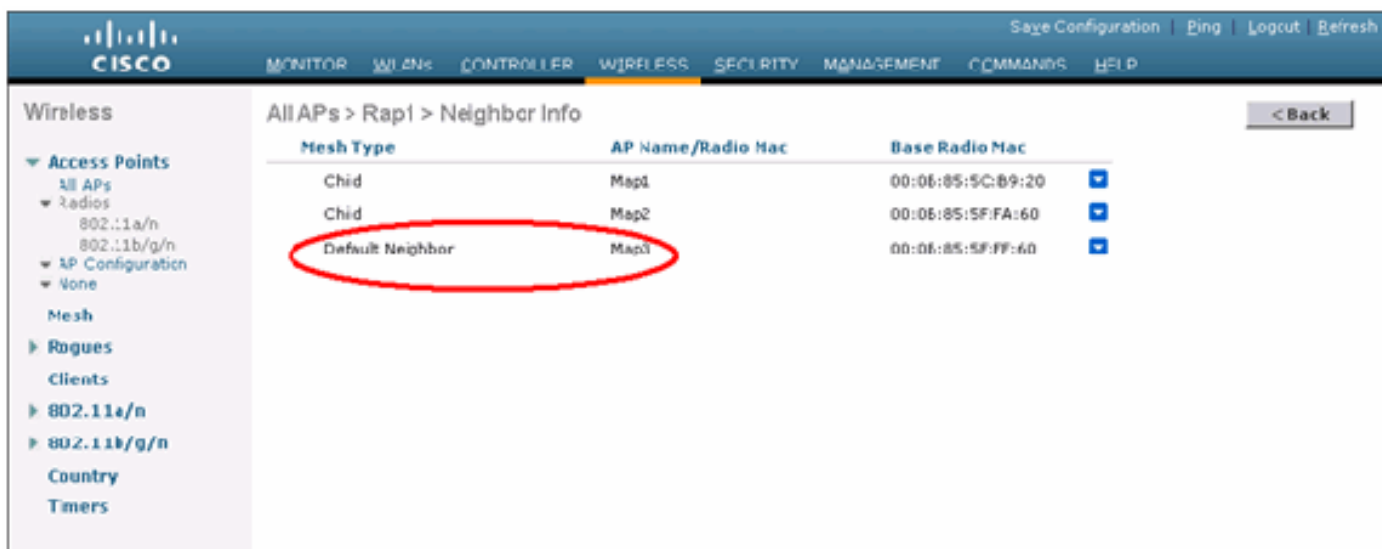
Il est possible qu'un point d'accès soit mal approvisionné avec un " " de nom de groupe de pont " pour lequel il n'était pas prévu. Selon la conception du réseau, ce point d'accès peut être en mesure ou non de joindre et de trouver son secteur/arborescence correct. S'il ne parvient pas à atteindre un secteur compatible, il peut devenir bloqué.

Afin de récupérer un point d'accès bloqué de ce type, le concept de 'default' bridgegroupname a été introduit avec le code 3.2.xx.x. L'idée de base est qu'un AP qui n'est pas en mesure de se connecter à un autre AP avec son nom de pont configuré, tente de se connecter avec " " par défaut (le mot) en tant que nom de pont. Tous les noeuds exécutant le logiciel 3.2.xx.x et les versions ultérieures acceptent d'autres noeuds avec ce bridgegroupname.

Cette fonctionnalité peut également aider à ajouter un nouveau noeud ou un noeud mal configuré à un réseau en cours d'exécution.

Si vous avez un réseau en cours d'exécution, prenez un AP préconfiguré avec un BGN différent et faites-le rejoindre le réseau. Vous verrez ce point d'accès dans le contrôleur en utilisant " BGN " par défaut après avoir ajouté son adresse MAC dans le contrôleur.

```
(CiscoController) >show mesh path Map3:5f:ff:60
00:0B:85:5F:FA:60 state UPDATED NEIGH PARENT DEFAULT (106B), snrUp 48, snrDown 4
8, linkSnr 49
00:0B:85:5F:FB:10 state UPDATED NEIGH PARENT BEACON (86B), snrUp 72, snrDown 63,
linkSnr 57
00:0B:85:5F:FB:10 is RAP
```



The screenshot shows the Cisco Wireless Controller GUI. The breadcrumb navigation is "All APs > Rap1 > Neighbor Info". The table below lists the neighbors for the selected AP.

Mesh Type	AP Name/Radio Mac	Base Radio Mac
Child	Map1	00:0B:85:5C:89:20
Child	Map2	00:0B:85:5F:FA:60
Default Neighbor	Map3	00:0B:85:5F:FF:60

L'AP utilisant le BGN par défaut peut agir comme un AP Maillé Intérieur normal associant des clients et formant des relations parent Maillage Intérieur enfant.

