Guide de déploiement d'un maillage en intérieur

Contenu

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 à une radio 2.4 gigahertz et à un compatible par radio 5.8 gigahertz 802.11b/g et 802.11a. Une radio peut être utilisée pour l'accès local (de client) pour le Point d'accès (AP) et la deuxième radio peut être configurée pour la liaison Sans fil. LAP1242/LAP1131 prend en charge le P2P, le P2MP, et le type de maille d'architectures.

Veillez à lire par le guide avant de tenter les installations l'unes des.

Ce document décrit le déploiement du Maillage sans fil d'entreprise pour la maille d'intérieur. Ce document permettra aux utilisateurs Sans fil de comprendre les principes fondamentaux de la maille d'intérieur, où configurer la maille d'intérieur, et comment configurer la maille d'intérieur. La maille d'intérieur est un sous-ensemble du Maillage sans fil d'entreprise de Cisco déployé utilisant des contrôleurs sans-fil et des aps légers.

La maille d'intérieur est un sous-ensemble de l'architecture de maille d'entreprise déployée sur l'architecture Sans fil unifiée. La maille d'intérieur est dans la demande aujourd'hui. Avec la maille d'intérieur, une des radios (typiquement 802.11b/g) et/ou le lien d'Ethernets câblés est utilisée pour se connecter aux clients, alors que la deuxième radio (typiquement 802.11a) est utilisée au trafic de client de liaison. La liaison peut être un saut simple ou au-dessus de plusieurs sauts. La maille d'intérieur t'apporte ces valeurs :

- Pas devant exécuter des Ethernets câblant à chaque AP.
- Le port de commutateur ethernet n'est pas exigé pour chaque AP.
- Connexion réseau où les fils ne peuvent pas fournir la Connectivité.
- Flexibilité dans le déploiement – non limité à 100m d'un commutateur ethernet.
- Facile de déployer un réseau Sans fil ad-hoc.

des revendeurs de Grand-case sont très attirés à la maille d'intérieur en raison des économies sur le câblage aussi bien que pour les raisons précédemment mentionnées.

Utilisation de spécialistes en inventaire qu'elle n exécutant l'inventaire compte pour des revendeurs, usines, et d'autres sociétés. Ils veulent déployer rapidement un réseau WiFi provisoire à un site client pour activer la Connectivité en temps réel pour leurs périphériques portables. Les séminaires, les conférences, la fabrication, et le tourisme éducatifs sont certains des endroits où l'architecture d'intérieur de maille est nécessaire.

Quand vous finissez de lire ce guide, vous comprendrez où à utiliser-et comment configurer la maille d'intérieur. Vous comprendrez également que la maille d'intérieur dans des rubriques de description NEMA n'est pas un remplacement pour la maille extérieure. De plus, vous comprendrez également la supériorité de la maille d'intérieur au-dessus de la flexibilité de rôle de lien (maille simple de saut) utilisée par des aps autonomes.

Suppositions :

Vous avez la connaissance du réseau sans fil unifié Cisco, de l'architecture, et des Produits. Vous

avez la connaissance des Produits extérieurs de maille de Cisco et une partie de la terminologie utilisée pour le réseau de maille.

Glossaire des acronymes	
LWAPP	Point d'accès léger Protocol – Le protocole de Tunnellisation de contrôle et de données entre les aps et le contrôleur LAN Sans fil.
Contrôleur WLAN /Controller /WLC	Contrôleur LAN Sans fil – Périphériques de Cisco qui centralisent et simplifient la Gestion de réseau d'un WLAN en réduisant le grand nombre de points finaux gérés dans un système simple et unifié, tenant compte d'un système intelligent unifié de réseau WLAN de l'information.
RAP	Point d'accès de toit de point d'Access de racine – Les périphériques sans fil de Cisco agissent en tant que passerelle entre le contrôleur et toute autre radio aps. Aps qui sont câblés au contrôleur.
MAP	Maille aps – Le périphérique sans fil de Cisco qui se connecte à un RAP ou à une MAP au-dessus de l'air sur une radio 802.11a et aussi entretient des clients sur une radio 802.11b/g.
Parent	AP (l'un ou l'autre un RAP/MAP) qui permet d'accéder à d'autres aps au-dessus de l'air sur une radio 802.11a.
Voisin	Tous les aps dans un réseau maillé sont des voisins et ont des voisins. Le RAP n'a pas un voisin en tant que lui a câblé au contrôleur.
Enfant	AP plus loin du contrôleur est toujours un enfant. Un

	enfant aura un parent et beaucoup de voisins dans un réseau maillé. Si le parent meurt, le prochain voisin avec la meilleure valeur de facilité sera parent choisi.
SNR	Rapport signal/bruit
BGN	Nom de groupe de passerelle
EAP	Extensible Authentication Protocol
PSK	Clé pré-partagée
AWPP	Chemin Sans fil adaptatif Protocol

Aperçu

Le Point d'accès d'intérieur de réseau maillé de Cisco est un périphérique d'infrastructure de WiFi de deux-radio pour des déploiements d'intérieur sélectionnés. C'est un produit basé sur le Protocole de point d'accès allégé (LWAPP). Il fournit à une radio 2.4 gigahertz et à un compatible par radio 5.8 gigahertz 802.11b/g, les normes 802.11a. Une radio (802.11b/g) peut être utilisée pour l'accès local (de client) pour AP et la deuxième radio (802.11a) peut être configurée pour la liaison Sans fil. Il fournit une architecture d'intérieur de maille, où les différents Noeuds (radios) parlent entre eux par l'intermédiaire de la liaison et fournissent également l'accès client local. Cet AP peut également être utilisé pour des architectures de pontage point par point et point-à-multipoint. La solution de réseau maillé d'intérieur Sans fil est idéale pour la grande couverture d'intérieur comme vous pouvez avoir les débits de données élevés et la bonne fiabilité avec l'infrastructure minimum. Ce sont les caractéristiques saillantes de base introduites avec la première release de ce produit :

- Utilisé dans l'environnement intérieur pour un nombre de sauts 3. Maximum 4.
- Noeud et hôte de relais pour des clients d'utilisateur. Une radio 802.11a est utilisée comme interface de liaison et radio 802.11b/g pour les clients de service.
- Sécurité d'intérieur de la maille aps – EAP et PSK pris en charge.
- Les cartes LWAPP dans un environnement de maille communiquent avec les contrôleurs de la même manière que des aps Ethernet-reliés comparés.
- Pont point par point en radio.
- Pont point-à-multipoint en radio.
- Sélection optimale de parent. SNR, FACILITÉ, et BGN
- Améliorations BGN. Mode NUL et par défaut.
- Accès local.
- Liste noire de parent. Liste d'exclusion.
- Individu guérissant avec AWPP.
- Transition d'Ethernets.
- Prise en charge de base de Voix de la release 4.0.
- Sélection dynamique de fréquence.
- Anti toronnage – Basculement par défaut BGN et DHCP.

Remarque: Ces caractéristiques ne seront pas prises en charge :

- Canal de sécurité publique 4.9 gigahertz
- Routage autour d'interférence
- Lecture de fond
- Accès universel
- Support de passerelle de groupe de travail

Logiciel d'intérieur de maille

Le logiciel d'intérieur de maille est une release spéciale car il se concentre sur les aps d'intérieur, particulièrement maille d'intérieur. Dans cette release, nous avons l'aps working d'intérieur dans le mode local et également dans le mode de passerelle. Certaines des caractéristiques qui sont disponibles dans la release de 4.1.171.0 ne sont pas mises en application dans cette release. Des améliorations ont été apportées à l'interface de ligne de commande (CLI), à l'interface utilisateur graphique (GUI – navigateur Web) et sur l'ordinateur d'état lui-même. L'objectif pour ces améliorations est d'obtenir des données de valeur de votre point de vue concernant ce produit nouveau et sa viabilité fonctionnelle.

Améliorations spécifiques de maille d'intérieur :

- **Environnement intérieur** – La maille d'intérieur est mise en application utilisant LAP1242s et LAP1131. Ceux-ci sont mis en application dans les environnements intérieurs où le câble Ethernet n'est pas disponible. L'implémentation est facile et plus rapide pour fournir une couverture Sans fil aux régions isolées dans le bâtiment (par exemple, la distribution au détail centre, formation pour des séminaires/conférences, fabrication, tourisme).
- **Jetez un pont sur les améliorations du nom de groupe (BGN)** – afin de permettre à un administrateur réseau pour organiser un réseau de la maille d'intérieur aps en secteurs spécifiés par utilisateur, Cisco fournit un mécanisme appelé le nom de groupe de Bridge, ou BGN. Le BGN, vraiment le nom de secteur, fait se connecter AP à d'autres aps au même BGN. En cas AP ne trouve aucun secteur approprié appariant son BGN, AP fonctionne en mode par défaut, et choisit le meilleur parent qui répond au par défaut BGN. Cette caractéristique a déjà reçu beaucoup d'appréciation du champ pendant qu'elle lutte contre les conditions échoués AP (si quelqu'un SIG-a configuré le BGN). Dans la version logicielle de 4.1.171.0, les aps, en utilisant le par défaut BGN, ne fonctionne pas comme noeud d'intérieur de maille et n'a aucun accès client. Il est dans le mode maintenance à accéder à par l'intermédiaire du contrôleur, et si l'administrateur ne répare pas le BGN, AP redémarrera après 30 minutes.
- **Améliorations de la sécurité** - La Sécurité sur le code d'intérieur de maille est par défaut configuré pour l'EAP (Extensible Authentication Protocol). Ceci est défini dans RFC3748. Bien que le protocole d'EAP ne soit pas limité aux réseaux locaux Sans fil et puisse être utilisé pour l'authentification de lan câblée, il est le plus employé souvent dans des réseaux locaux Sans fil. Quand l'EAP est appelé par un périphérique de NAS activé par 802.1X (serveur d'accès à distance) tel qu'un point d'accès sans fil du 802.11 a/b/g, les méthodes modernes d'EAP peuvent fournir un mécanisme d'authentification sécurisé et négocier un PMK sécurisé (pair-wise master key) entre le client et le NAS. Le PMK peut alors être utilisé pour la session de chiffrement sans fil qui utilise le cryptage TKIP ou CCMP (basé sur AES).Avant la version logicielle de 4.1.171.0, la maille extérieure aps a utilisé PMK/BMK pour joindre le contrôleur. C'était un processus de trois-cycle. Maintenant les cycles sont réduits pour une convergence plus rapide.Le but global de la Sécurité d'intérieur de maille est de fournir :Configuration zéro

de toucher pour la Sécurité de ravitaillement.Intimité et authentification pour des trames de données.Authentification mutuelle entre le réseau et les Noeuds.Capacité d'utiliser des méthodes standard d'EAP pour l'authentification des Noeuds d'intérieur de la maille AP.Découplage de LWAPP et de Sécurité d'intérieur de maille.La détection, le routage, et les mécanismes syncing sont améliorés de l'architecture en cours pour faciliter les éléments exigés pour prendre en charge les nouveaux protocoles de Sécurité.La maille d'intérieur aps découvrent l'autre maille aps en balayant et en écoutant les mises à jour voisines gratuites de l'autre maille aps. Tout le RAP ou cartes d'intérieur connectées au réseau annonce de principaux paramètres de Sécurité dans leurs trames NEIGH_UPD (tout comme des trames balise de 802.11).Une fois que cette phase est terminée, un lien logique entre une maille d'intérieur AP et l'AP racine est établi.

