Réseau sans fil unifié : Dépanner les problèmes des clients

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Conventions
Informations générales
Questions de configuration
Non-concordance SSID
Non-concordance de Sécurité
WLAN handicapé
Débits de données non vérifiés
Clients handicapés
Préambules par radio
Caractéristiques de Cisco Properietary - Questions avec des clients de tiers
Questions d'adresse IP
Questions de client
Questions rf
Messages d'erreur
Dépannage des questions de client avec WCS
Dépannage du WEP
Dépannage du WPA-PSK
Dépannage du 802.1X
Dépannage du Web-Auth
Dépannage du DHCP et de l'adressage IP
Informations connexes

Introduction

L'environnement de Radiofréquence (RF) est complexe et dynamique. De divers facteurs doivent être considérés comme pour créers un bon environnement sans fil. Il explique les divers problèmes que vous pouvez rencontrer lorsque vous connectez un client sans fil dans un environnement sans fil Cisco Unified, ainsi que les étapes à prendre pour dépanner et résoudre ces problèmes.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Solution de Cisco Unified Wireless
- Configurations de base Sans fil GUI des contrôleurs LAN de Cisco (WLC)

Composants utilisés

Ce document s'applique à tous les périphériques qui participent à l'environnement unifié par Cisco mais n'est pas limité au logiciel et aux versions de matériel spécifiques.

Conventions

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

Informations générales

Dans un environnement de Cisco Unified, le WLC assume un rôle central. Il gère le réseau Sans fil entier. Le Point d'accès léger (recouvrements), qui servent les clients sans fil, s'enregistre au WLC et télécharge la configuration entière de WLC. La mesure initiale est de vérifier si le RECOUVREMENT est enregistré au WLC. Cliquez sur le menu Sans fil du GUI WLC, et vérifiez si le RECOUVREMENT est répertorié à la page.

Questions de configuration

Pour une connexion Sans fil réussie, il est essentiel que la configuration sur le WLC soit faite correctement. Cette section décrit certaines le plus généralement - des questions vues de configuration.

Non-concordance SSID

Le client emploie son SSID pour l'identifier et s'associer au réseau Sans fil, ainsi assurez-vous que le SSID est configuré identiquement sur le WLC et le client. Afin de vérifier le SSID configuré sur le WLC, cliquez sur la page **WLAN**. Cliquez sur le *WLAN* approprié, et vérifiez le *SSID* configuré sous l'*onglet Général*.

Remarque: *Le SSID* distingue les majuscules et minuscules. Il pourrait aider le client sans fil à s'associer au WLAN si vous supprimez et recréez le WLAN.

Non-concordance de Sécurité

Les configurations de sécurité doivent s'assortir entre le WLC et le client. Si le type d'authentification est WEP statique, vérifiez si la clé de chiffrement/index de clé appropriés sur le WLC apparie cela du client. Si le type d'authentification est 802.1x ou WPA, assurez-vous que la taille de type/clé de chiffrement d'authentification s'assortit entre le client et le WLC. Pour plus d'informations sur la façon configurer le WLC et le client pour différentes solutions de sécurité,

référez-vous à l'authentification sur des exemples Sans fil de configuration de contrôleurs LAN.

Remarque: Posez 2 solutions de sécurité, telles que le WPA ou le 802.1x, ne pouvez pas être utilisé pour un WLAN configuré avec des solutions de sécurité de la couche 3, telles que l'authentification Web ou la fonction émulation. Pour plus d'informations sur les solutions de sécurité compatibles référez-vous à la matrice de compatibilité Sans fil de degré de sécurité de la couche 2 et de la couche 3 de contrôleur LAN.

WLAN handicapé

Pour une connexion Sans fil réussie, le WLAN correspondant doit être en activité sur le WLC. Par défaut, l'état du WLAN n'est pas activé sur le WLC. Afin de lancer le WLAN, cliquez sur le menu **WLAN** dans le WLC. La liste des WLAN configurés sur le WLC s'affiche. Cliquez sur le WLAN qui est configuré avec le SSID auquel le client veut s'associer. Sous l'onglet Général de la page de **WLANs > Edit**, cochez la case d'état.

Débits de données non vérifiés

Pour une norme particulière, 802.11b/g ou 802.11a, vous pouvez sur option placer certains débits de données en tant qu'obligatoire et d'autres débits de données comme pris en charge ou désactivés sur le WLC. Pour une association réussie, un client sans fil doit prendre en charge les débits de données qui sont configurés comme obligatoires sur le WLC. Afin de vérifier les débits de données configurés sur le WLC, cliquer sur le menu **Sans fil** sur le GUI WLC, et vérifier les débits de données configurés sous **802.11b/g/n > réseau ou 802.11a/n > option Network** qui apparaît du côté gauche de la page. Vérifiez la page de support du constructeur de client pour déterminer ceci. Si vous améliorez le pilote client, il peut aider le client à prendre en charge les débits de données exigés.

Remarque: Pour une meilleure Connectivité, placez le plus bas débit de données à **obligatoire** sur le WLC et d'autres débits de données à **pris en charge**.

Clients handicapés

Sur le WLC, il y a une option de désactiver manuellement les clients. Cette caractéristique aide à empêcher les clients escrocs d'essayer pour accéder au réseau. Vérifiez si l'adresse MAC du client qui ne peut pas s'associer est trouvée dans les clients handicapés les répertorient, et, si oui, le retirent. Vous pouvez trouver la liste de clients handicapés quand vous cliquez sur l'option de **clients handicapés** sous le **menu Security** dans le GUI.

Remarque: Des clients peuvent être refusés l'association au réseau s'ils ne se conforment pas aux stratégies par défaut d'exclusion de client configurées sur le WLC. Pour plus d'informations sur la stratégie d'exclusion de client, référez-vous à la section de configuration de stratégies d'exclusion de client du guide de configuration Sans fil de contrôleur LAN de Cisco, version 4.2.

Préambules par radio

Le préambule par radio (parfois appelé une en-tête) est une section de données à la tête d'un paquet, qui contient les informations dont les périphériques sans fil ont besoin quand ils envoient et reçoivent des paquets.

Quelques clients ne prennent en charge pas le **préambule court**, ainsi ils ne peuvent pas se

connecter au WLAN qui a le **préambule court** activé. Les préambules courts améliorent la représentation de débit, ainsi ils sont activés par défaut sur le WLC. Afin de désactiver le préambule court, cliquez sur le menu **Wireless** de la GUI du WLC. Cliquez ensuite sur le menu du réseau **802.11b/g >** à gauche. *Décochez la* case **courte de préambule**.

Caractéristiques de Cisco Properietary - Questions avec des clients de tiers

Si les périphériques de client qui ne peuvent pas se connecter au réseau sont des périphériques non-Cisco, désactiver certaines des fonctionnalités propriétaire de Cisco a comme conséquence une connexion réussie. Pour une liste de fonctionnalités que les supports de client, contactent le constructeur du tiers périphérique de client.