Dès que ce point d'accès utilisant le BGN par défaut trouvera un autre parent avec le BGN correct, il bascule vers lui.

Journaux - Messages, Sys, AP et interruptions

Journaux des messages

Activez le niveau de rapport pour les journaux de messages. À partir de l'interface de ligne de commande du contrôleur, exécutez cette commande :

```
(Cisco Controller) >config msglog level ?  
critical      Critical hardware or software Failure.  
error         Non-Critical software error.  
security      Authentication or security related error.  
warning       Unexpected software events.  
verbose       Significant system events.  
  
(Cisco Controller) >config msglog level verbose
```

Pour afficher les journaux des messages, exécutez cette commande à partir de l'interface de ligne de commande du contrôleur :

```
(Cisco Controller) >show msglog  
Message Log Severity Level ..... VERBOSE  
Mon Jul 11 01:42:08 2005 [SECURITY] apf_foreignap.c 765: Received a packet for  
which no AP was configured from 00:0F:B5:93:71:E7 on port 0.  
Fri Jul 8 06:12:02 2005 [ERROR] spam_radius.c 93: spamRadiusProcessResponse: A  
P Authorization failure for 00:0b:85:0e:04:80  
Fri Jul 8 05:40:15 2005 [ERROR] spam_tmw.c 501: Did not receive heartbeat reply  
from AP 00:0b:85:0e:05:80  
Fri Jul 8 05:38:45 2005 [ERROR] spam_lrad.c 1310: Validation of Config Request  
failed from AP 00:0b:85:0e:05:80  
Fri Jul 8 05:38:40 2005 [ERROR] spam_lrad.c 1310: Validation of Config Request  
failed from AP 00:0b:85:0e:14:00  
Fri Jul 8 05:38:40 2005 Previous message occurred 5 times  
Fri Jul 8 05:33:54 2005 [ERROR] spam_lrad.c 1310: Validation of Config Request  
failed from AP 00:0b:85:0e:05:80  
Fri Jul 8 05:32:23 2005 [ERROR] poe.c 449: poeInitPowerSupply : poePortResync  
returned FAILURE.  
Fri Jul 8 05:32:17 2005 [ERROR] dhcpd.c 78: dhcp server: binding to 0.0.0.0  
Fri Jul 8 05:32:17 2005 [ERROR] rrmgroup.c 733: Airewave Director: 802.11a swi  
tch group reset  
Fri Jul 8 05:32:16 2005 [ERROR] rrmgroup.c 733: Airewave Director: 802.11bg sw  
itch group reset  
Fri Jul 8 05:32:16 2005 Previous message occurred 2 times  
Fri Jul 8 05:31:19 2005 [CRITICAL] osapi_sem.c 794: Error! osapiMutexTake cal
```

Pour télécharger les journaux des messages, utilisez l'interface GUI du contrôleur :

1. Cliquez sur **Commandes > Télécharger.**

Commands

Download File
Upload File
 Reboot
 Reset to Factory Default
 Set Time

Download file to Controller Clear Download

File Type

TFTP Server

IP Address	<input type="text" value="10.51.1.51"/>
Maximum retries	<input type="text" value="10"/>
Timeout (seconds)	<input type="text" value="6"/>
file Path	<input type="text" value="/"/>
file Name	<input type="text" value="AS_4200_4_1_152_51.asp"/>

2. Entrez vos informations de serveur TFTP. Cette page vous donne différentes options de téléchargement et vous voulez que ces fichiers soient envoyés : Journal des messages Journal des événements Journal des interruptions Fichier de blocage (le cas échéant) Afin de rechercher les fichiers de blocage, cliquez sur **Management > Controller Crash**.

Management

Management: Via Wireless Apply

Enable Controller Management to be accessible from Wireless Clients

Summary

- SNMP
- HTTP
- Telnet-SSH
- Serial Port
- Local Management Users
- User Sessions
- Lags
- Mgmt Via Wireless
- Tech Support**
 - System Resource Information
 - Controller Crash**
 - AP Log

Journaux AP

Accédez à cette page GUI sur le contrôleur pour vérifier les journaux des points d'accès pour votre point d'accès local, le cas échéant :

Save Configuration | Ping | Logout | Refresh

MONITOR WLANs CONTROLLER WIRELESS SECURITY **MANAGEMENT** COMMANDS HELP

Management

AD Log Information

AP Name	AP ID	MAC Address	Admin Status	Operational States	Port	
Fap3:5fff:60	25	00:0b:05:5f:ff:60	Enable	REG	1	Get Log