- **Améliorations WCS**Des alarmes d'intérieur de maille ont été ajoutées.Des états d'intérieur de maille peuvent être générés affichant le compte de saut, le plus mauvais SNR, etc.Le test de liaison (Parent-à-enfant, Enfant-à-parent) peut être exécuté entre les Noeuds qui affiche les informations très intelligentes.L'information affichée d'AP est beaucoup plus que la plus tôt.On a une option de visualiser également les voisins potentiels.La surveillance de la santé est améliorée et plus commode pour accéder à.

Matériel et logiciel pris en charge

Il y a une configuration matérielle minimale et un logiciel nécessaire pour la maille d'intérieur :

- Cisco LWAPP aps AIR-LAP1242AG-A-K9 et AIR-LAP1131AG-A-K9 prennent en charge la configuration d'intérieur de maille.
- Maille d'entreprise de supports logiciels de version 2 de maille de Cisco (Produits d'intérieur et extérieurs). Ceci peut être installé sur le contrôleur de Cisco, le Cisco 440x/210x, et le WISMs seulement.
- Le logiciel de version 2 de maille d'entreprise de Cisco peut être téléchargé de Cisco.com.

D'intérieur contre extérieur

Ce sont certaines des différences saillantes entre la maille d'intérieur et extérieure :

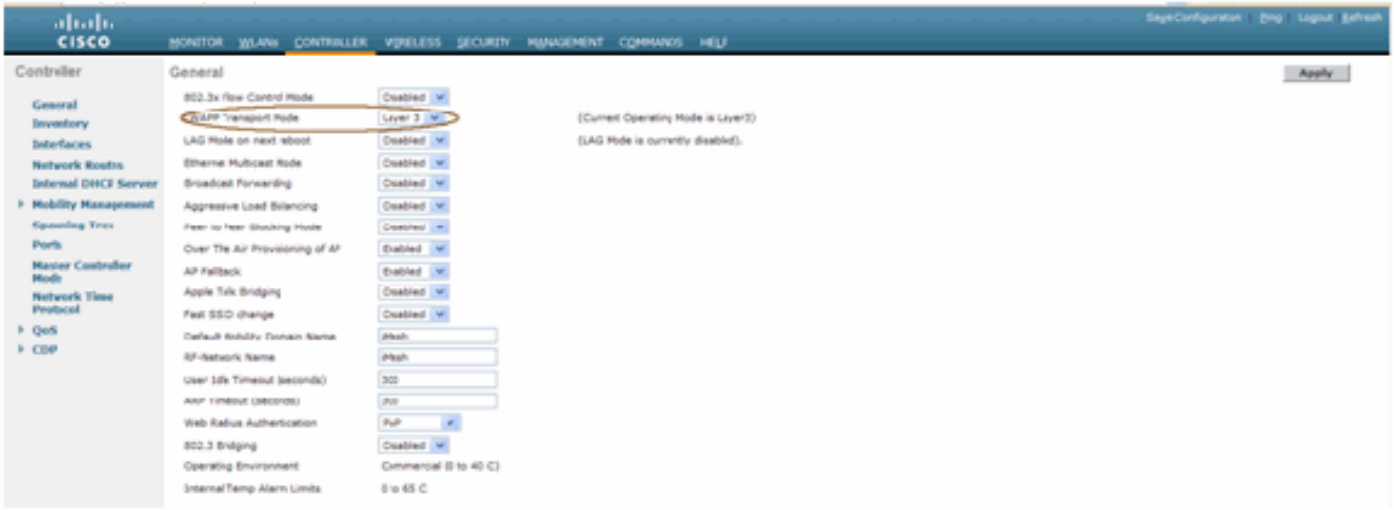
	Maille d'intérieur	Maille extérieure
Environnement	D'intérieur SEULEMENT, évalué d'intérieur de matériel	Extérieur SEULEMENT, matériel rocailleux
Matériel	AP d'intérieur utilisant LAP1242 et LAP1131AG	AP extérieur utilisant LAP15xx et LAP152x
Niveaux de puissance	2.4 Ghz:20dbm 5.8 Ghz:17dbm	2.4 Ghz:28dbm 5.8 Ghz:28dbm
Tailles de cellules	Approximativement 150ft	Approximativement 1000ft
Hauteur d'implémentation	12ft de la terre	30-40ft de la terre

Configuration

Veillez à passer en revue le guide complètement avant de commencer n'importe quelle implémentation, particulièrement si vous avez reçu le nouveau matériel.

Mode du contrôleur L3

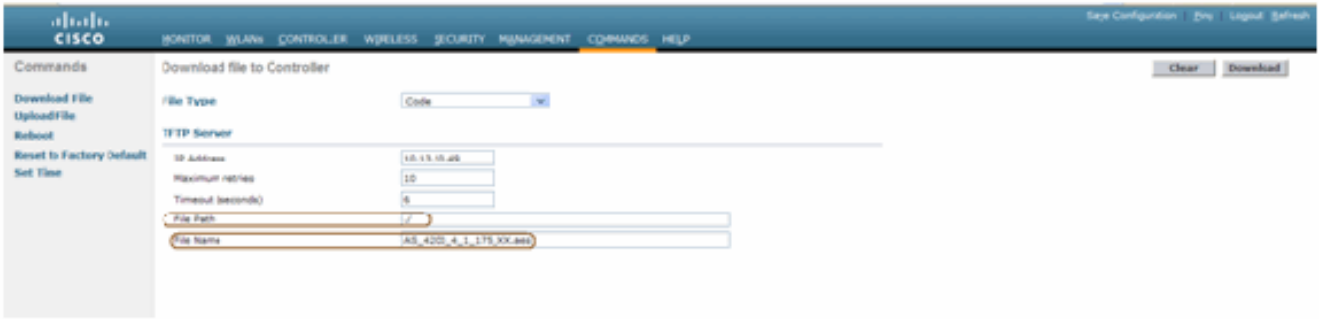
La maille d'intérieur aps peut être déployée comme réseau L3.



Améliorez le contrôleur au plus défunt code

Procédez comme suit :

1. Pour améliorer la version 2 de maille sur un réseau maillé d'intérieur, votre réseau doit s'exécuter sur 4.1.185.0 ou la maille Release1, disponible sur Cisco.com.
2. Téléchargez le dernier code pour le contrôleur à votre serveur TFTP. De l'interface gui de contrôleur, le clic **commande > fichier téléchargé**.
3. Sélectionnez le type de fichier comme **code** et donnez l'adresse IP de votre serveur TFTP. Définissez le chemin et le nom du fichier.



Remarque: Utilisez le serveur TFTP qui prend en charge plus de 32 transferts de taille de fichier de Mo. Par exemple, **tftpd32**. Sous le chemin de fichier mis **« . / »** comme affiché.

4. Si de finition en installant le nouveau micrologiciel, utilisez la commande de **show sysinfo** dans le CLI de 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...................................... 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
Number of WLANs.................................. 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 en charge pas des Downgrades pour des contrôleurs.

Adresse MAC

Il est obligatoire d'utiliser le filtrage MAC. Cette caractéristique a fait à Cisco la solution d'intérieur de maille comme vrai « toucher zéro. » À la différence des releases précédentes, le tamis à mailles n'aura plus l'option de filtrage MAC.

Remarque: Le filtrage MAC est activé par défaut.

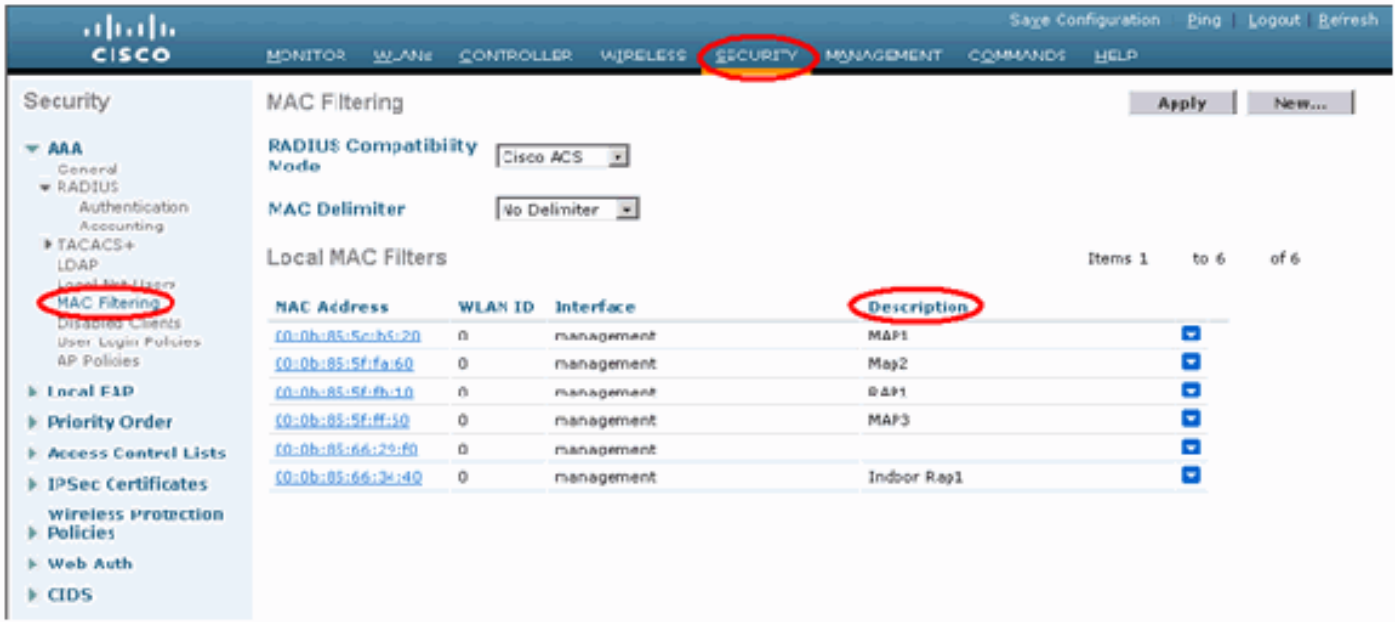
Enregistrez l'adresse MAC aux radios

Dans un fichier texte, enregistrez les adresses MAC de toute la maille d'intérieur AP vous transmet par radio se déploient dans votre réseau. L'adresse MAC peut être trouvée au dos des aps. Ceci vous aide pour le futur test, comme la plupart des commandes CLI exigent l'adresse MAC aps ou des noms soient écrits avec la commande. Vous pouvez également changer le nom des aps à quelque chose plus facilement retrouvée, comme, « type de construction de la nombre-zone nombre-AP : quatre derniers caractères hexadécimaux d'adresse MAC. »

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

Le contrôleur de Cisco met à jour une liste d'intérieur d'adresse MAC d'autorisation AP. Le contrôleur répond seulement aux demandes de détection des radios d'intérieur qui apparaissent sur la liste d'autorisation. Introduisez les adresses MAC de toutes les radios que vous tendez à utiliser dans votre réseau sur le contrôleur.

Sur l'interface gui de contrôleur, allez à la **Sécurité**, et cliquez sur en fonction le **filtrage MAC** du côté gauche de l'écran. Cliquez sur New afin d'introduire les adresses MAC comme affiché ici :



En outre, écrivez les noms des radios pour la commodité sous la description de **description** (telle que l'emplacement, l'AP #, etc.) peut également être utilisé pour où les radios ont été installées pour une consultation plus facile n'importe quand.