Ce sont certaines des importantes fonctionnalités propriétaire :

- Aironet IE - Aironet IE contient les informations, telles que le nom du point d'accès, la charge, le nombre de clients associés, etc. envoyées par le point d'accès dans les réponses de la balise et de la sonde du WLAN. Les clients CCX emploient ces informations pour choisir le meilleur point d'accès auquel s'associer.
- **MFP** — Le Management Frame Protection est une fonctionnalité introduite pour assurer l'intégrité des trames de Gestion, telles que la désauthentification, la dissassociation, les balises, et les sondes où le Point d'accès protège les trames de Gestion qu'il transmet quand il ajoute un élément d'information de Message Integrity Check (IE MIC) à chaque trame. N'importe quelle tentative faite par les intrus pour copier, modifier, ou rejouer la trame infirme la MIC, qui entraîne n'importe quel Point d'accès de réception, qui est configuré pour détecter des trames MFP, pour signaler l'anomalie.Ces fonctionnalités sont activées par défaut pour tout WLAN créé sur le WLC. Afin de désactiver ces fonctionnalités, cliquez sur le menu des WLAN dans le WLC. La liste des WLAN configurés sur le WLC s'affiche. Cliquez sur le WLAN auquel le client veut s'associer. Sous l'onglet Advanced des WLAN, dans la page Edit, désactivez les cases à cocher qui correspondent à Aironet IE et MFP.
- **Préambules par radio** — Le préambule par radio (parfois appelé une en-tête) est une section de données à la tête d'un paquet qui contient les informations dont les périphériques de périphérique sans fil et de client ont besoin pour envoyer et recevoir des paquets. Vous pouvez placer le préambule par radio à long ou à court selon quelle configuration est prise en charge sur le client sans fil.
- **Transformation d'encapsulation Ethernet** — Quand le périphérique sans fil reçoit les paquets de données qui ne sont pas 802.3 paquets, le périphérique sans fil doit employer une méthode de transformation d'encapsulation pour formater les paquets à 802.3. Voici les deux méthodes de transformation :802.1H : Cette méthode fournit la performance optimale pour les Produits Sans fil de Cisco Aironet. 802.1H est la valeur par défaut.RFC1042 : Employez cette configuration pour assurer l'Interopérabilité avec l'équipement sans fil d'Aironet de non-Cisco. RFC1042 ne fournit pas les avantages d'Interopérabilité de 802.1H, mais est utilisé par d'autres fabricants d'équipement sans fil.
- **délai d'attente de prise de contact de wpa** — Quelques constructeurs ont besoin de plus longs délais d'attente de prise de contact de wpa. Vous pouvez employer la commande de **dot11 wpa handshake timeout** afin de changer le délai d'attente de prise de contact de wpa.
- **ssid** — Quelques constructeurs exigent du ssid d'être émission. Afin d'annoncer le ssid, invité-*mode d'*enable sous la configuration de ssid.

Questions d'adresse IP

Les clients sans fil ont besoin d'adresses IP valides pour communiquer avec le reste du réseau.

Le contrôleur se comporte comme un routeur avec une adresse auxiliaire IP. C'est-à-dire, il complète l'adresse IP et les unicasts de passerelle il au serveur DHCP par l'intermédiaire de l'interface dynamique sur laquelle le client est installé. Rendez-vous ainsi compte que la surveillance DHCP sur des Commutateurs, par défaut, bloquera ces paquets DHCP sur les ports non approuvés.

Quand l'offre DHCP revient au contrôleur, il remplace l'adresse IP du serveur DHCP par son adresse IP virtuelle. La raison qu'il fait ceci est parce que quand Windows erre entre les aps, la première chose il fait est essai pour entrer en contact avec le serveur DHCP et pour renouveler son adresse.

Avec l'adresse de serveur DHCP de 1.1.1.1 (qui est l'adresse IP virtuelle typique sur un contrôleur), le contrôleur peut intercepter ce paquet et truquer Windows. C'est également pourquoi l'adresse IP virtuelle est identique sur tous les contrôleurs. Si un ordinateur portable Windows est en itinérance vers un AP sur un autre contrôleur, il essayera de contacter l'interface virtuelle sur le contrôleur. En raison de l'événement de mobilité et du transfert de contexte, le nouveau contrôleur auxquels le client Windows a erré déjà a toutes les informations pour truquer Windows de nouveau.

Si vous voulez utiliser le serveur DHCP interne, tout que vous devez faire est mis l'adresse IP de Gestion comme le serveur DHCP sur l'interface dynamique vous créez pour le sous-réseau. Attribuez ensuite cette interface au WLAN. Le contrôleur a besoin d'une adresse IP sur chaque sous-réseau car il peut ainsi remplir l'adresse de la passerelle DHCP dans la requête DHCP.

Nous voyons beaucoup de problèmes d'adresse IP DHCP. Voici les raisons et les étapes de résoudre ces problèmes :

1. Si le type d'authentification configuré est l'une de solutions de sécurité de la couche 2, telles que le 802.1x ou le WPA, le client doit avec succès authentifier pour obtenir une adresse IP valide. Premier contrôle si le client est avec succès authentifié.**Remarque:** Une exception est si le client est configuré pour des solutions de sécurité de la couche 3, telles que l'authentification Web, ou le client de fonction émulation de Web est assigné une adresse IP avant l'authentification.
2. Chaque WLAN défini sur le WLC est tracé à une interface dynamique du WLC, qui est configuré avec un VLAN qui appartient à un seul sous-réseau. Des clients qui s'associent à ce WLAN sont assignés des adresses IP du sous-réseau d'interface du VLAN. Vérifiez si l'IP de sous-réseau et la passerelle de ce WLAN sont définis sur le serveur DHCP pour que le client obtienne une adresse IP sur ce sous-réseau. Référez-vous à la documentation du constructeur compétent pour configurer le serveur DHCP.**Remarque:** Comme condition préalable, le contrôle si le serveur DHCP est accessible du WLC et si le service DHCP est activé.
3. Assurez-vous que l'adresse IP du serveur DHCP est définie correctement dans l'interface du WLC qui est tracé au WLAN. Afin de vérifier ceci, cliquez sur le menu de **contrôleur** dans le GUI. Cliquez sur le menu d'**interfaces du** côté gauche, et vérifiez le gisement de **serveur DHCP**. À la même page, contrôle que l'interface est tracée à un *port physique* qui est haut et en activité. Afin de dépanner des questions connexes DHCP, utilisez l'**enable de paquet de**

debug dhcp de commandes et l'**enable de message de debug dhcp** sur le WLC.**Remarque:** Vous pouvez également configurer WLC comme serveur DHCP. Pour plus d'informations sur la façon configurer le DHCP divisez sur le WLC, se rapportent à l'aide du GUI pour configurer la section DHCP du guide de configuration Sans fil de contrôleur LAN de Cisco de document, version 5.0.

4. Le proxy DHCP est activé par défaut sur le WLC. Unicasts WLC le paquet au serveur DHCP configuré sur l'interface du WLAN ou le WLAN elle-même. Si le serveur DHCP ne prend en charge pas le comportement de proxy DHCP de Cisco, désactivez le proxy DHCP sur le WLC. Pour plus d'informations sur la façon désactiver le proxy DHCP sur le WLC, référez-vous à la section de configuration de proxy DHCP du guide de configuration Sans fil de contrôleur LAN de Cisco, version 5.2.
5. WLC se connecte habituellement au réseau câblé par un commutateur. Vérifiez si des ports de commutateur qui sont connectés au WLC et au serveur DHCP sont configurés comme joncteur réseau et qui les VLAN appropriés sont permis sur ces ports. Pour plus d'informations sur la façon configurer les Commutateurs de Cisco, référez-vous au configurer le port de commutateur de la couche 2 qui se connecte au WLC comme section Port de joncteur réseau de l'invité WLAN et WLAN interne de document utilisant l'exemple de configuration de WLCs.
6. On ne permet pas aux des clients statiques pour s'associer au WLAN si l'**adr DHCP. Le champ d'affectation** est activé pour le WLAN. Cette option rend nécessaire que tous les clients qui s'associent à ce WLAN doivent obtenir des adresses IP par le DHCP. Afin de vérifier si cette option est activée, cliquez sur le menu WLAN dans le GUI WLC. La liste des WLAN configurés sur le WLC s'affiche. Cliquez sur le WLAN approprié. Allez à l'**onglet Avancé** et localisez le champ d'**affectation d'adresses DHCP**.
7. Quelques serveurs DHCP, tels qu'un Pare-feu de Cisco PIX, ne prennent en charge pas des services de relais DHCP. Ils reçoivent seulement des paquets DHCP d'émission, aucun paquet monodiffusion d'un agent de relais DHCP, ainsi assurez-vous que les clients DHCP sont directement connectés à l'interface sur laquelle le serveur est activé.**Remarque:** Vérifiez le document approprié de constructeur pour le support de relais DHCP.