Summary

SNMP
General
SNMP V3 Users
Communities
Trap Receivers
Trap Controls
Trap Logs

HTTP

Telnet-SSH

Serial Port

Local Management Users

User Sections

Syslog

Mgmt Via Wireless

Message Logs

Tech Support
System Resource Information
Controller Crash
AP Log

Journaux de déROUTement

Accédez à cette page GUI du contrôleur et vérifiez les journaux de déROUTement :

Save Configuration | Ping | Logout | Refresh

MONITOR WLANs CONTROLLER WIRELESS SECURITY **MANAGEMENT** COMMANDS HELP

Management

Trap Logs Clear Log

Number of Traps since last reset 1208
Number of Traps since log last viewed 1208

Log	System Time	Trap
0	Tue Mar 7 18:58:51 2006	Rogue AP: 00:0b:05:1e:53:66 detected on Base Radio MAC: 00:0b:05:5f:ff:10 Interface no:1(002.11b/g) with RSSI: -66 and SNR: 19
1	Tue Mar 7 18:58:51 2006	Rogue AP: 00:0b:05:1e:53:66 detected on Base Radio MAC: 00:0b:05:5c:b9:20 Interface no:1(002.11b/g) with RSSI: -79 and SNR: 11
2	Tue Mar 7 18:58:51 2006	Rogue AP: 00:0b:05:17:48:df detected on Base Radio MAC: 00:0b:05:5c:b9:20 Interface no:1(002.11b/g) with RSSI: -78 and SNR: 12
3	Tue Mar 7 18:58:51 2006	Rogue AP: 00:02:8a:58:46:f2 detected on Base Radio MAC: 00:0b:05:5c:b9:20 Interface no:1(002.11b/g) with RSSI: -85 and SNR: 3
4	Tue Mar 7 18:58:51 2006	Rogue AP: 00:0b:05:17:03:4d detected on Base Radio MAC: 00:0b:05:5c:b9:20 Interface no:1(002.11b/g) with RSSI: -80 and SNR: 11
5	Tue Mar 7 18:58:51 2006	Rogue AP: 00:0b:05:1e:49:8d detected on Base Radio MAC: 00:0b:05:5c:b9:20 Interface no:1(002.11b/g) with RSSI: -82 and SNR: 9
6	Tue Mar 7 18:58:51 2006	Rogue AP: 00:0b:05:1e:49:8e detected on Base Radio MAC: 00:0b:05:5c:b9:20 Interface no:1(002.11b/g) with RSSI: -80 and SNR: 11
7	Tue Mar 7 18:58:51 2006	Rogue AP: 00:40:96:a1:61:2a detected on Base Radio MAC: 00:0b:05:5c:b9:20 Interface no:1(002.11b/g) with RSSI: -80 and SNR: 5
8	Tue Mar 7 18:58:40 2006	Rogue: 00:40:96:a2:7d:c2 removed from Base Radio MAC: 00:0b:05:5c:b9:20 Interface no:1(002.11b/g)
9	Tue Mar 7 18:58:15 2006	Rogue: 00:0b:05:1b:60:5a removed from Base Radio MAC: 00:0b:05:5c:b9:20 Interface no:1(002.11b/g)
10	Tue Mar 7 18:58:15 2006	Rogue: 00:13:5f:55:ea:06 removed from Base Radio MAC: 00:0b:05:5c:b9:20 Interface no:1(002.11b/g)
11	Tue Mar 7 18:58:15 2006	Rogue: 00:0b:05:17:9c:61 removed from Base Radio MAC: 00:0b:05:5f:ff:d0 Interface no:1(002.11b/g)
12	Tue Mar 7 18:58:10 2006	AP Disassociated, Base Radio MAC:00:0b:05:5f:ff:60
13	Tue Mar 7 18:58:10 2006	AP's Interface:1(002.11b) Operation State Down: Base Radio MAC:00:0b:05:5f:ff:60 Cause=Heartbeat Timeout
14	Tue Mar 7 18:58:10 2006	AP's Interface:0(002.11a) Operation State Down: Base Radio MAC:00:0b:05:5f:ff:60 Cause=Heartbeat Timeout
15	Tue Mar 7 18:58:10 2006	AP Disassociated, Base Radio MAC:00:0b:05:5f:ff:60

Performances

Test de convergence de démarrage

La convergence est le temps nécessaire à un RAP/MAP pour établir une connexion LWAPP stable avec un contrôleur WLAN à partir du moment où il a démarré comme indiqué ici :