Filtrage MAC d'enable

Le filtrage MAC est activé par défaut.

On peut également faire un choix de la security mode comme EAP ou PSK sur la même page.

De l'interface gui du commutateur, utilisez ce chemin :

Chemin d'interface gui : **Radio > maille d'intérieur**

La security mode peut SEULEMENT être vérifiée le CLI par 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-- or (q)uit
Web Auth Redirect Ports ..................... 80
Fast SSID Change ............................ Disabled
802.3 Bridging .............................. Disable
```

Déploiement d'intérieur de la maille L3

Pour un réseau maillé L3 d'intérieur, configurez les adresses IP pour les radios si vous n'avez pas l'intention d'utiliser le serveur DHCP (interne ou externe).

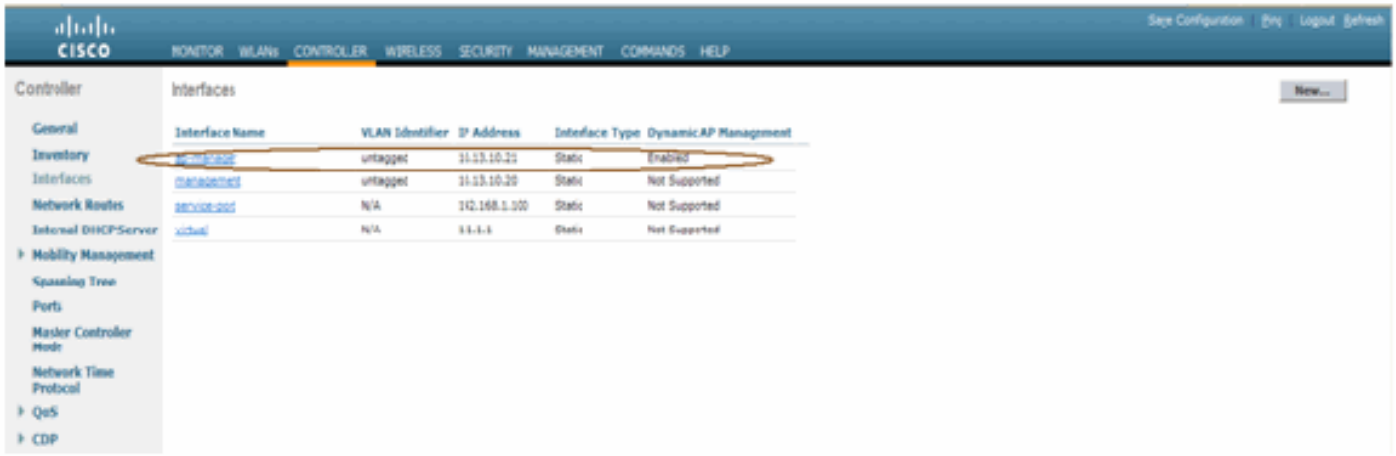
Pour un réseau maillé L3 d'intérieur, si vous voulez utiliser le serveur DHCP, configurez le contrôleur en mode L3. Sauvegardez la configuration et redémarrez le contrôleur. Veillez-vous pour configurer l'option 43 sur le serveur DHCP. Après que le contrôleur ait redémarré, les aps nouvellement connectés recevront leur adresse IP du serveur DHCP.

Définissez les interfaces sur le contrôleur

Gestionnaire AP

Pour un déploiement L3, vous devez définir l'AP-**gestionnaire**. Le gestionnaire AP agit en tant qu'adresse IP source pour la transmission du contrôleur aux aps.

Chemin : **Le Controller > Interfaces** > l'AP-**gestionnaire** > **éditent**.



L'interface d'AP-**gestionnaire** devrait être assignée une adresse IP dans le même sous-réseau et le VLAN que votre interface de gestion.

Rôles par radio

Il y a deux rôles par radio primaires possibles avec cette solution :

- Point d'accès de racine (RAP) - La radio à laquelle vous voulez se connecter au contrôleur (par l'intermédiaire du commutateur) jouera le rôle d'un RAP. Les coups secs et durs ont une connexion de câble et LWAPP-activée au contrôleur. Un RAP est un noeud de parent à n'importe quelle transition ou réseau maillé d'intérieur. Un contrôleur peut avoir un ou plusieurs le RAP, chacun parenting la même chose ou les différents réseaux Sans fil. Il peut y avoir plus d'un RAP pour le même réseau maillé d'intérieur pour la Redondance.
- Point d'accès d'intérieur de maille (MAP) - La radio qui n'a aucune connexion câblée au contrôleur joue le rôle d'une maille d'intérieur AP. Cet AP s'est autrefois appelé le dessus AP de Polonais. Les cartes ont une connexion Sans fil (par l'interface de liaison) peut-être à d'autres cartes et finalement à un RAP et ainsi au contrôleur. Les cartes peuvent également avoir une connexion d'Ethernets câblés à un RÉSEAU LOCAL et servir de point final de passerelle à ce RÉSEAU LOCAL (utilisant une connexion de P2P ou P2MP). Ceci peut se produire simultanément, si configuré correctement comme pont Ethernet. Clients de service de cartes sur la bande non utilisée pour l'interface de liaison.

Le mode par défaut pour AP est MAP.

Remarque: Les rôles par radio peuvent être placés par l'intermédiaire du GUI ou du CLI. Les aps redémarreront après que la modification de rôle.

Remarque: Vous pouvez utiliser le contrôleur CLI pour préconfigurer les rôles par radio sur AP avez fourni AP est physiquement connecté au commutateur ou vous pouvez voir AP sur le commutateur comme 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 de groupe de passerelle

Jetez un pont sur les noms de groupe (BGN) contrôle l'association des aps. BGNs peut logiquement grouper les radios pour éviter deux réseaux sur le même canal de la communication les uns avec les autres. Cette configuration est également utile si vous avez plus d'un RAP dans votre réseau dans le même secteur (zone). Le BGN est une chaîne de dix caractères maximum.

Un nom de groupe prémonté de passerelle est assigné à l'étape de fabrication (VALEUR NULLE). Il n'est pas visible à vous. En conséquence, même sans BGN défini, les radios peuvent encore joindre le réseau. Si vous avez deux coups secs et durs dans votre réseau dans le même secteur (pour plus de capacité), il est recommandé que vous configurez les deux coups secs et durs avec le même BGN, mais sur des différents canaux.

Remarque: Le nom de groupe de passerelle peut être placé du contrôleur CLI et GUI.

```
(Cisco Controller) >config ap bridgegroupname set ?

<bridgegroupname> Set bridgegroupname on Cisco AP.
```

Après avoir configuré le BGN, AP remettra à l'état initial.

Remarque: Le BGN devrait être configuré très soigneusement sur un réseau vivant. Vous devriez toujours commencer à partir du noeud le plus lointain (dernier noeud) et se déplacer vers le RAP. La raison est que si vous commencez configurer le BGN quelque part au milieu du de multi-alimentation, alors les Noeuds au delà de ce point seront abandonnés en tant que ces Noeuds auront un BGN différent (vieux BGN).

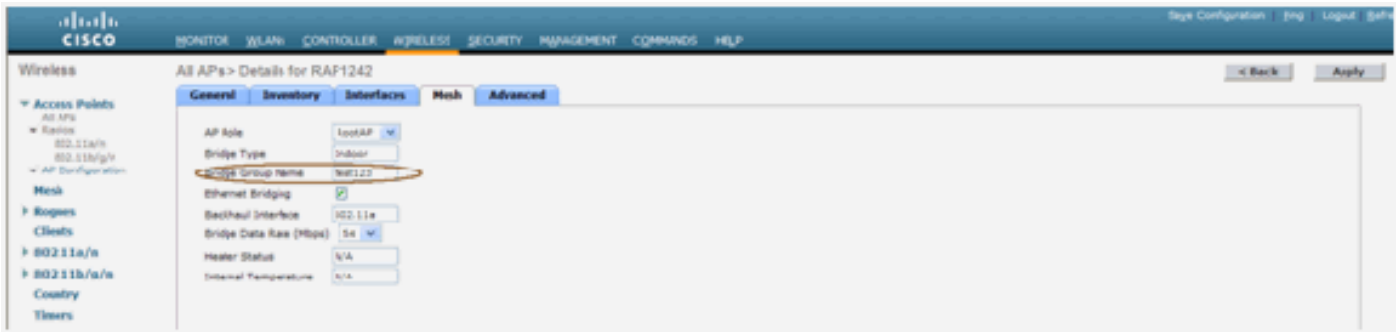
Vous pouvez vérifier le BGN en émettant cette commande CLI :

(Cisco Controller) **> show ap config general** *<apname>*

```
(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:-AB    802.11a:-AB
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
```

En outre, vous pouvez configurer ou vérifier le BGN utilisant le GUI de contrôleur :

Chemin : **Radio > All APs > Details**.



Vous pouvez voir que l'information sur l'environnement d'AP est également affichée avec cette nouvelle release.

Configuration de la sécurité

La security mode d'intérieur par défaut de maille est EAP. Ceci signifie qu'à moins que vous configuriez ces paramètres sur votre contrôleur, vos cartes ne se joindront pas :

Configuration d'intérieur CLI d'EAP de maille

```
(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 dans le mode PSK, utilisez cette commande de retourner 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 d'intérieur d'EAP de maille

Dans le mode d'EAP, vous pouvez vérifier ces **commandes show** de vérifier l'authentification de 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 .............................. 436973636f0000000000000000000000
      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 d'intérieur d'EAP de maille

Afin de mettre au point tous les problèmes de mode d'EAP, utilisez ces commandes dans le contrôleur :

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

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

Installation

Conditions préalables

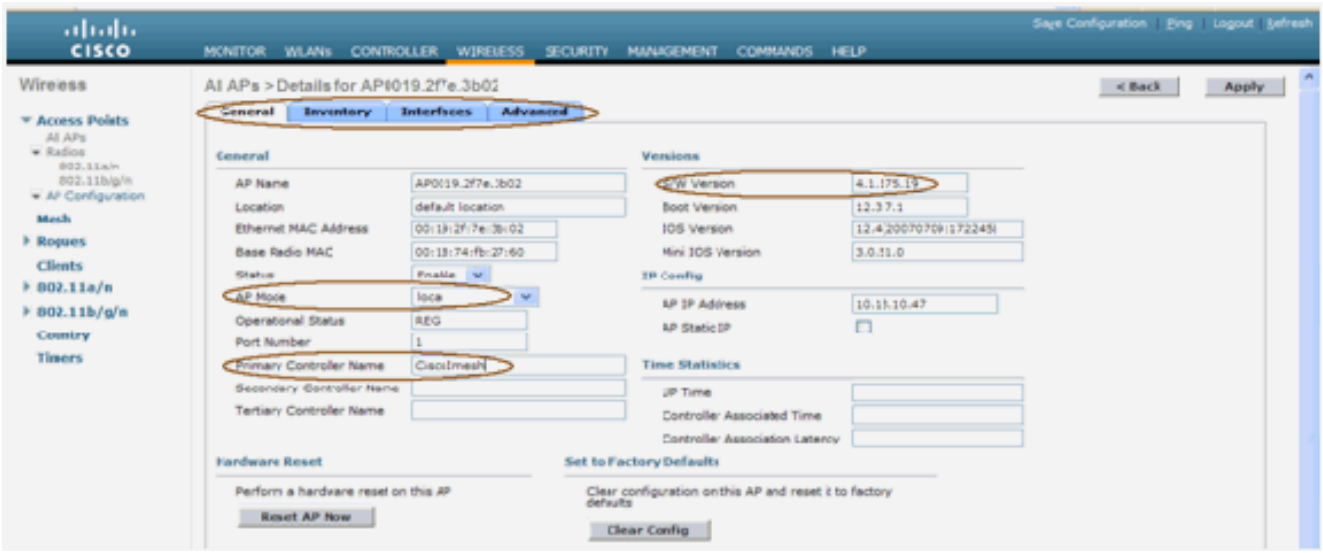
Le contrôleur doit exécuter la version recommandée du code. To cliquer sur Monitor pour vérifier la version de logiciel. Les mêmes peuvent être vérifiés par l'intermédiaire du CLI.

```
(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
Number of WLANs.................................. 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
```

