Accès invité sans fil - Forum Aux Questions

Table des matières

Introduction

Ce document décrit les informations pour les questions les plus fréquemment posées (FAQ) sur la fonctionnalité d'accès invité sans fil, qui fait partie du réseau sans fil unifié Cisco.

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

Qu'est-ce qu'un tunnel Ethernet sur IP (EoIP) vers une zone de réseau non sécurisé ?

Cisco recommande l'utilisation d'un contrôleur dédié au trafic invité. Ce contrôleur est connu comme contrôleur d'ancrage invité.

Le contrôleur d'ancrage invité est habituellement situé dans une zone de réseau non sécurisé, souvent appelée la zone démilitarisée (DMZ). D'autres contrôleurs WLAN internes se trouvant où le trafic est généré se situent dans le réseau local de l'entreprise. Un tunnel EoIP est établi entre les contrôleurs WLAN internes et le contrôleur d'ancrage invité afin d'assurer l'isolement du chemin du trafic invité vis-à-vis du trafic de données de l'entreprise. L'isolement du chemin est une fonctionnalité essentielle de la gestion de la sécurité pour l'accès invité. Il assure que les politiques de sécurité et de qualité de service (QoS) puissent être distinctes et différenciées entre le trafic des invités et le trafic de l'entreprise ou interne.

Une importante fonctionnalité de l'architecture du réseau sans fil unifié Cisco est la capacité d'utiliser un tunnel EoIP pour mapper statiquement un ou plusieurs WLAN équipés (c'est-à-dire, des SSID) vers un contrôleur spécifique d'ancrage invité dans le réseau. Tout le trafic - à destination et en provenance d'un WLAN mappé - traverse un tunnel EoIP statique établi entre un contrôleur distant et le contrôleur d'ancrage invité.

À l'aide de cette technique, tout le trafic invité associé peut être transporté d'une manière transparente à travers le réseau de l'entreprise vers un contrôleur d'ancrage invité qui réside dans la zone de réseau non sécurisé.

Comment est-ce que je sélectionne le contrôleur correct à déployer comme contrôleur d'ancrage invité ?

La sélection du contrôleur d'ancrage invité constitue une fonction du volume du trafic invité tel que défini par le nombre de sessions actives de clients invités ou tel que défini par la capacité d'interface de la liaison ascendante sur le contrôleur, ou les deux.

Les limites de débit total et de clients par contrôleur d'ancrage invité sont les suivantes :

- Contrôleur LAN sans fil Cisco 2504 - 4 interfaces 1 Gbit/s et 1 000 clients invités
- Contrôleur LAN sans fil (WLC) Cisco 5508 - 8 Gbit/s et 7 000 clients invités
- Module de services sans fil (WiSM-2) de la gamme Cisco Catalyst 6500 - 20 Gbit/s et 15 000 clients
- Contrôleur LAN sans fil (WLC) Cisco 8500 - 10 Gbit/s et 64 000 clients

---

Remarque : les WLC Cisco 7500 ne peuvent pas être configurés en tant que contrôleur d'ancrage invité. Référez-vous à Quels contrôleurs peuvent être utilisés pour prendre en charge l'accès invité dans la zone de réseau non sécurisée ? pour la liste des WLC qui prennent en charge la fonction d'ancrage invité.

Un maximum de 2048 noms d'utilisateur et mots de passe invités peut être stocké dans la base de données de chaque contrôleur. Par conséquent, si le nombre total d'informations d'identification d'invité actif dépasse ce nombre, plusieurs contrôleurs sont nécessaires. En alternative, les informations d'identification d'invités peuvent être enregistrées dans un serveur RADIUS externe.

Le nombre de points d'accès dans le réseau n'affecte pas la sélection du contrôleur d'ancrage invité.

Combien de tunnels Ethernet sur IP (EoIP) peuvent-ils être terminés sur un contrôleur d'ancrage d'invités ?