Test de convergence	Temps de convergence (min : s)			
	RAP	MAP1	MAP2	MAP3
Mise à niveau de l'image	2:34	3:50	5:11	6:38
Redémarrage du contrôleur	0:38	0:57	1:12	1:32
Mise sous tension du réseau maillé intérieur	2:44	3:57	5:04	6:09
Redémarrage RAP	2:43	3:57	5:04	6:09
Rejoindre le MAP		3:58	5:14	6:25
Modification MAP du parent (même canal)		0:38		

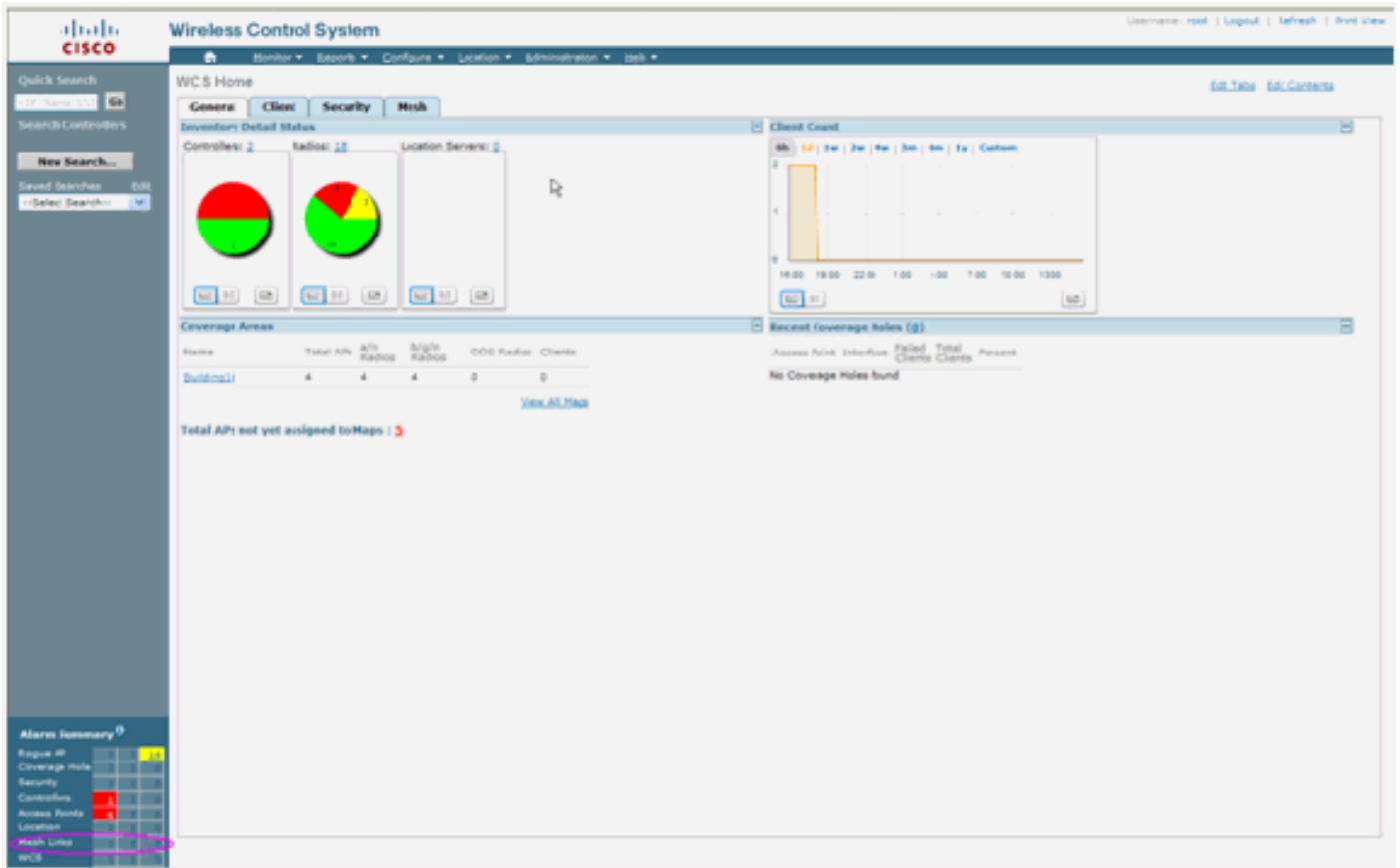
WCS

Alarmes de maillage intérieur

WCS génère ces alarmes et événements liés au réseau maillé intérieur en fonction des interruptions du contrôleur :

- SNR de liaison médiocre
- Parent modifié
- Enfant déplacé
- Le parent change fréquemment
- Événement du port de console
- Échec de l'autorisation MAC
- Échecs d'authentification
- Enfant exclu Parent

Cliquez sur **Liens maillés**. Il affiche toutes les alarmes liées aux liaisons maillées intérieures.