Questions de client

Il est également important que les choses soient en place sur le côté client. Exécutez ces contrôles sur le côté client :

1. Parfois, la carte client n'est pas identifiée par l'ordinateur. Dans ce cas, essayez la carte sur un emplacement différent. Si cela ne fonctionne pas, essayez-le sur un ordinateur différent. Pour plus d'informations sur des questions au sein de l'installation, référez-vous à la section dépannage du document Cisco Aironet 340, 350, et du guide d'installation et de configuration d'adaptateurs client LAN sans fil CB20A pour Windows.**Remarque:** Assurez-vous que la carte Sans fil est compatible avec le système d'exploitation qui est installé sur l'ordinateur. Ceci peut être vérifié de la fiche technique de la carte client.
2. Vérifiez si le client est installé correctement sur l'ordinateur. L'état de la carte client peut être vérifié de l'écran de **gestionnaire de périphériques de Windows**. Recherchez le message qui lit, *« ce périphérique fonctionne correctement. »* S'il n'est pas, il indique que les gestionnaires ne sont pas installés correctement. Essayez de désinstaller le gestionnaire et de réinstaller les gestionnaires sur l'ordinateur. Afin de désinstaller les gestionnaires, cliquer avec le

bouton droit l'adaptateur Sans fil de l'écran et du clic de gestionnaire de périphériques **désinstallez**. Pour plus d'informations sur la façon réinstaller l'adaptateur de client, référez-vous à installer la section d'adaptateur de client du document Cisco Aironet 340, 350, et du guide d'installation et de configuration d'adaptateurs client LAN sans fil CB20A pour Windows.**Remarque:** Si vous utilisez l'ACU pour configurer la carte client, assurez-vous que la radio n'est pas désactivée sur l'ACU. En outre, vérifiez si l'état de la carte est activé sous la **connexion réseau** sur le panneau de configuration de Windows.**Remarque:** Utilisez seulement un logiciel de suppliant pour la carte Sans fil. Il est toujours recommandé pour utiliser constructeur-a fourni le suppliant pour la carte. Comme option secondaire, vous pouvez utiliser celui fourni par le constructeur PC ou le WZC fourni par Windows.**Remarque:** Terminez-vous ces étapes afin de mettre au point WZC :Employez le **suivi réglé par ras de netsh *** commande **activée** afin d'activer l'élimination des imperfections WZC.Employez le **suivi réglé par ras de netsh *** commande **handicapée** afin d'arrêter l'élimination des imperfections WZC.Des logs sont écrits à *C:\Windows\tracing*. *eapol.log*, *rastls.log*, et *wzctrace.log* sont les logs les plus importants.**Remarque:** Référez-vous au pour en savoir plus Sans fil de diagnostics et de dépannage.

3. La configuration sur le client doit apparier cela de WLC. Ceci se rapporte principalement au SSID et à la configuration de sécurité sur le client. Si vous employez l'utilitaire de Cisco pour configurer le client, référez-vous à utiliser la section de gestionnaire de profil du document Cisco Aironet 340, 350, et du guide d'installation et de configuration d'adaptateurs client LAN sans fil CB20A pour Windows.
4. Si vous ne pouvez pas transférer des données, même après une association, un essai Sans fil réussis pour désactiver tous autres adaptateurs aussi bien que ceux du VPN et des adaptateurs de câble. S'il y a plus d'un adaptateur Sans fil dans l'ordinateur, désactivez d'autres adaptateurs pour éviter des conflits entre eux.
5. Si vous trouvez des problèmes de connectivité seulement avec un client simple, essayez d'améliorer les gestionnaires et le micrologiciel de ce client. Si vous trouvez des problèmes de connectivité avec une majorité des clients et vous avez éliminé d'autres questions, choisissez d'améliorer le WLC.
6. Assurez-vous que les périphériques, c.-à-d., client et le WLC, sont WiFi certifié pour éviter tous les problèmes d'interopérabilité liés à la Sécurité et exécutions.
7. Si vous utilisez un ordinateur Windows, assurez-vous que vous avez installé tous les derniers correctifs de sécurité ou correctifs fournis par Microsoft. Si vous utilisez l'utilitaire de client Windows, assurez-vous que vous avez installé le dernier correctif fourni par Microsoft.
8. Quelques clients répondent lentement à l'authentification EAP. Ceci a comme conséquence les minuteries sur le WLC, et vous pouvez recevoir ce message d'erreur sur le WLC :

```
Tue Jul 26 16:46:21 2005: 802.1x 'timeoutEvt' Timer expired for station <Mac address of the
client>
```

En réponse à ce message, augmentez les valeurs du dépassement de durée d'EAP sur le WLC pour fournir l'heure suffisante pour que le client authentifie. Utilisez ces commandes d'ajuster les temporisateurs d'EAP sur le WLC :

```
config advanced eap identity-request-timeout <1-120 secs>
config advanced eap identity-request-retries <1-20>
 !--- Specifies the amount of time and the maximum number of times the WLC attempts to send an
EAP identity request to wireless clients. config advanced eap request-timeout <1-120>
config advanced eap request-retries <1-20>
 !--- Specifies the amount of time and the maximum number of t imes the WLC attempts to send EAP
request to the Radius Server . config advanced eap eapol-key-timeout <1-5>
config advanced eap eapol-key-retries <0-4>
```

```
 !--- Specifies the amount of time and the maximum number of times the WLC attempts to negotiate
the encryption key.
```

Questions rf

L'interférence rf est l'une des causes principales pour la connexion pauvre. L'interférence peut sont provoqué par par les réseaux adjacents de 802.11 ou d'autres sources, telles que les fours à micro-ondes ou les téléphones sans fil qui fonctionnent dans la même fréquence. L'interférence entraînée par les réseaux adjacents de 802.11 est de deux types :

- **Interférence de co-canal :** Quand des Points d'accès, dont la zone de couverture superpose, sont configurés dans le même canal ou les canaux avec des fréquences superposantes, il entraîne des problèmes de connectivité pour des clients dans la zone de couverture superposante. Afin d'éviter cette question, changent le numéro de canal à un canal non-recouvert, ou écartent le Point d'accès plus loin de sorte que leurs zones de couverture ne superposent pas. Par exemple, dans 802.11b/g, les canaux de réseau 1, 6, et 11 sont les canaux non-recouverts.
- **Interférence à canal adjacent :** Quand des Points d'accès sont placés trop étroitement entre eux ou utilisent les niveaux de puissance à haute production, il entraîne l'interférence, même lorsque les Points d'accès sont configurés sur les canaux non-recouverts. Diminuez l'alimentation du Point d'accès de réparer cette question.**Remarque:** Des canaux non-recouverts s'appellent également les canaux adjacents, qui explique l'*interférence de canal adjacent de* nom.

Utilisez les analyseurs de spectre pour identifier des sources d'interférence, telles que les fours à micro-ondes ou les téléphones sans fil qui fonctionnent dans la chaîne 2.4 gigahertz, ou les périphériques qui fonctionnent dans la chaîne 5 gigahertz. Retirez les sources d'interférence une fois qu'ils sont identifiés. Alternativement, vous pouvez changer la norme sur laquelle votre réseau sans fil fonctionne, par exemple, à partir de 802.11b/g à 802.11a pour éviter l'interférence.