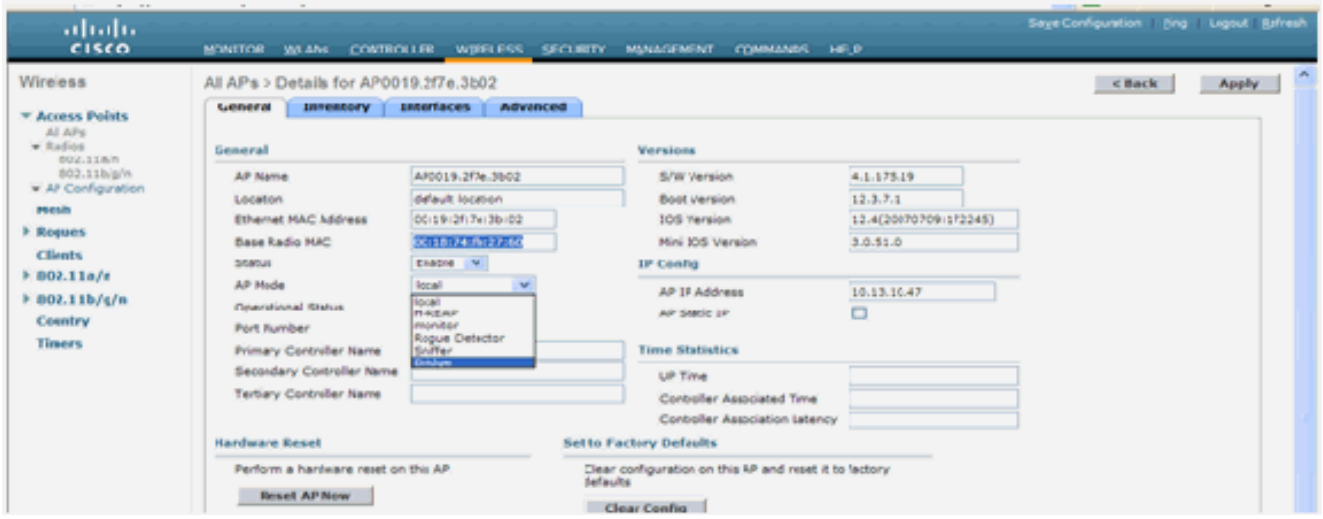
Les systèmes comme le serveur DHCP, le serveur ACS, et le serveur WCS devraient être accessibles.

Installation

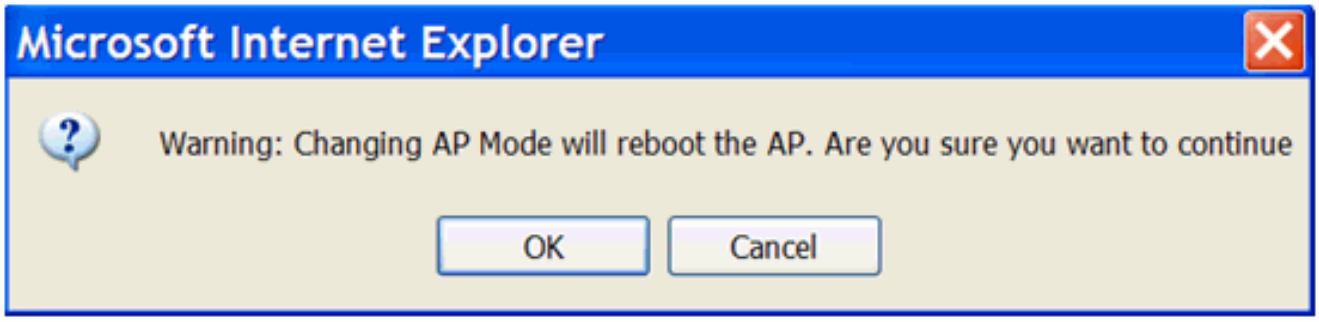
1. Connectez tous les recouvrements (1131AG/1242AG) à un réseau de la couche 3 sur le même sous-réseau que l'adresse IP de Gestion. Tous les aps joindront le contrôleur comme aps en mode local. En ce mode, amorcez les aps avec le nom primaire de contrôleur, le nom secondaire de contrôleur, et un nom tertiaire de contrôleur.



2. Capturez l'adresse MAC par radio de base d'AP (par exemple, 00:18:74 : FB : 27:60).
3. Ajoutez l'adresse MAC d'AP pour AP pour s'associer au mode de passerelle.
4. Cliquez sur Security **> filtrage MAC > nouveau**.
5. Ajoutez l'adresse MAC copiée, et nommez les aps dans la liste de filtre d'adresses MAC et la liste AP.
6. Choisissez la **passerelle de la** liste de **mode AP**.



7. Il vous incitera à confirmer car ceci redémarrera AP.



8. AP redémarrera et joindra le contrôleur en mode de passerelle. La nouvelle fenêtre AP aura un onglet supplémentaire : MAILLE. Cliquez sur l'onglet de **MAILLE** pour vérifier le rôle, le type de passerelle, le nom de groupe de passerelle, les Ethernets jetant un pont sur, l'interface arrière de transport, le débit de données de passerelle, etc.

9. Dans cette fenêtre, accédez à la liste de rôle AP et choisissez le rôle approprié. Dans ce cas, le rôle par défaut est une MAP.Le nom de groupe de passerelle est vide par défaut.L'interface arrière de transport est 802.11a.Le débit de données de passerelle (c'est-à-dire, débit de données arrière de transport) est 24Mbps.
10. Connectez AP que vous voulez comme RAP au contrôleur. Déployez les radios (cartes) aux emplacements désirés. Branchez 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 champ de vision entre les Noeuds. Si les états de champ de vision n'existent pas, créez les espaces de zone de Fresnel pour obtenir des états de proche-ligne-de-site.
12. Si vous avez plus d'un contrôleur connecté au même réseau maillé d'intérieur, alors vous devez spécifier le nom du contrôleur primaire sur chaque noeud. Autrement, le contrôleur qui est premier vu sera pris en tant que primaire.

Alimentation et configuration de la Manche

Le canal de liaison peut être configuré sur un RAP. Les cartes accorderont au canal RAP. L'accès local peut être configuré indépendamment pour des cartes.

Du GUI de commutateur, suivez le chemin : **La radio** > la **radio 802.11a** > **configurent**.

Remarque: Le niveau de puissance par défaut de Tx sur la liaison est le niveau de puissance le plus élevé (le niveau 1) et le Gestion des ressources radio (RRM) est éteint par défaut.

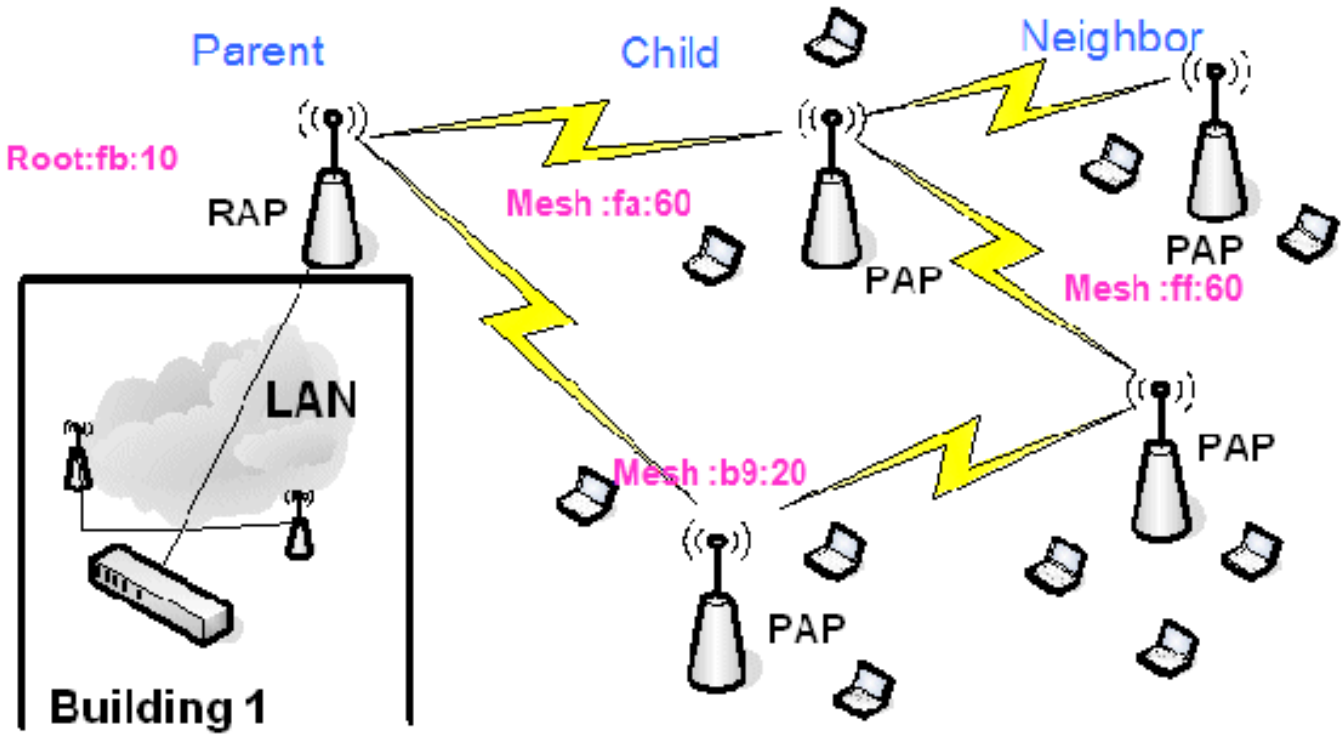
Si vous colloquez des coups secs et durs, nous vous recommandons les canaux adjacents alternatifs d'utilisation sur chaque RAP. Ceci réduira l'interférence de co-canal.

Contrôle rf

Dans un réseau maillé d'intérieur nous devons vérifier le rapport parent-enfant entre les Noeuds. **Le saut** est une liaison sans fil entre les deux radios. Le rapport parent-enfant change pendant que vous voyagez par le réseau. Il dépend d'où vous êtes dans le réseau maillé d'intérieur.

La radio plus près du contrôleur dans une connexion Sans fil (saut) est un **parent de la** radio de l'autre côté du saut. Dans un plusieurs système de saut il y a une structure d'arborescence-type 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 ultérieurs dans le deuxième saut sont en avant les **voisins** pour ce parent particulier.

Figure 1 : Réseau de deux sauts



Dans la figure 1, des noms AP sont mentionnés pour la commodité. Dans le tir d'écran suivant, le **RAP(fb:10)** est étudié. Ce noeud peut voir (dans le déploiement réel) la maille d'intérieur aps **(fa:60 et b9:20)** comme enfants et **TRACER ff:60 comme voisin**.