Ces alarmes s'appliquent aux liaisons maillées intérieures :

- Mauvaise liaison SNR : cette alarme est générée si la liaison SNR tombe en dessous de 12db. L'utilisateur ne peut pas modifier ce seuil. Si un SNR défectueux est détecté sur la liaison de liaison de liaison pour enfant/parent, le déroutement est généré. Le déroutement contient la valeur SNR et les adresses MAC. La gravité de l'alarme est majeure. Le rapport signal/bruit (SNR) est important, car la puissance élevée du signal ne suffit pas à garantir de bonnes performances au récepteur. Le signal entrant doit être plus fort que tout bruit ou toute interférence présent. Par exemple, il est possible d'avoir une puissance de signal élevée et d'avoir des performances sans fil médiocres en cas de forte interférence ou de niveau sonore élevé.
- Parent modifié : cette alarme est générée lorsque l'enfant est déplacé vers un autre parent. Lorsque le parent est perdu, l'enfant se joint à un autre parent, et l'enfant envoie un déroutement contenant les adresses MAC de l'ancien parent et du nouveau parent à WCS. Gravité de l'alarme : Informations.
- Enfant déplacé : cette alarme est générée lorsque WCS reçoit un piège perdu enfant. Lorsque le point d'accès parent a détecté la perte d'un enfant et qu'il n'est pas en mesure de communiquer avec cet enfant, il envoie un déroutement Enfant perdu à WCS. Le déroutement contient l'adresse MAC enfant. Gravité de l'alarme : Informations.
- Le parent MAP a changé fréquemment - Cette alarme est générée si le point d'accès maillé intérieur change fréquemment de parent. Lorsque le paramètre MAP parent-change-counter dépasse le seuil dans une durée donnée, il envoie un déroutement à WCS. Le déroutement contiendra le nombre de fois où des changements de MAP ont été effectués et la durée du temps. Par exemple, s'il y a 5 modifications dans les 2 minutes, le déroutement est envoyé. Gravité de l'alarme : Informations.
- Parent enfant exclu - Cette alarme est générée lorsqu'un enfant met un parent sur liste noire. Un enfant peut mettre un parent sur une liste noire lorsque l'enfant n'a pas pu s'authentifier

sur le contrôleur après un nombre fixe de tentatives. L'enfant se souvient du parent inscrit sur la liste noire et lorsque l'enfant se connecte au réseau, il envoie le dérivement qui contient l'adresse MAC parent inscrite sur la liste noire et la durée de la période de la liste noire.

Alarmes autres que les liaisons maillées intérieures :

- Accès au port de console : le port de console permet au client de modifier le nom d'utilisateur et le mot de passe pour récupérer le point d'accès extérieur échoué. Cependant, pour empêcher tout accès utilisateur autorisé au point d'accès, WCS doit envoyer une alarme lorsque quelqu'un tente de se connecter. Cette alarme est requise pour fournir une protection car le point d'accès est physiquement vulnérable lorsqu'il est situé à l'extérieur. Cette alarme sera générée si l'utilisateur s'est connecté avec succès au port de console AP, ou s'il a échoué trois fois de suite.
- Échec de l'autorisation MAC - Cette alarme est générée lorsque le point d'accès tente de rejoindre le maillage intérieur mais ne parvient pas à s'authentifier car il ne figure pas dans la liste de filtres MAC. WCS recevra un dérivement du contrôleur. Le dérivement contiendra l'adresse MAC du point d'accès qui a échoué à l'autorisation.

Rapport maillé et statistiques

Nous reprenons le cadre amélioré de rapport et de statistiques du 4.1.185.0 :

- Aucun autre chemin
- Sauts de noeud maillé
- Statistiques des erreurs de paquets
- Statistiques de paquets
- Pire saut de noeud
- Les pires liaisons SNR

The screenshot displays the Cisco Wireless Control System (WCS) interface. The top navigation bar includes the Cisco logo, the title "Wireless Control System", and user information: "Username: root | Logout | Refresh | Print View". Below the navigation bar, there are tabs for "Monitor", "Reports", "Configure", "Location", "Administration", and "Help". The "Reports" tab is active, showing a sub-section for "Mesh No Alternate Parent". A dropdown menu is set to "-- Select a command --" and a "GO" button is present. Below this, a table lists reports with columns for "Report Title", "Schedule", "Last Run Time", and "Next Scheduled Run". One report titled "test" is listed with a "Disabled" schedule and a "Run Now" link. On the left sidebar, the "Mesh Reports" section is highlighted with a red circle. Below the sidebar, an "Alarm Summary" table shows various metrics:

Metric	Value
Rogue AP	0 191
Coverage Hole	0
Security	0 0 0
Controllers	0 0 0
Access Points	0 0 2
Mesh Links	0 0 0
Location	0 0 0

[Aucun autre chemin](#)

Le point d'accès maillé intérieur a généralement plusieurs voisins. Dans le cas où un point d'accès maillé intérieur perd sa liaison parent, le point d'accès doit être en mesure de trouver le parent alternatif. Dans certains cas, s'il n'y a aucun voisin affiché, alors l'AP ne pourra pas aller à d'autres parents s'il perd ses parents. Il est essentiel pour l'utilisateur de savoir quels points d'accès n'ont pas de parents alternatifs. Ce rapport répertorie tous les AP qui n'ont aucun autre voisin autre que le parent actuel.

[Sauts de noeud maillé intérieur](#)

Ce rapport indique le nombre de sauts à l'écart du point d'accès racine (RAP). Vous pouvez créer le rapport en fonction de ces critères :

- AP par contrôleur
- AP par étage

[Taux d'erreur de paquet](#)

Les erreurs de paquets peuvent être causées par des interférences et des abandons de paquets. Le calcul du taux d'erreur des paquets est basé sur les paquets envoyés et envoyés avec succès. Le taux d'erreur de paquet est mesuré sur la liaison de liaison et est collecté pour les voisins et le parent. Le point d'accès envoie régulièrement des informations de paquet au contrôleur. Dès que le parent change, le point d'accès envoie les informations d'erreur de paquet collectées au contrôleur. WCS interroge les informations d'erreur de paquet du contrôleur toutes les 10 minutes par défaut et les stocke dans la base de données pendant 7 jours maximum. Dans WCS, le taux d'erreur de paquet est représenté sous forme de graphique. Le graphique des erreurs de paquets est basé sur les données historiques stockées dans la base de données.

[Statistiques de paquets](#)

Ce rapport indique les valeurs de compteur des paquets de transmission totale du voisin et du nombre total de paquets du voisin transmis avec succès. Vous pouvez créer le rapport en fonction de certains critères.

[Les pires liaisons SNR](#)

Des problèmes de bruit peuvent survenir à des moments différents et le bruit peut augmenter à des rythmes différents ou durer pendant des durées différentes. La figure suivante permet de créer des rapports pour les interfaces radio a et b/g ainsi que pour les interfaces sélectives. Le rapport répertorie par défaut les 10 pires liaisons SNR. Vous pouvez choisir entre 5 à 50 pires liens. Le rapport peut être généré pendant les 1 dernières heures, les 6 dernières heures, le dernier jour, les 2 derniers jours et jusqu'à 7 jours. Les données sont interrogées toutes les 10 minutes par défaut. Les données sont conservées dans la base de données pendant un maximum de sept jours. Les critères de sélection du type de voisin peuvent être Tous les voisins, Parent/Enfants uniquement.

Wireless Control System

Mesh Worst SNR Links > WorstSNRLinks

Save Save And Run Run Now Cancel Delete

General Schedule Results

Report Title: WorstSNRLinks

Mesh Worst SNR Links: 10

Neighbor Type: All Neighbors (Table Only)

Reporting Period: Last

Between: 00 Hour 00 Min

And: 00 Hour 00 Min

Wireless Control System

Mesh Worst SNR Links > WorstSNRLinks

Save Save And Run Run Now Cancel Delete

General Schedule Results

Report | Email | Printer Friendly

Mesh Worst SNR Links

Generated: Tuesday 22 15:58:55 PST 2017

Mesh Worst SNR Links: 10

Neighbor Type: All Neighbors (Table Only)

Reporting Period: Last 1 hours

Name	MAC Address	Neigh AP Name	Neigh MAC	Neigh SNR	Neigh Type
LAP1242-3	01:14:1b:59:07a0	LAP1242-2	01:14:1b:59:39d0	-17	parent
LAP1242-3	01:14:1b:59:07a0	LAP1242-2	01:14:1b:59:39d0	-20	parent
LAP1242-3	01:14:1b:59:07a0	LAP1242-2	01:14:1b:59:39d0	-22	parent
LAP1242-3	01:14:1b:59:07a0	LAP1242-2	01:14:1b:59:39d0	-18	parent
LAP1242-3	01:14:1b:59:07a0	LAP1242-2	01:14:1b:59:39d0	-22	parent

Pire sauts de noeud

Ce rapport répertorie les 10 points d'accès de sauts les plus mauvais par défaut. Si les points d'accès sont trop éloignés, les liaisons peuvent être très faibles. L'utilisateur peut isoler les points d'accès qui ont de nombreux sauts loin du point d'accès racine et prendre les mesures appropriées. Vous pouvez choisir de modifier ce **nombre de noeuds** entre 5 et 50. Les critères de filtre **Type de rapport** de cette figure peuvent être Tableau uniquement ou Tableau et Graphique :

