# Contenu



# Introduction

Ce document décrit comment dépanner l'accès invité dans un réseau de câble et Sans fil où WLC est déployé pour authentifier et assigner des adresses IP aux clients dans un VLAN invité.

# Conditions préalables

## Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès invité dans un réseau unifié
- Authentification Web

## Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- WLC 4400 qui exécute la version de logiciel 5.2
- Commutateur de gamme Cisco Catalyst 6500
- Ordinateur portable avec l'adaptateur de client du 802.11 a/b/g de Cisco sur le Win XP

## 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 scénario typique de déploiement d'invité, deux WLCs sont impliqués : on dans le réseau câblé local et l'autre se sont déployés dans la zone DMZ. Les gens du pays WLC sont ancrés au WLC dans la zone DMZ et un tunnel d'EoIP est établi entre le WLCs. Les gens du pays WLC dans le réseau câblé dirigent tout le trafic d'invité (de câble et radio) vers le WLC dans la zone DMZ par le tunnel dédié. DMZ WLC authentifie et assigne une adresse IP aux clients. Typiquement, l'authentification Web est le mécanisme utilisé pour authentifier des clients d'invité.

# Dépannez l'accès invité

Le dépannage des clients d'invité implique trois aspects principaux :

- Dépannez le tunnel d'EoIP
- Authentification client
- Questions d'adresse IP

## Dépannez le tunnel d'EoIP

Le tunnel d'EoIP est établi utilisant le protocole 97 IP pour passer le trafic d'invité entre les gens du pays WLC et le DMZ WLC. La panne dans le tunnel a comme conséquence l'interruption du flux de données. Exécutez ces contrôles afin de s'assurer que le tunnel est établi poperly :

- Vérifiez si le WLCs sont configurés dans la liste de chacun de mobilité quoiqu'ils pourraient être dans différents Groupes de mobilité.
- Assurez-vous que le contrôleur DMZ est configuré comme ancre de mobilité pour lui-même et pour le WLC dans le réseau câblé, de sorte que les clients de VLAN invité obtiennent ancré au DMZ WLC afin d'obtenir authentifié et obtenir une adresse IP.
- Assurez-vous que les paramètres SSID et d'authentification sont configurés exactement la même chose sur chacun des deux le WLCs.
- Assurez-vous que les DMZ et les gens du pays WLC dans le réseau câblé sont accessibles. Employez les pings de mobilité (**eping** et **mping**) pour tester.Ping de mobilité au-dessus d'UDP ? Ce essais au-dessus du port UDP 16666 de mobilité et des tests si le paquet de contrôle de mobilité peut être atteint au-dessus de l'interface de gestion.**mobility_peer_IP_address de mping**Ping de mobilité au-dessus d'EoIP ? Ce essais au-dessus d'EoIP - Le port 97 IP et teste le trafic de données de mobilité au-dessus de l'interface de gestion.**mobility_peer_IP_address d'epingRemarque:** Seulement un test de ping de mobilité par contrôleur peut être exécuté à un moment donné.
- S'il y a un présent de Pare-feu, assurez-vous que le port UDP 16666 et le port 97 IP sont ouverts pour la transmission entre le WLCs.

## Authentification client

L'authentification Web est la méthode d'authentification typiquement utilisée pour authentifier des clients dans un réseau d'invité. Les clients peuvent accéder à l'Internet seulement après l'authentification réussie. Même si ils essayent de parcourir avant l'authentification, le WLC réoriente l'utilisateur à la page de connexion d'authentification Web automatiquement, où l'utilisateur obtient authentifié.

Cependant, dans la version 3.2 ou antérieures WLC, le client doit manuellement taper *https://1.1.1.1.html* dans un navigateur Web afin d'obtenir à la page d'authentification Web. Pour

plus d'informations sur l'authentification Web, référez-vous à l'exemple Sans fil de configuration d'authentification Web de contrôleur LAN.

Si la caractéristique ne fonctionne pas comme prévu après que vous configuriez l'authentification Web, exécutez ces étapes de dépannage :

- Pour que l'authentification se produise, le client devrait d'abord s'associer avec le WLAN approprié sur le WLC. Pour plus d'informations sur dépanner cette question, référez-vous à la section de questions de configuration du réseau sans fil unifié : Dépannez le document de questions de client.
- Un bloqueur de Pare-feu ou de popup installé sur l'ordinateur client bloque parfois la page de connexion d'authentification Web, où les utilisateurs entrent dans leurs qualifications d'authentification. Désactivez-les avant que vous essayiez d'accéder à la page de connexion. Ils peuvent être activés de nouveau une fois que l'authentification Web est terminée.
- L'Internet Explorer 6.0 est SP1 ou plus tard le navigateur recommandé pour l'usage de l'authentification Web. D'autres navigateurs pourraient ou ne pourraient pas travailler.
- Désactivez les paramètres de proxy sur le navigateur de client jusqu'à ce que l'authentification Web soit terminée.

Pour plus d'informations sur l'authentification Web de dépannage, référez-vous à la redirection d'authentification Web de dépannage sur le WLC.

## Questions d'adresse IP

N'importe quel client sans fil a besoin d'une adresse IP valide afin de communiquer avec le reste du réseau. Une fois que le client s'associe au WLC, il initie le processus DHCP. Le WLC agit en tant qu'agent de relais et transmet par relais (c'est-à-dire, en avant) cette demande au serveur DHCP et apparaît comme serveur DHCP au client sur son interface virtuelle 1.1.1.1. Le WLC puis en avant l'adresse IP assignée par le serveur DHCP au client et enregistre l'adresse IP dans sa table.

**Remarque:** Le WLC peut également agir en tant que serveur DHCP. Pour plus d'informations sur la façon configurer le WLC en tant que serveur DHCP, référez-vous à la section de configuration DHCP du guide de configuration Sans fil de contrôleur LAN de Cisco, version 6.0.

Exécutez ces contrôles si une adresse IP valide n'est pas obtenue :

- Assurez-vous que l'adresse IP du serveur DHCP est définie correctement et que le serveur DHCP est accessible.
- Assurez-vous que le service DHCP est activé sur le serveur DHCP.
- Assurez-vous que le serveur est configuré avec un pool DHCP pour le VLAN invité de sorte que le serveur puisse assigner des adresses IP de ce VLAN.
- Certains serveurs DHCP ne reçoivent pas des demandes de relais DHCP. Puisque le WLC assure principalement le service de relais aux requêtes DHCP des clients, assurez-vous que le serveur DHCP est installé pour recevoir le service de relais.

Assignez une adresse IP statique du VLAN invité et assurez-vous les travaux de client. Pour plus d'informations sur des questions d'adresse IP de dépannage, référez-vous à la section de questions d'adresse IP du réseau sans fil unifié : Dépannez le document de questions de client.

# Informations connexes

- Exemple de configuration d'un accès invité filaire à l'aide de contrôleurs de réseau local sans fil Cisco
- Accès invité sans fil - Forum Aux Questions
- Réseau sans fil unifié : Dépanner les problèmes des clients
- Support et documentation techniques - Cisco Systems