Un contrôleur d'ancrage invité peut terminer jusqu'à 71 tunnels EoIP à partir des contrôleurs WLAN internes. Cette capacité est la même pour tous les modèles du contrôleur LAN sans fil Cisco, à l'exception du WLC-2504. Le contrôleur 2504 peut terminer jusqu'à 15 tunnels EoIP. Plusieurs contrôleurs d'ancrage invité peuvent être configurés si des tunnels supplémentaires sont requis.

Des tunnels EoIP sont comptés par contrôleur WLAN, indépendamment du nombre de WLAN tunnelisés ou de SSID (Secure Set Identifiers) dans chaque EoIP.

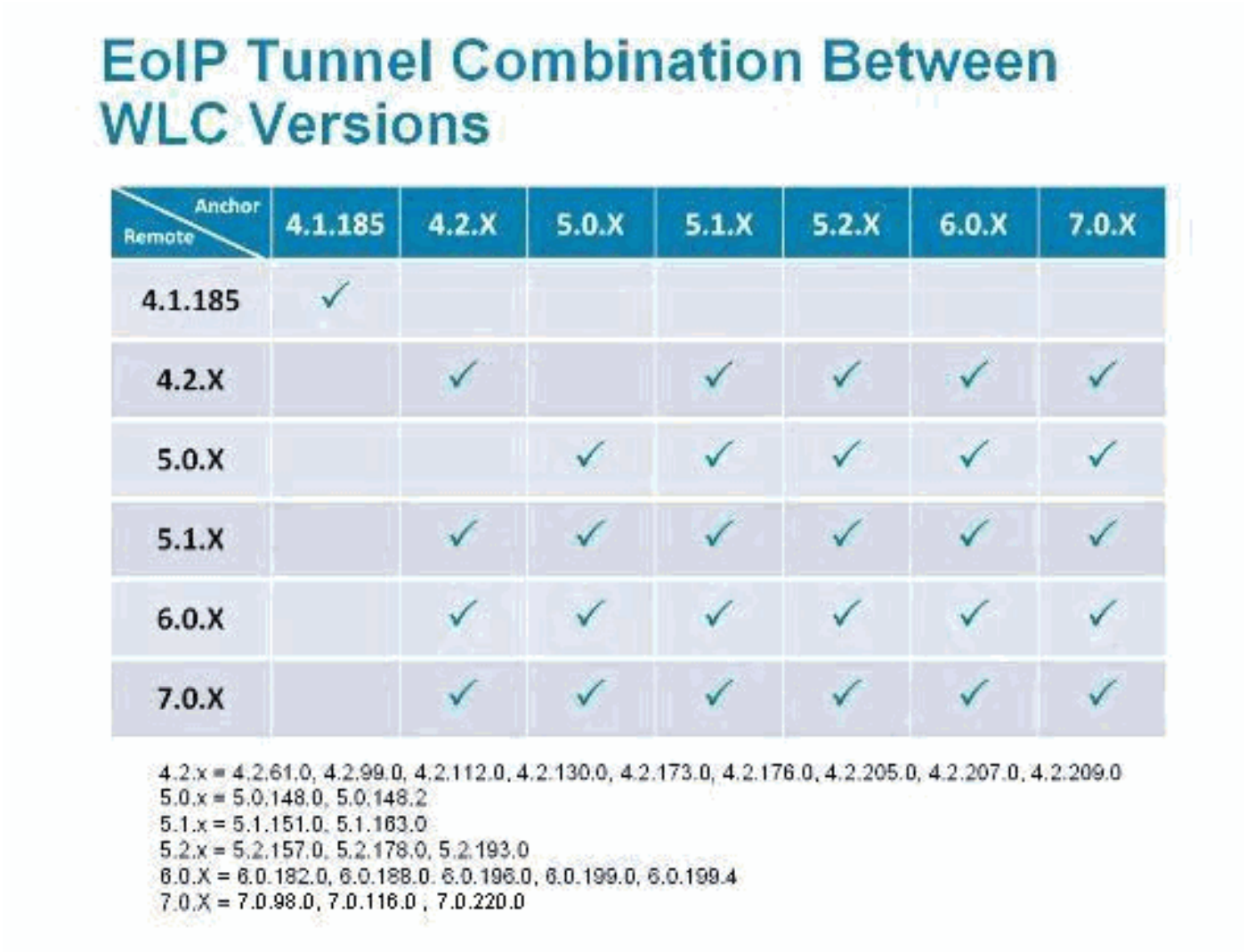
Un tunnel EoIP est configuré entre le contrôleur d'ancrage invité et chaque contrôleur interne qui prend en charge des points d'accès avec des associations de clients invités.