Wireless Control System

Mesh Worst Node Hops > WorstNodeHops

Save Save And Run Run Now Cancel Delete

General Schedule Results

Report Title: WorstNodeHops

Number Nodes: 10

Report Type: Table Only

Reporting Period: Last 1 hour

Between: 00 Hour 00 Min

And: 00 Hour 00 Min

Cette figure montre le résultat du dernier rapport :

Wireless Control System

Mesh Worst Node Hops > WorstNodeHops

Save Save And Run Run Now Cancel Delete

General Schedule Results

Export | Email | Printer Friendly

Mesh Worst Node Hops

Generated: Thu Nov 22 16:10:3 PST 2007

Number Nodes: 10

Report Type: Table Only

Reporting Period: Last 1 hour

AP Name	MAC Address	Node Hops	Parent AP Name	Parent MAC Address
LAP242-3	00:14:10:59:07:a0	2	LAP242-2	00:14:10:59:3f:10
LAP242-1	00:10:20:a7:af:90	1	RAP202	00:10:74:9c:7e:10
LAP242-2	00:14:10:59:3f:10	1	RAP202	00:10:74:9c:7e:10

Statistiques de sécurité

Les statistiques de sécurité maillée intérieure sont affichées sur la page de détails de l'AP sous la section Bridging info. Une entrée dans la table Statistiques de sécurité du noeud maillé intérieur est créée lorsqu'un noeud maillé intérieur enfant s'associe ou s'authentifie avec un noeud maillé intérieur parent. Les entrées sont supprimées lorsque le noeud Maillage intérieur se dissocie du contrôleur.