Un autre important aspect pour la transmission efficace rf est force du signal. La force du signal pauvre mène à la connexion intermittente. Les obstacles, tels que des murs, des métaux, absorbent et réfléchissent l'énergie rf, qui réduit la force du signal. Augmentez l'alimentation au niveau requis sur le Point d'accès de fournir la couverture adéquate. Vous pouvez également utiliser les Antennes à gain élevé pour étendre la plage et la force du signal, mais vous assurez que c'est FCC approuvée pour fonctionner avec le périphérique.

Remarque: Le rapport de signal-bruit (SNR), qui est la différence entre la force du signal et le bruit rf (le signal ou l'énergie rf d'autres sources qui fonctionnent dans la même fréquence que le réseau Sans fil), est un facteur clé pour mesurer la qualité du lien. Un SNR plus élevé indique une bonne qualité de lien, qui a comme conséquence un transfert des données plus rapide. Une valeur inférieure indique la mauvaise qualité, qui mène à la connectivité intermittente ou au mauvais fonctionnement. Les analyseurs Sans fil de paquet/logiciel d'analyse de site peuvent t'afficher le SNR et le débit à un emplacement particulier.

ÀCisco environnement unifié, il y a un concept appelé le Gestion des ressources radio (RRM) mis en application sur le WLCs. Le RRM est un logiciel inclus dans le contrôleur, qui agit en tant qu'ingénieur intégré rf pour fournir uniformément la Gestion en temps réel rf de votre réseau Sans fil. Il prend automatiquement soin de toutes les questions mentionnées rf. Pour plus d'informations sur RRM, référez-vous à la section Gestion de configuration de ressource par radio du guide de configuration Sans fil de contrôleur LAN de Cisco de document, version 5.0.

Messages d'erreur

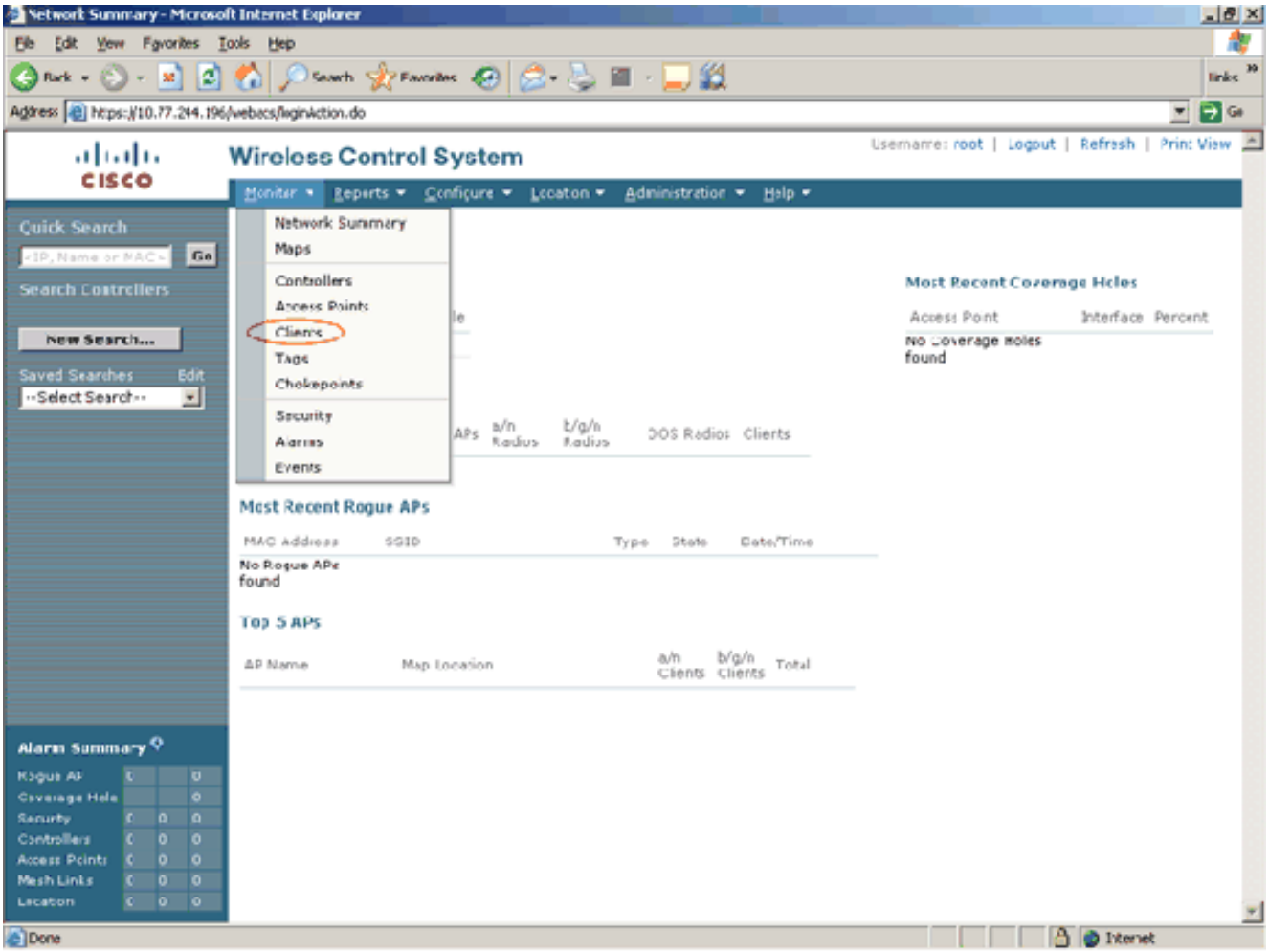
Parmi le cours de la Connectivité de client, vous pouvez recevoir de plusieurs messages d'erreur, sur le WLC et les côtés client.

- **Le client ne peut pas l'un ou l'autre obtenir un retard d'adresse IP ou de rencontre à obtenir l'adresse IP par le DHCP. Le debug dhcp sur le contrôleur indique ceci :**
  `Sun Nov 9 22:09:05 2008: <mac address of the client> DHCP processing DHCP NAK` *Le NAK DHCP* est habituellement envoyé par le serveur DHCP pour indiquer une tentative par le client d'obtenir une adresse IP du sous-réseau auquel elle n'appartient pas. Ceci se produit habituellement quand un client erre d'un WLC à l'autre, où le même WLAN est assigné un VLAN différent.Configurez le proxy DHCP sur le WLC pour fournir une difficulté pour ceci.