De l'interface gui de commutateur, suivez le chemin : **Radio > tout aps > Rap1 > informations sur les voisins**.

Assurez-vous que des relations de Parent-enfant sont établies et mises à jour correctement pour votre réseau maillé d'intérieur.

Vérifiez les interconnexions

la maille d'exposition est une commande instructive de vérifier l'interconnectivité dans votre réseau.

Vous devez donner ces instructions à chaque noeud (AP) utilisant le contrôleur CLI, et téléchargez les résultats dans Word ou le fichier texte au site le téléchargeant.

```
(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 d'intérieur, choisissez un plusieurs lien de saut et émettez ces commandes à partir du RAP. Téléchargez le résultat des commandes au site le téléchargeant.

Dans la section suivante, toutes ces commandes ont été émises pour le réseau représenté d'intérieur de maille de deux sauts dans la figure 1.

Affichez le chemin d'intérieur de maille

Cette commande t'affichera les adresses MAC, les rôles par radio des Noeuds, les rapports de signal-bruit dans les dBs pour la liaison ascendante/liaison descendante (SNRUp, SNRDown), et le lien SNR dans le 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.
```

Affichez le résumé d'intérieur de voisin de maille

Cette commande t'affichera les adresses MAC, les rapports parent-enfant, et la liaison ascendante/liaison descendante SNR dans le 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
```

Àcette heure, vous devriez pouvoir voir les relations entre les Noeuds de votre réseau et vérifier la Connectivité rf en voyant les valeurs SNR pour chaque lien.

Sécurité d'Access de console AP

Cette caractéristique donne la sécurité optimisée à l'accès de console d'AP. Un câble de console pour AP est exigé pour utiliser cette caractéristique.

Ceux-ci sont pris en charge :

- Un CLI pour pousser la combinaison d'user-id/mot de passe à AP 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 de pousser la combinaison de nom d'utilisateur/mot de passe à tous les aps enregistrés au contrôleur :

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

Avec ces commandes, la combinaison d'ID utilisateur/mot de passe poussée du contrôleur est persistante à travers la recharge sur les aps. Si AP est effacé du contrôleur, il n'y a aucun mode d'accès sécurisé. AP génère un déroutement SNMP avec une procédure de connexion réussie. AP génèrera également un déroutement SNMP sur une panne d'ouverture de session de console pendant trois fois consécutives.

Transition d'Ethernets

Pour des raisons de sécurité, le port Ethernet sur les cartes est désactivé par défaut. Il peut être activé seulement en configurant des Ethernets jetant un pont sur sur le RAP et les cartes respectives.

En conséquence, la transition d'Ethernets doit être activée pour deux scénarios :

- Quand vous voulez utiliser le d'intérieur engrenez les Noeuds comme passerelles.
- Quand vous voulez connecter n'importe quel périphérique Ethernet (tel que PC/ordinateur portable, caméra vidéo etc.) sur la MAP utilisant son port Ethernet.

Chemin : **Radio** > clic tout AP > **maille**.

Il y a une commande CLI qui peut être utilisée pour configurer la distance entre les Noeuds faisant la transition. Essayez connecter un périphérique Ethernet comme une caméra vidéo à chaque saut et voyez la représentation.

Amélioration de nom de groupe de passerelle

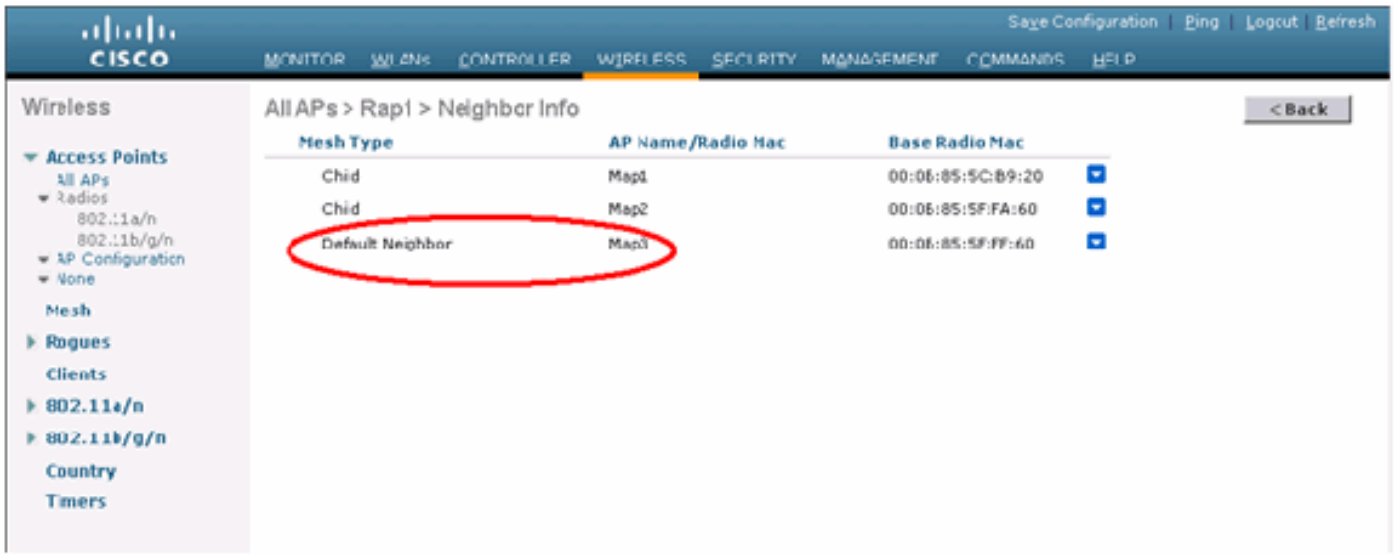
Il est possible qu'AP provisioned incorrectement avec un « bridgegroupname » pour ce qu'on n'a pas destiné le. Selon la conception de réseaux, cet AP peut ou peut ne pas pouvoir atteindre et trouver son secteur/arborescence corrects. S'il ne peut pas atteindre un secteur compatible, il peut devenir échoué.

Afin de récupérer un AP si échoué, le concept du bridgegroupname « par défaut » a été introduit avec le code 3.2.xx.x. L'idée de base est qu'AP qui ne peut pas se connecter à n'importe quel autre AP à son bridgegroupname configuré, tente de se connecter au « par défaut » (le mot) comme bridgegroupname. Tous les Noeuds exécutant 3.2.xx.x et logiciel postérieur reçoivent d'autres Noeuds avec ce bridgegroupname.

Cette caractéristique peut également aider en ajoutant un nouveau noeud ou un noeud configuré faux à un réseau courant.

Si vous avez un réseau courant, prenez AP préconfiguré avec un BGN différent et faites-le joindre le réseau. Vous verrez cet AP dans le contrôleur utilisant le « par défaut » BGN après que vous ajoutiez 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
```



AP utilisant le par défaut BGN peut agir en tant que maille d'intérieur normale AP associant des clients et formant des relations d'intérieur d'enfant de parent de maille.

Le moment où cet AP utilisant le par défaut BGN trouve un autre parent avec le BGN correct, il commutera à lui.