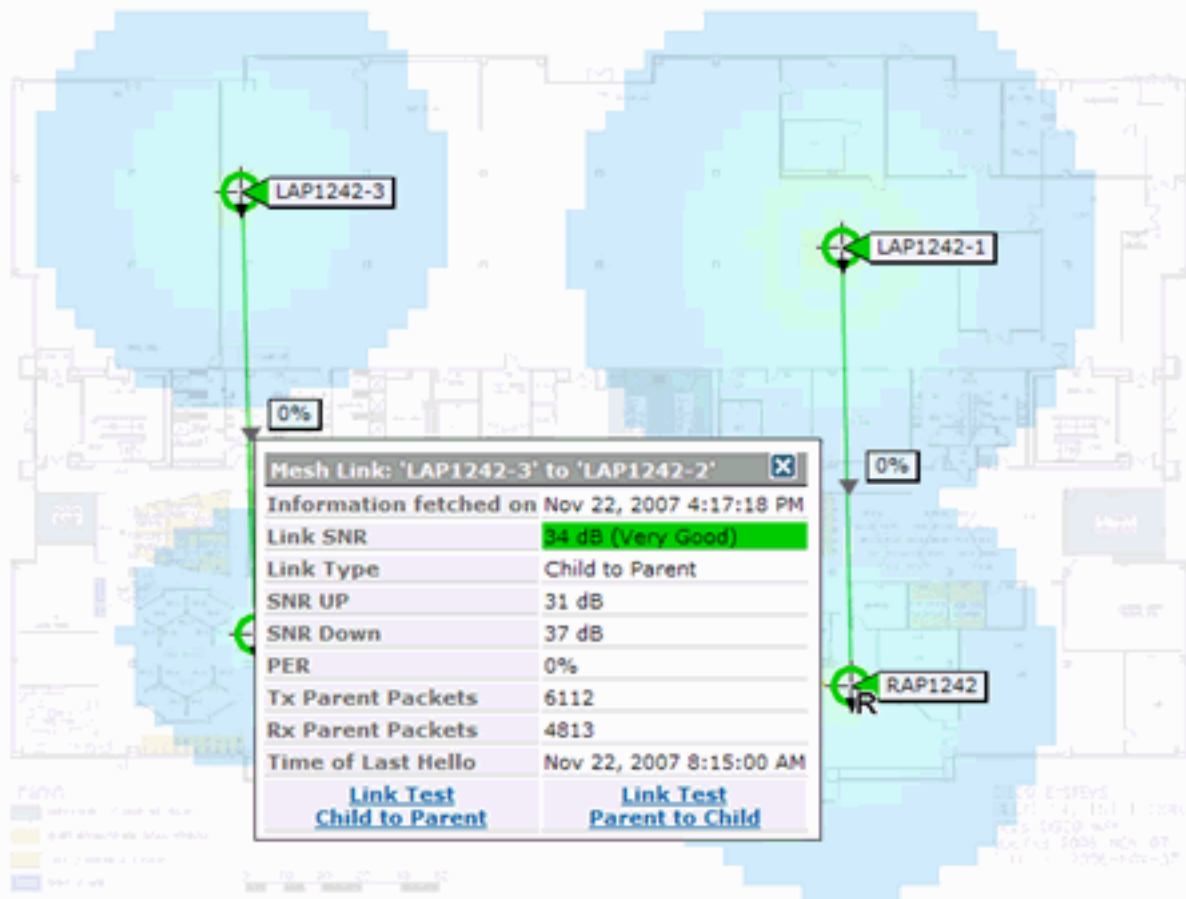
Test de liaison

Le test de liaison AP à AP est pris en charge sur le WCS. On peut sélectionner deux points d'accès et appeler un test de liaison entre les deux.

Si ces points d'accès sont des voisins RF, le test de liaison peut avoir un résultat. Le résultat est affiché dans une boîte de dialogue sur la carte elle-même sans rafraîchissement complet de la page. Le dialogue peut être facilement éliminé.

Cependant, si ces 2 points d'accès ne sont pas des voisins RF, alors WCS n'essaie pas de trouver un chemin entre les 2 points d'accès afin d'effectuer un test de liaison multiple combiné.

Lorsque la souris est déplacée sur la flèche de la liaison entre les deux noeuds, cette fenêtre apparaît :



Test de liaison de noeud à noeud

L'outil de test de liaison est un outil à la demande qui permet de vérifier la qualité de la liaison entre deux points d'accès. Dans WCS, cette fonctionnalité est ajoutée à la page de détails de l'AP.

Sur la page de détails de l'AP, sous l'onglet **Lien maillé intérieur** où les liens sont répertoriés à côté, il y a un lien pour effectuer le test de liaison.

L'outil Test de liaison CLI du contrôleur comporte les paramètres d'entrée facultatifs : Taille de paquet, nombre total de paquets de test de liaison, durée du test et débit de liaison de données. Le test de liaison a des valeurs par défaut pour ces paramètres facultatifs. Les adresses MAC des noeuds sont les seuls paramètres d'entrée obligatoires.

L'outil de test de liaison teste la force, le paquet envoyé et le paquet reçu entre les noeuds. Le lien pour le test de liaison est affiché dans le rapport détaillé de l'AP. Lorsque vous cliquez sur le lien, un écran contextuel affiche les résultats du test de lien. Le test de liaison ne s'applique qu'aux parents et aux voisins.

Le résultat du test de liaison génère des paquets envoyés, des paquets reçus, des paquets d'erreur (compartiments pour des raisons de différences), SNR, Noise Floor et RSSI.

Le test de liaison fournit au minimum les détails suivants sur l'interface utilisateur graphique :

- Paquets de test de liaison envoyés
- Paquets de test de liaison reçus
- Intensité du signal en dBm

- Rapport signal/bruit

[Liaisons de voisinage de point d'accès à la demande](#)

Il s'agit d'une nouvelle fonctionnalité de la carte WCS. Vous pouvez cliquer sur un point d'accès maillé et une fenêtre contextuelle contenant des informations détaillées s'affiche. Vous pouvez ensuite cliquer sur **Afficher les voisins maillés**, qui récupère les informations de voisinage pour le point d'accès sélectionné et affiche une table avec tous les voisins pour le point d'accès maillé intérieur sélectionné.

L'option View Mesh Neighbor Link affiche tous les voisins du point d'accès mis en surbrillance. Cet instantané affiche tous les voisins, le type des voisins et la valeur SNR.

[Test Ping](#)

Le test Ping est un outil à la demande utilisé pour envoyer des requêtes ping entre le contrôleur et le point d'accès. L'outil Test Ping est disponible dans la page de détails de l'AP et dans MAP. Cliquez sur le lien **Exécuter le test Ping** dans la page de détails du point d'accès ou à partir des informations du point d'accès MAP pour lancer la requête ping du contrôleur au point d'accès actuel.

[Conclusion](#)

Le maillage d'entreprise (c'est-à-dire le maillage intérieur) est une extension de la couverture sans fil de Cisco aux endroits où la connectivité Ethernet câblée ne peut pas être assurée. La flexibilité et la facilité de gestion d'un réseau sans fil sont assurées par le maillage d'entreprise.

La plupart des fonctionnalités des points d'accès câblés sont fournies par la topologie de maillage interne. Le maillage d'entreprise peut également coexister avec les points d'accès filaires sur le même contrôleur.

[Informations connexes](#)

- [Support et documentation techniques - Cisco Systems](#)