Est-ce que je peux créer des tunnels Ethernet sur IP (EoIP) entre des contrôleurs qui exécutent différentes versions du logiciel ?

Les versions du logiciel du contrôleur de réseau local sans fil ne le prennent pas toutes en charge. Dans ce cas, le contrôleur distant et le contrôleur d'ancrage doivent exécuter la même version du logiciel WLC. Cependant, les récentes versions du logiciel permettent aux contrôleurs d'ancrage et

distants d'avoir différentes versions.

Cette matrice énumère les versions du logiciel du contrôleur de réseau local sans fil avec lesquelles vous pouvez créer les tunnels EoIP.



Le contrôleur de réseau local sans fil de la gamme Cisco 2100/2500 peut-il être utilisé comme contrôleur d'ancrage invité dans la zone de réseau non sécurisé ?

Oui, à partir de la version 7.4 du logiciel Cisco Unified Wireless Network, le contrôleur LAN sans fil de la gamme Cisco 2500 peut interrompre (jusqu'à 15 tunnels EoIP) le trafic invité en dehors du pare-feu. Le contrôleur de réseau local sans fil de la gamme Cisco 2000 peut seulement initier des tunnels d'invités.

Le module contrôleur LAN sans fil Cisco pour routeurs à services intégrés (WLCM ou WLCM2) peut-il être utilisé comme contrôleur d'ancrage invité dans la zone de réseau non sécurisée ?

Non, le WLCM ou le WLCM2 ne peut pas terminer les tunnels invités. Le WLCM peut seulement initier des tunnels d'invités.

Quels contrôleurs peuvent-ils être utilisés pour prendre en charge l'accès invité dans la zone de réseau non sécurisé ?

La fonction d'ancrage du tunnel invité, qui inclut la terminaison du tunnel EoIP, l'authentification Web et le contrôle d'accès des clients invités, est prise en charge dans ces plates-formes de contrôleur LAN sans fil Cisco avec des images logicielles de version 4.0 ou ultérieure :

- Module de services sans fil Cisco Catalyst 6500 (WiSM2)
- Contrôleur LAN sans fil Cisco WiSM-2
- Contrôleur de réseau local sans fil intégré Cisco Catalyst 3750G
- Contrôleur de réseau local sans fil série 5508 de Cisco
- Contrôleur LAN sans fil Cisco 2500 (prise en charge introduite dans la version 7.4 du logiciel)

Si un contrôleur d'ancrage invité est utilisé en dehors du pare-feu, quels ports de pare-feu sont-ils ouverts pour que l'accès invité fonctionne ?

Sur n'importe quel pare-feu entre le contrôleur d'ancrage invité et les contrôleurs distants, ces ports doivent être ouverts :

- Mobilité héritée : protocole IP 97 pour le trafic de données utilisateur, port UDP 16666
- Nouvelle mobilité : ports UDP 16666 et 16667

Pour la gestion facultative, ces ports de pare-feu doivent être ouverts :

- SSH/Telnet - Port TCP 22/23
- TFTP - Port UDP 69
- NTP - Port UDP 123
- SNMP - Ports UDP 161 (gets et sets) et 162 (traps)
- HTTPS/HTTP - Port TCP 443/80
- Syslog - Port TCP 514
- Port UDP d'authentification/compte RADIUS 1812 et 1813

Le trafic invité peut-il passer à travers un pare-feu lorsque la traduction d'adresses réseau (NAT) est configurée ?