Se connecte - Messages, système, AP, et déroutement

Journaux des messages

Activez le niveau d'enregistrement pour des journaux des messages. Du contrôleur CLI, émettez 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 voir des journaux des messages, émettez cette commande du contrôleur CLI :

```
(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_tmr.c 501: Did not receive hearbeat 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 de contrôleur :

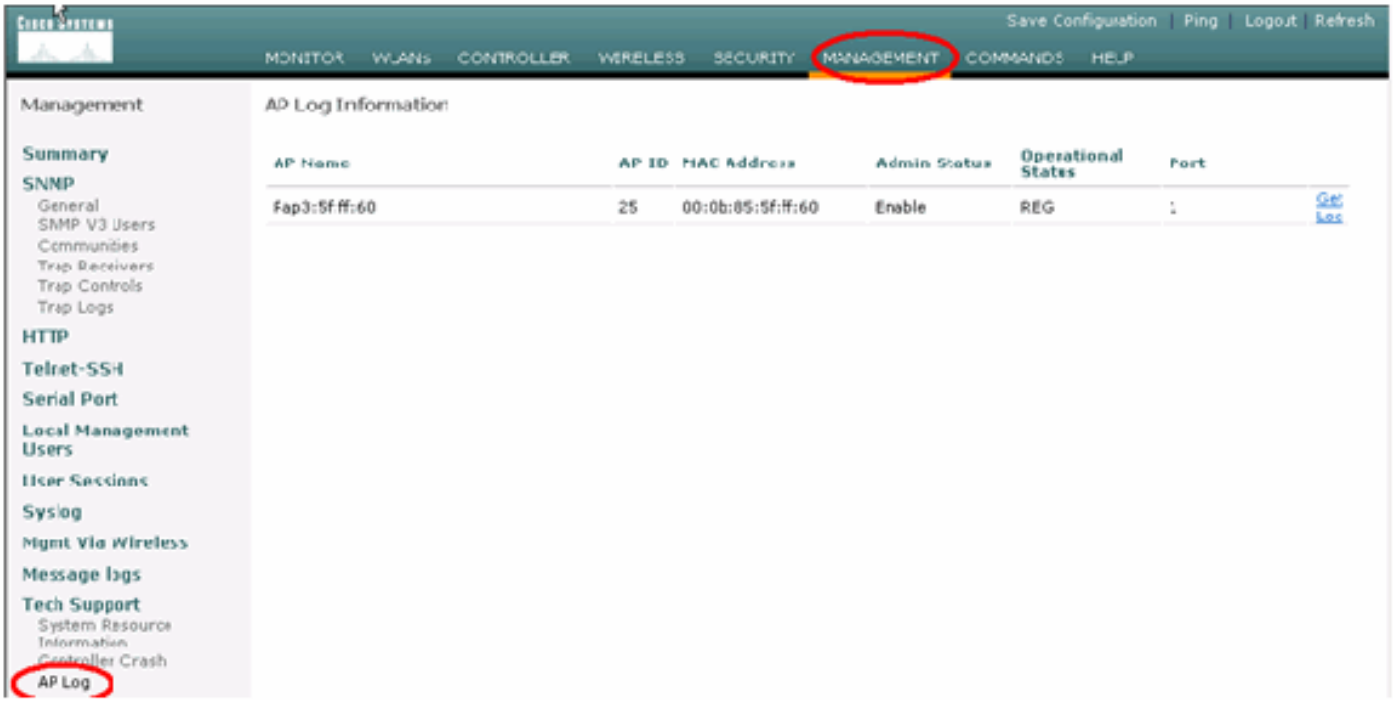
1. **Commandes > téléchargement de**
   clic.

2. Écrivez vos informations du serveur TFTP. Cette page te donnera de diverses options de télécharger, et vous voulez que ces fichiers soient envoyés :Journal des messagesJournal d'événementsLog de déroutementFichier de crash (le cas échéant)Afin de vérifier des

fichiers de crash, **Gestion de** clic **> crash de contrôleur**.

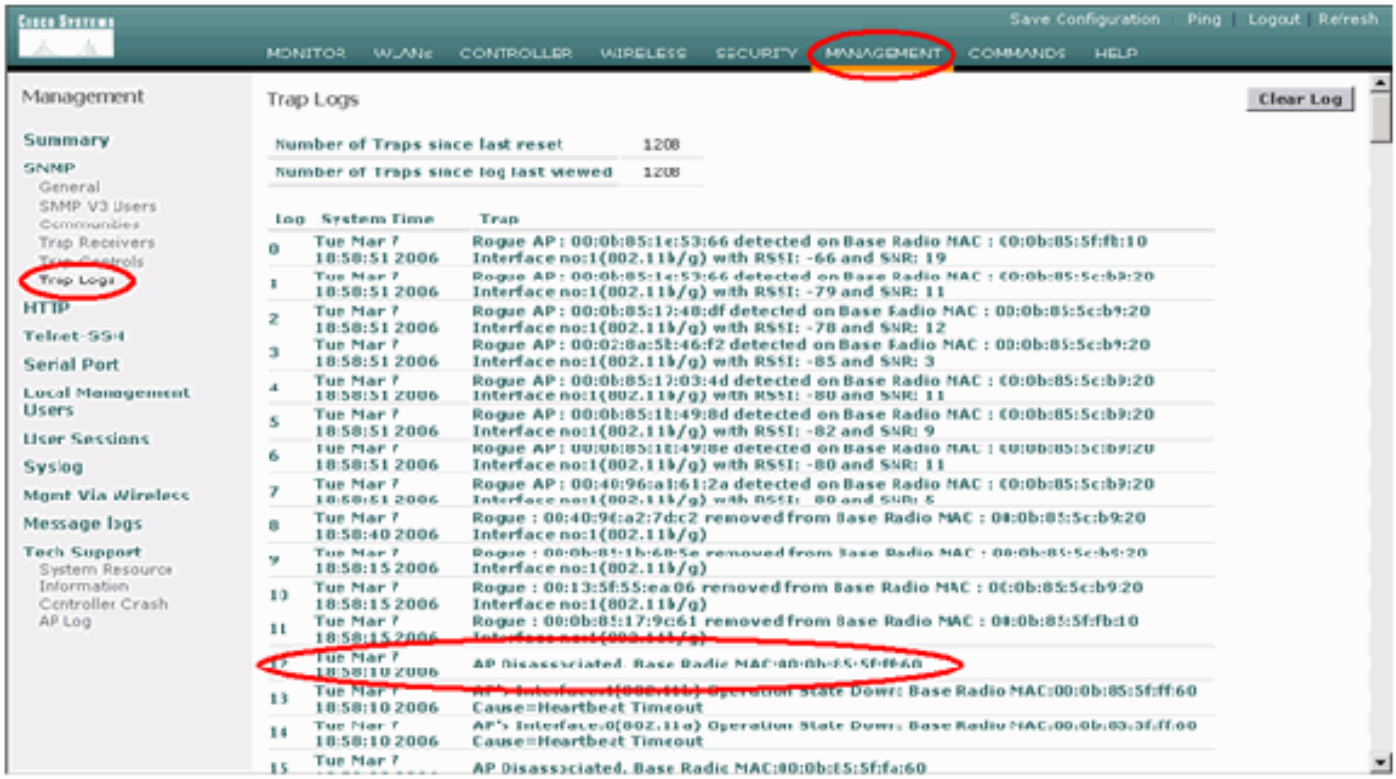
Logs AP

Allez à cette page GUI sur le contrôleur vérifier les logs AP pour vos gens du pays AP éventuel :



Logs de déroutement

Allez à cette page GUI du contrôleur et vérifiez les logs de déroutement :



Représentation

Test de convergence de démarrage

La convergence est le temps pris par un RAP/MAP pour établir une connexion stable LWAPP avec un contrôleur WLAN à partir du moment où elle a initialisé la première fois comme répertorié ici :

Test de convergence	Temps de convergence (minute : sec)			
	RAP	MAP1	MAP2	MAP3
Mise à niveau d'image	2:34	3:50	5:11	6:38
Réinitialisation de contrôleur	0:38	0:57	1:12	1:32
Mettez sous tension le réseau maillé d'intérieur	2:44	3:57	5:04	6:09
Réinitialisation RAP	2:43	3:57	5:04	6:09
La MAP re-se joignent		3:58	5:14	6:25
Modification de MAP de parent (le même canal)		0:38		

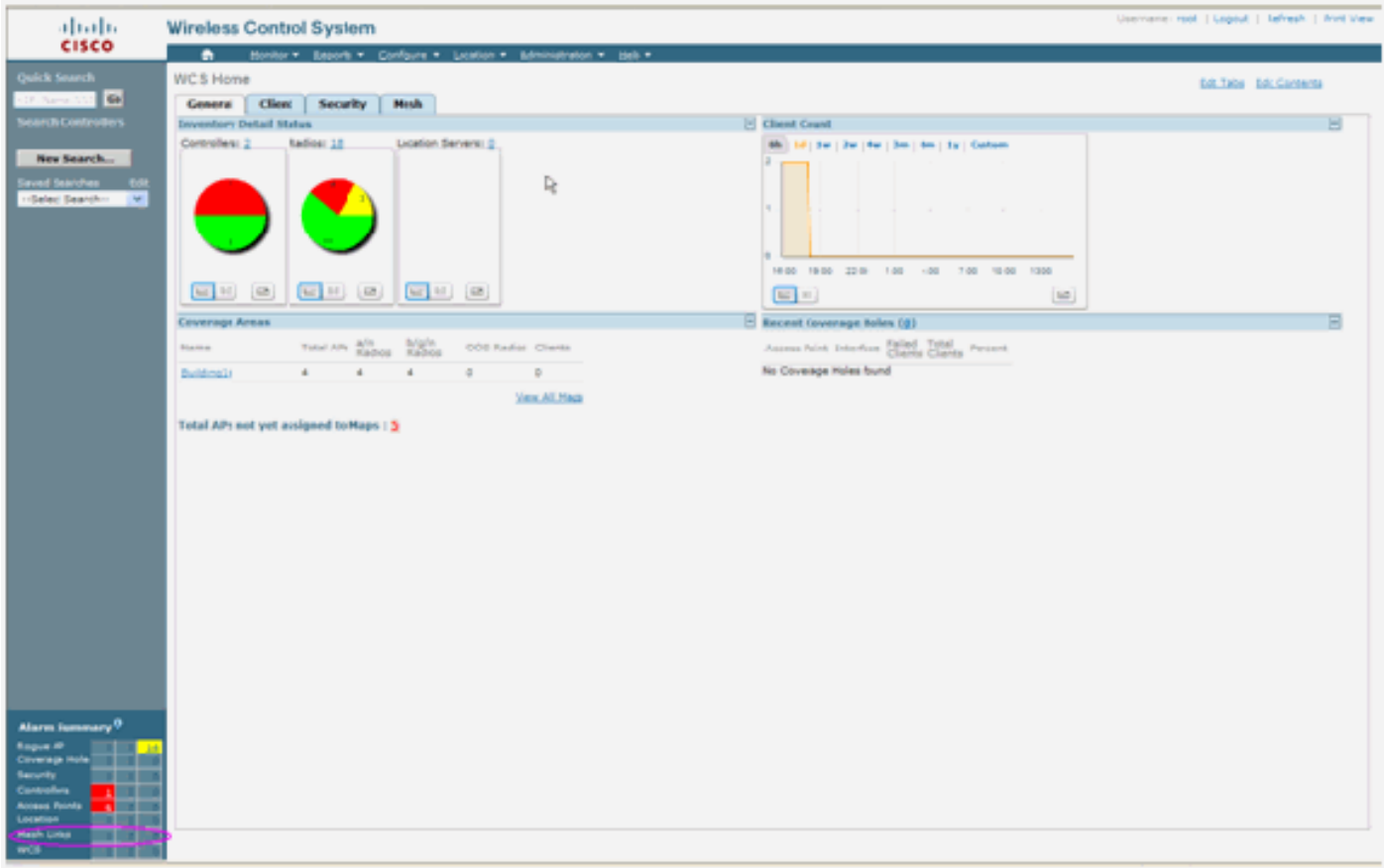
WCS

Alarmes d'intérieur de maille

WCS génèrera ces alarmes et événements liés au réseau maillé d'intérieur basé sur les déroutements du contrôleur :

- Lien SNR de pauvres
- Parent changé
- Enfant déplacé
- La MAP change le parent fréquemment
- Événement de port de console
- Panne d'autorisation de MAC
- Échecs d'authentification
- L'enfant a exclu le parent

Liens de maille de clic. Il affichera toutes les alarmes liées aux liens d'intérieur de maille.



Ces alarmes s'appliquent aux liens d'intérieur de maille :

- Lien SNR de pauvres - Cette alarme est générée si le lien SNR tombe ci-dessous 12db. L'utilisateur ne peut pas changer ce seuil. Si le SNR pauvre est détecté sur le lien de liaison pour l'enfant/parent, le déroutement sera généré. Le déroutement contiendra la valeur SNR et les adresses MAC. La sévérité d'alarme est principale. Le rapport (signal/bruit) SNR est important parce que la haute force du signal n'est pas assez pour assurer la bonne représentation de récepteur. Le signal en entrée doit être plus fort que n'importe quel bruit ou interférence qui est présente. Par exemple, il est possible d'avoir la haute force du signal et d'avoir toujours la performance sans fil pauvre s'il y a interférence forte ou un niveau sonore élevé.
- Parent changé - Cette alarme est générée quand l'enfant s'est déplacé à un autre parent. Quand le parent est perdu, l'enfant se joindra à un autre parent, et l'enfant enverra un déroutement contenant des adresses MAC de vieux parent et de nouveau parent à WCS. Sévérité d'alarme : Informationnel.
- Enfant déplacé - Cette alarme est générée quand WCS obtient un déroutement perdu par enfant. Quand le parent AP a détecté sa perte d'un enfant et non capable communiquer avec

cet enfant, il enverra un déroutement perdu par enfant à WCS. Le déroutement contiendra l'adresse MAC d'enfant. Sévérité d'alarme : Informationnel.
- Parent de MAP changé fréquemment - Cette alarme est générée si la maille d'intérieur AP change son parent fréquemment. Quand le parent-modification-compteur de MAP dépasse le seuil dans une durée donnée, il enverra un déroutement à WCS. Le déroutement contiendra le nombre de fois des modifications de MAP et la durée du temps. Par exemple, s'il y a 5 modifications dans un délai de 2 minutes, puis le déroutement sera envoyé. Sévérité d'alarme : Informationnel.
- L'enfant a exclu le parent - Cette alarme est générée quand un enfant a mis un parent sur la liste noire. Un enfant peut mettre un parent sur la liste noire quand l'enfant n'a pas authentifié au contrôleur après un nombre fixe de tentatives. L'enfant se souvient le parent mis sur la liste noire et quand l'enfant joint le réseau, il enverra le déroutement qui contient l'adresse MAC mise sur la liste noire de parent et la durée de la période de liste noire.