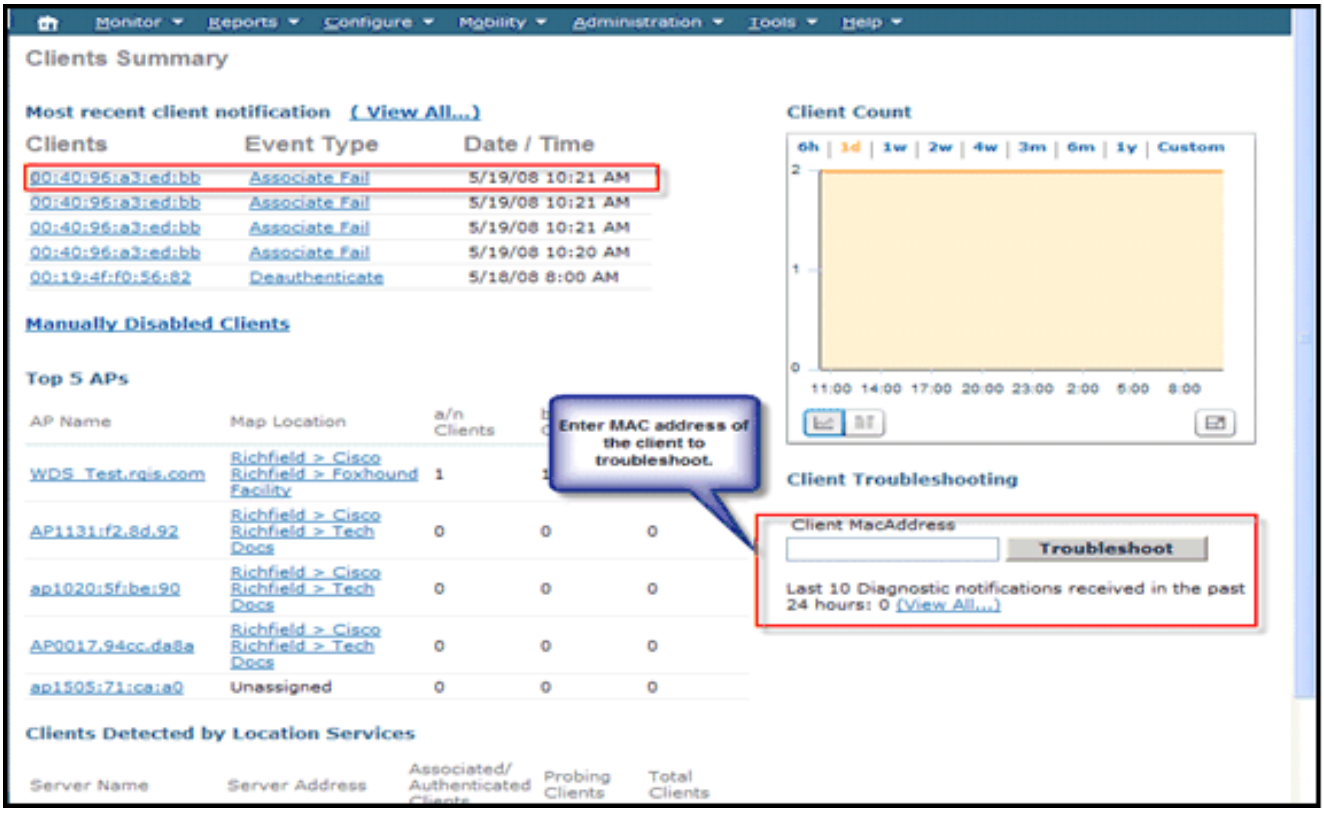
Dépannage des questions de client avec WCS

WCS peut être utilisé pour dépanner les questions liées au client dans un environnement sans fil. Il fait ceci à l'aide de l'outil de dépannage construit dans WCS. Afin de dépanner un client par le WCS, besoin de l'utilisateur d'exécuter ces étapes

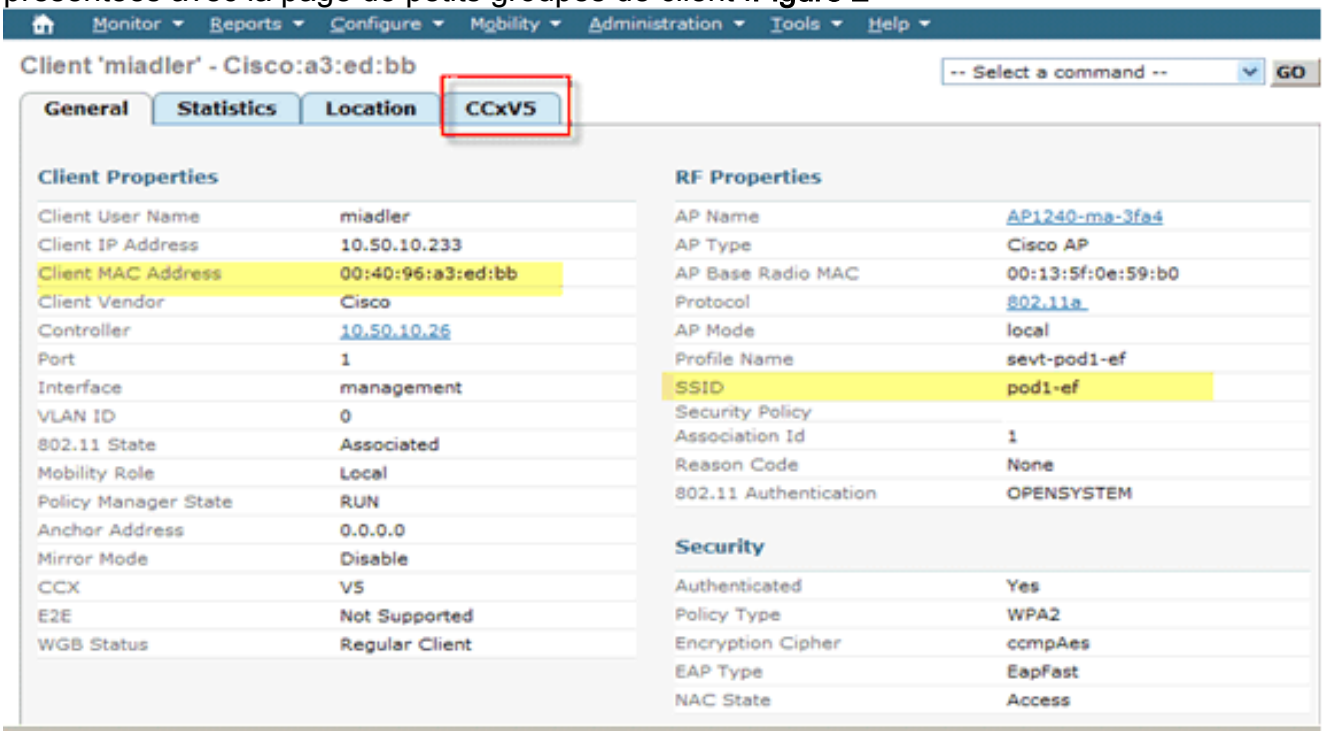
1. De la page de tableau de bord WCS, cliquez sur le menu de **moniteur** et choisissez les **clients de la**
   liste.



2. Ceci apporte au client la page récapitulative suivant les indications de la figure 1, qui affiche la liste de clients dans le réseau Sans fil.**Figure 1**



3. Cliquez sur un client pour obtenir des détails tels que le SSID ou la méthode d'authentification de client particulier. La figure 2 affiche un exemple de ceci. La zone de dialogue de **dépannage au** côté droit inférieur de la page récapitulative de client affichée dans la figure 1 permet à des utilisateurs pour entrer dans l'adresse MAC du périphérique pour dépanner. Ceci vous amène à la page d'outil de dépannage suivant les indications du schéma 3. lors de l'identification et la sélection du client à dépanner, des utilisateurs sont présentées avec la page de petits groupes de client :**Figure 2**