Une NAT linéaire doit être utilisée sur le tunnel EoIP passant à travers un pare-feu.

Dans un scénario ancrage - WLC étranger, quel WLC envoie-t-il la gestion des comptes RADIUS ?

Dans ce scénario, l'authentification est toujours effectuée par l'ancrage WLC. Par conséquent, la gestion des comptes de RADIUS est envoyée par l'ancrage WLC.

Remarque : dans un déploiement d'authentification Web centrale (CWA) et/ou de changement d'autorisation (CoA), la comptabilité RADIUS doit être DÉSACTIVÉE sur l'ancre et utilisée uniquement sur le WLC étranger.

Le tunnel des invités entre le contrôleur interne et le contrôleur d'ancrage échoue. Je vois ces journaux dans le WLC : `mm_listen.c:5373 MM-3-INVALID_PKT_RECVD: Received an invalid packet from 10.40.220.18. Source member:0.0.0.0. source member unknown.`. Pourquoi ?

Vous vérifiez l'état du tunnel à partir de la GUI du WLC sur la page des WLAN. Cliquez sur la liste déroulante près d'un WLAN et choisissez Ancres de mobilité , où figure l'état du contrôle et le chemin des données. Le message d'erreur s'affiche pour l'une des raisons suivantes :

1. Les contrôleurs d'ancrage et internes se trouvent sur différentes versions de code. Assurez-vous qu'ils exécutent les mêmes versions du code.
2. Configurations incorrectes dans la configuration de l'ancre de mobilité. Vérifiez que le DMZ est lui-même configuré en tant qu'ancre de mobilité et que les WLC internes ont le DMZ WLC configuré en tant qu'ancre de mobilité. Pour plus d'informations sur la façon de configurer l'ancre de mobilité, reportez-vous à la section Configuration automatique de la mobilité d'ancre duguide de configuration du contrôleur de réseau local sans fil Cisco, version 7.0. En conséquence, les utilisateurs invités ne seraient pas en mesure de transmettre le trafic.

Dans une configuration d'accès invité sans fil, les clients ne reçoivent pas l'adresse IP du serveur DHCP. Le message d'erreur THU Jan 22 16:39:09 2009: XX:XX:XX:XX:XX:XX DHCP Dropping REPLY from Export-Foreign STA s'affiche sur le

contrôleur interne. Pourquoi ?

Dans une configuration d'accès invité sans fil, le paramètre de proxy DHCP dans les contrôleurs d'ancrage invité et le contrôleur interne doit correspondre. Sinon, la requête DHCP des clients est abandonnée et vous voyez ce message d'erreur sur le contrôleur interne :

```
Thu Jan 22 16:39:09 2009: XX:XX:XX:XX:XX:XX  DHCP dropping REPLY from Export-Foreign STA
```

Utilisez cette commande afin de modifier le paramètre de proxy dhcp sur le WLC :

<#root>

```
(Cisco Controller) >
```

config dhcp proxy ?

```
enable          Enable DHCP processing's proxy style behaviour.
disable         Disable DHCP processing's proxy style behaviour.
```

Utilisez la commande show dhcp proxy sur les deux contrôleurs afin de vérifier que les deux contrôleurs ont le même paramètre de proxy DHCP.

<#root>

```
(Cisco Controller) >
```

show dhcp proxy

```
DHCP Proxy Behaviour: enabled

(Cisco Controller) >
```

Si le trafic invité est tunnelisé vers une zone de réseau non sécurisé, où les clients invités obtiennent-ils une adresse IP ?

Le trafic invité est transporté au sein de l'entreprise à la couche 3 via EoIP. Par conséquent, le premier point sur lequel les services de protocole de configuration dynamique d'hôte (DHCP) peuvent être mis en application réside au niveau local, sur le contrôleur d'ancrage invité. Le contrôleur d'ancrage invité peut également relayer des requêtes DHCP de clients vers un serveur externe. Il s'agit également de la méthode à travers laquelle la résolution d'adresse du système de noms de domaine (DNS) est prise en charge.