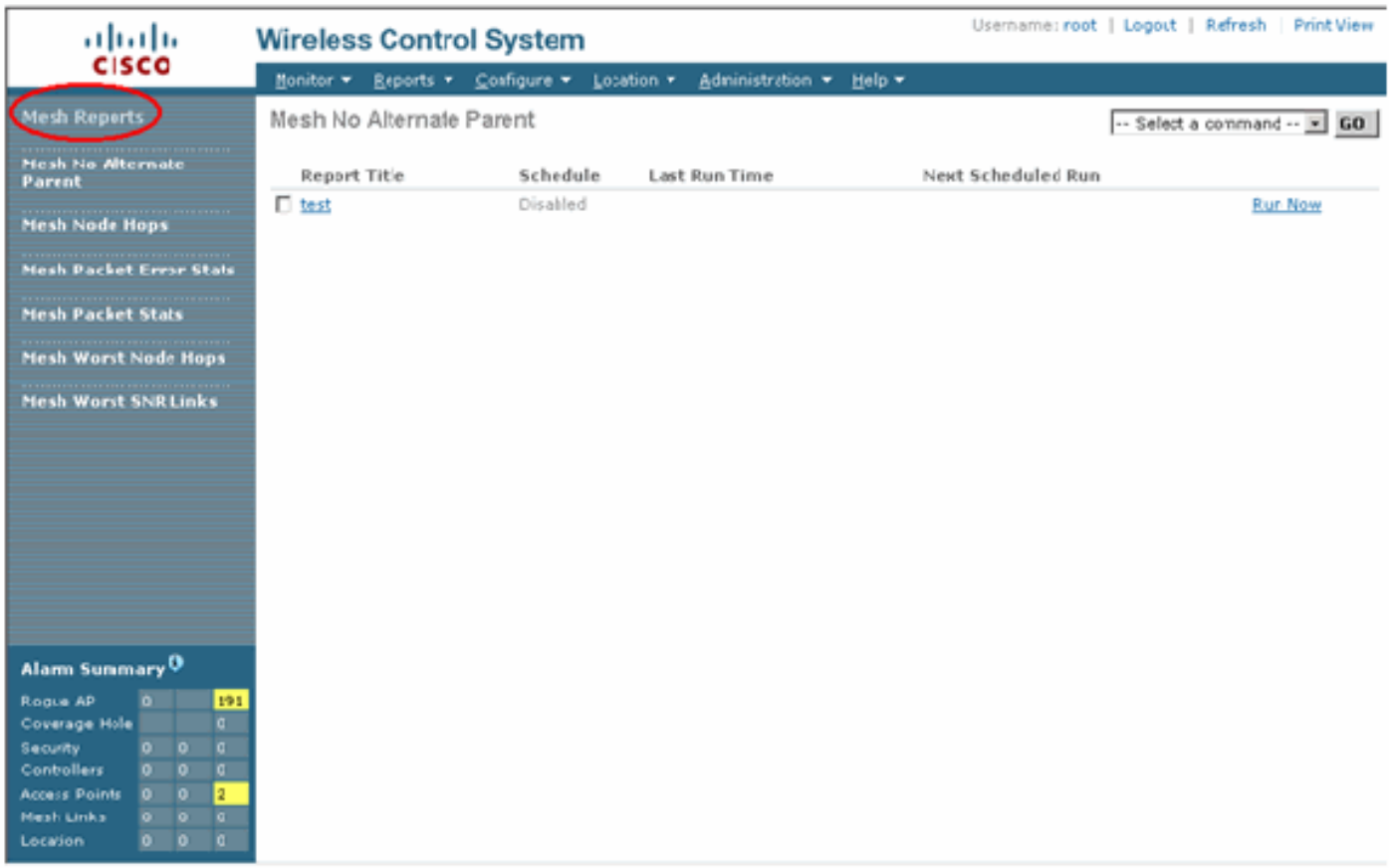
Alarmes autres que les liens d'intérieur de maille :

- Port de console Access - Le port de console fournit la capacité pour que le client change le nom d'utilisateur et le mot de passe pour récupérer AP extérieur échoué. Cependant, pour empêcher n'importe quel accès client autorisé à AP, WCS doit envoyer une alarme quand quelqu'un des essais pour ouvrir une session. Cette alarme est exigée pour assurer la protection car AP est physiquement vulnérable tandis que localisé dehors. Cette alarme sera générée si l'utilisateur a avec succès ouvert une session au port de console AP, ou s'il a manqué trois fois consécutives.
- Panne d'autorisation de MAC - Cette alarme est générée quand les essais AP pour joindre la maille d'intérieur mais n'authentifie pas parce qu'elle n'est pas dans la liste de filtre d'adresses MAC. WCS recevra un déroutement du contrôleur. Le déroutement contiendra l'adresse MAC d'AP qui autorisation défaillante.

État et statistiques de maille

Nous reportons le cadre amélioré d'état et de statistiques de 4.1.185.0 :

- Aucune voie de déroutement
- Sauts de noeud de maille
- Stats d'erreur de paquets
- Stats de paquet
- Le saut de noeud le plus gâté
- Les plus mauvais liens SNR



Aucune voie de déroutement

La maille d'intérieur AP a typiquement plus d'un voisin. Dans le cas qu'une maille d'intérieur AP desserre son lien de parent, AP devrait pouvoir trouver le parent alternatif. Dans un certain cas, s'il n'y a aucun voisin affiché, puis AP ne pourra pas n'aller à aucun autre parent s'il desserre ses parents. Il est essentiel que l'utilisateur sache quels aps n'ont pas les parents alternatifs. Listes de cet état tous les aps qui n'ont aucun autre voisin autres que le parent en cours.

Sauts d'intérieur de noeud de maille

Cet état affiche le nombre de sauts à partir de l'AP racine (RAP). Vous pouvez créer l'état basé sur ces critères :

- AP par le contrôleur
- AP par le plancher

Débits d'erreur de paquets

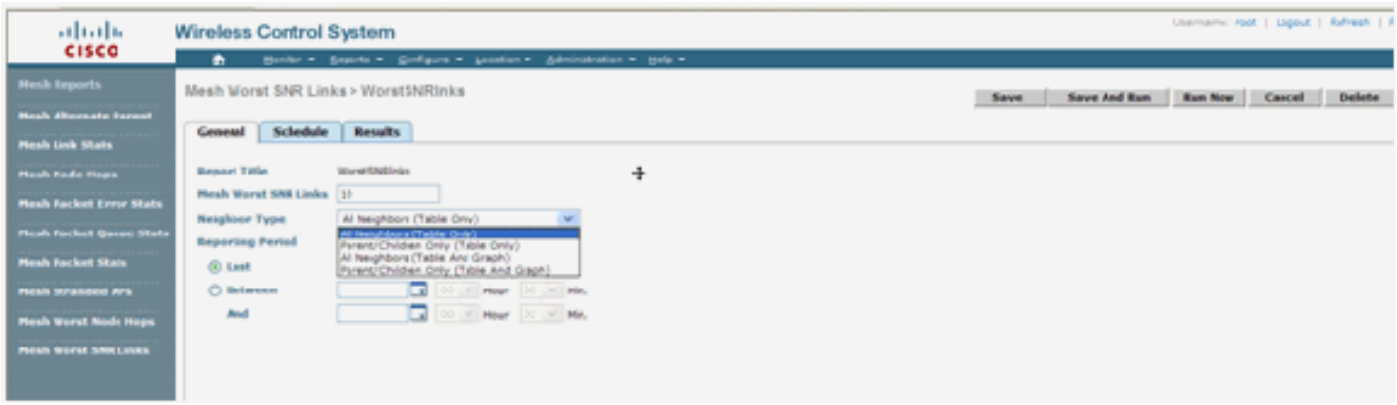
Les erreurs de paquets mettent en boîte sont provoqué par par interférence et pertes de paquets. Le calcul de débit d'erreur de paquets est basé sur des paquets envoyés et des paquets avec succès envoyés. Le débit d'erreur de paquets est mesuré sur le lien de liaison et est collecté pour les voisins et le parent. AP envoie périodiquement les informations de paquet au contrôleur. Dès que le parent changera, AP envoie les informations d'erreur de paquets collectées au contrôleur. WCS vote les informations d'erreur de paquets du contrôleur toutes les 10 minutes par défaut et les enregistre dans la base de données pendant jusqu'à 7 jours. Dans WCS, le débit d'erreur de paquets est affiché comme graphique. Le graphique d'erreur de paquets est basé sur les données historiques enregistrées dans la base de données.

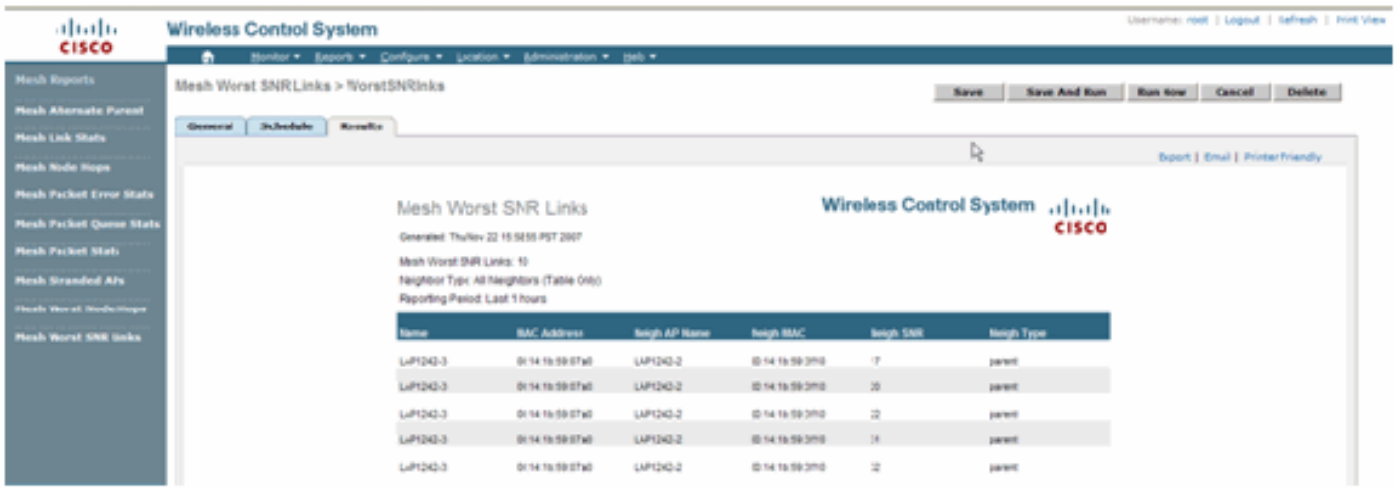
Stats de paquet

Cet état affiche que les valeurs du compteur du total voisin transmettent des paquets et des paquets totaux voisins avec succès transmis. Vous pouvez créer l'état basé sur certains critères.

Les plus mauvais liens SNR

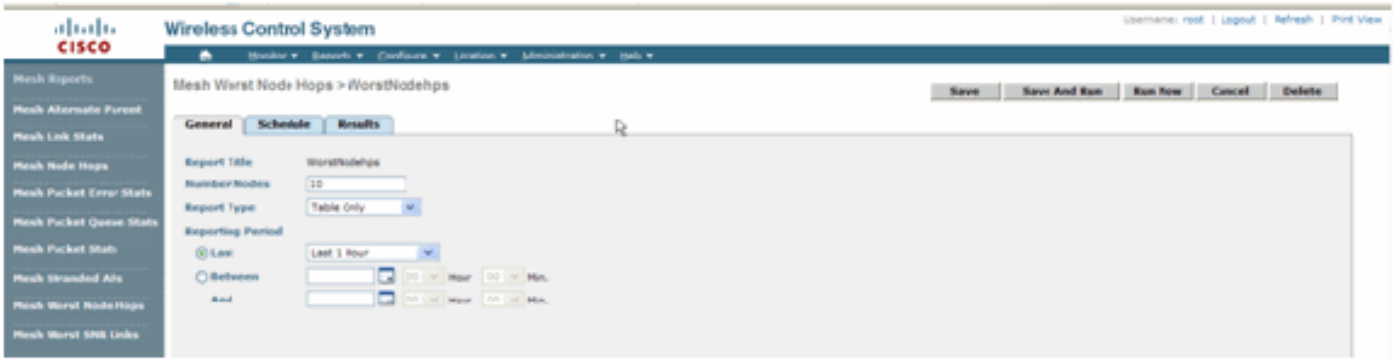
Les problèmes de bruit pourraient se poser aux heures différentes et le bruit pourrait augmenter à différents débits ou dure pour différentes durées. La prochaine figure fournit la capacité de créer l'état pour la radio a et le b/g aussi bien que les interfaces sélectives. Les listes d'état les 10 plus mauvais liens SNR par défaut. Vous pouvez choisir de 5 à 50 plus mauvais liens. L'état peut être généré pour la 1 dernière heure, les 6 dernières heures, le dernier jour, les 2 derniers jours, et jusqu'à 7 jours. Les données sont votées toutes les 10 minutes par défaut. Les données sont maintenues dans la base de données pour le maximum pendant sept jours. Les critères de sélection voisins de type peuvent être tous les voisins, parent/enfants seulement.



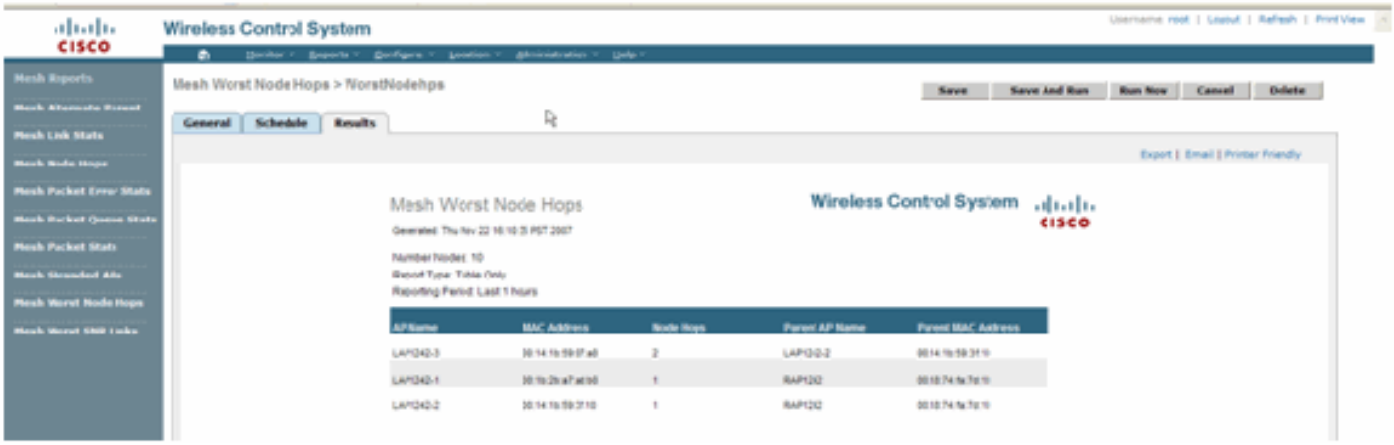


Les sauts de noeud les plus gâtés