Dépannage du WEP

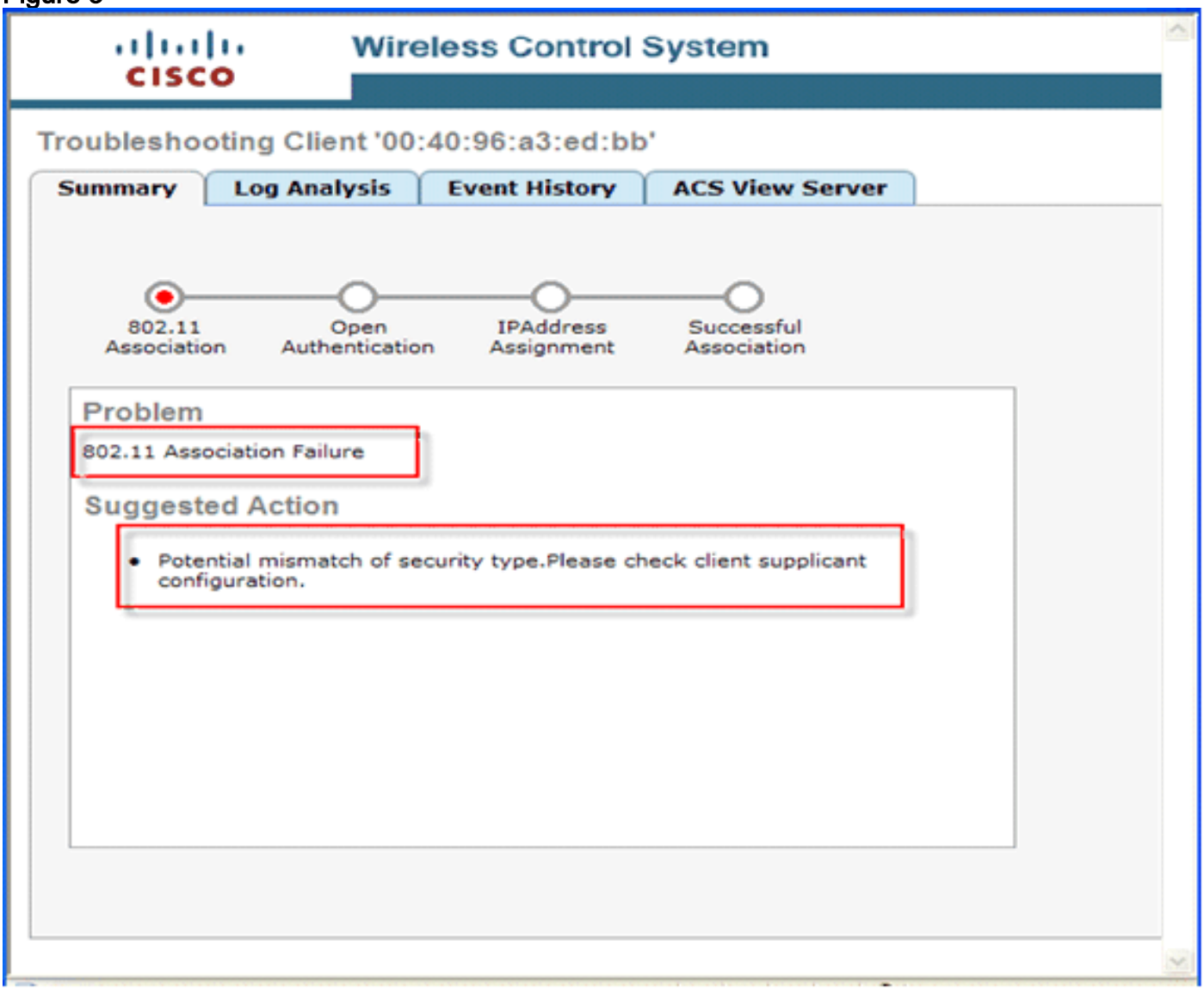
Il est souvent difficile de dépanner les clients sans fil existants qui utilisent toujours les mécanismes de sécurité WEP. Exécutez ces contrôles sur le client et l'AP :

- Non-concordances de longueur de clé WEP (et principales)
- Index de clé WEP (et disparités de configuration)
- Méthode d'authentification configurée (ouvrez-vous contre la clé partagée)

Non-concordance d'authentification

Bien que la capture des paquets puisse être un processus pénible, l'outil de dépannage de client WCS peut facilement aider à préciser où le problème existe. Souvent, ce petit "TIP" est ce qui réduit le temps de panne. La figure 2 affiche l'**outil de dépannage WCS**. Comme présenté dans la figure, l'étape problématique est identifiée et visualisée, qui prépare le terrain pour l'analyse détaillée.

Figure 3



Non-concordance d'index de clé WEP

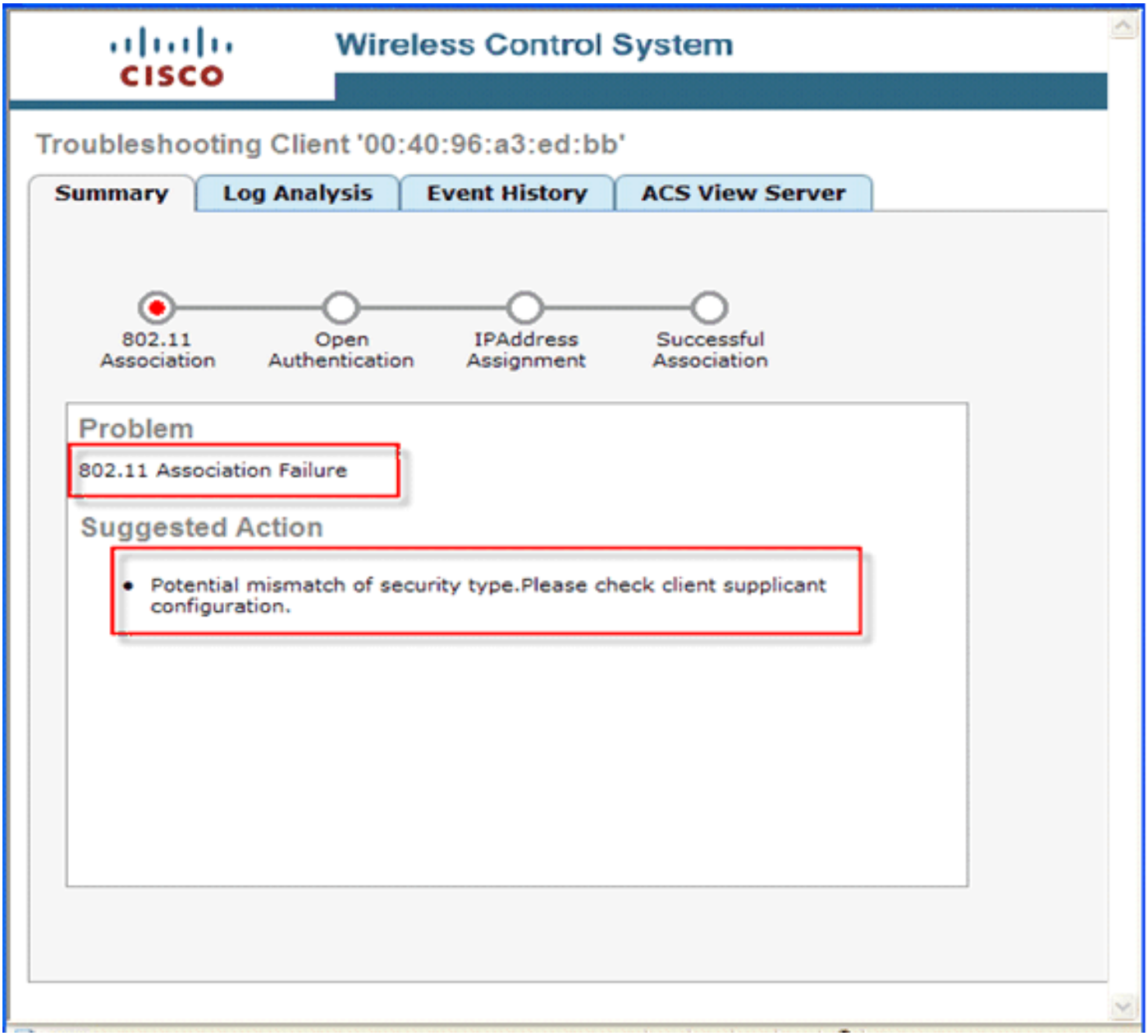
Généralement vous pouvez configurer jusqu'à 4 clés WEP sur le client et l'AP. Une des clés est choisie comme touche de transmission. Ceci doit s'assortir entre le client et l'AP. Par exemple, si la clé 2 est choisie comme touche de transmission sur le client, ceci doit s'assortir avec la clé 2 sur AP, mais AP peut avoir une clé différente que la touche de transmission. L'autre sujet est souvent ceci : les constructeurs de client et d'infrastructure interprètent les caractéristiques différemment, qui entraîne différentes réalisations dans le produit. Un exemple classique est l'utilisation des

index de clé de 0 à 3 contre les index de clé de 1 à 4. Ceci peut avoir comme conséquence la configuration mal adaptée et les tentatives défectueuses de connexion. À ce moment là, la grande attention de paiement au « ID de clé » classé dans le paquet décodent, qui indique si c'est l'origine du problème.