Le contrôleur de réseau local sans fil Cisco prend-il en charge des portails Web pour l'authentification des invités ?

Les contrôleurs de réseau local sans fil Cisco (version 3.2 ou ultérieure) fournissent un portail Web intégré qui saisit les informations d'identification d'invités en vue de leur authentification et offre des fonctionnalités de marquage simple, conjointement avec la capacité d'afficher l'avis de non-responsabilité ainsi que la politique d'utilisation acceptable.

Comment puis-je personnaliser le portail Web ?

Pour les informations relatives à la façon de personnaliser un portail Web, reportez-vous à Choisir la page de connexion d'authentification Web.

Comment les informations d'identification des invités sont-elles gérées ?

Les informations d'identification des invités peuvent être créées et gérées de manière centralisée à l'aide de Cisco Wireless Control System (WCS) Version 7.0 et/ou de Network Control System (NCS) Version 1.0. Un administrateur de réseau peut établir un compte administratif aux privilèges limités dans WCS qui permet l'accès « lobby ambassador » afin de créer les informations d'identification des invités. Dans WCS ou NCS, la personne disposant d'un compte d'ambassadeur du hall peut créer, attribuer, surveiller et supprimer des informations d'identification d'invité pour le contrôleur servant de contrôleur d'ancrage invité.

Le « lobby ambassador » peut entrer le nom de l'utilisateur invité (ou ID utilisateur) et le mot de passe, les informations d'identification pouvant également être autogénérées. Il y a également un paramètre de configuration globale qui permet l'utilisation d'un nom d'utilisateur et d'un mot de passe pour tous les invités, ou un seul nom d'utilisateur et mot de passe pour chaque invité.

Afin de configurer le compte « lobby ambassador » sur le WCS, reportez-vous à la section Créer des comptes d'utilisateurs invités du guide de configuration du système de contrôle sans fil Cisco, version 7.0.

La fonction « lobby ambassador » est-elle disponible dans le contrôleur LAN sans fil Cisco en plus du système de contrôle sans fil (WCS) ou du NCS ?

Oui. Si le WCS ou le NCS n'est pas déployé, un administrateur réseau peut établir un compte d'ambassadeur de hall sur le contrôleur d'ancrage invité. Une personne qui se connecte au contrôleur d'ancrage invité à l'aide du compte d'ambassadeur du hall a uniquement accès aux fonctions de gestion des utilisateurs invités.

S'il existe plusieurs contrôleurs d'ancrage invité, un WCS ou un NCS doit être utilisé pour

configurer simultanément des noms d'utilisateur sur plusieurs contrôleurs d'ancrage invité.

Pour les informations sur la façon de créer des comptes « lobby ambassador » utilisant des contrôleurs de réseau local sans fil, reportez-vous à la section Création d'un compte « lobby ambassador » du guide de configuration du contrôleur de réseau local sans fil Cisco, version 7.0.

Les invités peuvent-ils être authentifiés à travers une authentification externe, une autorisation et un serveur de gestion des comptes (AAA) ?

Oui. Des demandes d'authentification d'invités peuvent être relayées vers un serveur RADIUS externe.

Que se produit-il quand un invité ouvre une session ?

Quand un invité sans fil se connecte à travers le portail Web, le contrôleur d'ancrage invité prend en charge l'authentification en effectuant ces étapes :

1. Le contrôleur d'ancrage invité vérifie la présence du nom d'utilisateur et du mot de passe dans sa base de données locale et, le cas échéant, accorde l'accès.

2. Si aucune information d'identification des utilisateurs n'est présente localement sur le contrôleur d'ancrage invité, le contrôleur d'ancrage invité vérifie des paramètres de configuration WLAN pour déterminer si un ou plusieurs serveurs externes de RADIUS ont été configurés pour le WLAN invité. Le cas échéant, le contrôleur crée un paquet de demande d'accès RADIUS avec le nom d'utilisateur et le mot de passe et le transfère au serveur RADIUS sélectionné pour l'authentification.