Ce les sauts les plus gâtés aps des listes d'état the10 par défaut. Si les aps sont trop de sauts loin, les liens pourraient être très faibles. L'utilisateur peut isoler les aps qui ont beaucoup de sauts à partir d'AP racine et agissent la mesure appropriée. Vous pouvez choisir de changer ce **nombre de** critères de **Noeuds** entre 5 et 50. Les critères de filtre de **type d'état** dans cette figure peuvent être Tableau seulement ou tableau et graphique :



Cette figure donne le résultat pour le dernier état :



Statistiques de Sécurité

Les statistiques d'intérieur de Sécurité de maille sont affichées à la page de détail AP sous la section Informations traversière. Une entrée dans la table d'intérieur de statistique de MeshNodeSecurity est créée quand un noeud d'intérieur de maille d'enfant s'associe ou authentifie avec un noeud d'intérieur de maille de parent. Des entrées sont retirées quand le noeud d'intérieur de maille le dissocie du contrôleur.

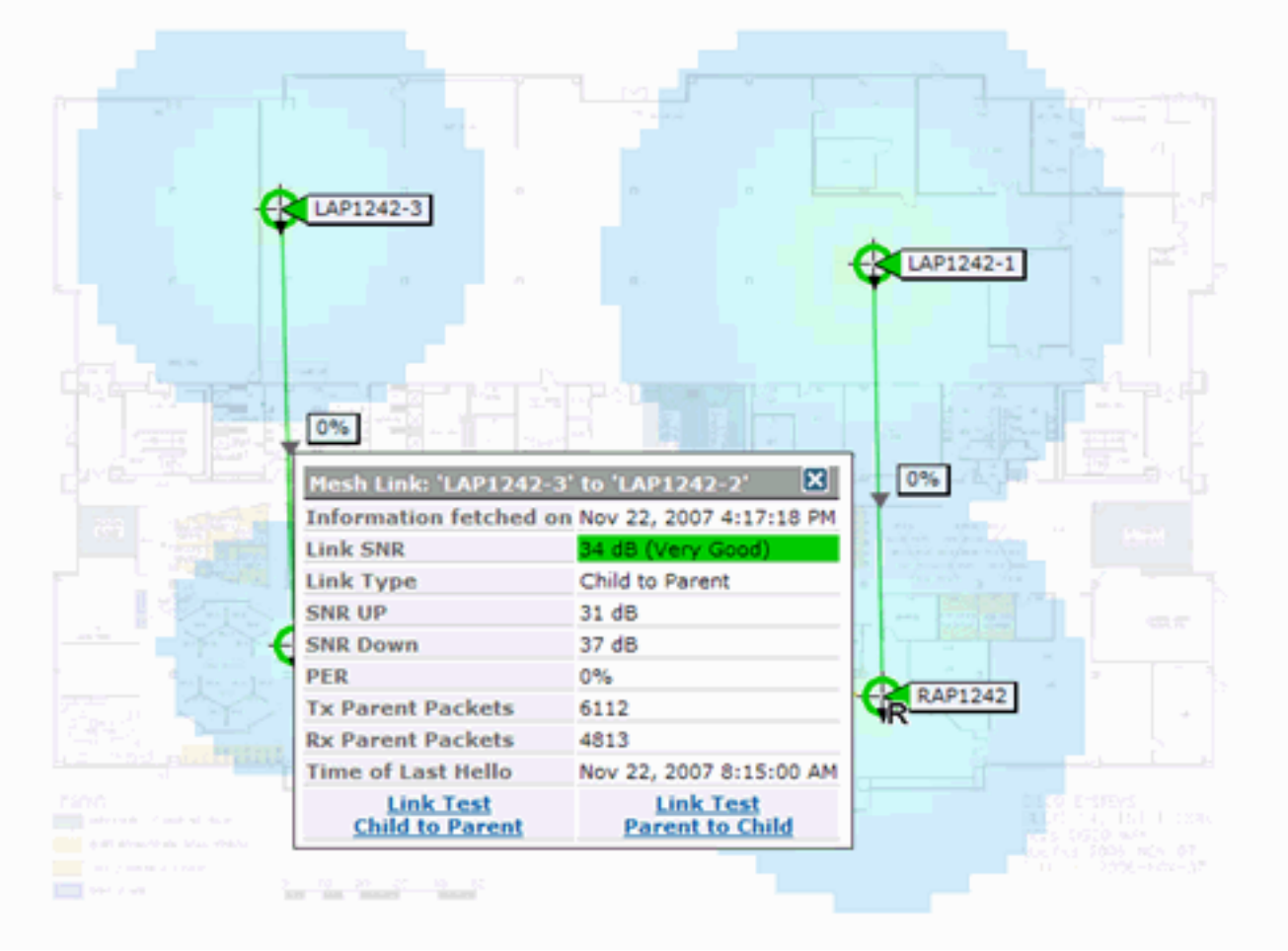
Test de liaison

Le test de liaison AP-à-AP est pris en charge sur le WCS. On peut sélectionner deux aps quelconques et appeler un test de liaison entre les deux.

Si ces aps sont des voisins rf, alors le test de liaison peut avoir un résultat. Le résultat est affiché dans un dialogue sur la carte lui-même sans page complète régénèrent. Le dialogue peut être rejeté facilement.

Cependant, si ces 2 aps ne sont pas des voisins rf, puis WCS n'essaye pas de figurer un chemin entre les 2 aps afin de faire un test de liaison de multiple de cartel.

Quand la souris est déplacée au-dessus de la flèche sur le lien entre les deux Noeuds, cette fenêtre apparaît :



Test de liaison de Noeud-à-noeud

L'outil de test de liaison est un outil sur demande pour vérifier la qualité de lien entre deux aps quelconques. Dans WCS, cette caractéristique est ajoutée à la page de détail AP.

Àla page de détail AP, sous l'onglet **d'intérieur de lien de maille** où des liens sont répertoriés à côté de elle, il y a un lien pour réaliser le test de liaison.

L'outil de test de liaison CLI de contrôleur a les paramètres d'entrée facultatifs : Longueur de paquet, paquets totaux de test de liaison, durée de test, et de débit de liaison de données. Le test de liaison a des valeurs par défaut pour ces paramètres optionnels. Les adresses MAC pour les Noeuds sont les seuls paramètres d'entrée obligatoires.

L'outil de test de liaison teste le point fort, le paquet envoyé, et le paquet reçu entre les Noeuds. Le lien pour le test de liaison est affiché sur l'état de détail AP. Quand vous cliquez sur le lien, il y a un écran instantané donnant les résultats de test de liaison. Le test de liaison s'appliquera seulement au parent – enfant et parmi des voisins.

La sortie de test de liaison génère des paquets envoyés, des paquets reçus, des paquets d'erreurs (positions pour des raisons de diff), le SNR, le plancher de bruit, et le RSSI.

Le test de Lnk fournit ces détails sur le GUI à un minimum :

- Paquets de test de liaison envoyés
- Paquets de test de liaison reçus
- Force du signal dans le dBm

- Rapport de signal-bruit

Liens sur demande de voisin AP

C'est une nouvelle caractéristique dans la carte WCS. Vous pouvez cliquer sur en fonction une maille AP et une fenêtre externe avec les informations détaillées apparaît. Vous pouvez alors cliquer sur des **voisins de maille de vue**, qui cherche les informations sur les voisins pour AP sélectionné et affiche une table avec tous les voisins pour la maille d'intérieur sélectionnée AP.

Le lien voisin de maille de vue affiche tous les voisins pour AP mis en valeur. Cet instantané affiche tous les voisins, type des voisins, et valeur SNR.

Test de ping

Le test de ping est un outil sur demande utilisé pour cingler entre le contrôleur et l'AP. L'outil de test de ping est disponible dans la page de détail AP et dans la MAP. Cliquez sur le lien de **test de ping de passage** dans la page de détail AP ou des informations de la MAP AP pour initier le ping du contrôleur au courant AP.

Conclusion

La maille d'entreprise (c'est-à-dire, maille d'intérieur) est une extension de couverture Sans fil de Cisco aux endroits où les Ethernets câblés ne peuvent pas fournir la Connectivité. La flexibilité et la gestionnabilité d'un réseau Sans fil est accomplie avec la maille d'entreprise.

La plupart des aps de câble par caractéristiques fournissent sont fournies par la topologie à maillage d'intérieur. La maille d'entreprise peut également coexister avec les aps de câble sur le même contrôleur.

Informations connexes

- Support et documentation techniques - Cisco Systems