Dépannage du WPA-PSK

Le dépannage de WPA-PSK est semblable au WEP de plusieurs manières. La plupart des essais ratés sont dus aux mauvaises configurations dans la clé. Avec l'outil de dépannage de client WCS, les administrateurs peuvent collecter les logs de la transaction WPA. Les logs, comme mis en valeur ci-dessous, affichage où le problème potentiel peut être *(configuration principale pré-partagée incorrecte sur le client dans cet exemple particulier)* et est dérivé de l'onglet d'**analyse de log de l'**outil de dépannage de client de WCS. Installez un WLAN avec le WPA-PSK comme stratégie de sécurité de la couche 2 et configurez le suppliant de client avec un PSK incorrect. Ce sont des logs des clés misconfigured PSK dans les événements :

```
<TIMESTAMP> INFO 10.10.10.2
   Controller association request message received.
<TIMESTAMP> INFO 10.10.10.2
   Received reassociation request from client.
<TIMESTAMP> INFO 10.10.10.2
   The wlan to which client is connecting requires 802 1x authentication.
<TIMESTAMP> INFO 10.10.10.2
   Client moved to associated state successfully.
<TIMESTAMP> ERROR 10.10.10.2
   802.1x authentication message received, static dynamic wep supported.
<TIMESTAMP> ERROR 10.10.10.2
   Expecting EAPOL key from client but not received yet.
<TIMESTAMP> ERROR 10.10.10.2
   EAPOL-key is retransmitted.
<TIMESTAMP> ERROR 10.10.10.2
   Expecting EAPOL key from client but not received yet.
<TIMESTAMP> ERROR 10.10.10.2
   EAPOL-key is retransmitted.
<TIMESTAMP> ERROR 10.10.10.2
   Expecting EAPOL key from client but not received yet.
<TIMESTAMP> ERROR 10.10.10.2
   Excluding client as max EAPOL-key re-transmissions reached.
<TIMESTAMP> ERROR 10.10.10.2
   Excluding client as max EAPOL-key re-transmissions reached.
<TIMESTAMP> ERROR 10.10.10.2
   Client 802.1x authentication failure exceeded the limit. <TIMESTAMP> ERROR 10.10.10.2 EAPOL-
key has possible incorrect psk configuration.
```

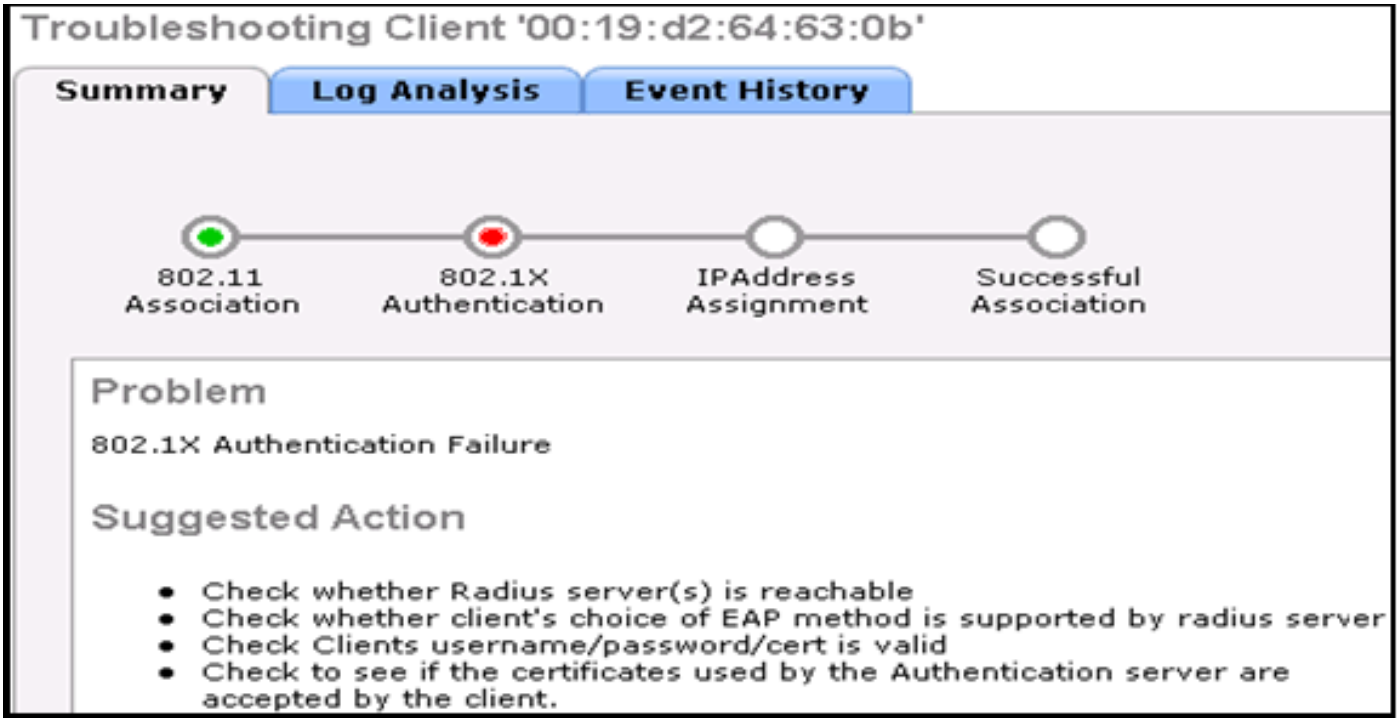


Dépannage du 802.1X

Comme l'adoption WLAN devient suppression progressive dominante et existante de clients ; le 802.1x est la direction pour la plupart des futurs déploiements. Il peut y avoir un grand choix de questions liées à la mauvaise configuration dans la chaîne (serveur d'AAA de <> de réseau de <> L2/L3 de <> WLC de <> AP de client). Ici on le suppose que les choses sont en place entre le WLC et le serveur d'AAA. Les questions qui surgissent entre le suppliant (client) et le serveur d'AAA sont généralement ceux-ci :

- Type inapproprié d'EAP
- Les qualifications fausses ont expiré des Certificats
- Méthode intérieure d'EAP faux

Sur le côté client, modifiez les qualifications de l'utilisateur sous des paramètres de sécurité ; par exemple, entrez le mot de passe incorrect et réexécutez le même test. L'outil de dépannage précise exactement où le problème se trouve, aussi bien que l'action suggérée.