3. Si aucun serveur RADIUS spécifique n'a été configuré pour le WLAN, le contrôleur vérifie les paramètres de configuration globale du serveur RADIUS. Tous les serveurs RADIUS externes configurés avec l'option d'authentification « utilisateur réseau » sont interrogés avec les informations d'identification de l'utilisateur invité. Sinon, si aucun serveur n'a sélectionné « utilisateur réseau » et que l'utilisateur n'a pas été authentifié au cours des étapes 1 ou 2, l'authentification échoue.

Est-il possible d'ignorer l'authentification de l'utilisateur invité et de n'afficher que l'option d'avis de non-responsabilité de la page Web ?

Oui. Une autre option de configuration d'accès invité sans fil est de contourner totalement l'authentification des utilisateurs et de permettre un accès ouvert. Cependant, il pourrait être nécessaire de présenter une page de politique d'utilisation acceptable et d'avis de non-responsabilité aux invités avant de leur concéder l'accès. À cette fin, un WLAN invité peut être configuré pour le passthrough de la politique Web. Dans ce scénario, un utilisateur invité est

redirigé vers une page de portail Web qui contient les informations d'avis de non-responsabilité. Afin de permettre l'identification de l'utilisateur invité, le mode passthrough a également une option pour qu'un utilisateur entre une adresse e-mail avant de se connecter.

Est-il nécessaire que le contrôleur distant et le contrôleur d'ancrage invité se trouvent dans le même groupe de mobilité ?

Non. Le contrôleur d'ancrage invité et le contrôleur distant peuvent se trouver sur des groupes de mobilité distincts.

En présence de plus d'un SSID invité, chaque WLAN (SSID) peut-il être dirigé vers un seul portail de page Web ?

Oui. Tout le trafic invité, sur un ou plusieurs WLAN, sont redirigés vers une page Web. À partir de la version 4.2 ou ultérieure de WLC, chaque WLAN peut être dirigé vers une seule page du portail Web. Reportez-vous à la section Attribution de connexion, échec de connexion et pages de déconnexion par WLAN duguide de configuration du contrôleur de réseau local sans fil Cisco, version 7.0.

Quelle est la fonctionnalité du nouveau paramètre dans le WLC version 7.0, WebAuth sur Mac Filter Failure ?

Si un WLAN a à la fois une sécurité de couche 2 (mac-filter) et de couche 3 (webauth-on-macfilter-failure) configurée, le client passe à l'état RUN si l'un ou l'autre est passé. Et s'il échoue à la sécurité de couche 2 (mac-filter), le client est déplacé à la sécurité de couche 3 (webauth-on-macfilter-failure).

Le client fonctionne-t-il correctement si le navigateur est configuré pour le serveur proxy ?

Avant la version 7.0, le client ne pouvait pas établir de connexion TCP lorsque le serveur proxy était configuré dans le navigateur. Après la version 7.0, cette prise en charge du serveur proxy WebAuth est ajoutée et l'adresse IP et le port du serveur proxy peuvent être configurés sur le contrôleur.

Existe-t-il un guide de déploiement pour l'accès invité sans fil ?

Voici le lien au guide de déploiement :

Guide de déploiement : Cisco Guest Access Using the Cisco Wireless LAN Controller

Existe-t-il un guide de conception pour l'accès invité sans fil ou

câblé ?

Voici les liens vers les guides de conception :

- Services d'accès invité de Cisco sans fil unifié
- Exemple de configuration d'un accès invité filaire à l'aide de contrôleurs de réseau local sans fil Cisco

Informations connexes

- Exemple de configuration d'un accès invité filaire à l'aide de contrôleurs de réseau local sans fil Cisco
- Guide de déploiement : Cisco Guest Access Using the Cisco Wireless LAN Controller, Release 4.1
- Assistance et documentation techniques - Cisco Systems

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

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