Cliquez sur l'onglet d'**analyse de log** dans la figure affichée ci-dessus et vérifiez les logs pour n'importe quelle indication d'une authentification infructueuse de 802.1x.

```
<TIMESTAMP> INFO 10.10.10.2
   Received EAP Response from the client.
<TIMESTAMP> INFO 10.10.10.2
   EAP response from client to AP received.
<TIMESTAMP> INFO 10.10.10.2
   Radius packet received
<TIMESTAMP> INFO 10.10.10.2
   Received Access-Challenge from the RADIUS server for the client
<TIMESTAMP> INFO 10.10.10.2
   Sending EAP request to client from radius server.
<TIMESTAMP> INFO 10.10.10.2
   EAP response from client to AP received.
<TIMESTAMP> INFO 10.10.10.2
   Radius packet received
<TIMESTAMP> ERROR 10.10.10.2 Received Access-Reject from the RADIUS server for the client.
<TIMESTAMP> ERROR 10.10.10.2 Received eap failurefrom the client.
```

Dépannage du Web-Auth

Généralement bon le dépannage de la pratique doit inclure une vérification du « état de Policy Manager » du client qui a des questions. Pendant qu'il est confirmé dans la copie d'écran WCS ci-dessous, le client en question est coincé à l'état *WEBAUTH_REQD*. Ceci signifie que le processus de 802.11 est complet sans aucune erreur, et ces questions possibles peuvent se produire :

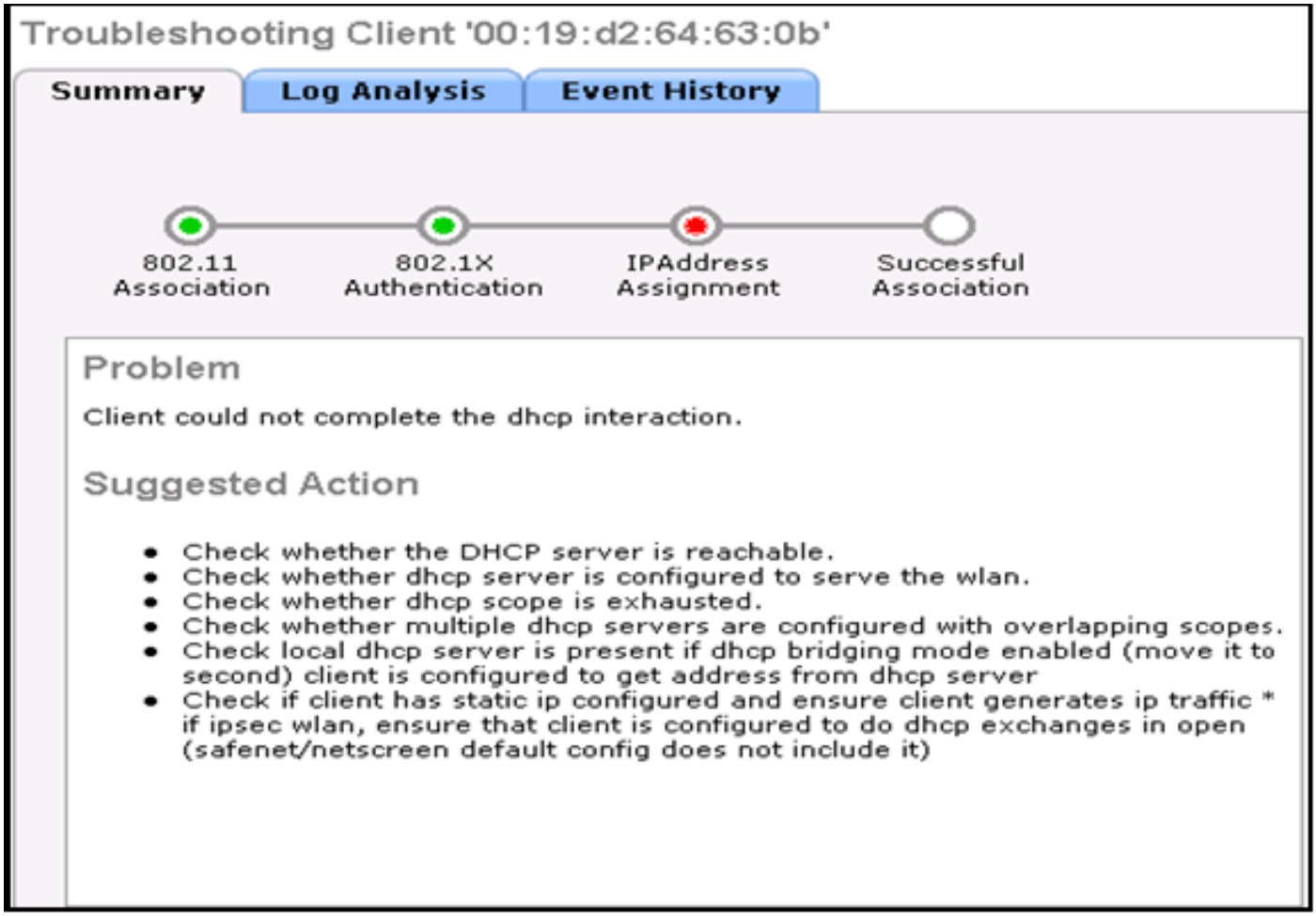
- Nom d'utilisateur incorrect/mot de passe
- Implémentation incorrecte d'ACL (pour atteindre le serveur externe de Web-auth, si quels)
- DN non configurés correctement et davantage**Remarque:** Pour plus d'informations sur l'authentification Web de dépannage, référez-vous à l'exemple de configuration d'authentification Web de contrôleur de
  document.

Les logs ont collecté de l'affichage WCS que le processus de Web-auth n'a pas été réussi. Une telle situation peut être simulée dans le laboratoire si vous placez la stratégie de la couche 3 WLAN au Web-auth et ne complète pas le processus de Web-auth ou entre dans qualifications incorrectes/inexistantes de procédure de connexion. Vérifiez la partie récapitulative d'outil de dépannage de client pour savoir où le problème s'est posé. Vous voyez ces logins WCS :

```
 <TIMESTAMP> INFO 10.10.10.2
   Controller association request message received
<TIMESTAMP> INFO 10.10.10.2
   Received reassociation request from client
<TIMESTAMP> INFO 10.10.10.2
   The wlan to which client is connecting does not require 802 1x authentication
<TIMESTAMP> INFO 10.10.10.2
   Client web authentication is required <TIMESTAMP> INFO 10.10.10.2 Client moved to associated
state successfully <TIMESTAMP> INFO 10.10.10.2 Controller association request message received
```

Dépannage du DHCP et de l'adressage IP

Souvent, les périphériques de client sont utilisés dans plus d'un réseau Sans fil. Un exemple peut être utilisation des employés d'un périphérique entreprise sur une maison ou un réseau public. Un employé peut faire assigner une adresse IP statique dans le réseau domestique. Il se connecte au réseau d'entreprise à une adresse IP statique précédemment assignée sans sa connaissance. Ceci mène à un problème de connectivité, qui peut être facilement précisé à l'aide de la suite de dépannage de client WCS (comme affiché ci-dessous). La majorité des questions dans ce royaume se trouve sur le client sans fil, mais ceci peut également se diriger vers un problème potentiel sur l'infrastructure câblée, telle qu'une portée épuisée, la portée incorrecte, la tentative etc. de créer ce scénario quand vous assignez une adresse IP statique incorrecte sur le client ou changez les paramètres de portée de DHCP sur le commutateur.



Informations connexes

- Guide de configuration Sans fil de contrôleur LAN de Cisco, version 5.1
- Gestion des ressources radio sous des réseaux sans fil unifiés
- Support et documentation techniques - Cisco Systems